UNIVERSITY OF OREGON
APPLIED INFORMATION MANAGEMENT

Presented to the Interdisciplinary Studies Program:
Applied Information Management and the Graduate School of the University of Oregon
in partial fulfillment of the requirement for the degree of Master of Science

Enhancing Home Computer User Information Security: Factors to Consider in the Design of Anti-phishing Applications

CAPSTONE REPORT

Melinda Geist
Project Manager
Intel Corporation

University of Oregon
Applied Information Management
Program

February 2008

722 SW Second Avenue
Suite 230
Portland, OR 97204
(800) 824-2714

Approved by

_____

Dr. Linda F. Ettinger
Academic Director, AIM Program

Enhancing Home Computer User Information Security:

Factors to Consider in the Design of Anti-phishing Applications

Melinda Geist

Intel Corporation

Abstract

As home computer users increase dependency on the Internet to complete electronic transactions, the need to resolve phishing vulnerabilities in the user interface becomes more urgent (Dhamija & Tygar, 2005a). Selected literature published between 2004 and 2007 is analyzed to provide designers and developers of anti-phishing applications with a set of fundamental user-centered design principles to consider prior to system design and technology solutions selection. The significance of anti-phishing user education is also examined.

Table of Contents

List of Figures and Tables

Literature Review Introduction

Topic Description

As businesses improve their online security infrastructures, attackers are turning to more vulnerable computer system targets: home computer users (Bryant, Furnell, & Phippen, 2007). Most home computer users commonly engage in online tasks that require security, including managing email, banking, and shopping (Whalen & Inkpen, 2005). Phishing, according to Wu, Miller, and Garfinkel (2006), is a technique used to illegally obtain a computer user's credit card, account, and login information. Phishing attacks, where phishers use deceptive emails and fraudulent Web sites to lure users into disclosing their credentials and financial information (Li & Helenius, 2007), have become a significant threat to home computer users (Wu, Miller, & Garfinkel, 2006). As a result, home computer users and the institutions to which they link, such as financial and communications, have become vulnerable to identity theft and financial losses (Dunham, 2004).

Research Problem

The purpose of the study is to identify the fundamental design principles that inform decisions for the development of usable and secure anti-phishing applications. It is designed to assist user interface designers and developers who are not trained in the "field of usability and security" (Garfinkel, 2005, p. 37) also known as HCI-Sec, to create secure and usable anti-phishing applications. User interface designers define computer product user experience and interaction through the practice of user-centered design techniques. Software security features often include graphical user interfaces that are designed to provide users with a clear indication of their

security status (Cranor, 2006). Further, Zurko (2005) believes that the work of user interface designers is significant to the practice of usable security design in that security mechanisms in user interfaces that are unclear or misunderstood by users cannot be effective. Developers are responsible for analysis of technical feasibility, elicitation of functional and non-functional requirements, system design, and implementation. Balfanz, Durfee, Grinter, and Smetters (2004) argue that the selection of hardware and software technologies for secure systems should occur early in the product development process. They go on to say that developers must consider the interplay between usability and security during system design and that security and usability cannot be afterthoughts or added to the product at the end of the project.

Problem Context

Research in the field of human-computer interaction highlights the challenges of balancing security and usability (Whalen & Inkpen, 2005). According to Dourish and Redmiles (2002), significant resources have been applied towards the development of secure computing technologies; however, comparatively small effort is made to ensure integration of secure capabilities in ways that are meaningful to home computer users. Careless disregard for usable security has allowed criminals, such as phishers, to take advantage of poor usability design (Gutmann, Naccache, & Palmer, 2005). Dhamija and Tygar (2005a) assert that “phishing is a model problem for usability concerns in privacy and security because both system designers and attackers battle in the user interface space” (p. 77). As a way to examine the larger topic of user interface design and security for the home computer user, three sub-topics are explored. Each is described briefly below.

Deployment of secure anti-phishing solutions must be based on a solid understanding of current and future threats (Jakobsson, 2005). In addition, Geer (2005) writes that “phishers are improving techniques for making counterfeit Web sites look more realistic and for convincing visitors to enter personal information on them” (p. 20). This component of the review examines selected literature that describes ways attackers leverage the user interface space to achieve their goals of deception and fraud.

A review of the literature in the area of security design and human-computer interaction reveals just how difficult it is to distinguish between secure and unsecure applications. Cranor (2006) states that user research is increasingly highlighting the ineffectiveness of security indicators that are intended to provide users with what they need to securely protect their personal information. This component of the review examines selected literature that describes which principles of human-computer interaction should be considered for the development of usable and secure anti-phishing applications in order to combat the tactics employed by phishers.

Anti-phishing applications that utilize automated methods for detecting phishing attacks will never be 100% effective and users will continue to make trust decisions based on their own knowledge (Sheng et al., 2007). Robila and Ragguci (2006) suggest that technology gains made in the fight against phishing will always be neutralized by new techniques developed by attackers. They go on to say that user education is, and will remain, a significant factor in the battle against phishing. This component of the review examines selected literature that describes principles of learning and human-computer interaction to be applied to the design and

development of complementary user education components that enhance the usability and effectiveness of anti-phishing applications.

Significance

The more dependent home users become on the Internet to complete electronic transactions (also known as e-commerce (U.S. Department of Commerce, 2002)), the more urgent it becomes to resolve phishing vulnerabilities (Dhamija & Tygar, 2005a). Phishing is not only harmful to the e-commerce industry in terms of financial losses due to consumer fear (Parno, Kuo, & Perrig, 2006), loss of reputation (Topkara, Kamra, Atallah, & Nita-Rotaru, 2005), and indirect losses due to increased customer support costs (Emigh, 2005), but more importantly for this study, it reduces trust in the processes and technologies that make it possible (Li & Helenius, 2007). Home users will not engage in electronic commerce if they do not trust the infrastructures that deliver the services to them (Dourish & Redmiles, 2002).

It is common knowledge that most developers are not trained in usability and they have a difficult time creating applications that are both secure and usable (Garfinkel, 2005). Formal methods for the design and development of secure computer applications exist; however, they typically focus on secure capabilities provided by hardware and software technologies alone. Developers often do not consider the needs of users (Flechais, 2005), such as user's knowledge level and usage environment (Kobsa & Schreck, 2003). According to Dhamiha and Tygar (2005), security designers have a long way to go to solve the phishing problem.

Dourish and Redmiles (2002) hypothesize that “a technical infrastructure which makes visible the configuration, activity, and implications of available security mechanisms will enable end users to make informed choices about their behavior, and these informed choices, in turn, will yield more secure system use” (p. 76). They further argue that creating infrastructures that home users can see are trustworthy is a major problem for both the security and human-computer interaction communities. According to Smetters and Grinter (2002), the most efficient way to increase the usability of security applications is to create them from the ground up with visibility and transparency as the prime focus.

Architecture and technology choices made during system design affect the way in which security is delivered to and understood by users (Guttman et al., 2005). When developers are unable to make informed decisions to enable usability in the systems they design, user interface designers are faced with fewer opportunities to create usable solutions. To this end, this inquiry provides developers of anti-phishing applications with a set of theories and fundamental design principles to consider prior to system design and the selection of technology solutions.

Limitations

Parno et al. (2006) write that “the research community and corporations need to make a concentrated effort to combat the increasingly severe economic consequences of phishing” (p. 2). For now, phishing remains a problem that must be solved through the user interface (Miller & Wu, 2005), and user interface designers and developers are in a good position to provide solutions. In fact, Sasse and Flechais (2005) point out that effective design principles must be employed by interface designers in order to increase the usability of secure applications. They go

on to say that developers are often left with the responsibility of making decisions about security in new applications. This study is limited in scope to informing the user interface design and development communities about common traits of phishing attacks and noting principles described in selected literature for user interface design based on evolving threats to home users.

The literature collected for this study is published between 2004 and 2007. Even though the challenges associated with security and usability have been recognized to a limited extent for the past 30 years (Garfinkel, 2005), examination of sources for this inquiry reveals that the focus on usability and security as a research area began in earnest during 2002 (see Search Strategy Report in Research Parameters, section 4). During 2005, Garfinkel describes HCI-Sec "as the newly emergent field of usability and security" (p. 37). Although the first phishing attacks are traced back to 1996, phishing is not considered a large-scale IT threat until 2004 (Abad, 2004).

Literature for this study is selected that directly addresses the area of HCI-Sec and its application to the recent tide of phishing attacks. According to Jakobsson (2005), developers of anti-phishing applications must understand current and future threats posed by phishing in order to deploy successful solutions. In order to do this, factors are considered in three areas. The first goal of this study is to provide user interface designers and developers with knowledge about how phishers attack home users through the computer user interface. The second goal of this study is to provide user interface designers and developers with design principles to enable them to create user interface solutions that better help home users defend themselves against attacks. The third goal of this study addresses the area of user education as a complementary element to anti-phishing applications. This component provides user interface designers and developers with

general learning and human-computer interaction principles necessary to build in visibility and transparency to augment anti-phishing applications with user education that enhances usability and informational security.

Other areas that are not explored but could be logical extensions of this study:

- Underlying technologies that should be used to shape the design of secure and usable anti-phishing applications
- Design research methodology for the development of anti-phishing solutions
- Other tactics for fighting phishing beyond the user interface, such as removal of phishing Web sites (Moore & Clayton, 2007) or visible watermarking (Topkara, Kamra, Atallah, & Nita-Rotaru, 2005)
- Managing phishing from the corporate perspective, such as deployment of customer service strategies to encourage use of online transactions by customers who have been victims of phishing and identity theft in the past

Literature is selected from books, journals, and academic, professional and association Web sites. Academic literature provides theoretical and practical guidance based on user research and case studies. Professional and association literature provides industry examples and perspectives about usable security and phishing. Reference lists from the literature found in these sources include additional material not located using traditional search methods. In addition, searches on names of several researchers cited repeatedly in various articles provide additional literature and reports for the study.

All the literature for this study is reviewed for quality of methods, results, and conclusions based on minimum criteria defined by Leedy and Ormrod (2005):

- Author affiliation, meaning that the author is affiliated with an accredited university or widely considered an industry expert
- Peer review, meaning that the literature is reviewed by experts in the field before publication
- Identification of a clear and focused research problem
- Inclusion of the collection of data, or synthesis of other research in the field
- A set of procedures that can be replicated
- The analysis of data and conclusions by the author that appear logical and valid

Literature that did not meet the defined criteria is not included in the study. White papers and articles from popular magazines are not considered. In addition, the study only includes literature that is available or reproducible in hard copy.

Writing Plan Introduction

A literature review is a written work that critically analyses, summarizes, and provides a synthesis of arguments and ideas held within a published body of knowledge (University of Wisconsin, 2006). Reviewed literature is comprised of research and expert opinion found in academic books and journal articles (Rapple, 2005). Literature reviews are useful for professionals because they provide a comprehensive overview of current research and knowledge in the field (University of North Carolina, n.d.).

The writing plan for the review of selected literature in this study provides an outline of the concepts and ideas that support the research topic. It organizes information contained within the literature around topic themes, and provides a framework that describes relationships among the research (Colorado State University, n.d.). The writing plan organizes the literature for this study into the following three broad categories:

1) Brief summaries of the most common forms of phishing attacks and their expected evolution and future threats, as described in literature by security industry and HCI-Sec experts; and
2) Usability research and the resulting fundamental principles for the user interface design of secure and usable anti-phishing applications; and
3) Usability research and resulting fundamental principles for phishing user education that increases the visibility and transparency of anti-phishing applications and reduces home user susceptibility to phishing.

The writing plan aligns with the “Swiss Cheese” rhetorical pattern as described by Oberzinger (2005). The Swiss Cheese rhetorical pattern presents current knowledge and gaps in the field, and then describes how current research resolves selected problems.

Definitions

The following definitions are organized according to two lexical categories that present common vocabularies used in the fields of anti-phishing and user-centered software design:

- Category 1: Phishing, related techniques, and technologies
- Category 2: Human factors, learning and user-centered design

The purpose of this brief lexicon is two-fold. First, it is intended to enhance understanding of the concepts examined within the body of the literature review. Second, it is intended to improve the communication among members of development teams. According to Bogue (2006), during the course of their work, software development teams often use terms that are obscurely defined and have various meanings to different team members. He goes on to say that the better the teams are able to understand the same language, the less risk there is for wasted time, mistakes, and costly product design and engineering rework.

Category 1: Phishing, Related Techniques, and Technologies

Anti-phishing is concerned with providing a holistic approach towards the fight against phishing, including technological innovation, legislation and law enforcement, industry collaboration, and consumer awareness (Microsoft, 2007).

An **application** is software, or a program, that performs specific tasks and functions, such as word processing, creation of graphics, facilitation of virus scanning, generation and management of email, etc. (Alliance for Telecommunications Industry Solutions [ATIS], 2001). For the

purpose of this study, the definition of application is narrowed to the phishing context and includes software toolbars and Web browser enhancements.

Bots are automated programs used by phishers to scan the Internet and grab email addresses for use in phishing scams. Bots gather email addresses from Web sites, newsgroups, and databases (James, 2005).

A **context aware attack** is a phishing technique in which the victim is manipulated into believing the authenticity of an email. The victim first receives an email that does not request sensitive information, with the goal ensuring that the victim expects a follow up email. The second email, which perpetrates the actual phishing attack, requests the victim's sensitive information (Berghel, Carpinter, & Jo, 2007).

Digital certificates are records that provide security information about an information system (ATIS, 2001). Server certificates vouch for the identity of e-commerce Web sites. They contain details about the Web site, including the owner and domain name. Certificate authorities (CA), such as VeriSign, guarantee the truth and accuracy of information stated within the certificate (Goleniewski, 2003).

Domain names are user-friendly names associated with IP addresses. For example, "antiphishing.org" is the friendly name for the IP address 208.254.36.103 (Lininger & Vines, 2005).

Hackers are people who are knowledgeable about computers and enjoy breaching security mechanisms in order to break into them (Lininger & Vines, 2005).

HTTP is the Hypertext Transfer Protocol. HTTP enables the use of hyperlinks on the Web. It is the standard mechanism for the transfer of documents between servers and personal computers (Goleniewski, 2003). Most e-commerce Web sites use HTTPS (HTTP over SLL) for online transactions (Milletary, 2005).

An **IP Address** is the 32-bit numeric address of a computer device that uses the Internet (Goleniewski, 2003). The current IP address format is four groups of numbers separated by periods. One part of the address represents the network from which the device is connected. The other part of the address represents the specific device within the network (ATIS, 2001).

JavaScript is coding on Web sites that can be used to modify the behavior of the browser and operating system without breaching browser security policies (Lininger & Vines, 2005). JavaScript is commonly used in pop-up phishing attacks (James, 2005).

Key logging is the technique of recording keystrokes entered by users in order for attackers to gain access to user credentials. Key loggers utilize various technologies, including browser objects that collect the information from targeted Web sites, and keyboard and mouse drivers that monitor user activities (Emigh, 2005).

Malware is any form of malicious software and includes viruses, worms and Trojans. Malware-based phishing attacks begin by installing and running malicious code on the user's computer. Malware steals confidential information stored on the computer, such as passwords, software activation keys, and sensitive email and transmits the information to the attackers over the Internet (Emigh, 2005).

A **mule** is someone who sets up accounts used for laundering money collected through phishing scams. Typically, mules are caught and arrested but phishers remain undiscovered. Mules work on commission, skimming 5-7% off of phishing profits (Lininger & Vines, 2005).

A **man-in-the-middle attack** is a form of phishing in which the attacker is positioned between the user and a legitimate Web site. Messages intended for a legitimate Web site are intercepted by the attacker, who collects valuable information and then passes the message on to the legitimate site. Responses from the legitimate Web site are also intercepted before they are forwarded on to the user (Emigh, 2005).

An **online security infrastructure** consists of technologies, tools, and strategies employed to protect the network perimeter and internal resources of an enterprise. Typically, a security infrastructure is managed by IT and includes firewalls, intrusion detection and prevention, anti-virus protection, security for wireless and mobile devices, and encryption technologies (Gartner, 2003).

Phishing is a technique used to illegally obtain personal information from computer users. Phishing is typically executed using spoofed, but legitimate-looking emails and Web sites. Another phishing tactic includes tricking users into downloading malicious software which searches computers for personal information and then transmits it to attackers over the Internet (Wu et al., 2006). The term is a derived from the word “fishing” because phishing lures victims into providing their personal information. The exchange of the letter “f” for “ph” is a hacker convention (e.g., hacking is sometimes referred to as phreaking) (Berghel et al., 2007). A phishing attack is considered successful if the user unknowingly submits his personal information to the attacker (Wu, Miller, & Little, 2006).

Session Hijacking is an attack technique that is deployed after a victim logs into an account or initiates a transaction. In some cases, malware perpetrates malicious actions once the user is authenticated. Other hijacking attacks utilize the man-in-the-middle technique (Emigh, 2005).

Secure Socket layer (SSL) provides a secure, encrypted Internet connection between the user’s browser and the Web server (Milletary, 2005). With SSL, information can move across the Internet without being intercepted or modified (University of Washington, Computing & Communications, 2007). Most e-commerce Web sites use HTTPS (HTTP over SLL) for online transactions (Milletary, 2005).

Spam is unsolicited email that is sent in bulk over the Internet (Lininger & Vines, 2005).

Spear phishing is an attack technique whereby an email that appears to be legitimate is sent to all employees of a specific company or government agency, or to all members of an organization. The message appears to have been sent by the employer or a company employee. Spear phishing attacks attempt to gain login information as the means to access a company's computer system (Binational Working Group on Cross-Border Mass Marketing Fraud, 2006).

Spoofing is the act of impersonating something, whether by looking identical to it or by pretending to have come from the same source. Phishing is sometimes referred to as spoofing (Lininger & Vines, 2005).

A **trojan** is a malicious software program that pops up and displays over login screens. The user mistakenly enters credentials into the trojan screen, which stores the information on the computer locally. The trojan then transmits the credential information to the attacker for misuse (Emigh, 2005).

A **URL** (uniform resource locator) describes the access method and location of a resource on the Internet. For the URL https://www.shopping.com, https indicates the access method (HTTP over SSL); www.shopping.com describes the location of the server that hosts the Web site (ATIS, 2001).

URL obfuscation is a technique used to trick users into believing a Web site is legitimate. The legitimate Web site URL is displayed to the user in plain text, or even as a graphic, but the actual link navigates users to a phishing Web site using a different URL address (Berghel et al., 2007).

A **virus** is a malicious software program that attaches itself to other applications that are shared among computer systems. Viruses replicate themselves and are typically destructive to the executable applications that they infect. They leave no clear signs of their existence (ATIS, 2001).

A **worm** is a malicious software program that replicates itself and spreads over a computer network. Typically, worms create disruptive effects, such as using up system resources and shutting it down (U.S. Computer Emergency Readiness Team, 2002).

Category 2: Human Factors, Learning and User-centered Design

Agents are illustrated characters that are used for interactive training. Agents guide the user through story-based learning tasks (Sheng et al., 2007).

An **attacker** is an enemy who carries out an attack against a victim (Allen, 2000). Phishing attackers trick their victims into disclosing credentials, credit card information, account numbers, and then use the information gained through the attack to commit identity theft and fraud (Dhamija & Tygar, 2005a). A phishing attack is considered successful if the user unknowingly submits their personal information to the attacker (Wu, Miller, & Little, 2006).

Browser chrome refers to the perimeter of the Web browser window and includes the borders, scroll bar, menus, and toolbars (PC Magazine, n.d.).

A **call to action** is a common marketing tactic used to entice consumers to go somewhere to read a message related to a brand, or to learn more about a potential threat to their own well-being (Steinberg, 2005). In a typical phishing scenario, the attacker sends email to potential victims with a “call to action” that demands that recipients click on a link. For example, the email may state that there is a problem with the recipient’s bank account, or that a new service is being offered at the financial institution which includes a limited-time option for free services (Emigh, 2005).

Credentials establish the identity of the user and are passed from one entity to another for the purpose of determining access rights. Credentials can include user name, password, social security number, account numbers, mother’s maiden name, and bio-metric parameters such as fingerprint or voiceprint (ATIS, 2001).

e-Commerce is concerned with using the Internet to conduct real-time business transactions. Tasks in e-commerce transactions often include browsing a Web site for products, selection of products to purchase, and then payment. The customer and retailer are typically located in different geographies and operate without prior arrangement or agreements (U.S. Department of Commerce, 2002).

Embedded training is a user training methodology whereby the training is integrated into the software application in a way that it is part of the user’s primary task (Kumaraguru, Sheng, et al., 2007).

Financial information is *personally identifiable* information that customers provide to financial institutions in order to acquire financial products and services. In addition, financial institutions may obtain other financial information from customers during the process of providing products or services to them (Federal Deposit Insurance Corporation, 2000).

HCI-Sec (or HCISEC) combines the disciplines of human-computer interaction and computer security (Long, Moskowitz, & Ganger, 2003). Garfinkel (2005) defines HCISEC as the "field of usability and security" (p. 37).

Home computer users are characterized as people who purchase computers and software primarily for home use. They are typically seen as computer-phobic. Office workers who bring work home are not classified within the home computer user profile (Winograd, 1996).

Human-computer interaction (HCI) is a well-established discipline that focuses on identification and resolution of conflicting technical and usability goals that are typical in computer systems. HCI professionals are essentially concerned with the usability of computer systems and how human factors shape the way in which people react to them (Flechais, 2005).

Human factors, according to Flechais (2005), are the "intrinsic properties of people, such as short-term memory, visual acuity, and physical dexterity" in terms of the way in which they relate to the underlying model of how a computer system operates (p. 22).

Identity theft is the use of information obtained through mechanisms such as phishing in order to use another person's identity. Typically, identity theft is the means to gain unlawful access to finances (Berghel et al., 2007).

Information privacy is concerned with an individual's ability to exercise control over the use of his personally identifiable information. Codes of fair information practice state that individuals must consent to the use of their information and that the information must only be used for the purpose for which it was collected (Regan, 2005).

Information security is concerned with the prevention of unauthorized access or modification of information during processing, transit, and storage. Information security threats are mitigated through administrative and technical countermeasures (ATIS, 2001).

Learning principles are used to identify opportunities for improved training solutions. They represent decades of research about learning and present a condensed understanding of current theory (University of Pittsburgh, Institute for Learning, n.d.).

Personal information that is obtained through Internet attacks typically includes the following: name, address, phone number, date of birth, social security number (SSN), and bank or credit card account numbers (Privacy Rights Clearinghouse, 2005).

Pop-up windows are initiated by Web pages using script technologies and are commonly used to display extra information to users. Typically, pop-up windows do not have a Web address bar (Lininger & Vines, 2005).

Social engineering is concerned with email schemes used to lure recipients to counterfeit Web sites where they are tricked into revealing login credentials, credit card numbers, and financial account numbers. Social engineering attackers leverage the brand names of banks, retailers and credit card companies to convince their victims to respond (Anti-Phishing Working Group, 2007).

A **task** is a user activity that is carried out in order to achieve a goal. For example, the task of reading email is concerned with the goal of managing email (Stone, Jarrett, Woodroffe, & Minocha, 2005). Gross and Rosson (2007) describe tasks as "goal-directed, bound by time and activity, and process oriented" (p. 3).

Transparency is the visibility of the internal workings of a system that enables users to develop an accurate mental model of its function and use (Soegaard, 2005).

Usability concentrates on a predefined set of software characteristics, including learnability (how easy it is to learn), efficiency (how efficient it is with which to complete desired tasks), and whether the software is inherently pleasing to the user (Li & Helenius, 2007)**.**

User-centered security refers to software applications, security models, components, and systems that are motivated by usability as the dominant goal (Zurko & Simon, 1996).

User feedback is visual, auditory, or tactile information that confirms results or indicates that a user or system action is completed. Visual feedback is accomplished through text or flashing alerts; auditory feedback can include computer sounds, such as beeps or key clicks; tactile feedback occurs when the user presses a user interface button (Stone et al., 2005).

The **user interface** is the layer of the computer system through which users carry out their tasks and achieve their goals. Stone et al. (2005) define the user interface as "the bridge between the world of the computer system and the world of the user. It is the means by which the computer reveals itself to the user and behaves in relation to their needs" (p. 627).

User interface design principles include generic guidance for designing usable user interfaces. One example of a design principle is "be generic." User interface design principles must be interpreted by the designer in accordance with the requirements of the project (Stone et al., 2005).

Warnings are displayed to users by applications when an unexpected condition is detected. Situations that are difficult for users to understand are typically clarified through warning messages (Flinn & Stoyles, 2005).

Research Parameters

This section provides the framework and methods in which the literature review is conducted. The search strategy for the study is described in detail, including the search terms, databases, and search engines used to find and collect literature. The documentation approach details the tools and methods used to record all information captured in relation to the study. Criteria for the evaluation and selection of materials are conveyed in terms of relevance to the topic and audience, and quality. Then, a writing plan is introduced that describes how selected literature is synthesized and presented in the Review of the Literature.

Search Terms

References for the literature review are collected using the search terms and controlled vocabularies listed below. Search terms are then mined from the analysis of literature found during initial searches.

Key search terms.

- Usable security
- Phishing
- Interface design
- Computer

Subtopic search terms.

Subtopic A: How phishers leverage user interfaces for attacks, and future threats

- Phishing attack

- Anti-phishing
- Spoofing

Subtopic B: Theories and fundamental design principles for anti-phishing applications

- Usability
- User-centered security
- HCISEC
- Visualization
- End-user threat

Subtopic C: Phishing user education and its impact on the usability and success of anti-phishing applications

- Learning
- Training
- User help
- Online help

Literature Collection

Literature is collected from books, journals, conference proceedings, government research reports, and Web documents found at public and university libraries and through keyword searches conducted using the indexes, search engines, and Web sites listed below. The selected search engines, indexes, and Web sites provide results that meet the literature quality and relevance criteria for this study. Additional resources are mined from bibliographies provided in the literature. In cases where potentially relevant literature is listed in bibliographies and URLs

are unavailable, the Yahoo! and Google Scholar search engines are used to locate a source for material. In addition, author-specific searches are conducted for influential authorities mentioned repeatedly, including Cranor, Dhamija, Garfinkel, Tygar, and Jakobsson using the Google Scholar search engine.

Search engines and databases.

- ACM Digital Library
- Alexandria Computing Center Documents
- CiteSeer Scientific Literature Digital Library
- EBSCO HOST Research Databases – Academic Search Premier index
- FirstSearch Electronic Collections Online
- Google CiteSeer search engine/index
- Google Scholar search engine
- IEEE Computer Science Digital Library
- Library of Congress
- OneSearch QuickSets / Sciences database
- Summit Union Catalog
- UO Libraries Catalog
- Web of Science index
- WorldCat index

Professional and organizational Web sites.

- Anti-phishing Working Group (www.antiphishing.org)
- Carnegie Mellon University Usability and Privacy Laboratory (cups.cs.cmu.edu)

- The Federal Trade Commission (www.ftc.gov)
- U.S. Department of Commerce (www.commerce.gov)

Journals.

- Communications of the ACM
- Computer Fraud and Security
- Interactions
- Journal of Computer Virology
- Transactions of Computer-Human Interaction

Documentation Approach

References and research notes for the study are documented using several methods which comprise a holistic approach to effectively capture and organize collected materials.

Search records are documented using Microsoft® Word in tabular format (*see next section below*). This method affords a complete view of search activities and the means to quickly assess which search engines, databases, and search terms achieve the best results.

- All references and associated bibliographic information are captured in an electronic database using the EndNote® software tool. This method provides the ability to quickly capture abstracts and other bibliography detail, and to conveniently sort references by author or title. In addition, the EndNote tool is configured to auto-generate the full bibliography in the correct academic format.
- Electronic copies of each reference are collected and categorized, then saved to computer folders that are organized by main topic and subtopics. Materials that are

eliminated after initial analysis are posted to a separate folder. Hard copies of all materials are created and stored in a three-ring binder in preparation for note taking. The electronic copies facilitate keyword searching within each reference or group of references, if necessary.

- Notations of information from each reference are recorded on note cards. Once all references are read, the note cards are organized into categories according to the writing plan. The note cards follow the format recommended by Leedy and Ormrod (2005) and include:
    - Serial number, which identifies the reference
    - Bibliographic information not previously captured
    - Page number
    - How the content item relates to the research problem
    - Content of the source. If the idea is not para-phrased, quotation marks indicate that the content item is a direct quote

Search Strategy Summary

Table 4, Detailed Record of Searches (located in Appendix A: Search Record) illustrates searches and results, and the rationale for excluding certain keyword terms. Categories of information included in Table 4 are:

- **Database / Search Engine** – the resources used in the search
- **Search Terms** – keywords based on the topic and subtopics and how the keywords and terms were configured within search fields (e.g., simple search versus Boolean logic)

- **Number of Search Results** – the number of documents yielded from each search
- **Number of Eligible Titles Found** – the number of titles found that were relevant and considered for inclusion in this study
- **Comments** – rationale for continuing with or abandoning specific search engines, databases, and search terms

Searches of the ACM Digital Library, the Worldcat index, and using the Google CiteSeer and Google Scholar search engines yielded the best sets of results that were of high relevancy and quality. Results found from searches of the CiteSeer Scientific Digital Library, IEEE Computer Science Digital Library, the Web of Science index, and of the OneSearch Quicksets / Sciences database were assessed as good, with a considerable number of references found of adequate quality. Searches on topic keywords using the EBSCO HOST Research database – Academic Search Premier index, FirstSearch Electronic Collections Online, the Summit Union Catalog, and of the UO Libraries Catalog produced only fair results; however, these resources were deemed worthy of continued investigation because they yielded at least one or more usable articles. Several other search engines and databases were abandoned because search results were redundant with other more productive resources, or search results were consistently inadequate. Summary of search results for databases, search engines, and professional Web sites is presented in Tables 1 and 2 below.

Table 1: Summary of Database and Search Engine Results

Database/ Search Engine	**Eligible Titles Found**
ACM Digital Library	76
Alexandria Computing Center Documents	0
CiteSeer Scientific Literature Digital Library	10
EBSCO HOST Research Databases – Academic Search Premier Database	5
FirstSearch Electronic Collections Online	2
Google CiteSeer Search Engine/Index	26
Google Scholar Search Engine	29
IEEE Computer Science Digital Library	14
Library of Congress	8
OneSearch Quicksets / Sciences	11
Summit Union Catalog	6
UO Libraries Catalog	0
Web of Science Index	15
WorldCat Index	24

Table 2: Summary of Professional and Association Web Site, and Online Publication Results

Professional/Association Web Sites and Online Publications	**Eligible Titles Found**
Anti-phishing Working Group (antiphishing.org)	1
Carnegie Mellon University Usability and Privacy Security Laboratory (cups.cs.cmu.edu)	7
The Federal Trade Commission (www.ftc.gov)	1
U.S. Department of Commerce (www.commerce.gov)	1

Literature Evaluation and Selection Criteria

All found literature was previewed for relevancy and quality by scanning the abstract, the introduction, headings, tables and figures, conclusions, and the reference lists. An initial assessment of any omissions, lack of detail, errors, and the depth of the reference list provided an initial impression of relevancy and quality (Hewitt, 2002). If the material was deemed acceptable, a more in-depth analysis of the literature continued as described below. Literature sources are analyzed for quality using Cornell University Library guidelines (Ormondroyd, Engle, & Cosgrave, 2004), University of Oregon guidelines (Bell & Smith, 2007), and criteria outlined by Hewitt (2002).

Relevance.

Literature is evaluated for relevancy by considering whether it addresses the research question (Bell & Smith, 2007), adds new information to the study, or validates materials previously collected (Ormondroyd et al., 2004). Although collected literature includes material that both extensively and marginally covers the topic to establish a variety of viewpoints, in order to focus this study, literature that covers deep-dive technical concepts, password management, and corporate phishing defense mechanisms is purposely excluded. Primary sources include books, journal articles, and conference proceedings written by scientists reporting the results of their research. Secondary sources are written by scholars interpreting the findings provided in various primary sources (Ormondroyd et al., 2004). The area of study related to the topic is evolving and under rapid development (Ormondroyd et al., 2004). As such, the literature collected for the study is published between 2004 and 2007.

Author.

Biographic information for each author is examined to assess educational and other experience within the topic area, and institutional affiliation. Material that reflects the values or goals of other authorities, such as corporations funding research or government organizations with a vested interest in specific outcomes, is not included in the study (Bell & Smith, 2007). In some cases, the reputation of the author's work is evident because it is frequently cited by other scholars (Bell & Smith, 2007; Ormondroyd et al., 2004). Research on the topic conducted by Cranor, Dhamija, Tygar, Jakobsson, Wu, and Yee are particularly relevant and prolific.

Publisher.

Publishers are evaluated for their offerings of scholarly materials of known quality. Literature included in this study is published by scholarly journals, universities, and other reputable institutions. Popular journals and industry white papers are excluded. Journal editorial guidelines and peer review processes are examined to ensure literature is critically reviewed prior to publication (Ormondroyd et al., 2004). In some cases, however, literature that may not be peer reviewed by an editorial board is included if the work is cited repeatedly by other authorities in the field.

Audience.

The literature collected for this study is limited to material intended to address scholarly and professional audiences (Ormondroyd et al., 2004). The material written for scholarly and professional audiences provides the appropriate level of information to inform the design and development decisions of user interface designers and developers. Advanced technical sources are not included because underlying phishing technology is beyond the scope of this study.

Furthermore, material intended to directly educate home users about the dangers of phishing is not included because this information would not meet the specific needs of the intended audience of this study.

Reasoning and writing style.

Information provided in the literature covers facts, not propaganda (Bell & Smith, 2007). Facts are supported by evidence, and assumptions are critically evaluated and deemed reasonable (Ormondroyd et al., 2004). Authors are impartial and the literature does not contain emotionally-charged or bias language (Bell & Smith, 2007; Ormondroyd et al., 2004). The literature for this study is evaluated to ensure that it is logically organized, arguments are clearly presented, and that the purpose of the research is well-defined and meets its stated objectives. Furthermore, all material is examined to verify that no arguments presented by the authors are repetitive (Ormondroyd et al., 2004) in order to appear more convincing than the stated results of their research.

Research methodology.

The research methodologies introduced in the literature are described in enough detail that techniques can be assessed for validity. The presentation of results is consistent with the data, and all potential interpretations are accounted for (Bell & Smith, 2007). Material and facts that radically depart from the other collected literature are carefully scrutinized for accuracy (Ormondroyd et al., 2004).

Writing Plan

The study outline is organized to examine the context of why phishing attacks are successful, and then prescribes design principles intended to combat phishing in the user interface space. Furthermore, it specifies learning principles and techniques that can be important to the over all success of anti-phishing solutions, so that education of the user is not simply a matter of default. According to Jakobsson (2005), the development of successful security solutions is dependent on a clear understanding of current and future threats. To this end, the review of literature begins by examining current phishing techniques and anticipated risks.

Dhamija et al. (2006) write that "…a usable design must take into account what humans do well and what they do not do well" (p. 590). Phishing is successful when users are fooled into assigning inaccurate meaning to content and unknowingly take actions that are inconsistent with their intentions (Miller & Wu, 2005). Downs, Holbrook, and Cranor (2006) state that a clear understanding of why people fall for phishing attacks must be established before user interfaces can be evaluated for susceptibility to them. To lay the foundation for design strategies and principles inherent to successful anti-phishing solutions, the review of literature reveals the human weaknesses that make people susceptible to phishing attacks.

The rapid growth and burden of phishing attacks has been a significant catalyst for academic and industry anti-phishing research (Topkara et al., 2005). The goal of ongoing research is to foster the deployment of robust and usable systems (Dhamija & Tygar, 2005a). Guiding principles and strategies can bring attention to system vulnerabilities and strengthen the design of security measures (Yee, 2005). They can advise the development of tools to help home computer users

protect themselves against phishing attacks (Downs et al., 2006). The review of literature will synthesize foundational knowledge and user research to reveal a set of principles that can be used in the design and development of successful anti-phishing solutions.

While technology and design address many aspects of the phishing problem, user education is also a significant contributor to the solution (Robila & Ragucci, 2006). Kumaraguru, Rhee, Acquisti, et al. (2007) argue that anti-phishing training should be provided to complement the functions of anti-phishing applications. Furthermore, Downs et al. (2007) state that "knowledge and experience predict behavioral responses to phishing attacks in ways that support the idea that better understanding can help to thwart phishing attacks." To augment user interface design strategies and principles, the review of literature analyzes and synthesizes learning principles and human-computer interaction that is concerned with the development of user education for anti-phishing applications.

The writing plan for the review of the literature is presented below, and aligns with the "Swiss Cheese" rhetorical pattern presented by Obenzinger (2005). In accordance with this format, the review of literature presents current knowledge and unresolved problems within the field, and then demonstrates how current research resolves open issues (Obenzinger, 2005).

Topic: Enhancing Home User Information Security: Factors to Consider in the Design of Anti-phishing Applications

1. **Attack methods phishers use, and future threats**

   Analyze and describe the anatomy of phishing from review of literature in Category 1 of the Literature Review Bibliography. *Review and summary of*:

   1.1. Literature that examines common types of phishing attacks

      1.1.1. Impersonation attack

      1.1.2. Pop-up attack

   1.2. Literature that addresses the execution method of phishing attacks

      1.2.1. Steps in a typical phishing attack

      1.2.2. Setting up the attack

      1.2.3. Post-attack activities

   1.3. Literature that examines phishing participants

      1.3.1. Who are phishers?

      1.3.2. Who do phishers target?

   1.4. Literature that examines anticipated future threats

      1.4.1. Context aware phishing

      1.4.2. Malware

2. Fundamental user interface design principles for anti-phishing applications

Analyze and describe human vulnerabilities and resulting user-centered design principles for anti-phishing applications based on review of literature in Category 2 of the Literature Review Bibliography. *Review and summary of*:

2.1. Literature that examines why home computer users fall for phishing attacks

2.1.1. Brief overview of user studies from the literature

2.1.2. Lack of knowledge

2.1.3. Visual deception

2.1.4. Lack of attention

2.2. Literature that examines anti-phishing application approaches and goals

2.2.1. Anti-phishing application approaches

2.2.2. Problems with browsers

2.2.3. Goals for anti-phishing applications

2.3. Literature that examines user-centered design principles for anti-phishing solutions

2.3.1. Security warnings

2.3.2. Layout and visual design

2.3.3. Security indicators

2.3.4. Trust indicators

2.3.5. User effort

2.3.6. Use of technology in securing the user interface

3. Phishing user education and its impact on the usability and success of anti-phishing applications

Analyze and describe the principles of learning and human-computer interaction for the development of user education designed to compliment and enhance the effectiveness of anti-phishing applications based on review of literature in Category 3 of the Literature Review Bibliography. *Review and summary of*:

3.1.1. Impacts of phishing user education

3.1.2. Learning and user-centered design principles for integration of user education into anti-phishing applications

3.1.3. Knowledge areas that best help home users avoid falling for phishing scams

Review of the Literature Bibliography

This annotated bibliography presents 32 specific references selected for the Review of the Literature. References represent current knowledge about phishing techniques, the threats anticipated in the future, and the results of qualitative and quantitative user studies intended to help contribute solutions to the anti-phishing effort. Annotations consist of the abstract published with the reference. Literature are grouped into three main categories, aligning with the top level of the outline defined in the Writing Plan:

- Category 1: How phishers leverage user interfaces for attacks, and future threats (includes 10 references)
- Category 2: User interface design of anti-phishing applications (includes 17 references)
- Category 3: Phishing user education and its impact on the usability and success of anti-phishing applications (includes 5 references)

Category 1: How Phishers Leverage User Interfaces for Attacks, and Future Threats

Berghel, H., Carpinter, J., & Jo, J.-Y. (2007). Phish Phactors: Offensive and Defensive Strategies. *Advances in Computers, 70*, 223-268. Retrieved November 3, 2007, from Web of Science database.

ABSTRACT: Phishing attacks attempt to fraudulently solicit sensitive information from a user by masquerading as a known trustworthy agent. They commonly use spoofed emails in association with fake websites in order to coerce a user into revealing personal financial data. Phishing is now a serious problem with criminals adopting the well-developed and well-known techniques to exploit Internet users with sophisticated attacks. Phishers are known to have successfully attacked an estimated 1.2 million users and stolen an estimated US$929 million in the twelve months to May 2005.

This chapter aims to provide the current status of phishing attack techniques and defense methods. We first provide an overview of the fundamental phishing techniques for delivering a successful attack, such as bulk emailing, fake websites and detection avoidance using a variety of obfuscation techniques. We then survey more sophisticated methods that may deceive even knowledgeable and vigilant users. These techniques do not rely on naive email users and simple websites, but use highly realistic fake websites, generic hacking techniques (such as DNS poisoning or cross site scripting) or actively exploit browser vulnerabilities. For example, a Man-In-The-Middle attack or the use of DNS poisoning can easily fool even an advanced user who may be aware of phishing attacks.

Chou, N., Ledesma, R., Teraguchi, Y., Boneh, D., & Mitchell, J.C. (2004). *Client-Side Defense Against Web-Based Identity Theft.* Paper presented at the 11th Annual Network and Distributed System Security Symposium, San Diego, CA. Retrieved November 17, 2007, from http://www.isoc.org/ndss04/proceedings/Papers/Chou.pdf

ABSTRACT: Web spoofing is a significant problem involving fraudulent email and web sites that trick unsuspecting users into revealing private information. We discuss some aspects of common attacks and propose a framework for client-side defense: a browser plug-in that examines web pages and warns the user when requests for data may be part of a spoof attack. While the plugin, SpoofGuard, has been tested using actual sites obtained through government agencies concerned about the problem, we expect that web spoofing and other forms of identity theft will be continuing problems in coming years.

Dhamija, R., & Tygar, J. D. (2005b). Phish and HIPs: Human Interactive Proofs to Detect Phishing Attacks. In H. S. Baird and D. P. Lopresti (Eds.), *Second International Workshop on Human Interactive Proofs* (pp. 127-141). Springer-Verlag Berlin Heidelberg. Retrieved November 19, 2007, from University of California, Berkeley, College of Engineering Web site: http://www.cs.berkeley.edu/~tygar/papers/Phishing/Phish_and_HIPs.pdf

ABSTRACT: In this paper, we propose a new class of Human Interactive Proofs (HIPs) that allow a human to distinguish one computer from another. Unlike traditional HIPs, where the computer issues a challenge to the user over a network, in this case, the user issues a challenge to the computer. This type of HIP can be used to detect phishing attacks, in which websites are spoofed in order to trick users into revealing private information. We define five properties of an ideal HIP to detect phishing attacks. Using these properties, we evaluate existing and proposed anti-phishing schemes to discover their benefits and weaknesses.

We review a new anti-phishing proposal, Dynamic Security Skins (DSS), and show that it meets the HIP criteria. Our goal is to allow a remote server to prove its identity in a

way that is easy for a human user to verify and hard for an attacker to spoof. In our scheme, the web server presents its proof in the form of an image that is unique for each user and each transaction. To authenticate the server, the user can visually verify that the image presented by the server matches a reference image presented by the browser.

Emigh, A. (2005). *Online Identity Theft: Phishing Technology, Chokepoints and Countermeasures*. Retrieved November 19, 2007, from http://www.antiphishing.org/Phishing-dhs-report.pdf

ABSTRACT: Phishing is online identity theft in which confidential information is obtained from an individual. Phishing includes deceptive attacks, in which users are tricked by fraudulent messages into giving out information; malware attacks, in which malicious software causes data compromises; and DNS-based attacks, in which the lookup of host names is altered to send users to a fraudulent server.

The Gartner group estimates that the direct phishing-related loss to US banks and credit card issuers in 2003 was $1.2 billion. Indirect losses are much higher, including customer service expenses, account replacement costs, and higher expenses due to decreased use of online services in the face of widespread fear about the security of online financial transactions. Phishing also causes substantial hardship for victimized consumers, due to the difficulty of repairing credit damaged by fraudulent activity.

This report examines the information flow in phishing attacks of all types. Technologies used by phishers are discussed, in combination with countermeasures that can be applied. The focus is primarily on technology that can be deployed to stop phishing. Both currently available countermeasures and research-stage technologies are discussed.

Jakobsson, M. (2005). *Modeling and Preventing Phishing Attacks*. Retrieved November 13, 2007, from Indiana University, School of Informatics Web site: http://www.informatics.indiana.edu/markus/papers/phishing_jakobsson.pdf

ABSTRACT: We introduce tools to model and describe phishing attacks, allowing a visualization and quantification of the threat on a given complex system of web services. We use our new model to describe some new phishing attacks, some of which belong to a new class of abuse introduced herein: the context aware phishing attacks. We describe ways of using the model we introduce to quantify the risks of an attack by means of economic analysis, and methods for defending against the attacks described.

Jakobsson, M., Young, A. (2005). Distributed Phishing Attacks. *Cryptology ePrint Archive, Report 2005/09*. Retrieved November 22, 2007, from http://eprint.iacr.org/2005/091.pdf

ABSTRACT: We identify and describe a new type of phishing attack that circumvents what is probably today's most efficient defense mechanism in the war against phishing, namely the shutting down of sites run by the phisher. This attack is carried out using what we call a distributed phishing attack (DPA). The attack works by a per-victim personalization of the location of sites collecting credentials and a covert transmission of credentials to a hidden coordination center run by the phisher. We show how our attack can be simply and efficiently implemented and how it can increase the success rate of attacks while at the same time concealing the tracks of the phisher. We briefly describe a technique that may be helpful to combat DPAs.

James, L. (2005). *Phishing Exposed*. Rockland, MA: Syngress Publishing.

ABSTRACT: Phishing Exposed provides an in-depth, high-tech view from both sides of the phishing playing field. In this unprecedented book, world-renowned phishing expert Lance James exposes the technical and financial techniques used by international clandestine phishing gangs to steal billions of dollars every year. The book is filled with technically detailed forensic examinations of real phishing schemes. Armed with this invaluable intelligence, law enforcement officers, system administrators, and fraud investigators can resolve existing cases and prevent future attacks.

Lininger, R., & Vines, R.D. (2005). *Phishing: Cutting the Identity Theft Line*. Indianapolis: Wiley Publishing.

ABSTRACT: They don't just want you to know who you are, they want to BE who you are. By duplicating a legitimate website, phishers can convince you that email asking for your personal information came from your bank, an online retailer, even your ISP. Their high-tech identity theft costs American consumers and businesses billions, and if you access the Internet, you're a target. Whether you manage corporate security or just shop online, this book is loaded with weapons you can't afford to be without.

Moore, T., & Clayton, R. (2007). *An Empirical Analysis of the Current State of Phishing Attack and Defence*. Retrieved November 18, 2007, from University of Cambridge, Computer Laboratory Web site: http://www.cl.cam.ac.uk/~rnc1/weis07-phishing.pdf

ABSTRACT: Banks and other organisations deal with fraudulent phishing websites by pressing the hosting service providers to remove the sites from the Internet. Until they are removed, the fraudsters will learn the passwords, personal identification numbers (PINs)

and other personal details of the users who are fooled into visiting them. We analyse empirical data on actual phishing website removal times and the number of visitors that the websites attract, and conclude that website removal is part of the answer to phishing, but it is not fast enough to completely mitigate the problem. We also identify a subset of phishing websites (operated by the `rock-phish' gang) which through architectural innovations have extended the average lifetime of their phishing websites.

Parno, B., Kuo, C., & Perrig, A. (2006). Phoolproof Phishing Prevention. In G. Di Crescenzo and A. Rubin (Eds.), *Tenth International Financial Cryptography and Data Security Conference* (pp. 1-19). IFCA/Springer-Verlag Berlin Heidelberg. Retrieved November 4, 2007, from the Web of Science database.

ABSTRACT. Phishing, or web spoofing, is a growing problem: the Anti-Phishing Working Group (APWG) received almost 14,000 unique phishing reports in August 2005, a 56% jump over the number of reports in December 2004 [3]. For financial institutions, phishing is a particularly insidious problem, since trust forms the foundation for customer relationships, and phishing attacks undermine confidence in an institution.

Phishing attacks succeed by exploiting a user’s inability to distinguish legitimate sites from spoofed sites. Most prior research focuses on assisting the user in making this distinction; however, users must make the right security decision every time. Unfortunately, humans are ill-suited for performing the security checks necessary for secure site identification, and a single mistake may result in a total compromise of the user’s online account. Fundamentally, users should be authenticated using information that they cannot readily reveal to malicious parties.

Placing less reliance on the user during the authentication process will enhance security and eliminate many forms of fraud. We propose using a trusted device to perform mutual authentication that eliminates reliance on perfect user behavior, thwarts Man-in-the-Middle attacks after setup, and protects a user’s account even in the presence of keyloggers and most forms of spyware. We demonstrate the practicality of our system with a prototype implementation.

Category 2: Fundamental Design Principles for Anti-Phishing Applications

Camenisch, J., Shelat, A., Sommer, D., & Zimmerman, R. (2006). Securing User Inputs for the Web. *Proceedings of the Second ACM Workshop on Digital Identity Management, USA*, pp. 33-44. Retrieved October 28, 2007, from ACM Digital Library.

ABSTRACT: The goal of this paper is to study secure and usable methods for providing user input to a website. Three principles define security for us: certification, awareness, and privacy. Four principles define usability: contextual awareness, semantic awareness, prodigious use of screen space, and the availability of recommended choices. We first describe how current approaches to the solicitation of user input on the web fail on both fronts: they either can not handle certified data, do not respect user privacy, or have various usability problems which frustrate and perhaps even mislead the user.To address security, we suggest the use of more sophisticated private certificate systems. To address usability, we propose a new contextual, browser-integrated interface for using private certificate systems. Our system incorporates many recent design principles discussed in the security and usability space. It works in the main content area of a webpage; it focuses on making the user aware of the who, what, where, when and why of a data request, and it does not use valuable screen space when it is not relevant.

Cranor, L. F. (2006). What Do They "Indicate?": Evaluating Security and Privacy Indicators. *Interactions, 13*, 45-47. Retrieved October 26, 2007, from ACM Digital Library.

ABSTRACT: Security- and privacy-related tools often feature graphical (or in some cases textual or audio) indicators designed to assist users in protecting their security or privacy. But a growing body of literature has found the effectiveness of many of these indicators to be rather disappointing.

Dhamija, R., & Tygar, J. D. (2005a). The Battle Against Phishing: Dynamic Security Skins. *Proceedings of the 2005 Symposium on Usable Privacy and Security, USA, 93*, 77-88. Retrieved October 29, 2007, from ACM Digital Library.

ABSTRACT: Phishing is a model problem for illustrating usability concerns of privacy and security because both system designers and attackers battle using user interfaces to guide (or misguide) users.We propose a new scheme, Dynamic Security Skins, that allows a remote web server to prove its identity in a way that is easy for a human user to verify and hard for an attacker to spoof. We describe the design of an extension to the Mozilla Firefox browser that implements this scheme.We present two novel interaction techniques to prevent spoofing. First, our browser extension provides a trusted window in the browser dedicated to username and password entry. We use a photographic image to create a trusted path between the user and this window to prevent spoofing of the window

and of the text entry fields. Second, our scheme allows the remote server to generate a unique abstract image for each user and each transaction. This image creates a "skin" that automatically customizes the browser window or the user interface elements in the content of a remote web page. Our extension allows the user's browser to independently compute the image that it expects to receive from the server. To authenticate content from the server, the user can visually verify that the images match. We contrast our work with existing anti-phishing proposals. In contrast to other proposals, our scheme places a very low burden on the user in terms of effort, memory and time. To authenticate himself, the user has to recognize only one image and remember one low entropy password, no matter how many servers he wishes to interact with. To authenticate content from an authenticated server, the user only needs to perform one visual matching operation to compare two images. Furthermore, it places a high burden of effort on an attacker to spoof customized security indicators.

Dhamija, R., Tygar, J. D., & Hearst, M. (2006). Why Phishing Works. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Canada,* pp. 581-590. Retrieved October 29, 2007, from ACM Digital Library.

ABSTRACT: To build systems shielding users from fraudulent (or phishing) websites, designers need to know which attack strategies work and why. This paper provides the first empirical evidence about which malicious strategies are successful at deceiving general users. We first analyzed a large set of captured phishing attacks and developed a set of hypotheses about why these strategies might work. We then assessed these hypotheses with a usability study in which 22 participants were shown 20 web sites and asked to determine which ones were fraudulent. We found that 23% of the participants did not look at browser-based cues such as the address bar, status bar and the security indicators, leading to incorrect choices 40% of the time. We also found that some visual deception attacks can fool even the most sophisticated users. These results illustrate that standard security indicators are not effective for a substantial fraction of users, and suggest that alternative approaches are needed.

Downs, J. S., Holbrook, M. B., & Cranor, L. F. (2006). Decision Strategies and Susceptibility to Phishing. *Proceedings of the Second Symposium on Usable Privacy and Security, USA,* pp. 79-90. Retrieved November 17, 2007, from ACM Digital Library.

ABSTRACT: Phishing emails are semantic attacks that con people into divulging sensitive information using techniques to make the user believe that information is being requested by a legitimate source. In order to develop tools that will be effective in combating these schemes, we first must know how and why people fall for them. This study reports preliminary analysis of interviews with 20 nonexpert computer users to reveal their strategies and understand their decisions when encountering possibly suspicious emails. One of the reasons that people may be vulnerable to phishing schemes

is that awareness of the risks is not linked to perceived vulnerability or to useful strategies in identifying phishing emails. Rather, our data suggest that people can manage the risks that they are most familiar with, but don't appear to extrapolate to be wary of unfamiliar risks. We explore several strategies that people use, with varying degrees of success, in evaluating emails and in making sense of warnings offered by browsers attempting to help users navigate the web.

Downs, J. S., Holbrook, M. B., & Cranor, L. F. (2007). *Behavioral Response to Phishing Risk.* Paper presented at the Second Anti-Phishing Working Group eCrime Researchers Summit, Pittsburgh, PA. Retrieved November 18, 2007, from http://www.antiphishing.org/ecrimeresearch/2007/proceedings/p37_downs.pdf

ABSTRACT: Tools that aim to combat phishing attacks must take into account how and why people fall for them in order to be effective. This study reports a pilot survey of 232 computer users to reveal predictors of falling for phishing emails, as well as trusting legitimate emails. Previous work suggests that people may be vulnerable to phishing schemes because their awareness of the risks is not linked to perceived vulnerability or to useful strategies in identifying phishing emails. In this survey, we explore what factors are associated with falling for phishing attacks in a roleplay exercise. Our data suggest that deeper understanding of the web environment, such as being able to correctly interpret URLs and understanding what a lock signifies, is associated with less vulnerability to phishing attacks. Perceived severity of the consequences does not predict behavior. These results suggest that educational efforts should aim to increase users' intuitive understanding, rather than merely warning them about risks.

Furnell, S. (2007). Phishing: Can We Spot the Signs? *Computer Fraud & Security*, *2007*, 10-15. Retrieved November 25, 2007, from Science Direct.

ABSTRACT: Dr. Steven Furnell at Plymouth University has conducted research, which looks at why some computer users still can't tell the difference between an official email and a phishing scam. Steven Furnell looks at the increasing sophistication of phishing emails and examines why users are still vulnerable.

Gross, J. B., & Rosson, M. B. (2007). Looking for Trouble: Understanding End-user Security Management. *Proceedings of the 2007 Symposium on Computer Human Interaction for the Management of Information Technology, USA*, pp. 1-10. Retrieved October 23, 2007, from ACM Digital Library.

ABSTRACT: End users are often cast as the weak link in computer security; they fall victim to social engineering and tend to know very little about security technology and policies. This paper challenges this view as derogatory and unconstructive, arguing that

users, as agents of organizations, often have sophisticated strategies regarding sensitive data, and are quite cautious. Existing work on user security practice has failed to consider how users view security; this paper provides content on and analysis of end user perspectives on security management. We suggest that properly designed systems would bridge the knowledge gap (where necessary) and mask levels of detail (where possible), allowing users to manage their security needs in synchrony with the needs of the organization. The evidence for our arguments comes from a set of in-depth interviews with users with no special training on, knowledge of, or interest in computer security. We conclude with guidelines for security and privacy tools that better leverage existing users knowledge.

Herzberg, A., & Gbara, A. (2004). TrustBar: Protecting (even Naïve) Web Users from Spoofing and Phishing Attacks. *Cryptology ePrint Archive, Report 2004/155*. Retrieved November 19, 2007, from http://eprint.iacr.org/2004/155

ABSTRACT: In spite of the use of standard web security measures (SSL/TLS), users often fail to detect `spoofed` web forms, and enter into them sensitive information such as passwords. Furthermore, users often access the spoofed sites by following a link sent to them in a (fraudulent) e-mail message; this is called `phishing`. Web spoofing and phishing attacks cause substantial damages to individuals and corporations. We analyze these attacks, and identify that most of them exploit the fact that users are not sufficiently aware of the secure site identification mechanisms in browsers. In fact, it appears that even web designers are often confused about the need to securely identify login forms; we show several sites that prompt users for passwords using unprotected forms.

We derive several secure user interface principles, and present TrustBar, a secure user interface add-on to browsers. For protected web pages, TrustBar identifies the site and the certificate authority, using logos or at least names (rather than URL). For unprotected pages, TrustBar displays highly visible warnings. Early experimental results indicate that these mechanisms provide substantial protection, even for naïve and off-guard web users, from spoofing/phishing attacks.

Herzog, A., & Shahmehri, N. (2007). User Help Techniques for Usable Security. *Proceedings of the 2007 Symposium on Computer Human Interaction for the Management of Information Technology, USA*, pp.1-10. Retrieved October 23, 2007, from ACM Digital Library.

ABSTRACT: There are a number of security-critical applications such as personal firewalls, web browsers and e-mail clients, whose users have little or no security knowledge and are easily confused, even frustrated by menus, messages or dialog boxes that deal with security issues.While there are evaluations of existing applications and proposals for new approaches or design guidelines for usable security applications, little

effort has been invested in determining how applications can help users in security decisions and security tasks. The purpose of this work is to analyse conventional and security-specific user help techniques with regard to their usefulness in supporting lay users in security applications.We analyse the following help techniques: online documentation, context-sensitive help, wizards, assistants, safe staging and social navigation, and complement these with the tempting alternative of built-in, hidden security. Criteria for the analysis are derived from the type of user questions that can arise in applications and from definitions of when a security application can be called usable. Designers of security applications can use our analysis as general recommendations for when and how to use and combine user help techniques in security applications, but they can also use the analysis as a template. They can instantiate the template for their specific application to arrive at a concrete analysis of which user help techniques are most suitable in their specific case.

Jakobsson, M. (2007). *The Human Factor in Phishing*. Retrieved November 21, 2007, from Indiana University, School of Informatics Web site: http://www.informatics.indiana.edu/markus/papers/aci.pdf

ABSTRACT: We discuss the importance of understanding psychological aspects of phishing, and review some recent findings. Given these findings, we critique some commonly used security practices and suggest and review alternatives, including educational approaches. We suggest a few techniques that can be used to assess and remedy threats remotely, without requiring any user involvement. We conclude by discussing some approaches to anticipate the next wave of threats, based both on psychological and technical insights.

Jakobsson, M., & Tsow, A. (2007). *Deceit and Deception: A Large User Study of Phishing*. Retrieved November 20, 2007, from Indiana University, School of Informatics Web site: http://www.informatics.indiana.edu/research/publications/publications.asp?id=23

ABSTRACT: This study is a large scale investigation of trust manipulation tactics used by phishing web sites and email messages. The experiment focuses on media authenticity evaluations, rather than content credibility with the assumption that its authors are known. It tests the effect of features ranging from URL plausibility to trust endorsement graphics on a population of 398 subjects. The experiment presents these trust indicators in a variety of stimuli since reactions will vary according to context. In addition to testing specific features, the test gauges the potential of a phishing tactic that spoofs third party program administrators rather than a brand itself. The results show that indeed graphic design can change authenticity evaluations *and* that their impact varies with context. We expected that authenticity inspiring design changes would have the opposite effect when paired with an unreasonable request, however our data suggest that *narrative strength* – rather than underlying legitimacy – limits the impact of graphic design on trust and that

these authenticity-inspiring design features improve trust in both genuine and forged media.

Li, L., & Helenius, M. (2007). Usability Evaluation of Anti-phishing Toolbars. *Journal of Computer Virology*, *3*, 163-184. Retrieved October 28, 2007, from FirstSearch Electronic Collections Online.

ABSTRACT: Phishing is considered as one of the most serious threats for the Internet and e-commerce. Phishing attacks abuse trust with the help of deceptive e-mails, fraudulent web sites and malware. In order to prevent phishing attacks some organizations have implemented Internet browser toolbars for identifying deceptive activities. However, the levels of usability and user interfaces are varying. Some of the toolbars have obvious usability problems, which can affect the performance of these toolbars ultimately. For the sake of future improvement, usability evaluation is indispensable. We will discuss usability of five typical anti-phishing toolbars: built-in phishing prevention in the Internet Explorer 7.0, Google toolbar, Netcraft Anti-phishing toolbar and Spoof-Guard. In addition, we included Internet Explorer plug-in we have developed, Anti-phishing IEPlug. Our hypothesis was that usability of anti-phishing toolbars, and as a consequence also security of the toolbars, could be improved. Indeed, according to the heuristic usability evaluation, a number of usability issues were found. In this article, we will describe the anti-phishing toolbars, we will discuss antiphishing toolbar usability evaluation approach and we will present our findings. Finally, we will propose advices for improving usability of anti-phishing toolbars, including three key components of anti-phishing client side applications (main user interface, critical warnings and the help system). For example, we found that in the main user interface it is important to keep the user informed and organize settings accordingly to a proper usability design. In addition, all the critical warnings an anti-phishing toolbar shows should be well designed. Furthermore, we found that the help system should be built to assist users to learn about phishing prevention as well as how to identify fraud attempts by themselves. One result of our research is also a classification of anti-phishing toolbar applications.

Miller, R. C., & Wu, M. (2005). Fighting Phishing at the User Interface. In L. F. Cranor & S. Garfinkel (Eds.), *Security and Usability: Designing Secure Systems That People Can Use* (pp. 276-292). Sebastopol, CA: O'Reilly.

ABSTRACT: This article explores systems that have been proposed for web browsers and email systems to help users resist so-called "phishing" attacks.

Wu, M., Miller, R. C., & Garfinkel, S. L. (2006). Do Security Toolbars Actually Prevent Phishing Attacks? *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Canada,* pp. 601-610. Retrieved October 28, 2007, from ACM Digital Library.

ABSTRACT: Security toolbars in a web browser show security-related information about a website to help users detect phishing attacks. Because the toolbars are designed for humans to use, they should be evaluated for usability -- that is, whether these toolbars really prevent users from being tricked into providing personal information. We conducted two user studies of three security toolbars and other browser security indicators and found them all ineffective at preventing phishing attacks. Even though subjects were asked to pay attention to the toolbar, many failed to look at it; others disregarded or explained away the toolbars' warnings if the content of web pages looked legitimate. We found that many subjects do not understand phishing attacks or realize how sophisticated such attacks can be.

Wu, M., Miller, R. C., & Little, G. (2006). Web Wallet: Preventing Phishing Attacks by Revealing User Intentions. *Proceedings of the Second Symposium on Usable Privacy and Security, USA,* pp. 102-113. Retrieved October 28, 2007, from ACM Digital Library.

ABSTRACT: We introduce a new anti-phishing solution, the Web Wallet. The Web Wallet is a browser sidebar which users can use to submit their sensitive information online. It detects phishing attacks by determining where users intend to submit their information and suggests an alternative safe path to their intended site if the current site does not match it. It integrates security questions into the user's workflow so that its protection cannot be ignored by the user. We conducted a user study on the Web Wallet prototype and found that the Web Wallet is a promising approach. In the study, it significantly decreased the spoof rate of typical phishing attacks from 63% to 7%, and it effectively prevented all phishing attacks as long as it was used. A majority of the subjects successfully learned to depend on the Web Wallet to submit their login information. However, the study also found that spoofing the Web Wallet interface itself was an effective attack. Moreover, it was not easy to completely stop all subjects from typing sensitive information directly into web forms.

Yee, K.- P. (2005). Guidelines and Strategies for Secure Interaction Design. In L. F. Cranor & S. Garfinkel (Eds.), *Security and Usability: Designing Secure Systems That People Can Use* (pp. 247-273). Sebastopol, CA: O'Reilly.

ABSTRACT: This article explores specific principles and techniques that can be used for aligning security and usability in the user interfaces of desktop operating systems.

Category 3: Phishing User Education and its Impact on the Usability and Success of Anti-phishing Applications

Kumaraguru, P., Rhee, Y., Acquisti, A., Cranor, L. F., Hong, J., & Nunge, E. (2007). Protecting People from Phishing: The Design and Evaluation of an Embedded Training Email System. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, USA,* pp. 905-914. Retrieved November 19, 2007, from ACM Digital Library.

ABSTRACT: Phishing attacks, in which criminals lure Internet users to websites that impersonate legitimate sites, are occurring with increasing frequency and are causing considerable harm to victims. In this paper we describe the design and evaluation of an embedded training email system that teaches people about phishing during their normal use of email. We conducted lab experiments contrasting the effectiveness of standard security notices about phishing with two embedded training designs we developed. We found that embedded training works better than the current practice of sending security notices. We also derived sound design principles for embedded training systems.

Kumaraguru, P., Rhee, Y., Sheng, S., Hasan, S., Acquisti, A., Cranor, L. F., & Hong, J. (2007). *Getting Users to Pay Attention to Anti-Phishing Education: Evaluation of Retention and Transfer*. Paper presented at the Second Anti-Phishing Working Group eCrime Researchers Summit, Pittsburgh, PA. Retrieved December 14, 2007, from http://www.ecrimeresearch.org/2007/proceedings/p70_kumaraguru.pdf

ABSTRACT: Educational materials designed to teach users not to fall for phishing attacks are widely available but are often ignored by users. In this paper, we extend an embedded training methodology using learning science principles in which phishing education is made part of a primary task for users. The goal is to motivate users to pay attention to the training materials. In embedded training, users are sent simulated phishing attacks and trained after they fall for the attacks. Prior studies tested users immediately after training and demonstrated that embedded training improved users' ability to identify phishing emails and websites. In the present study, we tested users to determine how well they retained knowledge gained through embedded training and how well they transferred this knowledge to identify other types of phishing emails. We also compared the effectiveness of the same training materials delivered via embedded training and delivered as regular email messages. In our experiments, we found that: (a) users learn more effectively when the training materials are presented after users fall for the attack (embedded) than when the same training materials are sent by email (non-embedded); (b) users retain and transfer more knowledge after embedded training than after nonembedded training; and (c) users with higher Cognitive Reflection Test (CRT) scores are more likely than users with lower CRT scores to click on the links in the phishing emails from companies with which they have no account.

Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L.F., & Hong, J. (2007). *Teaching Johnny Not to Fall for Phish* (Cylab Technical Report). Pittsburgh, PA: Carnegie Mellon University, Usable Privacy and Security Laboratory. Retrieved December 14, 2007, from http://www.cylab.cmu.edu/default.aspx?id=2275

ABSTRACT: Phishing attacks exploit users' inability to distinguish legitimate websites from fake ones. Strategies for combating phishing include: prevention and detection of phishing scams, tools to help users identify phishing web sites, and training users not to fall for phish. While a great deal of effort has been devoted to the first two approaches, little research has been done in the area of training users. Some research even suggests that users cannot be educated. However, previous studies have not evaluated the quality of the training materials used in their user studies or considered ways of designing more effective training materials. In this paper we present the results of a user study we conducted to test the effectiveness of existing online training materials that teach people how to protect themselves from phishing attacks. We found that these training materials are surprisingly effective when users actually read them. We then analyze the training materials using principles from learning sciences, and provide some suggestions on how to improve training materials based on those principles.

Robila, S. A., & Ragucci, J. W. (2006). Don't be a Phish: Steps in User Education. *Proceedings of the Eleventh Annual SIGCSE Conference on Innovation and Technology in Computer Science Education, Italy*, pp. 237-241. Retrieved November 19, 2007, from ACM Digital Library.

ABSTACT: Phishing, e-mails sent out by hackers to lure unsuspecting victims into giving up confidential information, has been the cause of countless security breaches and has experienced in the last year an increase in frequency and diversity. While regular phishing attacks are easily thwarted, designing the attack to include user context information could potentially increase the user's vulnerability. To prevent this, phishing education needs to be considered. In this paper we provide an overview of phishing education, focusing on context aware attacks and introduce a new strategy for educating users by combining phishing IQ tests and class discussions. The technique encompasses displaying both legitimate and fraudulent e-mails to users and having them identify the phishing attempts from the authentic e-mails. Proper implementation of this system helps teach users what to look for in e-mails, and how to protect their confidential information from being caught in the nets of phishers. The strategy was applied in Introduction to Computing courses as part of the computer security component. Class assessment indicates an increased level of awareness and better recognition of attacks.

Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L. F., Hong, J., & Nunge, E. (2007). Anti-Phishing Phil: The Design and Evaluation of a Game that Teaches People Not to Fall for Phish. *Proceedings of the Third Symposium on Usable Privacy and Security, USA*, pp. 88-99. Retrieved November 30, 2007, from ACM Digital Library.

ABSTRACT: In this paper we describe the design and evaluation of Anti-Phishing Phil, an online game that teaches users good habits to help them avoid phishing attacks. We used learning science principles to design and iteratively refine the game. We evaluated the game through a user study: participants were tested on their ability to identify fraudulent web sites before and after spending 15 minutes engaged in one of three anti-phishing training activities (playing the game, reading an anti-phishing tutorial we created based on the game, or reading existing online training materials). We found that the participants who played the game were better able to identify fraudulent web sites compared to the participants in other conditions. We attribute these effects to both the content of the training messages presented in the game as well as the presentation of these materials in an interactive game format. Our results confirm that games can be an effective way of educating people about phishing and other security attacks.

Review of the Literature

The purpose of the study is to identify the fundamental design principles that inform decisions for the development of usable and secure anti-phishing applications. It is designed to assist user interface designers and developers who are not trained in the “field of usability and security” (Garfinkel, 2005, p. 37) also known as HCI-Sec, to create secure and usable anti-phishing applications.

The review is organized around three components. The first component is framed to examine the context of how phishing attacks are carried out and why they are successful. The next component prescribes user interface design principles intended to combat phishing in the user interface space. Finally, the study specifies learning principles and techniques that can be important to the over all success of anti-phishing solutions, so that education of the user is not simply a matter of default.

The study provides developers of anti-phishing applications with a set of theories and fundamental design principles to consider prior to system design and the selection of technology solutions. According to Jakobsson (2005), the development of successful security solutions is dependent on a clear understanding of current and future threats. To this end, the review of literature begins by examining current phishing techniques and anticipated risks.

Attack Methods Phishers Use, and Future Threats

This component of the review presents a summary of literature connected with general phishing concepts and includes an overview of attack methods and future threats. The literature suggests that successful phishing attacks are dependent on both technology and social engineering techniques (Jakobsson, 2005). Further, Berghel et al. (2007) write that social engineering is the primary phishing technique used today and that phishing is a subset of two pre-existing problems in the online world:

- **Social engineering**, which leverages the trust established between individuals and organizations in order to manipulate users into revealing their personal information, and
- **Identity theft**, which uses the information obtained through social engineering techniques to gain access to financial accounts.

The goal of a phishing attack is to get the potential victim to perform a series of steps in which they reveal sensitive information to the attacker (Chou, Ledesma, Teraguchi, Boneh, & Mitchell, 2004). Jakobsson (2005) describes two social engineering techniques phishers commonly use to bait victims: they sometimes attract victims with promises of limited-time free offers, or they instill fear. Attackers propagate the idea that the Internet is unsafe, encouraging users to upgrade and protect their accounts (Dhamija & Tygar, 2005a). For example, phishers urge potential victims to log in and confirm their account details by threatening to shut it down if they do not comply (Jakobsson, 2005).

According to Emigh (2005), many types of phishing attacks are hybrids that use different approaches, and that the evolution and sophistication of phishing makes development of a

current list of attack types impossible. The body of literature identifies the two attacks types that are most commonly experienced by home users: the impersonation attack and the pop-up attack.

Impersonation phishing attack.

Impersonation is the most common type of phishing approach (James, 2005), and is implemented using legitimate-looking content (Emigh, 2005). In this approach, phishers exploit the relationships that companies build with home users (Dhamija & Tygar, 2005a) and the inclination of users to trust brands and logos (Lininger & Vines, 2005). In order to fool their victims, phishers create a presence that is so convincing that users fail to recognize and act upon legitimate security indicators (Dhamija, Tygar, & Hearst, 2006; Wu, Miller, & Garfinkel, 2006).

The phishing email.

Impersonation phishing attacks are commonly initiated through a bulk email (Berghel et al., 2007; Chou et al., 2004; Emigh, 2005; Jakobsson, 2005; Moore & Clayton, 2007). Typically, a single, large-scale spam phishing attack includes 100,000 emails (James, 2005). A mass mailing of 100,000 emails may achieve a 10% receive rate and yield a phishing success rate of 1% (James, 2005). Spam email is a primary phishing technique because it is inexpensive to carry out and difficult to trace back to the attacker (Herzberg & Gbara, 2004).

Almost all phishing emails utilize HTML technology, enabling phishers to create compelling, authentic-looking email through the use of graphical elements and URL obfuscation techniques (Chou et al., 2004). Phishing emails typically carry trusted brands and logos that are copied from legitimate Web sites (Berghel et al., 2007; Lininger & Vines, 2005). Since attackers cannot obtain customer lists from specific companies, they spoof companies that are popular amongst a

significant portion of the population, such as Amazon.com or eBay (Chou et al., 2004). With clever phishing scams, attackers personalize phishing emails so that they appear credible to home users (Lininger & Vines, 2005). Personalized elements, such as the user's name or digits from an account number, make phishing emails appear legitimate (Furnell, 2007). Lininger and Vines (2005) point out that sophisticated phishing scams include the first four numbers of users' credit card accounts. They explain that some users do not realize that each bank has its own format for an initial set of account numbers and that these numbers are readily available online. To further convince home users that emails are authentic, the URL of the legitimate Web site's support site is sometimes included in the email content (Berghel et al., 2007). In addition, phishing emails typically utilize fictitious "From" addresses, making the email appear to have come from a legitimate sender (Berghel et al., 2007).

Attackers lure users to spoofed Web sites using the links contained in the phishing emails (Berghel et al., 2007; Chou et al., 2004; Dhamija & Tygar, 2005b). Examples of phishing email calls to action include (Emigh, 2005):

- Notification about problems with an account (Chou et al., 2004)
- Ironically, offers for enrollment in anti-fraud programs
- Opportunities to cancel orders that were never placed
- Notification that a fictitious change will be made to an account, unless action is taken to stop it
- Limited-time offers for free services at financial institutions

Urgency, the perceived critical nature of the calls to action, and the apparent consequences of inaction distract users from common sense security-oriented considerations, such as why a bank would ask for a credit card number (Lininger & Vines, 2005).

The phishing Web site.

Phishing Web sites are nearly indistinguishable from legitimate Web sites (Berghel et al., 2007; Jakobsson & Young, 2005). Attackers create copies of legitimate Web site HTML using original logos and other graphics (Chou et al., 2004). User information pages and submission task flows typically mirror those of the legitimate Web site (Berghel et al., 2007). Visible differences between a phishing Web site and a legitimate Web site might include text anomalies, such as typos and misspellings, and the amount of personal information that is requested from the user (Dhamija & Tygar, 2005b). Once a phishing Web site is coded, it can be reused for multiple attacks (James, 2005).

The phishing Web site domain name and URL are cleverly designed so that they appear legitimate. For example, the legitimate URL www.paypal.com may be configured for phishing as www.paypals.com (with an extra “s”) (Chou et al., 2004). Berghel et al. (2007) describe an additional URL obfuscation technique where phishers register domain names in multiple languages. In some cases, and in some languages, parts of the character sets only *appear* to use the same values. For example, the ASCII character “o” uses a different look-up value than the Cyrillic character “o”. Phishers were able to spoof Microsoft.com using this technique.

The personal information most often collected by phishers includes login name and password, credit card information, bank account numbers, social security numbers, and driver’s license or

state identification numbers (Chou et al., 2004; Wu, Miller, & Little, 2006). Once victims enter their personal information, attackers steal their identity and use it to withdraw money from financial accounts (Chou et al., 2004), purchase goods, and take out second mortgages on the victims' homes (Emigh, 2005). Typically, phishing Web sites are online just long enough for attackers to collect personal information from enough users to make the phishing effort worthwhile (Chou et al., 2004).

Pop-up phishing attack.

A second basic phishing attack method is the pop-up attack (James, 2005; Parno et al., 2006). Instead of contacting victims through email, phishers initiate attacks from Web sites using pop-up windows (Parno et al., 2006). Pop-up attacks are used to spoof URLs, to imitate pages from legitimate Web sites, or for use as error messages to make a phishing site appear credible (Lininger & Vines, 2005).

Pop-up phishing attacks utilize technologies that place phishing windows on top of legitimate Web site windows (Dhamija & Tygar, 2005a). Pop-up attacks display the legitimate Web site in the main window of the browser and a borderless pop-up phishing window over the top of it (Dhamija & Tygar, 2005b; James, 2005; Lininger & Vines, 2005; Wu, Miller, & Garfinkel, 2006). Users have a difficult time distinguishing between the legitimate and fake windows when they are displayed on top of one another, or side-by-side (Dhamija & Tygar, 2005a). If the windows are correctly placed, the security and trust indicators from the first (and authentic) window appear to also apply to the second (phishing) window (Dhamija & Tygar, 2005b). Furthermore, if the windows use the same look and feel, it is unlikely that users will notice that the two windows are provided from two different sources (Dhamija et al., 2006).

Phishing pop-up attacks are easy to disguise because the pop-up windows do not display the URL and location of the source of the content (Lininger & Vines, 2005). In addition, Javascript technology can be used to display pop-ups that take over the browser address bar, making it easy to deceive users into believing that they have navigated to legitimate Web sites (Emigh, 2005; Lininger & Vines, 2005). Although pop-up attacks are an imposing threat, their success in luring phishing victims is waning because pop-up attacks do not work if the user has enabled browser pop-up blocker tools (James, 2005).

Attack Execution Methods

Steps in a phishing attack.

Typical phishing attacks leverage four common weapons: a database of email addresses, bulk email capabilities, a phishing email used to lure victims into the scam, and the phishing Web site used to collect personal information (Berghel et al., 2007). The flow of information illustrated in Figure 1, below, is the same for all phishing attacks (Emigh, 2005; Lininger & Vines, 2005).

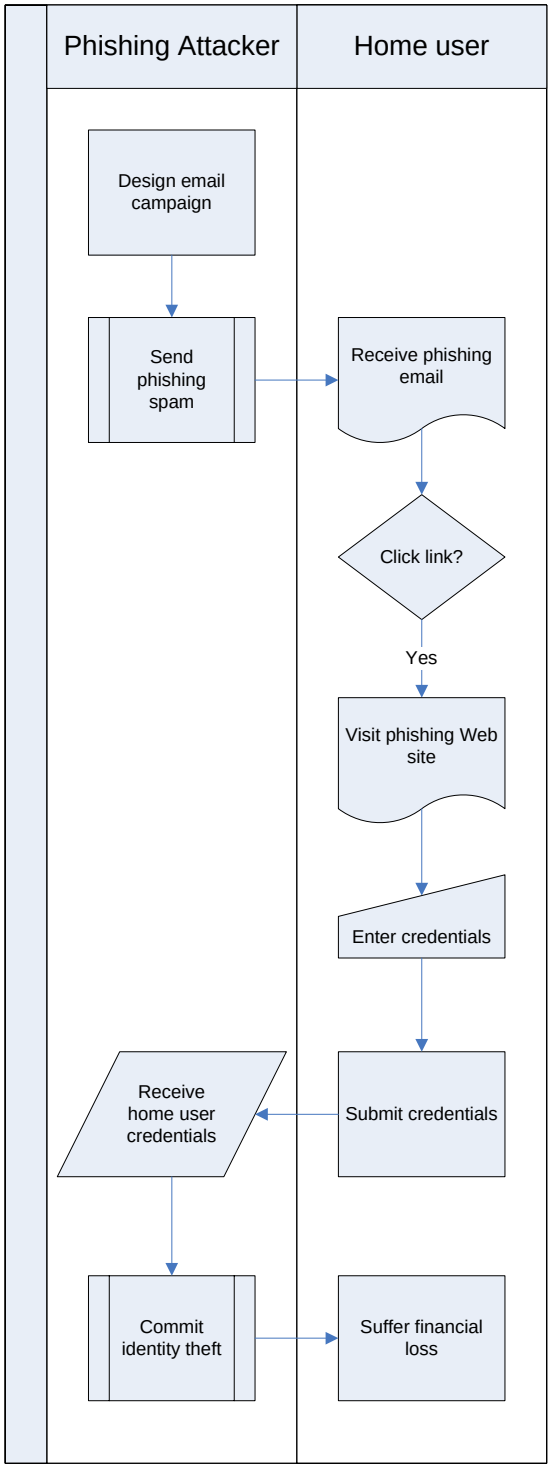

Figure 1. Information flow of a typical phishing attack.

Setting up the attack.

James (2005) alleges that it takes phishers a matter of a few hours to construct a phishing Web site, and that an attack can be set up and executed in full within a 24-48 hour period. He goes on to say that Phishers utilize the methods of spammers for obtaining email addresses, avoiding detection by spam filters, and sending out email in bulk. According to Berghel et al. (2007), databases full of email addresses can easily be obtained for a small fee from companies that market to spam distributors.

Berghel et al. (2007) write that phishing Web sites are typically hosted by computers that have been compromised and often reside in countries other than the location of the legitimate Web site. They go on to say that, as a result, detection is difficult and it takes longer to shut down them down. Phishers can hijack servers at legitimate companies (Wu, Miller, & Garfinkel, 2006), servers at online data centers, or even computers in homes (Moore & Clayton, 2007). Phishers gain control over hijacked computers by taking advantage of security vulnerabilities (Moore & Clayton, 2007).

Herzberg and Gbara (2004) reveal that it is easy and inexpensive for attackers to acquire unallocated top-level domain names for the purpose of hosting phishing Web sites. Furthermore, they report that most phishing Web sites do not have a security certificate because of the expense of obtaining one and the risk of traceability back to the attacker. In an effort to create the illusion of credibility and security, phishers sometimes obtain security certificates in one of three ways (Lininger & Vines, 2005):

- Purchase a certificate from a legitimate certificate authority, such as VeriSign (Berghel et al., 2007), or
- for a few hundred dollars, acquire and sign their own certificate, relying on most users' inability to decipher certificate details or realize that the certificate is self-signed (Parno et al., 2006), or
- implement a phishing pop-up window to replicate a valid security certificate.

Post-attack activities.

Home user identities that are stolen by phishers are sold through online brokering forums operated by organized crime syndicates (Jakobsson, 2005). Attackers hide the flow of funds by transferring stolen money between multiple accounts that are under their control (Jakobsson & Young, 2005). To avoid detection and arrest, phishers may enlist the services of "mules" to launder money (Lininger & Vines, 2005).

Phishing Participants

Who are phishers?

Lininger and Vines (2005) assert that "it's generally a good idea to know your enemy." According to James (2005), phishers are technology-savvy individuals and groups who go after the most reward with the least amount of risk. Phishers are not amateurs—they are highly innovative and technically sophisticated (Emigh, 2005). Professional phishers have resources available to invest in technologies (Emigh, 2005), and are known for their ability to analyze current technologies in order to develop new attack schemes (James, 2005).

In 2005, there were an estimated 36 phishing groups worldwide (James, 2005). The most far-reaching and damaging attacks are perpetrated by organized crime and terrorist organizations (Berghel et al., 2007; Emigh, 2005; Jakobsson & Young, 2005). Organized crime networks have the skills and resources necessary to destroy an individual's identity (Lininger & Vines, 2005). Furthermore, phishing schemes are a known funding resource of terrorist activities in Africa and the Middle East (Berghel et al., 2007). Phishing is commonly conducted from multiple countries (Emigh, 2005) and is expected to continue its expansion throughout the world (Robila & Ragucci, 2006).

Who do phishers target?

Phishers target home computer users and businesses (Lininger & Vines, 2005). Most phishing attacks target banking Web sites (e.g. Citibank), online auctions (e.g. eBay), and payment services (e.g. PayPal) (Berghel et al., 2007). Phishers target users with existing accounts (Parno et al., 2006) in developed countries because the banking systems are more robust, and the population generally, is more affluent (Lininger & Vines, 2005). The literature suggests that there is no correlation between user demographics, including sex, age, level of education, or Internet experience and usage, and user tendency to fall for phishing attacks (Dhamija et al., 2006; Kumaraguru, Rhee, Sheng, et al., 2007).

Future Threats

Phishing attacks are continually evolving into more sophisticated forms (Parno et al., 2006). Jakobsson and Young (2005) argue that "without any definitive attack or countermeasure in sight, this is likely to remain a cat-and-mouse race where each party keeps trying to anticipate

the others' next move" (p. 1). As users become better educated about the phishing threat (Jakobsson, 2005) and new methods designed to neutralize phishing become available, phishing techniques and attacks will continue to grow in sophistication (Chou et al., 2004).

Context aware phishing.

Once spam filters and other phishing countermeasures become effective in stopping phishing attacks, attackers will simply use alternate methods of connecting with their victims, such as through context aware email (Miller & Wu, 2005). Context aware phishing attacks do not use scare tactics or coerce their victims through the promise of free offers (Jakobsson, 2005). According to Jakobsson (2005), with context aware phishing, the attacker does not initially request the victim's personal information, but rather sets up a situation in which the user reveals his personal information voluntarily. As an illustrative, "physical world" analogy, Jakobson (2005) describes a apparent phone company repairman who cuts the victim's phone line, then waits for the victim to call the phone company. Once the phone company is called, the repairman shows up at the door and is let in to fix the problem. Jakobsson (2005) warns that a vast number of context aware techniques could be developed in the future, making the development of anti-phishing solutions vitally important.

Malware.

Malware is an alternate attack technique that could replace social engineering as the most common approach to phishing (Berghel et al., 2007). Simply clicking on a link from a phishing email can initiate the transmission of malware to a user's computer (Kumaraguru, Rhee, Acquisti, et al., 2007). Berghel et al. (2007) reveal that key logging software, such as malware, is being used more often in phishing and generally yields a greater amount of user personal

information than common phishing techniques because information about multiple accounts can be collected in a single attack.

Fundamental User Interface Design Principles for Anti-phishing Applications

This component of the review presents a summary of qualitative and quantitative data collected from a selected set of research studies designed to test the ability to recognize phishing cues. Downs et al. (2006) interviewed 20 non-expert Internet users to assess their awareness of phishing risks, their sensitivity to security cues, and to understand their motivation for choices made regarding email. Dhamija et al. (2006) asked 22 study participants to identify legitimate and phishing Web sites and describe the rationale for their decisions. Jakobsson (2007) conducted two laboratory studies with the goal of understanding what users react to and why. Test participants were shown emails and Web sites and asked to assess the probability of their being legitimate. Kumaraguru, Rhee, Acquisti, et al. (2007) created prototypes of training system concepts and conducted lab experiments to evaluate existing phishing training. Although these types of studies introduce some level of bias because participants are aware that they are being tested on their abilities to recognize phishing cues (Jakobsson, 2007), they provide valuable user insights for designers and developers and serve as the basis for the design principles described in the following sections.

Why Home Computer Users Fall for Phishing Attacks

Design principles for improved security indicators must take into account why current indicators fail (Cranor, 2006). In order to design effective systems, designers must have an understanding of user capabilities and how much effort users are willing to exert to protect their informational security (Gross & Rosson, 2007). Designers of email and Web page templates can proactively minimize phishing vulnerabilities if they understand what users find believable (Jakobsson, 2007). According to Downs et al. (2007), understanding user behavioral responses to phishing has a direct impact on the development of anti-phishing education. The authors go on to say that by knowing what causes users to fall for phishing, relevant training can be targeted towards audiences most in need of it.

Lack of knowledge.

The literature indicates that a surprisingly high percentage of users do not recognize the term phishing and that there is confusion about what it means (Furnell, 2007). User studies found that non-expert Internet users have little knowledge about the risks of phishing (Downs et al., 2006), and that some users are unaware that phishing even exists (Dhamija et al., 2006). In the cases where study participants believed they were knowledgeable about phishing and could recognize the signs of an attack, many of them were misinformed or held outdated beliefs (Gross & Rosson, 2007; Kumaraguru, Rhee, Acquisti, et al., 2007).

Today's technology makes it difficult for even experienced and knowledgeable users to make the correct decisions that enable them to protect their informational security (Parno et al., 2006).

Dhamija et al. (2006) argue that home users often make mistakes because they do not understand how computers and their operating systems function, or how to distinguish between applications, email, and the Internet. Home users are concerned about security, but are often confused about what action to take (Gross & Rosson, 2007).

Browser security indicators are generally unusable because they are displayed inconsistently (Herzberg & Gbara, 2004). Even when users notice security indicators, they often misinterpret their meaning or rationalize them as problems with the integrity of Web sites and content (Wu, Miller, & Garfinkel, 2006). For example, Downs et al. (2006) found that missing images were misinterpreted as a problem with the browser and not a suspicious Web site. Users are accustomed to unpredictable computer or Internet behavior (Emigh, 2005) and attribute the signs of phishing attacks to software bugs or Internet glitches (Miller & Wu, 2005; Parno et al., 2006).

Users do not always understand the role of the padlock icon display as a way to truly indicate security (Jakobsson, 2007). Many users confuse replicas of the padlock icon displayed in the content area of Email or Web pages with the actual padlock security indicator in the browser chrome (Dhamija & Tygar, 2005a, 2005b; Dhamija et al., 2006). Downs et al. (2006) found that only 40% of test participants realized that the padlock icon needed to display in the browser chrome in order for security status to be valid.

Evidence presented in the literature suggests that phishers are successful because typical users do not understand URL syntax, domain names, and security certificates (Dhamija & Tygar, 2005a; Herzberg & Gbara, 2004; Miller & Wu, 2005). Many users do not know that legitimate

URLs do not typically contain IP addresses (Lininger & Vines, 2005). In order to detect a phishing attack using certificate information, users must be able to distinguish the difference between the domain of the legitimate Web site and the domain of the phishing Web site (Dhamija & Tygar, 2005a). Most home users do not know how to check the validity of a certificate, nor do they understand the information that is presented within them (Dhamija et al., 2006). Survey results presented by Herberg and Gbara (2004) found that at least 22% of experienced computer users do not know the relevance of certificate authorities.

Visual deception.

According to Miller and Wu (2005), "users drive their mental models of the interaction from the presentation—the way it appears on the screen" (p. 280). Studies conducted by Dhamija et al. (2006) and Herzberg and Gbara (2004) found that most users are not able to distinguish between legitimate and fraudulent phishing Web sites. A good phishing Web site fooled participants in the Dhamija et al. (2006) study 90% of the time. When non-expert users base their trust and judgment on incorrect or unreliable cues, the risk of their informational security being compromised increases (Downs et al., 2006).

The literature provides convincing evidence that when evaluating a Web site to determine its authenticity, many users rely on the content alone, rather than security indicators on the browser, or those provided by anti-phishing applications (Dhamija et al., 2006; Jakobsson, 2007; Wu, Miller, & Garfinkel, 2006). Furthermore, phishing scams that spoof Web sites that are familiar to victims are successful, despite security warnings that indicate that the sites are suspicious (Wu, Miller, & Garfinkel, 2006).

The use of images and color help make phishing emails and Web sites appear more convincing (Furnell, 2007). However, phishers can easily spoof third-party seals to trick users into believing that emails and Web sites are legitimate (Dhamija & Tygar, 2005b). Two studies, Dhamija et al. (2006) and Jakobsson and Tsow (2007), reported that Web sites with professionally-designed graphical animations and advertisements increased user trust. In addition, Jakobsson and Tsow (2007) found that inclusion of third-party seals enhanced the perception of trust for emails.

Emails and Web sites that display banners, trademark symbols, footers, and copyright information appear more authentic to users (Furnell, 2007; Jakobsson & Tsow, 2007). Participants in the Jakobsson (2007) study rationalized that phishing emails and Web sites created by the phishers would not display copyright and legal disclaimer footnotes because phishers would not be concerned about that information. If content appears convincing, users explain away warnings that indicate they should be wary (Wu, Miller, & Garfinkel, 2006).

Email “From:” addresses can be forged (James, 2005; Yee, K.-P., 2005), and many users do not have the skills to recognize fraudulent email headers (Dhamija et al., 2006). Jakobsson (2007) states that users find personalized emails to be more believable, and as such, emails that are personalized are more likely to be judged as legitimate (Jakobsson, 2007).

Phishers easily trick users into believing that their Internet connection is secure (Dhamija & Tygar, 2005b). The body of literature suggests that expecting users to look for security indicators as the method to avoid phishing scams is ineffective because security indicators are susceptible to phishing attacks (Cranor, 2006; Downs et al., 2006; Emigh, 2005; Miller & Wu, 2005; Parno

et al., 2006). Javascript technology can be used to display fake padlock icons in the browser chrome, to spoof browser address bars, and to display false security certificate information (Miller & Wu, 2005). Furthermore, Jakobsson (2007) points out that many legitimate companies attempt to increase user perception of security by placing padlock icons in the content area, and he warns that "the use of the lock symbol in the content part of the page dilutes the importance of the true SSL lock symbol" (p. 2).

URL obfuscation is a common technique used in most phishing attacks (Berghel et al., 2007). Phishers exploit discrepancies between presentation and implementation by displaying URL text that does not match the actual hyperlink destination (Dhamija et al., 2006; Emigh, 2005; Miller & Wu, 2005). Many users cannot recognize deceptive hyperlinks (Parno et al., 2006), and when they click on a phishing link, they are unknowingly taken to a rogue Web site (Dhamija & Tygar, 2005a). Dhamija and Tygar (2005a) reveal that it is difficult for users to distinguish the difference between browser chrome and windows that are actually part of the Web page content area. They go on to say that phishers leverage this weakness to create fraudulent login dialog windows with which to collect user credentials. Furthermore, phishers trick their victims into believing that multiple windows belong to the same legitimate Web site, when in fact, one of the windows is displayed for the purpose of a phishing attack (Dhamija & Tygar, 2005b).

Lack of attention.

One of the key reasons why computer security tools fail is that home user security management is not task-oriented (Gross & Rosson, 2007). Users are interested in completing tasks such as purchasing goods and services, and transferring money between bank accounts (Parno et al., 2006; Wu, Miller, & Garfinkel, 2006). Because security is not the primary task of most users

(Herzog & Shahmehri, 2007; Parno et al., 2006; Wu, Miller, & Little, 2006), they do not remember to check security indicators, or inspect URLs (Dhamija et al., 2006; Parno et al., 2006; Wu, Miller, & Garfinkel, 2006).

Various security solutions are available to users; however, they require considerable diligence by users to pay attention to indicators (Downs et al., 2006). In fact, phishers count on potential victims failing to notice security indicators (Herzberg & Gbara, 2004). Visual security cues that display outside of the content area are less than effective because they are not within the user's area of focus (Miller & Wu, 2005). Browser security warnings are so commonplace that users tend to ignore them (Dhamija & Tygar, 2005a). The browser padlock icon is very small, and its presence (or lack there of) is often missed by users (Dhamija & Tygar, 2005a; Herzberg & Gbara, 2004).

Users rely on content to authenticate the source and legitimacy of email or Web pages because the content is what is at the center of their attention (Wu, Miller, & Garfinkel, 2006). Pop-up phishing attacks are very convincing because users do not notice that the second browser window is unsecure (Herzberg & Gbara, 2004). In addition, many users disable security features because they are annoying, disruptive to work tasks, or their relevance is unclear (Herzberg & Gbara, 2004). Users who feel rushed to comply with a phishing request are less likely to take the time to verify whether they are legitimate (Miller & Wu, 2005).

Users typically do not choose to view the details of security certificates (Emigh, 2005), and in the rare case when they do, they often do not understand the information that is presented

(Dhamija & Tygar, 2005a). Dhamija et al. (2006) reported that 15 of 22 participants in their study dismissed invalid security certificate warning messages without considering the possible consequences. Lininger and Vines (2005) point out that “we have all learned that it’s okay if the certificate is bad” (p. 139).

Anti-phishing Application Approaches and Goals

This component of the review provides an overview of current approaches, browser issues, and proposed goals for anti-phishing solutions.

Anti-phishing application approaches.

Numerous anti-phishing applications are available today. They utilize various technologies to analyze URLs, text, and images in order to determine if Web sites are legitimate (Emigh, 2005). The effectiveness of anti-phishing applications is dependent on the mechanisms they employ to report attacks to users (Berghel et al., 2007). Some solutions display visual indicators, such as colorful icons that represent levels of phishing risk. Others use explicit warning messages that alert the user about impending attacks (Kumaraguru, Rhee, Acquisti, et al., 2007). Other solutions offer the user specific information about the location and age of Web sites (Kumaraguru, Sheng, et al., 2007). Pilot studies of anti-phishing solutions conducted by Downs et al. (2006) indicate that current tools are ineffective in reducing the success rate of phishing attacks.

Problems with browsers.

Chou et al., (2004) allege that the browser is the most appropriate mechanism for stopping phishing attacks because brower plug-ins are easy to install. However, other researchers argue

that browsers are not the ideal solution in that they were not designed with secure usability as a primary goal (Dhamija & Tygar, 2005a). Browsers suffer from security vulnerabilities that sophisticated phishers use to their advantage, and the more functionality that is provided in a browser, the more prone it is to security flaws (Berghel et al., 2007).

Wu, Miller, and Little (2006) reveal that users recognize Web sites based on their content. Computers recognize Web sites based on their certificates and locations on the Internet. They go on to say that the browser has no way of knowing user intentions or why a user is using a Web site, and many users do not have the skills to interpret the system properties. Because users and the browser interpret the Web site in different ways, it is difficult for users to avoid phishing attacks.

Goals for anti-phishing applications.

With applications that ask users to make security-critical decisions, user decisions must be correct the first time (Herzog & Shahmehri, 2007). Home users can defend themselves and their interests against phishing attacks through comprehensive education and awareness and by using anti-phishing software applications (Chou et al., 2004). High-level goals for anti-phishing applications should include:

- An effective and usable interface that provides users with awareness of the relevant details of transactions (who, what, where and why) so that they can make informed security-related decisions (Camenisch et al., 2006).
- Users' personal information must be protected until it leaves their control (Dhamija & Tygar, 2005a).

- Home users who do not have knowledge and understanding about the Internet must be able to defend themselves against phishing attacks, and mis-use by non-expert users must never result in the user's personal information being compromised (Li & Helenius, 2007).

User-centered Design Principles for Anti-phishing Solutions

This component of the review presents the design principles identified in the selected literature that help reveal vulnerabilities and improve the design of anti-phishing application solutions (Yee, K.-P., 2005). Wu, Miller, and Garfinkel (2006) claim that "phishing is an attack that directly targets the human being in the security system" (p. 604). Security cues built into future anti-phishing applications must be intuitive, and users must have access to educational resources that interpret them (Downs, Holbrook & Cranor, 2007). According to Camenisch et al. (2006), the principles that define usability for anti-phishing solutions include context awareness, user advice, and efficient use of screen real estate. Yee (2005) argues that with effective designs, the user's workflow remains fluid, indicators are well understood, and the results of actions match the user's mental model.

Security warnings.

According to Wu, Miller, and Little (2006), security warnings often ask the user to stop doing something, but do not provide good alternative courses of action. Furthermore, the authors find that users who need to complete tasks will proceed, despite receiving warnings. Li and Helenius (2007) state that users must be able to take the correct action in response to phishing Web sites,

and that alert messages should provide the user with advice to help them recover from errors and dangers.

Some authors believe that users' prior experience with security warnings has resulted in their tendency to dismiss them without much thought and consideration of the consequences (Downs et al., 2006). Yee (2005) argues that expecting users to respond to message prompts about security in the middle of an important task teaches users that security is more trouble than it is worth, and trains them to dismiss warnings without acting on them. Other authors, such as Wu, Miller, and Garfinkel, (2006) insist that the most effective approach to the design of anti-phishing solutions is a pop-up warning message that interrupts the user's task before he takes action that may compromise his personal information. In their study, Wu, Miller, and Garfinkel (2006) found that anti-phishing pop-up warnings motivated test participants to be more cautious, and as a result, dramatically reduced the success rates of phishing attacks. By interrupting the users task, warning dialogs were successful in significantly reducing the spoof rate (see Figure 2).

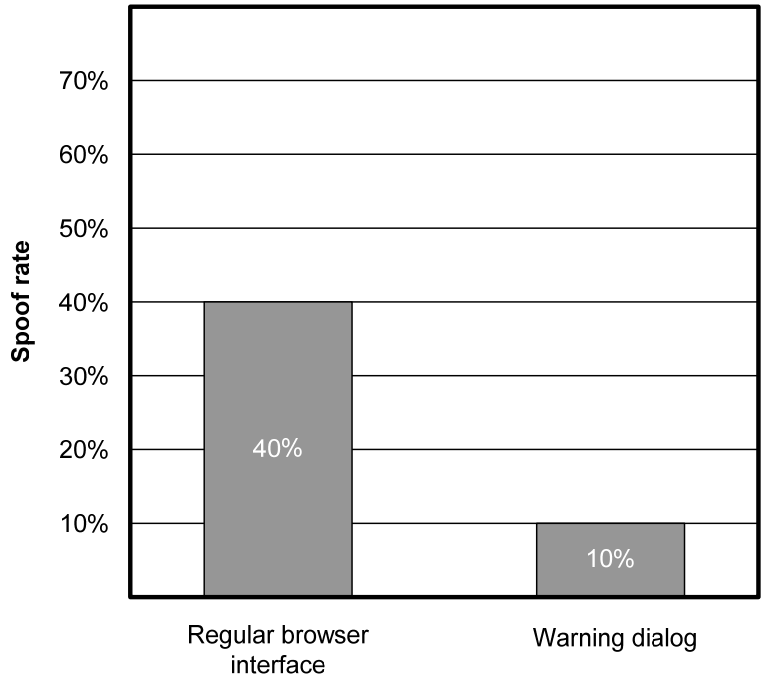

Figure 2. Spoof rates with regular browser and blocking warning box.(Note: From "Do Security Toolbars Actually Prevent Phishing Attacks?" by M. Wu, R. C. Miller, and S. L. Garfinkel, 2006, *Proceedings of the 2006 ACM SIGCHI Conference on Human Factors in Computing Systems*, pp. 601-610. Copyright 2006 by ACM. Adapted with permission. http://doi.acm.org/10.1145/1124772.1124863).

User warnings must interrupt the user with highly noticeable visual or audio signals, and their meanings must be clear (Herzberg & Gbara, 2004). Warnings should only be provided when an action needs to be taken by the user (Downs et al., 2006). They must be displayed to the user at the proper time (only when phishing is detected) and the message must provide explicit information and guidance (Wu, Miller, & Garfinkel, 2006). As an alternative, user warnings can be displayed unobtrusively, yet visibly, in the form of tips displayed in coordination with user mouse actions (Yee, K.-P., 2005).

Not warning users frequently enough puts their security at risk; warning them too often becomes an annoyance (Yee, K.-P., 2005). Phishing warnings based on computer operation will generate many false positives and will motivate users to by-pass warnings or disable security mechanisms (Miller & Wu, 2005). Anti-phishing solutions must minimize the potential for false alarms (Chou et al., 2004). Yee (2005) argues that even as low as a 1% rate of false positives could train users to dismiss warning messages without considering the problem that caused them.

The selected literature reveals that warning messages need to provide users with actionable choices, rather than just general warnings about risks (Camenisch et al., 2006; Downs et al., 2006; Kumaraguru, Rhee, Acquisti, et al., 2007; Wu, Miller, & Garfinkel, 2006; Wu, Miller, & Little, 2006). When presented with warning messages, users must be notified about the cause of the warnings (Kumaraguru, Rhee, Acquisti, et al., 2007) and consequences of various options (Li & Helenius, 2007). Messages that do not disclose the nature of the threat increase the risk that users will dismiss them without resolving the issue (Downs et al., 2007).

Failure to understand security messages can cause users to compromise their personal information (Herzog & Shahmehri, 2007). Security messages must not be written to include technical language and jargon that many home users will not understand (Herzberg & Gbara, 2004). Furthermore, to improve the chances that users will read messages and understand them, user interface text should be kept short and simple (Kumaraguru, Rhee, Acquisti, et al., 2007).

Layout and visual design.

Research shows that user interfaces that follow the design language with which users are familiar are more usable, therefore the design of anti-phishing applications should build upon the

operating system and browser user interface conventions for the platform on which they will be used (Li & Helenius, 2007). Nonetheless, designers of secure anti-phishing solutions must assume that consistent visual designs can be easily copied and spoofed (Dhamija et al., 2006). User interface designs that use general purpose operating system graphics are easy to imitate, and phishers use this weakness to their advantage when they develop attack strategies (Dhamija & Tygar, 2005a).

According to Yee (2005), designers must strive to create designs that are “noticeable by their proximity and to the matter at hand, not by their aggressiveness” (p. 262). Designers must understand that security indicators placed in the periphery or outside the user’s main area of focus will often be ignored entirely (Dhamija et al., 2006). Anti-phishing indicators should be noticeable without conscious effort by the user during execution of primary tasks (Cranor, 2006; Herzberg & Gbara, 2004). To this end, security indicators and content should be presented together (Herzberg & Gbara, 2004; Miller & Wu, 2005).

Camenisch et al.(2006) state that user interfaces must provide strong visual feedback in coordination with user actions and system transactions. The user interface must render content in a predictable manner so that it is evident when content is suspicious (Emigh, 2005). It should be clear and obvious to the user when important and relevant information, such as security indicators, are missing (Herzberg & Gbara, 2004; Jakobsson, 2007).

Phishing applications, such as toolbars, add user interface controls and icons to existing applications (e.g., the browser) (Camenisch et al., 2006). When toolbars are not being used, they

unnecessarily reduce the work area of the screen (Camenisch et al., 2006). Anti-phishing applications must not take up too much of the valuable workspace from the main browser window (Li & Helenius, 2007).

Security indicators.

The literature suggests that user interface security indicators are largely ineffective (Cranor, 2006). Today, the impact of security indicators is diluted by the draw of convincing-looking content that is central to the user's focus (Wu, Miller, & Little, 2006). The use of indicators in user interfaces is most effective for, and should be limited to, cases where they will provide users with information that will enable them to make decisions that they need to make on their own (Cranor, 2006).

Li and Helenius (2007) state that anti-phishing applications should provide clear and understandable security status information—whether or not Web pages are legitimate. The authors go on to say that applications must display the security status of Web pages before they are verified, during the validation process, and afterwards through verification results. Application performance must be good enough to display results within a reasonable amount of time (Li & Helenius, 2007). Anti-phishing applications must enable the user to distinguish between legitimate security indicators and those that are fake (Downs et al., 2006). Indicators must be resistant to spoofing and accurately indicate an attack when one is in progress (Cranor, 2006).

When designing a new indicator, designers and developers should ensure that the software is able to display state information (e.g. secure versus unsecure) accurately and to the user at the

correct point in time (Cranor, 2006). It is easier for humans to detect the presence of an indicator than it is to notice that one is missing (Wu, Miller, & Little, 2006). Security indicators must appear for both secure and unsecure states (Dhamija et al., 2006). Security indicators live amongst other indicators on users' systems, and collectively, they cannot display contradictory security states or create user confusion (Cranor, 2006).

Current user interfaces do not adequately inform users about who their data is sent to, and criminals exploit this weakness with phishing techniques (Camenisch et al., 2006). According to Wu, Miller, and Little (2006), Web site registration information can be helpful in detecting phishing. If users realize that a seemingly well-established Web site was registered overseas a few days ago, this information provides a good clue that it could be a phishing attack. During online transactions, anti-phishing user interfaces should alert users if they have not had a previous relationship with the recipient of the information they intend to submit (Camenisch et al., 2006). In addition, Web site reputation (Miller & Wu, 2005) and popularity (Wu, Miller, & Little, 2006) are very difficult to spoof and can be used as an indicator of legitimacy. For example, a Web site can be examined along the following criteria (Miller & Wu, 2005):

- How many times the user has visited the Web site
- How many other people have visited the Web site
- How many sites link to it
- How long the Web site has existed

The meanings of indicators must be clear, and when necessary, users need to understand how to take action on them (Cranor, 2006). It is important to test anti-phishing indicators to determine

whether users will understand them in the context of their own activity (Cranor, 2006). Cranor (2006) insists that successful anti-phishing indicator designs will stand up to the test of time. The author goes on to say that well-designed indicators will not eventually be ignored because they are inconvenient to monitor and act upon, or because they are unreliable.

Trust indicators.

Dhamija and Tygar (2005a) state that users place a great deal of trust in brand logos and icons, such as the browser padlock. The authors go on to say that anti-phishing solutions must push users to look beyond these cues in order to judge the legitimacy of email and Web sites. Some anti-phishing applications provide a user-customized user interface element, such as a name or image, to let the user know when they are visiting a Web site in which they have an established relationship (Emigh, 2005). Allowing users to assign names to Web sites frees them from relying on unfamiliar third parties, such as certificate authorities, to validate that they have (or should have) a relationship with a Web site (Yee, K.-P., 2005). User-assigned identities are more intuitive and recognizable by users (Herzberg & Gbara, 2004) and provide a proactive solution that prevents users from having to react to elements that are controlled by others (Yee, K.-P., 2005). In addition, user interface elements that are customized for each user provide a higher level of security because they are very difficult for phishers to copy (Dhamija & Tygar, 2005a; Emigh, 2005). This approach is showing promise as a viable solution for validating trust (Emigh, 2005).

According to Dhamija and Tygar (2005a), research shows that users understand the idea of Web sites proving their identity through display of customized indicators. The authors suggest that users prefer to use photographic image identifiers. For improved usability, it should be possible

to apply a single customized identifier across multiple Web sites commonly visited by the user (e.g., my shopping Web sites) (Herzberg & Gbara, 2004).

User effort.

Anti-phishing applications should not require excessive work and effort to install and use (Herzberg & Gbara, 2004). According to Gross & Rosson (2007), there is a trade off in end-user security management between reducing user responsibility and requiring user attention. They argue that if users are not made responsible, they may disengage. On the contrary, if managing security is too much work, users will become confused and annoyed.

Users are frustrated by the expectation to manage computer security outside of their work (Gross and Rosson, 2007). Computer security is seen as a secondary task, and users cannot be expected to interrupt primary tasks to address security countermeasures, such as viewing the details of security certificates (Dhamija & Tygar, 2005a). Successful anti-phishing solutions are integrated into the user workflow and command user attention (Wu, Miller, & Little, 2006). According to Jakobsson (2007), security “abilities” and security “habits” are not always aligned (p. 3). Users will reject anti-phishing methods that interfere with day-to-day browsing activities (Chou et al., 2004).

The problem is compounded by the fact that users are willing to incur risk in order to complete tasks that they view as important, and they are not good at analyzing the potential trade-offs between the benefits and risks of some tasks (Wu, Miller, & Garfinkel, 2006). If seemingly unnecessary security mechanisms get in the way, users are prone to disabling them, putting their informational security at risk (Parno et al., 2006). Li and Helenius (2007) state that anti-phishing

tools should enable expert computer users to skip or disable basic or optional features that are provided to help less-knowledgeable users. They insist that users should not be expected to remember complex steps in order to stop their personal information from being compromised (Li & Helenius, 2007).

Use of technology in securing the user interface.

Once a technology convention becomes mainstream, it is difficult to introduce something new (Chou et al., 2004). Herzberg and Gbara (2004) contend that to be adopted within the industry, anti-phishing solutions must benefit e-commerce companies and their customers. The authors go on to say that the solution should function well with legacy and next generation Web sites, and it must not increase the costs and effort required to create Web sites and publish content.

Phishing User Education and its Impact on the Usability and Success of Anti-phishing Applications

Exposure to user education raises users concerns about it (Jakobsson, 2007). Inexperienced Internet users who are unaware of the phishing threat are unlikely to download and install new anti-phishing applications, or will ignore the warnings provided by the tools they do have (Downs et al., 2006). This component of the review analyzes selected literature that describes principles of learning and human-computer interaction that can be applied to user education components of anti-phishing applications to increase visibility and transparency of the solution.

Impacts of phishing user education.

The literature is divided in its findings about whether or not user education provides value towards the usability and success of anti-phishing applications. Some researchers contend that

books and articles about phishing have had little impact on user awareness of phishing or how to recognize an attack (Jakobsson, 2007). According to Emigh (2005) user education is largely ineffective in attempts to instruct users not to act on links in emails, to be attentive to SSL indicators, or to verify domain names. The author says that user education has failed because the mechanisms used to verify the legitimacy of emails or Web pages, for example the “From:” address, the URL, or the lock security indicator, can all be spoofed. Kumaraguru, Rhee, Sheng, et al. (2007) argue that anti-phishing education is widely available, however, users often ignore it. Furthermore, Jakobson (2007) points out that educational opportunities are limited because phishing is obscure and complex and, in general, users are not actively interested in learning about it.

In contrast, other authors suggest that anti-phishing education is vital to the success rate of anti-phishing applications. While technology and design is addressing many aspects of the phishing problem, user education is also a significant contributor to the solution (Robila & Ragucci, 2006). According to Kumaraguru, Rhee, Acquisti, et al. (2007), phishing education for home users is necessary because users do not fully process and act upon security warnings, and law enforcement agencies have not been able to eliminate the problem. Several studies provide evidence of the important role that user education plays in the fight against phishing. The user study conducted by Kumaraguru, Sheng, et al. (2007) demonstrates that, despite long-standing opinion, existing online anti-phishing training is effective, as long as users take the time and effort to read it. In other testing by Kumaraguru, Sheng, et al. (2007), after training, test participants demonstrated a significant improvement in their ability to identify phishing Web sites. Parno et al. (2006) found that after training, users were less likely to rely on content in

order to assess its legitimacy. Furthermore, the participants inspected URLs more frequently and were more cautious to consider the amount and type of information the Web site requested from them. In a study conducted by Downs et al. (2007) users who correctly answered questions about the definition of phishing were much less likely to fall for phishing attacks.

Downs et al. (2007) claim that "knowledge and experience predict behavioral responses to phishing attacks in ways that support the idea that better understanding can help thwart such attacks" (p. 37). If users understand how a system works, they will be less likely to override it when it is inappropriate to do so, and they will be less susceptible to increasingly sophisticated phishing attacks. One study found that the presence or absence of an anti-phishing application tutorial had a profound impact on the success of the application. Participants who viewed the anti-phishing application tutorial prior to using it were far less likely to be fooled by phishing attacks (Wu, Miller, & Garfinkel, 2006). Kumaraguru, Rhee, Acquisti, et al. (2007) suggest that it is important that designers and developers provide users with anti-phishing education in parallel to the use of anti-phishing applications and automated means of phishing prevention at the system level.

Learning and user-centered design principles for integration of user education into anti-phishing applications.

Many users do not understand the complexity and sophistication of today's phishing attacks (Wu, Miller, & Garfinkel, 2006). Users need to be educated about phishing scams and how to avoid becoming victims (Downs et al., 2006). The goal of phishing education should be to provide users with the knowledge needed to make informed decisions about their security, based on cues and indicators (Kumaraguru, Rhee, Acquisti, et al., 2007).

User help techniques are usually combined in order to achieve the best over all solution (Herzog & Shahmehri, 2007). Users can be trained to identify phishing attacks if the training is well-designed and if it follows established learning principles (Kumaraguru, Rhee, Sheng, et al., 2007). Training approaches that focus on user education include online information provided by governments, non-profit agencies, and corporations, and phishing IQ tests (Kumaraguru, Sheng, et al., 2007). According to Kumaraguru, Rhee, Acquisti, et al. (2007), the most common approach to anti-phishing training is to provide users with access to articles about phishing on Web sites. The authors claim that interactive techniques, such as Web-based tests that allow users to self-assess their knowledge are proven to be more effective for enhancing phishing knowledge (Kumaraguru, Rhee, Acquisti, et al., 2007). In their study, Sheng et al. (2007) find that after using interactive forms of training, users became more confident in their informational security decisions.

Training materials are more effective when they are introduced in the context of the user's goals (Kumaraguru, Rhee, Acquisti, et al., 2007; Sheng et al., 2007). Furthermore, users learn more and retain the information longer if the training is presented just after they fall for an attack (Kumaraguru, Rhee, Sheng, et al., 2007). According to Gross and Rosson (2007), user education should be presented "just in time" to motivate and enable users to make informed decisions. They go on to say that training and information presented in this format is more likely to get the attention required for it to provide real value. In the user study conducted by Kumaraguru, Rhee, Sheng, et al. (2007), immediately after receiving embedded training, users were better able to detect phishing email and Web sites. Participants who viewed embedded training retained and

transferred knowledge better than participants who read non-embedded training. Embedded training is successful because users learn by doing, and feedback is immediate (Kumaraguru, Rhee, Sheng, et al., 2007; Sheng et al., 2007).

Users must be educated about phishing in a consistent manner and without information overload (Berghel et al., 2007; Li & Helenius, 2007). Kumaraguru, Rhee, Acquisti, et al. (2007) suggest training with less text and more graphics provides better communication of meaning. To avoid confusion and accurately convey warning information, they recommend that the design use simple and visually clear text and images. Furthermore, research indicates that incorporating illustrative character agents in a story-based format helps increase learning about phishing concepts (Sheng et al., 2007).

Knowledge areas that best help home users avoid falling for phishing scams.

When educating users about phishing, it is important not to assume that there is much pre-existing knowledge (Downs et al., 2006). Jakobsson (2007) found that the use of the term "phishing" may be too obsure for some users, prompting test participants to suggest the use of the term "identity theft" instead. There is little value in educating users about various phishing techniques. Rather, training should be focused on basic knowledge from the user's perspective (Kumaraguru, Rhee, Acquisti, et al., 2007; Li & Helenius, 2007). Focusing on generalized concepts provides users with a better understanding of phishing, and they can adapt that knowledge as the phishing landscape evolves (Downs et al., 2006).

According to Kumaraguru, Sheng, et al. (2007), users can be taught to avoid phishing scams without understanding complex security concepts. For example, study participants were able to identify phishing Web sites with training that provided knowledge about only a few simple security concepts. Users are easily fooled by phishing Web sites that use sub-domain names that are similar to a legitimate Web site's (Kumaraguru, Sheng, et al., 2007). They should be educated about the syntax of domain names and how to verify corporate domains (Herzberg & Gbara, 2004). Furthermore, user education focused on secure Web and email usage will help intercept phishing attacks before users get to phishing Web sites (Herzberg & Gbara, 2004; Kumaraguru, Rhee, Acquisti, et al., 2007).

In addition, poor security habits can be broken by instructing users not to judge the legitimacy of Web sites by the design and appearance of its content alone (Kumaraguru, Sheng, et al., 2007). According to Jakobsson (2007), users should be trained not to call phone numbers listed in email or on Web sites. Instead, instruct users to call the support phone numbers printed on the back of their credit cards, or from recent statements.

Conclusions

This study identifies and describes the strategies used in phishing and why home computer users fall for phishing attacks. Important usability issues with Web browsers and current tools in the fight against phishing are examined. Design principles intended to improve the transparency and visibility of anti-phishing applications are proposed. To be successful, phishing attacks must reach the appropriate target (e.g., potential victims), appear credible, and allow the attacker to disappear undetected (Berghel et al., 2007). Phishing is commonly conducted from multiple countries (Emigh, 2005) and is expected to continue its expansion throughout the world (Robila & Ragucci, 2006). It is likely that smaller scale attacks that leverage partial information about fewer victims and result in higher success rates will become an increasing threat (Jakobsson, 2005). Furthermore, the literature suggests a link between user education that empowers users to make informed decisions about their informational security and the success and usability of anti-phishing solutions.

The Role of Mental Models

Today's computer security problems, such as phishing, are a result of the failure of computer solutions to behave as users expect (Yee, K.-P., 2005). The behavior of *usable* computer systems matches the mental model of how users believe computers work, therefore, it is important that designers and developers understand the user's mental model (Downs, Holbrook, & Cranor, 2006; Yee, K.-P., 2005) when creating anti-phishing solutions. Miller and Wu (2005) explain that, when using email or a Web site for the purpose of e-commerce, the user's model is formed around who the other party is, the meaning of the incoming message, and the purpose of their

own actions. They go on to reveal that users are fooled when they formulate an inaccurate mental model of what is transpiring during online interactions.

The Role of Trust Decisions

Designers and developers must provide home users with the information that they need to make informed “trust” decisions (Emigh, 2005). During online commerce activities, users are forced into making trust decisions that are not only difficult, but often unrealized. This situation makes them susceptible to phishing attacks (Kumaraguru, Rhee, Sheng, et al., 2007). Phishing attacks focus on the gap between the intentions and expectations of naïve users (Herzberg & Gbara, 2004; Miller & Wu, 2005) and the functionality of the underlying system (Miller & Wu, 2005). Computers have no way of knowing user intentions or what is in their minds (Yee, K.-P., 2005).

The Role of Web Browser Interface Design

Herzberg and Gbara (2004) contend that phishing attacks are successful because of user interface design flaws in popular Web browsers. They point out that with current browsers, the user is expected to verify the legitimacy of Web sites by way of the user interface status areas: the address bar containing the URL and the lock icon indicating SSL protection. Browsers fail to effectively differentiate between pages that do or do not have SSL protection (Wu, Miller, & Little, 2006), and they could be more effective by providing additional visual indicators beyond logos, layout, and domain names that users could leverage to authenticate Web sites (Miller & Wu, 2005).

The Role of Anti-phishing Education

According to Downs et al. (2007), understanding user behavioral responses to phishing has a direct impact on the development of anti-phishing education. The authors contend that by knowing what causes users to fall for phishing, relevant training can be targeted towards audiences most in need of it. For example, users with a better understanding of the Internet environment and the ability to uncover the structure of URLs are more likely to recognize phishing attacks (Downs et al., 2007).

Strategies for Designers and Developers

Designers and developers can take a proactive approach to the phishing problem by identifying the strategies employed by phishers and designing user interfaces that support usable security (Jakobsson, 2007). Typical solutions are only incremental and reinforce the ongoing battle between phishing criminals and legitimate businesses and their customers, and holistic and fundamental approaches are required in order to solve the phishing problem (Parno et al., 2006). According to Kumaraguru, Rhee, Acquisti, et al. (2007) anti-phishing solution strategies intended to protect users from phishing fall into three general categories:

1. Visual indicators, or solutions that are integrated during online tasks, in order to visibly alert users about potential threats
2. User education, or solutions that educate users about phishing and how to avoid becoming a victim
3. Technology integration, or solutions that are embedded in the programming, designed to eliminate the threat silently, using technology alone

This study addresses the aspects of phishing described in the first two categories above: visual indicators and warnings and user education about phishing. As tools designed to fight phishing become more effective, attack strategies are expected to increase in sophistication (Jakobsson, 2007). Defenders seek to identify attackers as soon as possible to minimize damage, and attackers go after holes in their defenses (Moore & Clayton, 2007). Furthermore, it is important for *both* interface designers and developers to be knowledgeable about the system and where the security holes that phishers may eventually leverage lie (Moore & Clayton, 2007).

Balfanz, Durfee, Grinter, and Smetters (2004) argue that the selection of hardware and software technologies for secure systems should occur early in the product development process. Architecture and technology choices made during system design affect the way in which security is delivered to and understood by users (Guttman et al., 2005). URL obfuscation detection technologies could be used to provide visual feedback to users, providing the means for them to protect themselves against phishing attacks (Jakobsson & Young, 2005). According to Emigh (2005), phishers have not deployed attack mechanisms that are effective against screen-based entry. The author points out that alternative data entry techniques, such as selecting options from secure screens instead of typing them with the mouse and keyboard, will counter less common but severely damaging phishing attacks, such as key logging, in the future (Emigh, 2005).

According to Kumaraguru, Sheng, et al. (2007), the most effective anti-phishing systems will automatically defend users against attacks. Parno et al. (2006) recommends that developers concentrate on new architectures and system designs that do not rely on user decisions to determine whether Web sites are safe from phishing attacks. The authors argue that anti-phishing

solutions of the future must go beyond reliance on users to assist in the detection of phishing scams. According to Chou et al. (2004), increasingly sophisticated attacks could be stopped with the implementation of complimentary client and server-side technologies. Humans will continue to be a limitation in the battle against phishing, and security mechanisms that do not rely on users will bring security to a larger audience (Parno et al., 2006).

Table 3 (see Summary of Design Principles for Anti-phishing Applications) includes a collection of design principles identified in the selected literature. Principles are framed within six categories, including Security Warnings, Layout and Visual Design Elements, Security Indicators, Trust Indicators, User Effort, and User Education. The list is intended to provide guidance to user interface designers and developers in the design of usable and secure anti-phishing applications.

Table 3: Summary of Design Principles for Anti-phishing Applications

User Interface Categories	**Design Principles**
Security Warnings	• Display warnings only when phishing is detected (Wu, Miller, & Garfinkel, 2006). • Display warnings only when an action needs to be taken by the user (Downs et al., 2006). • Interrupt the user's task before they take action that may compromise their personal information (Wu, Miller, & Garfinkel, 2006). • Minimize the potential for false phishing alarms (Chou et al., 2004). • Provide users with actionable choices, not just risks (Camenisch et al., 2006; Downs et al., 2006; Kumaraguru, Rhee, Acquisti, et al., 2007; Wu, Miller, & Garfinkel, 2006; Wu,

User Interface Categories	Design Principles
	Miller, & Little, 2006). • Provide advice that enables users to recover from danger and errors (Li & Helenius, 2007). • Explain the causes of warnings (Kumaraguru, Rhee, Acquisti, et al., 2007). • State the consequences of various options available to users (Li & Helenius, 2007). • Do not use technical language and jargon that will confuse home users (Herzberg & Gbara, 2004). • Shorten and simplify message text (Kumaraguru, Rhee, Acquisti, et al., 2007).
Layout and Visual Design Elements	• Build user interface widgets and interactions upon the operating system and browser conventions of the platform (e.g., Microsoft Windows or Mac) (Li & Helenius, 2007). • Avoid use of generic user interface visual design elements, which can easily be imitated by phishers (Dhamija & Tygar, 2005a). • Display security indicators and content together within the focus area of users (Herzberg & Gbara, 2004; Miller & Wu, 2005). • Provide strong visual feedback in coordination with user actions and system transactions (Camenisch et al., 2006). • Minimize use of screen real estate, particularly within the browser's main window (Li & Helenius, 2007).
Security Indicators	• Use only to provide information that enables users to make informed decisions that the system cannot make for them (Cranor, 2006) • Provide status information when an interaction is secure *and* when it is unsecure (Dhamija et al., 2006; Li & Helenius, 2007).

User Interface Categories	Design Principles
	• Provide status information before, during, and after the security validation process is complete (Li & Helenius, 2007). • Display indicators that are tamper-resistant and accurate (Cranor, 2006). • Indicate the correct status, at the correct point in time (Cranor, 2006). • Do not display contradictory security states, or create user confusion with indicators that co-exist on the same computer (Cranor, 2006). • Provide clear meaning that enables users to take the correct action (Cranor, 2006).
Trust Indicators	• Provide user-customizable trust indicators (Dhamija & Tygar, 2005a; Emigh, 2005; Herzberg & Gbara, 2004). • Allow users to specify images, rather than just text, for customizable trust indicators (Dhamija & Tygar, 2005a). • Design the system architecture to allow the use of a single user-customized identifier across multiple Web sites (Herzberg & Gbara, 2004).
User Effort	• Minimize user effort to install and use the anti-phishing application (Herzberg & Gbara, 2004). • To command user attention, integrate security into the user's workflow (Wu, Miller, & Little, 2006). • Enable expert computer users to skip or disable basic or optional features that are provided to help less-knowledgeable users (Li & Helenius, 2007).
User Education	• Combine multiple user education techniques to achieve the best over all solution (Herzog & Shahmehri, 2007). • Do not assume that the user has pre-existing knowledge about phishing (Downs et al., 2006). • Use interactive training techniques for increased learning and retention (Kumaraguru, Rhee, Acquisti, et al., 2007).

User Interface Categories	Design Principles
	• Introduce training just after users fall for phishing attacks, in the context of their goals (Kumaraguru, Rhee, Acquisti, et al., 2007; Kumaraguru, Rhee, Sheng, et al., 2007; Sheng et al., 2007). • Use less text and more graphics to simplify and clarify meaning (Kumaraguru, Rhee, Acquisti, et al., 2007). • Focus training content on basic knowledge from the user's perspective, not on general techniques used by phishers (Kumaraguru, Rhee, Acquisti, et al., 2007; Li & Helenius, 2007). • Focus training on a few simple security concepts, including secure email and Web usage, and domain name syntax (Herzberg & Gbara, 2004). • Teach users not to judge the legitimacy of Web sites by the design and appearance of its content alone (Kumaraguru, Sheng, et al., 2007). • Instruct users to call support phone numbers printed on the back of their credit cards, or from recent billing statements, not from Web sites (Jakobsson, 2007).

References

Abad, C. (2005). The Economy of Phishing: A Survey of the Operations of the Phishing Market. *First Monday*, *10*. Retrieved November 15, 2007, from http://firstmonday.org/issues/issue10_9/abad/index.html

Allen, J., Christie, A., Fithen, W., McHugh, J., Pickel, J., & Stoner, E. (2000). *State of the Practice of Intrusion Detection Technologies*. Retrieved December 1, 2007, from Carnegie Mellon University, Software Engineering Institute Web site: http://www.sei.cmu.edu/publications/documents/99.reports/99tr028/99tr028abstract.html

Alliance for Telecommunications Industry Solutions. (2001). *ATIS Telecom Glossary 2000*. Retrieved December 1, 2007, from http://www.atis.org/tg2k/

Anti-Phishing Working Group. (2007). *What is Phishing and Pharming?* Retrieved December 1, 2007, from http://www.antiphishing.org/DOJ_Special_Report_On_Phishing_Mar04.pdf

Balfanz, D., Durfee, G., Smetters, D. K., & Grinter, R.E. (2004). In Search of Usable Security: Five Lessons from the Field. *IEEE Security & Privacy*, *2*, 19-24. Retrieved October 28, 2007, from IEEE Computer Science Digital Library.

Bell, C., & Smith, C. (2007). *Critical Evaluation of Information Sources*. Retrieved November 17. 2007, from University of Oregon Web site: http://libweb.uoregon.edu/guides/findarticles/credibility.html

Berghel, H., Carpinter, J., & Jo, J.-Y. (2007). Phish Phactors: Offensive and Defensive Strategies. *Advances in Computers, 70*, 223-268. Retrieved November 3, 2007, from Web of Science database.

Binational Working Group on Cross-Border Mass Marketing Fraud. (2006). *Report on Phishing: A Report to the Minister of Public Safety and Emergency Preparedness Canada and the Attorney General of the United States.* Retrieved December 1, 2007, from http://www.usdoj.gov/opa/report_on_phishing.pdf

Bogue, R. (2006). *Creating a Common Lexicon for Software Development in Your Organization.* Retrieved December 5, 2007, from http://articles.techrepublic.com.com/5100-3513-6081740.html

Bryant, P., Furnell, S. M., & Phippen, A. D. (2007). Assessing the Security Perceptions of Personal Internet Users. *Computers & Security, 26*, 410-417. Retrieved October 28, 2007, from ScienceDirect.

Camenisch, J., Shelat, A., Sommer, D., & Zimmerman, R. (2006). Securing User Inputs for the Web. *Proceedings of the Second ACM Workshop on Digital Identity Management, USA*, pp. 33-44. Retrieved October 28, 2007, from ACM Digital Library.

Chou, N., Ledesma, R., Teraguchi, Y., Boneh, D., & Mitchell, J.C. (2004). *Client-Side Defense Against Web-Based Identity Theft.* Paper presented at the 11th Annual Network and Distributed System Security Symposium, San Diego, CA. Retrieved November 17, 2007, from http://www.isoc.org/ndss04/proceedings/Papers/Chou.pdf

Colorado State University. (n.d.). *What is a Review Paper?* Retrieved November 15, 2007, from Colorado State University, Writing Studio Web site: http://writing.colostate.edu/guides/documents/review_essay/pop2a.cfm

Cranor, L. F. (2006). What Do They "Indicate?": Evaluating Security and Privacy Indicators. *Interactions, 13*, 45-47. Retrieved October 26, 2007, from ACM Digital Library.

Dhamija, R., & Tygar, J. D. (2005a). The Battle Against Phishing: Dynamic Security Skins. *Proceedings of the 2005 Symposium on Usable Privacy and Security, USA, 93,* 77-88. Retrieved October 29, 2007, from ACM Digital Library.

Dhamija, R., & Tygar, J. D. (2005b). Phish and HIPs: Human Interactive Proofs to Detect Phishing Attacks. In H. S. Baird and D. P. Lopresti (Eds.), *Second International Workshop on Human Interactive Proofs* (pp. 127-141). Springer-Verlag Berlin Heidelberg. Retrieved November 19, 2007, from University of California, Berkeley, College of Engineering Web site: http://www.cs.berkeley.edu/~tygar/papers/Phishing/Phish_and_HIPs.pdf

Dhamija, R., Tygar, J. D., & Hearst, M. (2006). Why Phishing Works. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Canada,* pp. 581-590. Retrieved October 29, 2007, from ACM Digital Library.

Dourish, P., & Redmiles, D. (2002). An Approach to Usable Security Based on Event Monitoring and Visualization. *Proceedings of the 2002 Workshop on New Security Paradigms, USA*, pp. 75-81. Retrieved October 29, 2007, from ACM Digital Library.

Downs, J. S., Holbrook, M. B., & Cranor, L. F. (2006). Decision Strategies and Susceptibility to Phishing. *Proceedings of the Second Symposium on Usable Privacy and Security, USA*, pp. 79-90. Retrieved November 17, 2007, from ACM Digital Library.

Downs, J. S., Holbrook, M. B., & Cranor, L. F. (2007). *Behavioral Response to Phishing Risk.* Paper presented at the Second Anti-Phishing Working Group eCrime Researchers Summit, Pittsburgh, PA. Retrieved November 18, 2007, from http://www.antiphishing.org/ecrimeresearch/2007/proceedings/p37_downs.pdf

Dunham, K. (2004). Phishing isn't So Sophisticated: Scary! *Information Systems Security, 13*, 2-7. Retrieved November 3, 2007, from FirstSearch Electronic Collections Online.

Emigh, A. (2005). *Online Identity Theft: Phishing Technology, Chokepoints and Countermeasures*. Retrieved November 19, 2007, from http://www.antiphishing.org/Phishing-dhs-report.pdf

Federal Deposit Insurance Corporation. (2000). *Privacy of Consumer Financial Information.* Retrieved December 1, 2007, from http://www.fdic.gov/regulations/laws/rules/background.html

Flechais, I. (2005). *Designing Secure and Usable Systems*. Unpublished Doctoral dissertation, University of London. Retrieved October 28, 2007, from Oxford University, Software Engineering Programme Web site: http://www.softeng.ox.ac.uk/personal/Ivan.Flechais/downloads/thesis.pdf

Flinn, S., Stoyles, S. (2005). Omnivore: Risk Management Through Bidirectional Transparency. *Proceedings of the 2004 Workshop on New Security Paradigms, Canada,* pp. 97-105. Retrieved October 24, 2007, from ACM Digital Library.

Furnell, S. (2007). Phishing: Can We Spot the Signs? *Computer Fraud & Security, 2007*, 10-15. Retrieved November 25, 2007, from Science Direct.

Garfinkel, S. (2005). *Design Principles and Patterns for Computer Systems that are Simultaneously Secure and Usable.* Doctoral dissertation, Massachusetts Institute of Technology. Retrieved October 23, 2007, from WorldCat index.

Geer, D. (2005). Security Technologies Go Phishing. *Computer: Interactive Technology for Computing Professionals, 38,* 18-21. Retrieved November 3, 2007, from IEEE Computer Science Digital Library.

Goleniewski, L. (2003). *Telecommunications Essentials: The Complete Global Source for Communications Fundamentals, Data Networking and the Internet, and Next-Generation Networks*. Boston: Pearson Education, Inc.

Gross, J. B., & Rosson, M. B. (2007). Looking for Trouble: Understanding End-user Security Management. *Proceedings of the 2007 Symposium on Computer Human Interaction for the Management of Information Technology, USA, 10*, 1-10. Retrieved October 23, 2007, from ACM Digital Library.

Gutmann, P., Naccache, D., & Palmer, C. C. (2005). Security Usability. *IEEE Security & Privacy, 3*, 56-58. Retrieved October 29, 2007, from IEEE Computer Science Digital Library.

Herzberg, A., & Gbara, A. (2004). TrustBar: Protecting (even Naïve) Web Users from Spoofing and Phishing Attacks. *Cryptology ePrint Archive, Report 2004/155*. Retrieved November 19, 2007, from http://eprint.iacr.org/2004/155

Herzog, A., & Shahmehri, N. (2007). User Help Techniques for Usable Security. *Proceedings of the 2007 Symposium on Computer Human Interaction for the Management of Information Technology, USA*, pp. 1-10. Retrieved October 23, 2007, from ACM Digital Library.

Hewitt, M. (2002). *Carrying Out a Literature Review*. Retrieved November 17, 2007, from http://128.223.179.107/aim/Capstone07/HewittLitReview.pdf

Institute of Electrical and Electronics Engineers. (1990). *IEEE Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries.* New York: Author.

Jakobsson, M. (2005). *Modeling and Preventing Phishing Attacks*. Retrieved November 13, 2007, from Indiana University, School of Informatics Web site: http://www.informatics.indiana.edu/markus/papers/phishing_jakobsson.pdf

Jakobsson, M. (2007). *The Human Factor in Phishing*. Retrieved November 21, 2007, from Indiana University, School of Informatics Web site: http://www.informatics.indiana.edu/markus/papers/aci.pdf

Jakobsson, M., & Tsow, A. (2007). *Deceit and Deception: A Large User Study of Phishing*. Retrieved November 20, 2007, from Indiana University, School of Informatics Web site: http://www.informatics.indiana.edu/research/publications/publications.asp?id=23

Jakobsson, M., Young, A. (2005). Distributed Phishing Attacks. *Cryptology ePrint Archive, Report 2005/09*. Retrieved November 22, 2007, from http://eprint.iacr.org/2005/091.pdf

James, L. (2005). *Phishing Exposed*. Rockland, MA: Syngress Publishing.

Kobsa, A., Schreck, J. (2003). Privacy Through Pseudonymity in User-Adaptive Systems. *ACM Transactions on Internet Technology, 3*, 149-182. Retrieved January 7, 2008, from ACM Digital Library.

Kumaraguru, P., Rhee, Y., Acquisti, A., Cranor, L. F., Hong, J., & Nunge, E. (2007). Protecting People from Phishing: The Design and Evaluation of an Embedded Training Email System. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, USA*, pp. 905-914. Retrieved November 19, 2007, from ACM Digital Library.

Kumaraguru, P., Rhee, Y., Sheng, S., Hasan, S., Acquisti, A., Cranor, L. F., & Hong, J. (2007). *Getting Users to Pay Attention to Anti-Phishing Education: Evaluation of Retention and Transfer*. Paper presented at the Second Anti-Phishing Working Group eCrime Researchers Summit, Pittsburgh, PA. Retrieved December 14, 2007, from http://www.ecrimeresearch.org/2007/proceedings/p70_kumaraguru.pdf

Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L.F., & Hong, J. (2007). *Teaching Johnny Not to Fall for Phish* (Cylab Technical Report). Pittsburgh, PA: Carnegie Mellon University, Usable Privacy and Security Laboratory. Retrieved December 14, 2007, from http://www.cylab.cmu.edu/default.aspx?id=2275

Leedy, P., & Ormrod, J. (2005). *Practical Research: Planning and Design*. New Jersey: Pearson/Prentice Hall.

Li, L., & Helenius, M. (2007). Usability Evaluation of Anti-phishing Toolbars. *Journal of Computer Virology*, *3*, 163-184. Retrieved October 28, 2007, from FirstSearch Electronic Collections Online.

Lininger, R., & Vines, R.D. (2005). *Phishing: Cutting the Identity Theft Line*. Indianapolis: Wiley Publishing.

Long, A. C., Moskowitz, C., & Ganger, G. R. (2003). *A Prototype User Interface for Coarse-grained Desktop Access Control*. Pittsburgh, PA: School of Computer Science, Carnegie Mellon University. Retrieved October 24, 2007, from WorldCat index.

Microsoft. (2007). *Anti-Phishing Technologies Overview*. Retrieved December 1, 2007, from http://www.microsoft.com/mscorp/safety/technologies/antiphishing/overview.mspx

Miller, R. C., & Wu, M. (2005). Fighting Phishing at the User Interface. In L. F. Cranor & S. Garfinkel (Eds.), *Security and Usability: Designing Secure Systems That People Can Use* (pp. 276-292). Sebastopol, CA: O'Reilly.

Milletary, J. (2005). *Technical Trends in Phishing Attacks.* Retrieved December 1, 2007, from http://www.us-cert.gov/reading_room/phishing_trends0511.pdf

Moore, T., & Clayton, R. (2007). *An Empirical Analysis of the Current State of Phishing Attack and Defence*. Retrieved November 18, 2007, from University of Cambridge, Computer Laboratory Web site: http://www.cl.cam.ac.uk/~rnc1/weis07-phishing.pdf

Nicolett, M. (2003). *Gartner Research Archive: Client Issues for Security and Privacy*. Retrieved December 1, 2007, from http://www.gartner.com/DisplayDocument?doc_cd=117614

Obenzinger, H. (2005). *"What Can a Literature Review Do For Me?": How to Research, Write, and Survive a Literature Review.* Retrieved November 15, 2007, from http://128.223.179.107/aim/Capstone07/LiteratureReviewHandout.pdf

Ormondroyd, J., Engle, M., & Cosgrave, T. (2004). *Critically Analyzing Information Sources*. Retrieved November 17, 2007, from Cornell University Library Web site: http://www.library.cornell.edu/olinuris/ref/research/skill26.htm#

Parno, B., Kuo, C., & Perrig, A. (2006). Phoolproof Phishing Prevention. In G. Di Crescenzo and A. Rubin (Eds.), *Tenth International Financial Cryptography and Data Security Conference* (pp. 1-19). IFCA/Springer-Verlag Berlin Heidelberg. Retrieved November 4, 2007, from the Web of Science database.

PC Magazine Encyclopedia: Definition of Browser Chrome. (n.d.). Retrieved December 1, 2007, from http://www.pcmag.com/encyclopedia_term/0,2542,t=browser+chrome&i=38972,00.asp

Privacy Rights Clearinghouse. (2005). *Alert: Watch Out for "Phishing" Emails Attempting to Capture Your Personal Information*. Retrieved November 1, 2007, from http://www.privacyrights.org/ar/phishing.htm

Rapple, B. (2005). *How Do I Write a Literature Review?* Retrieved December 5, 2007, from Boston College Web site: http://www.bc.edu/libraries/research/howdoi/s-litreview/

Regan, Priscilla. (2005). *The Role of Consent in Information Privacy Protection.* Retrieved December 1, 2007, from http://www.cdt.org/privacy/ccp/consentchoice2.shtml

Robila, S. A., & Ragucci, J. W. (2006). Don't be a Phish: Steps in User Education. *Proceedings of the Eleventh Annual SIGCSE Conference on Innovation and Technology in Computer Science Education, Italy*, pp. 237-241. Retrieved November 19, 2007, from ACM Digital Library.

Sasse, M.A., & Flechais, I. (2005). Usable Security. In L. F. Cranor & S. Garfinkel (Eds.), *Security and Usability: Designing Secure Systems That People Can Use* (pp. 13-30). Sebastopol, CA: O'Reilly.

Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L. F., Hong, J., & Nunge, E. (2007). Anti-Phishing Phil: The Design and Evaluation of a Game that Teaches People Not to Fall for Phish. *Proceedings of the Third Symposium on Usable Privacy and Security, USA,* pp. 88-99. Retrieved November 30, 2007, from ACM Digital Library.

Smetters, D. K., & Grinter, R. E. (2002). Moving from the Design of Usable Security Technologies to the Design of Useful Secure Applications. *Proceedings of the 2002 Workshop on New Security Paradigms, USA,* pp. 82-89. Retrieved October 28, 2007, from ACM Digital Library.

Soegaard, M. (2005). *Transparency*. Retrieved January 7, 2008, from http://www.interaction-design.org/encyclopedia/transparency.html

Steinberg, B. (2005, March 22). Call to Action Ads Give Clients Results They Can Measure. *The Wall Street Journal – Eastern Edition,* pp. B1-B4.

Stone, D., Jarrett, C., Woodroffe, M., & Minocha, S. (2005). *User Interface Design and Evaluation*. San Francisco: Elsevier.

Topkara, M., Kamra, A., Atallah, M., & Nita-Rotaru, C. (2005). *ViWiD: Visible Watermarking based Defense Against Phishing* (CERIAS Tech Report 2005-35). West Lafayette, IN: Purdue University, Center for Education and Research in Information Assurance and Security. Retrieved November 19, 2007, from https://www.cerias.purdue.edu/tools_and_resources/bibtex_archive/archive/2005-35.pdf

University of North Carolina. (n.d.). *Literature Reviews*. Retrieved December 5, 2007, from www.unc.edu/depts/wcweb/handouts/literature_review.html

University of Pittsburgh, Institute for Learning. (n.d.). *The Principle of Learning Tools*. Retrieved January 1, 2008, from http://ifl.lrdc.pitt.edu/ifl/index.php?section=pol

University of Washington, Computing & Communications. (2007). *Using Secure Sockets Layer*. Retrieved December 1, 2007, from http://www.washington.edu/computing/web/publishing/ssl.html

University of Wisconsin. (2006). *University of Wisconsin Writing Center Writer's Handbook: Review of Literature*. Retrieved December 5, 2007, from http://www.wisc.edu/writing/Handbook/ReviewofLiterature.html

U.S. Computer Emergency Readiness Team. (2002). *Home Computer Security Glossary*. Retrieved December 1, 2007, from http://www.us-cert.gov/reading_room/HomeComputerSecurity/glossary.html

U.S. Department of Commerce. (2002). *Definition: e-Commerce*. Retrieved November 22, 2007, from http://www.its.bldrdoc.gov/projects/devglossary/_e-commerce.html

van der Merwe, A., Loock, M., & Dabrowski, M. (2005). Characteristics and Responsibilities Involved in a Phishing Attack. *Proceedings of the Fourth International Symposium on Information and Communication Technologies, South Africa,* pp. 249-254. Retrieved November 20, 2007, from ACM Digital Library.

Whalen, T., & Inkpen, K. M. (2005). Gathering Evidence: Use of Visual Security Cues in Web Browsers. *Proceedings of Graphics Interface 2005, Canada,* pp. 137-144. Retrieved October 28, 2007, from ACM Digital Library.

Winograd, T. (1996). *Bringing Design to Software*. Indianapolis: Addison-Wesley Professional.

Wu, M., Miller, R. C., & Garfinkel, S. L. (2006). Do Security Toolbars Actually Prevent Phishing Attacks? *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Canada,* pp. 601-610. Retrieved October 28, 2007, from ACM Digital Library.

Wu, M., Miller, R. C., & Little, G. (2006). Web Wallet: Preventing Phishing Attacks by Revealing User Intentions. *Proceedings of the Second Symposium on Usable Privacy and Security, USA,* pp. 102-113. Retrieved October 28, 2007, from ACM Digital Library.

Yee, K.- P. (2005). Guidelines and Strategies for Secure Interaction Design. In L. F. Cranor & S. Garfinkel (Eds.), *Security and Usability: Designing Secure Systems That People Can Use* (pp. 247-273). Sebastopol, CA: O'Reilly.

Zurko, M. E. (2005). *User-centered Security: Stepping Up to the Grand Challenge*. Paper presented at the Twenty-first Annual Computer Security Applications Conference, Tucson, AZ. Retrieved October 24, 2007, from http://www.acsa-admin.org/2005/essay.html

Zurko, M.E., & Simon, T.(1996). User-Centered Security. *Proceedings of the 1996 Workshop on New Security Paradigms, USA,* pp. 27-33.

Appendix A – Search Record

Table 4: Detailed Record of Searches

Database/ Search Engine	Search Terms	Results: #	Eligible Titles Found	Comments
ACM Digital Library	Usability + security	200	**Eligible results:** 18	This library is an excellent resource for the topic.
	User-centered + security	200	**Eligible results:** 0 Eligible titles found are duplicates from other searches.	
	HCISEC	16	**Eligible results:** 0 Eligible titles found are duplicates from other searches.	
	Security + interface design	200	**Eligible results:** 4	
	End-user + security	200	**Eligible results:** 17 Most found titles do not apply to home users (or consumers).	
	Computer + security	200	**Eligible results:** 0 Found titles do not generally tie back to usability topic.	
	Visualization for computer security	200	**Eligible results:** 0 Found titles do not generally tie back to usability topic.	
	Computer security + usability	200	**Eligible results:** 0 Eligible titles found are duplicates from other searches.	
	Usable security + phishing + computer	143	**Eligible results:** 29	
	Phishing attack	200	**Eligible results:** 3	

Database/ Search Engine	Search Terms	Results: #	Eligible Titles Found	Comments
	Spoofing	200	**Eligible results:** 0 Eligible titles found are duplicates from other searches.	
	Phishing end-user threat	200	**Eligible results:** 1 Most eligible titles found are duplicates from other searches.	
	Phishing	200	**Eligible results:** 0 Eligible titles found are duplicates from other searches.	
	Anti-phishing	36	**Eligible results:** 3	
	Phishing + learning + training	200	**Eligible results:** 0 Eligible titles found are duplicates from other searches.	
	Phishing + user help + online	200	**Eligible results:** 1 Most titles found are duplicated from other searches.	
Alexandria Computing Center Documents	Usability + computer security	0	**Eligible results:** 0	This database is not productive for this topic and was dropped after initial searches.
	Security interface design	0	**Eligible results:** 0	
	End-user security	0	**Eligible results:** 0	
	Computer security usability	0	**Eligible results:** 0	
CiteSeer Scientific Literature Digital Library	Usability + security	588	**Eligible results:** 0	This search engine/index is a good resource for academic-quality literature related to the topic.
	Computer security + user interface design	500	**Eligible results:** 1 Found titles do not generally tie back to usability topic.	

Database/ Search Engine	Search Terms	Results: #	Eligible Titles Found	Comments
	Computer security + usability	500	**Eligible results:** 0	
	HCISEC	4	**Eligible results:** 1	
	Phishing	18	**Eligible results:** 7	
	Phishing attack	4	**Eligible results:** 0 Eligible titles found are duplicates from other searches.	
	Spoofing	490	**Eligible results:** 1	
	Phishing + end-user + threat	0	**Eligible results:** 0	
	Anti-phishing	4	**Eligible results:** 0 Eligible titles found are duplicates from other searches.	
	Phishing + learning + training	500	**Eligible results:** 0	
	Phishing + user help + online	500	**Eligible results:** 0	
EBSCO HOST Research Databases – Academic Search Premier Index	Usability + security	226	**Eligible results:** 5	This index provided some good results and is worth continued exploration with the focused topic: phishing.
	User-centered + security	5		
	HCISEC	0	**Eligible results:** 0	
	Security + user interface design	0	**Eligible results:** 0	
	End-user + security	3	**Eligible results:** 0	
	Computer + security + usability	1	**Eligible results:** 0	
	Visualization for computer security	0	**Eligible results:** 0	

Database/ Search Engine	Search Terms	Results: #	Eligible Titles Found	Comments
	Computer security + usability	1	**Eligible results:** 0	
	Usable security + phishing + computer	0	**Eligible results:** 0	
	Phishing attack	81	**Eligible results:** 0 A significant number of relevant titles are found, however they are not of academic quality.	
	Spoofing	225	**Eligible results:** 0 A significant number of relevant titles are found, however they are not of academic quality.	
	Phishing + end-user + threat	4	**Eligible results:** 0 Full text articles are unavailable.	
	Phishing	494	**Eligible results:** 0 A significant number of relevant titles are found, however they are not of academic quality.	
	Anti-phishing	70	**Eligible results:** 0 A significant number of relevant titles are found, however they are not of academic quality.	
	Phishing + learning + training	0	**Eligible results:** 0	
	Phishing + user help + online	0	**Eligible results:** 0	
FirstSearch Electronic Collections Online	Usability + security	69	**Eligible results:** 2	This index provided some good results and is worth continued exploration with the
	User-centered + security	4	**Eligible results:** 0	

Database/ Search Engine	Search Terms	Results: #	Eligible Titles Found	Comments
	HCISEC	0	**Eligible results:** 0	focused topic: phishing.
	Security + user interface design	9	**Eligible results:** 0	
	Computer security + user interface design	3	**Eligible results:** 0	
	End-user + security	16	**Eligible results:** 0	
	Visualization for computer security	6	**Eligible results:** 0	
	Computer security + usability	15	**Eligible results:** 0	
	Usable security + phishing	46	**Eligible results:** 2	
	Phishing	12	**Eligible results:** 0	
	Phishing + learning + training	0	**Eligible results:** 0	
	Phishing + user help + online	0	**Eligible results:** 0	
Google CiteSeer Search Engine/Index	Phishing	153	**Eligible results:** 18	This index is a good resource for academic-quality literature and is worth continued exploration with the focused topic: phishing.
	Phishing attack	41	**Eligible results:** 4 Most eligible titles found are duplicates from other searches.	
	Spoofing	573,000	**Eligible results:** 0 The search term is too broad and most results are not related to “phishing,” even when coupled with another term. Drop this term.	
	Phishing end-user threat	0	**Eligible results:** 0	

Database/ Search Engine	Search Terms	Results: #	Eligible Titles Found	Comments
	Anti-phishing	10	**Eligible results:** 4 Most eligible titles found are duplicates from other searches.	
	Phishing + learning + training	1	**Eligible results:** 0	
	Phishing + user help + online	57	**Eligible results:** 0 Eligible titles found are duplicates from other searches.	
Google Scholar Search Engine	Phishing + usable security + usability	262	**Eligible results:** 20	This search engine is an excellent resource for the topic. The results are accurate and the search engine provides the ability to filter by authors who are repeatedly cited in the field.
	Usability security	42,900	**Eligible results:** 0 Search is too broad.	
	Phishing	4,320	**Eligible results:** 0 Eligible titles found are duplicates from other searches.	
	Phishing attack	2,110	**Eligible results:** 1 Most eligible titles found are duplicates from other searches.	
	Spoofing phishing, then filtered to Spoofing phishing design	21,600	**Eligible results:** 2	
	Phishing + end-user + threat	432	**Eligible results:** 0	
	Anti-phishing	687	**Eligible results:** 2	
	Phishing + learning + training	624	**Eligible results:** 4	
	Phishing + user help	5	**Eligible results:** 0	

Database/ Search Engine	Search Terms	Results: #	Eligible Titles Found	Comments
IEEE Computer Science Digital Library	Usable security	100	**Eligible results:** 2	This library is a good resource for academic-quality literature and is worth continued exploration with the focused topic: phishing.
	Phishing	58	**Eligible results:** 12 Most (many) eligible titles found are duplicates from other searches.	
	Phishing attack	21	**Eligible results:** 0 Eligible titles found are duplicates from other searches.	
	Spoofing	210	**Eligible results:** 0 Most titles found are too technical in nature.	
	Phishing end-user threat	0	**Eligible results:** 0	
	Anti-phishing	9	**Eligible results:** 0 Eligible titles found are duplicates from other searches.	
	Phishing + learning + training			
	Phishing + user help + online			
Library of Congress	Usable security + phishing	20	**Eligible results:** 4	This index provided some good results and is worth continued exploration with the focused topic: phishing.
	Phishing	15	**Eligible results:** 0 Eligible titles found are duplicates from other searches.	
	Phishing attack	1	**Eligible results:** 0	
	Spoofing	10	**Eligible results:** 1	
	Phishing end-user threat	10,000	**Eligible results:** 1	
	Anti-phishing	10,000	**Eligible results:** 2	

Database/ Search Engine	Search Terms	Results: #	Eligible Titles Found	Comments
	Phishing + learning + training	0	**Eligible results:** 0	
	Phishing + online help	2	**Eligible results:** 0	
OneSearch Quicksets / Sciences	Usability + security	108	**Eligible results:** 3 Many titles are duplicates from other searches.	This index did not yield many successful searches, even though it incorporates databases and indexes from other sources in the search plan. It is interesting to note that this tool did not yield the productive results provided by individual searches of the same databases.
	User-centered + security	36	**Eligible results:** 2	
	HCISEC	0	**Eligible results:** 0	
	Security + user interface design	559	**Eligible results:** 4 Few relevant titles, search is too broad.	
	Computer security + user interface design	308	**Eligible results:** 1 Most titles are unrelated to the topic, despite significant number of results.	
	End-user + security	8	**Eligible results:** 0	
	Visualization for computer security	0	**Eligible results:** 0	
	Computer security + usability	4	**Eligible results:** 0	
	Usable security + phishing	57	**Eligible results:** 1	
	Phishing learning + training	1	**Eligible results:** 0	
	Phishing user help + online	5	**Eligible results:** 0	
Summit Union Catalog	Usable security	10	**Eligible results:** 0	This catalog provided limited value for the
	End-user security	7	**Eligible results:** 0	

Database/ Search Engine	Search Terms	Results: #	Eligible Titles Found	Comments
	User-centered Security	2	**Eligible results:** 0	topic. However, the catalog is very easy to search using the UO Libraries Catalog user interface.
	HCISEC	0	**Eligible results:** 0	
	Security interface design	12	**Eligible results:** 0	
	Usability + security	12	**Eligible results:** 3 Usability + security increased quality of results.	
	Phishing + security + computer	1	**Eligible results:** 1 This is the same title that was found in UO Library Catalog.	
	Human-computer interaction + phishing	0	**Eligible results:** 0	
	Phishing attack	1	**Eligible results:** 1	
	Spoofing	1	**Eligible results:** 1	
	Phishing end-user threat	0	**Eligible results:** 0	
	Phishing	16	**Eligible results:** 4 found; unable to obtain full text source. Result is then 0.	
	Anti-phishing	0	**Eligible results:** 0	
	Phishing + learning + training	0	**Eligible results:** 0	
	Phishing + user help + online	0	**Eligible results:** 0	
UO Libraries Catalog	Usable + security	4	**Eligible results:** 0	This catalog provided limited value for the topic.
	End-user security	2	**Eligible results:** 0	
	User-centered + security	2	**Eligible results:** 0	
	User interaction design + security	0	**Eligible results:** 0	
	HCIsec	0	**Eligible results:** 0	

Database/ Search Engine	Search Terms	Results: #	Eligible Titles Found	Comments
	Phishing + security + computer	18,771	**Eligible results:** 0 Search is too broad and after skimming titles, content found is not highly relevant. Worth continued search refinement.	
	Human-computer interaction + phishing	0	**Eligible results:** 0	
	Phishing attack	0	**Eligible results:** 0	
	Spoofing	1	**Eligible results:** 0	
	Phishing end-user threat	0	**Eligible results:** 0	
	Phishing	3	**Eligible results:** 0	
	Anti-phishing	0	**Eligible results:** 0	
	Phishing + learning + training	0	**Eligible results:** 0	
	Phishing + user help + online	0	**Eligible results:** 0	
Web of Science Index	Usable security	57	**Eligible results:** 4 Most eligible titles found are duplicates from Academic Search Premier.	This index is a good resource for eligible literature, however some articles are unavailable. It is worth pursuing as part of the search strategy.
	Phishing	41	**Eligible results:** 11 Many full text articles are unavailable.	
	Phishing attack	3	**Eligible results:** 0	
	Spoofing	133	**Eligible results:** 0 Eligible titles found are duplicates from other searches.	
	Phishing end-user threat	0	**Eligible results:** 0	

Database/ Search Engine	Search Terms	Results: #	Eligible Titles Found	Comments
	Anti-phishing	6	**Eligible results:** 0 Eligible titles found are duplicates from other searches.	
	Phishing + learning + training	0	**Eligible results:** 0	
	Phishing + user help + online	0	**Eligible results:** 0	
WorldCat Index	Usability + security	69	**Eligible results:** 6	This index provided some good results and is worth continued exploration with the focused topic: phishing.
	User-centered + security	2	**Eligible results:** 1	
	HCISEC	0	**Eligible results:** 0	
	Security + interface design	140	**Eligible results:** 2	
	End-user + security	82	**Eligible results:** 0	
	Computer + security	23,291	**Eligible results:** 0 Search is too broad. Based on the results, narrowed down the keyword list. Searched again adding the term “usability” (for a third keyword), which did not yield any new, eligible results.	
	Visualization for computer security	0	**Eligible results:** 0	
	Computer security + usability	13	**Eligible results:** 0	
	Usable security + phishing + computer	1	**Eligible results:** 1	

Database/ Search Engine	Search Terms	Results: #	Eligible Titles Found	Comments
	Phishing attack	99	**Eligible results:** 0 This search provided a good set of results. However, the articles and books found are duplicates from other searches, or literature is not of academic quality.	
	Spoofing	137	**Eligible results:** 0 This search provided some eligible results. However, the articles and books found are duplicates from other searches. Many results were not related to "phishing," so this keyword may not be a good strategy.	
	Phishing end-user threat	0	**Eligible results:** 0	
	Phishing	95	**Eligible results:** 14	
	Anti-phishing	11	**Eligible results:** 0 Eligible titles found are duplicates from other searches.	
	Phishing + learning + training	0	**Eligible results:** 0	
	Phishing + user help + online	0	**Eligible results:** 0	