Communications of the Association for Information Systems

# UNVEILING THE MASK OF PHISHING: THREATS, PREVENTIVE MEASURES, AND RESPONSIBILITIES

Indranil Bose
Alvin Chung Man Leung
School of Business
The University of Hong Kong
bose@business.hku.hk

**ABSTRACT**

Phishing, a new-rise identity fraud of this century has already caused huge financial loss and social disorder. This paper provides an overview of the evolution and forecasted trend of phishing activities with detailed analysis on common phishing features, proliferation channels, relevant anti-phishing measures, related legislation, and an anti-phishing framework from the perspective of social responsibility. The objective of the research is to enhance public awareness of phishing and to inform end users and owners of e-commerce sites proper measures to detect and prevent this criminal activity.

**Keywords:** anti-phishing, authentication, bogus Web sites, identity theft, fraudulent e-mail, phishing.

## I. INTRODUCTION

The Web is one of the most popular media for handling financial transactions in the new millennium. As it is a more efficient medium than conventional banking channels many people own one or more electronic bank accounts for monetary transactions. However, the new medium brings with it many new dangers. Phishing is one such new-rise online crime that aims to steal personal identity data and financial account credentials [Anti-Phishing Working Group (APWG) 2006]. Making use of the Internet, the adversary spreads e-mails to the general public to entice them to click on embedded links to bogus Web sites and in the process retrieves their usernames and passwords when they input their data at the bogus Web site. About 5 percent of phishing e-mail recipients respond to fraudulent e-mails [APWG 2006]. In another study conducted by Gartner, it was found that 57 million Internet users in the U.S. received e-mails related to phishing scams, and phishers were able to successfully entice about 2 million people to release their sensitive information [Kirda and Kruegel 2005]. The number of phishing incidents reported in the past few years is on a steady rise. A report released by APWG in 2006 claims that from December 2004 to December 2005, phishing incidents have grown at an astonishing rate of 72.66 percent. More surprisingly, during 2004 the number of reported phishing incidents has risen nearly 4,000 percent in just 6 months [James 2005]. It is an alarming situation, and action needs to be taken to prevent the proliferation of such a dangerous crime.

The main driving force behind this crime is the lucrative amount of money involved in online transactions. In a study conducted by Gartner, it was reported that for the year ending April 2004,

there were 1.8 million phishing attacks that caused financial loss worth U.S. $1.2 billion [Geer 2005]. In a single phishing incident that affected HSBC Hong Kong in October 2004, the total financial loss amounted to HK$66,000 and the incident affected a dozen customers [Richardson 2004]. The ubiquity of the Internet technology has made phishing an easy crime to accomplish. Setting up a bogus Web site does not require a lot of money or effort, and existing technology allows one to clone a genuine Web site at minimum cost and in little time.

In the next section, we provide a background of phishing. In the third section, we talk about some common characteristics of phishing followed by some ways to identify phishing, general guidelines to prevent this crime, and a description of relevant anti-phishing technologies. Next, we detail the latest trends in phishing attacks and counter measures. The following section lists the corporate and individual social responsibilities against phishing and proposes a suitable anti-phishing framework. Finally we conclude this paper with some advice on protection strategies against phishing.

## II. BACKGROUND OF PHISHING

The term *phishing* first appeared on the alt.2600 hacker newsgroup in January 1996. The word "phishing" consists of two parts – "ph" and "ishing." In the past, hackers commonly used the letters "ph" to mean "phone phreaking." In the hacker terminology, "ph" replaced the letter "f." The letter "f" joining the second word "ishing" (i.e. "fishing") describes the action of phishing, which means using bait to allure people. The first incidence of phishing can be traced back to the American Online (AOL) theft case that occurred in 1995 [James 2005]. Throughout the past decade, techniques of phishing have evolved a lot with the advancement of technology.

The most commonly used channel of phishing is e-mail. Making use of the loop hole of Simple Mail Transfer Protocol (SMTP), the phisher can arbitrarily set the "mail from" and "reply to" headers to impersonate another person, especially staff members of a financial institution. Phishers either ask victims to reply to the e-mail with confidential information or click on a link in the e-mail to a bogus Web site that can trap personal information. In the bogus Web sites the phishers typically use logos and trademarks downloaded from genuine Web sites.

The second channel to spread phishing messages is via instant messengers. Online communication software like ICQ, MSN Messenger, Yahoo! Messenger, etc. provides an excellent channel for peer-to-peer communication and broadcasting. Figure 1 illustrates an example of phishing message sent via ICQ. Phisher (called "Anonymous" in the example) may pretend to be a friend and spreads mass ICQ messages to entice people to click on the hyperlink to a phishing site that contains malicious programs or that resembles another popular Web site which the victim frequents from time to time. Once the user goes to the Web site (say www.phishing.com) the phisher will steal the user's personal information covertly or the phishing Web site that resembles a genuine one will request login information from the user.

The third popular channel for phishing is through malicious programs. Computer viruses that damage software and hardware of personal computers and Trojan, which provides a backdoor for remote access and control to an unauthorized third party, also belong to this category [Kienzle and Elder 2003]. Usually phishers send those programs as attachments using mass e-mail or through instant messengers. Once the malicious programs gain access to the victims' computers, they can steal personal information of victims and send them to the adversary surreptitiously. When these programs affect a large number of PCs, a wide phishing network is formed. Hijacked servers are used as servers to host bogus Web sites and spread phishing e-mails.


Figure 1. Example of Phishing Message Sent via Instant Messenger

The fourth phishing method is through Web-based delivery. Once a victim enters a Web site by clicking onto the link embedded in an e-mail or message of an instant messenger, malicious programs will be implanted on the computer of the victim that steal his/her private information once they conduct online transactions using the same computer. The transfer of malicious programs from the Web to a computer is difficult unless the user is careless and opens a suspicious file. By making use of pop-ups, frameless windows or zero-sized contaminated graphics it is easy to make the transfer unnoticeable to the user. Phishing channels such as e-mail and instant messenger are the most popular and they account for 90 percent of the phishing attacks. Malicious programs and Web-based malicious program delivery lead to 10 percent of phishing attacks. In December 2005, APWG recorded 180 cases of password stealing malicious code (unique applications) and 1912 password stealing malicious code URLs [APWG 2006].

In addition to these well-known paths, phishers have recently started to use a new trick called pharming [Madsen et al. 2005]. Instead of targeting individual customers of financial institutions, phishers hack Domain Name Servers (DNS) and change the pointer of the server from a genuine Web site to a bogus one. When users surf the Web, the DNS convert the Uniform Resource Locator (URL) they type in the address bar of the browser to binary address. When the DNS entry is modified, as the user types in the correct URL of a financial institution, the browser directs him/her to a bogus Web site. As pharming is very sophisticated and difficult to detect, experts believe that pharming will outgrow phishing in future.

Though techniques of phishing vary, the main idea is the same. A phisher tries different methods to make victims believe that he/she is a trustable third party and make them open an e-mail, click an embedded link, download attached documents or give away personal information. In the next section, we provide an in-depth analysis of phishing attacks and relevant anti-phishing measures.

## III. COMMON PHISHING TECHNIQUES

If one is careful enough, phishing attacks can be easily spotted. In this section, we discuss various ways to identify possible phishing tricks based on common features of phishing e-mails.

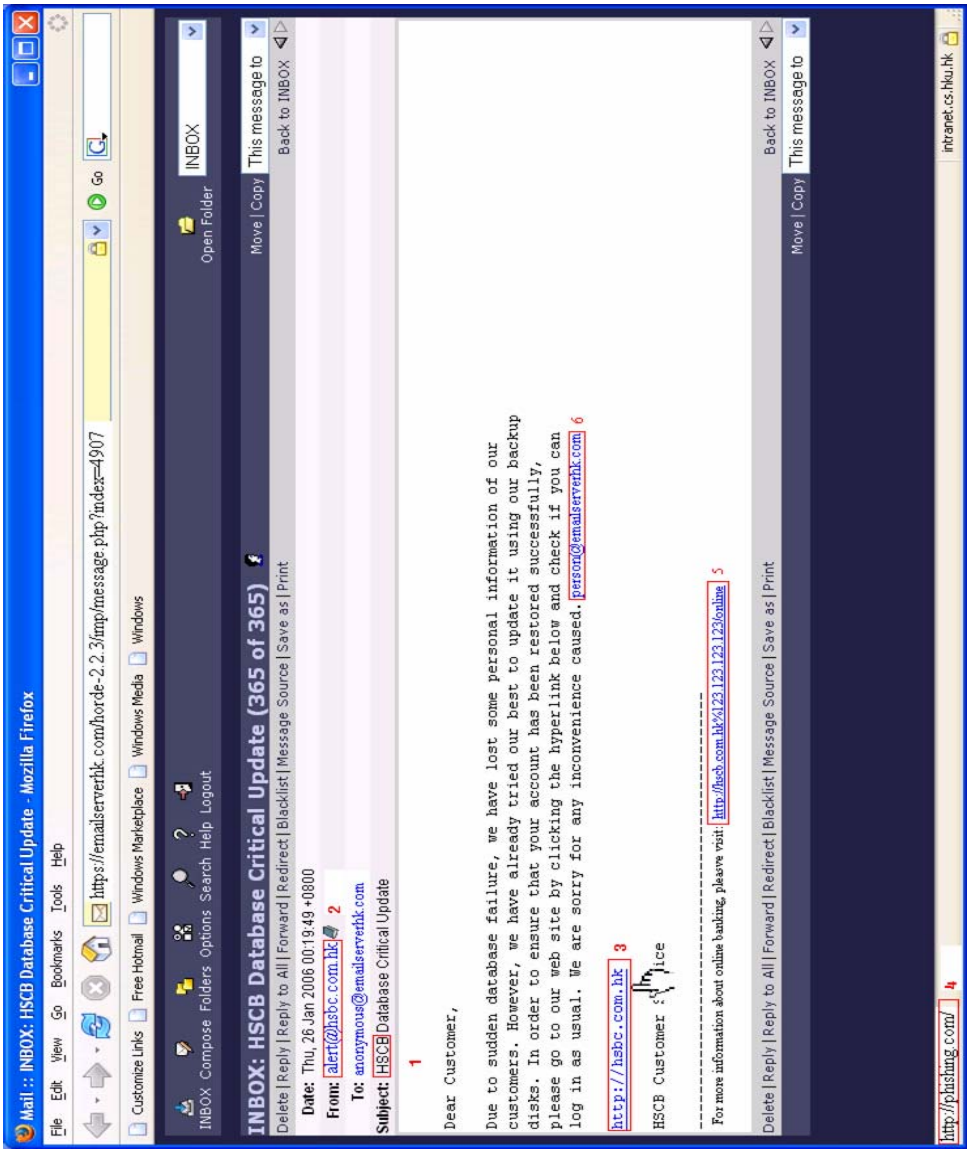


Figure 2. Example of Phishing E-mail

Figure 2 shows a typical phishing e-mail. Usually, a phishing e-mail may possess some special features as shown in Table 1.

### SPELLING MISTAKES

A common feature of phishing e-mails is that they usually contain some obvious spelling mistakes. Sometimes the difference between the incorrect and correct spellings may be a difference in the position of alphabet and the difference is so subtle that it remains unnoticed by unsuspecting users.

Table 1. Features of Phishing E-mail Shown in Figure 2

| | | |
|---|---|---|
| 1. | Spelling mistake | Instead of HSBC, phisher wrongly spells HSCB |
| 2. | Strange words in "From" field | alert@hsbc.com.hk, where "alert" usually does not appear in normal company circulated e-mails |
| 3. | Clickable link | http://hsbc.com.hk |
| 4. | Unmatched Web address | When one places a cursor over a clickable link, which appears to be true, the real address at the bottom of the browser shows otherwise. In the above example: http://phishing.com obviously does not match that of http://hsbc.com.hk |
| 5. | Special characters in hyperlinks | http://hscb.com.hk%123.123.123.123/online contains special characters "%" and numeric addresses "123.123.123.123", which may be an example of scripting language trick |
| 6. | Random name or e-mail address | Phishers usually use computer programs to generate phishing e-mails randomly. Due to program bugs some random names or e-mail addresses may appear in the content of e-mail. In the above example, the e-mail content contains a random e-mail address: person@e-mailserverhk.com |

**UNMATCHED LOGOS**

In order to enhance the trustworthiness of the e-mail, phishers usually include a company logo. Sometimes there exist some subtle differences between the forged logo in the phishing e-mail and the genuine one. Often the difference may be in the color of the logo.

**TITLES OF "FROM" FIELD**

In some phishing e-mails, although the domain name of the sender is the same as that of a genuine company, the "from" field may contain some wordings like "alert" and "danger," for instance, alert@citibank.com. It is the duty of the e-mail recipient to check whether the username of the sender makes sense or not.

**E-MAIL HEADERS**

In some phishing examples, the header of the e-mails received do not match that of the company being forged. As many people do not pay attention to e-mail headers, it is easy for phishers to allow this to happen.

**RANDOM NAMES IN BODY OF E-MAIL**

Phishers generate phishing e-mails using computer programs. Hence, it may happen that due to some program bug, some random name or e-mail address may appear in the body of the forged e-mail. If one goes through the content of the e-mail carefully, it can be spotted easily.

**CLICKABLE LINKS**

One of the major traps in a phishing e-mail is a clickable URL which usually leads to a bogus Web site. Phishers use the in-built function of HTML to disguise the actual address of the (URL). For example, let us consider the HTML trick <a href=http://fakebank.com>http://www.realbank.com</a>. Under this scheme, though the genuine URL http://www.realbank.com appears in the text of the e-mail, the default Web browser directs the recipient to a bogus Web site http://fakebank.com.

### SPECIAL CHARACTERS IN HYPERLINKS

Apart from URL many phishing e-mails also contain some hyperlinks with special characters such as "%", number or "@."Phishers usually try to use vulnerabilities of the Web browser or HTML built-in functions. Some old browsers ignore the first part of address before symbol "@."If one clicks a hyperlink such as http://realbank.com@www.123.123.123.123, he/she will be directed to www.123.123.123.123 instead of http://realbank.com.

### INCORRECT URLS

Bogus Web sites usually do not possess the same URL as real ones even though the content may appear the same. In general, a forged Web address is in numeric form, for instance http://123.456.789.012. Sometimes an adversary may register a domain name which looks quite similar to the actual one but is actually not the same one. Instead of http://realbank.com a bogus Web site may have an address with an extra character such as http://realbanke.com or have some characters in reverse order as in http://realbnak.com. This minor mistake is sometimes difficult to detect by a user.

### ABSENCE OF SERVER CERTIFICATES

Though one can easily clone the content of a Web site, it is difficult to forge a server certificate. Checking the pad lock at the bottom of a Web browser may reveal that it is a fake one and does not link to the server certificate.

## IV. MEASURES AGAINST PHISHING

In order to better protect customers, many financial institutions send mass e-mail instructing customers to be aware of phishing. Furthermore, some companies also take a proactive approach to combat potential phishing attacks. In this section we discuss the various measures adopted by companies to combat the threat of phishing.

### E-MAIL SCAN

In order to better protect customers or employees, some e-mail service providers (ESP) set up filters to get rid of potential phishing e-mails. Cyota set up an Anti Fraud Command Centre in Israel with 30 security analysts. Each day, they scanned 1 billion incoming e-mails and checked for signs of phishing [Knight 2005]. Using this proactive e-mail scan ESPs can filter out suspicious phishing e-mails and prevent them from reaching the destined e-mail recipients.

### MONITORING TRANSACTION LOGS

Phishers usually target a number of customers. Once they retrieve personal information such as usernames and passwords of adequate number of customers of a particular financial institution they try to withdraw money from the accounts of victims. Some companies have set up a special team for monitoring daily transaction logs. If various transactions of different accounts are conducted from the same IP address, the company may suspend action from that IP address and take immediate action against it. If a transaction involving a large amount of money occurs at a particular location which is not the usual location where the customer makes transactions the company may suspend the account and investigate the case by calling back the customer.

### MONITORING TRAFFIC FLOWS

Another measure to inhibit phishing before real implementation takes place is to keep track of any person who clones a company Web page or downloads company logos or files in large numbers. Usually phishers use software to clone a Web page or download large number of logos and files so as to construct a seemingly true Web site. If they conduct a series of downloading activities from a single IP address that address is recorded on the server log file. A program can be set up

by the security team to alert relevant members of staff if such an action happens. Corillian Fraud Detection System is software that looks for suspicious access patterns from Web log files [Geer 2005].

### PROACTIVE SCANNING OF WEB SITES

Many companies pay security companies to look for potential phishing Web sites in the market. Security companies usually carry out Internet search, chat room monitoring, or domain name registration checks to see if anyone newly registers a Web site or owns a Web site with similar domain name. They compare the visual similarity of those newly found Web sites with their customers' Web sites, and if they find one Web site they ask the ISP to shut down the Web site or notify all customers to watch out for it [Liu et al. 2005].

### POISONING PHISHING WEB SITES

Once a person finds a phishing Web site, it may happen that some customers have already given away their personal information. In order to minimize the financial impact to all customers, a company can send a huge amount of fake information to the phishing Web site. This can overwhelm the traffic of the bogus Web site and prevent other customers from giving away their confidential information to the Web site. At the same time it can also dilute the actual customer data collected so far so that the phishing site is unable to discover which account information are true and which are false. Computer professionals describe such a process as poisoning a phishing Web site [Geer 2005].

Table 2 provides a summary of the features provided by the different anti-phishing measures.

Table 2. Various Anti-Phishing Measures Adopted by Companies

| **Anti-phishing measures** | **Main features** |
|---|---|
| E-mail scan | Filter out phishing prone e-mails and reduce the chance of phishing |
| Transaction log monitoring | Monitor abnormal transactions stored in server logs and investigate if phishing has occurred |
| Traffic flow monitoring | Monitor abnormal online traffic flows one can catch phishers before the crime begins (e.g., series of downloading activities from a particular IP) |
| Proactive Web scanning | Check the visual and domain name similarity of newly registered Web sites and existing Web sites to deter phishing Web sites from burgeoning |
| Poisoning phishing Web | Submit chunks of garbage information to the phishing Web site so as to dilute the actual data already gathered by the site and to thwart further phishing activity by overwhelming traffic flow to the site |

## V. ANTI-PHISHING TOOLS

Phishing is complicated in nature. It is true that manual human effort is not sufficient to detect the various types of phishing attacks. Some anti-phishing applications for individual customers and companies may be useful to deter such kind of activities. Their functionalities and areas of prevention vary a lot. In this section we discuss the various types of anti-phishing applications.

## ANTI-MALICIOUS PROGRAM SOFTWARE

Malicious programs such as viruses and Trojan are common tools used by phishers to steal confidential information. In the past, phishing e-mails contained malicious programs. In recent times, due to the prevalence of virus filtering e-mail servers, malicious programs have become more prevalent on phishing Web sites. Once a person visits a phishing Web site the malicious program may get implanted in the computer of victim and pose a threat of potential information leakage. In order to combat these programs, it is recommended that one install anti-virus software with constant updates as well as firewall on his/her computer.

## ANTI-SPAM FILTER

Many companies install spam filters to protect internal employees. As reflected in the study of Kenyon College, introduction of spam filters was able to stop a significant number of attempts to commit identity theft from getting through users' e-mail [Murphy 2005]. For individual customers, there are many free spam filters available like Anti-Spam Filter and AllSpamGone Spam Killer Anti Spam. Open source software like Clear Search Anti-phishing and E-mail Xray can be used to filter out suspicious e-mails by comparing them with those available in the software's phishing libraries. For instant messengers, many vendors have launched features that prevent phishing (e.g., SpamGuard in Yahoo Messenger).

## PASSWORD MANAGEMENT TOOLS

Although password is one of the most commonly adopted means to protect a user's account information, most customers are used to giving away their passwords easily. Some software based protection measures can help in user password management. Whenever a user logs onto a system, the special software will automatically fill in a relevant field on the Web site. As the software will recognize a Web site by its actual IP address, if a user goes to a phishing Web site, the password field will not be auto-filled. Some password management software has additional powerful features as well. Whenever a user creates a new account, this software will add IP-specific characters to the password field. When users go to a Web site and supply a password the IP-specific characters will be appended automatically. In this way even if a customer leaks his/her own password, the adversary cannot steal the account information of customers because what the customer knows is only part of the password. Some commonly used password management applications are PwdHash, SpoofGuard, AntiPhish, [Kirda and Kruegel 2005], PVault [Jammalamadaka et al. 2005].

## TRUSTED PATH ENSURED BROWSER

Secure Sockets Layer (SSL) represents a trusted path between browser and Web server and is a strong protection against leakage of sensitive information. However SSL can be forged. Ye et al. demonstrated that the adversary can camouflage a secure Web session by simply creating an illusion that the browser has already displayed signals that a genuine SSL will display [Ye et al. 2005]. The adversary can also use scripting language to hide or display a fake URL in the address bar. Ye et al. suggested Synchronized Random Dynamic (SRD) boundaries that can ensure trusted path exists so that the users can distinguish between genuine status of messages from the browser itself and maliciously crafted content from the server. Dhamija and Tygar proposed an extension of Mozilla Firefox called Dynamic Security Skins that makes use of graphical pictures to visually determine if a trusted path exists or not. The authentication process takes place in two steps. First, a remote server generates a graphical picture. Then, the browser extension with Dynamic Security Skins generates another graphical picture that it expects to receive from the server. To authenticate the content, one needs to verify if the two images match. It is difficult for a phishing site to predict the image to be displayed in the Web browser. Therefore, even when a phisher captures a picture that is displayed on a genuine site, the chance that the same picture will appear again is very low. By comparing the pictures generated by both the server and the remote browser one can determine the existence of a trusted path [Dhamija and Tygar 2005].

## DIGITALLY SIGNED E-MAIL

In order to defend against phishing, Garfinkel et al. suggested that Internet users should adopt digitally signed mail. Digitally signed e-mail makes use of asymmetric key cryptography such as RSA and allows one to clearly distinguish the identity of sender. The ideology behind the scheme is that each user owns a pair of public key and private key [Boncella 2000]. Only the genuine user can sign a message with his/her own private key while the receiver can validate the originality of the message by using a relevant public key that is readily available to the public from a trustable third party. Under this scheme, even when a phisher claims to be a member of the staff of a certain company they cannot forge the signed message without the private key. Therefore, authentication using digitally signed e-mails is a strong measure against phishing [Garfinkel et al. 2005].

## ALIAS E-MAIL ADDRESS

Phishers typically use e-mail crawler programs that collect e-mail addresses from the Internet. Another approach is direct purchase of e-mail addresses from business entities that do not care about the privacy of their customers. Kawashima et al. suggested the use of alias e-mail addresses to prevent e-mail abuse. Under the scheme proposed by them, ESPs may possess a database consisting of actual and alias addresses of a customer together with relevant tracking IDs [Kawashima et al. 2005]. When a company wants to send mass e-mail, ESP may give it a list of alias addresses together with corresponding tracking ID. When the company sends e-mail, the ESP will convert the alias to actual address and deliver the e-mail to the final recipients. If spam is found, ESP will use the tracking ID accompanying the e-mail alias and trace back the source of e-mail leakage. In this way the identity of the end user can be preserved.

## ZERO-KNOWLEDGE PROOF

Verification of one's identity without letting the third party know the identification is the main interest of security analysts. Zero-knowledge proof is one such method that allows a third party to verify the identity of a user without knowing anything related to the secret. It is effective in deterring playback attacks where the adversary intercepts a password sent by a customer to a company and impersonates the customer by using the same password in the next transaction [Viega 2005]. An important way to implement zero-knowledge proof is by the use of challenge-response tokens. Under this method, it is assumed that a customer knows answers (or responses) to all questions (or challenges) posed by the server. The server first asks several questions randomly out of a large database of questions. If a customer can answer all of them correctly then he/she is an authenticated user. If the adversary happens to intercept the set of answers it does not mean he/she can impersonate the true person, because all the questions are posed randomly.

## 2-FACTOR AUTHENTICATION

Traditionally in order to provide authentication one has to memorize a password. If a third party knows the password an account gets compromised. In order to correct the inefficiency of password authentication, 2-factor authentication is suggested. To authenticate oneself, one must prove what one knows and what one has. "What you know" refers to the password that people use conventionally. "What you have" is something that is possessed only by the genuine user. This can include a hardware token that generates different Personal Identification Numbers (PINs) at different times. In the following paragraphs we describe the different means by which the user can prove "what you have."

### Hardware Security Box

In Sweden, a security box is distributed to customers of most banks for user verification [Nilsson et al. 2005]. When a user logs on to an Internet banking site, he/she has to supply a password ("what you know") and a personal PIN from a security box ("what you have"). The device

generates a random number based on an initial seed that serves as the PIN for the user. Banks in Hong Kong such as HSBC and Hang Seng Bank offer this kind of service.

**One Time Password (OTP)**

OTP is a random number generated by a company. Once it is used or once a certain amount of time has elapsed the password is discarded. When a customer of a bank conducts a high-risk transaction, the bank will supply an OTP through an alternative channel like the customers' mobile phone via Short Message Service (SMS). To carry out the transaction, the user will need to supply both the PIN and an OTP. This strategy is excellent in preventing play back attacks. Even though a hacker traps an OTP during an online transaction to a bank, the trapped password cannot be used for a second time. If an OTP is trapped by a phishing site after a period of time it becomes invalid. Banks in Hong Kong such as Bank of China and Standard Chartered Bank offer this service.

**Personal Certificate**

Personal certificate is a type of implementation of RSA asymmetric cryptography. The RSA scheme produces a pair of private and public keys. Personal certificate is a signed document with a person's name and a signature signed by a Certificate Authority (CA) private key that can be verified by CA's public key. Only those who register to a CA are given a personal certificate. Therefore, the identity of a person stated on the certificate is guaranteed by CA. In order to verify oneself to a company, one has to present his/her personal certificate apart from supplying a password. The company retrieves a public key from the CA and verifies the correctness of the signature on the certificate and in this way verifies the identity of the person. Bank of China and DBS Bank in Hong Kong allow Internet banking users to verify their identity using personal certificates.

Table 3. Types of Anti-Phishing Applications with Examples

| **Types of anti-phishing applications** | **Examples** |
|---|---|
| Anti-malicious software | Anti-virus: Norton Anti-Virus, McAfee Anti-Virus<br>Firewall: Sygate Firewall, ZoneAlarm |
| Anti-spam filter | E-mail spam filters: Anti-Spam Filter, AllSpamGone Spam Killer Anti Spam<br>Anti-phishing filters: Clear Search Anti-phishing, E-mail Xray |
| Password management tools | PwdHash, SpoofGuard, AntiPhish, Pvault |
| Trusted path ensured browser | Synchronized Random Dynamic (SRD) boundaries, Dynamic Security Skins browser plug-in |
| Digitally signed e-mail | RSA cryptography |
| Alias e-mail address | E-mail alias with tracking ID |
| Zero-knowledge proof | Challenge response token |
| 2-factor authentication | Conventional passwords with any of the following: Hardware security box, OTP, personal certificate |
| Multi-factor authentication | Any 2-factor authentication mechanism plus biometric features recognition |

### Multi-Factor Authentication

Based on the ideology of "what you know, what you have, and what you are," multi-factor authentication is often identified as a combination of knowledge-based authentication, possession based authentication, and biometrics based authentication [Zviran and Erlich 2006]. Unique biometric features are usually the extra properties that need to be verified. A common 3-factor authentication mechanism may include verification of password, OTP, and the user's finger print. Other types of biometric technologies can include face recognition, hand geometry, iris scanning, retina scanning, and voice recognition, among others [Boukhonine et al. 2005]. This mechanism is suitable for those highly confidential transactions that require highest level of authentication. Table 3 provides a summary of the various anti-phishing measures with examples of each measure.

## VI. EVALUATION OF ANTI-PHISHING TECHNIQUES

In Section V we discussed several anti-phishing techniques. In this section we evaluate the capabilities and limitations of each technique from the user perspective and draw a comparison between them.

Anti-malicious programs are the most rudimentary and popular tools to protect users against phishing. However, the price and user-friendliness of the different products varies. Although the adoption rate of anti-malicious programs is high many users neglect to update the virus definition files on a regular basis. As a result, users may not get full protection at all times. However anti-malicious programs only offer protection against malware. Phishers can still entice users with tricks such as phishing e-mails and bogus Web sites. Therefore, it is not enough to install anti-malicious programs as the only tools to fight phishing.

Anti-spam software is another protection tool. Some service providers install the software in their e-mail servers to filter potential phishing e-mails. For better protection individual users should install such a tool on their e-mail handler such as Outlook Express. However users need to update the spam library frequently to keep it up to date. Furthermore, anti-spam software cannot do much against attacks from bogus Web sites and Web-based malware.

Password management tools and trusted path ensured browsers are newer application programs that help in the prevention of phishing. Due to their newness, the adoption rate of such programs is not very high. Nevertheless, they are effective tools against bogus Web sites if the users pay attention to the warnings issued by these software tools. Most of these programs are open source and easy to install. However, these programs cannot offer protection against malware and phishing e-mails.

In order to deter phishing e-mails, digitally signed e-mail is an effective tool for user authentication. Users should apply for a private and public key from CA and this involves some expenditure on behalf of users. Also users should take special care of the private key and make it inaccessible to any third party. At present the adoption of digitally signed e-mail is not high, and it cannot fully protect users from Web-based malware and bogus Web sites.

Alias e-mail address is a useful way to cut off the source of e-mail addresses to phishers. However, maintenance of the alias e-mail database requires extra effort and high operating costs. Therefore, not many service providers adopt it. Again, it cannot fully protect users from Web-based malware and bogus Web sites.

User authentication is one of the key protective measures against phishing and identity theft. Zero-knowledge proof, 2-factor authentication, and multi-factor authentication are techniques specially designed for user authentication. But the implementation cost for these techniques is generally high, because it is necessary to install special hardware devices. For multi-factor authentication, the equipment cost can be many times higher than that for other methods depending on the level of authentication required. However, in some situations, even the three methods working in unison cannot offer thorough protection. In case of the man-in-the-middle

type of attack, the adversary can impersonate the victim by sending all the credentials supplied by the victim to the authentication server. Upon successful authentication, the adversary can gain full control of the user's account.

Table 4. Comparison of Different Anti-Phishing Techniques

| **Characteristics / Anti-phishing techniques** | **Target** | **Level of difficulty of use** | **Constraints** | **Potential phishing attacks** | **Rate of adoption by users** | **Cost of imple-mentation** |
|---|---|---|---|---|---|---|
| Anti-malicious program | Malware | Low to medium | Constant virus update | Phishing e-mail or bogus Web sites | High | Low to medium |
| Anti-spam filter | Spam and phishing e-mail | Low | Constant update of spam library | Web-based malware | Medium | Low to medium |
| Password management tools | Bogus Web sites | Low | User should not intentionally give away personal information | Web-based or e-mail attached malware | Low | Low |
| Trusted path ensured browser | Bogus Web sites | Low | User pays attention to indication of trusted path | Web-based or e-mail attached malware | Low | Low |
| Digitally signed e-mail | Phishing e-mail | Low | Personal certificate of sender is not compromised | Web-based malware | Low | Medium |
| Alias e-mail address | Phishing e-mail | Low | Alias e-mail database is not hacked | Web-based malware | Low | Medium |
| Zero-knowledge proof | User authentic-cation | Low | Only genuine users know and posses secret keys | Man-in-the-middle attack | Medium | High |
| 2-factor authentication | User authentic-ation | Low | Only genuine users know and posses secret keys | Man-in-the-middle attack | Medium | High |
| Multi-factor authentication | User authentic-ation | High | Only genuine users know and posses secret keys and other biometric features | Man-in-the-middle attack | Low | Extremely high |

Table 4 provides a comparison of the different anti-phishing techniques. It leads us to conclude that none of them can offer full-fledged protection against phishing. It is necessary to install more

than one anti-phishing tool so as to complement the inadequacies of others. The adoption of the tools depends on the situation and needs of the user. For users who are unaware of incoming e-mails, anti-spam filter is a preferred technique. Companies that use e-mail as the major means of business communication between partners and customers should consider the use of digitally signed e-mail to prevent phishers from gaining access to true e-mail addresses of e-mail recipients. To give protection against

malware anti-malicious programs are necessary. To thwart information leak to bogus Web sites, it is important to install password management tools and trusted-path ensured browsers. For safe online transactions, tools implementing zero-knowledge proof and 2-factor authentication are a must. In extremely critical circumstances that need the highest level of authentication, multi-factor authentication becomes compulsory. In order to have a thorough protection against phishing, we recommend that users install at least one application program in each anti-phishing category. Combating phishing is a social responsibility. In the next section, we describe how corporations and individuals can utilize anti-phishing tools and measures to achieve that goal.

## VII. SOCIAL RESPONSIBILITIES AGAINST PHISHING

Being a part of the global community, both corporations and individuals have certain social responsibilities to fight phishing. In this section, we discuss the importance of those social responsibilities from the corporate and individual perspectives and investigate how we can achieve comprehensive anti-phishing protection from a social and legal perspective.

### CORPORATE AND INDIVIDUAL SOCIAL RESPONSIBILITIES

Company owners have the duty to protect their customers by adopting adequate security measures to prevent any foreseeable crime due to a variety of reasons. Phishing undermines four fundamental Information Systems security objectives, namely “maximize privacy,” “maximize access control,” “enhance integrity of business process,” and “maximize data integrity” [Dhillon and Torkzadeh 2006] and puts customers’ personal information and safety of online transactions in danger. In fact, anti-phishing is one of the corporate social responsibilities (CSR) generally expected by the global community. Failure to take up CSR may deteriorate a company’s goodwill and public image, and these qualities are difficult to remediate once lost [Joyner and Payne 2002]. This may even lead to lower profitability as CSRs are generally perceived as critical advantages of a company by most CEOs [Simms 2002; Ogrizek 2002]. Some regional laws such as the Gramm-Leach-Bliley Act of the U.S. require companies to adopt effective measures to protect customers’ financial data [Anderson 2006]. Being socially responsible corporations, company owners have responsibilities to comply with the laws and safeguard customers’ personal data by thwarting phishing attacks.

Individuals also have social responsibilities to fulfill in the battle against phishing. They should protect personal data by taking a number of important steps. They should install the latest versions of anti-phishing software, and remain watchful of incoming messages. They should not click on embedded hyperlinks in e-mails. Any active content enabling options, such as ActiveX, Java, JavaScript, and cookies, available in e-mail applications or browsers should be turned off whenever necessary [Lininger and Vines 2005]. Anti-phishing requires collaborative effort of all parties involved, and individuals play an important role in reporting any evidences of phishing-related activities. Being dutiful members of the society, individuals have the responsibility to alert others about the dangers of potential phishing attacks. Based on the previous discussion, we can categorize corporate and individual social responsibilities in the context of anti-phishing into three main areas, namely combating phishing at all stages of activity, complying with legal obligations to safeguard personal data, and adopting standards for anti-phishing.

## UNDERSTANDING THE PHASES OF PHISHING

Phishing can be categorized into four phases: preparation, mass broadcast, mature, and account hijack. In the preparation phase, phishers build up bogus Web sites that look similar to genuine ones to lure unaware customers. In the second stage of mass broadcast, phishers target general public or specific customers of companies by retrieving relevant e-mail addresses from the Internet via e-mail crawler programs or purchasing them from spam vendors. In the mature phase that usually lasts about five days, phishers wait for victims to take the bait of fake e-mail and give away personal information at a spurious Web site. In the final phase of account, hijack phishers use trapped personal data to withdraw money from victims. There are four different ways to combat the crime of phishing in its four phases respectively. These include prohibition of bogus Web sites, thwarting the spread of phishing messages, preservation of data privacy, and deterrence of identity theft. Figure 3 provides an anti-phishing framework that shows which countermeasures and techniques should be adopted at which stage of phishing.

Table 5. Examples of Anti-Phishing Laws across the Globe

| **Types of anti-phishing laws** | **Examples of anti-phishing laws** |
|---|---|
| Thwarting the spread of phishing messages | - CAN-SPAM Act (18 U.S.C. § 1037) (US)<br>- Data Protection Directive (European Union)<br>- E-Privacy Directive (European Union) |
| Prohibition of bogus Web sites | - Copyright Ordinance (Cap. 528) (HK)<br>- Wire fraud (18 U.S.C. § 1343) (US)<br>- Offences related to infringements of copyright and related rights (Article 10, Convention on Cybercrime) |
| Preservation of data privacy | - Personal Data (Privacy) Ordinance (Cap. 486) (HK)<br>- Telecommunication Ordinance (Cap. 106) (HK)<br>- Telecommunication Privacy Directive (European Union)<br>- E-Privacy Directive (European Union)<br>- Data Interference (Article 4, Convention on Cybercrime)<br>- System interference (Article 5, Convention on Cybercrime) |
| Deterrence of identity theft | - Crime Ordinance (Cap. 200) (HK)<br>- Theft Ordinance (Cap. 210)<br>- Identity Theft and Assumption Deterrence Act (18 U.S.C. § 1028) (US)<br>- Credit card fraud (18 U.S.C. § 1029) (US)<br>- Bank fraud (18 U.S.C. § 1344) (US)<br>- Computer fraud (18 U.S.C. § 1030(a)(4)) (US)<br>- Computer-related fraud (Article 8, Convention on Cybercrime) |

## LEGISLATION AGAINST PHISHING

Legislation usually follows the social trend to protect the general interest of all citizens [Ogrizek 2002]. Throughout the world, governments have adopted a variety of anti-phishing laws that can be categorized into four types. The first type includes legislation that thwarts the spread of phishing messages. The CAN-SPAM Act adopted by the U.S. federal government is an example

of this [Hladjk 2005]. The second type of legislation prohibits the setup of bogus Web sites with an intention to deceive people. The Wire Fraud Act in the U.S. (18 U.S.C. § 1343), which prohibits anyone "having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses" is an example of this category [Chawki 2006]. The third type of anti-phishing laws is geared toward preservation of data privacy. The Personal Data (Privacy) Ordinance (Cap. 486) of Hong Kong belongs to this category. The fourth type of legislation deters identity theft like the Theft and Assumption Deterrence Act (18 U.S.C. § 1028) in the U.S. Table 5 lists several legislation currently in place in the U.S., Hong Kong, European Union, and Convention on Cybercrime that consists of member countries Canada, Japan, South Africa, U.S., and 15 states of the Council of Europe.

Apart from the above laws safeguarding public interests from phishing attacks, companies in some countries have special legal obligations to fulfill. In the state of California, U.S., companies have the obligation to report any breaches in computer security according to the state law SB1386 [Getronics 2005]. U.S. financial services and insurance companies are also obliged to report any suspicious transactions as part of anti-money laundering regulations according to the U.S. Patriot Act [Getronics 2005]. Finally, U.S. companies are obligated to adopt reasonable security and privacy policies and practices. Otherwise, they are likely to face prosecution from consumer protection authorities for deceptive trade practices [Matsuura 2004]. With the prevalence of these different types of legislation, it has become imperative for companies to provide customers with better protection in terms of privacy preservation and security enhancement.

## ROLE OF STANDARDS

Companies and individuals are often harassed by concerns such as confidentiality, integrity, availability, auditability, reliability, and amount of security necessary to achieve highest level of information security [Gerber et al. 2001]. In order to address these concerns, many international standards committees have developed security standards. A comprehensive theory of Information Security Management (ISM) should consist of five elements, namely integrated security policy theory, risk management theory, control and auditing theory, management system theory, and contingency theory [Hong et al. 2003]. Covering various essential aspects of ISM, many IS security standards have come into existence. Table 6 summarizes the major standards and areas related to anti-phishing.

Several organizations have started playing an important role in the development of standards and best practices that are geared toward anti-phishing. One of the organizations that is playing a pioneering role in educating the general public about the dangers of phishing is the Anti-Phishing Working Group (APWG), which consists of over 400 members from approximately 25 companies and includes banks, ISPs, e-commerce and e-business related businesses as their members. They provide anti-phishing resources as well as monthly phishing reports. The National Cyber Forensics & Training Alliance (NCFTA) is a U.S.-based organization dedicated to promoting security awareness among the general public. The Financial and Banking Infrastructure Committee (FBIC) works with the Department of Defense in the U.S. to fight financial crimes and with members from financial institutions and regulatory agencies to improve the security of their infrastructures. Other organizations like the Federal Trade Commission, Financial Services Technology Consortium, and Global Infrastructure Alliance for Internet Security also provide useful information and advice related to anti-phishing.

Although no one can deny the importance of standards, it is somewhat problematic to implement a uniform standard throughout the globe. Countries throughout the world need to collaborate with each other for this purpose. Phishing is borderless. A bogus Web site may be hosted in a developing country with loosely defined anti-phishing laws while phishing e-mails are distributed to developed countries causing tremendous economic loss. Adversaries may take advantage of a host country's liberal laws to escape or minimize the punishments for phishing. In view of this, collaboration between countries is almost imperative for evidence collection and prosecution. The European Convention on Cybercrime is a good start in international cooperation. Anti-phishing is

a global need that requires joint effort of individuals and corporate owners. Being part of the global community, they have responsibilities to fight phishing at all stages, comply with legal obligations, enhance anti-phishing awareness, and report any incidences of phishing. Legislation is an important means to deter the crime and punish the adversaries. The key points of the discussion in this section of the paper are summarized in the form of an anti-phishing framework that is depicted in Figure 3. It highlights the four different phases of phishing and the most important anti-phishing activities in each phase. It also relates the legislation that has been implemented in various parts of the globe as well as the key information technology based anti-phishing measures that are discussed in Section V to the various phases of phishing. The framework shows how corporations and individuals can fulfill their social responsibilities by counteracting the different phases of phishing.

Table 6. Major IS Security Standards and Areas Related to Anti-Phishing

| IS security standards | Areas related to anti-phishing |
|---|---|
| CERT security practices | In the detect step, transaction monitoring can discover suspicious behavior and minimize the threat of identity theft [Allen 2001] |
| Code of practice for information security management (ISO/IEC 17799) | In the domains of physical and environmental security, communications and operations management and access control, there are measures related to protection against unauthorized access of confidential information [Saint-Germain 2005] |
| Common criteria for IT security evaluation (ISO/IEC 15408) | Several functional classes such as security audit, cryptographic support, user data protection, identification and authentication, security management, privacy and trusted path/channels are relevant to the areas of anti-phishing [Herrmann 2003] |
| Control objectives for information and related technology (COBIT) | In the delivery and support domains, control objectives related to online access control, security surveillance, authorization procedures, and incident handling are relevant to anti-phishing. Also, control objectives such as collection of monitoring data and management reporting are important for deterring identity theft [Lahti 2005] |
| Generally accepted system security principles (GASSP) | Under broad functional principles, categories such as Information Management, Access Control and Information Risk Management require practitioners to routinely manage and assign levels of sensitivity and criticality to information assets. Under detailed security principles, the suggestion of using OTP to control access to critical information assets is a counter measure to identity theft [Poore 1999] |
| Information security forum standard of good practice (ISF SoGP) | Within security management, the principles and objectives related to malicious attacks are relevant to anti-phishing. In the category of networks, network monitoring, external access, and incident management are useful practices against unauthorized access to sensitive information. In the area of systems development, security awareness and security audit/review are useful measures to detect suspicious activities related to identity theft [ISF 2005] |

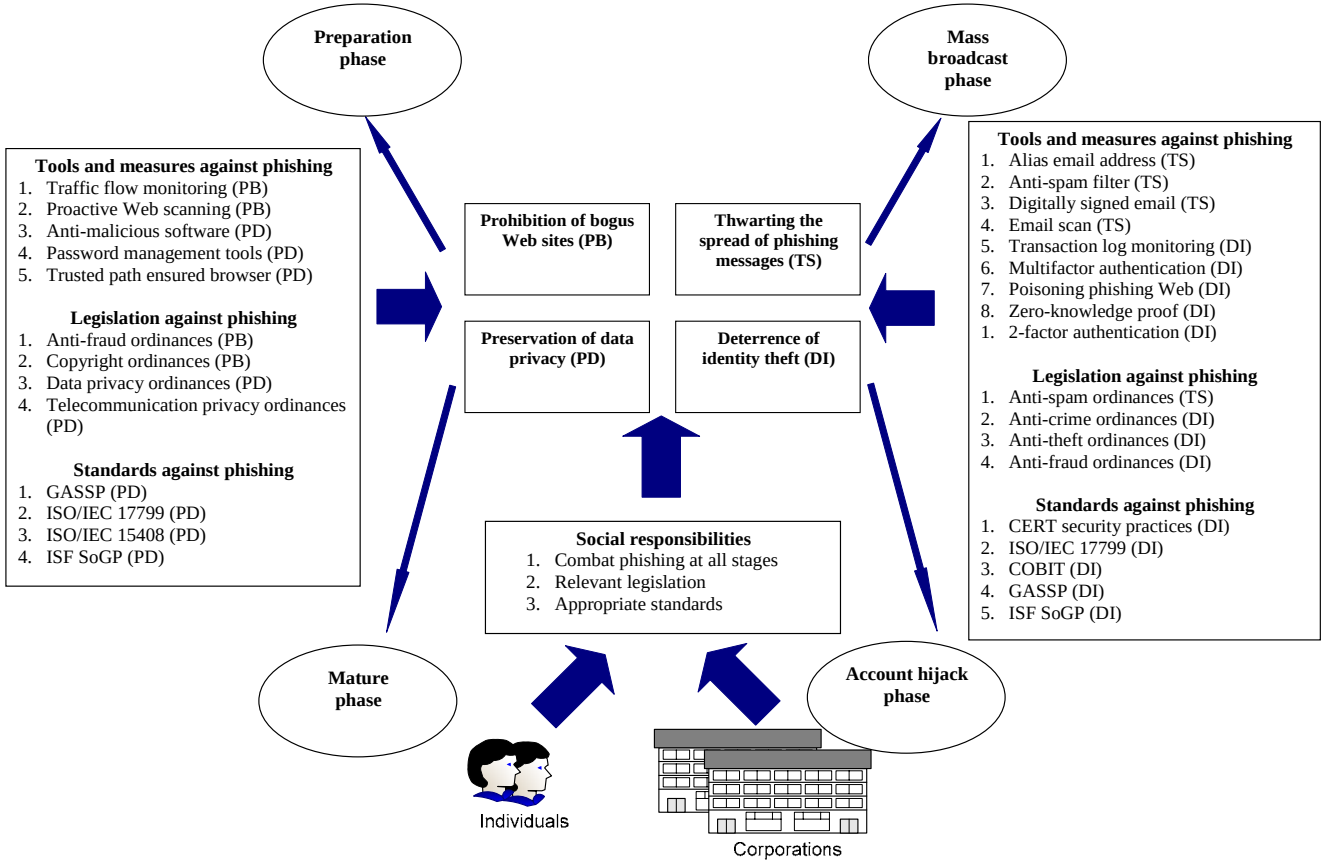


Figure 3. Anti-Phishing Framework

## VIII. FUTURE TRENDS OF PHISHING AND ANTI-PHISHING

Throughout the past decade, the technologies that support phishing have become more sophisticated making detection of phishing a difficult endeavor. In this section we discuss the future trends of phishing and anti-phishing.

### CHANGE OF PHISHING MEDIUM

Although e-mails and instant messengers are the major phishing media, they seem to have saturated. With the advent of mobile technology phishing through Short Messaging System (SMS) has become available. Recently SMS spam incidences have increased in number. Identity fraud is also possible via SMS spam. As mobile commerce becomes more and more popular, in the future phishers can easily forge logos and trademarks of a brand using specially designed Multimedia Messaging Service (MMS).

### ZOMBIE PHISHING NETWORK

To hide the IPs of spam servers, phishers set up the servers in a zombie network. Such a network sends spam by distributing the load and the apparent source of the messages across many computers. At this time, about 48 percent of spam comes from zombies [Lawton 2005]. Spam that is spread using a zombie network makes detection of the person behind the scene difficult. This distributed network also reduces the traffic flow and is successful in delivering spam because ISPs are less likely to block sources that generate low volumes of traffic.

### ADVANCED CRIMEWARE

Increasingly phishers are using new crimeware such as Keyloggers, Screen Scrapers, and malicious JavaScript programs. A keylogger is a program that transmits what a user types using a keyboard to a remote user. A Screen Scraper transmits information related to the user surreptitiously. It does not send keystrokes but sends screen dumps to a remote user. Malicious JavaScript programs are powerful phishing tools. Cross-site Scripting (XSS) attacks are forecasted to become more common in future [Hallaraker and Vigna 2005].

### INEFFICIENCY OF 2-FACTOR AUTHENTICATION

2-factor authentication cannot withstand man-in-the-middle attacks as well as Trojan. For such attacks, a phisher acts as an invisible middle man between the victim and the genuine company server. Once the victim gives the password to the server it is intercepted by the phisher and passed on to the server. The phisher then modifies the server transmission without being noticed by the end user. For example, the phisher can modify the transaction account number and total amount of money to be transferred. In this scenario, 2-factor authentication is of no use.

Some new directions of research in the area of anti-phishing are described as follows.

### MULTI-CHANNEL AUTHENTICATION

Mizuno et al. proposed a new authentication method that allows the user to verify whether he/she is connecting to a correct service provider rather than a phishing site using multiple communication channels [Mizuno et al. 2005]. A server can generate a session ID, and a user can use a mobile scanner or camera interface to capture the session ID and transmit it to the service provider. After verification of the registered mobile phone number and session ID, the service provider can authenticate the user and grant him/her permission to use the authorized service without supplying the user name or password.

### MULTIPLE CHALLENGE RESPONSE AUTHENTICATION

Verification of the identity of service provider or client requires client authentication and server authentication. Mizuno et al. demonstrated how the authentication protocols might work using the mistrusted Internet medium and the trusted mobile phone network. Once an authentication challenge reaches a mobile phone, one can use a keyboard to input a response. If the challenge is posed via the Internet, a barcode reader or a camera interface can transmit the data from the mobile phone to the service provider. However, such a scheme cannot deter man-in-the-middle attacks [Mizuno et al. 2005].

### E-MAIL AUTHENTICATION FRAMEWORKS

In order to combat e-mail frauds, three e-mail authentication frameworks are popular: Pobox.com's Sender Policy Framework (SPF), Yahoo's DomainKeys Indentified Mail (DKIM), and Microsoft's SenderID Framework (SIDF). They mark an outgoing message with an encrypted key so that the recipient e-mail server can determine the origin of the e-mail and verify if it matches what appears in the "From" field. SPF and DKIM are likely to become market leaders [Weiss 2004]. After SIDF combines Microsoft's Caller ID technology and SPF, it may become the most popular framework in future [Lawton 2005].

## IX. CONCLUSION

Within a decade, phishing has transformed itself from a territorial crime to an international threat. In this paper, we discussed the various ways in which phishing can take place. The most common one is via e-mail and instant messenger. Other methods include usage of malicious programs and pharming. Though phishing methods vary not all of them are flawless and unavoidable. If one pays attention to the phishing messages received one can easily identify spelling mistakes and clues such as URL in numeric form. By installing adequate anti-phishing software and continually updating anti-virus, firewall, anti-spam filter, and other domain-name-specific password management tools, one can minimize the chance of becoming a phish. A number of distinct anti-phishing techniques are discussed in this paper and their strengths are compared. As part of their social responsibility, organizations around the globe have adopted relevant laws and standards to thwart the spread of phishing messages, prohibit bogus Web sites, preserve data privacy, and deter identity theft. We present an anti-phishing framework that highlights the various anti-phishing measures that can be adopted to disrupt phishing in its four phases. In future we envisage phishing is likely to adopt alternative channels like mobile phones and phishing attacks may be conducted by zombie networks and through XSS. The crime is becoming more sophisticated and harder to detect but it is encouraging that researchers are devising new innovative methods to deter the growing online fraud.

## REFERENCES

EDITOR'S NOTE: The following reference list contains the address of World Wide Web pages. Readers, who have the ability to access the Web directly from their computer or are reading the paper on the Web, can gain direct access to these references. Readers are warned, however, that

1. these links existed as of the date of publication but are not guaranteed to be working thereafter.

2. the contents of Web pages may change over time. Where version information is provided in the References, different versions may not contain the information or the conclusions referenced.

3. the authors of the Web pages, not CAIS, are responsible for the accuracy of their content.

4. the author of this article, not CAIS, is responsible for the accuracy of the URL and version information.

Allen, J. H. (2001). "CERT System and Network Security Practices," in Proceedings of the Fifth National Colloquium for Information Systems Security Education. NCISSE 2001, Fairfax, VA, USA, 22-24 May, pp. 1-11.

Anderson, A. (2006). "Effective Management of Information Security and Privacy," *Educause Quarterly*. 29(1), pp. 15-20.

Anti-Phishing Working Group. (2006). "Phishing Activity Trends Report December 2005," Anti-Phishing Working Group. http://antiphishing.org/reports/apwg_report_DEC2005_FINAL.pdf (current 1 June, 2006).

Boncella, R. (2000). "Web Security for E-Commerce," *Communications of AIS*. 4(11), pp. 1-42.

Boukhonine, S., V. Krotov, and B. Rupert. (2005). "Future Security Approaches and Biometrics," *Communications of AIS*. 16(48), pp. 937-966.

Chawki, M. (2006). "Phishing in Cyberspace: Issues and Solutions," *Computer Crime Research Centre*. http://www.crime-research.org/articles/phishing-in-cyberspace-issues-and-solutions/5 (current 14 November, 2006)

Dhamija, R. and J. D. Tygar. (2005). "The Battle against Phishing: Dynamic Security Skins," in Proceedings of the 2005 Symposium on Usable Privacy and Security. SOUPS 2005, Pittsburgh, PA, USA, 6-8 July, pp. 77-88.

Dhillon, G. and G. Torkzadeh. (2006). "Value Focused Assessment of Information System Security in Organizations," *Information Systems Journal*. 16(3), pp. 293-314.

Garfinkel, S.L. et al. (2005). "How to Make Secure E-mail Easier to User," in Proceedings of the ACM Conference on Human Factors in Computing Systems. SIGCHI 2005, Portland, OR, USA, 2-7 April, pp. 701-710.

Geer, D. (2005). "Security Technologies Go Phishing," *IEEE Computer*. 38(6), pp. 18-21.

Gerber, M., R. von Solms, and P. Overbeek. (2001). "Formalizing Information Security Requirements," *Information Management and Computer Security*. 9(1), pp. 32-37.

Getronics. (2005). "Security Compliance: Practical Strategies to Alleviate Regulatory Frustration," http://www.getronics.com/NR/rdonlyres/edvvrxksbfdiitqixuxvokj2wbvq24njownuuloajjs2phvd6rkjby3gaazlu2wo3nr5qedffj2f4r3aawwmoy23esa/wpsecsecuritycompliance050809.pdf (current 16 November, 2006)

Hallaraker, O. and G. Vigna. (2005). "Detecting Malicious JavaScript Code in Mozilla," in Proceedings of the 10th IEEE International Conference on the Engineering of Complex Computer Systems. ICECCS 2005, Shanghai, PRC, 16-20 June, pp. 85-94.

Herrmann, D. S. (2003). *Using the Common Criteria for IT Security Evaluation*. Boca Raton: Auerbach.

Hladjk, J. (2005). "Effective EU and US Approaches to Spam? Moves towards a Coordinated Technical and Legal Response – Part I," *Tolley's Communications Law*. 10(3), pp. 71-83.

Hong, K. S., Y. P. Chi, L. R. Chao, and J. H. Tang. (2003). "An Integrated System Theory of Information Security Management," *Information Management and Computer Security*. 11(5), pp. 243-248.

ISF. (2005). "The Standard of Good Practice for Information Security," http://www.isfsecuritystandard.com/pdf/standard.pdf (current 5 January, 2007)

James, L. (2005). *Phishing Exposed*. 1st edition, Boston, Massachusetts: Syngress Publishing.

Jammalamadaka, R. C., S. Mehrotra, and N. Venkatasubramanian. (2005). "Pvault: A Client Server System Providing Mobile Access to Personal Data," in Proceedings of the 2005 ACM International Workshop on Storage Security and Survivability. StorageSS 2005, Fairfax, VA, USA, 11 November, pp.123-129.

Joyner, B. E. and D. Payne. (2002). "Evolution and Implementation: A Study of Values, Business Ethics and Corporate Social Responsibility," *Journal of Business Ethics*. 41(4), pp. 297-311.

Kawashima, M. et al. (2005). "Cryptographic Alias E-mail Addresses for Privacy Enforcement in Business Outsourcing," in Proceedings of the 2005 ACM Workshop on Digital Identity Management. DIM 2005, Fairfax, VA, USA, 11 November, pp. 46-53.

Kienzle, D. M. and M. C. Elder. (2003). "Recent Worms: A Survey and Trends," in Proceedings of the 2003 ACM workshop on Rapid Malcode. WORM 2003, Washington, DC, USA, 27 October, pp. 1-10.

Kirda, E. and C. Kruegel. (2005). "Protecting Users against Phishing Attacks with AntiPhish," in Proceedings of the 29th Annual International Conference on Computer Software and Applications. COMPSAC 2005, Edinburgh, Scotland, 26-28 July, 1, pp. 517-524.

Knight, W. (2005). "Caught in the Net," *IEEE Review*. 51(7), pp. 26-30.

Lahti, C. (2005). *Sarbanes-Oxley IT Compliance Using COBIT and Open Source Tools*, 1st edition. Rockland, MA: Syngress.

Lawton, G. (2005). "E-mail Authentication Is Here, But Has It Arrived Yet?" *IEEE Computer*. 38(11), pp. 17-19.

Lininger, R. and R. D. Vines. (2005). *Phishing: Cutting the Identity Theft Line*, 1st edition. Indianapolis, Indiana: Wiley.

Liu, W. et al. (2005). "Detection of Phishing Web Pages Based on Visual Similarity," in *Special Interest Tracks and Posters of the 14th International Conference on World Wide Web*. Chiba, Japan, 10-14 May, pp. 1060-1061.

Madsen, P., Y. Koga, and K. Takahashi. (2005). "Federated Identity Management for Protecting Users from ID Theft," in Proceedings of the 2005 ACM Workshop on Digital Identity Management. DIM 2005, Fairfax, VA, USA, 11 November, pp. 77-83.

Matsuura, J. H. (2004). "An Overview of Leading Current Legal Issues Affecting Information Technology Professionals," *Information Systems Frontiers*. 6(2), pp.153-164.

Mizuno, S., K. Yamada, and K. Takahashi. (2005). "Authentication Using Multiple Communication Channels," in Proceedings of the 2005 ACM Workshop on Digital Identity Management. DIM 2005, Fairfax, VA, USA, 11 November, pp. 54-62.

Murphy, J. M. (2005). "The Water Is Wide: Network Security at Kenyon College, 1995-2005," in Proceedings of the 33rd Annual ACM Conference on User Services. SIGUCCS 2005, Monterey, CA, USA, 6-9 November, pp. 237-240.

Nilsson, M., A. Adams, and S. Herd. (2005). "Building Security and Trust in Online Banking," in *Extended Abstracts of the ACM Conference on Human Factors in Computing Systems*. SIGCHI 2005, Portland, OR, USA, 2-7 April, pp. 1701-1704.

Ogrizek, M. (2002). "The Effect of Corporate Social Responsibility on the Branding of Financial Services," *Journal of Financial Services Marketing*. 6(3), pp. 215-228.

Poore, R. S. (1999). "Generally Accepted System Security Principles Release for Public Comment," http://www.infosectoday.com/Articles/gassp.pdf (current 5 January, 2007)

Richardson, T. (2004). "12 Arrested in HK Phishing Scam," *The Register*. 18 October, http://www.theregister.co.uk/2004/10/18/hk_phishing/ (current 1 June, 2006).

Saint-Germain, R. (2005). "Information Security Management Best Practice Nased on ISO/IEC 17799," *The Information Management Journal*. 39(4), pp. 60-66.

Simms, J. (2002). "Business: Corporate Social Responsibility - You Know It Makes Sense," *Accountancy*. 130(1311), pp. 48-50.

Viega, J. (2005). "Q Focus: Security - Problem Solved?" *Queue*. 3(5), pp. 40-50.

Weiss, A. (2004). "Trends for 2005," *netWorker*. 8(4), pp. 20-27.

Ye, Z., S. Smith, and D. Anthony. (2005). "Trusted Paths for Browsers," *ACM Transactions on Information and System Security*. 8(2), pp. 153-186.

Zviran, M., and Z. Erlich. (2006). "Identification and Authentication: Technology and Implementation Issues," *Communications of AIS.* 17(4), pp. 90-105.

**LIST OF ACRONYMS**

| | |
|---|---|
| APWG | Anti-Phishing Working Group |
| CA | Certificate Authority |
| COBIT | Control Objectives for Information and Related Technology |
| CSR | Corporate Social Responsibility |
| DKIM | DomainKeys Indentified Mail |
| DNS | Domain Name Server |
| ESP | E-mail Service Provider |
| GASSP | Generally Accepted System Security Principles |
| ISF SoGP | Information Security Forum Standard of Good Practice |
| ISP | Internet Service Provider |
| OTP | One Time Password |
| PIN | Personal Identification Number |
| SIDF | SenderID Framework |
| SMS | Short Message Service |
| SMTP | Simple Mail Transfer Protocol |
| SPF | Sender Policy Framework |
| SRD | Synchronized Random Dynamic |
| SSL | Secure Sockets Layer |
| URL | Uniform Resource Locator |

XSS Cross-site Scripting

## ABOUT THE AUTHORS

**Indranil Bose** is an associate professor of Information Systems at the School of Business, The University of Hong Kong. He holds a B.Tech. from the Indian Institute of Technology, MS from the University of Iowa, MS and Ph.D. from Purdue University. His research interests are in telecommunications, information security, data mining, and supply chain management. His publications have appeared in *Communications of the ACM*, *Communications of AIS*, *Computers and Operations Research*, *Decision Support Systems*, *Ergonomics*, *European Journal of Operational Research*, *Information & Management,* and *Operations Research Letters*. He is listed in the *International Who's Who of Professionals 2005-2006*, *Marquis Who's Who in the World 2006*, *Marquis Who's Who in Asia 2007*, *Marquis Who's Who in Science and Engineering 2007*, and *Marquis Who's Who of Emerging Leaders 2007*.

**Alvin Chung Man Leung** is pursuing MPhil in Information Systems at the School of Business, the University of Hong Kong. He obtained BBA (Information Systems) in 2005 and BEng (Software Engineering) in 2006 from the University of Hong Kong. His research interests are in the areas of phishing, assessing preparedness of phishing among banks, and financial data mining. His research has appeared in proceedings of international conferences.