Human Factors in Web Authentication

Chris K. Karlof

Electrical Engineering and Computer Sciences
University of California at Berkeley

Technical Report No. UCB/EECS-2009-26
http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-26.html

February 6, 2009

Human Factors in Web Authentication

by

Chris K. Karlof

B.S. (North Carolina State University) 1995

A dissertation submitted in partial satisfaction of the
requirements for the degree of
Doctor of Philosophy

in

Computer Science

in the

GRADUATE DIVISION
of the
UNIVERSITY OF CALIFORNIA, BERKELEY

Committee in charge:
Professor Doug Tygar, Co-Chair
Professor David Wagner, Co-Chair
Professor Schmuel S. Oren

Spring 2009

The dissertation of Chris K. Karlof is approved:

Co-Chair Date

Co-Chair Date

Date

University of California, Berkeley

Spring 2009

Human Factors in Web Authentication

Portions of this work drawn with permission from [68, 69, 70]:

Chris Karlof, Umesh Shankar, J.D. Tygar, and David Wagner. "Dynamic Pharming Attacks and Locked Same-origin Policies for Web Browsers." In *Proceedings of the Fourteenth ACM Conference on Computer and Communications Security (CCS 2007)*, pages 58-71, October 2007.

Chris Karlof, J.D. Tygar, and David Wagner. "A User Study Design for Comparing the Security of Registration Protocols." In *Proceedings of the First USENIX Workshop on Usability, Psychology, and Security (UPSEC 2008)*, April 2008.

Chris Karlof, J.D. Tygar, and David Wagner. "Conditioned-safe Ceremonies and a User Study of an Application to Web Authentication," In *Proceedings of the Sixteenth Annual Network and Distributed Systems Security Symposium (NDSS 2009)*, February 2009.

Abstract

Human Factors in Web Authentication

by

Chris K. Karlof
Doctor of Philosophy in Computer Science

University of California, Berkeley

Professor Doug Tygar, Co-Chair

Professor David Wagner, Co-Chair

This dissertation endeavors to improve the security of user authentication on the World Wide Web. One threat to Web authentication is *phishing*, a social engineering attack that solicits users' authentication credentials by spoofing the login page of a trusted Web site. We identify human psychological tendencies that make users susceptible to phishing attacks and apply these insights to develop design principles for *conditioned-safe ceremonies*. Conditioned-safe ceremonies are security protocols that deliberately condition users to reflexively act in ways that protect them from attacks. Our formulation of conditioned-safe ceremonies draws on several ideas and lessons learned from the human factors and human reliability community: forcing functions, defense in depth, and the use of human tendencies, such as rule-based decision making.

We apply these principles to develop a conditioned-safe ceremony based on email for initializing credentials in machine authentication schemes. We evaluated our email ceremony with a user study of 200 participants. We simulated attacks against the users and found that our email ceremony was significantly more secure than a comparable one based on challenge questions. We found evidence that conditioning helped the email users resist attacks, but contributed towards making challenge question users more vulnerable.

We also address stronger social engineering threats against Web authentication, e.g., pharming. We describe a new attack against Web authentication we call *dynamic pharm-*

ing. Dynamic pharming works by hijacking DNS and sending the victim's browser malicious Javascript, which then exploits DNS rebinding vulnerabilities and the name-based same-origin policy to hijack a legitimate session after authentication has taken place. To resist dynamic pharming attacks, we propose two *locked same-origin policies* for Web browsers. In contrast to the legacy same-origin policy, which enforces access control in browsers using domain names, the locked same-origin policies enforce access control using servers' X.509 certificates and public keys. We evaluate the security and deployability of our approaches and show how browsers can deploy these policies today to substantially increase their resistance to pharming attacks and provide a foundation for the development of pharming resistant authentication mechanisms.

Professor Doug Tygar
Dissertation Committee Co-Chair

Professor David Wagner
Dissertation Committee Co-Chair

Contents

List of Figures **iv**

List of Tables **v**

1 Introduction **1**

1.1 Conditioned-safe ceremonies 3

1.2 Securing machine authentication 4

1.2.1 The registration problem 5

1.2.2 Dynamic pharming attacks and the locked same-origin policies . . . 6

2 Preliminaries **9**

2.1 Background 9

2.1.1 HTTP cookies 9

2.1.2 The legacy same-origin policy 10

2.1.3 Secure Sockets Layer (SSL) and X.509 certificates 11

2.2 Threat models 12

2.2.1 Phishers 12

2.2.2 Pharmers 13

2.2.3 Active attackers 14

2.2.4 Other assumptions 15

3 Conditioned-safe ceremonies **16**

3.1 Why users are vulnerable 16

3.1.1 Automatic decision making strategies are exploitable 17

3.1.2 Web browser security indicators condition users to satisfice 17

3.1.3 Users are not good at recognizing attacks 18

3.2 Modeling user decision making during attacks 20

3.2.1 Skill, rule, and knowledge based performance 20

3.2.2 Human error and the Generic Error-Modeling System (GEMS) . . . 21

3.2.3 Applying GEMS to user behavior during social engineering attacks 23

3.3 Conditioned-safe ceremonies 24

3.3.1 Forcing functions 25
3.3.2 Analysis and discussion 27
3.3.3 Limitations 29

4 Registration ceremonies **30**
4.1 Current practice: Challenge questions 30
4.2 A conditioned-safe registration ceremony using email 32
4.2.1 Security analysis. 32
4.2.2 Implications and limitations of email based registration 34

5 A user study of registration ceremonies **36**
5.1 Design challenges 36
5.2 Study design 38
5.2.1 Overview 38
5.2.2 Recruitment 39
5.2.3 Registration procedures 40
5.2.4 Simulated attacks 46
5.2.5 Warnings 47
5.2.6 Attack success metrics 47
5.2.7 Debriefing and exit survey 48
5.2.8 Ethics 48
5.3 Study results 49
5.3.1 User demographics 49
5.3.2 Success of simulated attacks 52
5.3.3 Efficacy of our warnings 52
5.3.4 User suspicion of our attacks 54
5.3.5 User reasoning during our attacks 56
5.3.6 Usability and security opinions of registration mechanisms 58
5.3.7 Ecological validity 58
5.4 Analysis and discussion 62
5.4.1 Ineffectiveness of our warnings 62
5.4.2 Lack of user suspicion 63
5.4.3 The power of user conditioning and forcing functions 64
5.4.4 Ecological validity 66
5.4.5 Study limitations 67

6 Dynamic pharming attacks **70**
6.1 Overview 70
6.2 Attack details 73
6.2.1 Method 1: Proxying 73
6.2.2 Method 2: DNS rebinding 73
6.2.3 Discussion 76

6.2.4 Proof of concept implementation 77
6.3 Library import and data export pharming vulnerabilities 77

7 The locked same-origin policies 79
7.1 The weak locked same-origin policy 81
7.2 The strong locked same-origin policy 81
7.3 Security analysis 83
7.3.1 Weak locked same-origin policy 83
7.3.2 Strong locked same-origin policy 84
7.4 Deployability analysis 85
7.4.1 An SSL server survey 85
7.4.2 Certificate chain validation: Firefox and IE 86
7.4.3 Evaluation results 88
7.5 Policy files for supporting multiple keys and key updates 90
7.6 Support for subdomain object sharing 92
7.7 Support for library import and data export 93
7.7.1 With the weak locked same-origin policy 93
7.7.2 With the strong locked same-origin policy 95
7.8 Caching 95
7.9 Limitations 95
7.10 Applications to Web authentication 96
7.10.1 Client-side SSL 96
7.10.2 SSL-only cookies 97
7.10.3 Other authentication mechanisms 97

8 Related work 98
8.1 Anti-phishing mechanisms 98
8.2 Phishing and pharming resistant authentication 98
8.3 Key Continuity Management and applications 100
8.4 DNS rebinding 100
8.5 Email for authentication 101
8.6 Studies that attack users 101
8.7 User conditioning and education 102

9 Conclusion 104

Bibliography 106

A User study exit survey questions 121

B User study exit survey responses 128

List of Figures

5.1 **User interface for making predictions at our study Web site.** 39
5.2 **User interface for confirming registration.** 42
5.3 **User interface for setting up challenge questions.** 42
5.4 **Normal challenge questions interface vs. simulated attack instructions.** 43
5.5 **Registration emails.** 44
5.6 **Our simulated attacks against email registration.** 45

6.1 **An example of a dynamic pharming attack.** (1) Initially, the pharmer arranges for the victim's DNS queries for www.vanguard.com to resolve to the pharmer's IP address, 6.6.6.6. (2) Then, when the victim visits www.vanguard.com, the pharmer returns a trojan document containing malicious Javascript and a iframe referencing Vanguard's home page. (3) The pharmer then updates the DNS entry for www.vanguard.com to the IP address of Vanguard's legitimate server and denies subsequent connections from the victim. (4) This causes the victim's browser to renew its DNS entry for www.vanguard.com, and (5) load Vanguard's legitimate home page in the iframe. (6) After the user authenticates herself, the malicious Javascript in the trojan document hijacks her session with the legitimate server. 71
6.2 **Dynamic pharming attack document.** 72

List of Tables

5.1 **Summary of study groups.** 40

5.2 **User demographics by group number.** Some percentages may not add to 100% due to rounding. 50

5.3 **User demographics by group number.** Some percentages may not add to 100% due to rounding. 51

5.4 **Success rates of our simulated attacks against registration procedures in our user study.** Users in groups 2 and 4 received contextual warnings in registration emails against our simulated attacks, but users in groups 3 and 5 did not. 53

5.5 **Number of users who reported remembering seeing our warnings.** . . 54

5.6 **Effect of warning recall on resisting our simulated attacks.** Of the 200 users in our study, 9 users did not respond to this question. 54

5.7 **Self-reported effects of our warnings on users who remembered seeing them.** 55

5.8 **Users' opinions of the security benefits of registration.** 59

5.9 **Users' opinions of the convenience of registration.** For space constraint reasons, some of the answer choices have been shortened. Refer to Appendix A for the full text of the answer choices. 60

5.10 **Risk ratings.** This table summarizes how thoroughly and often the users reported applying security precautions when logging into various types of Web sites. 61

7.1 **Comparison of our locked same-origin policies with the legacy same-origin policy.** This table shows the strongest threat model under which each policy can isolate a legitimate server's Web objects (e.g., cookies, HTML documents, etc.) from adversaries. *Locked Web objects* refer to objects retrieved over SSL. *Shared locked Web objects* refer to objects retrieved over SSL which are intended to be shared among subdomains of a higher-level domain (e.g., domain cookies). *Untrusted certs* refer to a legitimate server using a self-signed certificate or a certificate issued by a root CA untrusted by browsers. 82

7.2 **Summary of browser mechanisms used to address missing and expired intermediate CA certificates.** AIA refers to the optional Authority Information Access X.509 extension. 87

7.3 **Summary of our deployability analysis of the locked same-origin policies using a sample of 14651 SSL domains.** This table shows the percentage of domains in our survey which may not correctly interoperate with the locked same-origin policies. 89

Acknowledgments

It is a pleasure to thank the many people who made this thesis possible.

I owe immense gratitude to my advisers, Doug Tygar and David Wagner. Doug and David co-advised me, and they made my studies at Berkeley enlightening, fruitful, and enjoyable. Doug and David time and again removed obstacles of all types to help keep me focused on my research. Their advice was complementary and insightful, and rarely conflicted. Doug taught me how to pick interesting and rewarding research problems, and repeatedly helped me uncover the "bigger picture" when I became too focused on the details. David listened patiently to my unrefined and flawed ideas, and helped me polish them into the final works I am now proud of. Most of all, I am thankful to Doug and David for continually improving my writing skills. I could not have had a better experience as a graduate student.

I am indebted to my many fellow graduate students and other colleagues for providing a stimulating and fun environment in which to learn and grow. I particularly would like to thank Yaping Li, Adrian Perrig, Dawn Song, Adam Barth, Rachna Dhamija, Kamin Whitehouse, AJ Shankar, Marco Barreno, David Molnar, Adrian Mettler, and Karl Chen. I am especially grateful to my frequent co-authors, Naveen Sastry and Umesh Shankar. We learned many things together, and I was lucky to have the opportunity to collaborate with them.

I would like to thank the many funding agencies who helped make my work at Berkeley possible: the Defense Advanced Research Projects Agency, the National Science Foundation, the US Postal Service, the iCast Project, the Army Research Office, Bosch, Intel, KDD, and Honda.

I can not end without graciously thanking my family, John, Gidget, and Kristie, and my loving partner, Monica Chew. My family has been a solid and reliable source of support my entire life, and without them, I would have not accomplished nearly as much as I have. My partner Monica deserves my deepest gratitude. She is a tremendous source of love, joy, soothing, encouragement, and insight, and gently helped me navigate the many potholes and bumps on the road to graduation.

Chapter 1

Introduction

This dissertation argues that since computer security mechanisms can have strong effects on users' behavior and choices, we must judiciously design these mechanisms such that human psychological tendencies help users resist attacks, rather than make them more vulnerable, as many current mechanisms do. Our focus is on user authentication schemes on World Wide Web. Despite the development of numerous cryptographic authentication mechanisms, user authentication on the World Wide Web remains firmly saddled in the 1970s: the vast majority of users authenticate themselves to Web sites by sending a plaintext password over the network. Although widespread deployment of the Secure Sockets Layer (SSL) helps protect password authentication against passive eavesdropping attacks, it does little to help users resist more devious threats, such as *phishing* [6]. A phishing attack is a type of social engineering attack, where an adversary lures an unsuspecting Internet user to a Web site posing as a trustworthy business with the goal of stealing sensitive personal information, e.g., the user's password. Phishers commonly lure victims by sending an email containing a warning about a "problem" which requires immediate attention, along with a link the user can click to take action. If a user clicks on the link, she will reach the phishing site. A phishing attack typically prompts the user to enter some personal information, such as a login name, password, or social security number, before the "problem" with her account can be addressed. Phishing attacks have become widespread over the last decade, and their success has created a multi-million dollar underground economy [33, 117]. Our goal is to develop authentication mechanisms resistant to phishing and other social engineering attacks that target users' Web accounts.

One explanation for the success of phishing attacks is a human psychological tendency to develop automatic responses to situations we encounter more than once. Our brains tend to classify stimuli according to a few key features, and if one or more features match stimuli we have encountered in the past, we often respond mindlessly with the action that we learned was most appropriate. Psychologist Robert Cialdini calls these *click-whirr* responses [16]. Cialdini compares these automatic responses to pre-recorded tapes in our head, and uses "click-whirr" to evoke the sound a tape machine makes after pressing "play". As the world becomes more intricate and variable, we increasingly rely on click-whirr responses. Without click-whirr responses, we would spend most of our time appraising and analyzing mundane situations in our daily lives. Philosopher Alfred North Whitehead recognized this when he asserted "civilization advances by the extending the number of operations we can perform without thinking about them [131]."

As we become more dependent on click-whirr responses to navigate our daily lives, some have learned to exploit this behavior. Stored schemas of past recollections and sensory inputs tend to only contain evidence of how a previously encountered situation *should* appear – they rarely store information about how that situation *should not* appear [100]. Salesman, fund raisers, and con men can create situations containing the stimuli necessary to trigger the desired click-whirr response, even though less visible features may differ substantially from past situations. For example, people tend to obey a person in a uniform, regardless of whether that person has any real authority.

The designers of many current Web authentication mechanisms, such as passwords, have all but ignored this fundamental psychological phenomenon. The most common Web authentication technique in use today is password authentication via an HTML form, where a user types her password directly into a Web page from the site to which she wishes to authenticate herself. Social engineering attacks on the Internet, such as phishing, have largely been successful because the Web is fertile ground for mimicry, and password authentication can condition users to fall for these attacks. Since a wide range of Web sites require a user to log in before she can do something interesting, many users have developed a click-whirr response to login forms and will automatically enter their login credentials on any page which on the surface appears familiar, legitimate, or trustworthy.

This dissertation makes two main contributions to the development of Web authentication mechanisms that resist phishing and other social engineering attacks. First, we introduce the notion of a *conditioned-safe ceremony*, a new approach for developing user-centric authentication and security mechanisms. Second, we address two security issues with *machine authentication*, a procedure that authenticates a user's computer, as opposed to herself. We discuss these contributions further in the following sections.

1.1 Conditioned-safe ceremonies

Web authentication is an example of a *ceremony*. A ceremony is similar to the conventional notion of a network protocol, except that a ceremony explicitly includes human participants as nodes in the network, distinct from the computers and devices they use [29].[1] Communications between human nodes and other nodes in the ceremony are usually not via network connections, but instead through user interfaces, face-to-face interactions, or peripheral devices.

Although current Web authentication ceremonies, such as password authentication, are vulnerable to attacks that exploit human psychological tendencies such as click-whirr responses, we argue that these tendencies are not something that we necessarily must avoid or suppress in ceremony design. Instead, in Chapter 3, we hypothesize that we can build ceremonies that turn the tables on adversaries and take advantage of these psychological tendencies to help users resist social engineering attacks. We identify several ways in which many current security mechanisms and ceremonies have disregarded human tendencies, and present a model for user behavior during social engineering attacks based on psychological research on human performance and error, such as Jens Rasmussen's skill-rule-knowledge framework [99] and James Reason's Generic Error-Modeling System [100]. Based on this model, we introduce the notion of a *conditioned-safe ceremony*. A conditioned-safe ceremony is one that deliberately conditions users to reflexively act in ways that protect them from attacks. Many existing ceremonies require users to make difficult and subtle security decisions or respond to exceptional situations to resist attacks. In

[1] The term *ceremony* was first coined for this purpose by Jesse Walker [29].

contrast, if a user of a conditioned-safe ceremony simply performs the same actions during an attack as she usually performs under normal conditions, she will resist – even if she is unaware of the threat. Our formulation of conditioned-safe ceremonies in Section 3.3 draws on several ideas and lessons learned from the human factors and human reliability community: forcing functions, defense in depth, and the use of human tendencies, such as rule-based decision making.

1.2 Securing machine authentication

To address the precipitous rise in social engineering attacks on the Internet, the Federal Financial Institutions Examination Council declared in October 2005 that passwords alone are "inadequate for high-risk transactions" [20]. In response, many institutions use *machine authentication*, which authenticates a user's *computer*, in addition to password authentication, which authenticates the user herself. For example, one widely used approach for machine authentication is to set a persistent cookie; since the user's browser will send that cookie every time the user returns to the Web site from that computer, the Web site can recognize the user's computer. To successfully log in, the user must provide her password and the user's browser must present a valid cookie. The intention is to take the human "out of the loop" and reduce the system's dependency on humans' abilities to detect attacks. Web sites currently using machine authentication include Bank of America [9], ING Direct [52] and Vanguard [123].

One potential advantage of machine authentication is that it increases the difficulty of social engineering attacks against users' accounts. The problem with password authentication is that it is too easy for users to reveal their passwords to phishers and other adversaries. In one standard classification of authentication schemes, passwords are "something you know"; but the problem with using "something you know" for authentication is that anything the user knows, she can—and in a nontrivial fraction of cases, will—reveal to an adversary. Instead, machine authentication relies on "something your computer knows." This is roughly equivalent to "something you have," except implemented in software, without requiring the physical hardware tokens normally used to fill that role.

To compromise a user's account, an attacker not only needs to phish the user's password, but must also steal the user's authentication cookie. Although simply requesting a user's password has proven to be a relatively successful attack, pilfering a user's cookie from her machine is not as straightforward; computers are not fooled by social engineering attacks. Browsers automatically determine the appropriate cookies for Web requests and require little to no user involvement to make security decisions, reducing the chance of human error.

We address two security issues with machine authentication: 1) initializing machine authentication credentials on users' computers, i.e., the *registration problem*, and 2) securing machine authentication against stronger threat models, such as pharming and active attackers.

1.2.1 The registration problem

Since users may use more than one computer, machine authentication systems must have a *registration* ceremony to authorize and set authentication cookies on multiple machines. Unfortunately, this additional functionality potentially brings the human back "in the loop" and exposes machine authentication systems to an alternative attack vector. Instead of trying to steal authentication cookies directly from a user's machine, an attacker can try to subvert the registration ceremony in a way that grants the attacker a valid cookie for the user's account. Consequently, registration ceremonies must resist these kinds of bootstrapping attacks.

Many machine authentication systems currently deployed by financial Web sites use *challenge question* based registration [9, 52, 123]. A challenge question is a user-specific question to which an adversary is unlikely to be able to guess an answer, e.g., "What is the name of your favorite teacher?" [30, 65]. Registration based on challenge questions is vulnerable to man-in-the-middle (MITM) attacks [113, 144]. Since these attacks exploit similar human tendencies as attacks against passwords, the security benefits of challenge questions over passwords alone may be minimal.

An email-based registration ceremony. We apply our design principles for conditioned-safe ceremonies to develop a registration ceremony for machine authentication based on email (Section 4.2). When a user attempts to log in from an unregistered computer, the Web site sends her an email containing a single-use HTTPS URL. When the user clicks on the registration link, the Web site sets a persistent authentication cookie on the user's computer. For subsequent logins from that computer, she only needs to complete any supplementary login procedures, e.g., enter her username and password. We discuss email-based registration further in Section 4.2.

A user study of registration ceremonies. To evaluate our email based registration ceremony, we conducted a user study with 200 participants to compare the security of email registration to the security of registration based on challenge questions (Chapter 5). We designed our study to be as ecologically valid as possible: we employed deception, did not use a laboratory environment, and attempted to create an experience of risk. We simulated social engineering attacks against the users and found email based registration was significantly more secure against our attacks (Table 5.4). Our simulated attacks succeeded against 93% of challenge question users, but succeeded against only 41% of email users. We also found evidence that conditioning helped email registration users resist our simulated attacks, but contributed towards making challenge question users more vulnerable. We asked users to complete an exit survey after they finished the study, and we analyze the results in Sections 5.3 and 5.4.

1.2.2 Dynamic pharming attacks and the locked same-origin policies

Although phishing has been one of the most prevalent types of social engineering attacks on the Web, stronger attacks, such as *pharming*, are a growing threat [4, 66, 97, 115, 120, 121]. In a *pharming* attack [91], the adversary subverts the domain-name lookup system (DNS), which is used to resolve domain names to IP addresses. In this attack, the DNS infrastructure is compromised so that DNS queries for the victim site's domain (say, `google.com`) return an attacker-controlled IP address. Pharming attacks are particularly devious because the browser's URL bar will display the domain name of the site the user intended to visit.

Dynamic pharming attacks. We describe a new type of DNS attack against Web authentication we call *dynamic pharming*. In a dynamic pharming attack, the adversary initially delivers a Web document containing malicious Javascript code to the victim, and then forces the victim's browser to connect to the legitimate server in a separate window or frame. The adversary waits for the victim to authenticate herself to the legitimate server, and then uses the malicious Javascript to hijack the victim's authenticated session.

Dynamic pharming takes advantage of how browsers currently implement the *same-origin policy*. The same-origin policy prohibits a Web object from one site from accessing Web objects served from a different site. Browsers currently enforce this by checking that the two objects' originating domain names, ports, and protocols match. However, when an adversary controls the domain name mapping, the legacy same-origin policy does not provide strong isolation between Web objects co-executing in a user's browser. In a dynamic pharming attack, malicious Javascript from the pharmer and content from the legitimate server both appear to have the same "origin" (i.e., same domain, port, and protocol), and the browser allows the Javascript to access to the user's authenticated session. As a result, the attacker can gain complete control of the session, enabling her to eavesdrop on sensitive content, forge transactions, sniff secondary passwords, etc. Since dynamic pharming hijacks users' sessions after authentication completes, irrespective of the authentication mechanism, it can be used to compromise even the strongest Web authentication schemes currently known, including all forms of machine authentication. We present dynamic pharming in more detail in Chapter 6.

The locked same-origin policies. Since dynamic pharming hijacks a user's session after initial authentication completes, it is unlikely any future Web authentication ceremony developed for currently deployed browsers will resist dynamic pharming either. To resist dynamic pharming, we address the root of the problem: we upgrade the browser's same-origin policy. We propose two *locked same-origin policies*: instead of comparing domain names to enforce access control, our policies enforce access control for Web objects retrieved over SSL by using servers' public keys and X.509 certificates. We refer to Web objects retrieved over SSL as *locked Web objects* because the browser can clearly associate the public key and X.509 certificate of server hosting the object with the object. Our first proposal, the *weak locked same-origin policy*, isolates a domain's locked Web objects with valid certificate chains from objects with invalid chains. This enables browsers to distinguish a legitimate server using a valid certificate from pharmers using invalid certificates, such as self-signed certificates or certificates with CN/domain mismatches. Our second proposal, the *strong locked same-origin policy*, enforces access control using cryptographic identity, namely Web sites' public SSL keys. In the strong locked same-origin policy, the browser compares the public keys it associates with locked Web objects; access is granted only if they match. In Chapter 7, show how our policies substantially increase browsers' resistance to pharming attacks and provide a solid foundation for developing pharming resistant machine authentication.

We evaluate our policies in terms of deployability, meaning how well they interoperate with existing Web servers. Based on the results of a study of 14651 SSL domains, we found strong evidence that the weak locked same-origin policy can replace the legacy same-origin policy today with minimal risk of breaking existing Web sites (Section 7.4). Although we did not find similar evidence for the strong locked same-origin policy, we propose a simple, incrementally deployable and backwards compatible mechanism for Web sites to opt in using policy files (Section 7.5). To opt in, we propose that a Web site should post a policy file which enables the site to specify how it would like the browser to enforce the strong locked same-origin policy. Policy files also support flexible server configurations and key updates. In contrast to the weak locked same-origin policy, the strong locked same-origin policy has better security properties, is compatible with sites using self-signed or untrusted certificates, and supports subdomain object sharing.

Chapter 2

Preliminaries

2.1 Background

2.1.1 HTTP cookies

HTTP cookies are a general mechanism for Web servers to store and retrieve persistent state on Web clients [94]. When a client makes an HTTP request to a server, the server has the option of including one or more `Set-Cookie` headers in its response. The `Set-Cookie` HTTP header allows several optional attributes. The `expires` attribute indicates when a browser should delete the cookie. If the `expires` attribute is omitted, then the cookie is called a *session cookie* and should be deleted when the user closes the Web browser. Cookies with an `expires` attribute are called *persistent cookies*.

The `domain` attribute specifies the set of HTTP requests for which a browser should include the cookie. For example, if the user requests the URL `http://www.foo.com/index.html`, then a cookie with `domain=foobar.com` or `domain=www.foo.com` would be included with this request, but a cookie with `domain=pics.foo.com` would not. The default value of the `domain` attribute is the host name of the server which generated the cookie response. We refer to a cookie with an explicit `domain` attribute as a *domain cookie* and a cookie which omits it as a *host cookie*.

The `secure` attribute indicates that the browser should only send the cookie over SSL connections. We refer to a cookie including the `secure` attribute as an *SSL-only cookie*.

Javascript may also access cookies through the `document.cookie` property. For this mode of access, Web browsers use the URL of the document executing the Javascript to determine the appropriate cookies.

Recent browsers support more structured persistent storage mechanisms with functionality similar to cookies. Some browser plugin architectures also provide persistent storage mechanisms, e.g., Adobe Flash and Google Gears.

2.1.2 The legacy same-origin policy

The same-origin policy (SOP) in Web browsers governs access control among different Web objects and prohibits a Web object from one origin from reading or modifying Web objects from a different origin [87]. By Web objects, we mean HTTP cookies, HTML documents, images, Javascript, CSS files, XML files, etc. A common example of "access" is Javascript referencing another object. In the remainder of this dissertation, we will use "SOP" as an abbreviation for "same-origin policy".

Browsers currently consider two objects to have the same origin if the originating host, port, and protocol are the same for both Web objects. A Web object can read and modify another object only if they have the same origin. For example, Javascript executing on `http://www.foo.com/index.html` is allowed to read and modify `http://www.foo.com/other.html`, but is not allowed to access `https://www.foo.com/secure.html` (different protocol) or `http://www.xyz.com/index.html` (different host). Other examples of "Web object accesses" subject to the SOP include determining which cookies to append to an HTTP request, Javascript `document.cookie` references, and XMLHTTPRequest.

Note there is a distinction between "access" and "causing to load". After the browser receives an HTML page, it processes dependent requests necessary to render the page, such as images, style sheets, etc. These requests can cause the browser to fetch and load a Web object from a different domain. However, these requests are not considered violations of the SOP. The document can read certain metaproperties of the object (e.g., height, width), but the SOP prevents the document from reading or modifying the content of the loaded object.

2.1.3 Secure Sockets Layer (SSL) and X.509 certificates

The Secure Sockets Layer (SSL) and its successor, Transport Layer Security (TLS), are cryptographic protocols for establishing end-to-end secure channels for Internet traffic [34, 119]. HTTP over SSL is also known as HTTPS.

SSL uses X.509 certificates [50] to identify the server participating in the SSL connection. An X.509 certificate contains the server's public key, the domain name of the Web site (specified in the `CN` subfield of the certificate), the public key of the issuer of the certificate, the time period for which the certificate is valid, and the issuer's signature over these fields. The private key corresponding to a X.509 certificate can be used to sign another certificate, and so on, creating a chain of trust. The root of this trust chain is typically a certificate authority (CA); Web browsers ship with the certificates of some CAs that are deemed to be trusted.

When the client's Web browser makes a connection to an SSL enabled Web server over HTTPS, the browser must verify the server's certificate is valid. This involves numerous checks, but at a high level the browser must:

- Verify that every certificate in the chain has a valid signature from its predecessor, using the public key of the predecessor, and that the last certificate in the chain is from a trusted CA.

- Verify that the `CN` field of the first certificate in the chain matches the domain name of the Web site the browser intended to visit.

- Verify every certificate has not expired.

If any of these checks fail, the browser warns the user and asks the user if it is safe to continue. If the user chooses, the user may permit the SSL connection to continue even though any or all of these checks have failed. The reason is to ensure compatibility with misconfigured certificates and SSL servers. Also, this behavior by browsers allows Web sites to use self-signed certificates if they choose, instead of paying a CA for a certificate. Unfortunately, asking users whether to continue in such cases is a serious security vulnerability. Researchers have shown that users routinely ignore such security warnings and just click “OK” [11, 24, 135]. In fact, users have become so ambivalent to security warnings, one vendor has developed “mouse auto-clicker” software, aptly titled “Press the Freakin Button” [95], to automatically click through dialogs like these. Instead of a dialog box, IE 7.0 and Firefox 3 use a full page warning within the browser window offering similar options (i.e., accept certificate and continue, or cancel connection), although bypassing the Firefox 3 warning requires several steps. Unfortunately, studies and anecdotal evidence suggest that users will ignore a full page warning as well [12, 108]. Accordingly, we consider a certificate that does not generate any warnings as *valid*. Otherwise, we consider it *invalid*.

After the browser validates the server’s certificate, it participates in a cryptographic protocol with the server where: 1) the server proves knowledge of the private key corresponding to the public key in the certificate, and 2) they negotiate a session key to encrypt and authenticate subsequent traffic between them. Unlike the certificate validation step, if there are any errors in this protocol, the browser closes the connection with no chance of user override.

Client-side SSL. The most common usage of SSL is for server authentication, but in the SSL specification, a server can also request client-side authentication, where the client also presents an X.509 certificate and proves knowledge of the corresponding private key. Using client-side SSL, servers can identify a user with her SSL public key and authenticate her using the SSL protocol.

2.2 Threat models

We consider three broad classes of adversaries, classified according to their capabilities.

2.2.1 Phishers

Phishing is a social engineering attack in which an adversary lures an unsuspecting Internet user to a Web site posing as a trustworthy business with which the user has a relationship [6]. The broad goal is identity theft; phishers try to fool Web visitors into revealing their login credentials, sensitive personal information, or credit card numbers with the intent of impersonating their victims for financial gain. Phishers commonly lure victims by sending an email containing a warning about a "problem" which requires immediate attention, along with a link the user can click to take action. If a user clicks on the link, she will reach the phishing site. Typically a phishing attack prompts the user to enter some personal information, such as a login name, password, or social security number, before the "problem" with her account can be addressed. We assume a phisher has the following capabilities:

- Complete control of a Web server with a public IP address. We assume a phisher uses a different domain name from the target domain.
- The ability to send communications such as emails and instant messages to potential victims.
- Mount application-layer man-in-the-middle attacks, representing a legitimate server to the victim and proxying input from the victim to the real server as needed.

There have been relatively few documented cases of application-layer man-in-the-middle attacks [7, 127, 128], most likely because of the extra effort required to implement the attack. However, researchers have discovered a "Universal Man-in-the-Middle Phishing Kit" [75], a hacker toolkit which enables a phisher to easily set up a MITM proxy attack against any site she wishes.

To date, phishers have been the most prevalent class of attacker; however, looking to the future, stronger attackers are a growing threat [4, 66, 97, 115, 120, 121], and it seems prudent to defend against these more powerful attackers as well, to the extent possible. We discuss these stronger threat models next.

2.2.2 Pharmers

In a *pharming* attack [91], the adversary subverts the domain-name lookup system (DNS), which is used to resolve domain names to IP addresses. In this attack, the DNS infrastructure is compromised so that DNS queries for the victim site's domain (say, google.com) return an attacker-controlled IP address. We assume a pharmer has all the abilities of a phisher, plus:

- The ability to change DNS records for the target site, such that the victim will resolve the target site's name to the attacker's IP address.

We assume the server under the pharmer's control does not have the same IP address as the victim and cannot receive packets destined to the victim's IP address.

Pharming can be accomplished via several techniques, including DNS cache poisoning, DNS response forgery, modifying a user's /etc/hosts file, tricking a user to modify her DNS settings, or by social engineering attacks against a domain name registry. Pharming attacks are particularly devious because the browser's URL bar will display the domain name of the legitimate site, potentially fooling even the most meticulous users.

Although pharming attacks have been relatively rare in practice, evidence suggests they may become a more serious threat in the near future. Recent research has exposed complex and subtle dependencies between names and name servers [97] and weaknesses in the DNS protocol [66], suggesting the DNS infrastructure is more vulnerable to DNS poisoning attacks than previously thought.

2.2.3 Active attackers

We assume an active attacker has all the abilities of a pharmer, plus

- The ability to modify, re-route, drop, and delay all traffic to and from the victim's IP address.

- The ability to eavesdrop on all traffic to and from the victim's IP address.

- The ability to mount active, network-layer, man-in-the-middle attacks against the victim.

The ubiquity of public wireless access points and wireless home routers introduces new opportunities for launching active attacks. Users are becoming accustomed to accessing wireless routers in airports, restaurants, conferences, libraries, and other public spaces. Adversaries can set up malicious wireless routers in these areas that offer free Internet access but redirect users to spoofed Web sites [4]. Also, many users leave the default password and security settings on their wireless home routers unchanged [110]. This enables *warkitting* attacks [120, 121], a combination of wardriving and rootkitting, where an adversary maliciously alters a router's configuration over a wireless connection. A related attack is where a malicious Web site serves content that scans a visitor's internal network and compromises home routers with default passwords. After the adversary has compromised the victim's router, she can change the router's settings or overwrite the router's firmware to intercept the victim's traffic [115].

2.2.4 Other assumptions

For the attacks we present in Chapter 6, we assume that many users will ignore certificate warnings. Several studies suggest that users routinely ignore and dismiss such warnings [11, 24, 108, 135]. For the defenses we present in Chapter 7, we assume that attackers do not have access to the target site's server machines or any secrets, such as private keys, contained thereon.

Chapter 3

Conditioned-safe ceremonies

In this chapter, we propose design principles for *conditioned-safe ceremonies*. At the high level, a conditioned-safe ceremony is one that deliberately conditions users to only perform safe actions during social engineering attacks and reflexively respond in ways that thwart attacks. Before discussing conditioned-safe ceremonies in detail, we first examine psychological tendencies that make users vulnerable to social engineering attacks on the Web and model user behavior during attacks with seminal psychological frameworks for human performance and error. In Chapter 4, apply our design principles to develop a conditioned-safe registration ceremony based on email.

3.1 Why users are vulnerable

Over the last decade, the success of Web based social engineering attacks, e.g., phishing, has created a multi-million dollar underground economy, largely by exploiting weaknesses in password authentication and other Web authentication ceremonies [33, 117]. Although it is tempting to blame the success of these attacks on the ignorance of users, researchers have offered an alternative explanation: computer security mechanisms such as passwords and browser security indicators are poorly suited for human use [2, 22, 24, 25, 46, 108, 129].

3.1.1 Automatic decision making strategies are exploitable

A recurring theme in the psychological literature is that humans tend to vastly prefer *rule-based decision making* over more tedious analytical approaches [99, 100]. The theory of rule-based decision making is based on psychological studies that suggest humans tend to learn and aggressively apply problem-solving rules of the form "if (*situation*) then (*action*)" for frequently encountered situations. When a user encounters a problem in a task, she matches the most prominent cues in the environment with the calling conditions of previously learned rules to find most appropriate one to apply.

Although rule-based decision making helps us navigate the minutia of our daily lives and reserve our time and energy for tasks requiring more detailed analysis, adversaries can exploit rule-based decision making in social engineering attacks [16]. Human reliability expert James Reason observed that frequently used rules, i.e., *strong* rules, may be "misapplied in environment conditions that share some common features with the appropriate states, but also possess elements demanding a different set of actions [100]." In other words, a rule which has been frequently useful in the past can become a *strong-but-wrong rule* when the situational cues change subtly. This helps explains why phishing attacks have been so successful. Since a wide range of Web sites require a user to log in before she can do something interesting, many users have developed a rule of the form "if (login form) then (enter username/password)" and will aggressively apply it when they encounter login prompts on Web pages which on the surface appear familiar, legitimate, or trustworthy. We discuss rule-based decision making further in Section 3.2.

3.1.2 Web browser security indicators condition users to satisfice

A frequently recommended defense against phishing attacks is for a user to verify a Web page's domain and SSL certificate before entering her password on that page; otherwise, she might inadvertently reveal her credentials to an attacker. However, research has shown that users often omit these checks [24, 25, 35, 37, 49, 56, 108, 130, 135]. Although some users ignore these indicators because they do not understand them, a more fundamental problem is that browser security indicators condition users to *satisfice*.

Satisficing is a decision-making strategy which means "to accept a choice or judgment as one that is good enough”, i.e., one that both satisfies and suffices [101]. Checking security indicators is easy to skip because it distracts the user from her primary focus, and there are rarely any immediate visible consequences for skipping these checks or rewards for making them. Since the vast majority of a user’s login attempts are probably not under attack (or at least do not obviously appear to be under attack), routinely skipping security checks and ignoring warnings seems deceivingly acceptable. Over time, users learn to quickly and instinctively perform a security task’s required actions (e.g., entering their passwords) and optimize out the optional actions (e.g., checking security indicators, responding to security warnings). Once a user has become conditioned into a satisficed behavior, psychologists have found it is difficult for her to change it, even if she recognizes overwhelming evidence that her behavior is wrong [16].

3.1.3 Users are not good at recognizing attacks

A recurring theme in the field of human reliability and error is that users often have difficulty in recognizing risky or dangerous situations, and as a result, users may be less vigilant of their choices in these situations than they should. For example, in a review of 100 maritime shipping accidents, Wagenaar and Groeneweg concluded: “Accidents do not occur because people gamble and lose, they occur because people do not believe that the accident that is about to occur is at all possible [126].” This suggests that we cannot rely on users’ abilities to detect social engineering attacks and respond appropriately either, and we must design defenses accordingly.

Several human tendencies contribute to this phenomenon. Psychological studies have shown that people are generally poor at evaluating risk and tend to believe they are less vulnerable to risks than others [112]. For example, many people believe they are better than average drivers and they will live longer than the average life expectancy. It stands to reason these tendencies also influence user behavior on the Internet, leading users to believe they are less likely to be the targets of attacks. One might respond that security mechanisms, such as warnings, can raise awareness and help users recognize attacks. However, not only are security tasks rarely users’ primary goal, but they often inhibit users from completing tasks. Security mechanisms often present users with two options: 1) terminate, or 2) proceed insecurely. Task failure is guaranteed by choosing option 1, but the probability of a security compromise is unclear with option 2. Since task failure is unsatisfying, there is a strong incentive to choose option 2. Decades of buggy software have conditioned users to expect errors, failures, and other incomprehensible system behavior, particularly with hastily developed and continually updated Web applications. Users routinely encounter warnings and errors messages, but rarely experience any immediate negative consequences for dismissing them, even during a real attack. This creates the (accurate) impression that false positives are the norm, and actual attacks are rare.

Unfortunately, frequent false alarms and errors may be molding recklessly obstinate users. Studies suggest that once someone adopts a particular belief, e.g., "it's unlikely I would be the victim of an attack", it is hard to change her mind, even in the face of strong disconfirmatory evidence [105]. In the psychology community, this is known as *belief perseverance*. Belief perseverance is often sustained by *confirmation bias* [89], a human tendency to overweight confirming evidence for one's belief and underweight disconfirming evidence. Researchers have observed evidence of confirmation bias in users' strategies for determining a Web site's trustworthiness. Studies suggest users tend to rely more on a Web site's look-and-feel, logos, their past experience at site, and personalized information to determine trustworthiness than standard browser security indicators such as the lock icon or URL bar [24, 25, 32, 59, 135]. Since adversaries can easily spoof look-and-feel, logos, and personalized information, these strategies are not likely to falsify her hypothesis, only confirm it.

Underweighting disconfirming evidence often manifests itself as "explaining away" the inconsistencies [133]. Studies suggest that users will readily "explain away" attack instructions, broken images, strange URLs, and security warnings as errors rather than potential attack cues [24, 25, 28, 135]. Since users have been forced to develop strategies to work around computer system errors, it's understandably tempting for user to interpret potential attack indicators as errors. Instead of having to terminate her task in response to an attack, by reclassifying the attack as an error, she can instead try to "work around" it by complying with the attacker's "helpful" instructions.

3.2 Modeling user decision making during attacks

3.2.1 Skill, rule, and knowledge based performance

To help understand users' decision making processes during social engineering attacks, we look to Jen Rasmussen's seminal skill-rule-knowledge classification of human performance [99]. Rasmussen's skill-rule-knowledge framework has been used within the systems reliability community to model human error [100]. Rasmussen's framework models human performance at three levels: skill-based, rule-based, and knowledge-based. Rasmussen distinguishes performance levels based on whether the user is actively engaged in problem solving. The rule-based and knowledge-based levels are typically associated with problem solving activities, while the skill-based level is not. Behavior at the skill-based level generally encompasses routine and highly practiced sensorimotor actions which require little conscious control after initiation. Although users may employ skill-based actions to achieve local goals in problem solving tasks, skills are primarily invoked during routine and nonproblematic tasks in familiar situations. For example, consider the task of browsing a Web site. To navigate Web pages, a user commonly employs skill-based actions such as clicking URLs and scrolling until she encounters an unexpected problem or new situation.

After identifying the existence of a problem, Rasumessen conjectures that users enter the rule-based level. The rule-based level applies to common, familiar problems for which the user has previously learned a successful solution. A recurring theme in the psychological literature is that humans are aggressive pattern matchers, and when they encounter a problem, they tend to search for a solution by matching prominent cues in the current situation against learned problem-solving rules of the form "if (*situation*) then (*action*)". For example, since many interesting Web sites require authentication, this framework suggests users will quickly learn a rule of the form "if (login form) then (enter username/password)" and aggressively apply it when they encounter login prompts on Web pages. Solutions generated at the rule-based level are analogous to Cialdini's click-whirr responses.

The knowledge-based level only comes into play during novel situations where a solution must be planned online, using conscious analytical processes and stored knowledge.

Operating at the knowledge-based level is expensive; it often requires the user to interrupt her primary task, switch her attention, analyze the situation, form a mental model, and hypothesize and evaluate solutions. While browsing the Web, a user might enter the knowledge-based level if after attempting to log in, she receives an incomprehensible error message or her browser crashes. Psychological studies suggest that human strongly prefer to pattern match and will only resort to detailed analysis at the knowledge-based level after exhausting all potential prepackaged solutions at the rule-based level. Users are often so overwhelmed at the knowledge-based level that problem solving resorts to "sticking their head in the data stream until a recognizable pattern appears", allowing them revert back to the rule-based level [100].

3.2.2 Human error and the Generic Error-Modeling System (GEMS)

The Generic Error-Modeling System (GEMS) is a framework developed by James Reason for understanding human error during decision making and problem solving [100]. GEMS relies heavily on Jen Rasmussen's skill-rule-knowledge framework and categorizes errors according to the performance level at which they occur. Errors at skill-based level are called *slips*, and errors at the rule-based and knowledge-based levels are called *mistakes*. Slips are execution failures, where the user decides on an action, but the resulting action is not what was intended. For example, a user commits a slip if she decides to left click the mouse to follow a HTML link, but accidentally right clicks instead. In contrast, mistakes are planning failures, where the user decides on a course of action, but the action is not appropriate. For example, if a user has different passwords for different Web sites, she commits a mistake if she enters the wrong one.

A frequent cause of rule-based mistakes is the misapplication of a *good* rule, i.e., a rule which has proven itself useful in the past. For example, "if (legitimate looking login form) then (enter username/password)" is usually a good rule in non-adversarial situations; its application allows a user to quickly authenticate herself and continue her primary task with minimal interruption. This rule is also *strong* for many users, meaning that it easily comes to mind due to repeated use. "Gambling" with strong rules makes sense if applying the rule frequently results in a winning solution. However, since users often match the calling conditions of rules with the most prominent cues in the environment, Reason observes that strong, good rules may be "misapplied in environment conditions that share some common features with the appropriate states, but also possess elements demanding a different set of actions" [100]. A rule which has been frequently useful in the past can become a *strong-but-wrong rule* when the situational cues change subtly. As Taylor and Crocker put it [116], "Like all gamblers, cognitive gamblers sometime lose." Phishers can create a severely rigged game for cognitive gamblers. Phishers provide situational cues which closely match the calling conditions "if (legitimate looking login form) then (enter username/password)", and applying this rule in the presence of an attacker results in an security failure, i.e., the compromise of the user's password.

Alternatively, a rule-based mistake may also occur if the user applies a bad rule. Bad rules are exactly that, but often do not cause accidents unless users apply them in risky situations. Reason terms this type of bad rule an *inadvisable rule*. Inadvisable rules may be perfectly adequate to achieve goals under normal conditions, but under risky conditions they may cause accidents. Reason explains that inadvisable rules "arise when an individual or organization is required to satisfy discrepant goals, among which the maintenance of safety is often a very feeble contender." Ignoring security warnings is excellent example of an inadvisable rule that many users have adopted. Carefully reading warnings is like "security maintenance" that users will quickly satisfice away if it becomes too burdensome.

At the knowledge-based level, mistakes occur because the user is essentially floundering. The fact that the user has reached the knowledge-based level means the situation is not immediately familiar to her and she has already exhausted any immediately applicable rules. The user must either form a mental model on-the-fly or reformulate the problem as a more familiar one. These tactics are highly prone to error, and confirmation bias and the tendency to explain away inconsistencies befog the decision making process. A faulty mental model or inappropriate problem reformulation may lead to the application of strong-but-wrong and inadvisable rules, further increasing the likelihood of errors.

3.2.3 Applying GEMS to user behavior during social engineering attacks

Although GEMS was originally conceived for modeling human errors which lead to accidents, researchers have observed GEMS is also useful for modeling human errors which lead to security failures [13, 21]. In particular, we argue that GEMS is useful for understanding human behavior during social engineering attacks on the Internet. By casting social engineering attacks in the context of GEMS, we can hopefully apply lessons learned by human reliability specialists to help users resist these attacks.

Generally, for an accident to occur, unsafe acts must combine with risky or unusual environmental conditions. During a social engineering attack, the presence of an adversary is the risky condition, and the adversary's goal is to intentionally trigger human errors, typically through a combination of environmental manipulation and active encouragement. Current Web ceremonies such as password authentication create a lose-lose situation for users. A common modus operandi of adversaries is to mimic trusted Web sites, and if the charade succeeds, an adversary gains the opportunity to exploit strong-but-wrong and inadvisable rules. Alternatively, if the user is suspicious, she is all but forced to proceed at the knowledge-based level to ultimately decide if the site is trustworthy. Attacks are an exceptional situation for most users, and users are ill-equipped to address them. Users are most likely to make mistakes at the knowledge-based level, and studies suggest that many users have erroneous mental models of Web security mechanisms and have a wide variety of faulty defense strategies for phishing attacks [24, 25, 135]. For example, a user in one phishing study believed that she could enter her username/password to authenticate a Web site, assuming that only the legitimate site would be able to respond correctly [24].

In summary, we hypothesize that social engineering attacks on the Internet succeed mostly due a combination of two tactics: 1) tricking users into applying strong-but-wrong and inadvisable rules, and 2) forcing users to make security decisions at the knowledge-based level, where they are most likely to make mistakes. To help users resist social engineering attacks on the Internet, we argue that ceremonies should condition users to apply rules that serve them well and help them thwart attacks. In the next section, we introduce the notion of a *conditioned-safe ceremony*, an approach for designing ceremonies that takes these observations into consideration.

3.3 Conditioned-safe ceremonies

One natural response to the weaknesses of current Web ceremonies such as challenge questions and passwords is to design ceremonies which try to eliminate user conditioning, click-whirr responses, and rule-based decision making. This approach is problematic. Rule-based decision making is fundamental to human behavior: it helps us complete routine tasks quickly and easily. Users may be willing to invest extra time and effort to learn a new security mechanism, but if they cannot learn how to use it efficiently, they will become frustrated and disable or circumvent the offending mechanism [41, 46, 141]. Some degree of conditioning may be necessary for the psychological acceptance of security mechanisms by users.

Since users will tend to adopt rules for completing a ceremony that minimize conscious effort, we should not fight users' tendencies to use rule-based decision making, but take advantage of these tendencies to help users resist social engineering attacks. We should prudently design ceremonies to condition rules that benefit security rather than undermine it. Towards achieving this goal, we introduce the notion of a *conditioned-safe ceremony*. A conditioned-safe ceremony is one that deliberately conditions users to reflexively act in ways that protect them from attacks. We propose two design principles for building conditioned-safe ceremonies:

- Conditioned-safe ceremonies should only condition *safe* rules, i.e., rules that are harmless to apply in the presence of an adversary.
- Conditioned-safe ceremonies should condition at least one *immunizing* rule, i.e., a rule which when applied during an attack causes the attack to fail. We discuss immunizing rules further in Section 3.3.1.

These principles also have important consequences on what conditioned-safe ceremonies should *not* do:

- Conditioned-safe ceremonies should not condition rules that require users to decide whether it is safe to apply them. Since many users are unreliable at recognizing risky situations, users should not need to refrain from conditioned behavior to resist attacks.

- Conditioned-safe ceremonies should not assume users will reliably perform actions that: 1) the ceremony has not conditioned her to perform, or 2) are voluntary. Satisficing users will learn to omit optional and voluntary actions, so ceremonies should not rely upon users to perform such actions.

For example, a ceremony should not condition the rule "if (legitimate looking login form) then (enter username/password)" because it causes a security failure when applied in the presence of an adversary. To determine if it is safe to apply this rule, a user must first verify the URL bar, the site's SSL certificate, and other security indicators. Burdening users with these decisions is unsatisfactory. Ideally, in a conditioned-safe ceremony, a user should be able to resist an attack even if she has no idea she is at risk and performs the same actions as she usually performs under benign conditions.

However, user behavior is unpredictable and an adversary may try to trick users into deviating from their normal, conditioned behavior in a way that causes a security failure. Conditioned-safe ceremonies need safeguards to resist these attacks. In the human reliability community, designers often introduce constraints called *forcing functions* to help prevent errors in safety-critical environments. We argue that forcing functions can also be useful for conditioned-safe ceremonies, and we discuss them further in the next section.

3.3.1 Forcing functions

A *forcing function* is a type of behavior-shaping constraint designed to prevent human error [90]. Forcing functions usually work by preventing a user from progressing in her task until she performs a particular action whose omission would result in a failure or accident. Because users must take this action during every instance of the task, the forcing function conditions users to always perform this action. With an effective forcing function, after a user performs the function's associated action, many mistakes become difficult or impossible to make. For example, consider the error of locking your keys in your residence. A potential forcing function in this situation is a door that can only be locked from the outside, keys in hand. This trains you to take your keys with you whenever you leave home, making it less likely you will be locked out in the future.

Forcing functions often have two benefits: 1) they help prevent *errors of omission*, where a user skips an important, protective step in a task, and 2) they condition correct, safe behavior, since users cannot normally proceed otherwise. To be effective, the cognitive and physical effort required to comply with a forcing function must be less than the effort required to circumvent it. Otherwise, users may routinely attempt to circumvent the forcing function, diminishing its benefits.

Since forcing functions have been useful for preventing errors in safety-critical environments, we hypothesize they can also help prevent errors during social engineering attacks. However, designing forcing functions that resist social engineering attacks is challenging. In conventional safety-critical environments, the risk elements rarely try to intentionally subvert protection mechanisms and cause errors. Designing electrical safety equipment would be a much trickier business if electricity had malicious intent. Also, deployability considerations for many ceremonies, e.g., no custom hardware, often require forcing functions to be implemented entirely in software. Software environments afford attackers many opportunities for mimicry.

One previous application of software-based forcing functions in computer security is the concept of a secure attention key (SAK). A SAK is a mandatory special key combination users must type before they can take a security-critical action, e.g., submitting their password. On Window NT systems, users must type Control-Alt-Delete to get a login prompt. The SAK diverts control to the OS kernel, foiling any user-level spoofed login prompts. Since typing the SAK is mandatory, the hope is that users will learn to always enter the SAK before submitting their password.

Unfortunately, a simple attack against many SAKs is to induce an error of omission. On Windows NT systems, an adversary can display a spoofed login prompt and hope users skip the SAK before entering their passwords. This attack creates a conflict between two click-whirr responses: SAK systems condition users to first type the SAK, but all password systems condition users to enter their passwords when they see a login form. Whether the attack succeeds depends on which click-whirr response is stronger in a particular user.

Since social engineering attacks can often misrepresent the state of a system and create the illusion that a forcing function has already been activated or disabled, ceremonies which fail solely due to errors of omission are suboptimal. Errors of omission are easy to make and hard to detect, even during routine tasks. Research suggests that users frequently do not notice when they have omitted routine procedural steps [5], and omission errors represent one of the most common causes of human performance problems [98].

To resist social engineering attacks, we argue that conditioned-safe ceremonies need *defense in depth*. Designers should build conditioned-safe ceremonies that have two levels of protection: an attack should fail unless a user both omits the conditioned action required by a forcing function and makes an *error of commission*. We consider an error of commission to be an anomalous user action not normally used in the ceremony. If the user omits the action required by the forcing function, but does not otherwise deviate from the ceremony, an attack should fail. Likewise, if the user performs the required action, but then makes an error of commission, the attack should also fail. With this approach, the action conditioned by the forcing function acquires an *immunizing* quality, since after a user performs this action, subsequent errors of commission will not compromise the ceremony.

We emphasize that the conditioned action required by the forcing function must be easy for users to perform; in particular, it should easier to perform than any unsafe error of commission. Since humans have been conditioned to work around buggy software, a user may willingly make an effortless error of commission if she feels it will complete the security task and allow her to continue with her primary task.

3.3.2 Analysis and discussion

Although a designer can choose the rules conditioned by a ceremony, an attacker can affect which rules a user chooses to apply by manipulating the environmental stimuli. Research by psychologists and human reliability specialists suggests that users mainly rely on two processes to determine the most appropriate rule to apply in a given situation: *similarity-matching* and *frequency-gambling* [100]. With similarity-matching, a user compares the situation's environmental cues against cues contained in the calling conditions of previously learned rules. If she finds a unique match, she performs the associated action. If the environmental cues are underspecified and partially match several rules, she will tend to "gamble" in favor of the useful, high frequency candidates, i.e., the "good" rules which have been most frequently applied in the past.

These tendencies suggest that conditioned-safe ceremonies will better resist the currently successful attack strategy of blatantly initiating a ceremony with the victim and presenting familiar environmental cues, e.g., spoofing a trusted Web site. Since a forcing function requires a user to perform the immunizing action every time (whether under attack or not), the forcing function will condition a high-frequency, "good" rule (namely, perform the immunizing action) that is likely to be routinely applied in the future – even when under attack. Mimicking a conditioned-safe ceremony becomes less advantageous to an adversary; if a user recognizes she is participating in the ceremony, she will tend to perform the conditioned, immunizing action, which thwarts attacks. This presents an attacker two options: 1) obviously initiate the ceremony and try to induce an error of commission before the user performs the immunizing action, or 2) surreptitiously initiate the ceremony and try to induce an error of commission without the user realizing she is participating in the ceremony.

If attackers resort to the first option, adversaries must prevent the human tendency to use rule-based decision making, rather than encourage it, as current attacks do. This creates a disadvantage for adversaries; preventing human tendencies is often difficult. If attackers resort to the second option, we hope adversaries will need to present unfamiliar situations to prevent users from recognizing the ceremony. Otherwise, users will tend to react with conditioned responses, i.e., apply safe rules and perform immunizing actions. This approach also disadvantages adversaries. Unfamiliar situations require additional cognitive effort to analyze and may cause feelings of suspicion and discomfort. User often reject unfamiliar experiences in favor of more familiar ones. For example, studies suggest that some users distrust phishing warnings because the familiar experience presented by the adversary appears more trustworthy [28, 135]. Conditioned-safe ceremonies turn the tables and force adversaries to be the ones required to present an awkward and unfamiliar experience.

3.3.3 Limitations

We acknowledge conditioned-safe ceremonies have their limits. Adversaries may try to convince users to disable protective mechanisms or take actions outside the scope of a ceremony which violate certain security assumptions. For example, with the configuration of many current computer systems, if a user chooses to install malware at any point, most ceremonies will be compromised. However, if we can design ceremonies that are so unproductive to attack directly that adversaries must resort to convincing users to install malware, it would be a tremendous step forward.

Chapter 4

Registration ceremonies

Since users may use more than one computer, machine authentication systems must have a *registration* ceremony to authorize and set authentication cookies on multiple machines. Many machine authentication systems currently deployed by financial Web sites use *challenge questions* in their registration ceremonies [9, 52, 123]. In this chapter, we describe weaknesses of registration ceremonies based on challenge questions and present a conditioned-safe registration ceremony we developed based on email.

4.1 Current practice: Challenge questions

A challenge question is a user-specific question which an adversary is unlikely to be able to guess an answer, e.g., "What is the name of your favorite teacher?" [30, 65]. When a user creates her account, she provides the answers to one or more challenge questions, and when she attempts to log in from an unregistered computer, the site prompts her to answer these questions. If the answers are correct, then the site sets a persistent authentication cookie on the user's computer. For future logins from that computer, the user only needs to enter her password.

Challenge questions are vulnerable to an active man-in-the-middle (MITM) attacker spoofing the login page of the target Web site [113, 144]. [1] When a user attempts to login

[1] Challenge questions also have other vulnerabilities [96, 118] which are not directly relevant to our work, e.g., the answers may be relatively easy to guess for many users.

via the spoofed page, the attacker forwards the user's login credentials to the legitimate Web site. Since the attacker is indistinguishable from the actual user logging from an unregistered machine, the Web site responds with challenge questions for the user. The attacker displays these questions to the user. After the user provides her answers, the attacker forwards them to the Web site and receives an authentication cookie for the user's account.

Challenge question based registration is vulnerable because, like password authentication, it disregards human tendencies and conditions users to fall for attacks. A user is most likely to resist an attack against her challenge questions if she recognizes the threat and refrains from the click-whirr response of providing her answers. However, since the attacker's registration request is indistinguishable from the Web site's legitimate registration requests, detecting attacks is non-trivial for many users. Users must actively and carefully check browser security indicators, e.g., the URL bar and SSL certificate, to detect spoofing attacks. Many users misinterpret these indicators, and satisficing users often ignore them.

In theory it is possible a user who has previously registered her machine and understands how registration works may be suspicious of the attacker's "spurious" registration request. However, users may not suspect they are under attack if there is any other reasonable explanation for the spurious request. If the user views the attacker's request as an error, e.g., her computer was accidentally "forgotten", the natural "fix" is for her to answer her challenge questions.

Regardless, this assumption about users' mental models is probably too strong. Since many users misunderstand browser security indicators, it is reasonable to expect many users will misunderstand registration procedures as well. A probable misinterpretation of registration procedures is that the Web site randomly asks challenge questions from time to time to verify the user's identity, and an attacker's request is hardly suspicious within this mental model.

Registration based on challenge questions threatens to undermine the promise of machine authentication. Since users who are vulnerable to phishing attacks against their passwords will probably also be vulnerable to phishing attacks against their challenge questions, a registration ceremony using challenge questions is hardly more secure than using passwords alone. We need better registration ceremonies to realize the benefits of machine authentication.

4.2 A conditioned-safe registration ceremony using email

In this section, we describe a conditioned-safe registration ceremony for machine authentication using email. When a user attempts to log in from an unregistered computer, the Web site sends her an email containing a single-use HTTPS URL with an unpredictable component, for example:

```
https://www.xyz.com/reg.php?url_id=r
```

where r is a 160 bit random number generated by the Web site.[2] We call this URL a *registration link*. The email includes instructions to click on the link. The Web site stores r in a database, along with the associated user ID, an expiration time, and validity bit. When the user clicks on the registration link, if r is still valid and has not expired, the Web site sets a persistent authentication cookie on the user's computer and invalidates r. A user only needs to complete this ceremony once at each computer. For subsequent logins, she only needs to complete any supplementary login procedures, e.g., enter her username and password. Several researchers have proposed using email in a similar way to help initialize authentication credentials [3, 8, 38, 44, 122].

4.2.1 Security analysis.

Against the phishing threat model, we argue email registration follows the principles of a conditioned-safe ceremony we propose in Section 3.3. The phisher can solicit the user's login name and password, but since the phisher's computer is unregistered, the site will not allow it to access the user's account without submitting a valid registration link. The attacker can trick the Web site to send the user a registration link, but to compromise the ceremony, an attacker must steal and use a registration link before the user submits it herself. [3]

[2] We assume the user has previously given the Web site her email address, e.g., during the account creation process.

[3] We do not consider attacks which enable adversaries to steal users' authentication cookies after they have been set, e.g., cross-site scripting attacks or malware. This problem is orthogonal to registration and requires a different solution.

The registration link acts as forcing function. Under normal conditions, a user must click on the link to proceed. Although there may be other ways of submitting the link, e.g., by copying and pasting it in the URL bar, clicking generally requires less effort, and sites can embed the URL of the link in an HTML element to make the alternatives more difficult. Also, clicking on the registration link is an immunizing action; after the Web site invalidates the link, it is useless to an attacker.

Email based registration has defense in depth. To compromise the ceremony an attacker must 1) prevent the user from clicking on the link (i.e., omit the forcing function action), and 2) trick the user into revealing the link (i.e., make an error of commission). One possible attack strategy would be to inform the user that she must register her computer, but due to "technical problems" she should not click on the link and instead give the link to the attacker. We identify two compelling and straightforward attacks of this kind: 1) ask the user to copy and paste the registration link into a text box, or 2) ask the user to forward the registration email to an address with a similar domain name as the target site. If a user does not notice the attacker's instructions and believes she is participating in the "normal" registration ceremony, we hypothesize she will likely resist these attacks. Email registration conditions users to click on the registration link, and if she clicks the link, she will resist the attack.

Alternatively, if the user notices the attacker's instructions to deviate from the ceremony, she will be safe as long as she clicks on the link before doing anything else. Since: 1) the Web site has conditioned the user to click on the registration link; 2) the credible repercussions of clicking on link are probably limited; and 3) clicking on the registration link is arguably at least as easy as complying with the instructions, the theory of rule-based decision making suggests that users will first tend to try clicking on the registration link before complying with the adversary's instructions.

The key question is the strength of users' tendencies to click the registration link rather than comply with the adversary's instructions. To help answer this question, we conducted a user study to estimate how well email registration helps users resist social engineering attacks against it. In the next chapter, we describe this study.

4.2.2 Implications and limitations of email based registration

One might argue that ceremonies that require users to click on email links will train users to click on phishing links and undermine some anti-phishing efforts which caution users to never click on links in email. However, we argue that relying on users to never click on email links is unrealistic. Sending and clicking on links in email is often useful for users, and many password reset and recovery ceremonies currently require users to click on an email link [38]. Some phishing studies suggest that many users regularly click on email links and employ a wide variety of link clicking strategies based on the current task, apparent source of the email, and other contextual cues [24, 26]. It would be a significant challenge to eliminate these practices. We argue that more comprehensive defenses which assume users will click on some email links are more likely to be effective.

Another potential criticism is that email based registration shifts many of the security and usability burdens onto email systems. The security of email systems relies on the security of email servers and users' email passwords. This raises several concerns [38]:

- A user might use a weak email password or use the same password for all her accounts.
- Some email providers use weak password reset and recovery mechanisms, such as challenge questions, which may be vulnerable to social engineering and inference attacks.
- Users may view their email accounts as less sensitive than their financial accounts and fail to adequately protect their email passwords. In our study presented in the next chapter, many users viewed the security of their email accounts as having the same level of importance as their accounts at social networking sites, but below their accounts at financial sites.
- Email is often sent over unencrypted connections, and POP and IMAP servers often accept passwords sent over unencrypted connections.
- Employees at businesses or ISPs might have access to their users' email.
- Several users might share a single email account.

- Email delivery is sometimes delayed.
- Spam filters may block legitimate messages.

Although the widespread use of email for password recovery and reset suggests that these issues may be manageable, we should not ignore them. Ideally, we should explore more secure and reliable messaging alternatives for security critical applications. One potential direction is to send registration links to users' mobile phones and develop software which enables easy transfer of the links to users' computers.

Chapter 5

A user study of registration ceremonies

In this chapter, we describe a user study we conducted to compare the security of email registration to the security of registration using challenge questions. Our study simulated man-in-the-middle (MITM) social engineering attacks against users of each of the ceremonies. Our hypothesis is that email registration is significantly more resistant to MITM social engineering attacks than registration using challenge questions.

5.1 Design challenges

Ecological validity is crucial: our study must realistically simulate experiences users have in the real world. This raises a number of challenges:

First, it is difficult to simulate the experience of risk for users without crossing ethical boundaries [58]. To address this, many experimenters employ role-playing, where users are asked to assume fictitious roles. However, role-playing participants may act differently than they would in the real world. If users feel that nothing is at stake and there are no consequences to their actions, they may take risks that they would avoid if their own personal information was at stake.

Second, we must limit the effect of demand characteristics. Demand characteristics refer to cues which cause participants to try to guess the study's purpose and change their behavior in some way, perhaps unintentionally. For example, if they agree with the hypothesis of the study, they may change their behavior in a way which tries to confirm it. Since security is often not users' primary goal, demand characteristics are particularly challenging for security studies. An experiment which intentionally or unintentionally influences users to pay undue attention to the security aspects of the tasks will reduce its ecological validity.

Third, we must minimize the impact of authority figures during the study. Researchers have shown that people have a tendency to obey authority figures and the presence of authority figures can cause study participants to display extreme behavior they would not normally engage in on their own. Classic examples of this are Milgram's "shocking" experiment [81] and the Stanford prison experiment [48]. For security studies, this tendency may underestimate the strength of some defense mechanisms and overestimate the success rate of some attacks. For example, if we simulate a social engineering attack during the study, users may be more susceptible to adversarial suggestions because they misinterpret these to be part of the experimenter's instructions. They may fear looking incompetent or stubborn if they do not follow the instructions correctly. This problem may be exacerbated if there is an experimenter lurking nearby.

Fourth, we must identify an appropriate physical location for the experiment. The vast majority of previous security user studies simulating attacks have been conducted in a controlled laboratory environment. They are many advantages to a laboratory environment: the experimenter can control more variables, monitor more subtle user behavior, and debrief and interview participants immediately upon completion, while the study is still fresh in their minds. But a laboratory environment also has some drawbacks for security studies. Since laboratories often lack the distractions and noise of the real world, users may be more likely to notice subtle or exceptional events. Also, users may evaluate risk differently than they would in the real world. A user may view the laboratory environment as safer because they feel that the experimenter "wouldn't let anything bad happen". Lastly, a short laboratory study may implicitly pressure users to ignore an option they sometimes have in the real world – to put off a security decision indefinitely.

It may be tempting to ignore some or all of these issues in a comparative study such as ours. Since the effects of these factors will be present in both the control group (i.e., challenge question users) and the treatment group (i.e, email registration users), then one might conclude that ignoring these factors would not hinder a valid, realistic comparison between the two groups.

This is a dangerous conclusion. It is not clear to what degree these issues affect various types of security-related mechanisms. In particular, there is no evidence that these issues have a similar magnitude of effect on challenge question users as on email registration users. Therefore, it is prudent to control these issues in our design as much as possible.

5.2 Study design

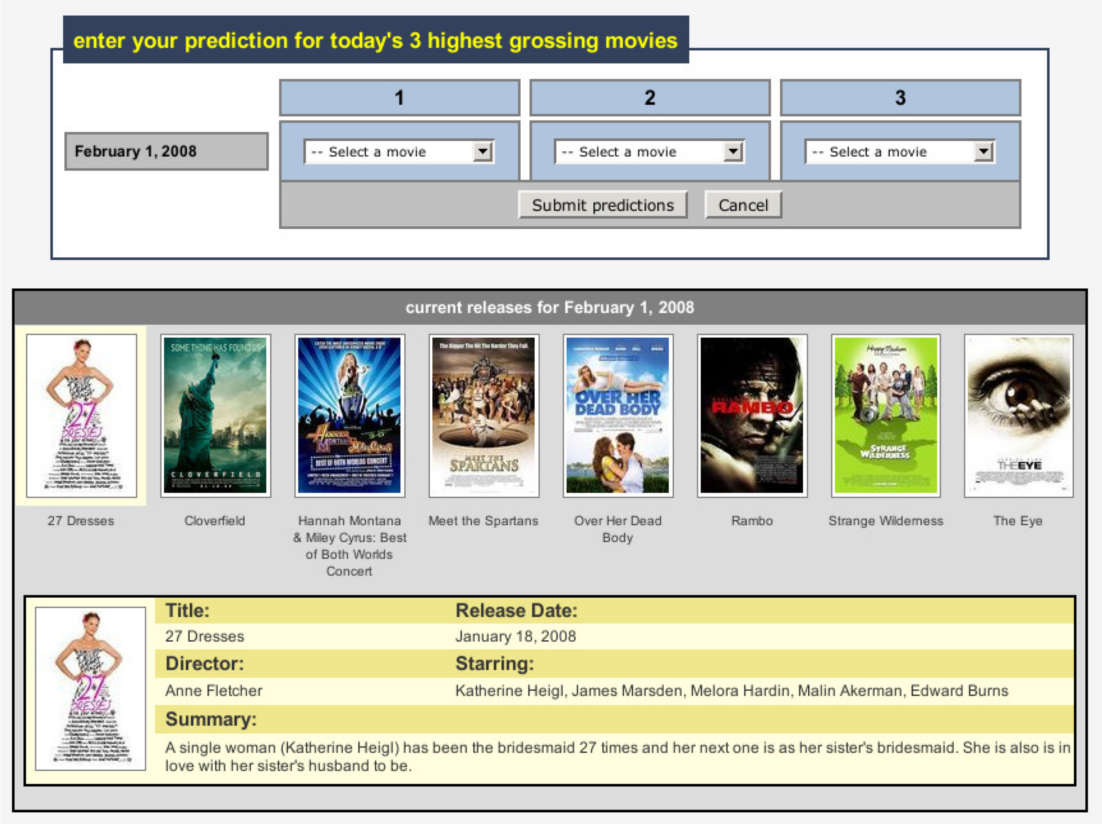
5.2.1 Overview

Our study addressed the challenges we identified in Section 5.1 with two techniques: 1) we did not use a laboratory, and 2) we employed deception to hide the study's true purpose. We recruited users remotely, and during the consent process, we told users that our experiment aimed to determine how well individuals can predict high grossing movies. We told each user she will log into our Web site over a seven day period and make a prediction of what she thinks will be the top three highest grossing movies each day. Each user logged in from her "natural habitat": from her own computer, from anywhere, and at any time she wished. We show a screenshot of our interface in Figure 5.1.

Each user received $20 as base compensation, and we rewarded her up to an additional $3 per prediction depending on the accuracy of her predictions. We told each user that she must make seven predictions to complete the experiment, so the total maximum a user could receive is $41.

We simulated the experience of risk by giving users password-protected accounts at our Web site and creating an illusion that money they "win" during the study was "banked" in these accounts. We paid users at the end of the study via PayPal and solicited each user's PayPal email address at the beginning of the study.[1] To help suggest that there was a risk that the user's compensation could be stolen if her account was hijacked, we provided an "account management" page which allowed the user to change the PayPal email address associated with her account.

[1] Although we did not verify each user's PayPal account was valid at the start of the study, each user explicitly acknowledged she either had an account or was willing to get one.



February 1, 2008

current releases for February 1, 2008

27 Dresses | Cloverfield | Hannah Montana & Miley Cyrus: Best of Both Worlds Concert | Meet the Spartans | Over Her Dead Body | Rambo | Strange Wilderness | The Eye

Title: 27 Dresses

Release Date: January 18, 2008

Director: Anne Fletcher

Starring: Katherine Heigl, James Marsden, Melora Hardin, Malin Akerman, Edward Burns

Summary: A single woman (Katherine Heigl) has been the bridesmaid 27 times and her next one is as her sister's bridesmaid. She is also is in love with her sister's husband to be.

Figure 5.1: **User interface for making predictions at our study Web site.**

Although we told users they must make seven predictions to complete the study, after each user made her fifth prediction, we simulated a MITM social engineering attack against her the next time she logged in. After she entered her username and password, we redirected her to an "attack" server. We discuss the simulated attacks in Section 5.2.4. After the simulated attack, we debriefed each user about the true purpose of the study and requested her reconsent for the use of her data.

5.2.2 Recruitment

We recruited users through the Experimental Social Science Laboratory (Xlab) at UC Berkeley. The Xlab is an interdisciplinary facility that supports UC Berkeley investigators in running behavioral and social science experiments. Members of the UC Berkeley community (i.e., students, staff, etc.) register with the Xlab over the Web and receive solic-

Group	Size	Registration method	Attack description	Warnings in email?
1	41	Challenge questions	Solicit answers	N.A.
2	40	Email	Forward email to attacker	✓
3	39	Email	Forward email to attacker	
4	40	Email	Copy and paste link into text box	✓
5	40	Email	Copy and paste link into text box	

Table 5.1: **Summary of study groups.**

itations to participate in experiments via email. One limitation of this recruitment method is that our user pool was primarily composed of university students and staff and may not be representative of the general population. Our experiment used only native English speakers, and the subject pool included approximately 1950 eligible users.

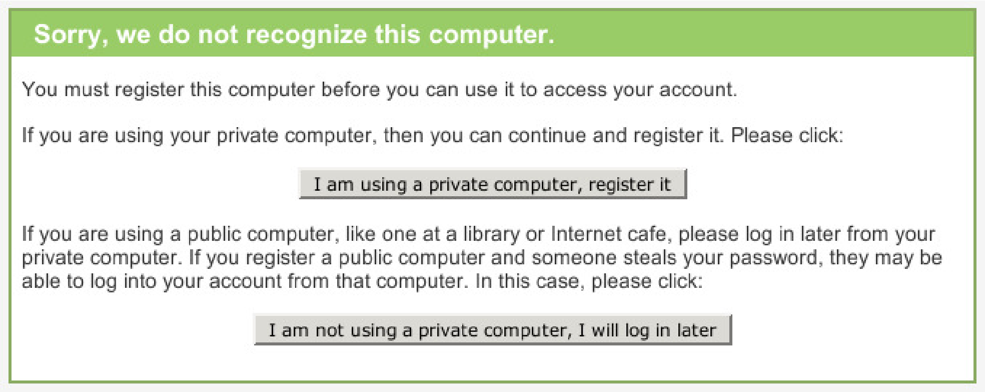
We contacted 225 randomly selected users in April 2008 through the Xlab. Interested users signed up through the Xlab's system and received instructions to visit our study Web site. We did meet any of the users in person. 208 users signed up for our study, and we assigned them round-robin to 5 study groups. One group used challenge questions for registration and the other four groups used different variants of email registration links. We discuss the email registration groups further in Section 5.2.4. We excluded the results of 8 users and give details in Section 5.3.1. We show a summary of the user groups and their sizes in Table 5.1.

5.2.3 Registration procedures

Each user created an account at our site, with a username and password. We also asked for the user's email address and PayPal email address, if different. During a user's first login attempt, we redirected her to the page shown in Figure 5.2 after she entered her username and password. This page informed her that she must register her computer before she can use it to access her account at our Web site. We also showed a user this page if she subsequently attempted to access our site from an unregistered computer. We wished to encourage users to register only private computers, so the site mentioned that it is a generally a bad idea to register public computers and if the user was using one, then she should wait until later to register her private computer. However, we did nothing to prevent or detect a user registering a public computer, such as a library computer. If the user chose to register her computer, we redirected her to the registration page. If she was in the challenge question group, we prompted her to set up her challenge questions with the page shown in Figure 5.3. She selected two questions and provided answers. After confirming the answers, she entered her account and proceeded with her first prediction.

If she was part of an email registration group, then she saw a page informing her that she had been sent a registration email and must click on the link labeled "Click on this secure link to register your computer". After clicking on the link, she entered her account and made a prediction. We sent registration emails in HTML format, but also included a plain text alternative (using the `multipart/alternative` content type) for users who had HTML viewing disabled in their email clients. We embedded the same registration link in both parts, but included a distinguishing parameter in the link to record whether the user was presented with the HTML or plain text version of the email. We discuss how we used this information in Section 5.2.4. Screenshots of registration emails are shown in Figures 5.5(a) and 5.5(b).

Both registration procedures set an HTTP cookie and a Flash Local Shared Object on the user's computer to indicate the computer is registered. For subsequent login attempts, we first prompted the user for her username and password. If the username and password were valid, our server checked if the user's computer was registered for that username. If she was logging in from a registered computer, then we redirected her to her account. If she was logging in from a computer we didn't recognize, then we prompted her to answer her challenge questions (Figure 5.4(a)) or sent her a new registration link to click on, depending on the user's group.



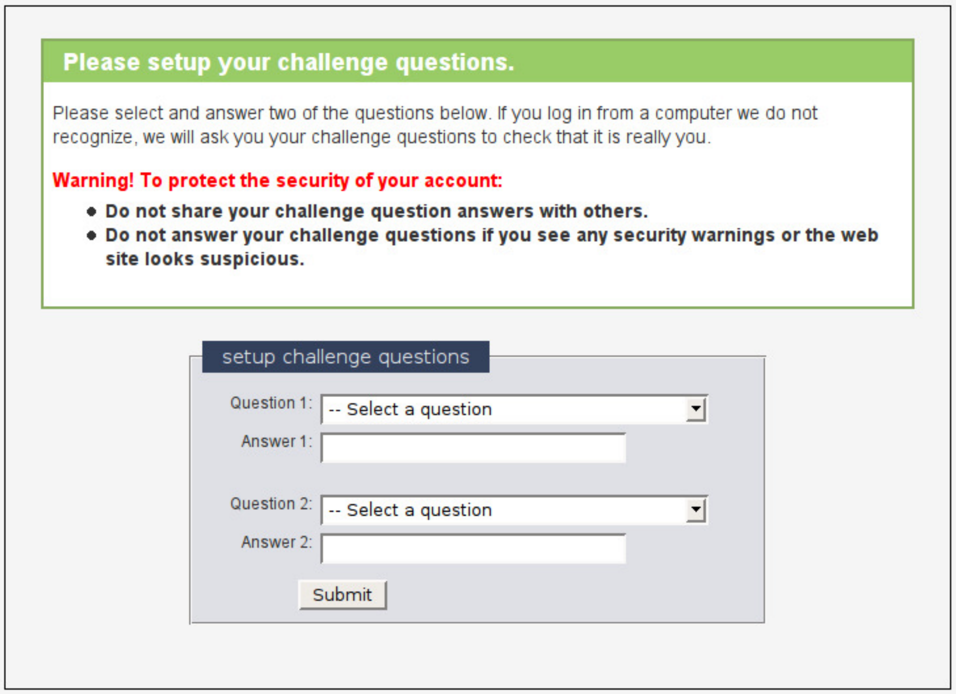
Sorry, we do not recognize this computer.

You must register this computer before you can use it to access your account.

If you are using your private computer, then you can continue and register it. Please click:

If you are using a public computer, like one at a library or Internet cafe, please log in later from your private computer. If you register a public computer and someone steals your password, they may be able to log into your account from that computer. In this case, please click:

Figure 5.2: **User interface for confirming registration.**



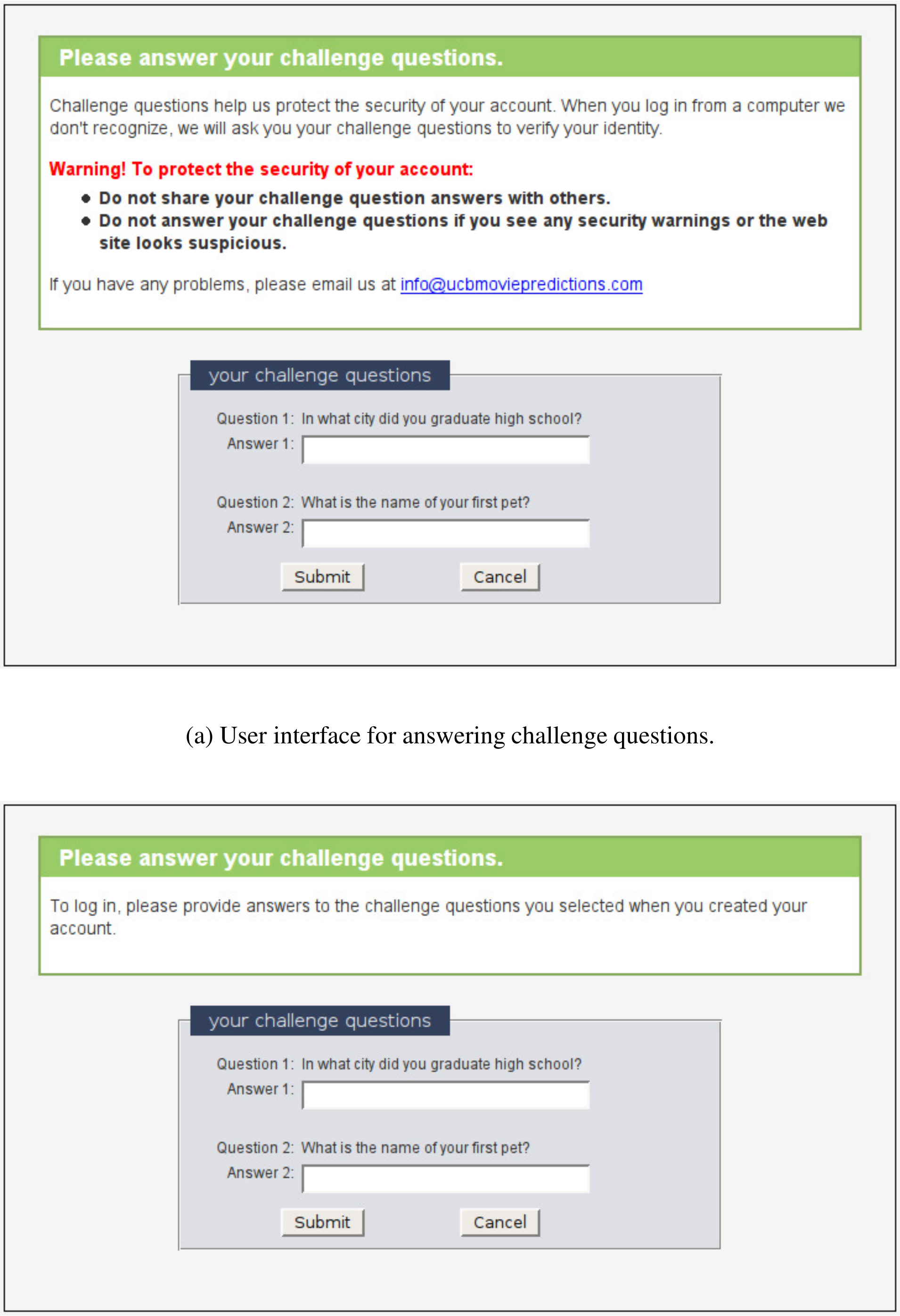
Please setup your challenge questions.

Please select and answer two of the questions below. If you log in from a computer we do not recognize, we will ask you your challenge questions to check that it is really you.

Warning! To protect the security of your account:

- Do not share your challenge question answers with others.
- Do not answer your challenge questions if you see any security warnings or the web site looks suspicious.

Figure 5.3: **User interface for setting up challenge questions.**



Please answer your challenge questions.

Challenge questions help us protect the security of your account. When you log in from a computer we don't recognize, we will ask you your challenge questions to verify your identity.

Warning! To protect the security of your account:

- **Do not share your challenge question answers with others.**
- **Do not answer your challenge questions if you see any security warnings or the web site looks suspicious.**

If you have any problems, please email us at info@ucbmoviepredictions.com

your challenge questions

Question 1: In what city did you graduate high school?
Answer 1:

Question 2: What is the name of your first pet?
Answer 2:

(a) User interface for answering challenge questions.

Please answer your challenge questions.

To log in, please provide answers to the challenge questions you selected when you created your account.

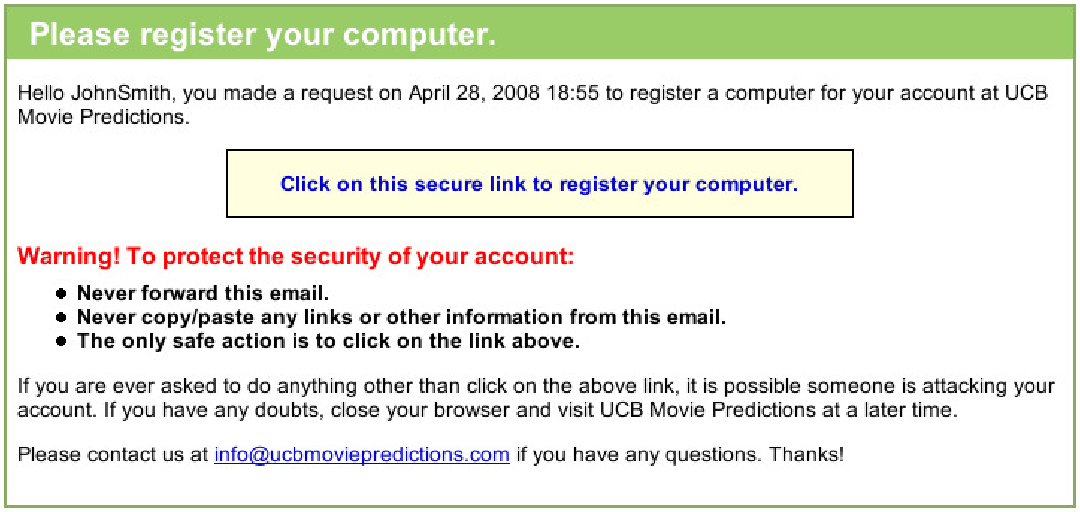
your challenge questions

Question 1: In what city did you graduate high school?
Answer 1:

Question 2: What is the name of your first pet?
Answer 2:

(b) Screenshot of the attack against challenge questions.

Figure 5.4: **Normal challenge questions interface vs. simulated attack instructions.**



Please register your computer.

Hello JohnSmith, you made a request on April 28, 2008 18:55 to register a computer for your account at UCB Movie Predictions.

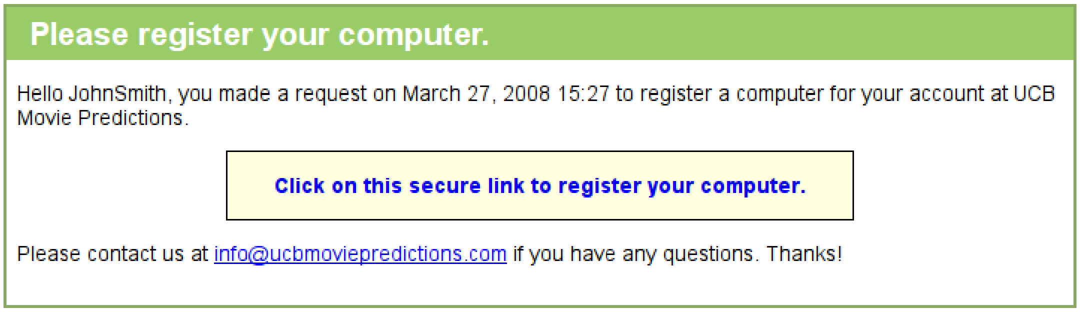
Warning! To protect the security of your account:

- Never forward this email.
- Never copy/paste any links or other information from this email.
- The only safe action is to click on the link above.

If you are ever asked to do anything other than click on the above link, it is possible someone is attacking your account. If you have any doubts, close your browser and visit UCB Movie Predictions at a later time.

Please contact us at info@ucbmoviepredictions.com if you have any questions. Thanks!

(a) HTML registration email with warnings.



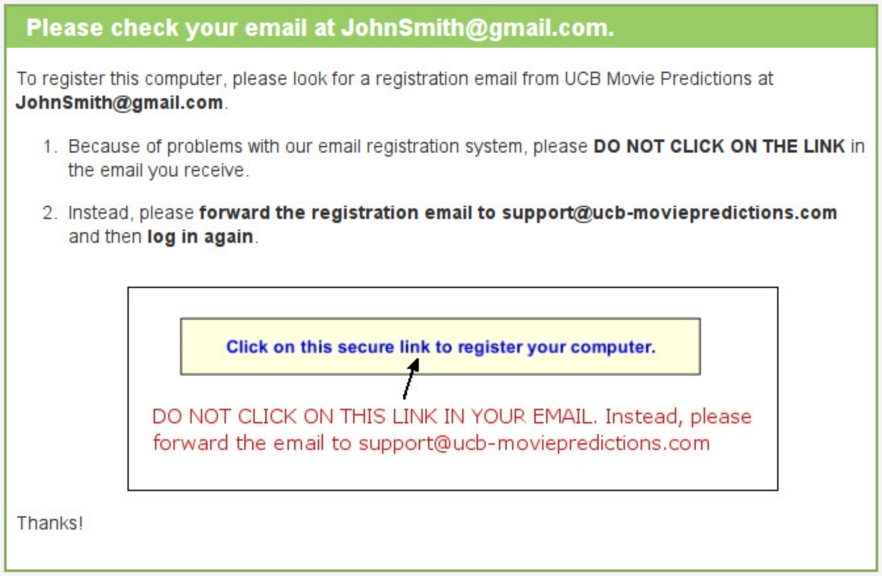
Please register your computer.

Hello JohnSmith, you made a request on March 27, 2008 15:27 to register a computer for your account at UCB Movie Predictions.

Please contact us at info@ucbmoviepredictions.com if you have any questions. Thanks!

(b) HTML registration email without warnings.

Figure 5.5: **Registration emails.**



Please check your email at JohnSmith@gmail.com.

To register this computer, please look for a registration email from UCB Movie Predictions at **JohnSmith@gmail.com**.

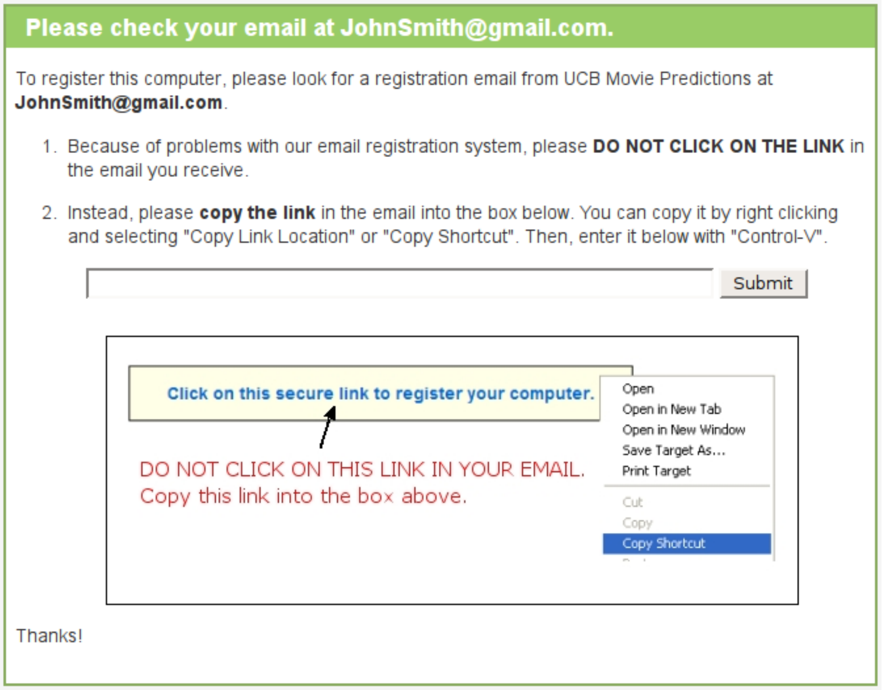
1. Because of problems with our email registration system, please **DO NOT CLICK ON THE LINK** in the email you receive.
2. Instead, please **forward the registration email to support@ucb-moviepredictions.com** and then **log in again**.

Click on this secure link to register your computer.

DO NOT CLICK ON THIS LINK IN YOUR EMAIL. Instead, please forward the email to support@ucb-moviepredictions.com

Thanks!

(a) Screenshot of the forwarding attack against email registration.



Please check your email at JohnSmith@gmail.com.

To register this computer, please look for a registration email from UCB Movie Predictions at **JohnSmith@gmail.com**.

1. Because of problems with our email registration system, please **DO NOT CLICK ON THE LINK** in the email you receive.
2. Instead, please **copy the link** in the email into the box below. You can copy it by right clicking and selecting "Copy Link Location" or "Copy Shortcut". Then, enter it below with "Control-V".

Click on this secure link to register your computer.

DO NOT CLICK ON THIS LINK IN YOUR EMAIL. Copy this link into the box above.

Thanks!

(b) Screenshot of the cut and paste attack against email registration.

Figure 5.6: **Our simulated attacks against email registration.**

5.2.4 Simulated attacks

Challenge questions: Group 1

For the challenge question group, the attack attempted to convince users to answer their challenge questions by presenting the page shown in Figure 5.4(b). This is essentially the same page users saw when they answered their challenge questions under "normal" conditions, but with the warning and informative text removed.[2] This attack: 1) is straightforward, 2) closely mimics the legitimate registration process, and 3) was previously disclosed in the security community as a major weakness of challenge questions [113, 144].

Email: Groups 2-5

For the email groups, we simulated the two attacks we identified in Section 4.2: the copy and paste attack and the forwarding attack. The copy and paste attack asked the user to copy the registration link into a text box, and the forwarding attack asked the user to forward the registration email to an address with a similar domain name as our study site. We simulated the forwarding attack against groups 2 and 3, and simulated the cut and paste attack against groups 4 and 5.

We chose these attacks because we believed they are the most compelling and straightforward attacks that we could ethically implement. Another potentially effective attack would be to try to hijack each user's email account, but we did not believe this attack was ethical. We leave other attacks as a subject for future work.

For both attacks, the attack page first told the user that "because of problems with our email registration system" she should not click on the link in the email she received. For the copy and paste attack, the attack page presented a text box with a "submit" button and instructed the user to copy and paste the registration link into the box. For the forwarding attack, it instructed the user to forward the email to the attacker's email address. We show screenshots of the attack pages in Figures 5.6(a) and 5.6(b).

These attacks also presented pictorial versions of the instructions, with a screenshot

[2] Even if users select their challenge questions from a pool of possible questions, an attacker can easily determine a particular user's questions by relaying communications between the legitimate site and the user [113, 144].

of how the registration link appears in the email. To maximize the effectiveness of this picture, we gave the attacker the advantage of knowing the distribution of HTML and plain text registration emails previously viewed by the user during the study (see Section 5.2.3). The attack displayed the pictorial instructions corresponding to the majority; in case of a tie we displayed a screenshot of the HTML version.

5.2.5 Warnings

Some Web sites warn users about safe security practices, e.g., how to resist phishing attacks against challenge questions. Although these warnings are sometimes useful, they will likely be absent during an attack, when a user needs them the most. Email registration has the advantage of being able to include advisory information and contextual warnings in each registration email. To measure the effectiveness of these kinds of warnings, we subdivided the email groups into two groups: those who received warnings in registration emails (groups 2 and 4) and those who did not (groups 3 and 5). Everyone saw these warnings on legitimate registration pages. A screenshot of these warnings is shown in Figure 5.5(a).[3] Group 1 users also received warnings about safe practices when answering their challenge questions, but we only showed group 1 users these warnings during legitimate registrations. Group 1 users never received warnings in email.

5.2.6 Attack success metrics

If a group 1 user answered her challenge questions correctly on the attack page, we considered the attack a success and ended the experiment. We assumed an attacker could distinguish between correct and incorrect answers (e.g., by relaying the user's responses in real time to the legitimate site), so if a user entered an incorrect answer, the attacker prompted her again.

If a group 2-5 user clicked on the registration link first, then we considered the attack a failure.[4] If the user forwarded the email or submitted the link first, then we considered the

[3] These warnings specifically warned against the attacks we simulated. Although in the real world it may not be feasible to concisely warn users against all the possible attacks, a site can certainly warn users against the most successful or common attacks they have observed in the past.

[4] These attacks actually simulated network level MITM attacks. Such attackers might be able to intercept

attack a success. Either way, we ended the experiment for the user.

For all users, attempts to navigate to other parts of the site redirected the user back to the attack page. If the user resisted the attack for 30 minutes, then on her next login, the experiment ended and we considered the attack a failure. The attack pages for groups 1, 4, and 5 contained a Javascript key logger, in case a user began to answer her challenge questions or entered the link, but then changed her mind and did not submit. If our key logger detected this, we considered the attack a success.

5.2.7 Debriefing and exit survey

After a user completed the study, we redirected her to a page that debriefed her about the true purpose of the experiment and explained the reasons for deception. The debriefing page explained the concept of machine authentication and the different ways of registering computers. We then obtained reconsent from each user. If a user reconsented, we redirected her to an exit survey.

Our exit survey started with general demographic questions such as gender, age range, and occupational area. The second section of the survey collected information on the user's general computing background, attitudes, and habits. The final section asked more specific questions about the user's experiences during the study. The exit survey questions are shown in Appendix A. Users' responses are in Appendix B.

5.2.8 Ethics

Our simulated attacks were ethical. The risk to users during the attacks was minimal. We only used data from users who explicitly reconsented after a debriefing on the true nature of the study. The study protocol described here was approved by the UC Berkeley's Institutional Review Board on human experimentation.

To protect users' privacy, all connections to our Web site used SSL. We purchased a certificate for our domain which is accepted by major Web browsers. In a real world attack,

registration links and steal any registration tokens stored on the user's computer. There are various proposals that can help protect registration links and cookies against stronger adversaries [18, 54, 70], but we do not discuss the details here. Regardless, the results of this study are applicable to a wide variety of social engineering attacks, including phishing.

an attacker would most likely not be able to obtain a valid certificate for the target site. To avoid certificate warnings, an attacker would probably use HTTP rather than HTTPS to host the attack page. However, to protect users' privacy, our simulated attack page used SSL. Since our hypothesis is that email registration is more secure than challenge questions, we had to ensure that our imperfect simulation did not bias the results against challenge questions. Our solution was to maximize the benefits of SSL for the challenge question users and minimize the benefits of SSL for the email registration users. In particular, we conservatively assumed that our simulated adversary attacking email registration had obtained a valid certificate for the target domain while our simulated adversary attacking challenge question based registration had not obtained a valid certificate. Group 2-5 users did not see certificate warnings during the attack, but group 1 users did. We implemented this by redirecting group 1 users to a different Apache instance (at port 8090) with a self-signed certificate, while group 2-5 users continued to use the original Apache instance in "attack mode". This implies the "attack" domain shown in the URL bar for group 1 users included a port number, but the "attack" domain for group 2-5 users did not.

5.3 Study results

5.3.1 User demographics

One email registration user did not complete the study, and one email registration user did not reconsent. Due to a misconfiguration, our server did not send registration emails to 6 users during the simulated attack. We excluded these users' data from our results, leaving 200 users total. We summarize the demographics of the 200 non-excluded users in Tables 5.2 and 5.3, broken down by group number.

56% of users self-reported themselves as female, 41% reported themselves as male, and 3% did not respond. Our users were mostly young: 91% reported themselves as 18-25 years old and 89% reported themselves as undergraduate students. Among students, the mix of major areas was diverse. The largest group was physical sciences (i.e., chemistry, physics, biology, etc.), accounting for 25% of users, and the second largest was economics and business, accounting for 20% of users. Computer science and engineering accounted

Gender	**1**	**2**	**3**	**4**	**5**
Female	49%	50%	62%	63%	60%
Male	49%	40%	39%	38%	38%
No resp.	2%	10%	-	-	3%

(a) Gender

Status	**1**	**2**	**3**	**4**	**5**
Undergrad	88%	83%	90%	95%	90%
Graduate	7%	3%	8%	3%	3%
Non-student	2%	5%	3%	3%	5%
No resp.	2%	10%	-	-	3%

(b) Student status

Age	**1**	**2**	**3**	**4**	**5**
18-21	59%	70%	80%	78%	80%
22-25	27%	20%	18%	15%	10%
26-30	-	-	3%	5%	3%
31-40	7%	-	-	-	3%
41-50	2%	-	-	3%	3%
No resp.	5%	10%	-	-	3%

(c) Age. We had no users over 50.

Major area	**1**	**2**	**3**	**4**	**5**
Economics or business	22%	20%	18%	25%	18%
Computer science	-	5%	-	3%	-
Engineering	2%	10%	18%	5%	3%
Social sciences	12%	13%	13%	25%	20%
Humanities	12%	8%	15%	3%	10%
Physical sciences	30%	18%	23%	28%	30%
Other	17%	13%	10%	10%	13%
No resp.	5%	15%	3%	3%	8%

(d) Student major area

Table 5.2: **User demographics by group number.** Some percentages may not add to 100% due to rounding.

OS	1	2	3	4	5
Windows	66%	65%	69%	75%	73%
Mac OS	24%	23%	31%	23%	25%
Linux	5%	-	-	-	-
No resp.	5%	13%	-	3%	3%

(a) Primary OS

Browser	1	2	3	4	5
IE	12%	8%	15%	10%	13%
Firefox	66%	68%	72%	73%	75%
Safari	12%	8%	10%	13%	10%
Opera	-	3%	-	3%	-
Other	5%	3%	3%	-	-
No resp.	5%	13%	-	3%	3%

(b) Primary browser

Type	1	2	3	4	5
PayPal	56%	43%	64%	50%	65%
Banking	81%	63%	90%	80%	85%
Investing	17%	8%	13%	13%	13%
Auctions	50%	33%	44%	30%	55%
Shopping	78%	73%	82%	75%	90%
Other	2%	-	3%	5%	5%
No resp.	7%	13%	-	3%	3%

(c) Types of financial transactions conducted online

Length	1	2	3	4	5
Never	7%	8%	5%	10%	5%
$<$ 6 months	5%	10%	8%	13%	5%
6-12 months	5%	8%	10%	10%	23%
1-2 years	24%	18%	26%	18%	13%
$>$ 2 years	54%	45%	51%	48%	53%
No resp.	5%	13%	-	3%	3%

(d) How long each user has conducted financial transactions online

Table 5.3: **User demographics by group number.** Some percentages may not add to 100% due to rounding.

for 1.5% and 7.5% of users, respectively.

Most users reported using Windows (69%) and Mac OS (25%) as their primary operating systems, and most users reported using Firefox (70%), Internet Explorer (11%), and Safari (10%) as their primary Web browsers. This differs significantly from recent statistics, which report Windows as having 91% market share and Internet Explorer as having 72% market share [14].

78% of users reported using a Web browser at least 10 hours a week, and 70% of users reported they have conducted financial transactions online for at least a year. Types of online transactions reported include PayPal (55%), banking (80%), investing (12%), auctions (42%), and shopping (80%).

5.3.2 Success of simulated attacks

We summarize our results by group number in Table 5.4. Our attack succeeded against 92.7% of challenge question users and 41.5% of email users. This difference is statistically significant ($p < 0.001$, Fisher's exact test). The cut and paste attack was slightly more effective than the forwarding attack (47% vs. 40% with warnings, and 47% vs. 31% without warnings), but we did not find this difference significant ($p = 0.65$ with warnings, and $p = 0.17$ without warnings; Fisher's exact test). We found no significant correlations between attack success and the demographics we reported in Section 5.3.1. In particular, we found no evidence that frequent browser use, previous experience with online financial transactions, or a technical undergraduate major area helped users resist our attacks.

5.3.3 Efficacy of our warnings

We found no evidence that including warnings in registration emails helped users resist our attack. To evaluate the effectiveness of our contextual email warnings, we compared the attack success rates of group 2 vs. group 3 (forwarding attacks, with and without warnings, resp.), and group 4 vs. group 5 (cut and paste attacks, with and without warnings, resp.). For the forwarding attack, 40% of group 2 users were vulnerable, and 31% of group 3 users were vulnerable ($p = 0.48$ for Fisher's exact test). For the cut and paste attack, 47% of users in both group 4 and group 5 were vulnerable ($p = 1$ for Fisher's exact test).

Group	Registration method	Attack	Warnings in email?	Size	Attack successful
1	Challenge questions	Solicit answers	N.A.	41	92.7% (38)
2	Email	Forwarding	✓	40	40.0% (16)
3	Email	Forwarding		39	30.8% (12)
4	Email	Cut and paste	✓	40	47.5% (19)
5	Email	Cut and paste		40	47.5% (19)

Table 5.4: **Success rates of our simulated attacks against registration procedures in our user study.** Users in groups 2 and 4 received contextual warnings in registration emails against our simulated attacks, but users in groups 3 and 5 did not.

During the exit survey, we showed each user a screenshot of the warning corresponding to her study group (Section 5.2.5) and asked her "Do you remember seeing the above warning at any point during the study?", and if yes, "describe how it affected your decisions (if at all) while interacting with the study Web site." Table 5.5 summarizes the number of yes/no responses. For group 2 and 4 users, who received warnings in registration emails, 31% reported that they did not remember the warning. Among group 3 and 5 users, who only received warnings on the study Web page, 68% did not remember the warning. This difference is statistically significant ($p < 0.001$ for Fisher's exact test). 66% of challenge question users also did not remember the warning.

We found no evidence that users who recalled seeing our warnings were more likely to resist our attack. Of the 191 users responding to the warning recall question, 85 remembered seeing our warning and 106 did not (see Table 5.6). Among the users who remembered seeing our warning, 45% were vulnerable, and among the users who did not remember seeing our warning, 56% were vulnerable. This difference is not statistically significant ($p = .147$ for Fisher's exact test). We found no statistically significant difference within groups, either.

Among the users who remembered seeing the warning, Table 5.7 summarizes the self-reported effects that the warnings had on those users. Of the 85 users who remembered our warnings, only 10 users' responses (12%) indicated that our warnings helped them resist our attack. 38 of these users (45%) indicated that the warnings had little or no impact on

	Warnings	User remembered seeing our warning?		
Group	in email?	No	Yes	No response
1	N/A	65.9% (27)	31.7% (13)	2.4% (1)
2	✓	25.0% (10)	62.5% (25)	12.5% (5)
3		59.0% (23)	41.0% (16)	0.0% (0)
4	✓	37.5% (15)	57.5% (23)	5.0% (2)
5		77.5% (31)	20.0% (8)	2.5% (1)

Table 5.5: **Number of users who reported remembering seeing our warnings.**

	Safe	Vulnerable	Total
Users who remembered seeing our warnings	55.3% (47)	44.7% (38)	85
Users who did not remember seeing our warnings	44.3% (47)	55.7% (59)	106

Table 5.6: **Effect of warning recall on resisting our simulated attacks.** Of the 200 users in our study, 9 users did not respond to this question.

their decisions. 4 users (5%) indicated that the warning slightly influenced their decision making during the attack, but they ultimately followed the attack instructions. 7 users (8%) mentioned that the warnings made them "feel safer" at our site or be more careful in general. The responses of 11 users were inconclusive or did not clearly fit in one of these categories.

5.3.4 User suspicion of our attacks

To gauge users' suspicion during our simulated attack, we asked users "During your interactions with UCB Movie Predictions, did you ever see something which looked suspicious or dangerous?" and "describe what your reaction was and if you did anything, what you did." Overall, only 6 (15%) challenge questions users and 13 (8%) email users reported seeing anything suspicious during the study. Four of the challenge question users reported that the certificate warning caused their suspicion, but only 1 of those users resisted the

		Self-reported effect of warning on user						
Group	**Warnings in email?**	**Little or none**	**Helped resist atk.**	**Recalled during atk. but no help**	**“Felt safer”**	**Other**	**No resp.**	**Total**
1	N/A	8	0	0	2	0	3	13
2	✓	8	7	2	2	4	2	25
3		11	1	1	0	1	2	16
4	✓	7	2	1	2	5	6	23
5		4	0	0	1	1	2	8
Total		38	10	4	7	11	15	85

Table 5.7: **Self-reported effects of our warnings on users who remembered seeing them.**

attack.[5] One challenge question user reported that the fact that the attack required her to re-register her machine made her suspicious. The 13 suspicious email users reported the attack instructions as the cause of their suspicion, but only 6 of those users resisted the attack.

5.3.5 User reasoning during our attacks

To help understand users' thought processes during the simulated attack, we showed each user a screenshot of the attack instructions corresponding to her group and asked her: "If you followed the above instructions, explain why. If you chose not follow the instructions, explain why not. If you don't remember this page or what you did, tell us what you don't remember." We did not explicitly identify this as the "attack".

Challenge question users. Among the 38 vulnerable users in the challenge question group, 22 users (58%) said that they complied with the attack instructions because they thought it was what they needed to do to log in. Representative responses include: "Those were my challenge questions, so I answered them" and "I thought it was procedure to answer these questions." 10 vulnerable users (26%) viewed the attack as an error that they should try to fix, e.g., "I thought the site's cookie may have been erased which is why it wasn't recognizing my computer, so I answered." 4 vulnerable users (11%) trusted the Web site or indicated that since the site was associated with UC-Berkeley, it should be safe. Of the 3 challenge question users who resisted the attack, one user noticed the certificate warning and stopped, and the other two users did not respond to this question.

Email users. Among the 66 vulnerable email users, 26 users (39%) complied with the attack instructions because they thought it was what they needed to do to log in. A representative response is "I copy and pasted the link because it said in bold to do so. It seemed

[5] Most browsers show certificate warnings in popup windows. Firefox 3 and Internet Explorer 7 present full screen interstitial warning pages, but Firefox 3 was not officially released until after we completed our study. Among the 41 challenge question users (who were the only users who saw certificate warnings – see Section 5.2.8), twenty five used Firefox 1 or 2, two used IE 6, six used IE 7, seven used Safari, and one used Epiphany. Among the 4 users who reported the certificate warning as the cause of their suspicion, three used Firefox 2 and one used IE 7.

like that was what I was supposed to do." 11 vulnerable users (17%) viewed the attack as an error that they should fix, e.g., "I figured something was wrong with your registration system and thus followed instructions." 20 vulnerable users (30%) trusted the Web site or indicated that since the site was associated with UC-Berkeley, it should be safe. 8 vulnerable users (12%) indicated that they complied with our attack instructions because they did not associate much risk with our Web site.

Among the 93 email users who resisted the attack, the responses of 37 users (40%) indicated that although they may have recognized the instructions were different from previous registrations, they decided to click the registration link first, despite instructions to the contrary, or did not read the attack instructions carefully. Representative responses include: "I did not follow the instructions because it was easier to just click" and "Usually, in a verification email, you are supposed to click the link."

17 resisting users (18%) indicated that they did not notice the attack instructions. For example, "I never saw these instructions." All except two of these users clicked on the registration link; the other two users timed out the attack.

10 users (11%) cited our warnings as helping them resist the attack, e.g., "The Website and the email I received were telling me contradicting things so I just went with what the email told me" and "I didn't follow the instructions because they were contradictory to the warnings in the previous email."

We found evidence that 15 users (16%) initially considered the attack instructions, but eventually gave up because they found them too difficult, decided it was not worth the hassle, or made a mistake in following them. 5 users explicitly indicated this in their responses, e.g., "I did not because it was too much of a hassle" and "I figured I would see if the site would be on track later." The remaining 10 users attempted to follow the attack instructions, but made a "mistake", e.g., they forwarded our welcome email or copy and pasted a previously used registration link. Although we count these users as resisting our attack, they may be more likely to fall for future attacks than other users who resisted.

The responses of 3 resisting users (3%) were hard to interpret. They stated that they followed the attack instructions, but we have no evidence that they attempted to do so; they all clicked on the link quickly. One possible explanation is that they did not actually notice the attack instructions, but attempted to please us during the survey or avoid appearing as if they disregarded our instructions.

5.3.6 Usability and security opinions of registration mechanisms

To evaluate users' impressions of the security benefits of the registration mechanisms, we asked users: "Rate how safe you would feel using a Web site which uses the following different login mechanisms: 1) Password for logins + no registration, and 2) Password for logins + <challenge questions/email> for registration". The answer choices were: "Not secure at all", "Somewhat secure", "Fairly secure", "Very secure", and "I don't know". We summarize users' responses in Table 5.8.

To evaluate the usability of the registration mechanisms, we asked users: "Rate the convenience of each of the following login mechanisms: 1) Password for logins + no registration, and 2) Password for logins + <challenge questions/email> for registration". The answer choices were: "Nearly impossible or very annoying", "Hard or slightly annoying", "I could get used to it, "I hardly noticed it", and "I don't know". We summarize users' responses in Table 5.9.

5.3.7 Ecological validity

To evaluate the ecological validity of our study, we sought to determine how much risk users perceived while using our site. Since risk is subjective, we asked each user to tell us the biggest security concerns she has while browsing the World Wide Web and the precautions she takes to protect herself when logging into Web sites. Then, we asked her to rank how often and thoroughly she applies those precautions when logging into the following types of Web sites: banking, shopping, PayPal, Web email, social networking, and our study site. The answer choices were: "rarely", "sometimes", "usually", "always", and "I don't use this type of Web site". We summarize the responses in Table 5.10. Users reported that they did not take the same level of precautions on our site as they do with other sites which handle money. Over 64% of users reported that they at least "usually" take security precautions at those sites, but only 27% of users said they at least "usually" took precautions at our study Web site. Users more closely associated the risks at our study Web site with a Web email site or social networking site.

Group	Login mechanism	**Not secure at all**	**Somewhat secure**	**Fairly secure**	**Very secure**	**I don’t know**	**No response**
Challenge question users	Password + no registration	4.9% (2)	43.9% (18)	36.6% (15)	2.4% (1)	7.3% (3)	4.9% (2)
	Password + challenge questions for registration	0% (0)	7.3% (3)	36.6% (15)	48.8% (20)	0% (0)	7.3% (3)
Email users	Password + no registration	9.4% (15)	43.4% (69)	28.9% (46)	3.8% (6)	6.9% (11)	7.5% (12)
	Password + email for registration	0.6% (1)	9.4% (15)	48.4% (77)	30.2% (48)	4.4% (7)	6.9% (11)

Table 5.8: **Users’ opinions of the security benefits of registration.**

Group	Login mechanism	Very annoying	Slightly annoying	I could get used to it	I hardly noticed it	I don’t know	No response
Challenge question users	Password + no registration	0% (0)	0% (0)	22.0% (9)	63.4% (26)	7.3% (3)	7.3% (3)
	Password + challenge questions for registration	2.4% (1)	19.5% (8)	31.7% (13)	36.6% (15)	2.4% (1)	7.3% (3)
Email users	Password + no registration	0% (0)	6.3% (10)	18.9% (30)	62.3% (99)	5.7% (9)	6.9% (11)
	Password + email for registration	0.6% (1)	16.4% (26)	38.4% (61)	35.8% (57)	1.9% (3)	6.9% (11)

Table 5.9: **Users’ opinions of the convenience of registration.** For space constraint reasons, some of the answer choices have been shortened. Refer to Appendix A for the full text of the answer choices.

Site type	**Rarely**	**Sometimes**	**Usually**	**Always**	**Don't use**	**No resp.**
Banking	10.5% (21)	8.5% (17)	15.5% (31)	55.5% (110)	3.5% (7)	7.0% (14)
Shopping	13.0% (26)	12.5% (25)	26.5% (53)	37.5% (75)	3.0% (6)	7.5% (15)
PayPal	14.0% (28)	9.0% (18)	23.0% (46)	44.0% (88)	3.5% (7)	6.5% (13)
Email	34.0% (68)	16.5% (33)	18.5% (37)	22.0% (44)	2.0% (4)	7.0% (14)
Social networking	34.5% (69)	21.5% (43)	16.0% (32)	20.0% (40)	1.0% (2)	7.0% (14)
Our study Web site	46.0% (92)	18.5% (37)	12.5% (25)	14.5% (29)	1.5% (3)	7.0% (14)

Table 5.10: **Risk ratings.** This table summarizes how thoroughly and often the users reported applying security precautions when logging into various types of Web sites.

In users' responses to other questions, 2 users explicitly mentioned that they took precautions because we had their PayPal email address, e.g., "I wanted to stay secure so that people couldn't come in and take my PayPal account." However, 14 users explicitly mentioned that they considered our study site to be low risk because they felt they had little to lose, e.g., "even if someone had hacked the site, what had I to lose? An experiment account? I was not particularly worried."

5.4 Analysis and discussion

5.4.1 Ineffectiveness of our warnings

Our results suggest that our warnings had little impact users' decisions, even when users had the opportunity to see warnings during the simulated attacks. We found no evidence that including warnings in registration emails helped users resist our attacks. Many users did not remember our warnings or indicated they had little impact on their decisions during the study. Although including contextual warnings in email seemed to improve the likelihood that a user would recall seeing them, we found no evidence that users who recalled seeing our warnings were more likely to resist our attack. Our results are consistent with a recent study by Egelman et al. which suggests that passive warnings such as ours are ineffective in helping users resist attacks [28].

Research from the warning sciences community suggests that if a warning does not sufficiently stimulate users, or if users cannot meaningfully process and apply a warning's message, it will have limited effect [134]. Some responses from email users suggested that we failed to both get their attention and communicate a meaningful message. They assumed our warnings were similar to other "standard" warnings, or our warnings just made them feel our site was generally more secure. For example:

- "I figured it was just standard stuff."
- "It looked like a standard confidentiality issue, so I didn't think of it as anything particularly special."
- "I just chalked it up to general security advice and more or less forgot about it."

- “It made me feel that the Website was more secure.”
- “This bit of information made me feel like the site was trying to protect my privacy.”
- “It did not affect my decisions much, but it did help the validity of the survey.”

5.4.2 Lack of user suspicion

Our attacks raised suspicion in only small percentage of users. Many of the other users had alternative interpretations. Some users saw the attack as the result of an error with the Web site, her browser, her computer, or the network, e.g., “I thought that the link was broken.” Some users did not view that complying with the attack instructions might be risky, but rather thought it was necessary for their own safety. For example,

- “I followed the instructions because it was for my own safety.”
- “I did because I wanted to stay secure so that people couldn’t come in and take my PayPal account.”
- “The site is verifying I am who I say I am; I never thought of it in terms of me questioning the site’s identity.”

Some users indicated they did not have a clear understanding of how the registration procedure works and its purpose, and when they would be required to participate in the registration ceremony. For example,

- “I figured that because I switched connections, as I was using Berkeley’s wireless as opposed to my dormitory’s ethernet Internet, they needed to re-verify my account.”
- “I followed the instructions because I assumed my password was wrong so the alternate method of login was by answering the security questions.”
- “I figured it had been too many days since I’d signed in.”
- “I answered them because I couldn’t remember if you guys said that we will randomly be asked to answer them in place of our password and login name.”

- “I remembered this page, and I followed the instructions because they are often used to verify a user if a username seems unsafe or has been tampered with.”
- “The link in the email contains a data string that, when clicked, changes account details to confirm that that was a valid email address. Security benefits to the user may be minimal.”
- “I think it prevents hackers from just creating accounts and using them but they would have to go to the extra step of doing the email registrations.”
- “I actually didn’t think it had anything to do with the security of my money/identity.”

These results are consistent with previous work which suggests that users have a limited understanding of Web security mechanisms, Internet social engineering attacks, and effective defense strategies [24, 25, 49, 135]. This evidence supports our design principle for conditioned-safe ceremonies that argues designers should not assume users will be able to detect attacks, or sufficiently understand ceremonies to know when they should refrain from participating or perform voluntary defensive actions.

5.4.3 The power of user conditioning and forcing functions

Challenge question based registration conditions users to provide their answers when they are asked their challenge questions. The responses of 58% of the vulnerable challenge question users indicated that conditioning was the primary influence on their decision to comply with the simulated attack’s request for their answers. User responses of this type include:

- “I answered the questions because I thought I was being asked to identify myself.”
- “I answered it because it was required in order to log in.”
- “I wanted to log in, so I answered the challenge questions.”

This supports our hypothesis that challenge questions condition users to answer their challenge questions whenever prompted.

In contrast, the responses of 56% of email users who resisted the simulated attack suggested that conditioning was a factor in their resistance. The responses of 40% of resisting email users suggested they may have noticed the attack was somewhat different from a normal registration, but either chose to ignore the attack instructions and click the link, or did not read the attack instructions carefully. User responses of this type include:

- "I didn't follow the instructions because I didn't pay attention to this page (I just followed the usual procedures to register my computer)."
- "I didn't follow the directions because it sounded sketchy and I wanted to see what happened."
- "I must have glossed over the instructions to not click the registration email link, I didn't think there would be two opposing instructions so I just went with the one that was more obvious."
- "I didn't read it carefully, and instinctively clicked on the link in the email."

The responses of 16% of resisting email users suggested that they probably did not notice any differences between our simulated attack and a normal registration, and proceeded to click on the registration link in the email sent to them. User responses of this type include:

- "I don't remember ever seeing this page, but I think what I might have seen was simply that I thought this page was giving me the same instructions as the first time when I had to register my computer."
- "I don't remember because it has been a hectic week. I just didn't notice."
- "I don't really remember this or I misread it."
- "It's currently 2:20am and I just got back from 5 hours of dance practice. Honestly, I didn't even see the instructions!!! How scary!"

These results suggest that conditioning played a significant role in a large fraction of users' decision making processes during our simulated attacks – to the benefit of email registration, but to the detriment of challenge question based registration.

One factor our study did not control is to what degree challenge questions and clicking on email links had conditioned users prior to participating in our study. Several sites currently implement challenge question based registration [9, 52, 123], and many use challenge questions for password reset. Although we do not know of any sites that implement email registration for machine authentication, many Web sites send an email link to reset a user's password or validate her email address [38]. We did not screen users based on previous exposure to these mechanisms, but we did ask users whether they had previously used them. 80% of challenge question users and 70% of email users reported having used the respective mechanisms prior to participating in our study. However, we found no significant correlation between previous exposure to these mechanisms and attack success rate. We leave better understanding of this issue as a subject of future work.

5.4.4 Ecological validity

We asked users to give feedback about their impressions of the study, and their responses suggested that predicting popular movies can be fun and engaging. Some users expressed disappointment that we ended the study before they had the opportunity to make all 7 predictions. Some users admitted they had no idea as to the true purpose of the study, and no user claimed to have figured out that the study was security related. Based on this evidence, we argue the effects of demand characteristics were sharply diminished in our study.

Our study created an experience of risk for some users, but many users indicated that the risk level they associated to our site was roughly equivalent to Web email or social networking sites, and below financial-related sites such as banking or shopping. Some users explicitly stated in their comments that they did not experience much risk during our study, e.g., "And even if someone had hacked the site, what had I to lose? An experiment account? I was not particularly worried." Some users suggested that they felt safer at our site because it was associated with Berkeley, e.g., "I figured that since this was a Berkeley research affiliated Website, it would be safe." Creating a significant experience of risk in studies like ours remains a challenge.

Our design attempted to limit the effect of authority figures during the study by conducting it in users' "natural habitats". One concern we had was that users would interpret the attack as instructions from us, the researchers. Although this is similar to the problem users face during a real phishing attack, academic researchers might appear more as an authority figure to a user than, say, a bank. There was evidence that this may have been an issue for some users, e.g., "I followed the instructions because I thought it was a legitimate set of instructions from respected researchers who could not possibly have a motive to deceive me", but maybe not for others, e.g., "My security is more important to me than their system problems." We did not design our study to evaluate this issue in depth; further research is needed.

5.4.5 Study limitations

Our study had several limitations. Although we took great efforts to make our study as ecologically valid as possible (while remaining ethical), some users' responses suggested we fell short in some aspects, most notably in simulating the experience of risk in the real world and completely eliminating the influence of authority figures. The size of the compensation may not have been large enough to warrant extra attention, and the fact that our Web site was implicitly associated with UC-Berkeley may have influenced users' decisions. Also, since the vast majority of our users were undergraduates at UC-Berkeley, we cannot easily generalize our results to the general population.

We acknowledge that there may be more effective attacks against email based registration. One potentially effective attack might be to try to hijack users' email accounts, but we did not implement this attack for ethical reasons. Another type of attack we did not evaluate is a *prediction attack*. In a prediction attack, the adversary creates the illusion that she can reliably predict the future. Being able to predict the future affords credibility, which an adversary may be able to exploit. If an adversary sends the user an email predicting that she will receive a registration email, but requests that she handles it unsafely, she may be more likely to comply. Stock market scams employing this technique are often effective.

Although our results suggest that the notion of conditioned-safe ceremonies may be useful for helping users resist some types of Internet social engineering attacks, further research is necessary. We acknowledge that it remains to be seen whether the notion of conditioned-safe ceremonies will be more generally applicable to other types of ceremonies, environments, and attack strategies. For example, it may be more challenging to develop conditioned-safe ceremonies to resist attacks whose only goal is to solicit and steal sensitive personal information.

Our study collected a limited amount of information from each user. Since we never met our users, we could not directly observe users' reactions, record comments, or probe for details during the study. Also, due to the remote nature of our study, there were many aspects we did not control that may have affected a user's vulnerability to our attack. For example, we did not control how many times a user could log in or the number of computers she could register. These factors are difficult to control in a field study such as ours without introducing artificial constraints.

Our study did not attempt to address any *high-beam* effects [31]. A high-beam effect refers to the situation where a driver may warn other drivers of upcoming law enforcement vehicles by flashing her high-beam headlights. A high-beam effect could arise in a user study that uses deception if users are debriefed at different times. A user who finishes earlier than others may inform them of the true purpose of the study before they have finished, which may introduce demand characteristics.

We chose not to control for high-beam effects in our study because we anticipated several problems with waiting to debrief all the users at once. One problem is that it may have affected the quality of users' exit survey responses. We expected that the duration for each user to finish the study would vary widely. This turned out to be the case. Many users finished within a week, but others took much longer, and one user never finished. If we had waited to debrief all the users at the same time, we were concerned the early finishers would have forgotten many details of the study – in particular, details about their behavior during the simulated attack. Another problem is that since our study employed deception, to ethically use a user's data, we must debrief her on the study's true purpose. If we had waited to debrief all the users at the same time, we were concerned that after early finishers had been paid, there may have been less incentive for them to respond to subsequent requests.

For these reasons, we felt it was necessary to debrief each user immediately after the simulated attack, obtain reconsent, and give her the exit survey. Although we did not attempt to measure any high-beam effects in our study, our potential subject pool was relatively large compared to our sample (200 vs. 1950), which at least minimizes the chances of any chatter among users.

Chapter 6

Dynamic pharming attacks

In this chapter, we show a new attack against Web authentication we call *dynamic pharming*. In a simple, static pharming attack, the adversary causes the victim's requests for the target domain to connect to a server under its control, typically by arranging for the victim's DNS queries for the target domain to return the adversary's IP address. In contrast, in a dynamic pharming attack, the adversary causes the victim's requests to connect to the legitimate server or its own, depending on the situation.

We show how an adversary can use dynamic pharming to infect the victim's browser with malicious Javascript and use this Javascript to hijack the victim's session with the target domain's legitimate server. Dynamic pharming enables an adversary to compromise all known authentication schemes for existing browsers, including passwords and machine authentication. In addition, the adversary can eavesdrop on sensitive content, forge transactions, sniff secondary passwords, and so on. This attack is particularly dangerous because it also affects cryptographic authentication mechanisms in browsers designed to resist man-in-the-middle attacks, such as client-side SSL.

6.1 Overview

Suppose the pharmer can control the results of DNS queries for `www.vanguard.com`, and users authenticate themselves to `www.vanguard.com`. The specific type of authentication used is not relevant to our attack.

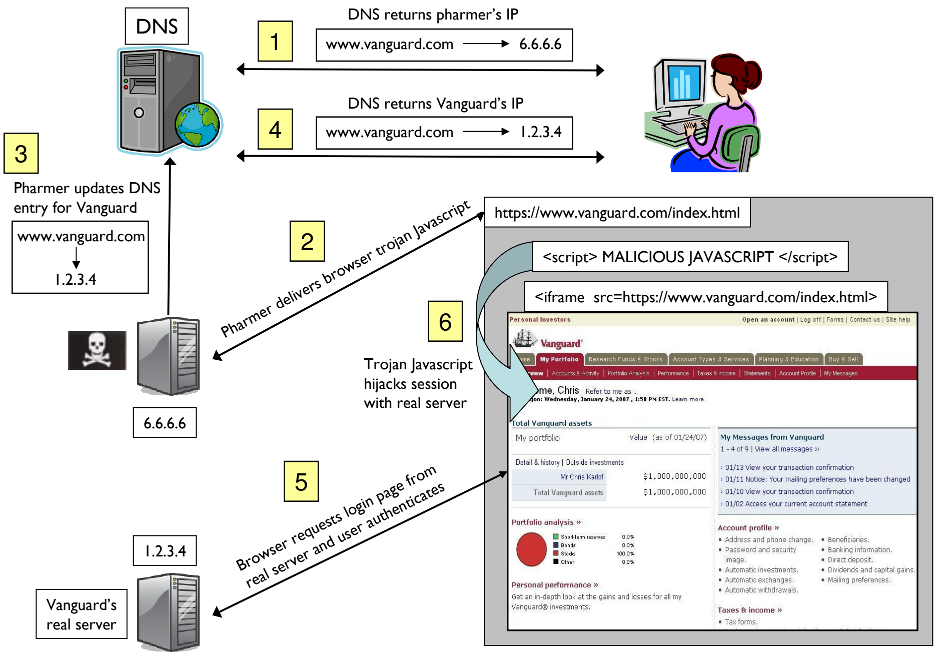

DNS
1
DNS returns pharmer's IP
www.vanguard.com → 6.6.6.6
4
DNS returns Vanguard's IP
www.vanguard.com → 1.2.3.4
3
Pharmer updates DNS entry for Vanguard
www.vanguard.com
1.2.3.4
2
Pharmer delivers browser trojan Javascript
6.6.6.6
https://www.vanguard.com/index.html
<script> MALICIOUS JAVASCRIPT </script>
<iframe src=https://www.vanguard.com/index.html>
6
Trojan Javascript hijacks session with real server
5
Browser requests login page from real server and user authenticates
1.2.3.4
Vanguard's real server
Vanguard
My Portfolio
Total Vanguard assets
My portfolio
Mr Chris Karlof
$1,000,000,000
Total Vanguard assets
$1,000,000,000
My Messages from Vanguard
Portfolio analysis »
Account profile »
Personal performance »
Taxes & income »

Figure 6.1: **An example of a dynamic pharming attack.** (1) Initially, the pharmer arranges for the victim's DNS queries for www.vanguard.com to resolve to the pharmer's IP address, 6.6.6.6. (2) Then, when the victim visits www.vanguard.com, the pharmer returns a trojan document containing malicious Javascript and a iframe referencing Vanguard's home page. (3) The pharmer then updates the DNS entry for www.vanguard.com to the IP address of Vanguard's legitimate server and denies subsequent connections from the victim. (4) This causes the victim's browser to renew its DNS entry for www.vanguard.com, and (5) load Vanguard's legitimate home page in the iframe. (6) After the user authenticates herself, the malicious Javascript in the trojan document hijacks her session with the legitimate server.

First, the pharmer initializes the DNS entry for `www.vanguard.com` to the pharmer's IP address, say 6.6.6.6. Now suppose a user Alice visits `https://www.vanguard.com/index.html` with the intention of authenticating herself. The user's browser will attempt to establish an SSL connection, requiring the pharmer to present an X.509 certificate. If the server certificate is not signed by one of the trusted CAs in the browser or the certificate's `CN` does not match the server's domain (i.e., `www.vanguard.com`), the browser will warn the user and ask her if it is safe to proceed. If the user heeds the warning and answers "no", the browser will cancel the connection and the attack fails. If the user accepts the pharmer's certificate—and there is substantial evidence that the user would (see

```
<html>
<body>
<script>
  ---MALICIOUS JAVASCRIPT CODE---
</script>
<iframe
src="https://www.vanguard.com/index.html">
</iframe>
</body>
</html>
```

Figure 6.2: **Dynamic pharming attack document.**

Section 2.1.3)—Alice's browser will establish an SSL connection to the pharmer at 6.6.6.6 and request `index.html`.

In response, the pharmer returns a "trojan" `index.html` document. The purpose of this trojan document is to monitor and influence Alice's subsequent interactions with the legitimate `www.vanguard.com`. We show the general structure of the trojan document in Figure 6.2. The attacker then causes the browser to load the legitimate `https://www.vanguard.com/index.html` document into the `<iframe>` and display it to the user. [1] We discuss the details of how the attacker accomplishes this in the next section.

Suppose the user now authenticates herself to `www.vanguard.com` in the `<iframe>` using any method supported in current browsers, e.g., password authentication or machine authentication via cookies or client-side SSL.[2] After authentication completes, the malicious Javascript in the outer document takes control and monitors the user's interactions in the `<iframe>` with the legitimate server for `www.vanguard.com`. Since the outer

[1] Iframes are HTML elements which enable embedded documents. To prevent infinite recursion, most browsers disallow nesting where the URL of the framed document is the same as an ancestor. To address this issue, the attack could redirect the victim's first request to `https://www.vanguard.com/index2.html` or arrange so that the legitimate home page from `www.vanguard.com` loads in a separate window.

[2] We use `www.vanguard.com` only as an example here, and there is nothing specific about our attack to `www.vanguard.com`.

document and the <iframe> both have the same domain (www.vanguard.com) and same protocol (https), the SOP will allow the malicious Javascript running in the outer document to access the content in the <iframe>. The trojan effectively hijacks control of Alice's session – it can eavesdrop on sensitive content, forge transactions, sniff secondary passwords, etc. We show an example of a dynamic pharming attack in Figure 6.1.

6.2 Attack details

In this section, we present two ways in which the adversary can cause the user's browser to load the legitimate https://www.vanguard.com/index.html document after previously connecting to the adversary.

6.2.1 Method 1: Proxying

One way to implement our attack is for the adversary to act as a port forwarding proxy tunnel between the user and the legitimate www.vanguard.com. After the adversary delivers the trojan attack document in Figure 6.2, it no longer responds directly to the user's HTTP requests, but instead forwards SSL packets back and forth between the user's computer and the legitimate www.vanguard.com. Since the first forwarded SSL packet will contain a session identifier unknown to the www.vanguard.com server, the server will re-initiate the SSL session with the user's browser. The user's browser will handle this automatically without any user involvement. After the SSL session renegotiation completes, the user's browser will be connected to the legitimate www.vanguard.com and the legitimate index.html will load in the iframe in the adversary's trojan document (Figure 6.2).

6.2.2 Method 2: DNS rebinding

One drawback of the proxying attack in the previous section is that when the adversary starts to forward the user's requests to www.vanguard.com, from Vanguard's perspective, the requests appear to originate from the adversary's IP address. This is undesirable because it may increase the likelihood that Vanguard is able to detect the attack. For example, Vanguard may be suspicious if the adversary uses a blacklisted IP address, uses an IP address in foreign country, or proxies many attacks through a single IP address. In this section, we describe a technique exploiting *DNS rebinding* vulnerabilities that enables the adversary to cause all requests to Vanguard during the attack (both from the user and from the adversary) to appear to have originated from the user's IP address. This enables the adversary to mount attacks (e.g., forge transactions) directly from the user's IP address, significantly reducing the chance of detection.

First, the pharmer initializes the DNS entry for `www.vanguard.com` to the pharmer's IP address, say 6.6.6.6, and the pharmer also indicates in the DNS record that requesters should not cache this result, i.e., it sets the TTL=0. After the pharmer returns the trojan document to Alice, it updates the DNS entry for `www.vanguard.com` to the IP address of the legitimate server for `www.vanguard.com`, say 1.2.3.4.

The adversary's goal is to force the user's browser refresh its DNS entry for `www.vanguard.com`, connect directly to Vanguard, and load the legitimate `https://www.vanguard.com/index.html` document into the `<iframe>`. However, one complication to this method is Web browsers' use of *DNS pinning*. With DNS pinning, a Web browser caches the result of a DNS query for a fixed period of time, regardless of the DNS entry's specified lifetime. Browsers implement DNS pinning to defend against variants of the "Princeton attack" [42], also known as *DNS rebinding* attacks. In the "Princeton attack", a malicious Web server first lures a victim who resides within a firewalled network containing privileged Web servers.[3] After the victim connects to the malicious server, the adversary changes its DNS entry to the IP address of a sensitive Web server located on the victim's internal network. The SOP restricts malicious code from accessing other domains, but since the adversary's domain now resolves to an internal IP address, this attack enables Javascript served by the adversary to access internal Web servers.

DNS pinning poses a problem for dynamic pharming attacks because once a browser resolves a domain name using DNS, it will continue to use the IP address and ignore any subsequent changes the pharmer makes in the DNS system. However, since DNS pinning

[3] Assume these servers are accessible only to machines behind the firewall.

"breaks the Web" in certain scenarios, e.g., dual homed IPv6-IPv4 servers, dynamic DNS, and automatic failover, browsers implementers have recently relaxed their DNS pinning policies.

Martin Johns discovered a technique for circumventing DNS pinning policies [61]. Johns discovered that a pharmer can force a victim to renew its DNS entry for a given domain on demand by rejecting connections from the victim, e.g., by sending an ICMP "host not reachable" message in response to subsequent attempts to connect to the server. The browser reacts by refreshing its DNS entry for the domain.

In the basic dynamic pharming attack, we exploit Johns's technique. After the pharmer delivers the trojan document to the user, it rejects subsequent requests from user's machine and updates the DNS entry for `www.vanguard.com` to the IP address of the legitimate server. Now, when the user's browser loads the `<iframe>`, it will first attempt to contact the pharmer, fail, refresh its DNS entry, receive the IP address of the legitimate server, and load the legitimate `index.html` document into the `<iframe>`. The attack continues as before.

Using round robin DNS. To parallelize dynamic pharming attacks against multiple concurrent users, it is inefficient to repeatedly update the DNS entry for `www.vanguard.com`. If the adversary has compromised a local, root, or authoritative DNS server, or changed the authoritative server of record for `www.vanguard.com`, the adversary can selectively respond with the pharmers IP or the legitimate server's IP depending on the stage of attack. However, if the adversary only has the ability to change DNS entries for `www.vanguard.com` on a DNS server (e.g., by cache poisoning), this attack is unscalable because the pharmer must update the DNS entry for each instance of the attack and reset it after the attack completes.

A pharmer can use round robin DNS entries to make this attack scalable. A round robin DNS entry consists of multiple IP addresses for a single domain name. The DNS server returns an ordered list of the IP addresses in response to a query, but rotates the order for each response. Web sites typically use round robin DNS to implement load balancing or automatic failover. Browsers usually connect to the first IP address in the list, and this achieves some degree of load balancing among clients. When the connection fails, the browser tries the next IP address on the list, until it successfully makes a connection.

To leverage round robin DNS entries in a dynamic pharming attack, the pharmers creates a round robin DNS entry containing two IP addresses: the pharmer's IP and the legitimate server's IP. Roughly half the DNS responses will be in the order: pharmer's IP, server's IP. In this case, the user will connect to the pharmer first, and the pharmer will deliver the trojan document. The pharmer rejects subsequent connections from the user, and the user's browser will automatically fail over to the legitimate server, after which the attack proceeds as before. For the other half of responses, the user will be delivered directly to the legitimate server and the pharming attack will silently fail. This shows how an attacker with the ability to replace a single DNS record, once, (e.g., by cache poisoning) can still attack thousands or millions of users.

6.2.3 Discussion

Dynamic pharming attacks do not leverage vulnerabilities in any particular authentication mechanism; rather, they exploit how browsers currently enforce the SOP. Since dynamic pharming hijacks the victim's session after she authenticates herself to the legitimate server, this attack most likely affects all known authentication mechanisms for current browsers, and probably all future ones as well.

In some cases, pharming attacks can also steal users' authentication credentials, e.g., passwords and machine authentication cookies. Since the users' URL bar will show the correct domain name, even the most meticulous user might be fooled into revealing her password. Also, since browsers enforce the SOP based on domain names, pharmers can steal user's machine authentication cookies for the target site. Although dynamic pharming attacks against client-side SSL authentication do not enable pharmers to steal users' authentication credentials (i.e., their private keys), as we have seen, they can compromise users' sessions in real time.

Some Web sites use Javascript to detect and prevent framing, e.g.,

```
if (parent.frames.length > 0)
   top.location.replace(document.location);
```

However, Javascript anti-framing techniques are not sufficient to resist dynamic pharming. Our attack does not depend on the use of iframes to be successful. For instance, the attacker could load the legitimate `index.html` in another tab or window. The SOP still allows malicious Javascript access to the second window, and this situation is much harder for the legitimate site to detect.

6.2.4 Proof of concept implementation

We implemented a proof of concept dynamic pharming attack using a pair of Apache SSL Web servers (i.e, a pharmer and a target) and round robin DNS. We tested the attack against two browsers: Firefox 2.0 running on Debian GNU/Linux 3.1 and Microsoft Internet Explorer 7.0 running on Windows XP Professional SP2. After the adversary delivers the trojan document, she refuses further connections from the client. This causes the browser to renew its DNS entry for the target domain and connect to the legitimate server, after which the adversary hijacks the session with the malicious Javascript in the trojan document. We found both browsers to be vulnerable to this dynamic pharming attack.

6.3 Library import and data export pharming vulnerabilities

Pharmers can also launch attacks by exploiting browsers' *library import* and *data export* features. Library import allows Web pages to import additional documents (e.g., Javascript libraries and cascading style sheets), for example:

```
<script type="text/javascript"
   src="https://xyz.com/login.js">
```

Data export allows Web documents to export information back to servers, e.g., by submitting a form. Many library import and data export features are not governed by the same-origin policy.[4] Browsers allow documents to import libraries from and export data to

[4] An example of an import/export mechanism that *is* governed by the same-origin policy is `XMLHTTPRequest`, which is restricted to sending and receiving requests to the domain of the enclosing document.

any domain. For example, a document from abc.com could import Javascript both from its own domain and from xyz.com and submit a form to foo.com.

Jackson and Barth discuss how pharmers can exploit these features [53]. One problem is that if a document imports a library containing executable code, e.g., Javascript, the code inherits the protection domain of the enclosing document. For example, if a pharmers hijacks control of DNS for xyz.com and a document from abc.com imports libraries from xyz.com, the pharmer can inject malicious Javascript into the document from abc.com, giving it access to other documents and objects from abc.com. A Web document can be vulnerable to these pharming attacks even if it only imports libraries from its own domain (either explicitly or via relative URLs). For example, suppose a pharmer has hijacked DNS for abc.com. If a document from abc.com imports a library from abc.com, instead of interposing on the main document, the pharmer can wait until the browser requests the library and supply a file containing malicious Javascript.

Pharmers can exploit similar vulnerabilities in data export features, such as form submission. If pharmer hijacks control of DNS for the domain of a form's target, it intercept the form submission and steal any sensitive information contained within, including cookies.

Chapter 7

The locked same-origin policies

Since dynamic pharming hijacks a user's session after initial authentication completes, this attack is independent of the authentication mechanism and affects all known authentication schemes for current browsers, including passwords, authentication cookies, and client-side SSL. It is therefore unlikely that any future Web authentication protocol developed for existing browsers will resist dynamic pharming either. Although dynamic pharming attacks leverage the implementation details of DNS pinning, "fixing" DNS pinning to resist DNS rebinding attacks is challenging. DNS pinning has a lengthy and controversial history in Firefox and Mozilla [83], and the current implementation is an explicit compromise to support dynamic DNS and round robin DNS for failover [82, 84]. From the browser's point of view, a dynamic pharming attack is indistinguishable from a failure of a site and DNS round robin recovery. Lastly, it is unlikely Web sites can resist dynamic pharming attacks effectively. The adversary has the advantage of loading her document first; she can read and modify all of the legitimate server's documents in the victim's browser, as well as control their execution environment.

To resist dynamic pharming, we must address the root of the problem: we must upgrade browsers' same-origin policy (SOP). A SOP based on domain names will fail because pharmers control the mapping from domain name to subject. For Web objects retrieved over insecure HTTP, it is unclear how the browser can distinguish a pharmer from the legitimate server. However, for objects retrieved over SSL, which we refer to as *locked Web objects*, we argue browsers should enforce the SOP using cryptographic identity.

A YURL based same-origin policy. A YURL [18] consists of a URL and a public key hash. The intention is for browsers to use the public key hash to authenticate the Web server using SSL before requesting the URL. For example, if browser requests a YURL for `xyz.com`, the browser uses DNS to resolve `xyz.com` to an IP address, and then establishes an SSL connection with the server. After a connection is established, the browser compares the public key hash in the YURL against the public key of the server. If the hash is consistent with the server's public key, the browser proceeds with the request; otherwise it cancels the connection with no opportunity for user override.

Upgrading browsers' same-origin policy to support YURLs is sufficient to resist dynamic pharming attacks against locked Web objects. The basic idea is to extend the notion of origin to include the public keys referenced in YURLs. A YURL based SOP would not consider two objects from the same origin unless: 1) their domains match, and 2) both objects were retrieved over SSL from servers with the same public key. This restriction would only apply to locked Web objects; for non-SSL Web objects, the legacy SOP (namely, using domain names) would still apply.

Unfortunately, this solution imposes a non-trivial deployment burden on Web sites. To take advantage of a YURL based SOP, a Web site must alter its servers to use YURLs in all places it currently uses HTTPS URLs, including all instances of library import and data export; otherwise the site may be vulnerable to the attacks discussed in Section 6.3. Since users do not type YURLs into the URL bar, a Web site must be careful to redirect all non-YURLs to YURLs before performing any sensitive operations, e.g., setting authentication cookies. These alterations must also be backwards compatible with legacy browsers.

Our goal is develop extensions to browsers' same-origin policy that provide comparable security to a YURL based SOP, but minimize the deployment burden for Web sites. Ideally, our goal is to develop solutions that require browser changes, but no or minimal server changes. In addition, we require our solutions to be backwards compatible with existing browsers and servers.

Towards achieving this goal, we propose two *locked same-origin policies*, which like the YURL based SOP, enforce access control based on cryptographic identity. We first present the *weak locked same-origin policy*, which isolates a domain's locked Web objects with valid certificate chains from objects with invalid chains. We then present the *strong* *locked same-origin policy*, which enforces access control based on Web sites' SSL public keys.

Both policies only apply new restrictions to locked Web objects. For non-SSL Web objects, the legacy SOP (namely, using domain names) still applies. Like the legacy SOP, both locked SOPs deny unlocked Web objects (that is, objects not retrieved over SSL) access to locked Web objects. We summarize our policies in comparison to the legacy SOP in Table 7.1.

7.1 The weak locked same-origin policy

The legacy SOP currently allows access to locked Web objects only from other locked Web objects originating from the same domain.[1] However, the legacy SOP does not distinguish between locked Web objects retrieved from a legitimate server with valid certificate and those from a pharmer spoofing the server's domain name with an invalid certificate, and will allow access if the user ignores any certificate warnings. To resist pharming attacks, the weak locked SOP augments the legacy SOP by tagging each locked Web object with a validity bit indicating whether the certificate chain corresponding to the SSL connection over which the object was retrieved contained any errors (e.g., self-signed certificate, CN/domain mismatch), irrespective of how the user responded to any certificate warnings. Then, the browser allows a locked Web object to access another locked Web object if and only if 1) the legacy SOP would allow access and 2) the validity bits match.

7.2 The strong locked same-origin policy

With the strong locked SOP, we propose browsers augment the legacy SOP by tagging each locked Web object with the public key of the other endpoint of the SSL connection (i.e., the Web server). Then, the browser allows a locked Web object to access another locked Web object if and only if 1) the legacy SOP would allow access and 2) the associ-

[1] Exception: if a Web site sets a non SSL-only cookie (i.e., without the `secure` attribute) over an SSL connection, then this policy allows the same domain to access the cookie over non-SSL connections as well. Essentially, a non SSL-only cookie set over an SSL connection gets downgraded to an unlocked Web object.

	Information used	Strongest threat model protected against for:		
Policy	to enforce access	Locked Web objects	Shared locked Web objects	Untrusted certs
Legacy SOP	(protocol,domain,port)	phishers	phishers	phishers
Weak locked SOP	(protocol,domain,port, validity of cert chain)	active attackers	phishers	phishers
Strong locked SOP (w/ policy files)	(protocol,domain,port, server public key)	active attackers	active attackers	active attackers

Table 7.1: **Comparison of our locked same-origin policies with the legacy same-origin policy.** This table shows the strongest threat model under which each policy can isolate a legitimate server's Web objects (e.g., cookies, HTML documents, etc.) from adversaries. *Locked Web objects* refer to objects retrieved over SSL. *Shared locked Web objects* refer to objects retrieved over SSL which are intended to be shared among subdomains of a higher-level domain (e.g., domain cookies). *Untrusted certs* refer to a legitimate server using a self-signed certificate or a certificate issued by a root CA untrusted by browsers.

ated public keys match. The strong locked SOP was inspired by Key Continuity Management [39, 45, 102, 143], a technique for associating public keys with subjects and taking defensive action when a subject's public key unexpectedly changes in a future interaction.

The strong locked SOP is similar to the YURL based SOP, but unlike the YURL based SOP, the strong locked SOP does not require Web sites to upgrade all instances of URLs into YURLs. The tradeoff is that while a YURL completely specifies a Web object's origin, an object's origin under the strong locked SOP is not completely specified until after the browser connects to the server and determines its public key. We discuss the consequences of this tradeoff in Section 7.7.

7.3 Security analysis

7.3.1 Weak locked same-origin policy

If a Web server hosting domain D (i.e., the target domain) uses a valid X.509 certificate signed by a trusted root CA, the weak locked SOP resists phishing, pharming, and active attacks against D's locked Web objects (i.e., illegitimate access by the adversary's Web objects) as long as the adversary is unable to obtain a valid certificate for D. The weak locked SOP resists phishing attacks because a phisher has a different domain name. For pharming and active attacks, the adversary can arrange for her Web objects to have the same name as the target domain, but if she does not have a valid certificate for the target domain, the validity bit will be `false`, while the validity bit of the Web server's locked objects will be `true`. Thus, the adversary is denied access.

If the legitimate target site uses an invalid X.509 certificate (e.g., expired, CN/domain mismatch, or self-signed), the weak locked SOP provides no additional protection over the legacy SOP. It resists phishing attacks, but does not protect against pharmers or active attackers.

In contrast to the legacy SOP, the weak locked SOP does not depend on users correctly answering prompts in response to certificate errors (e.g., if an adversary presents a self-signed certificate with a spoofed domain name). The browser tags locked Web objects according to the validity of the server's certificate and its domain name, and nothing else.

However, the weak locked SOP does assume that the trusted root CAs do not issue valid certificates for D to unauthorized parties. Although CAs take measures to prevent this, mistakes have been made in the past [80].

7.3.2 Strong locked same-origin policy

If a Web server hosting domain D uses an X.509 certificate with public key PK, the strong locked SOP resists phishing, pharming, and active attacks against D's locked Web objects as long as the adversary does not know the corresponding private key for PK. As with the weak locked SOP, the strong locked SOP resists phishing attacks because a phisher has a different domain name. In order to access D's locked Web objects, the adversary must pharm D and also arrange for its own objects to be tagged with PK. However, the browser will only do this if 1) the adversary presents a X.509 certificate with PK, and 2) the browser and adversary can successfully establish an SSL connection. If the adversary tries to present a certificate for PK and she does not know the private key corresponding to PK, she will not be able to successfully complete the SSL handshake; the browser will automatically cancel the connection with no option of user override. Thus, since the browser will only tag the adversary's locked Web objects with a public key different from PK, the browser will deny the adversary access to D's locked Web objects. For the same reason, the strong locked SOP protects D's locked Web objects against active attackers as well.

As with the weak locked SOP, the strong locked SOP does not depend on users correctly answering prompts in response to certificate errors. Furthermore, in contrast to the weak locked SOP, the strong locked SOP does not require a Web site to trust root CAs not to issue certificates to unauthorized parties for its domain. Enforcement relies only on servers' public keys.

7.4 Deployability analysis

If our locked same-origin policies are to be successful, they need to be easy to deploy and backwards compatible; they should not "break the Web" because of problems with deployment or interoperability with existing Web servers. Since no browser developer is likely to embrace a policy that makes her browser incompatible with existing Web sites, legacy Web servers had better continue to work even when visited with locked SOP enabled browsers.

Our policies are more restrictive than the legacy SOP, but we only want to deny access to an attacker – never the legitimate server. We will "break" a Web site if there is a situation where our policy would deny a legitimate server access to one of its locked Web objects, but the legacy SOP would allow access.

There are a few situations where our policies could potentially break a Web site. For example, suppose server A for `xyz.com` has an valid certificate, but server B for `xyz.com` has an invalid certificate (or vice versa). Then the weak locked SOP would deny Javascript from server A from accessing an HTML document from server B, but the legacy SOP would allow access. This situation might arise if `xyz.com` uses round robin DNS for load balancing and a browser request objects from both servers during a session. Note that the weak locked SOP will not break a domain which uses invalid certificates on all its servers (e.g., it uses self-signed certificates) since objects from these servers have equivalent validity: they are all invalid.

If server A and server B use different public keys, then the strong locked SOP would also deny access. However, the strong locked SOP does not necessarily require the domain to use certificates issued by a root CA trusted by browsers. As long as all servers use the same public key, the Web site can use certificates issued by a root CA untrusted by browsers or self-signed certificates.

7.4.1 An SSL server survey

To evaluate the deployability of our policies, we must determine how many sites we could potentially break; in other words, how often the above configurations actually arise in practice. To measure this, we surveyed SSL servers in the real world to determine how many servers may not currently interoperate with our policies. We constructed a sample of SSL servers by first crawling the Web, starting from a list of major news, portal, and financial sites. Whenever we found an HTTPS link, we added the domain in the link to our sample. For the sake of simplicity, we restricted our study to the following top-level domains: com, org, net, gov, edu, biz, info, and name. We excluded international top-level domains. We found 14651 fully qualified SSL domains from 6192 second-level domains.[2] This corresponds to roughly 6.5% of the number of SSL domains found by the more extensive monthly SSL survey conducted by E-Soft and securityspace.com [109].

We are primarily interested in finding domains hosted by multiple servers, since it is these domains that our policies could potentially break. We can discover some servers by looking for use of round robin DNS; if a server uses round robin DNS, a DNS query returns a list of IP address. However, Akamai-style load balancing often considers the physical location of the DNS querier and may only return the IP address of most appropriate server. To take Akamai-style load balancing into account, we constructed a list of servers for each domain by requesting recursive DNS queries to 15 geographically distributed public DNS servers [125].[3] Of the 14651 domain names, we found 1464 that resolved to multiple IP addresses. For each of these domains, we established an SSL connection to each of the domain's servers and recorded each server's certificate chain and public key.

7.4.2 Certificate chain validation: Firefox and IE

The next step was to validate the certificates we collected. To maximize the practical relevance of our study, we simulated the validation procedures of Firefox 2.0 and Internet Explorer 7.0. The validation procedures of Firefox and IE are close to the process we described in Section 2.1.3, but there are some differences in how each browser handles missing and expired intermediate CA certificates. Intermediate CA certificates are certifi-

[2] For our study, a second-level domain means the last two components of a non-international fully qualified domain name, e.g., yahoo.com.

[3] A limitation of this approach is that we cannot discover multiple servers behind a front-end load balancer with a single IP address.

Browser	Session caching of CA certs	Persistent caching of CA certs	Uses AIA
IE	✓	✓	✓
Firefox	✓		

Table 7.2: **Summary of browser mechanisms used to address missing and expired intermediate CA certificates.** AIA refers to the optional Authority Information Access X.509 extension.

cates issued by a CA's root certificate which it uses to directly issue certificates to Web servers. This results in certificate chains of length 3 or more. Since most browsers only ship with root CA certificates, to guarantee a client can verify its chain, a server must also send any intermediate CA certificates in addition to its own.

Unfortunately, many servers are not configured to send intermediate CA certificates. Also, there are several widely used intermediate CA certificates which have expired, and although the CA has reissued a replacement with the same name (and often, the same public key), many servers have not updated them and are still sending the expired version. We found that Firefox and Internet Explorer handle these situations slightly differently. We determined each browser's validation procedure through source code analysis, empirical testing, and various public sources [40, 85, 86].

First, both Firefox and Internet Explorer cache the intermediate CA certificates they encounter during a user's browsing session and use this cache to help verify certificate chains. This means if the user visits a site with a missing intermediate CA certificate, and previously in the session, the user visited a different site using the same intermediate certificate, the browser uses the cached copy to verify the chain. In addition, if the user visits a site which sends an expired intermediate CA certificate, both Firefox and Internet Explorer will automatically replace it with the more recent version if they have seen it previously in the session.

Internet Explorer takes some additional measures to address missing intermediate CA certificates that Firefox does not. First, in addition to caching intermediate CA certificates within a session, Internet Explorer caches these certificates persistently, across sessions. Second, Internet Explorer takes advantage of the Authority Information Access (AIA) extension included in some X.509 certificates. The AIA extension "indicates how to access CA information for the issuer of the certificate in which the extension appears" [106]. We found for many server certificates issued by an intermediate CA certificate, they include the AIA extension with a URL for the intermediate CA certificate, and Internet Explorer automatically downloads and uses it to verify the chain. Firefox does not use the AIA extension. It is unclear exactly why not, but discussions on Mozilla Bugzilla suggest it might be because some of the Mozilla developers believe the AIA standard is not well specified [85]. As a result of these additional mechanisms in Internet Explorer, Firefox generates more certificate warnings on average for sites with missing or expired intermediate CA certificates. We summarize these differences in Table 7.2.

7.4.3 Evaluation results

Weak-locked same-origin policy

To evaluate the deployability of the weak locked SOP, we validated the servers' certificate chains in our survey using two procedures: Pessimistic Validation and Optimistic Validation. Pessimistic Validation models the worse case scenario: a Firefox user visits a Web site with a missing or expired intermediate CA certificate at the start of a session, or a user freshly installs IE and visits the same site, and the server certificate does not support AIA. Through empirical analysis we identified 18 widely used intermediate CA certificates, and for Optimistic Validation, we assume the user's browser has cached valid versions of these certificates. We intend Optimistic Validation to model a long Firefox session or a "broken in" Internet Explorer installation with a substantial intermediate CA certificate cache.

Then, for the 1464 fully qualified SSL domains which use multiple servers, we counted the number of domains which had servers with both valid and invalid certificate chains, since it is these domains that the weak locked SOP may break. Using Pessimistic Validation, we found 8 such domains, and for Optimistic Validation we found 4 domains. For each of the other 1456 domains, its servers either had all valid certificates or all invalid certificates.

The difference between the Optimistic and Pessimistic Validation results means we

Policy	Percentage of potentially non-interoperating domains
Weak locked SOP	0.05%
Strong locked SOP	0.6%

Table 7.3: **Summary of our deployability analysis of the locked same-origin policies using a sample of 14651 SSL domains.** This table shows the percentage of domains in our survey which may not correctly interoperate with the locked same-origin policies.

found 4 domains that contained a mix of servers with missing or expired intermediate certificates and correctly configured servers. Of the 4 remaining domains which still cause problems with Optimistic Validation, 3 are probably the result of virtual hosting issues. For example, of the 3 servers we found for `signin.half.ebay.com`, one had a valid certificate, and the other two had CN/domain name mismatch problems. These two servers presented certificates for `signin.ebay.com`. The remaining problem domain was the result of an expired certificate on one of its servers. When the domain's administrators updated their certificates, they probably overlooked this server.

This means the weak locked SOP would potentially break at most 0.05% of the SSL domains we found in our survey. These results are strong evidence that browsers could enforce the weak locked SOP today and still interoperate with the vast majority of Web sites while providing increased protection against pharming attacks. Furthermore, since the number of problem domains is relatively small, browser developers can conceivably work with these domains' administrators to make their servers consistent. In conclusion, we can safely deploy the weak locked SOP in a way which requires minor browser changes, but does not require changes to the HTTP specification, SSL, or Web servers.

Strong locked same-origin policy

To evaluate the deployability of the strong locked SOP, we counted the number of fully qualified SSL domains with multiple servers that do not use the same public key on all of the servers. We found 83 such domains, representing 0.6% of the total number of SSL domains in our survey. This is problematic for two reasons. First, it represents an order of magnitude more servers than that are affected by the weak locked SOP. Second, unlike before, these servers are not necessarily misconfigured, so browser developers cannot work with the domain's administrators to "fix" the problem. Using a different key on each server is good security practice, since it limits the scope of key compromise. In fact, VeriSign explicitly recommends customers use different public keys on each server [124].

Another problem concerns certificate expiration. The business model of many CAs is to issue certificates that are valid only for a relatively modest period of time, e.g., one or two years, and require customers to renew their certificates when they expire. When Web sites renew their certificates they often follow good security practice and generate a new public key. Since the strong locked SOP applies to all locked Web objects, if a Web site uses persistent SSL-only cookies to authenticate users (see Section 7.10), every user's cookie will simultaneously "expire" (i.e., become inaccessible by the server) when the site starts using the new public key, regardless of the value of the cookie's `expires` attribute.

Based on this evidence, we conclude browsers cannot currently enforce the strong locked SOP without potentially breaking a significant number of Web sites. However, this does not mean that deploying the strong locked SOP is hopeless; it only means a browser must first get the site's explicit cooperation and approval to enforce it. In the next section, we describe a simple incrementally deployable solution using policy files for the strong locked SOP which supports multiple public keys and key updates.

7.5 Policy files for supporting multiple keys and key updates

We propose an incrementally deployable solution where a Web site can opt in to the strong locked SOP; then, browsers which support the policy can safely enforce it without the risk of unintentionally breaking the site. To opt in, we propose a site's servers post a policy file with a well-known file name, say `pk.txt`. Sites can notify clients that they support the strong locked SOP, e.g., via a special HTTP header. Legacy clients will ignore this header. Compatible Web clients can retrieve the `pk.txt` file over SSL, parse it, and start enforcing the strong locked SOP for that domain.

If all the domain's servers use the same public key and persistent objects are not an issue, a site can simply post an empty `pk.txt`, since it will already interoperate with the strong locked SOP. If the site uses multiple servers, labeled $i = 1 \ldots n$, with different public keys, then `pk.txt` on server k contains a list of the form:

$$(pk_1, \{pk_k\}_{sk_1}),\ (pk_2, \{pk_k\}_{sk_2}),\ \ldots,\ (pk_n, \{pk_k\}_{sk_n})$$

where pk_k is the public key of the server hosting this `pk.txt` file and $\{pk_k\}_{sk_i}$ represents a signature of pk_k by the secret key corresponding to pk_i. The browser then verifies each of the signatures, and for $i = 1 \ldots n$, if the i^{th} signature is valid, then it considers pk_k to "speak for" pk_i. We then extend the strong locked SOP with the following rule: a browser allows a locked Web object tagged with (D, pk_j) to access another locked Web object tagged with (D, pk_l) if a policy file attests that pk_j speaks for pk_l.

Note that `pk.txt` cannot simply list the public keys $(pk_1, pk_2, \ldots, pk_n)$; otherwise a pharmer can serve the same file to a victim, and the victim's browser will infer that the pharmer's public key speaks for each of the keys of the legitimate servers. However, since the pharmer does not know the legitimate servers' private keys, it will not be able to generate any valid signatures required for the victim's browser to infer the "speaks for" relation.

Policy files also address the problem of public key updates discussed in Section 7.4.3. For example, suppose a Web site wants to renew its certificate with a new public key pk_{new}. Then, several months before the certificate expires, the site can include $(pk_i, \{pk_{\text{new}}\}_{sk_i})$ in its `pk.txt` files for each server i, $i = 1 \ldots n$. Then, users that retrieve `pk.txt` during this transition period will not "lose" persistent objects tagged with an old public key.

In conclusion, policy files address the deployability problems with the strong locked SOP we identified in Section 7.4.3. They enable us to enforce the strong locked SOP in current browsers in a way which is incrementally deployable and backwards compatible with legacy servers. The strong locked SOP in conjunction with policy files requires browser changes and server configuration changes for sites wishing to take advantage of the policy, but does not require changes to the HTTP specification or SSL.

7.6 Support for subdomain object sharing

Up until now we have implicitly assumed a Web site consists of a single fully qualified domain name, e.g., `www.xyz.com`. More generally, a Web site might be composed of several domain names, e.g., `mail.xyz.com`, `www.xyz.com`, `login.xyz.com`, and the legacy SOP supports some exceptions which enable these sites to share information among subdomains through certain Web objects. For example, a user might authenticate herself to the server for `login.xyz.com`, and this server will set a domain cookie with `domain=xyz.com` for authenticating the user to the other subdomain servers. The user's browser will allow any subdomain of `xyz.com` to access this cookie. Another way subdomains can share information is by setting the DOM property `document.domain`. For example, if a document from `www.xyz.com` sets `document.domain=xyz.com`, the browser permits any object from a subdomain of `xyz.com` to access the document.

However, these domain sharing mechanisms are vulnerable to pharming attacks. For example, if an adversary pharms any host name in `xyz.com`, she can steal users' domain cookies for `xyz.com`. Ideally, we would like to enforce our locked same-origin policies in these situations as well. Fortunately, extending the strong locked SOP to support subdomain sharing is straightforward with policy files. The site simply adds the servers' public keys to its policy files and we extend the strong locked SOP with the following rule: if S is locked Web object hosted by server l and is designated to be shared among subdomains of a higher-level domain TD (e.g., `xyz.com`), a browser allows a locked Web object tagged with (D, pk_j) to access S if D is a subdomain of TD and a policy file attests that pk_j speaks for pk_l.

Unfortunately, it is not clear how to extend the weak locked SOP to support shared domain objects without any server cooperation. An natural candidate extension would be to allow access if both subdomain servers have valid certificates or invalid certificates. However, we must have confidence this policy will not "break the Web" and not deny access to a legitimate server when the legacy SOP would allow access. Roughly, this would require for each higher-level domain, either all its subdomain servers have valid certificates or all its subdomain servers have invalid certificates. Unfortunately, our survey survey shows this is far from the case. Of the 6192 second-level SSL domains we found, over 1000 did not satisfy this property. This means for browsers enforcing the weak locked SOP, they must default back to the legacy SOP for shared domain objects, which provides no protection against pharming.

7.7 Support for library import and data export

In Section 6.3, we discussed pharming vulnerabilities with library import and data export features in browsers. Many import and export features are not governed by the same-origin policy. Web sites can import libraries from and export data to any domain. Since Web sites routinely use import and export features, without additional protection mechanisms, the locked same-origin policies alone are insufficient to protect sites from pharming attacks. Using YURLs for all library import and data export operations resists pharming and active attacks because a YURL explicitly specifies the public key of the server hosting the library or receiving the data. However, as we discussed at the beginning of this chapter, YURLs may be troublesome for Web sites to manage and deploy. In this section, we discuss some alternative solutions for protecting library import and data export features that work in conjunction with the locked same-origin policies to resist pharming and active attacks.

7.7.1 With the weak locked same-origin policy

The weak locked same-origin policy isolates a domain's locked Web objects with valid certificate chains from objects with invalid chains. Our goal is to provide similar guarantees for Web documents that use library import and data export features. Currently, many browsers will display a warning if a document imports from or exports to a server with an invalid certificate. This warning may be a "ribbon-type" warning, a pop up warning, or a full page warning, depending on the browser and the circumstances. Many of these warnings offer a user override option, which allows the import or export to continue, potentially compromising the integrity of the Web application during a pharming or active attack.

One solution to this problem we propose is a variant of YURLs we call *weak* YURLs. A weak YURL is an HTTPS URL together with a bit flag indicating that the browser should only connect to a server that provides a valid certificate for the domain in the URL. The security properties of weak YURLs are similar to those the weak locked same-origin policy. In conjunction with the weak locked same-origin policy, weak YURLs resist pharming and active attacks against library import and data export operations as long as an adversary can not obtain a valid certificate for the target domain. If the adversary attempts to intercept the import or export operation, it will cause a certificate error, and the browser will cause the operation to fail without any option for user override.

An advantage of weak YURLs over "strong" YURLs is that weak YURLs are easier to manage and deploy. Strong YURLs require Web sites to maintain an accurate list of public keys for the servers involved in library import and data export operations. Some Web sites import libraries from "third parties", for example the home page for `www.paypal.com` includes the following import:

```
<script type="text/javascript"
   src="https://www.paypalobjects.com/...">
```

If the server for `www.paypalobjects.com` updates its public key and `www.paypal.com` fails to update its "strong" YURL to use the new public key, this import will fail, potentially breaking the functionality of the application. Weak YURLs avoid this problem. As long `www.paypalobjects.com` always uses a valid certificate, then a weak YURL will always resolve successfully (except during an attack, of course). One easy protocol to take advantage of weak YURLs is for a Web site to include a special HTTP or HTML header indicating that compliant browsers should interpret all URLs in the document as weak YURLs.

A disadvantage of this solution is that unlike the weak locked same-origin policy, weak YURLs require minor server modifications. However, if the enclosing document was fetched from a server with a valid certificate, we argue that browsers could by default safely interpret all "first-party" URLs (i.e., URLs with the same domain as the enclosing document, including relative URLs) in import and export operations as weak (valid) YURLs with little risk of breaking those applications. In other words, if the enclosing document was fetched from a server with a valid certificate, all import and export operations (in the enclosing document) to the same domain must also be to a server with a valid certificate, otherwise the operation will fail with no chance of override. This would only cause a problem if a domain has multiple servers with a mix of valid and invalid servers, and only 0.05% of the domains in our survey had this property (Section 7.4.3). This policy does not require any server changes and helps Web applications that only import from and export to their originating domain resist pharming and active attacks.

7.7.2 With the strong locked same-origin policy

To resist pharming and active attacks against import and export operations in conjunction with the strong locked same-origin policy, we propose extending the policy file mechanism in Section 7.5. To authorize a domain for import or export operations, a Web site includes the domain and its associated public keys in the policy file. Although, conceptually this is similar to using YURLs for all import and export operations, we argue that this solution is easier for sites to deploy than YURLs. Policy files allow sites to consolidate the public keys of the import/export servers in a single location without requiring significant changes to their server infrastructure or Web application framework.

7.8 Caching

Browsers do not by default persistently cache HTTPS Web objects (except SSL-only cookies), but they do use session caching. As we demonstrated in Chapter 6, adversaries can use the cache to launch subtle dynamic pharming attacks. To resist attacks involving the browser cache, compliant browser must be careful to apply the locked same-origin policies to cache elements as well.

7.9 Limitations

Our locked same-origin policies do not address attacks where the adversary tricks a victim into installing malicious software such as executable malware, an ActiveX plugin, or a browser extension. These objects usually execute with elevated privileges and are not governed by the SOP.

The locked same-origin policies must also be incorporated into plugin architectures such as Flash, Java, and Adobe Reader. To resist pharming and active attacks, these architectures must enforce the locked same-origin policies for network requests and other accesses done on behalf of plugins. Also, some plugins architectures allow direct socket access, and the locked same-origin policies cannot govern network requests made using direct socket access. We consider it the Web site's responsibility to provide appropriate protections when direct socket access is used.

The locked same-origin policies do not address problems in the Javascript language or implementation (e.g., Javascript Prototype Hijacking) [92], cross-side scripting (XSS) vulnerabilities in servers, and cross-site request forgery (XSRF) attacks. Other research efforts address XSS vulnerabilities [43, 51, 74, 79, 107, 137, 138] and XSRF attacks [10, 60, 63, 64], and these techniques complement our work. We also do not address browser-side cross-site scripting vulnerabilities, such as Universal XSS [92].

7.10 Applications to Web authentication

In this section, we discuss how the locked same-origin policies can help protect two existing machine authentication mechanisms, client side-SSL and SSL-only cookies, against pharmers and active attackers. However, the Web authentication problem is actually two distinct subproblems: the initialization of users' authentication credentials, i.e., the registration problem, and the use of those credentials to authenticate users to Web sites. Our discussion in this section focuses primarily on the latter; we discussed the registration problem in Chapter 4.

7.10.1 Client-side SSL

Intuitively, since client-side SSL authenticates users with end-to-end cryptography, one might expect it would protect sensitive Web sessions against pharming and active attacks, but unfortunately, the presence of dynamic pharming vulnerabilities proves this is not the case. However, using the strong locked same-origin policy in conjunction with client-side SSL results in an authentication scheme with strong security properties. The user is not required to memorize her private key. After the user imports her private key, her browser uses it automatically. Although an adversary may be able to trick a user into participating in mutual authentication using SSL, the adversary cannot use this interaction to impersonate the user at another Web site. Authentication requires knowledge of the private key, which the user's browser always keeps secret. As a result, the browser authenticates the user's requests cryptographically and the strong locked SOP isolates the user's authenticated sessions from malicious subjects – even if the adversary is a pharmer or active attacker.

7.10.2 SSL-only cookies

Many Web sites use cookies for machine authentication. For example, some Web sites offer a "remember me" option, which sets a persistent cookie on a user's machine. The browser will present this cookie during subsequent visits to the Web site, enabling the user to bypass the initial login process. Some existing anti-phishing solutions also use machine authentication cookies to complement regular password authentication. Examples include Bank of America's SiteKey [9] and similar approaches by ING Direct [52], Vanguard [123], and Yahoo [139]. In current browsers, cookie authentication resists phishing attacks but is vulnerable to pharming attacks. Our locked same-origin policies protect SSL-only cookies against pharmers and active attackers. Thus, in conjunction with browsers enforcing a locked SOP, Web sites can use SSL-only persistent cookies to authenticate users and resist phishing, pharming, and active attacks.

7.10.3 Other authentication mechanisms

The locked same-origin policies nicely complement other authentication mechanisms designed to resist pharming, such as Phoolproof phishing prevention [93] and Passpet [142]. Our policies also help these schemes resist dynamic pharming attacks. For more information on these mechanisms, see Chapter 8.

Chapter 8

Related work

8.1 Anti-phishing mechanisms

Several anti-phishing mechanisms help provide information to users regarding the trustworthiness of Web sites. Since studies have shown that users can be fooled by misleading domain names and do not understand browser security indicators [24, 25, 35, 37, 49, 56, 108, 130, 135], several researchers and security vendors have developed browser extensions to make it easier for users to interpret relevant security information [17, 49, 78, 114], use a blacklist to help identify known phishing sites [27, 88], or establish trusted paths with sites users have a relationship with [23, 136, 140]. Recent versions Firefox and Internet Explorer have adopted similar mechanisms. However, these approaches still expect some degree of diligence from users to reliably observe security warnings and indicators to operate securely, and studies have shown that users still have troubling interpreting improved security indicators and warnings [56, 108, 135, 136]. In addition, studies have also shown that many browser extensions which try to automatically detect phishing sites are often wrong and inconsistent [145].

8.2 Phishing and pharming resistant authentication

Another approach to resisting phishing attacks is better password management. Passwords are still the dominant method of Web authentication. Password databases included with most modern Web browsers automatically fill in passwords for users. However, users might still manually disclose their passwords to phishing sites or use the same password for multiple sites. Password hashing addresses these problems by hashing the user's secret password together with a variable, non-secret string (e.g., each site's domain name) to produce per-site passwords [1, 36, 47, 71, 72, 104, 142]. Recent work in this area has made usability one of the primary goals [47, 104, 142], but studies have shown some users still have trouble using them correctly and securely [15]. Also, if a password hashing scheme generates passwords based on the site's domain [47, 104], it is vulnerable to pharming attacks. Passpet [142] provides some resistance to pharming attacks, but is still vulnerable to dynamic pharming.

The Phoolproof phishing prevention system uses cell phones to manage client-side SSL certificates for authentication on behalf of users [93]. In Phoolproof, a user logs in using a secure bookmark on her cell phone. The cell phone then 1) initiates an SSL connection to the Web site via a Bluetooth connection with a Web browser on the user's computer; 2) checks the site's X.509 certificate against the one stored in the bookmark; and 3) authenticates the user via client-side SSL. Although Phoolproof verifies the site's certificate in step 2, this protocol is still vulnerable to a dynamic pharming attack if the adversary is able to pharm the user (i.e., serve the user a Web page which appears to come from the target domain) before she activates the login process.

ForceHTTPS is a browser policy designed to help resist pharming and active attacks by making certificate errors less ambiguous to the browser [54]. When a Web site opts in to ForceHTTPS, the browser does not allow users to override certificate errors for the site's domain and refuses to import non-HTTPS libraries for the site's documents. ForceHTTPS stores the "opt-in" information in a cookie. Since, like all cookies, ForceHTTPS cookies can be used to track users, ForceHTTPS allows users to clear ForceHTTPS cookies, after which time users are vulnerable to pharming attacks until the site can reset the cookie.

8.3 Key Continuity Management and applications

The locked same-origin policies were inspired by the concept of Key Continuity Management (KCM), a model for key management first proven successful by SSH [102, 143] and later made more explicit by Gutmann [45]. KCM associates public keys with subjects and takes defensive action when a subject's public key unexpectedly changes. Garfinkel expands on KCM further, and applies it to S/MIME [39].

The locked same-origin policies are similar to work done independently and concurrently by Masone et al. on Web Server Key Enabled Cookies, a new cookie policy inspired by KCM that tags SSL-only cookies with the server's public key and allows access only to a server which can authenticate itself to the same key [76]. However, their proposal falls short of protecting cookies against dynamic pharming attacks. Also, they do not address pharming attacks against other Web objects or other Web authentication mechanisms, e.g., client-side SSL, nor do they address subdomain object sharing or key updates.

8.4 DNS rebinding

Security researchers and browser developers have been aware of DNS rebinding vulnerabilities since as early as 1996 [42]. In 2001 and 2002, Jim Roskind and Adam Megacz, resp., described firewall circumvention DNS rebinding attacks using DNS records with short TTLs [77, 103]. DNS pinning was adopted by browsers to defend against these kinds of attacks, but pinning has a lengthy and controversial history in Firefox and Mozilla [82, 83, 84]. The current implementation is an explicit compromise to support dynamic DNS and round robin DNS for failover. In August 2006, Martin Johns discovered a reliable technique for circumventing DNS pinning completely [61], and in early 2007, Johns and Kanatoko found additional DNS rebinding vulnerabilities with Flash and Java [62, 67].

Jackson et al. present a comprehensive analysis of DNS rebinding vulnerabilities, including issues with Flash, Java, VPNs, caching, and proxies [55]. They discuss several countermeasures, including host name authorization, a technique based on a variant of reverse DNS lookups. With cooperation from Web sites' DNS servers, host name authorization enables clients to determine the valid set of domain names for a particular IP address.

Host name authorization is promising approach, but since it relies on DNS, it is ineffective against adversaries capable of subverting DNS.

8.5 Email for authentication

Other researchers have proposed leveraging email for authentication [3, 8, 38, 44, 122]. In particular, the design of Simple Authentication for the Web (SAW) by Horst and Seamons is similar to our email registration ceremony [122]. The main difference is that we propose using email only for relatively infrequent machine registrations, i.e., credential initialization, while the SAW authors propose using email authentication as a direct replacement for passwords. In SAW, users receive a fresh email link during each authentication attempt. Also, the SAW authors do not consider social engineering attacks that try to steal authentication links.

8.6 Studies that attack users

Security researchers have conducted a number of studies that simulate attacks against users. Several studies have tried to evaluate how well individuals can identify phishing emails and pages [24, 56, 135]. However, these studies do not fully address the design issues we identified in Section 5.1. They were all conducted in a laboratory environment, and the users were either told the purpose of the experiment or asked to role-play a fictitious identity.

To help create the experience of risk, some laboratory studies have employed deception and required users to participate with their own accounts. Egelman et al. conducted such a study to evaluate the effectiveness of browser phishing warnings [28]. Users made purchases with their own credentials, and the researchers sent the users spear phishing emails related to those purchases which triggered phishing warnings in Firefox and Internet Explorer. Schecter et al. asked real Bank of America SiteKey customers to log into their accounts from a laptop in a classroom [108]. Although SiteKey uses challenge questions, Schecter et al. did not evaluate SiteKey's use of them. Instead, they focused on whether each user would enter her online banking password in the presence of clues indicating her connection was insecure. They simulated site-forgery attacks against each user by removing various security indicators (e.g., her personalized SiteKey image) and causing certificate warnings to appear, and checked if each user would still enter her password. Since SiteKey will only display a user's personalized image after her computer is registered, Schecter et al. first required each user to answer her challenge questions during a "warm-up" task to re-familiarize her with the process of logging into her bank account. No attack was simulated against the users during this task.

Requiring users to use their own accounts is certainly a good start for creating a sense of risk, but the degree to which the academic setting of the physical location of these studies affected the users' evaluation of their actual risk is unclear. Even if the experimenters were not in the same room as the users while they used the computer, the fact that they were nearby may have influenced the users to appear "helpful" and behave with less caution than they normally would.

A few studies have simulated attacks against users in the field without obtaining prior consent. One study at the United States Military Academy at West Point sent cadets a simulated phishing email from a fictitious Colonel "commanding" them to click on a link [31]. Studies by Jagatic et al. [57] and Jakobsson et al. [58] also remotely simulated phishing attacks against users. Although these studies closely simulated real attacks, provided large data sets, and achieved a high level of ecological validity, the absence of prior consent raises ethical issues. After learning that they were unknowing participants in one study, some users responded with anger and some threatened legal action [19]. Also, these studies collected only a limited amount of demographic and behavioral data and did not conduct a exit survey to probe users' decisions.

8.7 User conditioning and education

Previous anti-phishing research has attempted to take advantage of user conditioning by using secure attention keys. Two anti-phishing tools, PwdHash [104] and Web Wallet [136], employ a secure attention key to create a trusted path between the user and the browser. Although these tools require users to activate the secure attention key before entering any sensitive information, they may be vulnerable to attacks which persuade users to omit the SAK (Section 3.3.1). A user study of Web Wallet suggests that this attack strategy can be effective [136].

Related to conditioning is training and education. Several researchers have proposed innovative educational methods for teaching users about Internet security and social engineering attacks [73, 111, 132]. Their initial results are promising, and related research suggests that users who better understand Internet risks may be more likely to resist attacks [26]. However, user education may have its limitations. If education is not periodically reinforced, satisficing users may forget or omit defensive habits they have learned. Also, a study consisting of interviews designed to reveal users' decision making strategies for suspicious emails suggests that while users may be able to manage risks they are familiar with, it can be difficult for them to generalize this knowledge to resist unfamiliar attacks [25]. These results suggest that educational approaches may require continual adaptation to address new attacks; otherwise users' defensive strategies may become outdated and ineffective.

Chapter 9

Conclusion

Over the last decade, social engineering attacks on Internet, such as phishing, have grown considerably, and we anticipate human factors will remain one of the most important and challenging aspects of computer security for the foreseeable future. Although users are often considered the weakest link in computer security, few security mechanisms address this problem constructively. To remain safe, many current ceremonies burden users to detect attacks and refrain from actions they often instinctively perform to complete routine tasks, e.g., entering their usernames and passwords.

Our user study results suggest that 1) ceremonies can affect user behavior, for better or worse, and 2) the resiliency of a ceremony to social engineering is related to whether the actions it conditions users to take are safe to perform in the presence of an adversary. These results suggest that conditioned-safe ceremonies may be a useful notion for building user-centric ceremonies that resist social engineering attacks. We proposed several design principles for conditioned-safe ceremonies and described one ceremony, email registration, designed according to these principles. Although email registration may be an imperfect approximation of what we would ultimately like out of a conditioned-safe ceremony, we believe it is nonetheless a useful example for exploring and evaluating this notion further.

Stronger social engineering threats, e.g., pharming, have also become more visible over the last decade, and it vital that we develop mechanisms to resist these attacks. We demonstrated how adversaries can use dynamic pharming attacks to hijack users' authenticated sessions in current browsers, irrespective of the authentication mechanism. Dynamic pharming enables an adversary to eavesdrop on sensitive content, forge transactions, sniff secondary passwords, etc. To address dynamic pharming attacks, we introduced two locked same-origin policies, which enforce access control using servers' X.509 certificates and public keys, rather than domain names. We evaluated the security and deployability of our approaches and showed how browsers can deploy these policies today to substantially increase their resistance to pharming attacks and provide a foundation for the development of pharming resistant authentication ceremonies.

The fact that 42% of email users in our study were vulnerable to our simulated attacks exemplifies the formidable challenge in designing ceremonies to resist social engineering attacks. However, we are hopeful that the future deployment of user-centric mechanisms like conditioned-safe ceremonies and the locked same-origin policies will help tip the advantage away from malicious elements on the Internet.

Bibliography

[1] Martin Abadi, T. Mark A. Lomas, and Roger Needham. Strengthening Passwords. Technical Report 1997-033, SRC, September 1997.

[2] Anne Adams and Martina Angela Sasse. Users Are Not the Enemy. *Communications of the ACM*, 42(12):40–46, 1999.

[3] Ben Adida. BeamAuth: Two-Factor Web Authentication with a Bookmark. In *Proceedings of the Fourteenth ACM Conference on Computer and Communications Security (CCS 07)*, pages 48–57, October 2007.

[4] P. Akritidis, W.Y. Chin, V.T. Lam, S. Sidiroglou, and K.G. Anagnostakis. Proximity Breeds Danger: Emerging Threats in Metro-area Wireless Networks. In *Proceedings of the* 16^{th} *USENIX Security Symposium*, pages 323–338, August 2007.

[5] Carl Martin Allwood. Error Detection Processes in Problem Solving. *Cognitive Science*, 8(4):413–437, 1984.

[6] Anti-Phishing Working Group. `http://www.antiphishing.org/`.

[7] Anti-Phishing Working Group. Ebay - Update Your Account MITM attack. `http://www.antiphishing.org/phishing_archive/05-03-05_Ebay/05-03-05_Ebay.html`.

[8] Dirk Balfanz. Usable Access Control for the World Wide Web. In *Proceedings of the 19th Annual Computer Security Applications Conference*, pages 406–416, December 2003.

[9] Bank of America SiteKey: Online Banking Security. http://www.bankofamerica/privacy/sitekey/.

[10] Adam Barth, Collin Jackson, and John C. Mitchell. Robust Defenses for Cross-Site Request Forgery. In *15th ACM Conference on Computer and Communications Security (CCS '08)*, November 2008.

[11] Stephen Bell. Invalid Banking Cert Spooks Only One User in 300. ComputerWorld New Zealand, http://www.computerworld.co.nz/news.nsf/NL/-FCC8B6B48B24CDF2CC2570020018FF73, May 2005.

[12] Nelson Bolyard. MITM in the Wild. http://www.mail-archive.com/dev-tech-crypto@lists.mozilla.org/msg04900.html, October 18, 2008.

[13] Sacha Brostoff and M. Angela Sasse. Safe and Sound: A Safety-Critical Approach to Security. In *Proceedings of the 2001 Workshop on New Security Paradigms*, pages 41–50, 2001.

[14] Browser Market Share. http://marketshare.hitslink.com/report.aspx?qprid=0, retrived Sept. 11, 2008.

[15] Sonia Chiasson, P.C. van Oorschot, and Robert Biddle. A Usability Study and Critique of Two Password Managers. In *Proceedings of the 15th USENIX Security Symposium*, pages 1–16, August 2006.

[16] Robert Cialdini. *Influence: Science and Practice, 5th edition.* Allyn and Bacon, 2008.

[17] Tyler Close. Petname Tool. http://petname.mozdev.org/.

[18] Tyler Close. Waterken YURL. http://www.waterken.com/dev/YURL/httpsy/.

[19] Colleen Corley. Students Go 'Phishing' for User Info. http://www.idsnews.com/news/story.aspx?id=29400&comview=1.

[20] Federal Financial Institutions Examination Council. Authentication in an Internet Banking Environment. http://www.ffiec.gov/pdf/authentication_guidance.pdf, October 2005.

[21] Lorrie Faith Cranor. A Framework for Reasoning About the Human in the Loop. In *Usability, Psychology and Security (UPSEC)*, 2008.

[22] Lorrie Faith Cranor and Simson Garfinkel, editors. *Security and Usability: Designing Secure Systems That People Can Use*. O'Reilly, 2005.

[23] Rachna Dhamija and J. D. Tygar. The Battle Against Phishing: Dynamic Security Skins. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*, pages 77–88, July 2005.

[24] Rachna Dhamija, J. D. Tygar, and Marti Hearst. Why Phishing Works. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 581–590, 2006.

[25] Julie S. Downs, Mandy B. Holbrook, and Lorrie Faith Cranor. Decision Strategies and Susceptibility to Phishing. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*, pages 79–90, July 2006.

[26] Julie S. Downs, Mandy B. Holbrook, and Lorrie Faith Cranor. Behavior Response to Phishing Risks. In *APWG 2nd Annual eCrime Researchers Summit*, pages 37–44, October 2007.

[27] Earthlink Toolbar Featuring ScamBlocker for Windows Users. http://www.earthlink.net/software/free/toolbar/.

[28] Serge Egelman, Lorrie Faith Cranor, and Jason Hong. You've Been Warned: An Empirical Study of the Effectiveness of Web Browser Phishing Warnings. In *Proceedings of the CHI 2008 Conference on Human Factors in Computing Systems*, 2008.

[29] Carl Ellison. Ceremony Design and Analysis. Cryptology ePrint Archive, Report 2007/399, 2007.

[30] Carl Ellison, Chris Hall, Randy Milbert, and Bruce Schneier. Protecting Secret Keys with Personal Entropy. *Future Generation Computer Systems*, 16(4):311–318, 2000.

[31] Aaron J. Ferguson. Fostering E-Mail Security Awareness: The West Point Carronade. *EDUCASE Quarterly*, 28(1):54–57, 2005.

[32] B. J. Fogg, Jonathan Marshall, Othman Laraki, Alex Osipovich, Chris Varma, Nicholas Fang, Jyoti Paul, Akshay Rangnekar, John Shon, Preeti Swani, and Marissa Treinen. What Makes Web Sites Credible?: A Report on a Large Quantitative Study. In *CHI '01: Proceedings of the SIGCHI conference on Human factors in computing systems*, pages 61–68, 2001.

[33] Jason Franklin, Vern Paxson, Adrian Perrig, and Stefan Savage. An Inquiry into the Nature and Causes of the Wealth of Internet Miscreants. In *14th ACM Conference on Computer and Communications Security (CCS '07)*, November 2007.

[34] Alan O. Freier, Philip Karlton, and Paul C. Kocher. The SSL Protocol Version 3.0. `http://wp.netscape.com/eng/ssl3/`, 1996.

[35] Batya Friedman, David Hurley, Daniel C. Howe, Edward Felten, and Helen Nissenbaum. Users' Conceptions of Web Security: A Comparative Study. In *Proceedings of the Conference on Human Factors in Computing Systems – CHI '02 extended abstracts*, pages 746–747, 2002.

[36] Eran Gabber, Phillip B. Gibbons, Yossi Matias, and Alain J. Mayer. How to Make Personalized Web Browsing Simple, Secure, and Anonymous. In *Proceedings of Financial Cryptography (FC '97)*, pages 17–32, 1997.

[37] Evgeniy Gabrilovich and Alex Gontmakher. The Homograph Attack. *Communications of ACM*, 45(2):128, February 2002.

[38] Simson Garfinkel. Email-based Identification and Authentication: An Alternative to PKI? *IEEE Security & Privacy Magazine*, 1(6):20–26, 2003.

[39] Simson Garfinkel. *Design Principles and Patterns for Computer Systems That Are Simultaneously Secure and Usable*. PhD thesis, Massachusetts Institute of Technology, 2005.

[40] David Goldsmith. How a 'Catch-22' Turns into a 'Shame on You'. `http://isc.sans.org/diary.html?storyid=1230`, March 2006.

[41] Nathan Good, Rachna Dhamija, Jens Grossklags, David Thaw, Steven Aronowitz, Deirdre Mulligan, and Jospeh Konstan. Stopping Spyware at the Gate: A User Study of Notice, Privacy and Spyware. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*, pages 43–52, July 2005.

[42] Princeton Secure Internet Programming Group. DNS Attack Scenario. `http://www.cs.princeton.edu/sip/news/dns-scenario.html`, February 1996.

[43] Matthew Van Gundy and Hao Chen. Noncespaces: Using Randomization to Enforce Information Flow Tracking and Thwart Cross-site Scripting Attacks. In *Proceedings of the 16th Annual Network and Distributed System Security Symposium (NDSS 2009)*, 2009.

[44] Peter Gutmann. Underappreciated Security Mechanisms. `http://www.cs.auckland.ac.nz/~pgut001/pubs/underappreciated.pdf`.

[45] Peter Gutmann. Why Isn't the Internet Secure Yet, Dammit. In *AusCERT Asia Pacific Information Technology Security Conference 2004*, May 2004.

[46] Peter Gutmann. Security Usability Fundamentals (Draft). `http://www.cs.auckland.ac.nz/~pgut001/pubs/usability.pdf`, retrieved Sept. 7, 2008.

[47] J. Alex Halderman, Brent Waters, and Edward W. Felten. A Convenient Method for Securely Managing Passwords. In *Proceedings of the 14th International World Wide Web Conference*, May 2005.

[48] C. Haney, W.C. Banks, and P.G. Zimbardo. Study of Prisoners and Guards in a Simulated Prison. *Naval Research Reviews*, 9:1–17, 1973.

[49] Amir Herzberg and Ahmad Jbara. Security and Identification Indicators for Browsers Against Spoofing and Phishing Attacks. *ACM Transactions on Internet Technology (TOIT)*, 8(4), September 2008.

[50] Russell Housley, Warwick Ford, Tim Polk, and David Solo. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. `http://tools.ietf.org/html/rfc3280`, 2002.

[51] Yao-Wen Huang, Fang Yu, Christian Hang, Chung-Hung Tsai, D. T. Lee, and Sy-Yen Kuo. Securing Web Application Code by Static Analysis and Runtime Protection. In *Proceedings of 13th international conference on World Wide Web (WWW'06)*, pages 40–52, 2006.

[52] ING Direct Privacy Center. `https://home.ingdirect.com/privacy/privacy_security.asp?s=newsecurityfeature`.

[53] Collin Jackson and Adam Barth. Beware of Finer Grained Origins. In *Web 2.0 Security and Privacy*, May 2008.

[54] Collin Jackson and Adam Barth. ForceHTTPS: Protecting High-Security Web Sites from Network Attacks. In *Proceedings of the 17th International World Wide Web Conference (WWW 2008)*, April 2008.

[55] Collin Jackson, Adam Barth, Andrew Bortz, Weidong Shao, and Dan Boneh. Protecting Browsers from DNS Rebinding Attacks. In *14th ACM Conference on Computer and Communications Security (CCS '07)*, November 2007.

[56] Collin Jackson, Daniel R. Simon, Desney S. Tan, and Adam Barth. An Evaluation of Extended Validation and Picture-in-Picture Phishing Attacks. In *Proceedings of Usable Security (USEC'07)*, February 2007.

[57] Tom Jagatic, Nathaniel Johnson, Markus Jakobsson, and Filippo Menczer. Social Phishing. *Communications of the ACM*, 50(10):94–100, October 2007.

[58] Markus Jakobsson and Jacob Ratkiewicz. Designing Ethical Phishing Experiments: A Study of (ROT13) rOnl Auction Query Features. In *Proceedings of the 15th annual World Wide Web Conference (WWW 2006)*, pages 513–522, May 2006.

[59] Markus Jakobsson, Alex Tsow, Ankur Shah, Eli Blevis, and Youn kyung Lim. What Instills Trust? A Qualitative Study of Phishing. In *Proceedings of Usable Security (USEC'07)*, February 2007.

[60] Martin Johns. On XSRF and Why You Should Care. Talk at the PacSec 2006 conference, `http://www.informatik.uni-hamburg.de/SVS/personnel/martin/psj06johns-e.pdf`, November 2006.

[61] Martin Johns. (Somewhat) Breaking the Same-origin Policy by Undermining DNS Pinning. `http://shampoo.antville.org/stories/1451301/`, August 2006.

[62] Martin Johns. Using Java in Anti DNS-pinning Attacks. `http://shampoo.antville.org/stories/1566124/`, February 2007.

[63] Martin Johns and Justus Winter. RequestRodeo: Client Side Protection against Session Riding. In *Proceedings of the OWASP Europe 2006 Conference, refereed papers track, Report CW448*, pages 5 – 17. Departement Computerwetenschappen, Katholieke Universiteit Leuven, May 2006.

[64] Nenad Jovanovic, Engin Kirda, and Christopher Kruegel. Preventing Cross Site Request Forgery Attacks. In *Proceedings of the Second IEEE Conference on Security and Privacy in Communications Networks (SecureComm)*, August 2006.

[65] Mike Just. Designing Authentication Systems with Challenge Questions. In Lorrie Faith Cranor and Simson Garfinkel, editors, *Security and Usability: Designing Secure Systems That People Can Use*, chapter 8, pages 143–155. O'Reilly, 2005.

[66] Dan Kaminsky. Black Ops 2008: It's the End of the Cache as We Know It. `http://www.doxpara.com/DMK_BO2K8.ppt`. Talk given at Black Hat 2008.

[67] Kanatoko. Anti-DNS Pinning (DNS Rebinding) + Socket in FLASH. `http://www.jumperz.net/index.php?i=2&a=3&b=3`, January 2007.

[68] Chris Karlof, J.D. Tygar, and David Wagner. A User Study Design for Comparing the Security of Registration Protocols. In *First USENIX Workshop on Usability, Psychology, and Security (UPSEC 2008)*, April 2008.

[69] Chris Karlof, J.D. Tygar, and David Wagner. Conditioned-safe Ceremonies and a User Study of an Application to Web Authentication. In *Proceedings of the Sixteenth Annual Network and Distributed Systems Security Symposium (NDSS 2009)*, February 2009.

[70] Chris Karlof, Umesh Shankar, J.D. Tygar, and David Wagner. Dynamic Pharming Attacks and Locked Same-origin Policies for Web Browsers. In *Fourteenth ACM Conference on Computer and Communications Security (CCS 2007)*, pages 58–72, October 2007.

[71] Alan H. Karp. Site-Specific Passwords. Technical Report HPL-2002-39R1, HP Labs, 2002.

[72] John Kelsey, Bruce Schneier, Chris Hall, and David Wagner. Secure Applications of Low-Entropy Keys. *Lecture Notes in Computer Science*, 1396:121–134, 1998.

[73] Ponnurangam Kumaraguru, Yong Rhee, Alessandro Acquisti, Lorrie Faith Cranor, Jason Hong, and Elizabeth Nunge. Protecting People from Phishing: The Design and Evaluation of an Embedded Training Email System. In *CHI '07: Proceedings of the SIGCHI conference on Human factors in computing systems*, pages 905–914, 2007.

[74] V. Benjamin Livshits and Monica S. Lam. Finding Security Vulnerabilities in Java Applications Using Static Analysis. In *Proceedings of the 14th USENIX Security Symposium*, pages 271–286, August 2005.

[75] Uriel Maimon. Universal Man-in-the-Middle Phishing Kit – Why is This Even News? `http://www.rsa.com/blog/entry.asp?id=1160`.

[76] Chris Masone, Kwang-Hyun Baek, and Sean Smith. WSKE: Web Server Key Enabled Cookies. In *Proceedings of Usable Security (USEC)*, February 2007.

[77] Adam Megacz. XWT Foundation Advisory: Firewall Circumvention Possible with All Browsers. `http://www.megacz.com/research/papers/sop.txt`, July 2002.

[78] Microsoft. Better Website Identification and Extended Validation Certificates in IE7 and Other Browsers. `http://blogs.msdn.com/ie/archive/2005/11/21/495507.aspx`.

[79] Microsoft. Mitigating Cross-site Scripting With HTTP-only Cookies. `http://msdn.microsoft.com/workshop/author/dhtml/httponly_cookies.asp`.

[80] Microsoft. Microsoft Security Bulletin MS01-017: Erroneous VeriSign-Issued Digital Certificates Pose Spoofing Hazard. `http://www.microsoft.com/technet/security/Bulletin/MS01-017.mspx`, March 2001.

[81] Stanley Milgram. *Obedience to Authority: An Experimental View*. Harper Collins, 1974.

[82] Mozilla Bugzilla Bug 149943 – Princeton-like Exploit May Be Possible. `https://bugzilla.mozilla.org/show_bug.cgi?id=149943`.

[83] Mozilla Bugzilla Bug 162871 – DNS: Problems with New DNS Cache (”Pinning” Forever). `https://bugzilla.mozilla.org/show_bug.cgi?id=162871`.

[84] Mozilla Bugzilla Bug 205726 – nsDnsService Rewrite. `https://bugzilla.mozilla.org/show_bug.cgi?id=205726`.

[85] Mozilla Bugzilla Bug 245609 – Mozilla Not Getting Certificate Issuer from Authority Information Access CA Issuers, June 2004.

[86] mozilla.dev.security. VeriSign Class 3 Secure Server CA? http://groups.google.com/group/mozilla.dev.security/browse_thread/threa%d/6830a8566de24547/0be9dea1c274d0c5, March 2007.

[87] mozilla.org. The Same-Origin Policy. http://www.mozilla.org/projects/security/components/same-origin.html.

[88] Netcraft Anti-phishing Toolbar. http://toolbar.netcraft.com/.

[89] Raymond Nickerson. Confirmation Bias: A Ubiquitous Phenomenon in Many Guises. *Review of General Psychology*, 2(2):175–220, June 1998.

[90] Donald A. Norman. *The Design of Everyday Things*. Basic Books, 1988.

[91] Gunter Ollmann. The Pharming Guide. http://www.ngssoftware.com/papers/ThePharmingGuide.pdf.

[92] Stefano Di Paola and Giorgio Fedon. Subverting Ajax. In *23rd Chaos Communication Congress*, December 2006.

[93] Bryan Parno, Cynthia Kuo, and Adrian Perrig. Phoolproof Phishing Prevention. In *Proceedings of Financial Cryptography (FC'06)*, February 2006.

[94] Persistent Client State: HTTP Cookies, Preliminary Specification. http://wp.netscape.com/newsref/std/cookie_spec.html.

[95] PTFB Pro. http://www.ptfbpro.com/.

[96] Ariel Rabkin. Personal Knowledge Questions for Fallback Authentication. In *Proceedings of the 2008 Symposium on Usable Security and Privacy (SOUPS)*, pages 13–23, 2008.

[97] Venugopalan Ramasubramanian and Emin Gun Sirer. Perils of Transitive Trust in the Domain Name System. In *Proceedings of the Internet Measurement Conference (IMC)*, October 2005.

[98] Jens Rasmussen. What Can be Learned from Human Error Reports? In K. D. Duncan, M. M. Gruenberg, and D. Wallis, editors, *Changes in Working Life*, pages 97–113. Wiley, 1980.

[99] Jens Rasmussen. Skills, Rules, and Knowledge: Signals, Signs, Symbols and Other Distinctions in Human Performance Models. *IEEE Transactions on Systems, Man, and Cybernetics*, 13(3):257–266, 1983.

[100] James Reason. *Human Error*. Cambridge University Press, 1990.

[101] Arthur Reber. *Penguin Dictionary of Psychology, 2nd Edition*. Penguin Books, 1995.

[102] Nicholas Rosasco and David Larochelle. How and Why More Secure Technologies Succeed in Legacy Markets: Lessons from the Success of SSH. In *Proceedings of the Second Annual Workshop on Economics and Information Security*, May 2003.

[103] Jim Roskind. Attacks Against the Netscape Browser. Invited talk, RSA conference, April 2001.

[104] Blake Ross, Collin Jackson, Nicholas Miyake, Dan Boneh, and John C. Mitchell. Stronger Password Authentication Using Browser Extensions. In *Proceedings of the 14th USENIX Security Symposium*, pages 17–32, August 2005.

[105] Lee Ross, Mark R. Lepper, and Michael Hubbard. Perseverance in Self-perception and Social Perception: Biased Attributional Processes in the Debriefing Paradigm. *Journal of Personality and Social Psychology*, 32(5):880–892, 1975.

[106] Stefan Santesson and Russell Housley. Internet X.509 Public Key Infrastructure Authority Information Access Certificate Revocation List (CRL) Extension. http://www.ietf.org/rfc/rfc4325.txt, December 2005.

[107] Prateek Saxena, Dawn Song, and Yacin Nadji. Document Structure Integrity: A Robust Basis for Cross-site Scripting Defense. In *Proceedings of the 16th Annual Network and Distributed System Security Symposium (NDSS 2009)*, 2009.

[108] Stuart Schechter, Rachna Dhamija, Andy Ozment, and Ian Fischer. Emperor's New Security Indicators: An Evaluation of Website Authentication and the Effect of Role Playing on Usability Studies. In *Proceedings of the 2007 IEEE Symposium on Security and Privacy*, pages 51–65, May 2007.

[109] Security Space and E-Soft. Secure Server Survey. `http://www.securityspace.com/s_survey/sdata/200704/certca.html`, May 2007.

[110] Rajiv Shah and Christian Sandvig. Software Defaults as De Facto Regulation: The Case of the Wireless Internet. In *The 33rd Research Conference on Communication, Information, and Internet Policy*, September 2005.

[111] Steve Sheng, Bryant Magnien, Ponnurangam Kumaraguru, Alessandro Acquisti, Lorrie Faith Cranor, Jason Hong, and Elizabeth Nunge. Anti-Phishing Phil: The Design and Evaluation of a Game That Teaches People Not to Fall for Phish. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*, pages 88–99, July 2007.

[112] Paul Slovic, Baruch Fischhoff, and Sarah Lichtenstein. Facts Versus Fears: Understanding Perceived Risk. In Daniel Kahneman, Paul Slovic, and Amos Tversky, editors, *Judgment Under Uncertainty: Heuristics and Biases*, chapter 33, pages 463–489. Cambridge University Press, 1982.

[113] Christopher Soghoian and Markus Jakobsson. A Deceit-Augmented Man in the Middle Attack Against Bank of America's SiteKey Service. `http://paranoia.dubfire.net/2007/04/deceit-augmented-man-in-middle-attack.html`, April 2007.

[114] Spoofstick. `http://www.spoofstick.com/`.

[115] Sid Stamm, Zulfikar Ramzan, and Markus Jakobsson. Drive-by Pharming. In *Information and Communications Security, 9th International Conference, ICICS 2007*, pages 495–506, December 2007.

[116] S.E. Taylor and J. Crocker. Schematic Bases of Social Information Processing. In E.T. Higgins, C.P. Herman, and M.P. Zanna, editors, *Social Cognition: The Ontario Symposium (Vol. 1)*, pages 89–134. Erlbaum Associates, 1981.

[117] Rob Thomas and Jerry Martin (a.k.a. Team Cymru). The Underground Economy: Priceless. *;login: The USENIX Magazine*, 31(6):7–16, December 2006.

[118] Herbert H. Thompson. How I Stole Someone's Identity. `http://www.sciam.com/article.cfm?id=anatomy-of-a-social-hack`, August, 2008.

[119] Win Treese and Eric Rescorla. The Transport Layer Security (TLS) Protocol Version 1.1. `http://tools.ietf.org/html/rfc4346`, 2006.

[120] Alex Tsow. Phishing with Consumer Electronics – Malicious Home Routers. In *Models of Trust for the Web Workshop at the 15th International World Wide Web Conference (WWW2006)*, May 2006.

[121] Alex Tsow, Markus Jakobsson, Liu Yang, and Susanne Wetzel. Warkitting: the Drive-by Subversion of Wireless Home Routers. *Journal of Digital Forensic Practice*, 1(3), November 2006.

[122] Timothy W. van der Horst and Kent E. Seamons. Simple Authentication for the Web. In *3rd International Conference on Security and Privacy in Communication Networks (SecureComm)*, September 2007.

[123] Vanguard Security Center. `https://www.vanguard.com/`.

[124] VeriSign. Licensing VeriSign Certificates Securing Multiple Web Server and Domain Configurations. `http://www.verisign.com/static/001496.pdf`, June 2005.

[125] VivilProject. List of public DNS servers.

[126] Willem A. Wagenaar and Jop Groeneweg. Accidents at Sea: Multiple Causes and Impossible Consequences. *International Journal of Man-Machine Studies*, 27(5/6), Nov/Dec 1987.

[127] Washington Post. Citibank Phish Spoofs 2-Factor Authentication. http://blog.washingtonpost.com/securityfix/2006/07/citibank_phish_spoofs_2factor_1.html.

[128] Washington Post. Not Your Average Phishing Scam. http://blog.washingtonpost.com/securityfix/2007/01/not_your_average_amazon_phishi.html.

[129] Ryan West. The Psychology of Security: Why Do Good Users Make Bad Decisions? *Communications of the ACM*, 51(4):34–40, April 2008.

[130] Tara Whalen and Kori M. Inkpen. Gathering Evidence: Use of Visual Security Cues in Web Browsers. In *Proceedings of Graphics Interface 2005*, pages 137–144, May 2005.

[131] Alfred North Whitehead. *Introduction To Mathematics*. Williams and Northgate, 1911.

[132] Alma Whitten and J.D. Tygar. Safe Staging for Computer Security. In *Workshop on Human-Computer Interaction and Security Systems*, April 2003.

[133] Timothy D. Wilson and Daniel T. Gilbert. Explaining Away: A Model of Affective Adaptation. *Perspectives on Psychological Science*, 3(5):370–386, 2008.

[134] Michael S. Wogalter, editor. *Handbook of Warnings*. Lawrence Erlbaum Associates, 2006.

[135] Min Wu, Robert C. Miller, and Simson Garfinkel. Do Security Toolbars Actually Prevent Phishing Attacks? In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 601–610, 2006.

[136] Min Wu, Robert C. Miller, and Greg Little. Web Wallet: Preventing Phishing Attacks by Revealing User Intentions. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*, pages 102–113, July 2006.

[137] Yichen Xie and Alex Aiken. Static Detection of Security Vulnerabilities in Scripting Languages. In *Proceedings of the 15th USENIX Security Symposium*, pages 179–192, August 2006.

[138] Wei Xu, Sandeep Bhatkar, and R. Sekar. Taint-Enhanced Policy Enforcement: A Practical Approach to Defeat a Wide Range of Attacks. In *Proceedings of the 15th USENIX Security Symposium*, pages 121–136, August 2006.

[139] Yahoo sign-in seal. `http://security.yahoo.com/`.

[140] Eileen Ye and Sean Smith. Trusted Paths for Browsers. In *Proceedings of the 11th USENIX Security Symposium*, pages 263–279, August 2002.

[141] Ka-Ping Yee. Guidelines and Strategies for Secure Interaction Design. In Lorrie Faith Cranor and Simson Garfinkel, editors, *Security and Usability: Designing Secure Systems That People Can Use*, chapter 13, pages 247–273. O'Reilly, 2005.

[142] Ka-Ping Yee and Kragen Sitaker. Passpet: Convenient Password Management and Phishing Protection. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*, pages 32–43, July 2006.

[143] Tatu Ylonen. SSH – Secure Login Connections Over the Internet. In *Proceedings of the 6th USENIX Security Symposium*, pages 37–42, 1996.

[144] Jim Youll. Fraud Vulnerabilities in SiteKey Security at Bank of America. `cr-labs.com/publications/SiteKey-20060718.pdf`, July 2006.

[145] Yue Zhang, Serge Egelman, Lorrie Faith Cranor, and Jason Hong. Phinding Phish: Evaluating Anti-Phishing Tools. In *Proceedings of the 14th Annual Network and Distributed System Security Symposium (NDSS 2007)*, February 2007.

Appendix A

User study exit survey questions

1. What is your UCB Movie Predictions login name?

2. What is your gender?

   Female

   Male

3. What is your age?

   18-21

   22-25

   26-30

   31-40

   41-50

   51-60

   60 and over

4. Please choose one of the following:

   Undergraduate student

   Graduate student

   Non-student, please describe:

5. If you are a student, please enter your major area

   Economics or business

   Social sciences (i.e., psychology, sociology, etc.)

   Computer science

   Chemistry, physics, biology, or other natural sciences

   Humanities (i.e., literature, languages, history, etc.)

   Engineering

   Other (please specify)

6. What operating system do you primarily use?

   Windows

   Linux

   Mac OS

   Other (please specify)

7. What Web browser do you primarily use?

   Internet Explorer

   Firefox

   Opera

   Safari

   Other (please specify)

8. How many hours a week do you use a Web browser?

   0-5

   5-10

   10-20

   20+

9. What kind of financial transactions do you conduct online?

Auctions (e.g., Ebay)

Banking

Investing (e.g., stocks and mutual funds)

PayPal (and other money transfer services)

Shopping

Other (please specify)

10. Aside from this study, how long have you conducted financial transactions online?

Never

Less than six months

Six months to a year

One year to two years

Over two years

11. What are your biggest security concerns when browsing the Web? Enter up to three concerns.

12. Briefly describe what precautions, if any, you may take when logging into a Web site. Please feel free to list precautions you only sometimes take or take only at certain sites.

13. In the previous question, you were asked to list what precautions you may take when you log into a Web site. In this question, we would like you to evaluate how often and thoroughly you apply these precautions when logging into different types of Web sites.

Site types:

a shopping Web site?

a social networking site (e.g., Facebook, MySpace)?

PayPal?

Web email (e.g., Gmail, Hotmail)?

UCB Movie Predictions (the Web site for this study)?

Choices for each site type:

"I rarely take the precautions I listed when logging into this type of Web site"

"I sometimes take the precautions I listed when logging into this type of Web site"

"I usually take the precautions I listed when logging into this type of Web site"

"I always take the precautions I listed when logging into this type of Web site"

"I don't use this type of Web site"

14. What was average amount of time you spent interacting with UCB Movie Predictions each time you logged in?

0-5 minutes

5-10 minutes

10-20 minutes

20+ minutes

15. During your interactions with UCB Movie Predictions, did you ever see something which looked suspicious or dangerous?

no

yes – if yes, describe what it looked like and when you saw it.

16. If you answered yes to the previous question, describe what your reaction was and if you did anything, what you did.

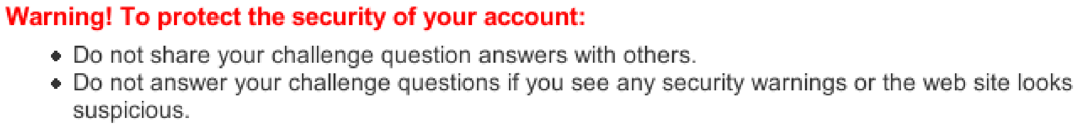
17. Do you remember seeing the above warning at any point during the study?

no, I don’t remember seeing the warning

yes, I remember seeing the warning

If you remember seeing it, describe how it affected your decisions (if at all) while interacting with the study Web site. Please be specific as possible.

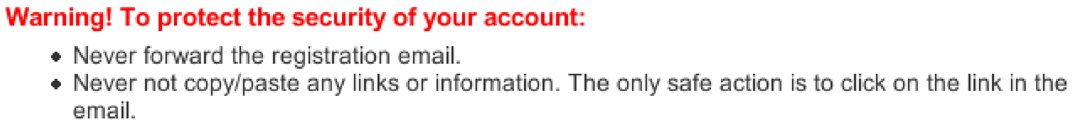
Image shown to challenge question users:



Warning! To protect the security of your account:

- Do not share your challenge question answers with others.
- Do not answer your challenge questions if you see any security warnings or the web site looks suspicious.

Image shown to email users:



Warning! To protect the security of your account:

- Never forward the registration email.
- Never not copy/paste any links or information. The only safe action is to click on the link in the email.

18. During the study, you might remember seeing a page similar to the one below. Study it for a moment and then answer the next question.

- Challenge question users were shown Figure 5.4(b).
- Forwarding attack emails users were shown Figure 5.6(a) (or a similar text version, depending on the attack details – see Section 5.2.4).
- Cut and paste attack emails users were shown Figure 5.6(b) (or a similar text version, depending on the attack details – see Section 5.2.4).

If you followed the above instructions to forward the registration email, explain why. If you chose not follow the instructions, explain why not. If you don’t remember this page or what you did, tell us what you don’t remember.

19. UCB Movie Predictions used <challenge questions/email registration> to help make your logins more secure. Have you used <challenge questions/email registration> before at other Web sites?

no

yes – if yes, which Web sites?

20. Briefly describe how you think registration using <challenge questions/email> works and what, if any, security benefits it has.

21. Rate how safe you would feel using a Web site which uses the following different login mechanisms:

Login mechanisms:

Password for logins + no registration

Password for logins + <challenge questions/email> for registration

Answer choices:

Not secure at all

Somewhat secure

Fairly secure

Very secure

I don't know

22. Rate the convenience of each of the following login mechanisms:

Login mechanisms:

Password for logins + no registration

Password for logins + <challenge questions/email> for registration

Answer choices:

Nearly impossible or very annoying

Hard or slightly annoying

I could get used to it

I hardly noticed it

I don't know

23. Did you find anything difficult or annoying about this study?

24. Did you feel engaged/interested during the entire duration of the study?

25. Do you have any general comments about this study?

Appendix B

User study exit survey responses

Group 1 (challenge questions): Demographics

User #	**Gender**	**Age**	**Student status or occupation**	**Details**	**OS**	**Primary browser**	**Web use/week (hrs)**	**Financial transactions done online**	**Experience doing financial transactions online**
73	Female	22-25	Undergraduate	Natural sciences	Windows	Firefox	10-20	Banking, Investing, Shopping	> 2 years
78	Male	22-25	Undergraduate	Natural sciences	Windows	Firefox	20+	Banking, Shopping, Auctions, PayPal	> 2 years
83	Male	31-40	Graduate	Social sciences	Mac OS	Flock	20+	Banking, Investing, Shopping, Auctions, PayPal	> 2 years
88	Male	18-21	Undergraduate	Economics or business	Windows	Firefox	10-20	Banking, Auctions	1–2 years
93	Male	22-25	Undergraduate	Economics or business	Windows	Firefox	10-20	Banking, Shopping, Auctions	> 2 years
98	Female	18-21	Undergraduate	Natural sciences	Mac OS	Firefox	20+	Banking, Shopping	> 2 years
103	Male	18-21	Undergraduate	Engineering	Windows	Firefox	10-20	Banking	1–2 years
108	Female	18-21	Undergraduate	Economics or business	Mac OS	Safari	5-10	Banking, Shopping	1–2 years
113	Male	18-21	Undergraduate	Natural sciences	Windows	Firefox	10-20	Banking, Shopping, Auctions, PayPal	> 2 years
118	Male	18-21	Undergraduate	Humanities	Mac OS	Firefox	5-10	Banking, Shopping, Auctions, PayPal	> 2 years
123	Female	18-21	Undergraduate	Social sciences	Windows	Firefox	10-20	Banking, Shopping, Auctions, PayPal	< 6 months
128	Female	22-25	Graduate	Optometry	Windows	Firefox	20+	Banking, Investing, Shopping, Auctions, PayPal	> 2 years
133	Male	18-21	Undergraduate	Economics or business	Windows	Firefox	20+	Investing, Shopping, Auctions, PayPal	> 2 years
138	Male	18-21	Undergraduate	Economics or business	Windows	Firefox	10-20	Shopping, Auctions	1–2 years
143	Female	18-21	Undergraduate	Humanities	Mac OS	Safari	5-10	Shopping	< 6 months

Group 1 (challenge questions): Demographics

User #	Gender	Age	Student status or occupation	Details	OS	Primary browser	Web use/week (hrs)	Financial transactions done online	Experience doing financial transactions online
148	Male	18-21	Undergraduate	Public Health	Windows	Internet Explorer	5-10	Banking, PayPal	6–12 months
153	Male	18-21	Undergraduate	Economics or business	Windows	Firefox	10-20	Banking, Shopping, Auctions, PayPal	> 2 years
158	Male	18-21	Undergraduate	Economics or business	Windows	Internet Explorer	5-10	Banking, Shopping, Auctions	> 2 years
163	Female	No response	Undergraduate	Humanities	Windows	Firefox	20+	Banking, Shopping, PayPal	Never
168	Female	31-40	staff	architecture	No response	Firefox	20+	Banking, Shopping, Auctions, PayPal	> 2 years
173	Female	22-25	Undergraduate	Humanities	Windows	Firefox	10-20	Banking	1–2 years
178	Female	18-21	Undergraduate	Social sciences	Windows	aol explorer	10-20	Banking	> 2 years
183	Male	41-50	Undergraduate	Humanities	Windows	Firefox	5-10	Banking, Investing, Shopping, Auctions, PayPal	6–12 months
188	Male	31-40	Graduate	Social sciences	Windows	Firefox	10-20	Banking, Shopping, Auctions, PayPal	1–2 years
193	Female	18-21	Undergraduate	Math and music	Windows	Firefox	10-20	PayPal	Never
198	Female	22-25	Undergraduate	computer science and philosophy	Linux	Firefox	20+	poker, Banking, Shopping	> 2 years
203	Female	22-25	Undergraduate	No response	Windows	No response	No response	No	Never
208	Female	22-25	Undergraduate	Economics or business	Windows	Internet Explorer	10-20	Banking, Shopping, Auctions, PayPal	> 2 years
213	No response	No response	No response	No response	No response	No response	No response	No	Never

Group 1 (challenge questions): Demographics

User #	Gender	Age	Student status or occupation	Details	OS	Primary browser	Web use/week (hrs)	Financial transactions done online	Experience doing financial transactions online
218	Female	18-21	Undergraduate	Music	Mac OS	Firefox	10-20	Banking, Shopping, PayPal	> 2 years
223	Female	18-21	Undergraduate	Economics or business	Windows	Firefox	10-20	Banking, Shopping	> 2 years
228	Female	18-21	Undergraduate	Social sciences	Windows	Firefox	20+	Banking, Shopping, PayPal	> 2 years
233	Male	18-21	Undergraduate	Natural sciences	Mac OS	Safari	10-20	Banking, Shopping, Auctions, PayPal	> 2 years
238	Male	18-21	Undergraduate	Statistics	Windows	Firefox	20+	Banking, Investing, Shopping, Auctions, PayPal	1–2 years
243	Male	18-21	Undergraduate	Natural sciences	Windows	Internet Explorer	10-20	No	Never
248	Male	18-21	Undergraduate	Natural sciences	Mac OS	Safari	5-10	Shopping, PayPal	1–2 years
253	Male	22-25	Undergraduate	Natural sciences	Linux	Firefox	5-10	Banking, Shopping, PayPal	> 2 years
258	Female	18-21	Undergraduate	Natural sciences	Mac OS	Safari	10-20	Banking, Shopping, PayPal	> 2 years
273	Female	18-21	Undergraduate	Natural sciences	Windows	Internet Explorer	20+	Banking, Shopping, PayPal	1–2 years
278	Male	22-25	Undergraduate	Natural sciences	Windows	Firefox	10-20	Banking, Investing, Shopping, Auctions	> 2 years
283	Female	22-25	Undergraduate	Natural sciences	Mac OS	Firefox	10-20	Banking, Shopping, Auctions	1–2 years

Group 1 (challenge questions): Web security attitudes

			How often & thoroughly user applies precautions when logging into:					
User #	**Biggest security concerns while browsing the Web**	**Precautions taken when logging into a Web site**	**Banking**	**Paypal**	**Web email**	**Shopping**	**Social networking**	**Study site**
73	Data leaks (personal information leaked from a database), phishing	I use a slightly different password for each site. There's a basic password, and one component of it changes to match the nth letter of the website name.	Always	Always	Always	Always	Always	Always
78	spyware password theft	secure passwords check security certificate block javascript for unknown sites (NoScript plugin for FF)	Always	Always	Usually	Always	Sometimes	Rarely
83	1) Hacking into my financial accounts; 2) Phishing scams	Assuming this is a site where I will be providing sensitive information, I check for the "lock" on my browser to see if the site is secure, as well as for the "https://" beginning to the URL. I also make sure that whatever security precautions the website has match what I am expecting.	Always	Always	Sometimes	Usually	Sometimes	Rarely
88	Spyware, Data privacy, spam mail	I check to see if the site address is correct. (i.e. facebook.com as opposed to facebook.da.ru)	Rarely	Rarely	Rarely	Usually	Usually	Rarely
93	having my personal information compromised. catching a virus from an unsafe website.	i make sure that it is a site i trust and sometimes review their security protocol.	Always	Always	Rarely	Always	Rarely	Rarely
98	safety, identity theft	only used highly secured and proved sites, log out after using	Always	Don't use	Usually	Don't use	Usually	Don't use
103	loss of personal information	to see whether everything looks the same	Sometimes	Sometimes	Rarely	Rarely	Rarely	Rarely

Group 1 (challenge questions): Web security attitudes

			How often & thoroughly user applies precautions when logging into:					
User #	Biggest security concerns while browsing the Web	Precautions taken when logging into a Web site	Banking	Paypal	Web email	Shopping	Social networking	Study site
108	Access to my online bank account. Someone accessing and using my credit card information.	I usually only log into websites when I am familiar with them and I know that they are secure.	Always	Always	Usually	Usually	Usually	Rarely
113	Hackers Viruses Spam/spyware	I just make sure it seems legit by it's content, design and the amount of pop-ups or ads it may have. I make sure my password and user name isn't saved if it's an important website with money transactions.	Always	Always	Rarely	Always	Sometimes	Rarely
118	The only real concern is the trustworthiness of those on the opposite end of financial transactions (ie ebay)	Well, if I get warnings that a page is not encrypted, I won't enter any sensitive information. Other than that, few precautions	Usually	Usually	Sometimes	Usually	Rarely	Sometimes
123	Security Privacy issues Viruses	I try not to visit websites I haven't heard about. I also don't click on anything people send me through e-mails or chats.	Always	Usually	Usually	Always	Sometimes	Usually
128	Identity theft	Make sure the URL is correct (typed it in correctly myself or use a bookmark), and make sure it's a secure site.	Always	Always	Always	Usually	Usually	Usually
133	1. Viruses 2. Pornography 3. Security	None, just make sure it looks legitimate.	Always	Always	Usually	Usually	Sometimes	Sometimes
138	Credit card fraud Identity theft	I only use trusted sites such as Ebay and PayPal	Usually	Rarely	Rarely	Rarely	Rarely	Rarely
143	None	Block popups	Always	Always	Usually	Usually	Sometimes	Sometimes

Group 1 (challenge questions): Web security attitudes

			How often & thoroughly user applies precautions when logging into:					
User #	**Biggest security concerns while browsing the Web**	**Precautions taken when logging into a Web site**	**Banking**	**Paypal**	**Web email**	**Shopping**	**Social networking**	**Study site**
148	A virus will infect my computer. Pop-ups will contain something harmful to my computer.	To make sure everything on the website looks the exact same as when I logged in the last time.	Always	Usually	Usually	Don’t use	Always	Usually
153	Spyware/	I only log into websites that I believe could be legitimate. If I have any suspicion, I log off. Intuition is my primary weapon.	Always	Always	Always	Always	Always	Always
158	Identity theft, scams, and viruses.	None really.	Rarely	Rarely	Rarely	Rarely	Rarely	Rarely
163	Someone monitoring my actions. Someone copying down my personal information.	I look at the address bar and make sure it was the website I typed in when I log in. I also look for things that may look weird about the page.	Always	Always	Sometimes	Usually	Sometimes	Rarely
168	Don’t want identity/credit card info stolen	I don’t really take precautions – I assume the web sites I visit have taken adequate measures already. This isn’t too clever of me.	Sometimes	Sometimes	Rarely	Sometimes	Rarely	Rarely
173	identity theft, credit card fraud, and dishonest sellers/buyers	unusual password; not entering when the site’s security certificate is questioned by my browser; not using the back/forward keys; and not doing any personal banking, or any other activities involving sensitive information, on public computers.	Always	Usually	Rarely	Always	Sometimes	Always
178	that my personal information will be taken	i don’t do a lot of downloading	Rarely	Rarely	Rarely	Rarely	Don’t use	Rarely

Group 1 (challenge questions): Web security attitudes

			How often & thoroughly user applies precautions when logging into:					
User #	**Biggest security concerns while browsing the Web**	**Precautions taken when logging into a Web site**	**Banking**	**Paypal**	**Web email**	**Shopping**	**Social networking**	**Study site**
183	Stolen passords. Unauthorized transactions. Privacy issues-personal details leaked.	Only access the site through Yahoo or Google to avoid mistyping the web address.	Always	Usually	Rarely	Rarely	Rarely	Rarely
188	No response	No response	No response	No response	No response	No response	No response	No response
193	identity theft, financial theft, viruses	see how others feel about that site, look for headquarters and a toll free number to verify, see if it looks professional	Don't use	Always	Rarely	Don't use	Sometimes	Rarely
198	none	For sites where security is important, I use unique passwords.	Always	Always	Always	Always	Rarely	Rarely
203	No response	No response	No response	Rarely	No response	No response	No response	Rarely
208	1. Stolen credit card numbers 2. Stolen social security number 3. Unreliable sellers (esp. on eBay)	Look for certification of authenticity before entering any information	Always	Always	Always	Always	Always	Always
213	No response	No response	No response	No response	No response	No response	No response	No response
218	Accidentally giving my credit card information to a phishing site that looks like a legit online vendor	I always double check that links I click on go to a URL I'm familiar with. I also use the firefox plugin AdBlock Plus to make sure I don't click on advertisements.	Always	Always	Rarely	Always	Always	Rarely
223	phishing, viruses	i usually always type the original website (no clicking on links) and look for my passkey if there is one	Always	Always	Sometimes	Always	Rarely	Sometimes
228	Identity Theft	No response	Always	Always	Sometimes	Usually	Sometimes	Usually

Group 1 (challenge questions): Web security attitudes

			How often & thoroughly user applies precautions when logging into:					
User #	**Biggest security concerns while browsing the Web**	**Precautions taken when logging into a Web site**	**Banking**	**Paypal**	**Web email**	**Shopping**	**Social networking**	**Study site**
233	Fraud	Sometimes I will close the website and re-open it. Sometimes facebook asks me to re-enter my password, to which I exact this measure.	Usually	Usually	Usually	Usually	Usually	Rarely
238	being tracked	none	Rarely	Rarely	Rarely	Rarely	Rarely	Rarely
243	Phishing scams	Has to look authentic	Always	Always	Always	Always	Always	Sometimes
248	identity theft	if it's a secure server or not	Always	Always	Always	Always	Always	Sometimes
253	Credit card numbers being stolen. Email passwords leaking. ISP/Government spying on my packets	Depends on the website. Verifying ssl certificates is a good start and one I should of caught this time but didn't think about it because of the nature of this site.	Always	Always	Rarely	Usually	Rarely	Rarely
258	Getting my password stolen Getting personal information stolen	Making sure the web site asks for the password	Always	Always	Always	Always	Always	Always
273	Viruses, hacking, and stalking	I usually read the privacy contract, but I usually am ok with logging in.	Always	Always	Always	Usually	Usually	Rarely
278	downloading viruses, such as trojans	No response	Always	Always	Sometimes	Usually	Always	Usually
283	Scams Identity Theft	Good passwords Secure computer Security Questions	Always	Usually	Sometimes	Sometimes	Rarely	Sometimes

Group 1 (challenge questions): Study experiences

User #	Fell for attack?	How attack ended	Saw something suspicious/dangerous?	If yes, reaction?	Remembered seeing warning? If yes, effect on decisions?	Followed attack instructions? Why or why not? (Question 18)
73	yes	entered answers	yes: During this final login, a window popped up which said something about security concerns.	I clicked OK or continue or whatever button would allow me to access the site. I was not concerned about security related to this site, since it's an obscure study. Had it been my bank website or a website that had my credit card information, I would hope I would pay more attention.	yes: It didn't affect my decisions. I thought the creators of this study were being completely paranoid: the security was tighter than for my bank (in that it did not "allow" me to use public computers–I did anyway).	I answered the questions. I was in a hurry to make the predictions for today. I didn't think anything could really be suspicious with the site: I followed the same link I always do.
78	yes	entered answers	no	N/A	no	I thought the site's cookie may have been erased which is why it wasn't recognizing my computer, so I answered
83	yes	entered answers	no	N/A	no	I followed the instructions because I remember being told to create these questions when I created my account at the website, and the questions matched those I chose as my challenge questions.
88	yes	entered answers	no	N/A	no	I thought it was procedure to answer these questions

Group 1 (challenge questions): Study experiences

User #	Fell for attack?	How attack ended	Saw something suspicious/dangerous?	If yes, reaction?	Remembered seeing warning? If yes, effect on decisions?	Followed attack instructions? Why or why not? (Question 18)
93	yes	entered answers	no	N/A	yes: it didnt affect my decisions at all because many websites have similar warnings, i usually know whether or not i trust the site before i see the warnings to begin with.	I answered them because i was instructed to do so.
98	yes	entered answers	no	N/A	yes: It did not	I trusted the site because it was school-affiliated and followed the instructions. I was asked different questions.
103	yes	entered answers	no	N/A	no	Those were my challenge questions, so I answered them
108	yes	entered answers	no	N/A	no	I was trying to access my account and I did not associate any danger with this.
113	yes	entered answers	no	N/A	yes: I saw it as a usual precaution since my account does involve paypal.	I remember answering these two challenge questions without a doubt. I just assumed it was proper protocol since my account did have my paypal account name. I just entered it assuming it was necessary to properly login.
118	yes	entered answers	no	N/A	yes: Well, I didn't notice anything suspicious. So I guess I didn't act on the warning.	I chose to follow the instructions because I thought, ”oh, there must be an issue when logging in with safari, or maybe I typed my password in wrong.” normally i use firefox
123	yes	entered answers	no	N/A	yes: I didn't take too much precaution even after seeing it. I just thought I would trust it since this is part of UC Berkeley's experiment.	I answered it because it was required in order to log in, otherwise there was no way for me to enter.

Group 1 (challenge questions): Study experiences

User #	Fell for attack?	How attack ended	Saw something suspicious/dangerous?	If yes, reaction?	Remembered seeing warning? If yes, effect on decisions?	Followed attack instructions? Why or why not? (Question 18)
128	yes	entered answers	no	N/A	yes	I answered the questions because I thought I was being asked to identify myself.
133	yes	entered answers	no	N/A	no	I did because I wanted to stay secure so that people couldn’t come in and take my paypal account
138	yes	entered answers	no	N/A	no	I thought that maybe I hadn’t made a prediction in a while so I had to reverify my identity by answering challenge questions.
143	yes	entered answers	no	N/A	yes	I did, I thought it was necessary
148	yes	entered answers	no	N/A	no	I answered them because I couldn’t remember if you guys said that we will randomly be asked to answer them in place of our password and login name.
153	yes	entered answers	no	N/A	no	I had no inkling of foul play. I had bookmarked the page, and so the only way there could be a problem is if someone hacked into the system. And even if someone had hacked the site, what had I to lose? An experiment account? I was not particularly worried.

Group 1 (challenge questions): Study experiences

User #	Fell for attack?	How attack ended	Saw something suspicious/dangerous?	If yes, reaction?	Remembered seeing warning? If yes, effect on decisions?	Followed attack instructions? Why or why not? (Question 18)
158	yes	entered answers	yes: After logging in last (this log in), I was warned that my computer didn't trust the website before it let me enter the site. I was asked if I wanted to proceed.	I was confused and slightly apprehensive because that had never happened to me before when logging in to the site. At first I pressed the "back" button and tried again, but the same result occurred. I chose to continue anyways.	no	I answered my challenge questions because I thought the site wanted to make sure that it was in fact myself that was logging in.
163	yes	entered answers	no	N/A	no	I followed the instructions because it was for my own safety.
168	yes	entered answers	yes: On the final login (simulated attack), I was given a notice that security was insecure, and was given the opportunity to view a certificate.	Nothing. I wish I had looked at that certificate.	no: I could have mentally dismissed it because I don't think I gave you any important information about myself.	(I answered the questions)It's 7am and I wasn't really thinking about it; I didn't imagine that a group of UCB students would be doing anything evil.
173	no	timeout	yes: i tried to log in the session before this one, and a pop-up told me that the security certificate was questionable (maybe out of date?).	i exited out of the browser, and tried again to see if the same message came up.	no	I don't think I did, because the pop-up told me the security certificate was faulty.

Group 1 (challenge questions): Study experiences

User #	**Fell for attack?**	**How attack ended**	**Saw something suspicious/dangerous?**	**If yes, reaction?**	**Remembered seeing warning? If yes, effect on decisions?**	**Followed attack instructions? Why or why not? (Question 18)**
178	yes	entered answers	no	N/A	no	i did it because it told me i needed to pick two for each time i logged in and i didn't have a problem with that
183	yes	entered answers	no	N/A	no	I could not get logged on. It kept giving me an error message. But it knew my answers were wrong-I initially misspelled 'Mitsubishi.'
188	yes	entered answers	No response	No response	no	figured it had been too many days since I'd signed in.
193	yes	entered answers	no	N/A	yes: The site felt more authentic and safer.	I thought I mis-typed my password and was unable to read the dialog box that came before this.
198	yes	entered answers	yes	No response	no	I filled out the fields, because I wanted to access the website, and it told me to.
203	no	timeout	No response	No response	yes	No response
208	no	timeout	no	N/A	no	In case I forgot my password
213	yes	entered answers	No response	No response	No response	No response
218	yes	entered answers	no	N/A	yes: It's such a common warning, and a given that I wouldn't tell people my security question answers. I disregarded it.	I followed the instructions because I had already logged in, and my information was saved on my computer. When I came across the instructions the first time, I closed the window, cleared my firefox cache, and opened it in a new window to login again. Then it appeared a 2nd time, and I assumed I had to fill out the questions to progress– or maybe I assumed that someone had tried to hack my account, and I needed to verify the correct answers to the questions.

Group 1 (challenge questions): Study experiences

User #	Fell for attack?	How attack ended	Saw something suspicious/dangerous?	If yes, reaction?	Remembered seeing warning? If yes, effect on decisions?	Followed attack instructions? Why or why not? (Question 18)
223	yes	entered answers	no	N/A	yes: it didn't because i forgot	i thought it would be safe since i used the saved link directly to the experiment and i just accidentally deleted a cookie or something.
228	yes	entered answers	no	N/A	no	To correctly identify the user.
233	yes	entered answers	no	N/A	no	I figured that because I switched connections, as I was using Berkeley's wireless as opposed to my dormitory's ethernet internet, they needed to re-verify my account.
238	yes	entered answers	no	N/A	no	I wanted to pick movies
243	yes	entered answers	no	N/A	no	Because it said so
248	yes	entered answers	no	N/A	yes: it made me more cautious about my login information	i wanted to log in, so i answered the challenge questions
253	yes	entered answers	no	N/A	no	I followed the instructions because I assumed my password was wrong so the alternate method of login was by answering the security questions.
258	yes	entered answers	no	N/A	no	I followed the above instructions because I figured it was just part of the logging on process to get to the webpage.
273	yes	entered answers	no	N/A	no	I remembered this page, and I followed the instructions because they are often used to verify a user if a username seems unsafe or has been tampered with.
278	yes	entered answers	no	N/A	no	i don't remember.

Group 1 (challenge questions): Study experiences

User #	Fell for attack?	How attack ended	Saw something suspicious/dangerous?	If yes, reaction?	Remembered seeing warning? If yes, effect on decisions?	Followed attack instructions? Why or why not? (Question 18)
283	yes	entered answers	yes: When it asked me for my security questions again at the end I felt that was odd.	I thought I had somehow been logged out. I tried to log in using different links. In the end, when I used the old link from the email, I decided to just input my security question again.	no	I did it because I thought I had been logged out completely from the study instead of my computer remembering my login information. I had accessed the site using a different method than usual, so I believed that to be the reason I was being asked again (usually I used the link from my email, but this time I tried to type in the site address from memory).

Group 1 (challenge questions): Registration attitudes

			Security of:		Convenience of:	
User #	**Used challenge questions before? If yes, where?**	**Benefits of registration via challenge questions**	**Passwords + no registration**	**Passwords + challenge questions for registration**	**Passwords + no registration**	**Passwords + challenge questions for registration**
73	yes: banking websites, like golden1.com	It has a security benefit if the questions are used to register private computers and allow users temporary access from public computers. It's essentially adding multiple passwords; these are not needed on trusted computers, however.	Fairly secure	Very secure	I hardly noticed it	I could get used to it
78	yes: I don't remember	Considering I was fooled into giving up my answers, not much benefit	I don't know	Somewhat secure	I don't know	I don't know
83	yes: ingdirect.com, mfa.lanxtra.com	You are asked to provide answers to questions that ideally should be easy for the user to know, but difficult for others to guess. Using these on top of usernames and passwords creates an additional wall that potential hackers have to break through.	Somewhat secure	Very secure	I hardly noticed it	I could get used to it
88	yes: Almost all websites	It allows you to retrieve your password if you forget it	Fairly secure	Very secure	I hardly noticed it	I hardly noticed it
93	yes: i dont know specifically, but many websites have them	i think it works similar to a password, just that it is something a person is more likely to remember. it is basically a backup password that you are not likely to forget. the security benefit is that it is something more for a person to get past if they are trying to access your information. just another safeguard.	Somewhat secure	Fairly secure	I hardly noticed it	I hardly noticed it

Group 1 (challenge questions): Registration attitudes

			Security of:		**Convenience of:**	
User #	**Used challenge questions before? If yes, where?**	**Benefits of registration via challenge questions**	**Passwords + no registration**	**Passwords + challenge questions for registration**	**Passwords + no registration**	**Passwords + challenge questions for registration**
98	yes: Bank of America	I think that they are not that safe. I would rather use other means of password retrieval and person recognition, etc. Sometimes its hard to remember the answers to questions.	Fairly secure	Fairly secure	I hardly noticed it	Hard or slightly annoying
103	yes: Bank of America	If you forget your password, they ask the challenge questions	Somewhat secure	Fairly secure	I don't know	I hardly noticed it
108	yes: Bank	It secures the account by only letting those who know the answers access the account in case of suspicous activity. I think it makes the accounts more secure.	Fairly secure	Very secure	I hardly noticed it	Hard or slightly annoying
113	yes: Bank of America Email	Challenge questions are an extra precaution to personalize one's account. It provides a safeguard against those that may try steal account information but they don't know personal details in the challenge questions.	Not secure at all	Very secure	I hardly noticed it	I hardly noticed it
118	yes: paypal, email websites... I think of it as a pretty common system	I guess I usually imagine that it has a negative affect on security, because it offers criminals another route to access your information	Somewhat secure	Very secure	I hardly noticed it	I hardly noticed it
123	yes: Bank of America Chase.com	I think it really does have benefits, although a person shouldn't use simple answers that most people know.	Somewhat secure	Very secure	I hardly noticed it	I could get used to it
128	yes: Emigrant Direct, Paypal	Makes it harder for robots to break into an account	Somewhat secure	Very secure	I hardly noticed it	I could get used to it

Group 1 (challenge questions): Registration attitudes

			Security of:		Convenience of:	
User #	Used challenge questions before? If yes, where?	Benefits of registration via challenge questions	Passwords + no registration	Passwords + challenge questions for registration	Passwords + no registration	Passwords + challenge questions for registration
133	yes: paypal, ebay	it helps prevent anyone from signing in.	Somewhat secure	Fairly secure	I could get used to it	I could get used to it
138	yes: Bank of America	If you forget your password, you are still able to log in, because you use your challenge questions	Fairly secure	Very secure	I could get used to it	I could get used to it
143	no	No response	Somewhat secure	Fairly secure	I could get used to it	Hard or slightly annoying
148	yes: vanguard	They are questions that are supposed to ONLY be answerable by you.	I don't know	Very secure	I don't know	I could get used to it
153	yes: E-mail sites are the only ones that really come to mind.	I find it fairly silly, because people will either choose questions that *they* forget the answer to (or an answer that changes with time), or they will choose a question that's easy to figure out.	Somewhat secure	Fairly secure	I hardly noticed it	I could get used to it
158	yes: Bank of America online banking, most other sites that require a log in.	It allows users to recover forgotten passwords. It provides the benefits of allowing people to recover their passwords while theoretically making sure that the correct user is recovering the password.	Very secure	Very secure	I hardly noticed it	I hardly noticed it
163	yes: Yahoo, paypal...	If someone does get your password but mistype it, the security questions are great in protecting them from accessing your account.	Not secure at all	Very secure	I could get used to it	I could get used to it

Group 1 (challenge questions): Registration attitudes

			Security of:		Convenience of:	
User #	**Used challenge questions before? If yes, where?**	**Benefits of registration via challenge questions**	**Passwords + no registration**	**Passwords + challenge questions for registration**	**Passwords + no registration**	**Passwords + challenge questions for registration**
168	no	The site is verifying I am who I say I am; I never thought of it in terms of me questioning the site's identity.	Fairly secure	Fairly secure	I could get used to it	Hard or slightly annoying
173	yes: banking websites, email	it's a good check, especially with specific questions like pet's names or mother's maiden name, when a customer forgets a password. if it's something as basic as "the street you grew up on" or your pet's name, then the information isn't that sensitive anyway.	Somewhat secure	Very secure	I hardly noticed it	I could get used to it
178	yes: bankofamerica	it makes it more personalized/secretive for logging in, in addition to one's password	Fairly secure	Very secure	I could get used to it	I hardly noticed it
183	yes: PayPal?	I always forget them anyway, unless I write them down. Do I really want anonymous people to know my mother's maiden name and the like?	Somewhat secure	Somewhat secure	I hardly noticed it	I could get used to it
188	yes: banking sites (yikes!)	i don't like it. you need to use a simple question and even still you end up forgetting it.	Fairly secure	Fairly secure	I could get used to it	I could get used to it
193	yes: neopets, paypal, fafsa	It feels safer to be asked a few questions that others may not know the answer to.	I don't know	Fairly secure	I hardly noticed it	Hard or slightly annoying

Group 1 (challenge questions): Registration attitudes

			Security of:		Convenience of:	
User #	Used challenge questions before? If yes, where?	Benefits of registration via challenge questions	Passwords + no registration	Passwords + challenge questions for registration	Passwords + no registration	Passwords + challenge questions for registration
198	yes: Lots. I specifically remember this from ING Direct (a banking site).	I think it has very few security benefits. It seems easy for an attacker to present a convincing fake of the question form, and harvest my answers to the questions.	Fairly secure	Fairly secure	I hardly noticed it	Hard or slightly annoying
203	No response	No response	Somewhat secure	No response	No response	No response
208	yes: Bank of America	I have no idea.	Somewhat secure	Fairly secure	I could get used to it	I hardly noticed it
213	No response	No response	No response	No response	No response	No response
218	yes: Wachovia, Gmail, a million others...	I think what's best is when you're allowed to ask your own question and answer it, not just pick from a drop-down preset menu with no personalized option. Security benefits it has- it eliminates people who don't know you from the list of ppl able to hack your account. But in reality too many people know the information, so it can't ever be completely effective. Anyone I knew in high school could have figured out the answers.	Somewhat secure	Very secure	I hardly noticed it	I hardly noticed it
223	yes: all email	there should definitely be more than one question, but if someone knows the answers they can get your pw right away	Fairly secure	Fairly secure	I hardly noticed it	I hardly noticed it
228	yes: Banking, email, password retrieval, etc.	It works when the questions ask things only you would know.	Somewhat secure	Very secure	I hardly noticed it	I could get used to it

Group 1 (challenge questions): Registration attitudes

			Security of:		Convenience of:	
User #	**Used challenge questions before? If yes, where?**	**Benefits of registration via challenge questions**	**Passwords + no registration**	**Passwords + challenge questions for registration**	**Passwords + no registration**	**Passwords + challenge questions for registration**
233	yes: Websites, Amazon.com	Challenge questions make it so that only those who actually know your background can access your account.	Fairly secure	Very secure	I hardly noticed it	I hardly noticed it
238	no	No response	No response	No response	No response	No response
243	no	Not much benefits.	Fairly secure	Fairly secure	I hardly noticed it	I hardly noticed it
248	no	challenge questions prevent people from hacking your account and resetting your password	Somewhat secure	Fairly secure	I hardly noticed it	I hardly noticed it
253	yes: Don't remember but usually porely made ones.	No security benefits, I think its a waste of time.	Fairly secure	Somewhat secure	I hardly noticed it	Nearly impossible or very annoying
258	yes: Lots, banking sites, shopping sites, email	The challenge questions are beneficial because they are personal enough to prevent people who don't know you from hacking into your account.	Fairly secure	Very secure	I hardly noticed it	I hardly noticed it
273	yes: A lot- shopping websites, school websites, and email accounts.	It makes the account safer and harder to hack into, which makes the account safer and the user feel that the site is more reliable.	Somewhat secure	Very secure	I hardly noticed it	Hard or slightly annoying
278	no	It can add another layer of defense.	Fairly secure	Very secure	I could get used to it	Hard or slightly annoying
283	yes: Bank websites.	It is a question that only you should know the answer to. It is a two-fold check because you are able to check if you are being asked the right security questions and if you know the correct answer.	Somewhat secure	Fairly secure	I hardly noticed it	I hardly noticed it

Group 1 (challenge questions): General questions/feeback

User #	Average length of each visit	Anything annoying or difficult?	Engaging or interesting?	General comments
73	5-10 minutes	Yes, I found the security questions annoying.	yes	Had I been on a private, personal computer that I had registered before, I would have known not to answer the extra questions. As it is, I am using a public computer and so expected to have to answer security questions.
78	0-5 minutes	No	yes	Well done! I was so focused on making money from the predictions that I failed to take any security precautions
83	0-5 minutes	No, it was easy to follow.	yes	No response
88	0-5 minutes	No response	yes	No response
93	0-5 minutes	no	yes	No response
98	0-5 minutes	no	yes	no
103	0-5 minutes	no	yes	No response
108	5-10 minutes	No	yes	None
113	5-10 minutes	Only when I was wrong!	yes	Great website design - easy to use and it looks good. Study was easy to access and complete.
118	0-5 minutes	No, not really. Well done. However, I feel like I missed something that was supposed to indicate a security compromise	yes	No response
123	5-10 minutes	None	yes	None
128	5-10 minutes	No	yes	I kept forgetting to do my movie predictions - I think there should be a reminder email everyday.
133	5-10 minutes	no	yes	I enjoyed this study, it was very interesting.
138	5-10 minutes	No	yes	No response
143	5-10 minutes	No	yes	No response
148	0-5 minutes	No not really.	yes	No response
153	5-10 minutes	No, it was nice. :)	no	The debriefing really took me by surprise. I was completely unable to guess the hypothesis. Kudos!
158	5-10 minutes	Sometimes it was hard to remember to predict the movies every day.	yes	No.
163	0-5 minutes	no	yes	no
168	5-10 minutes	no	yes	interesting study, thanks!
173	0-5 minutes	the deception was a little annoying - i was enjoying predicting which movies would do well!	yes	nice one, guys.
178	0-5 minutes	no	yes	No response

Group 1 (challenge questions): General questions/feeback

User #	Average length of each visit	Anything annoying or difficult?	Engaging or interesting?	General comments
183	0-5 minutes	No.	yes	I liked trying to figure out the winning movies!
188	No response	No response	No response	No response
193	0-5 minutes	I watch movies once a year. I basically took a poll from my friends before I answered the questions.	no	No response
198	5-10 minutes	I was frustrated that the box office results were slow to update.	yes	I still don't understand how the attack against me was supposed to work. Does it assume that the actual site's server has been compromised?
203	5-10 minutes	No response	No response	No response
208	0-5 minutes	No	yes	I like the twist! =)
213	No response	No response	No response	No response
218	5-10 minutes	Yeah! The results for top grossing movie for a particular day would switch over time, decreasing my bonus $!	yes	No response
223	0-5 minutes	No response	yes	No response
228	0-5 minutes	Exit survey is kind of long.	yes	Fun to predict movies.
233	0-5 minutes	No.	yes	Clever.
238	5-10 minutes	No response	yes	No response
243	5-10 minutes	no	yes	no
248	0-5 minutes	no	yes	it was a good study, there was lots to interpret from the information
253	5-10 minutes	I didn't fully understand that the order of predictions makes a difference until after the 3rd try because I didn't fully read the FAQ until then.	yes	No response
258	0-5 minutes	no	yes	no
273	5-10 minutes	No, not really.	yes	No, except that the login part at the end was a little weird. I was a bit hesitant on entering the site.
278	5-10 minutes	nope	yes	The movie prediction process was alluring and distracting from the true motives of the study.
283	0-5 minutes	No, just now I am very cautious about answering these questions.	yes	No response

Group 2 (email with warnings, forwarding attack): Demographics

User #	Gender	Age	Student status or occupation	Details	OS	Primary browser	Web use/week (hrs)	Financial transactions done online	Experience doing financial transactions online
77	No response	No response	No response	No response	No response	No response	No response	No	Never
87	Female	22-25	staff	No response	No response	No response	No response	No	Never
92	No response	No response	No response	No response	No response	No response	No response	No	Never
97	Male	22-25	Undergraduate	Economics or business	Windows	Firefox	20+	Banking, Investing, Shopping, Auctions	> 2 years
102	Male	18-21	Undergraduate	Computer science	Mac OS	Safari	20+	Shopping	> 2 years
107	Female	22-25	Graduate	Engineering	Windows	Firefox	20+	Banking, Shopping, Auctions	> 2 years
112	Female	18-21	Undergraduate	Humanities	Windows	Internet Explorer	5-10	Banking, Shopping, PayPal	> 2 years
117	Male	18-21	Undergraduate	Bioengineering	Windows	Firefox	20+	Banking, Shopping	> 2 years
122	Female	22-25	recent	No response	Windows	Firefox	20+	Banking, Shopping, PayPal	> 2 years
127	Female	18-21	Undergraduate	Social sciences	Windows	Firefox	20+	Banking, Shopping	> 2 years
132	Female	18-21	Undergraduate	Economics or business	Windows	Firefox	20+	Shopping	Never
137	Female	18-21	Undergraduate	public health	Mac OS	Firefox	5-10	Banking, Shopping	Never
142	Female	22-25	Undergraduate	biology and psychology	Windows	Firefox	10-20	Banking, Shopping, Auctions, PayPal	1–2 years
147	Male	18-21	Undergraduate	Natural sciences	Windows	Opera	10-20	Banking, Shopping, Auctions, PayPal	6–12 months
152	Female	18-21	Undergraduate	Social sciences	Windows	Internet Explorer	0-5	Shopping	1–2 years

Group 2 (email with warnings, forwarding attack): Demographics

User #	Gender	Age	Student status or occupation	Details	OS	Primary browser	Web use/week (hrs)	Financial transactions done online	Experience doing financial transactions online
157	Male	22-25	Undergraduate	Computer science	Mac OS	Safari	20+	Banking, Investing, PayPal	> 2 years
162	Female	18-21	Undergraduate	Humanities	Mac OS	Firefox	10-20	Banking, PayPal	> 2 years
167	Female	18-21	Undergraduate	Social sciences	Windows	Firefox	10-20	Banking, Shopping, Auctions	> 2 years
172	Male	18-21	Undergraduate	Natural sciences	Windows	Firefox	10-20	Banking, PayPal	> 2 years
177	Male	18-21	Undergraduate	Economics or business	Windows	Firefox	20+	Banking, Investing, Shopping, Auctions, PayPal	> 2 years
182	Female	18-21	Undergraduate	Natural sciences	Windows	Firefox	10-20	Banking, Shopping	6–12 months
187	Female	18-21	Undergraduate	Natural sciences	Mac OS	Safari	5-10	Banking, Shopping	1–2 years
192	Male	18-21	Undergraduate	Economics or business	Mac OS	Firefox	20+	Banking, PayPal	1–2 years
197	Female	22-25	Undergraduate	Social sciences	Mac OS	Firefox	5-10	Banking, Shopping, Auctions, PayPal	6–12 months
202	Female	18-21	Undergraduate	Economics or business	Windows	Firefox	10-20	Shopping	1–2 years
207	Male	18-21	Undergraduate	Engineering	Windows	Firefox	20+	Shopping	> 2 years
212	Female	18-21	Undergraduate	Humanities	Windows	Firefox	10-20	Banking, Auctions, PayPal	> 2 years
217	No response	No response	No response	No response	No response	No response	No response	No	Never
222	Male	22-25	Undergraduate	Humanities	Mac OS	Camino	5-10	Banking, Shopping, Auctions, PayPal	> 2 years
227	Male	18-21	Undergraduate	Natural sciences	Windows	Firefox	10-20	Shopping	< 6 months
232	Male	18-21	Undergraduate	Engineering	Windows	Firefox	20+	Banking, Shopping	> 2 years

Group 2 (email with warnings, forwarding attack): Demographics

User #	Gender	Age	Student status or occupation	Details	OS	Primary browser	Web use/week (hrs)	Financial transactions done online	Experience doing financial transactions online
237	Female	18-21	Undergraduate	Engineering	Windows	Internet Explorer	10-20	Banking, Shopping	Never
242	No response	No response	No response	No response	No response	No response	No response	No	Never
247	Female	18-21	Undergraduate	Economics or business	Windows	Firefox	10-20	Shopping, Auctions	1–2 years
252	Male	18-21	Undergraduate	Social sciences	Windows	Firefox	5-10	Banking, Shopping, Auctions, PayPal	1–2 years
257	Female	18-21	Undergraduate	Natural sciences	Windows	Firefox	5-10	Banking, Shopping, Auctions, PayPal	> 2 years
267	Male	18-21	Undergraduate	Natural sciences	Windows	Firefox	20+	Banking, Shopping, Auctions, PayPal	> 2 years
272	Male	18-21	Undergraduate	Economics or business	Windows	Firefox	10-20	Shopping, PayPal	< 6 months
277	Female	18-21	Undergraduate	Cognitive Science	Mac OS	Firefox	20+	PayPal	< 6 months
282	Male	18-21	Undergraduate	Economics or business	Windows	Firefox	10-20	Shopping	< 6 months

Group 2 (email with warnings, forwarding attack): Web security attitudes

			How often & thoroughly user applies precautions when logging into:					
User #	Biggest security concerns while browsing the Web	Precautions taken when logging into a Web site	Banking	Paypal	Web email	Shopping	Social networking	Study site
77	No response	No response	No response	No response	No response	No response	No response	No response
87	No response	No response	No response	No response	No response	No response	No response	No response
92	No response	No response	No response	No response	No response	No response	No response	No response
97	safety of my personal information	ensure passwords are hidden when typed never save passwords	Always	Always	Always	Always	Always	Always
102	Someone stealing my information.	None	Don't use	Don't use	Rarely	Rarely	Rarely	Rarely
107	Viruses, Identity theft	Double checking information security, especially for payments	Usually	Usually	Sometimes	Always	Rarely	Rarely
112	I don't have any concerns. I play it safe.	Sometimes I will type my passwords in really really quickly if I'm at a public computer with people around...	Sometimes	Rarely	Rarely	Rarely	Rarely	Rarely
117	Security of my personal information that's stored on someone else's server, security of my financial accounts, and the security of my personal computer from outside attack.	Never log into sites that look suspicious, or that ask for a user name/password for a different site. Check the URL to make sure it's not merely a look-alike page trying to phish my information.	Always	Usually	Usually	Always	Sometimes	Sometimes
122	stealing my password stealing my credit card number storing my credit card number	changing passwords clearing history and cookies	Usually	Usually	Sometimes	Sometimes	Sometimes	Rarely

Group 2 (email with warnings, forwarding attack): Web security attitudes

			How often & thoroughly user applies precautions when logging into:					
User #	**Biggest security concerns while browsing the Web**	**Precautions taken when logging into a Web site**	**Banking**	**Paypal**	**Web email**	**Shopping**	**Social networking**	**Study site**
127	viruses	nothing in particular	Sometimes	Sometimes	Rarely	Sometimes	Rarely	Sometimes
132	1) total/comprehensive profiling on every level (ie personal emails, shopping preferences, locations) 2) 3rd party profit-makers selling my profile	different passwords, fake answers to security questions (ie Mother's maiden name)	Don't use	Always	Usually	Usually	Usually	Sometimes
137	bank account kacing	i never save passwords	Always	Always	Usually	Usually	Usually	Sometimes
142	identity theft, especially relating to monetary matters	only logging in from my personal computer if sensitive information is involved, clearing browser data after making a credit card purchase online	Usually	Usually	Rarely	Usually	Rarely	Rarely
147	Keylogging, fake sites, identity theft	Visual keyboards	Sometimes	Usually	Rarely	Always	Rarely	Rarely
152	Someone stealing my credit card information	I don't tell anyone my passwords, and I only buy things with my credit card from my personal computer	Always	Always	Rarely	Always	Rarely	Rarely
157	fake wifi access points, keyloggers, wifi eavesdropping	enter address manually, check address bar, look for lock icon in browser, watch for bad certificates	Always	Always	Always	Usually	Usually	Always
162	entering my credit card number accessing my bank account	only using secure internet connections	Always	Usually	Usually	Usually	Rarely	Rarely
167	Getting viruses	Use Norton 360 and have the browsing protector on	Always	Always	Always	Always	Always	Always

Group 2 (email with warnings, forwarding attack): Web security attitudes

			How often & thoroughly user applies precautions when logging into:					
User #	**Biggest security concerns while browsing the Web**	**Precautions taken when logging into a Web site**	**Banking**	**Paypal**	**Web email**	**Shopping**	**Social networking**	**Study site**
172	Identity theft, key loggers.	Not saving my password, using script blockers.	Usually	Sometimes	Rarely	Usually	Always	Rarely
177	-identity theft	-logout always -be cautious when entering information i.e. making sure it's a legit website	Sometimes	Sometimes	Rarely	Rarely	Sometimes	Always
182	safety, consistency, password	password	Always	Always	Always	Always	Always	Always
187	someone finding my credit card information	I do not save passwords when financial transactions occur	Always	Always	Rarely	Always	Rarely	Rarely
192	hacking	see if it is a legitimate site	Usually	Usually	Usually	Usually	Usually	Usually
197	hacking, other people viewing private information	I usuallly delete any cookies once a week or after visiting sites that have information I don't want others to try to get	Usually	Sometimes	Sometimes	Sometimes	Rarely	Sometimes
202	Identity theft, viruses	I now check the website, which I usually have bookmarked because once I was redirected to login and someone got my account info. I also now change passwords often.	Don't use	Rarely	Always	Always	Usually	Sometimes
207	Giving my credit card number to someone unreliable.	I make sure the website is legitimate, a website that is frequently used by many people.	Usually	Usually	Rarely	Usually	Rarely	Don't use

Group 2 (email with warnings, forwarding attack): Web security attitudes

			How often & thoroughly user applies precautions when logging into:					
User #	**Biggest security concerns while browsing the Web**	**Precautions taken when logging into a Web site**	**Banking**	**Paypal**	**Web email**	**Shopping**	**Social networking**	**Study site**
212	1. Getting a virus from a random site when doing searches. 2. Hackers getting my passwords or identification information 3. Someone taking over my email, facebook, etc account.	I never save my password into the computer, even with my own computer, and I usually check the address to make sure it's the original site and not just a copycat. Before this study, I've never forwarded an email for a website I use or given password info in an email.	Usually	Always	Sometimes	Usually	Usually	Sometimes
217	No response	No response	No response	No response	No response	No response	No response	No response
222	My biggest concern is that, while connected to a WiFi spot, I'll be entering my banking information and someone else will acquire it.	I make sure that I see the little secure logo thingy in the address bar. I also don't enter secure information over non-encrypted WiFi connections.	Always	Always	Rarely	Always	Rarely	Rarely
227	Trojans and Spyware	I do not use the auto-save option for username and password	Usually	Always	Usually	Always	Sometimes	Usually
232	viruses/trojans/spyware hackers identity theft	do not save user name or password	Always	Always	Always	Always	Always	Always
237	stealing credit card numbers, stealing identity, spyware	none	Rarely	Rarely	Rarely	Rarely	Rarely	Rarely
242	No response	No response	No response	No response	No response	No response	No response	No response

Group 2 (email with warnings, forwarding attack): Web security attitudes

			How often & thoroughly user applies precautions when logging into:					
User #	Biggest security concerns while browsing the Web	Precautions taken when logging into a Web site	Banking	Paypal	Web email	Shopping	Social networking	Study site
247	1. Password hacking 2. Web viruses 3. Identity theft	I put my computer on high security detection ensuring that my computer notifies me when I am accessing a website that is dangerous to my computer.	Rarely	Sometimes	Rarely	Sometimes	Sometimes	Rarely
252	keylogging hacks into my own computer to steal cookies phished sites	antivirus/firewall auto-login where allowed different passwords	Usually	Usually	Usually	Sometimes	Sometimes	Sometimes
257	Phishing sites, Spy-mechanisms, Privacy and Security of personal information	I double check the website's address. I make sure the secured lock symbol is shown at the bottom right corner of the browser window. And I only access website addresses that I know	Always	Always	Usually	Usually	Usually	Usually
267	I worried about where my credit card information goes.	I don't really take any, but I do monitor my credit card bills after I make a purchase.	Sometimes	Usually	Don't use	Always	Rarely	Rarely
272	viruses, hacking, and identity theft	using uncommon screenames and a combination of numbers and letters for passwords	Always	Usually	Usually	Always	Always	Usually
277	Picking up viruses and getting accounts hacked with fake websites that ask for login information.	At facebook and myspace, I check the urls when I'm logging in to make sure they look right before I enter in my login information.	Rarely	Sometimes	Rarely	Usually	Sometimes	Sometimes
282	None	Secure, hacker safe, legitimate	Usually	Usually	Usually	Usually	Usually	Usually

Group 2 (email with warnings, forwarding attack): Study experiences

User #	**Fell for attack?**	**How attack ended**	**Saw something suspicious/dangerous?**	**If yes, reaction?**	**Remembered seeing warning? If yes, effect on decisions?**	**Followed attack instructions? Why or why not? (Question 18)**
77	yes	forwarded url	No response	No response	No response	No response
87	yes	forwarded url	No response	No response	No response	No response
92	yes	forwarded url	No response	No response	No response	No response
97	no	followed plain url	no	N/A	yes: was confused on what to do	i didnt follow it because i didnt know what to do
102	no	followed html url	no	N/A	no	I did not forward the email. It looked like the first time I logged in, so I thought there was something wrong with my account. I did not notice the instructions to forward the email.
107	no	timeout	no	N/A	yes: I didn't forward the email because of it. I decided to just wait and perhaps log in later.	I didn't follow the instructions because the email sent said otherwise.
112	yes	forwarded url	no	N/A	yes: Not at all, because it's just a silly website that doesn't have any of my deeply personal information.	WHICH instructions? To click it or not to click it? I forwarded the link. If this appeared twice in the process of this study, then I definitely clicked it once.

Group 2 (email with warnings, forwarding attack): Study experiences

User #	Fell for attack?	How attack ended	Saw something suspicious/dangerous?	If yes, reaction?	Remembered seeing warning? If yes, effect on decisions?	Followed attack instructions? Why or why not? (Question 18)
117	no	followed plain url	yes: When it asked me to forward an email to them despite an explicit warning to do no such thing in the past, on the last time I logged in.	My reaction was first confusion, then deep suspicion - why would they need me to forward them an email they had just sent me? And why this time and not the previous several times I'd logged in? I disregarded the instructions on the suspicious page and followed through with my regular procedure for registration.	yes: It made me deeply suspicious about being asked to forward the email, so I did not.	I chose not to follow the instruction, because it seemed extremely fishy - it didn't make any sense to me that they would send me an email with a link in it and then ask me NOT to click it (especially after having done it a couple of times before). Also, the email address listed ”ucb-moviepredictions.com”, which I realized was not the correct URL for the study.
122	no	followed html url	no	N/A	yes: I didn't choose to cut and paste the link.	I don't really remember this or I misread it.
127	no	timeout + forwarded invalid emails	no	N/A	no	it looked authentic
132	yes	forwarded url	no	N/A	yes: It didn't because clicking was the easiest path regardless.	I wanted to log in and make my predictions. The email address looked legitimate enough.
137	yes	forwarded url	no	N/A	no	because that is what it said to do

Group 2 (email with warnings, forwarding attack): Study experiences

User #	Fell for attack?	How attack ended	Saw something suspicious/dangerous?	If yes, reaction?	Remembered seeing warning? If yes, effect on decisions?	Followed attack instructions? Why or why not? (Question 18)
142	no	timeout	yes: the login screen which instructed to forward the login email. the original login email's warnings were also a bit suspicious	I ignored the instructions about forwarding the email, since they contradicted the first one, and tried to log in again normally.	yes: It helped me avoid the security "attack" at the end of the study.	I didn't follow the instructions because they were contradictory to the warnings in the previous email. And forwarding an email doesn't seem like a logical way to log in to a website.
147	yes	forwarded url	no	N/A	no	My security system did not alert me to any falsehood. Paypal is secure enough even if it is false.
152	no	followed plain url	no	N/A	yes: I didn't see it the first time I opened the e-mail, but about a week later I read it. It didn't change my interaction with the website.	I remember seeing this page and I was confused. I did not follow the instructions because I thought it was a mistake.
157	no	followed html url	yes: suspicious message on ucbmoviepredictions.com asking to send an email to ucb-moviepredictions.com, which has a bad certificate.	thought about what to do for 5 minutes, looked carefully at email. Usually the email is the less trustworthy but in this case I decided the website was hijacked.	yes: I partly ignored it because I left the site open in a browser tab for the whole study, and I don't know of any reasons not to cut-and-paste URLs. When the attack came at the end, I went back and read it again.	Did not follow– seemed suspicious. URL was different (had a dash in it) and explanation was bogus-sounding ("problems with our email system"?)
162	no	followed html url	no	N/A	yes: i followed the directions to protect my security.	I did not. I didn't read the instructions thoroughly and instead clicked.

Group 2 (email with warnings, forwarding attack): Study experiences

User #	Fell for attack?	How attack ended	Saw something suspicious/dangerous?	If yes, reaction?	Remembered seeing warning? If yes, effect on decisions?	Followed attack instructions? Why or why not? (Question 18)
167	no	timeout	no	N/A	yes: Did not affect my decisions.	I followed the instructions because I know that sometimes e-mails are given to people which might look like they are from a legitimate source when really they are viruses. I assumed that the UCB Movie Predictions webmaster was alerted that maybe someone was sending out e-mails with viruses.
172	yes	forwarded url	no	N/A	no	I replied because the e-mail address looked familiar and because I thought there really might have been problems with the system.
177	no	followed html url	no	N/A	no	I assumed the link was safe since the previous screen said that an email would be sent to me. I trusted the survey process at this point.
182	yes	forwarded url	no	N/A	yes: seems normal nowadays	says you should
187	no	timeout	no	N/A	no	I did not do anything with this because I thought it was a mistake, and that the error might be fixed tomorrow. I was going to try tomorrow, and if it came up again I would decide what to do.
192	no	followed html url	no	N/A	yes: nothing alarming	so i could continue with the study
197	no	followed html url	no	N/A	no	I believe I always just clicked the link. I don’t really recal seeing the warning below it and always just clicked the link because it was habit and I felt that after ”trying” to log in and getting the e-mail that it was safe.

Group 2 (email with warnings, forwarding attack): Study experiences

User #	Fell for attack?	How attack ended	Saw something suspicious/dangerous?	If yes, reaction?	Remembered seeing warning? If yes, effect on decisions?	Followed attack instructions? Why or why not? (Question 18)
202	no	followed html url	no	N/A	yes: I was confused because the website said to do the opposite. I sent an e-mail to the contact listed in the e-mail. Then I reread the website and e-mail and figured forwarding was only convenience and the link was to protect my security, so i clicked the link.	I didn't forward the e-mail because the e-mail told me not to for security reasons and this just said it would help them with their system problems. My security is more important to me than their system problems.
207	no	followed html url	no	N/A	yes	I did not get this.
212	yes	forwarded url	no	N/A	yes: It unfortunately didn't affect my reaction to the prompt to forward the registration email, because I thought if I didn't forward the email I would not be able to log in to complete the experiment.	I thought there had been a problem with the experiment site and it had tried to get me to re-activate my account, which would make me lose my movie prediction data. I must admit that I felt much safer and less suspicious responding to this site than I would with any other website, since I know this website is affiliated with a study for Xlab.
217	yes	forwarded url	No response	No response	No response	No response
222	yes	forwarded url	no	N/A	yes: I thought it was odd that it said never to forward the registration email, as I've never seen that warning before, but it didn't affect my decision making at all. I just chalked it up to general security advice and more or less forgot about it.	I followed the instructions, because with these sort of things I'm always afraid that if I don't do exactly what it says, I'm somehow going to mess up the entire system and my data will be lost, or I'll have to start from the beginning, etc. I did think it was a bit strange, as I've never seen this sort of thing before, but it wasn't outside the realm of reason, so I thought nothing of it.

Group 2 (email with warnings, forwarding attack): Study experiences

User #	Fell for attack?	How attack ended	Saw something suspicious/dangerous?	If yes, reaction?	Remembered seeing warning? If yes, effect on decisions?	Followed attack instructions? Why or why not? (Question 18)
227	no	timeout	no	N/A	yes: I checked my account information often to make sure it was still correct	I had already read the directions to NEVER forward that e-mail, so that is why I e-mailed to inquire about the situation
232	no	followed html url	no	N/A	yes: I followed the directions of the warning	I did not follow the instructions (i clicked the link because I was using a different operating system on the same computer and figured I needed to register the computer. I did not read the warning either; I assumed it was as same as before.
237	no	followed html url	no	N/A	yes: ignored it	didn't read it
242	no	followed plain url	No response	No response	No response	No response
247	yes	forwarded url	no	N/A	yes: It made me feel that the website was more secure.	I'm used to following what the website says so I just followed through with the actions stated.
252	yes	forwarded url	no	N/A	yes: I have a tendency to think beyond the absolute wording of rules, and any actions I take I try to keep within the spirit of the rules. I only forwarded the link to either myself or the first party (i.e. UCB Movie Predictions).	I thought that ucb-moviepredictions.com was the originating website (ucbmoviepredictions.com). I have been lacking in sleep over the past two weeks, and am currently pulling an all-nighter right now (filling out this survey is my study break). I believe I may have been somewhat more resistant to forwarding the email, but I probably would have sent it anyway: I noticed that a forwarded link did not seem to work on my second computer, and that probably affected my decision.

Group 2 (email with warnings, forwarding attack): Study experiences

User #	Fell for attack?	How attack ended	Saw something suspicious/dangerous?	If yes, reaction?	Remembered seeing warning? If yes, effect on decisions?	Followed attack instructions? Why or why not? (Question 18)
257	no	followed html url	no	N/A	yes: It enhanced my awareness of the vulnerability that personal information that's to remain confidential encounters. It encourages me to take more precautionary steps to make sure that the account remains secure.	I didn't follow the instructions because I thought it odd for that to show despite my numerous efforts to log-in sin clicking on the link. I just thought my log in process was just going through a minor glitch. I didn't think anything of it, honestly.
267	no	timeout	no	N/A	no	I only remember getting this email once today. I did not do anything because I had been accessing the predictions page just fine for the past couple days. I may have clicked on it the first time just out of habit from registering for some many other shopping sites.
272	yes	forwarded url	no	N/A	no	I followed the above instructions because it clearly said to not click on the link. The list of directions, along with the structure, was easy to follow.
277	yes	forwarded url	no	N/A	yes: It made me double check the e-mail I got about my information being disrupted, telling me to forward the e-mail to the support group for ucb movie predictions– because I wasn't quite sure what was going on. But after comparing the two, I went ahead and forwarded the e-mail.	I understood that email registration problems seemed likely for a small-scale program like ucb movie predictions, so I accepted what the information asked me to do.

Group 2 (email with warnings, forwarding attack): Study experiences

User #	Fell for attack?	How attack ended	Saw something suspicious/dangerous?	If yes, reaction?	Remembered seeing warning? If yes, effect on decisions?	Followed attack instructions? Why or why not? (Question 18)
282	no	timeout	no	N/A	yes	I chose to follow the instructions because it seemed like it would register the specific computer the survey was being taken from.

Group 2 (email with warnings, forwarding attack): Registration attitudes

			Security of:		Convenience of:	
User #	**Used email registration before? If yes, where?**	**Benefits of email registration**	**Passwords + no registration**	**Passwords + email for registration**	**Passwords + no registration**	**Passwords + email for registration**
77	No response	No response	No response	No response	No response	No response
87	No response	No response	No response	No response	No response	No response
92	No response	No response	No response	No response	No response	No response
97	yes: paypal	ensures you have access to the email address supplied	Somewhat secure	Very secure	I could get used to it	I hardly noticed it
102	no	When you click the link in the email to register your computer, the site stores information from the computer which the link was clicked. This will help defend against logins from other non-authorized computers.	Fairly secure	Fairly secure	I hardly noticed it	I could get used to it
107	yes: Facebook	Email registration allows a possibility of sending an email to the user to ensure that the login is authentic	Somewhat secure	Fairly secure	I could get used to it	I could get used to it
112	yes: Paypal, flickr, freakin' myspace.	It keeps my password within my email. But if the email account is hacked, I'm pretty much screwed.	Fairly secure	Fairly secure	I hardly noticed it	I hardly noticed it
117	yes: Can't remember off the top of my head	I'm not entirely sure. I can validate the owner of an email address used to sign up, which can be an important way of preventing identity theft.	Fairly secure	Fairly secure	I hardly noticed it	I hardly noticed it
122	yes: emails, groups	It keeps the person from registering multiple or fake IDs–or makes it more difficult in any case.	Somewhat secure	Fairly secure	I hardly noticed it	I could get used to it
127	yes	not sure	Fairly secure	Fairly secure	I hardly noticed it	I hardly noticed it

Group 2 (email with warnings, forwarding attack): Registration attitudes

			Security of:		Convenience of:	
User #	Used email registration before? If yes, where?	Benefits of email registration	Passwords + no registration	Passwords + email for registration	Passwords + no registration	Passwords + email for registration
132	yes: Shopping	directly confirms a connection with the subscriber and an address with which to contact them	Not secure at all	Somewhat secure	I could get used to it	Hard or slightly annoying
137	yes	you needa valid email that you have access to to register on a webite	Somewhat secure	Fairly secure	I hardly noticed it	I could get used to it
142	yes: various sites, can't remember them all, I think facebook, photo sites, gmail, etc.	It ensures that the email you enter belongs to you (or that you know the password to the email account at least), it prevents others from signing up using your email, and makes more of a hassle for people trying make fake accounts.	Somewhat secure	Fairly secure	I could get used to it	I could get used to it
147	no	Email is the only thing revealed.	Somewhat secure	Somewhat secure	I could get used to it	I could get used to it
152	no	Email registration makes it easier for me to remember my login name.	Somewhat secure	Fairly secure	I hardly noticed it	I hardly noticed it
157	yes: most sites I use, I think.	I sign up; I get an email; I click a link in the email to verify my address. It prevents me from signing up with a bogus email address.	Not secure at all	Fairly secure	I could get used to it	I hardly noticed it
162	no	No response	Fairly secure	Fairly secure	I hardly noticed it	Hard or slightly annoying
167	yes: Don't remember.	To make sure that the e-mail account really exists.	Fairly secure	Very secure	I hardly noticed it	I could get used to it

Group 2 (email with warnings, forwarding attack): Registration attitudes

			Security of:		Convenience of:	
User #	**Used email registration before? If yes, where?**	**Benefits of email registration**	**Passwords + no registration**	**Passwords + email for registration**	**Passwords + no registration**	**Passwords + email for registration**
172	no	I think that when I click the link something gets saved on my computer or my IP address is saved on their site.	Somewhat secure	Fairly secure	I hardly noticed it	I hardly noticed it
177	yes	it makes sure the person has access to the email address they are using	Somewhat secure	Very secure	I could get used to it	I could get used to it
182	yes: buying things	ensures correct information	Fairly secure	Very secure	I could get used to it	I could get used to it
187	yes	Only the person who has access to the e-mail account can register. This helps to insure that it is the correct person signing in, because only that person will have information about themselves and have access to their e-mail.	Fairly secure	Very secure	I hardly noticed it	I hardly noticed it
192	yes: facebook	click the link to verify the user	Somewhat secure	Fairly secure	I could get used to it	I could get used to it
197	no	I think it could work but would be weary because of other people creating false e-mail accounts, logging into others e-mail accounts, or people just switching accounts could cause problems	Fairly secure	Fairly secure	I hardly noticed it	I could get used to it
202	yes: Facebook, myspace, amazon.com	It allows me to get my password if I forget it. It also usually involves an e-mail to verify the account when setting up the account.	Somewhat secure	Very secure	I don't know	I hardly noticed it
207	no	You click on a link provided to you by email.	Somewhat secure	Somewhat secure	I hardly noticed it	I could get used to it

Group 2 (email with warnings, forwarding attack): Registration attitudes

			Security of:		Convenience of:	
User #	Used email registration before? If yes, where?	Benefits of email registration	Passwords + no registration	Passwords + email for registration	Passwords + no registration	Passwords + email for registration
212	yes: Ebay, facebook, Soompi, etc.	It ensures that only the person who holds the password to the user email account can register for the account, therefore ensuring the identity of the user, and that someone cannot sign up using another person's email address.	Somewhat secure	Fairly secure	I hardly noticed it	I could get used to it
217	No response	No response	No response	No response	No response	No response
222	yes: A lot of forums that I've joined, but I can't really remember any of them.	I think it works to prevent people from signing other people up for things that they don't want to be signed up for. I have no idea how the security works.	Very secure	Very secure	I hardly noticed it	I could get used to it
227	yes: Amazon, NewEgg, Best Buy, Circuit City, etc.	I feel it works similar to re-entering a password, and am not sure what security benefits it has	Fairly secure	Very secure	I hardly noticed it	Hard or slightly annoying
232	no: do not remember	People are not able to register others unless they also have access to their emal	Fairly secure	Fairly secure	Hard or slightly annoying	Hard or slightly annoying
237	no	to make sure it's actually you	Somewhat secure	Somewhat secure	Hard or slightly annoying	Hard or slightly annoying
242	No response	No response	No response	No response	No response	No response
247	yes	It ensures greater security by making the person log on to their email, hence taking a further step to register for the site. This increases the verification of the site.	Fairly secure	Very secure	I could get used to it	Hard or slightly annoying

Group 2 (email with warnings, forwarding attack): Registration attitudes

			Security of:		Convenience of:	
User #	**Used email registration before? If yes, where?**	**Benefits of email registration**	**Passwords + no registration**	**Passwords + email for registration**	**Passwords + no registration**	**Passwords + email for registration**
252	no	No response	Somewhat secure	Fairly secure	I hardly noticed it	I could get used to it
257	yes: ING, Yahoo Mail's Personalized symbols that show when logging in from a familiar computer.	I think the website recognizes the individual ip address, and/or cookies. But I really don't know.	Not secure at all	Very secure	I could get used to it	I hardly noticed it
267	no	I'm not comfortable with it because I don't feel like my email is particularly secure	Somewhat secure	Fairly secure	I hardly noticed it	I could get used to it
272	no	No response	Very secure	Very secure	I hardly noticed it	I hardly noticed it
277	yes: Hotmail, probably PayPal...it's hard to remember.	I think it assures that the person you say you are corresponds with you who you say you are in the general internet world.	Somewhat secure	Fairly secure	I could get used to it	Hard or slightly annoying
282	yes: Forums	Email registration just checks to make sure that it is a legitimate email address not a spam bot.	Fairly secure	Fairly secure	I could get used to it	I could get used to it

Group 2 (email with warnings, forwarding attack): General questions/feedback

User #	Average length of each visit	Anything annoying or difficult?	Engaging or interesting?	General comments
77	No response	No response	No response	No response
87	No response	No response	No response	No response
92	No response	No response	No response	No response
97	0-5 minutes	nope	yes	none
102	0-5 minutes	No	yes	No response
107	5-10 minutes	No.	yes	No response
112	0-5 minutes	When the predictions didn't update on Sunday. I wanted my money. My fiance and I were actually secretly competing.	yes	NOOOOOOOO
117	5-10 minutes	Nope.	yes	Clever! I wouldn't have guessed the real nature of the study until that bogus email forwarding request made me suspicious
122	5-10 minutes	no	yes	I really did enjoy it!
127	0-5 minutes	no	no	No response
132	0-5 minutes	(minor) subscribing to paypal	yes	tricky
137	0-5 minutes	no	yes	No response
142	0-5 minutes	the fake "pharming attack" was a little annoying	yes	nope
147	0-5 minutes	slow movie updates	yes	no
152	0-5 minutes	no	yes	No response
157	5-10 minutes	no	yes	the security situations seemed a little unrealistic (don't cut and paste the URL?)
162	0-5 minutes	I was unsure whether you could register and participate from more than one computer	yes	No response
167	0-5 minutes	No.	yes	No response
172	5-10 minutes	The movie rankings were sometimes delayed.	yes	No response
177	0-5 minutes	No response	yes	No response
182	5-10 minutes	remembering to sign in	yes	No response
187	0-5 minutes	No	no	No response
192	5-10 minutes	no	no	No response
197	5-10 minutes	no	yes	no

Group 2 (email with warnings, forwarding attack): General questions/feedback

User #	**Average length of each visit**	**Anything annoying or difficult?**	**Engaging or interesting?**	**General comments**
202	0-5 minutes	Having to set up a paypal account and the ucb movie prediction account. Also, I did not like that the movies to choose from were the same throughout the whole experiment.	no	I think the fake reason for the experiment was too obvious given what we were doing. It might have been better to be more vague or misdirecting there, so there is no chance people think there is a different reason for the experiment.
207	5-10 minutes	No	yes	No response
212	5-10 minutes	Nope, not especially	yes	Tricky tricky.
217	No response	No response	No response	No response
222	5-10 minutes	No, not really. Even the whole ”register this computer” thing wasn’t too bad.	yes	Well done! I love movies so I was completely oblivious to the ulterior motives of the study.
227	5-10 minutes	Not at all	yes	The inclusion of movies made it more appealing for me
232	0-5 minutes	no	yes	No response
237	5-10 minutes	no	yes	no
242	No response	No response	No response	No response
247	5-10 minutes	Registering each computer.	no	No response
252	0-5 minutes	constant timeouts (both my computers are relatively secured from other users besides me)	yes	I study social psychology and this study fooled me pretty well. Great job, guys!
257	0-5 minutes	not at all	yes	Great turn-around purpose of the study. Very intriguing.
267	5-10 minutes	It ask me to register a few times. I don’t know if it is because I didn’t read the instructions or if it was because of an error.	yes	Predicting movies was kinda fun. It’s like gambling without losing money.
272	0-5 minutes	no	yes	no

Group 2 (email with warnings, forwarding attack): General questions/feedback

User #	Average length of each visit	Anything annoying or difficult?	Engaging or interesting?	General comments
277	5-10 minutes	Well I don't feel like I understand what the purpose was of the 'movie predictions' bit of this study...was it related to it at all or was it all fake and it was just a security breach simulation via internet? I wasn't expecting this at all, really.	no	I feel more lost and confused about what happened in this study than engaged...that debriefing was way too long and inundated with strange information...maybe I need to read it over more slowly but I think this sudden change in experimenting needs to be better illuminated. Plus, not that many people are familiar with internet hacking and how to detect it so I suspect a lot more people in this study are even more lost than I am about what this study was actually about.
282	0-5 minutes	No	yes	No response

Group 3 (email without warnings, forwarding attack): Demographics

User #	Gender	Age	Student status or occupation	Details	OS	Primary browser	Web use/week (hrs)	Financial transactions done online	Experience doing financial transactions online
74	Female	18-21	Undergraduate	Humanities	Windows	Internet Explorer	20+	Banking, Shopping, Auctions	> 2 years
79	Female	18-21	Undergraduate	Natural sciences	Windows	Firefox	10-20	Banking, Auctions, PayPal	6–12 months
84	Female	22-25	Undergraduate	Economics or business	Windows	Firefox	20+	Banking, Investing, Shopping	> 2 years
89	Female	18-21	Undergraduate	Economics or business	Windows	Firefox	10-20	Banking, Shopping, Auctions, PayPal	> 2 years
94	Male	18-21	Undergraduate	Engineering	Mac OS	Safari	5-10	Banking, Shopping	> 2 years
99	Female	22-25	staff	No response	Windows	Firefox	20+	Banking, Shopping, Auctions, PayPal	> 2 years
104	Male	18-21	Undergraduate	Economics or business	Windows	Firefox	10-20	Banking, Shopping, Auctions, PayPal	> 2 years
109	Female	22-25	Undergraduate	Humanities	Windows	Internet Explorer	20+	Banking	Never
114	Male	18-21	Undergraduate	Natural sciences	Windows	Firefox	20+	Banking, Shopping, PayPal	> 2 years
119	Male	18-21	Undergraduate	Humanities	Mac OS	Firefox	20+	Banking, Shopping, Auctions, PayPal	1–2 years
134	Female	26-30	Graduate	Social sciences	Mac OS	Firefox	5-10	Banking, Shopping, Auctions, PayPal	> 2 years
139	Female	18-21	Undergraduate	Natural sciences	Windows	Internet Explorer	10-20	Banking, Shopping, PayPal	Never
149	Female	22-25	Graduate	Optometry	Windows	Internet Explorer	20+	Banking, Shopping	6–12 months

Group 3 (email without warnings, forwarding attack): Demographics

User #	Gender	Age	Student status or occupation	Details	OS	Primary browser	Web use/week (hrs)	Financial transactions done online	Experience doing financial transactions online
159	Male	18-21	Undergraduate	Engineering	Windows	Firefox	10-20	Banking, Shopping, Auctions, PayPal	> 2 years
164	Female	18-21	Undergraduate	Architecture	Windows	Firefox	10-20	Banking, Shopping	> 2 years
169	Male	18-21	Undergraduate	Engineering	Windows	Firefox	10-20	Banking, PayPal	1–2 years
174	Female	18-21	Undergraduate	Humanities	Mac OS	Safari	10-20	Banking, Investing, Shopping, Auctions, PayPal	6–12 months
179	Female	18-21	Undergraduate	Natural sciences	Windows	Firefox	10-20	Banking, Shopping, PayPal	1–2 years
184	Female	18-21	Undergraduate	Economics or business	Windows	Internet Explorer	10-20	Banking, PayPal	< 6 months
189	Female	18-21	Undergraduate	Natural sciences	Mac OS	Firefox	10-20	Banking, Shopping	> 2 years
194	Male	18-21	Undergraduate	Natural sciences	Windows	Firefox	20+	Banking, Shopping, Auctions, PayPal	> 2 years
199	Female	22-25	Undergraduate	Double: Biology AND Theater	Mac OS	Firefox	10-20	Banking, Shopping	1–2 years
204	Male	18-21	Undergraduate	Engineering	Mac OS	Internet Explorer	20+	Banking, Investing, PayPal	> 2 years
209	Female	18-21	Undergraduate	Natural sciences	Windows	Firefox	5-10	Auctions, PayPal	6–12 months
214	Male	18-21	Undergraduate	Social sciences	Mac OS	Safari	10-20	Banking, Shopping	1–2 years
219	Male	18-21	Undergraduate	Social sciences	Windows	Firefox	20+	Banking, Shopping, PayPal	1–2 years
224	Female	18-21	Undergraduate	Economics or business	Windows	Firefox	10-20	Banking, Shopping	> 2 years
234	Female	18-21	Undergraduate	biology	Windows	Firefox	20+	Banking, Shopping, Auctions, PayPal	< 6 months

Group 3 (email without warnings, forwarding attack): Demographics

User #	Gender	Age	Student status or occupation	Details	OS	Primary browser	Web use/week (hrs)	Financial transactions done online	Experience doing financial transactions online
239	Male	18-21	Undergraduate	Economics or business	Mac OS	Safari	10-20	Banking, Investing, Auctions, PayPal	1–2 years
244	Female	18-21	Undergraduate	Natural sciences	Mac OS	Firefox	20+	Banking, Shopping	> 2 years
249	Female	18-21	Undergraduate	Social sciences	Windows	Firefox	10-20	Banking, Shopping, Auctions, PayPal	> 2 years
254	Male	18-21	Undergraduate	Engineering	Windows	Firefox	20+	Banking, Shopping, Auctions, PayPal	> 2 years
262	Female	18-21	Undergraduate	Humanities	Mac OS	Flock	20+	Shopping, PayPal	1–2 years
263	Female	18-21	Undergraduate	Social sciences	Windows	Firefox	20+	Shopping	< 6 months
264	Male	22-25	Graduate	Engineering	Windows	Firefox	20+	Banking, Investing, Shopping, Auctions, PayPal	> 2 years
266	Male	18-21	Undergraduate	Natural sciences	Windows	Firefox	0-5	Banking, Shopping	> 2 years
269	Female	22-25	Undergraduate	Economics or business	Windows	Firefox	10-20	Banking, Shopping, Auctions, PayPal	1–2 years
274	Female	18-21	Undergraduate	Humanities	Mac OS	Firefox	20+	School, Banking, Shopping, PayPal	1–2 years
279	Male	18-21	Undergraduate	Engineering	Windows	Firefox	10-20	Shopping	> 2 years

Group 3 (email without warnings, forwarding attack): Web security attitudes

			How often & thoroughly user applies precautions when logging into:					
User #	**Biggest security concerns while browsing the Web**	**Precautions taken when logging into a Web site**	**Banking**	**Paypal**	**Web email**	**Shopping**	**Social net-working**	**Study site**
74	That my credit card information will be stolen, that someone will hack into an acount of mine and figure out my password, or that I will get a virus on my computer	Nothing really. I only have accounts at well-established and secure sites like ebay.com.	Always	Always	Always	Always	Always	Rarely
79	Someone will be able to log into my accounts	Create complicated passwords Only access sites from my private computer	Always	Always	Rarely	Rarely	Rarely	Rarely
84	My credit card information getting transferred/identity theft and getting viruses.	I limit the types of sites I look at, generally keep it to those I trust. I rarely ever download anything.	Always	Sometimes	Rarely	Usually	Sometimes	Sometimes
89	Not many	I don't log on to any sites that would compromise my personal information.	Sometimes	Sometimes	Rarely	Sometimes	Usually	Rarely
94	Identity theft, viruses, spyware	I trust the security of my web browser.	Always	Always	Always	Always	Always	Always
99	Password security, credit card numbers, having someone else use a service I am logged into	Read the privacy policy, check the web address, check what information is requested	Usually	Usually	Sometimes	Always	Sometimes	Rarely
104	viruses, hackers, ad-aware	looking at the web address to see if its a secure "locked" site.	Usually	Usually	Sometimes	Usually	Rarely	Sometimes
109	that someone will steal my information or be able to access my personal info	??	Rarely	Rarely	Rarely	Rarely	Rarely	Rarely

Group 3 (email without warnings, forwarding attack): Web security attitudes

			How often & thoroughly user applies precautions when logging into:					
User #	**Biggest security concerns while browsing the Web**	**Precautions taken when logging into a Web site**	**Banking**	**Paypal**	**Web email**	**Shopping**	**Social networking**	**Study site**
114	Identity theft Credit card number theft	I don't take many precautions, but if it's an important site, I won't save the password.	Always	Always	Rarely	Sometimes	Rarely	Rarely
119	Redirections due to packet interception.	I briefly check to see if I have a secure connection when doing online banking. I also make sure to change my passwords every month or so.	Always	Always	Rarely	Sometimes	Rarely	Rarely
134	Someone else gaining access to my credit card information.	I do not follow links from email to get to financial websites such as banks, paypal, ebay, etc. I only log in to such websites from the homepages that I search for myself.	Usually	Sometimes	Sometimes	Sometimes	Rarely	Rarely
139	giving my credit card information when shopping	No response	Always	Always	Always	Always	Always	Always
149	1. Someone is able to hack into my computer through the websites I'm using 2. Access of personal information on banking sites 3. Viruses	1. If the security certificate is invalid my anti-virus catches it and I usually don't continue onto the website 2. I don't save my log-in information on public computers 3. I disable pop-ups	Always	Always	Always	Always	Always	Always
159	People stealing my passwords.	I never save passwords, and I always clear my cache, cookies, and temporary internet files when I close my browser.	Always	Always	Always	Rarely	Rarely	Rarely

Group 3 (email without warnings, forwarding attack): Web security attitudes

			How often & thoroughly user applies precautions when logging into:					
User #	**Biggest security concerns while browsing the Web**	**Precautions taken when logging into a Web site**	**Banking**	**Paypal**	**Web email**	**Shopping**	**Social networking**	**Study site**
164	1. hacked account 2. forgotten password 3. password that does not work	I make sure there is no personal information I may be targeted with, such as my SSN.	Always	Usually	Rarely	Always	Rarely	Rarely
169	identity theif	none	Sometimes	Sometimes	Sometimes	Sometimes	Sometimes	Sometimes
174	having my private information stolen.	i do not give them any personal information unless i think they're legit/are well-known like ebay, amazon, yahoo, etc.	Always	Always	Always	Always	Always	Always
179	People finding my password to logins People finding my IP address People hacking to bank account	Don't really take precaution. Only do money-related or identity-related work online with credible companies/organizations/institutions.	Rarely	Rarely	Rarely	Rarely	Rarely	Rarely
184	Viruses, spyware, and identity theft.	I try to avoid giving out personal information or having to register an email address.	Rarely	Rarely	Rarely	Always	Sometimes	Rarely
189	I dislike coming across trashy websites/spam when I'm searching or browsing normal websites. I've heard of fake Bank of America login sites which are alarming, but I've never been scammed personally.	I only sign in to my online banking and credit card accounts from my home computer.	Always	Usually	Rarely	Usually	Sometimes	Always
194	getting my information stolen	check for SSL encryption when giving my CC information	Don't use	Don't use	Rarely	Always	Rarely	Rarely

Group 3 (email without warnings, forwarding attack): Web security attitudes

			How often & thoroughly user applies precautions when logging into:					
User #	Biggest security concerns while browsing the Web	Precautions taken when logging into a Web site	Banking	Paypal	Web email	Shopping	Social networking	Study site
199	someone getting into my email or bank account online	i never type my social security number when online. i rarely give out several pieces of personal information to one site (ie mothers maiden name, credit card number, home address).	Always	Always	Always	Always	Usually	Rarely
204	Identity Theft, security of the website, and quality/validity of the website	Make sure it looks like a reliable website and check to see if anything looks wrong.	Sometimes	Rarely	Rarely	Usually	Rarely	Rarely
209	People stealing debit/credit card info	I dont log into porn sites	Always	Always	Don't use	Always	Always	Always
214	Someone stealing my passwords to secure important information, like my social security number or financial information.	I don't take any.	Always	Always	Always	Always	Always	Always
219	Viruses and people breaking into my system	I try to see if a site is legitimate	Rarely	Rarely	Rarely	Rarely	Rarely	Rarely
224	someone stealing my credit card number or identity	i look at the privacy policy and look to see if there is an image of a lock with the url. i also make sure the url is legitimate	Always	Don't use	Sometimes	Always	Sometimes	Rarely
234	fraud, keylogger	see if they save my info or not	Always	Usually	Usually	Always	Usually	Usually
239	No response	No response	No response	No response	No response	No response	No response	No response

Group 3 (email without warnings, forwarding attack): Web security attitudes

			How often & thoroughly user applies precautions when logging into:					
User #	**Biggest security concerns while browsing the Web**	**Precautions taken when logging into a Web site**	**Banking**	**Paypal**	**Web email**	**Shopping**	**Social networking**	**Study site**
244	Viruses	Never open something that I am unsure of, and I only put in info on an https site	Sometimes	Usually	Sometimes	Rarely	Sometimes	Rarely
249	No response	No response	Rarely	Rarely	Rarely	Sometimes	Rarely	Rarely
254	security of location being used to connect malicious websites	Only log in to certain websites from secure locations. Only buy or give personal information to websites that I am reasonably confident are trustworthy.	Always	Always	Sometimes	Always	Rarely	Rarely
262	My biggest concern when browsing the web is that I'm going to accidentally push a button/link that could negatively affect me/give me a virus.	I don't really take any precautions; I just don't log into anything I'm not familiar with.	Always	Usually	Usually	Always	Sometimes	Usually
263	Identity theft	always sign out	Always	Sometimes	Rarely	Usually	Rarely	Always
264	No response	No response	No response	No response	No response	No response	No response	No response
266	Viruses, identity theft	If it looks shady, close it.	Usually	Usually	Usually	Sometimes	Sometimes	Sometimes
269	No response	No response	Rarely	Rarely	Rarely	Rarely	Rarely	Rarely
274	Phishing, viruses, Pop-ups and unapproved downloads	Limiting use/input of SSN or other sensitive information, making sure to turn off pop-up blocker, (normally but for only certain websites) checking the URL in the browser before proceeding to login	Usually	Always	Rarely	Sometimes	Always	Rarely

Group 3 (email without warnings, forwarding attack): Web security attitudes

			How often & thoroughly user applies precautions when logging into:					
User #	Biggest security concerns while browsing the Web	Precautions taken when logging into a Web site	Banking	Paypal	Web email	Shopping	Social networking	Study site
279	Viruses, Malware, Spam	Check that it is a legitimate site sponsored by a legitimate company.	Always	Always	Always	Always	Always	Always

Group 3 (email without warnings, forwarding attack): Study experiences

User #	Fell for attack?	How attack ended	Saw something suspicious/dangerous?	If yes, reaction?	Remembered seeing warning? If yes, effect on decisions?	Followed attack instructions? Why or why not? (Question 18)
74	no	timeout	no	N/A	yes: It did make me feel a little unsecure and just made me decline to register another one of my friend's personal computers. I decided to just wait until I got home and use my computer that was already registered so I would not have to deal with whatever the UCB movie predictions was saying in the email.	I did not because it was too much of a hassle so I just thought forget it I will just wait until I get home and use my own computer that was already registered and will log in that way.
79	yes	forwarded url	no	N/A	no	I followed the instructions because I thought it contained genuine directions from the site.
84	no	followed html url	no	N/A	yes: It didn't.	I didn't notice that it said not to click on it, I clicked.
89	no	followed html url	no	N/A	no	It's currently 2:20am and I just got back from 5 hours of dance practice. Honestly, I didn't even see the instructions!!! How scary!
94	no	followed html url + timeout + forwarded invalid emails	no	N/A	no	I wasn't able to log in to continue making movie predictions and I wanted to be able to continue doing so, and it seemed like this was the only way to do it.

Group 3 (email without warnings, forwarding attack): Study experiences

User #	Fell for attack?	How attack ended	Saw something suspicious/dangerous?	If yes, reaction?	Remembered seeing warning? If yes, effect on decisions?	Followed attack instructions? Why or why not? (Question 18)
99	yes	forwarded url	yes: The page saying that there was a problem with the machine registration and that I needed to forward a copy of the e-mail I was sent.	I naively assumed that it was a strange/dubious choice on the part of the designers and forwarded the e-mail because I wanted my money. Boy do I have egg on my face!	no	I did, because I wasn't thinking very hard about it.
104	no	timeout	no	N/A	yes: It did not	I figured I would see if the site would be on track later. I did not see the email to do it the first time and the second time I was lazy.
109	no	timeout	no	N/A	yes: i kind of remember that... but i wasnt sure - an di figured it wouldnt ask me to do it if it wasn't ok...	i forwarded it because it told me to... but said not to click on the link...
114	yes	forwarded url	no	N/A	no	I followed the above instructions, even though I thought they were a little weird. I checked the website and it looked official, so I thought it was legitimate.
119	no	timeout	no	N/A	yes: It didn't, I went ahead and sent the forwarding email because I am fairly gullible and I wasn't taking the ucbpredictions site terribly seriously	I went ahead and forwarded the email to the aforementioned website because I was in a rush to be able to log in again so I could make more money.

Group 3 (email without warnings, forwarding attack): Study experiences

User #	Fell for attack?	How attack ended	Saw something suspicious/dangerous?	If yes, reaction?	Remembered seeing warning? If yes, effect on decisions?	Followed attack instructions? Why or why not? (Question 18)
134	no	followed html url	no	N/A	yes: It didn't affect me after my initial login.	I did not follow the instructions because I did not initially read it carefully enough. I saw the arrow and clicked without reading the text below.
139	yes	forwarded url	no	N/A	yes: I followed the instructions when I read them. But with further instructions that conflicted with these warnings, I followed the most recent instructions to forward it to the given email address.	I followed the isntructions because there seemed to be no way of logging into the website without forwarding and registering the computer. Also, those were the most recent instructions given, so i followed them
149	yes	forwarded url	no	N/A	yes: the first time i saw it i clicked on it the second time i forwarded it (i forgot)	I thought that since it was coming from the direct site that it would be okay to follow the instructions
159	yes	forwarded url	no	N/A	no	I didn't think about it. It didn't seem like a security issue. Also, I didn't consider the security of this account to be vital. In other words, if my account information were to be found by an intruder, I wouldn't care that much.
164	yes	forwarded url	no	N/A	no	I forwarded it because it seemed as though it was part of the study, and I also wanted to help fix the problem of the email registration system.
169	no	timeout	no	N/A	no	I followed it, because it said so
174	no	followed html url	no	N/A	no	I did not follow the instructions because the first thing I saw was "Click on this secure link to register your computer." So I did...

Group 3 (email without warnings, forwarding attack): Study experiences

User #	Fell for attack?	How attack ended	Saw something suspicious/dangerous?	If yes, reaction?	Remembered seeing warning? If yes, effect on decisions?	Followed attack instructions? Why or why not? (Question 18)
179	yes	forwarded url	no	N/A	no	I followed the instructions because the warning was in CAPS.
184	no	followed html url	no	N/A	no	I was attracted by the colored, capitalized font and skipped ahead to click on the link. That is the part of the page that drew my attention.
189	no	followed html url	no	N/A	yes: It didn't really affect my decisions about interacting with the website, I thought it was kind of a hassle to always have to check the website from only a registered computer.	I must have glossed over the instructions to not click the registration email link, I didn't think there would be two opposing instructions so I just went with the one that was more obvious.
194	no	followed html url	no	y	no	I didn't read it, instead I assumed it was like all other sites that required you to click on the link.

Group 3 (email without warnings, forwarding attack): Study experiences

User #	Fell for attack?	How attack ended	Saw something suspicious/dangerous?	If yes, reaction?	Remembered seeing warning? If yes, effect on decisions?	Followed attack instructions? Why or why not? (Question 18)
199	yes	forwarded url	no	N/A	yes: Yes! i did exactly what it said the day that i received that message and then forgot about it by the time the simulated scam/hack was pulled on me. I actually didn't think it had anything to do with the security of my money/identity. I thought it was necessary simply to make the study work the correct way and was for your benefit, not my own. I guess the word "safe" made me wonder a bit, but since this study was through a public university and through a service (x-lab) that I've used before I felt completely at ease about my security and I didn't even consider it being compromised.	I did. I had no reason to doubt its validity and nothing seemed to be at stake. If this had appeared on a site that I'm familiar with that I need to keep secure (ie my email or bank account) red flags would have gone off in my head for sure. Like I said earlier, I trust this study. Also, I'm still not too proficient at computers, and have a Mac that often has to go through complicated procedures to do simple tasks online, so this kind of prompt doesn't seem to uncommon. Lastly, the fact that it looked just like other messages from the study AND that it sent and email to my personal address that I gave to the study made it seem valid.
204	no	followed html url	no	N/A	yes: It did not affect my decisions much, but it did help the validity of the survey.	I wanted to make sure everything went well and that the survey would work for me.
209	yes	forwarded url	no	N/A	no	I have been drinking, and was only attempting to follow instructions rather than scrutinize the validity of the website.

Group 3 (email without warnings, forwarding attack): Study experiences

User #	Fell for attack?	How attack ended	Saw something suspicious/dangerous?	If yes, reaction?	Remembered seeing warning? If yes, effect on decisions?	Followed attack instructions? Why or why not? (Question 18)
214	yes	forwarded url	yes: The error message at the end, which required me to forward the registration email to the support@ucbmoviepredictions.com address.	I didn't do anything, because I only realized how you got me now.	no	I did, because I don't tend to think about security issues when I'm on the web, and because I got it while I was in your site.
219	no	followed plain url	no	N/A	no	I didn't read carefully
224	no	followed plain url + forwarded invalid emails	no	N/A	yes: by the time i was told to forward the email, i had forgotten about the warning above.	i thought the notice was from the moviepredictions website and that there really was a problem...
234	no	followed html url	no	N/A	no	i clicked on it because i only ready the blue part. i guess i dindt' see the red warning
239	no	followed plain url	No response	No response	yes	No response
244	no	followed html url	no	N/A	no	I didn't follow the directions because it sounded sketchy and I wanted to see what happened
249	no	followed html url	no	N/A	yes	i didn't do anything because I didn't think anything of it.

Group 3 (email without warnings, forwarding attack): Study experiences

User #	Fell for attack?	How attack ended	Saw something suspicious/dangerous?	If yes, reaction?	Remembered seeing warning? If yes, effect on decisions?	Followed attack instructions? Why or why not? (Question 18)
254	yes	forwarded url	yes: I was told to send an email which a link in it and not to click the link.	I reacting by sending the email.	no	I followed the instructions. If this was a banking website or something else important I definitely would have thought twice. However, because Movie Predictions has no information that would put me at risk there was no reason to assume that something odd was going on. Just because you can put money into my Paypal account doesn't mean you can take it out.
262	no	followed plain url	no	N/A	yes: It made me a double take; I didn't necessarily let it concern me (though I probably should have, in retrospect)	I chose not to follow the instructions because I thought I had done something incorrectly. I wasn't sure what was going on, so I was opening up old e-mails in my deleted folder, etc.
263	no	timeout	no	N/A	no	I did not read it carefully so I didn't follow the instructions.
264	no	followed html url	No response	No response	no	I didn't follow the instructions because I didn't pay attention to this page (I just followed the usual procedures to register my computer).
266	no	followed html url	no	N/A	yes: I followed the instructions to not forward/copy the email	I didn't read it carefully, and instinctively clicked on the link in the email. It's kinda late and I wasn't paying attn
269	no	followed html url	no	N/A	no	I don't remember seeing this page.

Group 3 (email without warnings, forwarding attack): Study experiences

User #	Fell for attack?	How attack ended	Saw something suspicious/dangerous?	If yes, reaction?	Remembered seeing warning? If yes, effect on decisions?	Followed attack instructions? Why or why not? (Question 18)
274	no	followed html url	yes: It didn't look suspicious at the time, but I kept having to register my computer. I thought it was just a precaution or a bug in the programming	I didn't think anything of it so I proceeded as directed	no	I guess the page always had the same format and, I am a Berkeley student with too much to read all the time. So, I assumed it was more of the same and that, yet again, I had to register my computer. Oops.
279	no	followed plain url	no	N/A	no	Not used to forwarding an email to register an account.

Group 3 (email without warnings, forwarding attack): Registration attitudes

			Security of:		Convenience of:	
User #	**Used email registration before? If yes, where?**	**Benefits of email registration**	**Passwords + no registration**	**Passwords + email for registration**	**Passwords + no registration**	**Passwords + email for registration**
74	no	You have to log in to your email account and click on the link for you to create an account. I think it has the security benefit that a potential hacker does not know your email password.	Somewhat secure	Fairly secure	I hardly noticed it	I could get used to it
79	yes: singlemuslim.com	I don't have any idea.	Fairly secure	Very secure	I hardly noticed it	I could get used to it
84	yes: Paypal	I think it makes sure that you are who you say you are to an extent, but I think a lot of people fake email addresses so it's really not that secure at all.	Somewhat secure	Fairly secure	I hardly noticed it	Hard or slightly annoying
89	no	No response	I don't know	Fairly secure	I could get used to it	I could get used to it
94	yes: Paypal, etc.	It adds another layer of security - you have to have an active email address. However, it's not a huge benefit because it's easy enough to make and register to a webmail account.	Somewhat secure	Fairly secure	I could get used to it	I hardly noticed it
99	yes: Most sites requiring registration.	No response	Fairly secure	Fairly secure	I hardly noticed it	I hardly noticed it
104	yes: email, facebook	only people you email and know you know your email address.	Fairly secure	Fairly secure	I hardly noticed it	I could get used to it
109	yes: dont know...	...	Somewhat secure	Very secure	I hardly noticed it	I hardly noticed it

Group 3 (email without warnings, forwarding attack): Registration attitudes

			Security of:		**Convenience of:**	
User #	**Used email registration before? If yes, where?**	**Benefits of email registration**	**Passwords + no registration**	**Passwords + email for registration**	**Passwords + no registration**	**Passwords + email for registration**
114	yes: Many, including Facebook, woot.com, Paypal...too many to name.	It makes sure that the email you're submitting actually works and that you're not just starting some kind of a fake account.	Not secure at all	Fairly secure	I hardly noticed it	I hardly noticed it
119	no	The benefit I see in email registration is to be able to double verify that the initial account creator is the one in control of the websites account, i.e. for password retrieval.	Somewhat secure	Fairly secure	I hardly noticed it	I hardly noticed it
134	yes: Facebook, Amazon, Ebay	I thought that it prevented other people (who do not have access to your email account) from changing account settings, changing the email address associated, etc. I don't think it has any security benefits - someone could take over your account by gaining access to your email account.	Fairly secure	Very secure	I hardly noticed it	I hardly noticed it
139	no	No response	Fairly secure	Somewhat secure	I hardly noticed it	I could get used to it
149	yes: evite.com facebook.com	it makes sure that the person who signed up for the account should be the only person who has the power to register that account, to prevent people from making fake accounts under their name and email address	Somewhat secure	Fairly secure	I hardly noticed it	I hardly noticed it

Group 3 (email without warnings, forwarding attack): Registration attitudes

			Security of:		Convenience of:	
User #	Used email registration before? If yes, where?	Benefits of email registration	Passwords + no registration	Passwords + email for registration	Passwords + no registration	Passwords + email for registration
159	yes: Like everything.	Email registration works ONLLY when the security of one's email is maintained. This ensures that if anything happens to any accounts, the person is contacted via email, and it is for sure that person, not an imposter.	Somewhat secure	Fairly secure	I could get used to it	Hard or slightly annoying
164	yes: Bank of America, yahoo email, other email sites, amazon, ebay, etc	I think it works by only contacting whoever first was interested in the site, so that only they will be contacted. It works to me because if a password is lost, it will only be sent to that person, and not another email that a hacker might put in to try to get the password.	Not secure at all	Fairly secure	I don't know	I could get used to it
169	yes: dont remember	No response	Somewhat secure	Very secure	Hard or slightly annoying	Hard or slightly annoying
174	yes: Bank of America, I believe.	your IP address will be taken down and you can only sign in when the site registers your IP address. it would be similar to having a fingerprint to identify a user with.	Fairly secure	Very secure	I hardly noticed it	I could get used to it
179	yes: publications	Not sure	Not secure at all	Fairly secure	I hardly noticed it	I could get used to it
184	yes: Facebook, Paypal	It has the benefit of securing your email address and yours and possibly preventing identity theft.	I don't know	Very secure	I don't know	Hard or slightly annoying

Group 3 (email without warnings, forwarding attack): Registration attitudes

			Security of:		Convenience of:	
User #	**Used email registration before? If yes, where?**	**Benefits of email registration**	**Passwords + no registration**	**Passwords + email for registration**	**Passwords + no registration**	**Passwords + email for registration**
189	yes: Banking websites, facebook websites, all kinds of websites	I think it gives the website owner a way of contacting the email user to legitimize the account. I'm not sure what security benefits it has for the user besides the convenience of password/username recovery sent to your email	Somewhat secure	Fairly secure	I could get used to it	I hardly noticed it
194	yes: forums and certain promotions	so you can't just create an account and cant commit malicious activities	Somewhat secure	Fairly secure	I hardly noticed it	Hard or slightly annoying
199	yes: Too many to count... Registration for email lists (dance clubs, nonprofits). I'm sorry but I can't recall specifics. It seems like an increasing number of sites are using this type of registration.	I have no idea how it works. I always thought it was good for the company because you can't give a fake email address to avoid spam. I also keep very tight reigns on my email password so it feels safe if I must go there to register because nobody else would ever be able to.	Fairly secure	Fairly secure	I hardly noticed it	I hardly noticed it
204	yes: Almost all websites which need me to sign in at another time - such as forums and shopping websites.	It confirms that the email the person put in when registering is the same person - and if it's someone different, that person can fix the problem.	Not secure at all	Fairly secure	I hardly noticed it	I hardly noticed it
209	yes: Lots of them	it is easy to rememnber	Somewhat secure	Somewhat secure	I hardly noticed it	I hardly noticed it

Group 3 (email without warnings, forwarding attack): Registration attitudes

			Security of:		Convenience of:	
User #	Used email registration before? If yes, where?	Benefits of email registration	Passwords + no registration	Passwords + email for registration	Passwords + no registration	Passwords + email for registration
214	yes: Do not remember. Many. Facebook.	They make sure that the email you are providing is valid.	Very secure	Very secure	I hardly noticed it	I hardly noticed it
219	no: various	makes sure the person is the correct person	Somewhat secure	Somewhat secure	I could get used to it	I could get used to it
224	yes: don't remember, quite a few though	i think they send me an email and then i have to use a link from the email. it verifies that the email address is actually me	Fairly secure	Fairly secure	I hardly noticed it	I could get used to it
234	no	it sends confirmations to your email so when peopel do fraud it, you can catcwh it in your own email.	Not secure at all	Fairly secure	I hardly noticed it	I could get used to it
239	no	No response	No response	No response	No response	No response
244	yes: Most	I don't know	I don't know	I don't know	I hardly noticed it	Hard or slightly annoying
249	yes	No response	I don't know	I don't know	I don't know	I don't know

Group 3 (email without warnings, forwarding attack): Registration attitudes

			Security of:		Convenience of:	
User #	Used email registration before? If yes, where?	Benefits of email registration	Passwords + no registration	Passwords + email for registration	Passwords + no registration	Passwords + email for registration
254	yes: virtually any website that requires you to sign up	I don't think just registering by email has any particular benefits if you can just register with any old email address. But, if you have to use a cal one it ensures that you are a student and allows another barrier if say you need to reset your password. Note: The following question is hard to answer because I would judge security on many factors and whether or not they have registration is only a small factor. If amazon didn't require registration I would still trust them. If a random site required registration but looked sketchy I still wouldn't trust it.	I don't know	I don't know	I hardly noticed it	I hardly noticed it
262	yes: Livejournal, etc.	I just think it's a better way of maintaining validity of a person.	Somewhat secure	Very secure	I hardly noticed it	I could get used to it
263	no	I don't really know what it is.	Somewhat secure	Fairly secure	I hardly noticed it	Hard or slightly annoying
264	yes: Forums	No response	No response	No response	No response	No response
266	no: Don't remember but a lot	Only seems to have security benefits for the site, not the user (prevents bots from registering)	Fairly secure	Fairly secure	I hardly noticed it	I could get used to it
269	yes	No response	No response	Fairly secure	I could get used to it	I could get used to it

Group 3 (email without warnings, forwarding attack): Registration attitudes

			Security of:		Convenience of:	
User #	**Used email registration before? If yes, where?**	**Benefits of email registration**	**Passwords + no registration**	**Passwords + email for registration**	**Passwords + no registration**	**Passwords + email for registration**
274	yes: Myspace, Facebook, Shopping sites and pretty much any site where I'd need an account	An email with a unique and secure link is sent to my inbox once I register for a website. This way, they can verify that my email address is real and that they have my correct information. For me, there is a loss of security that I just have to accept and base my decisions regarding disclosure on the given website's trustworthiness.	Somewhat secure	Fairly secure	I hardly noticed it	I could get used to it
279	yes: Forums and online merchants.	Prevents the store/forum from being spammed. I don't believe it has any real security benefits, just a way for the company to attach an account to a real person.	Somewhat secure	Somewhat secure	I hardly noticed it	I hardly noticed it

Group 3 (email without warnings, forwarding attack): General questions/feedback

User #	Average length of each visit	Anything annoying or difficult?	Engaging or interesting?	General comments
74	5-10 minutes	Just the fact that I could not log in on just any computer. Usually I am at the library until pretty late at night and it was annoying that I could not use the library computer because it was a ”public computer” to just quickly log into the UCB movie predictions website.	no	I thought the whole study was a little weird since there was so little information on the site on the different movies.
79	5-10 minutes	No	yes	No response
84	10-20 minutes	No response	yes	I think it would have been interested if it lasted a few days longer. I think just after a few days I started to get an idea of how people behave on weekends versus weekdays and how that would affect their movie-going behavior and I didn’t have a chance to test my theory.
89	5-10 minutes	Nope. It was pretty fun.	yes	No response
94	0-5 minutes	This little twist of events at the end is a bit confusing - I also have not yet made 7 predictions, and I am uncertain if I will still be compensated.	no	No response
99	0-5 minutes	No response	yes	No response
104	10-20 minutes	no rss feed	yes	No response
109	0-5 minutes	nope	yes	nope
114	5-10 minutes	Forgetting when movies debuted.	yes	Y’all duped me. Nice.
119	0-5 minutes	No, it was easy to use.	yes	None
134	0-5 minutes	No response	yes	No response
139	0-5 minutes	the previoous day’s predictions were not posted promptly.	yes	No response
149	5-10 minutes	no	yes	no
159	0-5 minutes	No.	no	No.
164	5-10 minutes	no.	yes	none.
169	0-5 minutes	No	yes	No response
174	5-10 minutes	No, it was simple and easy and well-explained in the beginning.	yes	Great study.
179	5-10 minutes	No	yes	No response

Group 3 (email without warnings, forwarding attack): General questions/feedback

User #	Average length of each visit	Anything annoying or difficult?	Engaging or interesting?	General comments
184	0-5 minutes	It was annoying that sometimes the previous day's movie results were not updated by the time I logged in to make another prediction the following day.	yes	I am surprised that I didn't follow directions in terms of forwarding the email.
189	5-10 minutes	Many times the daily gross wasn't posted so I would check a few times a day, but I could only do it from my computer.	yes	No response
194	0-5 minutes	No response	yes	No response
199	0-5 minutes	actually yeah. it was annoying and threw me off that i had to register my computer in the first place.	yes	tricky, tricky, tricky. but you got me so i guess that means that it's good you're doing this study, right? thanks!
204	0-5 minutes	No.	yes	It reminds me of the book called ”The Wisdom of Crowds”
209	0-5 minutes	No response	no	I dont even have TV, so the movie predictions were totally random
214	0-5 minutes	Nope.	yes	Fun!
219	0-5 minutes	registration only	no	nope
224	0-5 minutes	no	yes	No response
234	0-5 minutes	no	yes	it was fun! very realistic
239	No response	No response	No response	No response
244	0-5 minutes	No	yes	No response
249	0-5 minutes	No response	yes	No response
254	5-10 minutes	Not really. The ”error” happening at the same time as the exit survey confused me because I thought it was possible that something had gone wrong, rather than the survey being intentionally short and I was hesitant to take the exit survey because I assumed at the time that that would mess up your data if I didn't do all 7 guesses. But I suppose that is something you want intentionally there so there's no much you can do about it.	yes	I think it's pretty effective
262	0-5 minutes	Sometimes I find it annoying that I'm being asked an open-ended questions (I'd rather just have choices to make a decision about)	yes	No

Group 3 (email without warnings, forwarding attack): General questions/feedback

User #	Average length of each visit	Anything annoying or difficult?	Engaging or interesting?	General comments
263	0-5 minutes	Having to make a paypal account.	yes	No
264	No response	No response	No response	No response
266	0-5 minutes	We didn't get a chance to make as much money as I though we could? But I guess that was part of the surprise/deception.	no	Creative, got me.
269	10-20 minutes	No response	yes	No response
274	5-10 minutes	Being tricked is frustrating. Also, this study makes you guys seem condescending and overly pedantic	yes	It makes no sense for us not to trust a new link that sends us a registration email from the site with which we are registered. A ”fishy” web link would not have access to our email address unless the original site disclosed that information. Should we not trust websites linked to Berkeley?
279	0-5 minutes	No response	yes	No response

Group 4 (email with warnings, cut and paste attack): Demographics

User #	Gender	Age	Student status or occupation	Details	OS	Primary browser	Web use/week (hrs)	Financial transactions done online	Experience doing financial transactions online
75	Male	18-21	Undergraduate	Social sciences	Windows	Firefox	5-10	Banking, Shopping, Auctions, PayPal	> 2 years
80	Female	18-21	Undergraduate	Social sciences	Windows	Firefox	10-20	Banking, Shopping	> 2 years
85	Male	18-21	Undergraduate	Engineering	Windows	Opera	20+	Shopping, Auctions, PayPal	< 6 months
90	Male	18-21	Undergraduate	Natural sciences	Mac OS	Safari	20+	Investing, Shopping	> 2 years
95	Female	18-21	Undergraduate	Humanities	Windows	Internet Explorer	5-10	Banking, Shopping	> 2 years
100	Female	18-21	Undergraduate	Natural sciences	Windows	Firefox	20+	Banking, Shopping, Auctions, PayPal	1–2 years
105	Male	18-21	Undergraduate	Engineering	Windows	Firefox	10-20	Banking, Shopping, PayPal	6–12 months
110	Female	18-21	Undergraduate	Economics or business	Windows	Firefox	20+	Banking, Shopping, Auctions, PayPal	> 2 years
115	Female	26-30	Graduate	Economics or business	Windows	Internet Explorer	20+	Banking, Shopping, PayPal	> 2 years
120	Female	18-21	Undergraduate	Computer science	Windows	Firefox	20+	Banking, PayPal	1–2 years
125	Female	18-21	Undergraduate	Economics or business	Windows	Firefox	5-10	Banking	Never
135	Male	18-21	Undergraduate	Economics or business	Windows	Firefox	20+	Banking	Never
140	Female	18-21	Undergraduate	Natural sciences	Windows	Firefox	10-20	Banking, Shopping, Auctions	> 2 years
145	Male	22-25	Undergraduate	Social sciences	No response	No response	No response	No	Never
150	Female	18-21	Undergraduate	Social sciences	Mac OS	Safari	20+	Banking	1–2 years

Group 4 (email with warnings, cut and paste attack): Demographics

User #	Gender	Age	Student status or occupation	Details	OS	Primary browser	Web use/week (hrs)	Financial transactions done online	Experience doing financial transactions online
155	Female	22-25	Undergraduate	Natural sciences	Mac OS	Firefox	10-20	Banking, Shopping, PayPal	> 2 years
160	Female	18-21	Undergraduate	Social sciences	Mac OS	Safari	10-20	Banking, Shopping, Auctions, PayPal	< 6 months
165	Male	41-50	employee	No response	Windows	Firefox	20+	Banking, Investing, Shopping, Auctions, PayPal	> 2 years
170	Female	18-21	Undergraduate	Natural sciences	Windows	Firefox	20+	Banking, Shopping	> 2 years
175	Male	22-25	Undergraduate	architecture	Windows	Firefox	20+	Banking	> 2 years
180	Female	18-21	Undergraduate	Economics or business	Mac OS	Firefox	0-5	Banking, Shopping	1–2 years
185	Female	22-25	Undergraduate	Social sciences	Windows	Firefox	10-20	Banking, Shopping	> 2 years
190	Female	18-21	Undergraduate	Social sciences	Windows	Firefox	5-10	Banking, Auctions, PayPal	> 2 years
195	Female	18-21	Undergraduate	Natural sciences	Windows	Firefox	5-10	Banking	> 2 years
200	Female	18-21	Undergraduate	Economics or business	Windows	Safari	5-10	Banking, Shopping	< 6 months
205	Female	18-21	Undergraduate	Natural sciences	Windows	Firefox	5-10	Banking, Investing, Shopping	< 6 months
210	Female	18-21	Undergraduate	Social sciences	Windows	Firefox	20+	Banking, Shopping, Auctions, PayPal	1–2 years
215	Male	18-21	Undergraduate	Economics or business	Windows	Firefox	5-10	Banking, Shopping, PayPal	> 2 years
220	Female	18-21	Undergraduate	Natural sciences	Windows	Firefox	10-20	Shopping	< 6 months
225	Male	18-21	Undergraduate	Social sciences	Windows	Internet Explorer	5-10	Shopping, Auctions, PayPal	6–12 months

Group 4 (email with warnings, cut and paste attack): Demographics

User #	Gender	Age	Student status or occupation	Details	OS	Primary browser	Web use/week (hrs)	Financial transactions done online	Experience doing financial transactions online
230	Male	18-21	Undergraduate	Architecture	Windows	Firefox	10-20	Banking, Shopping, PayPal	1–2 years
235	Female	18-21	Undergraduate	Natural sciences	Mac OS	Firefox	10-20	Banking, Investing, Shopping, PayPal	6–12 months
240	Male	18-21	Undergraduate	Peace and Conflict Studies	Mac OS	Safari	5-10	none	Never
245	Female	18-21	Undergraduate	Natural sciences	Windows	Firefox	20+	Banking	Never
250	Female	18-21	Undergraduate	Natural sciences	Windows	Firefox	20+	Banking, Shopping, PayPal	> 2 years
255	Female	18-21	Undergraduate	Social sciences	Windows	Firefox	10-20	Shopping	6–12 months
260	Female	22-25	Undergraduate	Economics or business	Mac OS	Firefox	20+	amazon, Banking, Shopping	1–2 years
270	Male	22-25	Undergraduate	landscape architecture	Mac OS	Firefox	10-20	Shopping, Auctions, PayPal	> 2 years
275	Male	18-21	Undergraduate	Economics or business	Windows	Firefox	10-20	Banking, Investing, Shopping, PayPal	> 2 years
280	Male	26-30	Undergraduate	Economics or business	Windows	Internet Explorer	20+	Banking, Shopping, Auctions, PayPal	> 2 years

Group 4 (email with warnings, cut and paste attack): Web security attitudes

			How often & thoroughly user applies precautions when logging into:					
User #	**Biggest security concerns while browsing the Web**	**Precautions taken when logging into a Web site**	**Banking**	**Paypal**	**Web email**	**Shopping**	**Social networking**	**Study site**
75	Identity theft, credit card theft, people seeing what I am browsing	I make sure that the site is trustworthy and try not give too much personal info on iffy sites	Sometimes	Sometimes	Usually	Always	Always	Always
80	Having an account hacked into; private data viewed when using a public computer;	Just make sure to log-out every time. Also not using a very personal site (like my bank statement) on a public computer.	Always	Don't use	Always	Always	Sometimes	Usually
85	phishing unencrypted information	proper browser, checking for secure site	Usually	Usually	Usually	Usually	Usually	Usually
90	phishing, viruses	checking the URL	Always	Always	Always	Always	Always	Sometimes
95	That I am not getting the best resources because a search engine gives links preference over other links.	I don't really take precautions, but I also do not log into website I do not trust.	Always	Don't use	Always	Always	Always	Don't use
100	That others can see what I'm doing, expecially when i'm conducting financial transactions	Is it a legitimate website that's not asking me for private identity information when not neccesary	Always	Usually	Rarely	Always	Rarely	Rarely
105	viruses, popups, trojans	firewall, scanning my computer	Usually	Usually	Sometimes	Sometimes	Rarely	Sometimes
110	virus	dont open emails from unknown sources	Rarely	Sometimes	Always	Sometimes	Usually	Rarely
115	Hacking Viruses	No response	Rarely	Rarely	Rarely	Rarely	Rarely	Rarely
120	people hacking into my accounts and finding out my passwords for everything	I never save my password on computers	Always	Always	Always	Always	Usually	Usually
125	finding my bank information	making sure it's a secure site	Sometimes	Rarely	Rarely	Usually	Rarely	Rarely

Group 4 (email with warnings, cut and paste attack): Web security attitudes

			How often & thoroughly user applies precautions when logging into:					
User #	**Biggest security concerns while browsing the Web**	**Precautions taken when logging into a Web site**	**Banking**	**Paypal**	**Web email**	**Shopping**	**Social networking**	**Study site**
135	Identity Theft	Not giving out credit card or any other personal information unless it is a legitimate website	Always	Rarely	Rarely	Always	Rarely	Rarely
140	Identity theft, scams	for banking, I always make sure that my ”site key” is correct.	Always	Usually	Rarely	Usually	Rarely	Rarely
145	No response	No response	No response	No response	No response	No response	No response	No response
150	spam, virus, adware	make sure my passwords do not get stored	Always	Always	Always	Don’t use	Usually	Always
155	Loss of personal information (bank account & social security numbers), although as a student I really don’t know how attractive these would be to an identity thief. Also, I download the occasional mp3 from music blogs, so I guess I fear the recording industry.	I look and see if there’s a little padlock in the navigation bar. I also just don’t go to sketch websites.	Always	Always	Always	Always	Usually	Usually
160	1. people looking if from a unsecured wireless line. 2. The company misusing information.	none.	Sometimes	Rarely	Rarely	Rarely	Rarely	Rarely

Group 4 (email with warnings, cut and paste attack): Web security attitudes

			How often & thoroughly user applies precautions when logging into:					
User #	**Biggest security concerns while browsing the Web**	**Precautions taken when logging into a Web site**	**Banking**	**Paypal**	**Web email**	**Shopping**	**Social networking**	**Study site**
165	direct packet interception, password sniffers, malware masquerading as amusing java games, physical breach, mostly worried about stealth attacks that will not be noticed	’hard’ passwords, only use private machines, firewall, making sure the site has at least minimal encryption, monitoring of any online accounts. use the email address used for this account instead of my ’real’ email accounts	Always	Always	Always	Always	Don’t use	Always
170	identity theft	check security	Always	Always	Usually	Usually	Sometimes	Sometimes
175	Passwords, Identity Theft, SPAM	Avoid using ’Remember Me on this Site’ feature; Pop-up blocker	Always	Always	Usually	Always	Usually	Usually
180	credit card fraud	passwords	Always	Always	Always	Always	Always	Always
185	Someone stealing my personal and financial information.	-firewall -secure log in	Always	Always	Always	Always	Always	Always
190	trojans	On websites I use frequently and trust I take few precautions. I always have a firewall and my antivirus software on, though.	Usually	Usually	Usually	Usually	Usually	Usually
195	No response	No response	No response	No response	No response	No response	No response	No response
200	No response	No response	Usually	Always	Sometimes	Always	Usually	Sometimes
205	People hacking into my computer and obtaining my password. The leakage of my sensitive numbers (SSN, School ID, etc)	Bank of America has a secure site with extra password needed.	Usually	Don’t use	Rarely	Usually	Rarely	Rarely
210	Identity theft, viruses	Password manager	Always	Always	Always	Always	Sometimes	Rarely

Group 4 (email with warnings, cut and paste attack): Web security attitudes

			How often & thoroughly user applies precautions when logging into:					
User #	**Biggest security concerns while browsing the Web**	**Precautions taken when logging into a Web site**	**Banking**	**Paypal**	**Web email**	**Shopping**	**Social networking**	**Study site**
215	People stealing my identity leaving myself logged in double - paying	my passwords are slightly esoteric	Always	Always	Usually	Always	Rarely	Sometimes
220	Identity theft, spyware, viruses.	I make sure to see if there is a little lock at the bottom of the screen and I judge from the website if I think it is trustworthy.	Always	Usually	Sometimes	Usually	Sometimes	Rarely
225	Spyware and viruses. Giving out important information accidentally.	None unless it seems like an unreliable site. I avoid these websites.	Always	Sometimes	Usually	Sometimes	Sometimes	Sometimes
230	fishing, release of personal information, untrustworthy websites	only purchasing form major or reliable dealers	Don’t use	Usually	Usually	Always	Sometimes	Rarely
235	That someone may be able to take my identification and banking information.	For sites I go to less frequently, I request that the computer does not remember my password or never remembers. For sites I visit every day, my password is remembered.	Always	Usually	Rarely	Usually	Rarely	Sometimes
240	Identity fraud, viruses	none, just don’t give away vital information	Always	Usually	Sometimes	Always	Usually	Sometimes
245	I am worried that a third party may get access to my account without me even knowing it. I am worried that important information that I have entered may be used under someone else’s name. (identity theft)	I make sure that when I sign in I do not have the save password option checked	Always	Always	Don’t use	Don’t use	Always	Always

Group 4 (email with warnings, cut and paste attack): Web security attitudes

			How often & thoroughly user applies precautions when logging into:					
User #	**Biggest security concerns while browsing the Web**	**Precautions taken when logging into a Web site**	**Banking**	**Paypal**	**Web email**	**Shopping**	**Social networking**	**Study site**
250	1. Someone being able to access my financial/personal information 2. Getting a computer virus/spyware	If my antivirus tells that a website is not authenticated I won't proceed. I have a clear private data feature on my web browser.	Always	Always	Usually	Always	Usually	Usually
255	banking confidence	none	Usually	Sometimes	Sometimes	Sometimes	Rarely	Sometimes
260	invasion of privacy, private data, hacking	authorized signatures,safety lock at the bottom of the screen	Usually	Usually	Always	Usually	Always	Usually
270	phishing, identity theft	make sure it is the correct address.	Don't use	Always	Usually	Usually	Rarely	Rarely
275	No response	No response	Rarely	Rarely	Rarely	Rarely	Usually	No response
280	personal identification leakage	use the add-on progrmas that the website offers + use multiple protection programs	Always	Always	Usually	Always	Usually	Sometimes

Group 4 (email with warnings, cut and paste attack): Study experiences

User #	Fell for attack?	How attack ended	Saw something suspicious/dangerous?	If yes, reaction?	Remembered seeing warning? If yes, effect on decisions?	Followed attack instructions? Why or why not? (Question 18)
75	yes	entered html url	no	N/A	yes: I had forgotten about this	I trusted this site, so I just followed the instructions. I did not approach this experiment site with much caution.
80	yes	entered html url	no	N/A	yes: I didn't forward the email, but also had no reason to forward it.	I did copy/paste the link. I thought it was a little weird since it had not happened before, so to double-check, I opened up another tab and re-logged-into the site, and found the same page. After seeing the same page, I then copied the link, figuring it was part of the experiment.
85	no	timeout	no	N/A	no	I looked for a specific link to copy and paste into a window, but I did not do this because: 1) I closed the window that said to paste it into its box. 2) There was no specific, written out link in the email. Rather, it was hyperlinked.
90	no	followed html url	no	N/A	yes: No effect	I did not, I didn't read the below instructions
95	yes	entered html url	yes: It was just now when I logged in and they said their email system was not working and not to click on a certain link.	I was a little fearful that UCB movie predications had been hacked and so I followed the website's directions, which might have not been the best idea in case the website itself was trying to fool me.	yes: It did not affect my interactions with the site. This bit of information made me feel like the site was trying to protect my privacy.	I followed the instructions because I thought that if I clicked on the link someone might be able to see what was going on with my account and/or my computer.

Group 4 (email with warnings, cut and paste attack): Study experiences

User #	Fell for attack?	How attack ended	Saw something suspicious/dangerous?	If yes, reaction?	Remembered seeing warning? If yes, effect on decisions?	Followed attack instructions? Why or why not? (Question 18)
100	yes	entered plain url	no	N/A	no	I copied it because it told me to and I wouldn't have been able to continue if I didn't
105	no	followed html url	no	N/A	yes	i didnt think about it so i just clicked it
110	yes	entered plain url	no	N/A	no	because it said to, i didnt think twice about it
115	no	timeout	no	N/A	no	I don't remember seeing this, and if I did I am likely to have ignored it.
120	yes	entered plain url	no	N/A	no	I copy and pasted the link because it said in bold to do so. It seemed like that was what I was supposed to do.
125	yes	entered html url	no	N/A	yes: i totally forgot about it.	because you told us to and I trusted you as a study site that everything was secure.
135	yes	entered plain url	no	N/A	yes	I just assumed that it was legitimate because it came after I logged into your website
140	no	timeout	no: I already registered my computer, but it asked me to register again in the middle of the study, so I took it to be some sort of error.	The website and the email I received were telling me contradicting things so i just went with what the email told me.	yes: I took heed in the warning and did not copy the email link.	I didn't because the email I received with the link explicitly stated not to copy the link. Usually, in a verification email, you are supposed to click the link.
145	no	followed plain url	No response	No response	No response	No response
150	yes	entered html url	no	N/A	no	i followed them because i don't remember reading the warning and it said because of problems with the email reg system; i figured it was legitimate because its an xlabbb

Group 4 (email with warnings, cut and paste attack): Study experiences

User #	Fell for attack?	How attack ended	Saw something suspicious/dangerous?	If yes, reaction?	Remembered seeing warning? If yes, effect on decisions?	Followed attack instructions? Why or why not? (Question 18)
155	no	timeout	no	N/A	no	I did see this e-mail. I thought it was completely legit, because I had recently bought a new computer and was logging onto the site with the new computer for the first time. I thus had to request my password again, and thought this was part of the verification process (perhaps the site didn't recognize the new IP Address). So, ironically, I thought this was an attempt to try to keep my information MORE secure, not the opposite. I'm still unclear on how the whole experiment worked, though.
160	yes	entered plain url	no	N/A	yes	I believed the website more than I believed the e-mail. I assumed since the survey thing was new it was more up to date than the email.
165	yes	entered html url	yes: final login when password wasn't accepted, then the reconfirm email. that was odd.	followed directions, my correct email address was cited in the directions, so assumed was legitimate request.	yes: blindly followed instructions in spite of years of training...	you cited an email address that I had given you, that had previous been used by you for legitimate purposed. I had not bothered to confirm that i was actually at the URL that I had seen previously.
170	no	timeout	yes: the e-mail about copying and pasting a link	I did what the website said and closed the browser until later.	yes: I re-read the e-mail about registering my computer by copying the link and did not do it.	I did not because I remember reading not to do so.

Group 4 (email with warnings, cut and paste attack): Study experiences

User #	Fell for attack?	How attack ended	Saw something suspicious/dangerous?	If yes, reaction?	Remembered seeing warning? If yes, effect on decisions?	Followed attack instructions? Why or why not? (Question 18)
175	no	followed plain url + keylog data	no	N/A	no	Probably because UCB sounds safe and trustworthy to follow experiment instructions. Since the link might not work due to technical issues on your site; so I follow through with instructions.
180	no	followed html url	no	N/A	yes	No response
185	yes	entered plain url	no	N/A	yes	I just figured it was apart of the study so I had to do it.
190	yes	entered html url	no	N/A	no	I thought this was a legitimate error from the website. I didn't remember previous warnings (and probably didn't read them).
195	yes	entered html url	No response	No response	No response	No response
200	no	followed html url	no	N/A	yes	I was rushed.
205	no	followed html url	no	N/A	yes: I did not do any of the above except to click on the link to direct me to the study website	I don't remember this page. I only remeber the instruction to click on the link. I never seen the instruction " DO NOT CLICK ON THE LINK".
210	no	timeout + keylog data	yes: When it would not let me log in...	I kept trying to log in like an idiot ... Hmmm I guess since it's from Berkeley, and I know the email of the guy part of it because I forgot to put in the right number in the beginning?	no	I tried to copy and paste...

Group 4 (email with warnings, cut and paste attack): Study experiences

User #	Fell for attack?	How attack ended	Saw something suspicious/dangerous?	If yes, reaction?	Remembered seeing warning? If yes, effect on decisions?	Followed attack instructions? Why or why not? (Question 18)
215	no	followed html url	no	N/A	yes: It didn't I don't do that	I don't remember because It has been a hectic week. I just didn't notice
220	yes	entered plain url	yes: The e-mailer asked for my ID on sona system, but hackers could easily act like something was wrong and ask for your ID and password.	I acted like it was nothing and gave him my sona ID.	yes: No, it really didn't affect my decision. I completely forgot about it.	THis page seemed official and I thought there was stuff wrong with the system. But now as I am answering this question I am thinking about it and thinking hmmm I should have not done that.
225	no	followed plain url	no	N/A	yes: Made me feel like the experimenters tried to keep my information secure..	No response
230	yes	entered html url	no	N/A	no	I've recently reformated my computer and was previously asked to reregister my computer, I did not realize this process was serperate from that
235	no	followed html url	no	N/A	yes: I never forwarded or copied any links from the email.	I don't remember ever seeing this page, but I think what I might have seen was simply that I thought this page was giving me the same instructions as the first time when I had to register my computer.
240	no	timeout	no	N/A	yes: I was confused because it wouldn't let me access the website, so I just did what it did and it still didn't work so I didn't go on for a while until now.	I did this but nothing happened

Group 4 (email with warnings, cut and paste attack): Study experiences

User #	Fell for attack?	How attack ended	Saw something suspicious/dangerous?	If yes, reaction?	Remembered seeing warning? If yes, effect on decisions?	Followed attack instructions? Why or why not? (Question 18)
245	no	followed plain url	no	N/A	no	I did not follow the directions because I just assumed that the first line was what was most important which was to check my e-mail like I had been directed to do for all the previous times.
250	yes	entered plain url	no	N/A	yes: It didn't really affect my interactions with the website until the final login where I was requested to copy and paste the link sent to me. This made me feel a little uneasy, but I decided to do it anyway.	I thought maybe the email registration problem was legitimate and I didn't want to go through the trouble of emailing the coordinator of the experiment to find out.
255	no	followed html url	no	N/A	no	I thought this page was a mistake. I thought i had done something wrong to have received this.
260	no	followed html url	no	N/A	yes: i took it as advice, not as a safety hazard.	usually when registering a username in a website, you click on the link given to your email to authorize the validity of the account being accessed and the account the email was sent to.
270	yes	entered html url	no	N/A	no	I followed the instructions because they told me to do it. I don't feel any risk from a uc berkeley website, and I don't think there could be any harm in copying the shortcut.
275	no	followed html url + keylog data	no	N/A	no	i did not paste the link. my computer did not have a copy shortcut button

Group 4 (email with warnings, cut and paste attack): Study experiences

User #	Fell for attack?	How attack ended	Saw something suspicious/dangerous?	If yes, reaction?	Remembered seeing warning? If yes, effect on decisions?	Followed attack instructions? Why or why not? (Question 18)
280	yes	entered plain url	no	N/A	yes: it makes me more care of my account.	I followed the instruction simply because it poped up after logging in.

Group 4 (email with warnings, cut and paste attack): Registration attitudes

			Security of:		Convenience of:	
User #	**Used email registration before? If yes, where?**	**Benefits of email registration**	**Passwords + no registration**	**Passwords + email for registration**	**Passwords + no registration**	**Passwords + email for registration**
75	yes: apple	This enables them to make sure that the email belongs to me	Somewhat secure	Very secure	I could get used to it	I could get used to it
80	no	I guess it sends you a link so that you can log in from the email.	Fairly secure	Not secure at all	I hardly noticed it	Hard or slightly annoying
85	yes: virtually all sites dealing with transcations - paypal, ebay, amazon, etc.	it verifies the identity of the user and that the email provided is valid.	Fairly secure	Very secure	I could get used to it	I could get used to it
90	yes: paypal	prevents people from registering for things under your name and email, they must use a fake email	Somewhat secure	Somewhat secure	I hardly noticed it	I could get used to it
95	yes: Paypal.	I think that it confirms whether or not the email address you entered is actually yours, but I don't know how that makes everything secure. How it is better for security that you have the email you said you did. I mean you could just have someone else's email passwork and user name and it wouldn't actually by your email.	Somewhat secure	Very secure	I don't know	I hardly noticed it
100	no	It works to ensure that I'm the only one that has the password information and that it would be harder for others to get my information if I have email registration	Somewhat secure	Very secure	I could get used to it	I could get used to it

Group 4 (email with warnings, cut and paste attack): Registration attitudes

			Security of:		**Convenience of:**	
User #	**Used email registration before? If yes, where?**	**Benefits of email registration**	**Passwords + no registration**	**Passwords + email for registration**	**Passwords + no registration**	**Passwords + email for registration**
105	yes: i dont remember	no idea	Fairly secure	Very secure	I hardly noticed it	I could get used to it
110	yes: i cant remember	i have no idea	Fairly secure	Fairly secure	Hard or slightly annoying	Hard or slightly annoying
115	yes: Oh, multiple sites. Blog sits, newspaper and RSS feeds, etc.	You have to verify your email address so that the website/host knows that you aren't providing a fraudulent email.	Fairly secure	Very secure	I could get used to it	Hard or slightly annoying
120	no	I think that it is supposed to be a secure connection between the user and the site.	Somewhat secure	Very secure	I don't know	I could get used to it
125	yes: lots of them	makes sure you know what youre doing, sort of.	Somewhat secure	Fairly secure	I hardly noticed it	I hardly noticed it
135	no	Allows less people to hack into your accounts	Not secure at all	Very secure	I hardly noticed it	I hardly noticed it
140	yes: Various ones	No response	No response	No response	No response	No response
145	No response	No response	No response	No response	No response	No response
150	yes: facebook	one extra step in the security process	I don't know	I don't know	I hardly noticed it	I could get used to it
155	yes: Banking, any site that requires you to "sign up," really. Flickr, facebook, etc.	It may help ensure that a real person is actually registered, not a program.	I don't know	Fairly secure	I hardly noticed it	Hard or slightly annoying
160	no	it just confirms you are using the same email and not signing up under other peoples' accounts.	Somewhat secure	Somewhat secure	I hardly noticed it	I hardly noticed it

Group 4 (email with warnings, cut and paste attack): Registration attitudes

			Security of:		Convenience of:	
User #	Used email registration before? If yes, where?	Benefits of email registration	Passwords + no registration	Passwords + email for registration	Passwords + no registration	Passwords + email for registration
165	yes: several, don't recall craigslist?	register at site, site sends info back to addy, Never considered it for my particular benefit, more for the site to limit 'bot' registration.	Somewhat secure	Somewhat secure	I hardly noticed it	I hardly noticed it
170	no	It is personal and requires a password.	Somewhat secure	Fairly secure	I could get used to it	I could get used to it
175	yes: financial related sites, shopping sites, etc.	if you make a specific email that you don't give to everyone, less people would ever guess that it is your email address to begin with.	Not secure at all	Fairly secure	Hard or slightly annoying	Hard or slightly annoying
180	no	I don't know	Somewhat secure	Somewhat secure	Hard or slightly annoying	Hard or slightly annoying
185	no	No response	Somewhat secure	Fairly secure	I don't know	I don't know
190	yes: Paypal, neopets, social networking sites.	It makes sure that whoever has access to the email password is the only one with access to the registered account.	Not secure at all	Very secure	I hardly noticed it	I hardly noticed it
195	No response	No response	No response	No response	No response	No response
200	no	No response	Somewhat secure	Somewhat secure	I could get used to it	I could get used to it
205	yes: Pickaprof.com, kaiserpermanente.org, etc	It allows only that person to retrieve the account password just incase if someone else put in your information to activate an account	Somewhat secure	Fairly secure	I hardly noticed it	I hardly noticed it
210	no	No response	Somewhat secure	Fairly secure	I hardly noticed it	I hardly noticed it

Group 4 (email with warnings, cut and paste attack): Registration attitudes

			Security of:		Convenience of:	
User #	Used email registration before? If yes, where?	Benefits of email registration	Passwords + no registration	Passwords + email for registration	Passwords + no registration	Passwords + email for registration
215	yes: paypal, askfred I can't remember all of them there are so many	They make sure that 1- the person signing up for the account is the actual person 2- ensures that the info you entered was correct (to an extent) 3- keeps traffic down by limiting the number of fake registrations	Somewhat secure	Fairly secure	I hardly noticed it	I hardly noticed it
220	yes: Tons of them like photo uploading websites, etc.	At least you know that it isn't a computer program that is signing up and that these people really have e-mail addresses.	Somewhat secure	Fairly secure	I hardly noticed it	I hardly noticed it
225	no	I'm not sure.	Fairly secure	Fairly secure	I hardly noticed it	I hardly noticed it
230	yes: amazon.com, facebook	it offers a second level of verification with the confirmation e-mails, but it still seems a bit risky, since e-mails are something people give out all the time	Very secure	Very secure	I hardly noticed it	Hard or slightly annoying
235	no	I think it works by remembering aspects of the registered computer you are using, and it has benefits because then others accessing your accounts through another computer would not be able to get through.	Somewhat secure	Fairly secure	I hardly noticed it	I could get used to it
240	no	It's more direct, stops spammers or hackers or computer-generated systems from breaking into your account.	Somewhat secure	Very secure	I hardly noticed it	I could get used to it

Group 4 (email with warnings, cut and paste attack): Registration attitudes

			Security of:		Convenience of:	
User #	**Used email registration before? If yes, where?**	**Benefits of email registration**	**Passwords + no registration**	**Passwords + email for registration**	**Passwords + no registration**	**Passwords + email for registration**
245	yes: facebook	email registration allows me to feel like I am exclusively the only one that can view information being sent to me (because I have never told anyone my password)	Not secure at all	Fairly secure	I could get used to it	I could get used to it
250	yes: online shopping websites , online banking	presumably you are the only one with access to your email passwords, so providing a login through there helps to make sure that no one else can login to your account	I don't know	Fairly secure	I hardly noticed it	I hardly noticed it
255	yes: craigslist	it makes sure you entered your correct email to be private	Fairly secure	Very secure	I don't know	I hardly noticed it
260	yes: i can't remember	i explained my reasoning earlier	Fairly secure	Very secure	Hard or slightly annoying	I could get used to it
270	yes: almost every one	it makes sure you are signing up for your own account.	Somewhat secure	Fairly secure	I hardly noticed it	I hardly noticed it
275	yes: google.com	No response	Fairly secure	Somewhat secure	I hardly noticed it	I could get used to it
280	yes: homework manager by mcgrow hills.	it's somewhat bothersome, but seems to be safer	Fairly secure	Very secure	I hardly noticed it	I could get used to it

Group 4 (email with warnings, cut and paste attack): General questions/feedback

User #	Average length of each visit	Anything annoying or difficult?	Engaging or interesting?	General comments
75	5-10 minutes	Nope	yes	It was fun and interesting. I really thought I was trying to predict movie trends. Haha.
80	0-5 minutes	Not really. I guess disappointed it had nothing to do with predicting movies, haha.	yes	The idea of email registration sounds inconvenient. Emails often get sent to people's spam, or something just flat-out dont go through. Also, they dont always arrive promptly, which I imagine would get annoying if you want log in and out quickly.
85	5-10 minutes	No response	yes	I did not realize we had a limited amount of 10 days to get in 7 votes. This was not explicitly stated anywhere on the UCB movie predictions website itself and thus was very very misleading.
90	5-10 minutes	no	yes	No response
95	5-10 minutes	No.	yes	No.
100	5-10 minutes	not particularly	yes	Haha really tricky...didn't see that coming that's for sure!
105	0-5 minutes	no	no	didnt have time to do it everyday wish i could do it whenever i wanted
110	0-5 minutes	no	yes	No response
115	0-5 minutes	Not enough time, no daily reminders to visit the site.	yes	No response
120	5-10 minutes	This last survey was a bit long, but the rest of the study was fine.	yes	It was fun and finding out the little twist at the end was entertaining.
125	0-5 minutes	Yes, filling out this survey. Especially because this has nothing to do with movie predictions.	yes	What exactly is this study about? Movie predictions or web site safety?
135	0-5 minutes	NO	yes	No response
140	5-10 minutes	No	yes	Very tricky! :P
145	No response	No response	No response	No response
150	5-10 minutes	no	yes	No response
155	0-5 minutes	NO. There should be more like it.	no	Good job.
160	0-5 minutes	no.	yes	No response
165	5-10 minutes	nope...ease of entrapment at the end is testimony :)	yes	No response
170	0-5 minutes	No	yes	None
175	0-5 minutes	nothing comes into mind.	yes	none.

Group 4 (email with warnings, cut and paste attack): General questions/feedback

User #	Average length of each visit	Anything annoying or difficult?	Engaging or interesting?	General comments
180	0-5 minutes	no	yes	no
185	5-10 minutes	No	yes	n/a
190	0-5 minutes	Not at all.	yes	I failed :(
195	No response	No response	No response	No response
200	5-10 minutes	No response	yes	No response
205	0-5 minutes	No	yes	What is this for? Is it for security concerns?
210	5-10 minutes	No response	yes	No response
215	0-5 minutes	nope	yes	I would have liked to have more info on the other movie grosses.
220	5-10 minutes	I think I would have forgot about the movies if there were not constant reminders about the 7 log-ins.	yes	Um, if you want to make it more legit for the movie study, you shouldn't allow people to change their answer once they input or at least don't let them see how previous movies did so they can change their answers.
225	0-5 minutes	Not really.	yes	No response
230	0-5 minutes	no	yes	no
235	0-5 minutes	No, except when I wanted the movie information to get in sooner.	yes	This study was interesting, we should have more like it.
240	0-5 minutes	no	yes	good design/idea
245	0-5 minutes	No	yes	No response
250	5-10 minutes	no	no	I had no idea this was about internet security, I sincerely believed it was about predicting market events. Your methods work.
255	0-5 minutes	no	no	No response
260	5-10 minutes	No response	yes	No response
270	5-10 minutes	no	yes	i had a false sense of security because it was a berkeley site so i never suspected it could be ”dangerous” and my guard was definitely down.
275	20+ minutes	No response	yes	No response
280	0-5 minutes	no	yes	n/a

Group 5 (email without warnings, cut and paste attack): Demographics

User #	Gender	Age	Student status or occupation	Details	OS	Primary browser	Web use/week (hrs)	Financial transactions done online	Experience doing financial transactions online
76	Female	18-21	Undergraduate	Economics or business	Windows	Firefox	20+	Banking, Investing, Shopping, Auctions, PayPal	> 2 years
81	Female	18-21	Undergraduate	Social sciences	Windows	Firefox	20+	Banking	> 2 years
86	Female	18-21	Undergraduate	Natural sciences	Windows	Firefox	10-20	Banking, Shopping	> 2 years
91	Male	18-21	Undergraduate	Economics or business	Windows	Firefox	20+	Banking, Investing, Shopping	> 2 years
96	Female	22-25	Undergraduate	Natural sciences	Mac OS	Safari	5-10	Banking, Shopping, PayPal	> 2 years
101	No response	No response	No response	No response	No response	No response	No response	No	Never
106	Female	18-21	Undergraduate	Economics or business	Mac OS	Firefox	20+	Shopping	6–12 months
111	Male	18-21	Undergraduate	Social sciences	Windows	Internet Explorer	10-20	Banking, Shopping, Auctions, PayPal	> 2 years
116	Male	18-21	Undergraduate	Engineering	Mac OS	Safari	10-20	Shopping, PayPal	Never
121	Female	18-21	Undergraduate	Natural sciences	Windows	Firefox	20+	Banking, Auctions	> 2 years
126	Male	22-25	Recent	No response	Windows	Internet Explorer	20+	Banking, Shopping, Auctions, PayPal	> 2 years
136	Female	18-21	Undergraduate	undeclared	Mac OS	Firefox	20+	Banking, Shopping, PayPal	< 6 months
141	Female	18-21	Undergraduate	Social sciences	Windows	Firefox	10-20	Listing, Banking, Shopping, Auctions, PayPal	> 2 years
146	Male	31-40	staff	No response	Windows	Firefox	20+	Banking, Investing, Shopping, Auctions, PayPal	> 2 years

Group 5 (email without warnings, cut and paste attack): Demographics

User #	**Gender**	**Age**	**Student status or occupation**	**Details**	**OS**	**Primary browser**	**Web use/week (hrs)**	**Financial transactions done online**	**Experience doing financial transactions online**
151	Male	18-21	Undergraduate	Cognitive Science	Windows	Firefox	10-20	Banking, Shopping, Auctions, PayPal	> 2 years
156	Female	18-21	Undergraduate	Humanities	Windows	Firefox	10-20	Banking, Shopping	> 2 years
161	Male	26-30	Graduate	Social sciences	Windows	Firefox	20+	Banking, Shopping, Auctions, PayPal	> 2 years
166	Female	22-25	Undergraduate	Natural sciences	Mac OS	Firefox	20+	Banking, Shopping, PayPal	> 2 years
171	Male	18-21	Undergraduate	Natural sciences	Windows	Firefox	20+	Banking, Shopping	1–2 years
176	Female	18-21	Undergraduate	Natural sciences	Windows	Firefox	20+	Banking, Shopping, Auctions, PayPal	1–2 years
181	Male	18-21	Undergraduate	Natural sciences	Windows	Firefox	20+	Banking, Investing, Shopping, Auctions, PayPal	1–2 years
186	Male	18-21	Undergraduate	Applied Math	Windows	Firefox	10-20	Forum, Banking, Shopping, Auctions	6–12 months
191	Female	18-21	Undergraduate	Economics or business	Windows	Firefox	20+	Banking, Shopping, Auctions, PayPal	> 2 years
196	Male	18-21	Undergraduate	Economics or business	Windows	Firefox	10-20	Banking, Shopping, Auctions, PayPal	> 2 years
201	Female	18-21	Undergraduate	Social sciences	Windows	Internet Explorer	10-20	Banking, Shopping	6–12 months
206	Male	18-21	Undergraduate	Natural sciences	Windows	Firefox	20+	Shopping, PayPal	> 2 years
211	Male	18-21	Undergraduate	Economics or business	Windows	Firefox	10-20	Banking, Shopping, PayPal	6–12 months

Group 5 (email without warnings, cut and paste attack): Demographics

User #	Gender	Age	Student status or occupation	Details	OS	Primary browser	Web use/week (hrs)	Financial transactions done online	Experience doing financial transactions online
216	Female	41-50	Undergraduate	Social sciences	Windows	Firefox	10-20	Banking, Investing, Shopping, Auctions, PayPal	> 2 years
221	Male	18-21	Undergraduate	Natural sciences	Windows	Firefox	10-20	Banking, Shopping, PayPal	6–12 months
226	Female	18-21	Undergraduate	Humanities	Mac OS	Firefox	20+	Banking, Shopping, Auctions, PayPal	> 2 years
231	Female	18-21	Undergraduate	Natural sciences	Windows	Firefox	5-10	Banking, Shopping, PayPal	< 6 months
236	Female	18-21	Undergraduate	Humanities	Mac OS	Safari	5-10	Banking, Shopping, Auctions	1–2 years
241	Female	18-21	Undergraduate	natural resources	Windows	Firefox	10-20	Banking, Shopping, Auctions, PayPal	6–12 months
246	Female	22-25	Undergraduate	Social sciences	Mac OS	Safari	10-20	Banking, PayPal	6–12 months
251	Female	18-21	Undergraduate	Social sciences	Windows	Internet Explorer	20+	Banking, Shopping, Auctions, PayPal	6–12 months
256	Female	18-21	Undergraduate	Natural sciences	Mac OS	Firefox	10-20	Banking, Shopping, Auctions, PayPal	1–2 years
268	Female	18-21	Undergraduate	Humanities	Mac OS	Firefox	10-20	Shopping, Auctions	> 2 years
271	Male	18-21	Undergraduate	Natural sciences	Windows	Firefox	10-20	Shopping, Auctions	Never
276	Female	18-21	Undergraduate	Economics or business	Windows	Internet Explorer	20+	Banking, Shopping, Auctions, PayPal	> 2 years
281	Female	18-21	Undergraduate	interdisciplinary	Windows	Firefox	5-10	Banking, Shopping	6–12 months

Group 5 (email without warnings, cut and paste attack): Web security attitudes

			How often & thoroughly user applies precautions when logging into:					
User #	**Biggest security concerns while browsing the Web**	**Precautions taken when logging into a Web site**	**Banking**	**Paypal**	**Web email**	**Shopping**	**Social networking**	**Study site**
76	Someone hacking into my computer and getting my information; someone placing a virus into my computer; someone hacking and watching what I do on the internet	I learned that websites with https are more secured than websites with just http so I trust the https websites more.	Always	Usually	Rarely	Usually	Rarely	Usually
81	Invasion of Privacy	I only take precautions when logging into a website that is concerned with either private, school, or financial concerns.	Always	Always	Sometimes	Usually	Sometimes	Rarely
86	Malicious software downloaded into my personal computer to steal personal information or track my movements on the internet	Have software installed to inform me if anything is trying to get downloaded into my computer and I can choose to reject or accept the download. The program identifies risks from a list of known risks. I also downloaded software to tell me if a site I am about to enter is listed as dangerous or safe.	Usually	Usually	Usually	Usually	Usually	Usually
91	I'm afraid of my private information being stolen. I know people that had their credit card information stolen online, so identity theft is a big concern of mine.	I always use a secure connection, i have a firewall and I make sure I only visit sites that I know about in advance.	Always	Always	Always	Always	Always	Always

Group 5 (email without warnings, cut and paste attack): Web security attitudes

			How often & thoroughly user applies precautions when logging into:					
User #	**Biggest security concerns while browsing the Web**	**Precautions taken when logging into a Web site**	**Banking**	**Paypal**	**Web email**	**Shopping**	**Social networking**	**Study site**
96	1. My personal information will be viewed by third parties. 2. My personal information will be sent to advertisers who will then spam my email till I'm blue.	I don't take much precaution except when I log on site where I enter personal information. In that case I try to make sure it is secure.	Always	Always	Always	Always	Always	Always
101	identity theft	giving too much information	No response	No response	No response	No response	No response	No response
106	Credit card theft. Spyware Adware	Not logging into shady looking sites. Making sure there is some software to protect privacy when using credit card.	Always	Always	Sometimes	Usually	Always	Rarely
111	None. I know what to avoid on the internet and therefore do not feel like I will fall victim to any security threats.	If the site is poorly constructed, I will avoid it.	Rarely	Rarely	Rarely	Usually	Sometimes	Rarely
116	none	none	Sometimes	Rarely	Rarely	Sometimes	Rarely	Rarely
121	identity theft, mistake in transaction	I would only use my personal computer for anything that would require money transaction and I would not save my password on sites relating to financial topics.	Always	Always	Rarely	Don't use	Rarely	Rarely
126	financial transactions. i don't want my info compromised	I check to see if there is a "secure website" lock symbol near the top of the navigation bar whenever I enter financial information.	Usually	Always	Sometimes	Usually	Rarely	Rarely

Group 5 (email without warnings, cut and paste attack): Web security attitudes

			How often & thoroughly user applies precautions when logging into:					
User #	**Biggest security concerns while browsing the Web**	**Precautions taken when logging into a Web site**	**Banking**	**Paypal**	**Web email**	**Shopping**	**Social networking**	**Study site**
136	security issues	i dont log onto my bank account using wireless	Always	Usually	Usually	Always	Always	Sometimes
141	Someone hacking the database, selling or buying items from unreliable/dishonest people, someone else hacking into my information/accounts	I never click the link to a financial website through an email. I will type in the web address myself.	Always	Always	Sometimes	Usually	Sometimes	Sometimes
146	phishing	look for the lock symbol, check the correct web site addresses	Always	Always	Usually	Always	Sometimes	Usually
151	Debit card/credit card	No response	Always	Usually	Sometimes	Usually	Rarely	Rarely
156	privacy identity theft viruses	entering passwords, social security numbers etc.	Always	Always	Usually	Always	Usually	Sometimes
161	privacy, health of my computer	none	No response	No response	No response	No response	No response	No response
166	Having my activity tracked, obtaining my ssn, and having credit card information leaked.	I try to remember to log out when I am done and close the browser, but that does not always happen.	Always	Always	Don’t use	Always	Rarely	Rarely
171	1. Viruses 2. Hackers 3. Fraud	No response	Sometimes	Rarely	Rarely	Rarely	Rarely	Rarely
176	My biggest security concern is that my personal information may be stolen in the process of a transaction.	I do not conduct any personal financial transactions on computers other than my own.	Always	Usually	Rarely	Rarely	Sometimes	Usually

Group 5 (email without warnings, cut and paste attack): Web security attitudes

			How often & thoroughly user applies precautions when logging into:					
User #	**Biggest security concerns while browsing the Web**	**Precautions taken when logging into a Web site**	**Banking**	**Paypal**	**Web email**	**Shopping**	**Social networking**	**Study site**
181	Viruses, Theft of Personal Information, Misuse of personal information	Manually typing in the url for banking/investing websites, not storing the passwords for sensitive accounts	Always	Always	Rarely	Sometimes	Rarely	Rarely
186	Afraid that my account might get hacked into.	Enabling some sort of spyware security monitor system.	Always	Always	Always	Always	Sometimes	Usually
191	viruses when downloading	for financial sites, i look for the s in https as a security measure	Always	Always	Rarely	Usually	Rarely	Sometimes
196	Viruses	No response	Rarely	Rarely	Rarely	Rarely	Rarely	Rarely
201	Viruses, and identity theft.	I try to make sure I have secure passwords.	Always	Always	Always	No response	Always	Always
206	Being Spyed on Having Information stolen	I make sure the site is secure. Sometimes I give false information	Sometimes	Sometimes	Sometimes	Sometimes	Sometimes	Rarely
211	That personal information, especially passwords and financial information, could be stolen.	I'm careful to always check the URL of the site I am entering my password in.	Always	Always	Usually	Usually	Sometimes	Rarely
216	Someone will get my credit card information or steal my identity.	I look for a secure server. I use credit cards that protect against theft. If I'm suspicious I don't make a transaction.	Always	Always	Sometimes	Always	Rarely	Rarely
221	No response	No response	Usually	Always	Sometimes	Sometimes	Sometimes	Sometimes

Group 5 (email without warnings, cut and paste attack): Web security attitudes

			How often & thoroughly user applies precautions when logging into:					
User #	**Biggest security concerns while browsing the Web**	**Precautions taken when logging into a Web site**	**Banking**	**Paypal**	**Web email**	**Shopping**	**Social networking**	**Study site**
226	Stolen credit card and other personal information.	In regards to entering credit card information, I check if the website is authenticated with security features (i.e., the little lock in the bottom right corner of browser).	Always	Always	Rarely	Usually	Rarely	Rarely
231	bank passwords	go to secure sites.	Always	Usually	Always	Usually	Sometimes	Rarely
236	Stay logged into sites on public computers	I do not check ”remember me” on public computers. i have complicated passwords.	Always	Always	Always	Always	Always	Rarely
241	viruses and computer hackers	check for the security lock at the bottom of the page...by the way, i dont see one on this page!	Usually	Usually	Sometimes	Sometimes	Always	Rarely
246	Identity theft, charging multiple times for an item, getting a computer virus	If I buy anything online, I check the security policies I make sure to not have my passwords saved	Always	Always	Always	Always	Always	Sometimes
251	my credit card information being stolen	none	Rarely	Rarely	Rarely	Rarely	Rarely	Rarely
256	Hackers, viruses, identity theft.	Never really take any...	Rarely	Rarely	Rarely	Rarely	Rarely	Rarely
268	Stolen identity.	NOne.	Always	Always	Always	Always	Always	Sometimes
271	identity theft computer viruses	hope the browser blocks any pop ups or viral downloads	Rarely	Rarely	Rarely	Rarely	Rarely	Rarely
276	email security (spam), financial security	checking for security logos, making sure the web address is correct	Usually	Usually	Rarely	Sometimes	Usually	Rarely
281	someone hacking into my computer, identity theft	No response	Always	Usually	Sometimes	Usually	Sometimes	Rarely

Group 5 (email without warnings, cut and paste attack): Study experiences

User #	Fell for attack?	How attack ended	Saw something suspicious/dangerous?	If yes, reaction?	Remembered seeing warning? If yes, effect on decisions?	Followed attack instructions? Why or why not? (Question 18)
76	yes	entered html url	no	N/A	no	I followed the instructions to copy/paste because I rather be safe than sorry. It only takes two more seconds to follow the instructions.
81	no	followed html url	no	N/A	no	I did not follow those instructions; this website seems legitimate and I didn't see the need to take extra precautions.
86	yes	entered html url	no	N/A	no	I followed the instructions because I thought it was a legitimate set of instructions from respected researchers who could not possibly have a motive to deceive me.
91	no	followed plain url	no	N/A	no	I figured that since this was a Berkeley research affiliated website, it would be safe.
96	yes	entered plain url	no	N/A	no	I followed the prompt because I thought the website leading to the study from X-lab was secure.
101	yes	entered html url	No response	No response	No response	I followed the instructions to copy/paste the link because it told me to do so. I thought that something would go wrong if I didn't, and I didn't want to run into any problems
106	yes	entered html url	no	N/A	no	I followed the instructions because I did not think there was anything to lose if it was a security breach since I was only making movie predictions.

Group 5 (email without warnings, cut and paste attack): Study experiences

User #	Fell for attack?	How attack ended	Saw something suspicious/dangerous?	If yes, reaction?	Remembered seeing warning? If yes, effect on decisions?	Followed attack instructions? Why or why not? (Question 18)
111	no	followed html url	no	N/A	yes: I think I remember seeing that when another registration email was sent to me this morning. It looked like a standard confidentiality issue, so I didn't think of it as anything particularly special.	I don't remember seeing instructions that say not to click the email link.
116	yes	entered plain url	no	N/A	no	i followed the instructions because it said in bold and capital letters that we should not click the link on the email we received explicitly.
121	yes	entered html url	no	N/A	no	The screen was instruction from the site and it felt trustworthy.
126	no	followed html url	no	N/A	yes: I just clicked on the link. Didnt think twice.	I copied the link because it said to copy the link.
136	no	followed html url	no	N/A	no	i just clicked the link
141	no	followed html url + keylog data	no	N/A	no	I knew that the email was sent from a reliable source and felt comfortable enough to click the link in the email instead.
146	no	followed plain url	no	N/A	no	Unfortunately, I clicked on the link because I was tired and didn't look at it very carefully.
151	no	followed html url	no	N/A	no: not at all, I thought it was a little serious for just some study	Didn't notice that it said "don't click on this link"
156	yes	entered html url	no	N/A	yes: It didn't really affect my decisions at all. I sort of ignored it.	I did because the instructions were explicit and told me not to. I did not want anything bad to happen if I did it the wrong way.

Group 5 (email without warnings, cut and paste attack): Study experiences

User #	Fell for attack?	How attack ended	Saw something suspicious/dangerous?	If yes, reaction?	Remembered seeing warning? If yes, effect on decisions?	Followed attack instructions? Why or why not? (Question 18)
161	no	followed html url	no: (actually responded yes) Data for previous days weren't always available; data actually changed (along with my bonus total) at one point.	I assumed the data wasn't available to anyone yet, so it wasn't a problem with the website. As for when the data and my totals changed, I assumed that the system was correcting for an inaccuracy. My total went down 50 cents, so I was a little annoyed, but I didn't really do anything about it (I assumed the site had it right).	no	I vaguely remember this page, but I don't think I read it too carefully considering the fact that I did indeed click the link in my email.
166	no	followed html url	no	N/A	no	I didn't follow the instructions because I thought it was weird I was asked to re-register my computer when I had already done this initially.
171	yes	entered plain url	yes: Repeated need to register computer.	I was annoyed.	yes: I didn't really care.	I thought that the link was broken.
176	no	followed html url	no	N/A	no	I did not follow the instructions from previous experiences that has basically conditioned me to avoid clicking links.

Group 5 (email without warnings, cut and paste attack): Study experiences

User #	Fell for attack?	How attack ended	Saw something suspicious/dangerous?	If yes, reaction?	Remembered seeing warning? If yes, effect on decisions?	Followed attack instructions? Why or why not? (Question 18)
181	yes	entered html url	no	N/A	no	The website was the same as the one I visited before, so I trusted the instructions the website gave me.
186	yes	entered html url	no	N/A	no	I followed the instructions because the website told me to.
191	no	followed html url	no	N/A	no	I did both, because I accidentally clicked the link, which opened a new tab, and also followed the instructions, and noticed the results were the same.
196	no	followed html url	no	N/A	no	I never saw these instructions.
201	no	timeout + keylog data	no	N/A	no	I followed the instructions because I thought they were being given by the UCB movie predictions website. I normally log in from my home but I was connected to the AIRBears network on campus when I received this message and thought it might be affecting my ability to connect to the website since I was not allowed to use an on campus computer to log in. It didn't occur to me that this message was a virus or security threat.
206	yes	entered plain url	no	N/A	yes: It made it seem more legit	I did because it seemed necessary for the study

Group 5 (email without warnings, cut and paste attack): Study experiences

User #	Fell for attack?	How attack ended	Saw something suspicious/dangerous?	If yes, reaction?	Remembered seeing warning? If yes, effect on decisions?	Followed attack instructions? Why or why not? (Question 18)
211	no	followed html url	no	N/A	yes: It didn't, I figured it was just standard stuff.	I don't think I followed the instructions. I was confused because I hadn't made all 7 predictions and I got back to this site using my browser history. I figured I clicked on the wrong subdomain and somehow broke the study, so I tried to go back in through the last e-mail I got from you.
216	yes	entered plain url	no	N/A	no	I figured something was wrong with your registration system and thus followed instructions. Since I was dealing with a UCB experiment I thought of it as a trusted site.
221	yes	entered plain url	no	N/A	no	I followed the instructions because they seemed legitimate.
226	no	followed html url	no	N/A	no	I thought there was a security feature where the registration must have been set to expire every so often, so I followed the procedure to (re-)register my computer.
231	yes	entered html url	no	N/A	yes	didn't see 'johnsmith'
236	yes	entered plain url	no	N/A	no	I followed the instructions because it told me to, saying there were problems with the email system, which I assumed meant that clicking the link would not work.
241	yes	entered plain url	no	N/A	no	i followed the instructions because i was asked to

Group 5 (email without warnings, cut and paste attack): Study experiences

User #	Fell for attack?	How attack ended	Saw something suspicious/dangerous?	If yes, reaction?	Remembered seeing warning? If yes, effect on decisions?	Followed attack instructions? Why or why not? (Question 18)
246	no	followed plain url	no	N/A	no	I do remember seeing it but not paying much attention because I figured UCB would not send an insecure link. If the link didn't work, then I would have gone back and tried the other way.
251	yes	entered html url	no	N/A	no	i followed the instructions because i thought i had to to access the website
256	no	followed plain url	no	N/A	no	No response
268	no	followed html url	no	N/A	yes	I don't remember... and therefore don't remember.
271	no	timeout	no	N/A	no	I was about to but I had to leave for class. However, I do not remember receiving a link that resembled the one in the error page.
276	yes	entered html url	no	N/A	no	I thought it was weird because I had already registered. On the other hand, I didn't see a way to navigate past it and I trusted the site. So I followed the instructions. Right after I did it I started thinking it was a bit suspicious but it was too late.
281	no	followed html url	no	N/A	no	I did not follow the instructions because it was easier to just click.

Group 5 (email without warnings, cut and paste attack): Registration attitudes

			Security of:		Convenience of:	
User #	**Used email registration before? If yes, where?**	**Benefits of email registration**	**Passwords + no registration**	**Passwords + email for registration**	**Passwords + no registration**	**Passwords + email for registration**
76	yes: When applying to have login names for bank accounts, credit card accounts, etc.	I think it prevents hackers from just creating accounts and using them but they would have to go to the extra step of doing the email registrations.	Somewhat secure	Very secure	I hardly noticed it	I hardly noticed it
81	yes: PG&E and AT&T	It prevents spambots and hackers (maybe) from utilizing information from such sites.	Fairly secure	Very secure	I hardly noticed it	I hardly noticed it
86	yes: To register at RunnersWorld.com - in their email to me it actually said the email confirmation will help ”to protect us and you”	I always thought it was just to make sure that the person who registered at the site entered a correct email address in order to be sent email from that site or third parties.	Fairly secure	Fairly secure	I hardly noticed it	I could get used to it
91	yes: Many job websites.	It links your profile to your e-mail and gives you easy accessibility	Fairly secure	Fairly secure	I hardly noticed it	I hardly noticed it
96	yes: BankofAmerica.com	It works by sending an email to the applicant that should verify a persons identity. I don’t necessarily know how this is meant to stop impostors from misrepresenting themselves as another.	I don’t know	I don’t know	Hard or slightly annoying	Hard or slightly annoying
101	No response	No response	No response	No response	No response	No response
106	yes: forums, accounts.	It makes sure that people are not making mass usernames.	Somewhat secure	Very secure	I hardly noticed it	I could get used to it

Group 5 (email without warnings, cut and paste attack): Registration attitudes

			Security of:		Convenience of:	
User #	Used email registration before? If yes, where?	Benefits of email registration	Passwords + no registration	Passwords + email for registration	Passwords + no registration	Passwords + email for registration
111	yes: I cannot remember specific sites, but I've done it many times.	It forces the user to validate the email address used during registration. It helps to prevent generation of multiple accounts by the same user. For example: instead of making 5 accounts in order to earn $100 + forthissurvey, Ionlyhadoneandcouldonlyearn$20+.	Somewhat secure	Fairly secure	I hardly noticed it	I hardly noticed it
116	yes: online shopping	filters out computers or spammers	Fairly secure	Fairly secure	Hard or slightly annoying	Hard or slightly annoying
121	yes: When I set up accounts with amazon, facebook, paypal, and ebay, I had to have email registration.	It allows for some tracing of the owner since the registration of the email should be the same as the person registering to the new website	Fairly secure	Fairly secure	I hardly noticed it	I hardly noticed it
126	yes: Don't remember. But many sites on initial sign up tell me to check my email and click the link.	I thought it was just to confirm that you had a valid email address.	Fairly secure	Fairly secure	I hardly noticed it	I could get used to it
136	no	No response	Somewhat secure	Very secure	I hardly noticed it	I hardly noticed it
141	yes: Too many to remember.	It's a good way to check that the person who is requesting to access the account is indeed, the person who owns the email associated with the account.	Not secure at all	Fairly secure	I hardly noticed it	I hardly noticed it

Group 5 (email without warnings, cut and paste attack): Registration attitudes

			Security of:		Convenience of:	
User #	Used email registration before? If yes, where?	Benefits of email registration	Passwords + no registration	Passwords + email for registration	Passwords + no registration	Passwords + email for registration
146	yes: paypal	it sends a verification message to your e-mail account before you can use the site.	Not secure at all	Very secure	Hard or slightly annoying	I hardly noticed it
151	yes: Don't Remember. Craigstlist I think	makse it so that people can't just spam some site with lots of fake accounts. Requires a checked email	Somewhat secure	Fairly secure	I hardly noticed it	I hardly noticed it
156	yes: facebook gmail any new account activation wamu checking	So random people cannot register or steal your identity, it wants to confirm that the people who own the email address are the ones who are actually creating the account.	Somewhat secure	Fairly secure	I hardly noticed it	I hardly noticed it
161	yes: mechbank.com	I'm guessing that it identifies which computer you are logging in from so that someone can't steal your password and log onto your account from another location.	Very secure	Very secure	I could get used to it	Hard or slightly annoying
166	yes: facebook, myspace, paypal	You are logged in based off of your email, which is verified by a confirmation email. It is beneficial because the person has to access their email also, so it is an additional precautionary step.	Fairly secure	Very secure	I hardly noticed it	Hard or slightly annoying
171	yes: Amazon	Only I should know my own password for email.	Fairly secure	Very secure	I hardly noticed it	Nearly impossible or very annoying

Group 5 (email without warnings, cut and paste attack): Registration attitudes

			Security of:		Convenience of:	
User #	**Used email registration before? If yes, where?**	**Benefits of email registration**	**Passwords + no registration**	**Passwords + email for registration**	**Passwords + no registration**	**Passwords + email for registration**
176	yes: Shopping websites, paypal	I think that email registration utilizes the fact that the individual already has a password that must be set up in order to access the email account so that would be the real ensurement of security. It just adds in an extra factor	Fairly secure	Very secure	I hardly noticed it	I could get used to it
181	yes: Various forum websites	The link in the email contains a data string that, when clicked, changes account details to confirm that that was a valid email address. Security benefits to the user may be minimal.	Somewhat secure	Fairly secure	I hardly noticed it	I could get used to it
186	yes: paypal.com ebay.com	to verify that a person is actually setting up a genuine account and not some sort of computer setting up an account for conspicuous purposes.	Somewhat secure	Fairly secure	I could get used to it	I could get used to it
191	yes: don't remember, but some shopping sites, and some emails or school related websites	it makes sure that people do not fraudulently sign up for things using your email, as you need both email access and the email itself in order to conduct transactions.	Somewhat secure	Fairly secure	I hardly noticed it	I hardly noticed it
196	no	No response	Fairly secure	Very secure	I hardly noticed it	I hardly noticed it
201	yes: Paypal and others I cannot recall.	I do not really understand internet security very well at all. I think it would be helpful if I knew more about it.	Fairly secure	Very secure	I hardly noticed it	I hardly noticed it

Group 5 (email without warnings, cut and paste attack): Registration attitudes

			Security of:		Convenience of:	
User #	Used email registration before? If yes, where?	Benefits of email registration	Passwords + no registration	Passwords + email for registration	Passwords + no registration	Passwords + email for registration
206	yes: Many different ones	It makes it so that you at least need access to an email address to sign up for something	Somewhat secure	Fairly secure	I hardly noticed it	I hardly noticed it
211	yes: Tons of websites, especially forums, use this to confirm accounts.	Usually they just confirm that you are a real person and give you someone to retrieve your password if necessary.	Somewhat secure	Somewhat secure	I hardly noticed it	I hardly noticed it
216	yes: numerous...	To give validity to an email?	Not secure at all	Fairly secure	I hardly noticed it	I hardly noticed it
221	yes	No response	Somewhat secure	Fairly secure	I hardly noticed it	I could get used to it
226	yes: Shopping websites, forums	It's kind of like the randomized alphanumeral phrase that needs to be entered when signing up for an account to ensure that the user is a real person. By adding an extra step–while somewhat annoying and inconvenience to wait for–helps ensure random accounts are not made using another's identity to commit fraud and so forth.	Somewhat secure	Fairly secure	I hardly noticed it	I could get used to it
231	yes	no benefits	Fairly secure	Fairly secure	I could get used to it	I could get used to it
236	no	I guess it works; it just seems like more trouble for a site people would probably not care enough to break into.	Very secure	Very secure	I hardly noticed it	Hard or slightly annoying
241	yes: lots of them	i dont know	Somewhat secure	Fairly secure	I hardly noticed it	I could get used to it

Group 5 (email without warnings, cut and paste attack): Registration attitudes

			Security of:		**Convenience of:**	
User #	**Used email registration before? If yes, where?**	**Benefits of email registration**	**Passwords + no registration**	**Passwords + email for registration**	**Passwords + no registration**	**Passwords + email for registration**
246	yes: experimetrix (Berkeley psychology labs) and others that I don't remember	It just adds another step in verifying that you are who you say you are and thus helps prevent other people from logging into your account.	Somewhat secure	Very secure	I hardly noticed it	I could get used to it
251	no	makes sure that the person registering is a real person?	Somewhat secure	Fairly secure	I could get used to it	I could get used to it
256	yes: pay pal, ebay	It provides only the user with the password of the email to register their own computer so information cannot be stolen.	Fairly secure	Very secure	I hardly noticed it	I could get used to it
268	yes: Numerous	It forces the person with the e-mail address to confirm their account, you therefore cannot pose as other people. (Or you could only do so with their so-called consent.)	I don't know	I don't know	I don't know	I don't know
271	yes: facebook	I believe that when a person is signed up with an email it not only has to be a real email address but the person has to go to their email and confirm that it is their's. I assume this limits some identity theft.	Fairly secure	Very secure	I hardly noticed it	I could get used to it
276	no	I don't really know	I don't know	I don't know	I hardly noticed it	I hardly noticed it
281	yes: multiple	No response	Somewhat secure	Fairly secure	I hardly noticed it	I hardly noticed it

Group 5 (email without warnings, cut and paste attack): General questions/feedback

User #	Average length of each visit	Anything annoying or difficult?	Engaging or interesting?	General comments
76	0-5 minutes	No	yes	The study saids I have to make predictions for 7 days but I've only made predictions for 4 days and then I'm already completing the exit survey. That means I don't have the chance to make more money by predicting for more days.
81	5-10 minutes	No, I enjoyed it.	yes	Interesting study.
86	0-5 minutes	no	yes	no
91	0-5 minutes	No.	yes	No.
96	0-5 minutes	Nothing.	no	No.
101	No response	no	No response	No response
106	0-5 minutes	No.	yes	No response
111	0-5 minutes	The study said I was going to make 7 predictions and then gave me the exit survey after only 5. That was annoying because I am now worried I won't get credited for completing the whole study.	yes	It was fairly enjoyable and easy to access thanks to its distribution online.
116	5-10 minutes	no	yes	No response
121	5-10 minutes	No response	yes	No response
126	0-5 minutes	no	yes	nope
136	5-10 minutes	No	no	No response
141	0-5 minutes	No.	no	No.
146	0-5 minutes	no	yes	No response
151	0-5 minutes	No response	yes	Great trick.
156	0-5 minutes	Not really, maybe the design of the actual webpage. It looked a little amateur-ish.	yes	I liked predicting movie box office grosses. Movies interest me, so this study was interesting to me, even though it seems to be less about predictions now, and more about Internet security.
161	0-5 minutes	I wanted to base my future predictions on previous data, but that wasn't always available.	yes	It ended a few days earlier than I expected it to.
166	0-5 minutes	No	yes	It was fun trying to guess everyday.
171	0-5 minutes	No.	yes	It was very deceptive.
176	0-5 minutes	The multiple registrations (or was that me being tricked...) was kind of annoying.	yes	Thanks for letting me participate! Hope this helps.
181	5-10 minutes	No response	yes	No response

Group 5 (email without warnings, cut and paste attack): General questions/feedback

User #	Average length of each visit	Anything annoying or difficult?	Engaging or interesting?	General comments
186	5-10 minutes	No response	yes	No response
191	0-5 minutes	no	yes	nope
196	5-10 minutes	No	yes	No response
201	5-10 minutes	No it was very easy.	yes	No response
206	0-5 minutes	No	yes	No response
211	0-5 minutes	Not really.	yes	I didn't make the full 7 predications, but somehow triggered the end of the study anyways. Not sure if this is intended behavior.
216	0-5 minutes	No. I thought predicting high-grossing movies was fun.	yes	no.
221	0-5 minutes	No response	yes	No response
226	0-5 minutes	Waiting for e-mail confirmation was annoying. It didn't say how long to wait for the confirmation, so I was going to wait a few hours until I decided to e-mail you about the problem, but that was cleared up within the hour since you sent an e-mail explaining the website was having server problems in sending out registration e-mails.	yes	So I take it you're not drafting up a set of statistics of how well/badly we're churning out movie predictions. :(
231	0-5 minutes	the registered computer thing.	no	no
236	0-5 minutes	Email registration	yes	No response
241	0-5 minutes	no	yes	no
246	5-10 minutes	Nope, I really liked it.	yes	No response
251	0-5 minutes	no	no	No response
256	0-5 minutes	no, it was very easy	yes	explain that there is a rated order of the movies and it affects how much money you get
268	5-10 minutes	No.	yes	It's easy to look up box office predictions, ratings, and potential forecasts on the internet. Nowhere in the study does it ask a person to refrain. Additionally, newspapers are a good resource and one's own family if they work in the movie industry.
271	5-10 minutes	no	yes	It was difficult to remember that I was signed up for the study. Perhaps consider sending daily reminders to do the study would be beneficial

Group 5 (email without warnings, cut and paste attack): General questions/feedback

User #	Average length of each visit	Anything annoying or difficult?	Engaging or interesting?	General comments
276	0-5 minutes	no	yes	I felt pretty dumb after I'd been duped. I think if there was an obvious way to by-pass the registration at the end I might not have done it but it seemed like I didn't have a choice.
281	0-5 minutes	no	yes	No response