A

Seminar report

On

Phishing

Submitted in partial fulfillment of the requirement for the award of degree
of Bachelor of Technology in Computer Science

SUBMITTED TO:
www.studymafia.org

SUBMITTED BY:
www.studymafia.org

Acknowledgement

I would like to thank respected Mr…….. and Mr. ……..for giving me such a wonderful opportunity to expand my knowledge for my own branch and giving me guidelines to present a seminar report. It helped me a lot to realize of what we study for.
Secondly, I would like to thank my parents who patiently helped me as i went through my work and helped to modify and eliminate some of the irrelevant or un-necessary stuffs.
Thirdly, I would like to thank my friends who helped me to make my work more organized and well-stacked till the end.
Next, I would thank Microsoft for developing such a wonderful tool like MS Word. It helped my work a lot to remain error-free.

Last but clearly not the least, I would thank The Almighty for giving me strength to complete my report on time.

Preface

I have made this report file on the topic **Phishing**; I have tried my best to elucidate all the relevant detail to the topic to be included in the report. While in the beginning I have tried to give a general view about this topic.

My efforts and wholehearted co-corporation of each and everyone has ended on a successful note. I express my sincere gratitude to ……..who assisting me throughout the preparation of this topic. I thank him for providing me the reinforcement, confidence and most importantly the track for the topic whenever I needed it.

CONTENTS

1. INTRODUCTION

In the field of computer security, Phishing is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication. Phishing is a fraudulent e-mail that attempts to get you to divulge personal data that can then be used for illegitimate purposes.

There are many variations on this scheme. It is possible to Phish for other information in additions to usernames and passwords such as credit card numbers, bank account numbers, social security numbers and mothers' maiden names. Phishing presents direct risks through the use of stolen credentials and indirect risk to institutions that conduct business on line through erosion of customer confidence. The damage caused by Phishing ranges from denial of access to e-mail to substantial financial loss.

This report also concerned with anti-Phishing techniques. There are several different techniques to combat Phishing, including legislation and technology created specifically to protect against Phishing. No single technology will completely stop Phishing. However a combination of good organization and practice, proper application of current technologies and improvements in security technology has the potential to drastically reduce the prevalence of Phishing and the losses suffered from it. Anti-Phishing software and computer programs are designed to prevent the occurrence of Phishing and trespassing on confidential information. Anti-Phishing software is designed to track websites and monitor activity; any suspicious behavior can be automatically reported and even reviewed as a report after a period of time.

This also includes detecting Phishing attacks, how to prevent and avoid being scammed, how to react when you suspect or reveal a Phishing attack and what you can do to help stop Phishers.

The simplified flow of information in a Phishing attack is:-

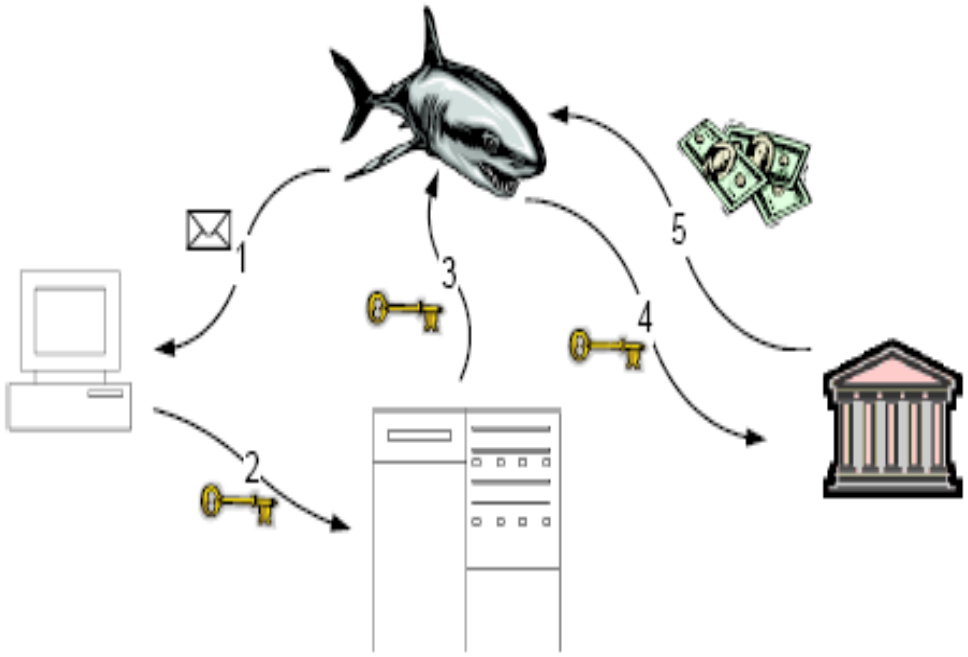

Figure 1.1

1. A deceptive message is sent from the Phishers to the user.
2. A user provides confidential information to a Phishing server (normally after some interaction with
   the server).
3. The Phishers obtains the confidential information from the server.
4. The confidential information is used to impersonate the user.
5. The Phishers obtains illicit monetary gain.

Steps 3 and 5 are of interest primarily to law enforcement personnel to identify and prosecute Phishers. The discussion of technology countermeasures will center on ways to disrupt steps 1, 2 and 4, as well as related technologies outside the information flow proper.

2. PHISHING TECHNIQUES

Phishers use a wide variety of techniques, with one common thread.

2.1. LINK MANIPULATION

Most methods of Phishing use some form of technical deception designed to make a link in an e-mail appear to belong to the spoofed organization. Misspelled URLs or the use of sub domains are common tricks used by Phishers. In the following example, `http://www.yourbank.example.com/`, it appears as though the URL will take you to the *example* section of the *yourbank* website; actually this URL points to the "*yourbank*" (i.e. Phishing) section of the *example* website.

An old method of spoofing used links containing the '@' symbol, originally intended as a way to include a username and password. For example, `http://www.google.com@members.tripod.com/` might deceive a casual observer into believing that it will open a page on `www.google.com`, whereas it actually directs the browser to a page on `members.tripod.com`, using a username of `www.google.com`: the page opens normally, regardless of the username supplied.

2.2. FILTER EVASION

Phishers have used images instead of text to make it harder for anti-Phishing filters to detect text commonly used in Phishing e-mails.

2.3. WEBSITE FORGERY

Once a victim visits the Phishing website the deception is not over. Some Phishing scams use JavaScript commands in order to alter the address bar. This is done either by

placing a picture of a legitimate URL over the address bar, or by closing the original address bar and opening a new one with the legitimate URL.

2.4. PHONE PHISHING

Messages that claimed to be from a bank told users to dial a phone number regarding problems with their bank accounts. Once the phone number (owned by the Phishers) was dialed, prompts told users to enter their account numbers and PIN. Vishing (voice Phishing) sometimes uses fake caller-ID data to give the appearance that calls come from a trusted organization.

3. PHISHING EXAMPLES

3.1. PAYPAL PHISHING

In an example PayPal phish, spelling mistakes in the e-mail and the presence of an IP address in the link are both clues that this is a Phishing attempt. Another giveaway is the lack of a personal greeting, although the presence of personal details would not be a guarantee of legitimacy. A legitimate Paypal communication will always greet the user with his or her real name, not just with a generic greeting like, "Dear Accountholder." Other signs that the message is a fraud are misspellings of simple words, bad grammar and the threat of consequences such as account suspension if the recipient fails to comply with the message's requests.

Note that many Phishing emails will include, as a real email from PayPal would, large warnings about never giving out your password in case of a Phishing attack. Warning users of the possibility of Phishing attacks, as well as providing links to sites explaining how to avoid or spot such attacks are part of what makes the Phishing email so deceptive. In this example, the Phishing email warns the user that emails from PayPal will never ask for sensitive information. True to its word, it instead invites the user to follow a link to "Verify" their account; this will take them to a further Phishing *website*, engineered to look like PayPal's website, and will *there* ask for their sensitive information.

3.2. RAPID SHARE PHISHING

On the RapidShare web host, Phishing is common in order to get a premium account, which removes speed caps on downloads, auto-removal of uploads, waits on downloads, and cool down times between downloads.

Phishers will obtain premium accounts for RapidShare by posting at warez sites with links to files on RapidShare. However, using link aliases like TinyURL, they can disguise the real page's URL, which is hosted somewhere else, and is a look-a-like of Rapid Share's "free user or premium user" page. If the victim selects free user, the Phishers just passes them along to the real RapidShare site. But if they select premium, then the Phishing site records their login before passing them to the download. Thus, the Phishers has lifted the premium account information from the victim.

Examples of Phishing E-mails

Phishing e-mail messages take a number of forms. They might appear to come from your bank or financial institution, a company you regularly do business with, such as Microsoft, or from your social networking site.

The main thing Phishing e-mail messages have in common is that they ask for personal data, or direct you to Web sites or phone numbers to call where they ask you to provide personal data. The following is an example of what a Phishing scam in an e-mail message might look like.

Figure 3.2.1

Example of a Phishing e-mail message, which includes a deceptive Web address that links to a scam Web site.

To make these Phishing e-mail messages look even more legitimate, the scam artists may place a link in them that appears to go to the legitimate Web site (1), but actually takes you to a phony scam site (2) or possibly a pop-up window that looks exactly like the official site.

Phishing links that you are urged to click in e-mail messages, on Web sites, or even in instant messages may contain all or part of a real company's name and are usually *masked*, meaning that the link you see does not take you to that address but somewhere different, usually an illegitimate Web site.

Notice in the following example that resting (but not clicking) the mouse pointer on the link reveals the real Web address, as shown in the box with the yellow background. The string of cryptic numbers looks nothing like the company's Web address, which is a suspicious sign.

Figure 3.2.2

Example of a masked Web address

4. REASONS OF PHISHING

Let's consider some of the reasons people fall victim to Phishing scams.

4.1. TRUST OF AUTHORITY

When a Phishing email arrives marked as "High Priority" that threatens to close our bank account unless we update our data immediately, it engages the same authority response mechanisms that we've obeyed for millennia. In our modern culture, the old markers of authority – physical strength, aggressiveness, ruthlessness – have largely given way to signs of economic power. "He's richer than I am, so he must be a better man". If you equate market capitalization with GDP then Bank of America is the 28th most powerful country in the world. If you receive a personal email purported to come from BOA questioning the validity of your account data, you will have a strong compulsion to respond, and respond quickly.

4.2. TEXTUAL AND GRAPHIC PRESENTATION LACKS TRADITIONAL CLUES OF VALIDITY

Most people feel that they can tell an honest man by looking him in the eye. You can spot a "professional" panhandler before he gets to the fourth word in his spiel. Without clues from the verbal and physical realms, our ability to determine the validity of business transactions is diminished. This is a cornerstone of the direct mail advertising business. If a piece of mail resembles some type of official correspondence, you are much more likely to open it. Car dealers send sales flyers in manila envelopes stamped "Official Business" that look like the envelopes tax refund checks are mailed in. Banks send

credit card offers in large cardboard envelopes that are almost indistinguishable from FedEx overnight packages. Political advertisements are adorned with all manner of patriotic symbols to help us link the candidate with our nationalistic feelings.

4.3. E-MAIL AND WEB PAGES CAN LOOK REAL

The use of symbols laden with familiarity and repute lends legitimacy (or the illusion of legitimacy) to information—whether accurate or fraudulent—that is placed on the imitating page. Deception is possible because the symbols that represent a trusted company are no more 'real' than the symbols that are reproduced for a fictitious company. Certain elements of dynamic web content can be difficult to copy directly but are often easy enough to fake, especially when 100% accuracy is not required. Email messages are usually easier to replicate than web pages since their elements are predominately text or static HTML and associated images. Hyperlinks are easily subverted since the visible tag does not have to match the URL that your click will actually redirect your browser to. The link can look like

http://bankofamerica.com/login but the URL could actually link to

http://bankofcrime.com/got_your_login

5. DAMAGES CAUSED BY PHISHING

The damage caused by Phishing ranges from denial of access to e-mail to substantial financial loss. This style of identity theft is becoming more popular, because of the readiness with which unsuspecting people often divulge personal information to Phishers, including credit card numbers, social security numbers, and mothers' maiden names. There are also fears that identity thieves can add such information to the knowledge they gain simply by accessing public records. Once this information is acquired, the Phishers may use a person's details to create fake accounts in a victim's name. They can then ruin the victims' credit, or even deny the victims access to their own accounts.

It is estimated that between May 2004 and May 2005, approximately 1.2 million computer users in the United States suffered losses caused by Phishing, totaling approximately US$929 million

6. ANTI-PHISHING

There are several different techniques to combat Phishing, including legislation and technology created specifically to protect against Phishing.

6.1. SOCIAL RESPONSES

One strategy for combating Phishing is to train people to recognize Phishing attempts, and to deal with them. Education can be effective, especially where training provides direct feedback. One newer Phishing tactic, which uses Phishing e-mails targeted at a specific company, known as ***Spear Phishing***, has been harnessed to train individuals at various locations.

People can take steps to avoid Phishing attempts by slightly modifying their browsing habits. When contacted about an account needing to be "verified" (or any other topic used by Phishers), it is a sensible precaution to contact the company from which the e-mail apparently originates to check that the e-mail is legitimate. Alternatively, the address that the individual knows is the company's genuine website can be typed into the address bar of the browser, rather than trusting any hyperlinks in the suspected Phishing message.

Nearly all legitimate e-mail messages from companies to their customers contain an item of information that is not readily available to Phishers. Some companies, for example PayPal, always address their customers by their username in e-mails, so if an e-mail addresses the recipient in a generic fashion ("*Dear PayPal customer*") it is likely to be an attempt at Phishing. E-mails from banks and credit card companies often include partial account numbers. However, recent research has shown that the public do not typically distinguish between the first few digits and the last few digits of an account number—a significant problem since the first few digits are often the same for all clients of a financial institution. People can be trained to have their suspicion aroused if the

message does not contain any specific personal information. Phishing attempts in early 2006, however, used personalized information, which makes it unsafe to assume that the presence of personal information alone guarantees that a message is legitimate. Furthermore, another recent study concluded in part that the presence of personal information does not significantly affect the success rate of Phishing attacks, which suggests that most people do not pay attention to such details.

The Anti-Phishing Working Group, an industry and law enforcement association has suggested that conventional Phishing techniques could become obsolete in the future as people are increasingly aware of the social engineering techniques used by Phishers. They predict that Pharming and other uses of malware will become more common tools for stealing information.

6.2. TECHNICAL RESPONSES

Anti-Phishing measures have been implemented as features embedded in browsers, as extensions or toolbars for browsers, and as part of website login procedures. The following are some of the main approaches to the problem.

6.2.1 Helping to identify legitimate sites

Most Phishing websites are secure websites, meaning that SSL with strong cryptography is used for server authentication, where the website's URL is used as identifier. The problem is that users often do not know or recognize the URL of the legitimate sites they intend to connect to, so that the authentication becomes meaningless. A condition for meaningful server authentication is to have a server identifier that is meaningful to the user. Simply displaying the domain name for the visited website as some some anti-Phishing toolbars do is not sufficient. A better approach is the pet name extension for Firefox which lets users type in their own labels for websites, so they can later recognize when they have returned to the site. If the site is not recognized, then the

software may either warn the user or block the site outright. This represents user-centric identity management of server identities.

Some suggest that a graphical image selected by the user is better than a pet name

6.2.2 Browsers alerting users to fraudulent websites

Another popular approach to fighting Phishing is to maintain a list of known Phishing sites and to check websites against the list. Microsoft's IE7 browser, Mozilla Firefox 2.0, and Opera all contain this type of anti-Phishing measure. Firefox 2 uses Google anti-Phishing software. Some implementations of this approach send the visited URLs to a central service to be checked, which has raised concerns about privacy.

To mitigate the problem of Phishing sites impersonating a victim site by embedding its images (such as logos), several site owners have altered the images to send a message to the visitor that a site may be fraudulent. The image may be moved to a new filename and the original permanently replaced, or a server can detect that the image was not requested as part of normal browsing, and instead send a warning image.

6.2.3 Augmenting password logins

The Bank of America's website is one of several that ask users to select a personal image, and display this user-selected image with any forms that request a password. Users of the bank's online services are instructed to enter a password only when they see the image they selected. However, a recent study suggests few users refrain from entering their password when images are absent. In addition, this feature (like other forms of two-factor authentication) is susceptible to other attacks.

Security skins are a related technique that involves overlaying a user-selected image onto the login form as a visual cue that the form is legitimate. Unlike the website-based image schemes, however, the image itself is shared only between the user and the

browser, and not between the user and the website. The scheme also relies on a mutual authentication protocol, which makes it less vulnerable to attacks that affect user-only authentication schemes.

6.2.4 Eliminating Phishing mail

Specialized spam filters can reduce the number of Phishing e-mails that reach their addressees' inboxes. These approaches rely on machine learning and natural language processing approaches to classify Phishing e-mails.

6.2.5 Monitoring and takedown

Several companies offer banks and other organizations likely to suffer from Phishing scams round-the-clock services to monitor, analyze and assist in shutting down Phishing websites. Individuals can contribute by reporting Phishing to both volunteer and industry groups, such as PhishTank.

6.3. LEGAL RESPONSES

On January 26, 2004, the U.S. Federal Trade Commission filed the first lawsuit against a suspected Phisher. The defendant, a Californian teenager, allegedly created a webpage designed to look like the America Online website, and used it to steal credit card information. In the United States, Senator Patrick Leahy introduced the ***Anti-Phishing Act of 2005.*** Companies have also joined the effort to crack down on Phishing.

7. DEFEND AGAINST PHISHING ATTACKS

7.1. PREVENTING A PHISHING ATTACK BEFORE IT BEGINS

A Phisher must set up a domain to receive phishing data. Pre-emptive domain registration may reduce the availability of deceptively named domains. Additionally, proposal have been made to institute a "holding period" for new domain registration during which trademark holders could object to a new registration before it was granted. This might help with the problem of deceptively named domains, but would not address the ability of phishers to impersonate sites. As email authentication technologies become more widespread, email authentication could become a valuable preventive measure by preventing forged or misleading email return addresses. Some services attempt to search the web and identify new phishing sites before they go "live," but phishing sites may not be accessible to search spiders, and do not need to be up for long, as most of the revenues are gained in the earliest

7.2. DETECTING A PHISHING ATTACK

Many different technologies may be employed to detect a phishing attack, including:

- Providing a spoof reporting E-mail address that customers may send spoof emails to. This may both provide feedback to customers on whether communications are legitimate, and provide warning that an attack is underway.
- Monitoring "bounced" email messages. Many Phishers email bulk lists that include nonexistent email addresses, using return addresses belonging to the targeted institution
- Establishing "honeypots" and monitoring for email purporting to be from the institution.

There are contractors that will perform many of these services. Knowing when an attack is underway can be valuable, in that it may permit a targeted institution to

institute procedural countermeasures, initiate an investigation with law enforcement, and staff up for the attack in a timely manner.

7.3. PREVENTING THE DELIVERY OF PHISHING MESSAGES

Once a phishing attack is underway, the first opportunity to prevent a phishing attack is to prevent a phishing message from ever reaching a user.

7.3.1. Filtering

Email filters intended to combat spam are often effective in combating phishing as well. Signature-based anti-spam filters may be configured to identify specific known phishing messages and prevent them from reaching a user. Statistical or heuristic anti-spam filters may be partially effective against phishing, but to the extent that a phishing message resembles a legitimate message, there is a danger of erroneously blocking legitimate email if the filter is configured to be sufficiently sensitive to identify phishing email. Phishers depend on being able to make their messages visually appear to be from a trusted sender. One possible countermeasure is to detect unauthorized imagery in emails. There are many countermeasures that Phishers may employ against a simple image comparison, including displaying many tiled smaller images as a single larger image, and stacking up transparent images to create a composite image. This means that imagery should be fully rendered before analysis. An area of future research is how to recognize potentially modified trademarks or other registered imagery within a larger image such as a fully rendered email. A similar approach may be fruitful when applied to web sites, when a user has clicked on a link.

7.3.2. Authentication

Message authentication techniques such as Sender-ID have considerable promise for anti-phishing applications. Sender-ID prevents return address forgery by checking DNS records to determine whether the IP address of a transmitting mail transfer

agent is authorized to send a message from the sender's domain. Yahoo! Domain Keys provides similar authentication, using a
domain-level cryptographic signature that can be verified through DNS records. Some form of lightweight message authentication may be very valuable in the future in combating phishing. For the potential value to be realized, Sender-ID or a similar technology must become sufficiently widespread that invalid messages can be summarily deleted or otherwise treated prejudicially, and security issues surrounding the use of mail forwarders need to be resolved.

7.4. PREVENTING DECEPTION IN PHISHING MESSAGES AND SITES

There are two different points to thwart phishing presentation deception: at the message, and at the site to which the message points.

7.4.1. Signing

Cryptographic signing of email is a positive incremental step in the short run, and an effective measure if it becomes widely deployed in the long run. Signing may be performed either at the client or at the gateway. However, current email clients simply display an indication of whether an email is signed. A typical user is unlikely to notice that an email is unsigned and avoid a phishing attack. Signing could be more effective if the functionality of unsigned emails were reduced, such as by warning when a user attempts to follow a link in unsigned email. However, this would place a burden on unsigned messages, which today constitute the vast majority of email messages. If critical mass builds up for signed emails, such measures may become feasible.

7.4.2. Personally identifiable information

The simplest way to reduce the deceptiveness of phishing messages is to include personally identifiable information with all legitimate communications. For

example, if every email from bank.com begins with the user's name, and every email from bank.com educates the user about this practice, then an email that does not include a user's name is suspect. While implementing this practice can be complex due to the widespread use of third-party mailing services, it is an effective measure.

Personalized imagery may also be used to transmit messages. For example, when a user creates or updates account information, he or she may be allowed (or required) to enter textual and/or graphical information that will be used in subsequent personalized information. In this example, a customer of the Large Bank and Trust Company has typed in the personalized text "You were born in Prague" and selected or uploaded a picture of a Canadian penny.

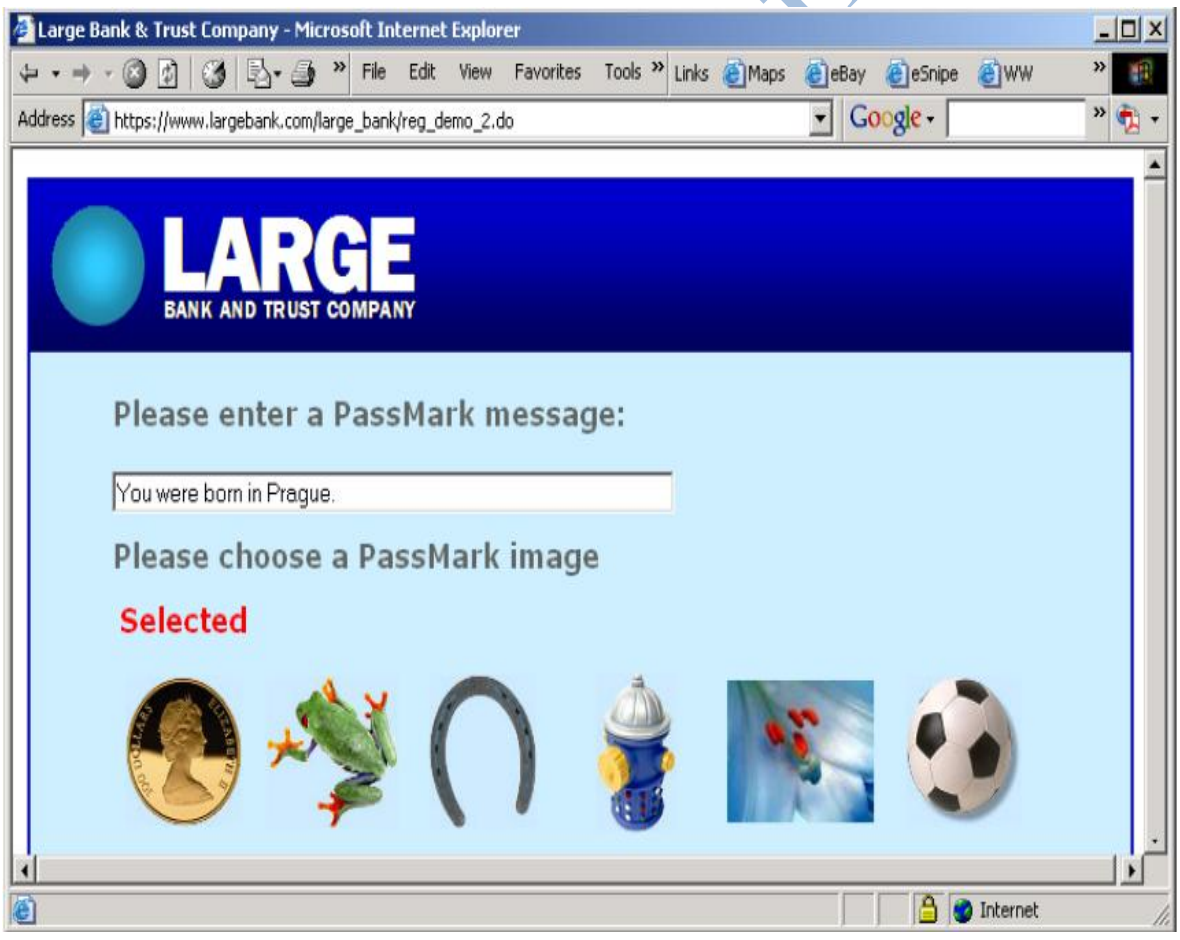

Figure 7.4.2.1 A subsequent email from Large Bank and Trust Company will include this personalized information, e.g.

Since Phishers will not know what personalized information a user has elected, they will not be able to forge deceptive emails.

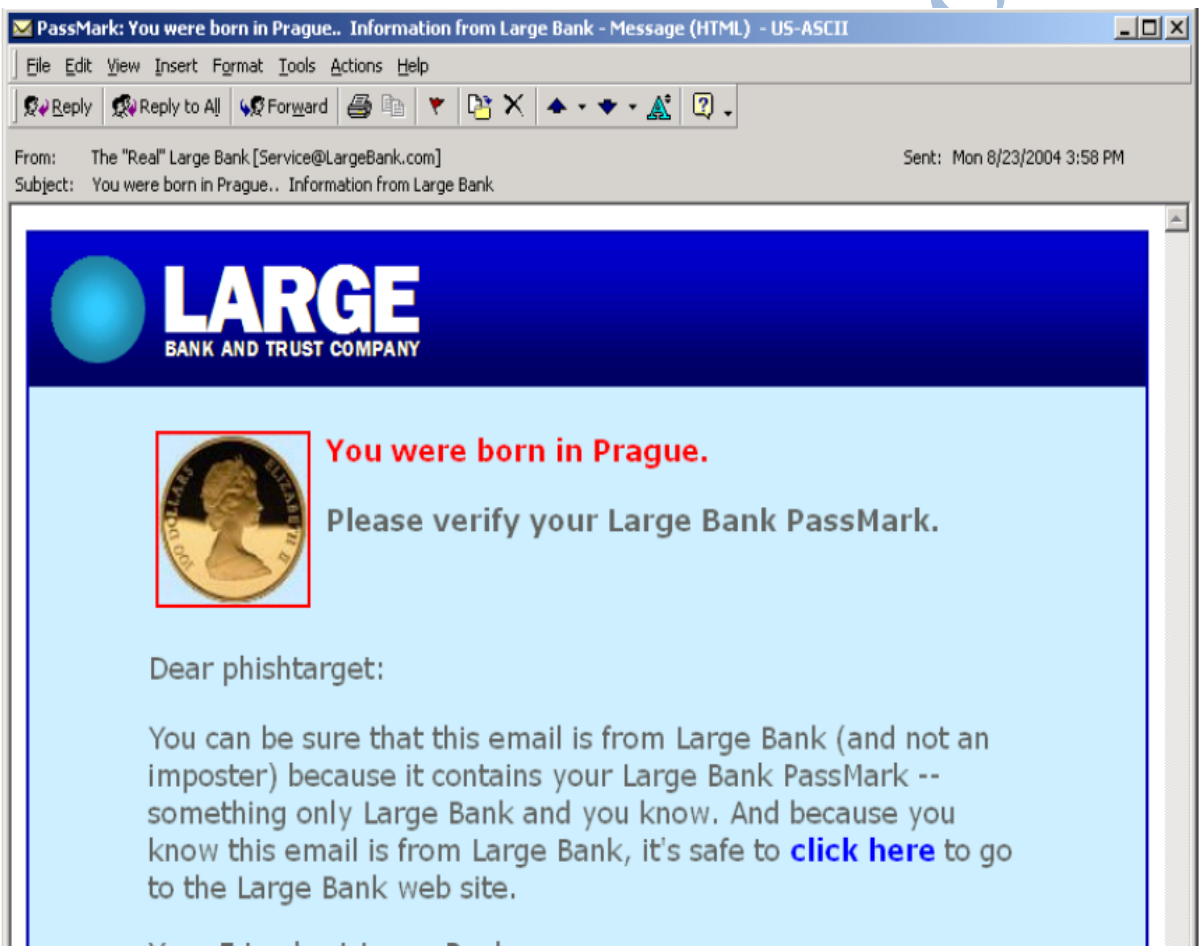

Figure 7.4.2.2

7.5. COUNTER MEASURES

7.5.1. INTERFERING WITH THE CALL TO ACTION

A phishing attack using email and a browser asks a user to perform an action, such as clicking on a link. One class of countermeasures focuses on disrupting the initial call to action.

7.5.1.1. Increasing information sharing

An area of future work is fighting phishing by increasing information sharing between spam filters, email clients and browsers. Important information is often lost in boundaries between a spam filter, an email client and a browser. A spam filter may have classified a message as being possible spam, but as long it scored below the rejection threshold, it is typically rendered by the email client on an equal basis as signed email from Microsoft.

Information gleaned while processing messages can help thwart phishing. If an email is known to be suspicious, it can be treated differently than an authenticated message from a sender on the user's whitelist or a member of a bonded sender program. Scripts can be disallowed, links can be shown with their true names, forms can be disallowed, etc. Similarly, once a user clicks on a link in an email message, information about the trustworthiness of the message can help determine whether to allow a traversal. Once a link is traversed, capabilities (scripting, form submissions, display of links, etc.) can be restricted for links pointed to in less trustworthy messages. Interfaces between spam filters, email clients and browsers that allow trustworthiness information to be transmitted would enable many new ways to combat phishing.

7.5.1.2. Warning about unsafe actions

When a user clicks on a link that is suspicious, such as a cloaked, obfuscated, mapped, or misleadingly named link, a warning message can be presented advising the user of the potential hazards of traversing the link. Information should be presented in a straightforward way, but need not be simplistic. To help the user make an informed decision, data from sources such as reverse DNS and WHOIS lookups could be usefully included:

An informative warning has the benefit of allowing legitimate links even if of a suspicious nature, while providing a risk assessment with the information a user needs to determine an appropriate action.

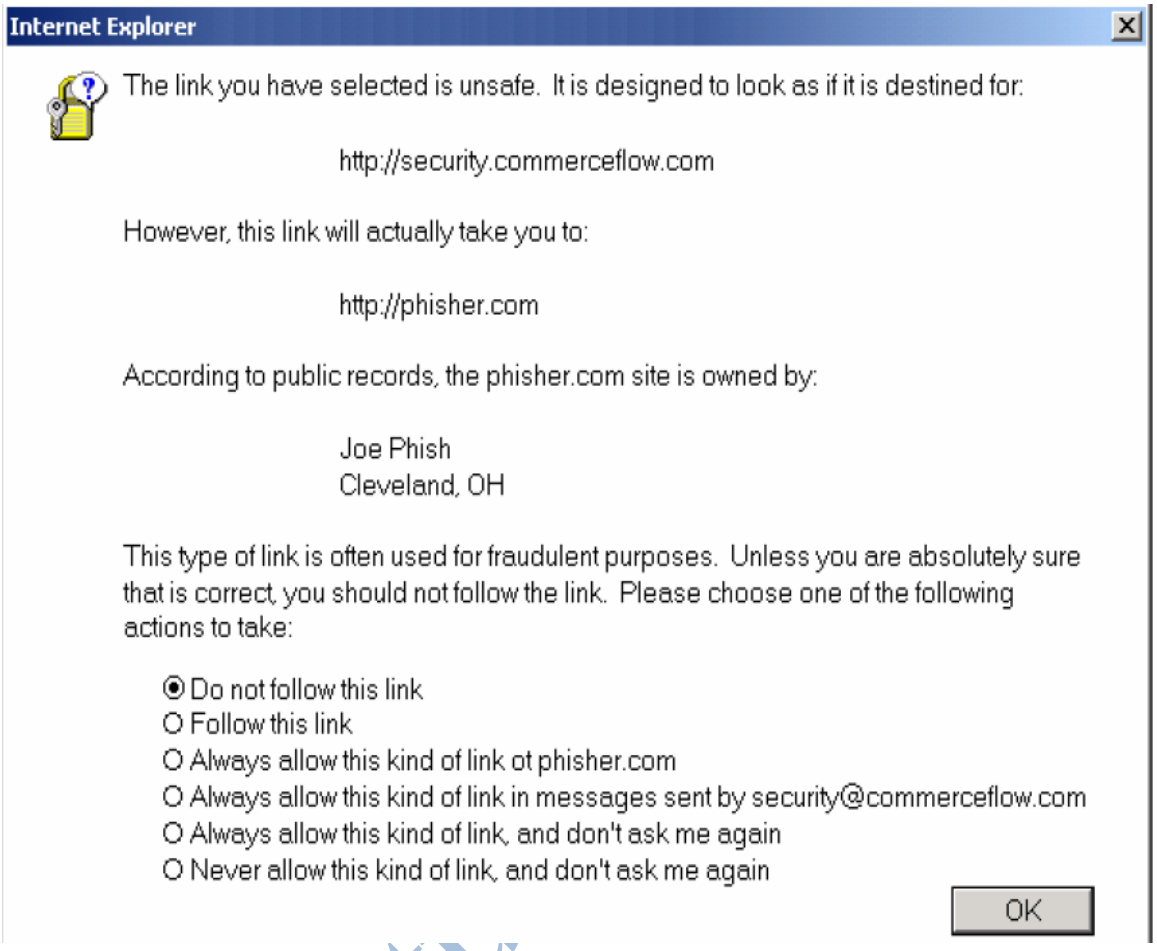

Figure 7.5.1.2.1

7.5.2. INTERFERING WITH TRANSMISSION OF CONFIDENTIAL INFORMATION

Another point at which phishing attacks may be disrupted is when a user attempts to transmit confidential information (step 2 of the phishing information flow). If the information flow can be disrupted or altered to render the confidential information unavailable or useless to the phisher, the attack can be thwarted.

7.5.2.1. Outgoing data monitoring

One class of technology to intercept the transmission of confidential information is the toolbar approach. A browser plug-in such as a toolbar can store hashes of confidential information, and monitor outgoing information to detect confidential information being transmitted. If confidential information is detected, the destination of the information can be checked to ensure that it is not going to an unauthorized location. This approach has a challenging obstacle to overcome. Phishers may scramble outgoing information before transmitting it, so keystrokes must be intercepted at a very low level. Moreover, some users enter keystrokes out-of-order for account and password information to avoid compromise by keyloggers, rendering even a protective keylogger ineffective. The long-term

viability of outgoing data monitoring as an anti-phishing technology is unclear, but presently most phishing attacks do not include effective countermeasures.

7.5.2.2. Data destination blacklisting

Some proposals have been fielded to block data transmissions to specific IP addresses known to be associated with Phishers. However, this would not prevent information transmission in a lasting manner, as information could be transmitted through covert communications channels using the internet Domain Name System (DNS) that is used to translate host names into IP addresses. A simple

example of this in which a Phishers controls the DNS server for phisher.com and wants to transmit "credit-card-info" is to incur a DNS lookup on "credit-cardinfo. phisher.com." The result of the DNS lookup is not important; the data has already been transmitted through the DNS request itself. Blocking DNS lookups for unknown addresses is not feasible, as DNS is a fundamental building block of the internet. Similarly, a blacklist based on hostnames is also susceptible to circumvention via DNS. Information can be transmitted via DNS even if the Phishers does not control any DNS server whatsoever, by using the time-to-live fields in DNS responses from innocent third-party DNS servers.

7.5.2.3. Domain-specific passwords and password hashing

Phishing for passwords only works if the password sent to the phishing site is also useful at a legitimate site. One way to prevent phishers from collecting useful passwords is to encode user passwords according to where they are used, and transmit only an encoded password to a web site. Thus, a user could type in the same password for multiple sites, but each site – including a phishing site – would receive a differently encoded version of the password. A proposed implementation of this idea is called password hashing. This method hashes password information with the domain name to which it is going, so that the actual transmitted passwords can be used only at the domain receiving the password data. Such hashing could be provided by a browser as a built-in mechanism that is automatically performed for password fields. This provides excellent data security for compromised sites as long as passwords are difficult to guess through a dictionary attack, in that stolen password data cannot be applied to any other site. However, the user still types in his or her usual password in a browser to gain account access, and it would be difficult to prevent phishers from simulating password input, bypassing any hashing, to capture the raw password data. If combined with reserved screen real estate for password entry, password hashing would be rendered less susceptible to attack.

7.6. INTERFERING WITH THE USE OF COMPROMISED INFORMATION

Another technology-based approach to combating phishing is to render compromised information less valuable. Apart from technologies to render information irretrievable, such as hashing passwords with domains and a trusted path that encrypts information with a public key, additional requirements may be placed on the use of information to mitigate the impact of compromise.

7.6.1. Conventional two-factor authentication

The most prevalent approach to reducing the impact of data compromise is known as "two-factor authentication." This refers to requiring proof of two out of the following three criteria to permit a transaction to occur:

• What you are (e.g. biometric data such as fingerprints, retinal scans, etc.)

• What you have (e.g. a smartcard or dongle)

• What you know (e.g. an account name and password)

Phishing attacks typically compromise what a user *knows*. In a remote computing environment such as the internet, it is difficult to ascertain what the user *is*, so the usual second factor is to verify something that the user *has* in addition to account information. In order for this to be effective, two-factor authentication must be required for every transaction. For example, a user must have a USB dongle, or type in a time-sensitive code from a hardware device, or swipe a smart card. This is a highly effective measure, though expensive in the cost of purchasing and distributing security devices, the deployment of infrastructure for reading them, and the inconvenience to customers in using them. Conventional two-factor authentication is appropriate for high-value targets such as commercial banking accounts, but so far has not taken root in the United States for typical consumer applications.

7.6.2. Light-weight two-factor authentication

A less costly approach to two-factor authentication is to have a device identifier, such as a checksum of all available machine information, which can authenticate the device. Such a device identifier must be transmitted only to a secure location, or employ other measures to prevent man-in-the-middle attacks. This has the advantage of not requiring additional hardware, and the disadvantage that it does not permit a user to use normal transaction authorization procedures when away from an authorized machine.

8. CROSS SITE SCRIPTING PROBLEM

Cross-site scripting, in which rather than sending an email, a phisher inserts malicious code into a web page of a targeted institution. Any web page that contains externally supplied information, such as an auction listing, product review or web-based email message, may be the target of a cross-site scripting attack. Once inserted, a script can modify elements of the host site so that a user believes he or she is communicating with the targeted institution, but actually is providing confidential information to a phisher.

8.1. FILTERING OUT CROSS SITE SCRIPTING

Any user data that is ever displayed on the screen should be filtered for cross site scripting. Malicious parties have mounted cross-site scripting attacks in unexpected areas, such as date fields of web-based email pages. Rather than filtering out forbidden script elements with a "keep-out" filter, user-supplied data should be parsed with a "let-in" filter, and only permitted data elements should be
allowed through.

8.2. BROWSER SECURITY ENHANCEMENTS TO PREVENT CROSS SITE SCRIPTING

There are many ways in which cross-site scripting may be introduced. It is difficult, expensive and error-prone to write an adequate filter, and often content that should be filtered is inadvertently overlooked. A browser extension could provide protection against cross-site scripting in the future. If a new tag was introduced that could be included in HTML, such as <noscript>, regions could be defined in which no scripting whatsoever could occur, or in which particular functionality was prohibited. The browser could guarantee this behavior, and employing sufficient filtering would be as simple as enclosing areas of user-supplied text, such as search results or auction listings, with

appropriate <noscript> and </noscript> tags. To prevent a cross-site script from including a valid </noscript> tag and inserting cross-site scripting, a dynamically generated random key should be used that must match in the <noscript> and </noscript> tags. Since the user-supplied content would have no way to know what random number was used for the key, it would lack the information required to re-enable scripting privileges. For example:

[Site-supplied HTML and scripts]
<noscript key="432097u5iowhe">
[User-supplied HTML in which scripts/features are disabled]
</noscript key="432097u5iowhe">
[Site-supplied HTML and scripts]

9. HOW ANTI-PHISHING SOFTWARE WORKS

Anti-phishing software consists of computer programs that attempt to identify phishing content contained in websites and e-mail. It is often integrated with web browsers and email clients as a toolbar that displays the real domain name for the website the viewer is visiting, in an attempt to prevent fraudulent websites from masquerading as other legitimate web sites. Anti-phishing functionality may also be included as a built-in capability of some web browsers

Common phishing tactics take advantage of a visitor by requesting them to link out to another site, asking that the enter personal information and passwords, or redirecting them to another site completely for registration. The process usually begins by sending out a forged e-mail that looks like it was sent from the company. Some tactics include saying an account has expired and needs to be updated, or has experienced unauthorized use and needs to be verified. Many banking and financial institutions become targets for these types of scams, and they can be a considerable threat to millions of account holders and users.

Many leading web browsers and software programs have realized the impact of this trend, and have created programs that can limit the frequency of these types of scams. Micirosoft Windows Internet Explorer 7, Firefox 2.0, Google Safe Browsing, and Earthlink ScamBlocker are just a few programs that have reduced the risks involved.

In Firefox 2.0, Phishing Protection is always turned on and checks the sites automatically for any potential risks or hazards. The list is reviewed on a regular basis, and can be configured to Firefox Security settings for maximum control. When Phishing Protection in enabled, the sites are downloaded into a list and checked for any anti-phishing services. A warning sign will appear if any suspicious activity is detected. The Netcraft toolbar makes use of a risk rating system, allowing you the option of entering a password (or not). TrustWatch makes the Internet Explorer toolbar, and can help validate a Web site and provide a site report when needed. This option also allows you to review

all suspected sites and find out which ones use SSL technology. Earthlink Toolbar with ScamBlocker will verify any popup messages that you may encounter as you visit a site, and can help you find out all the details on current phishing scams.

Anti-phishing software is designed to track websites and monitor activity; any suspicious behaviour can be automatically reported, and even reviewed as a report after a period of time. Anti-phishing toolbars can help protect your privacy and reduce the risk of landing at a false or insecure URL. Although some people have concerns over how valuabe anti-phishing software and toolbars may be, security threats can be reduced considerably when they are managed by the browser program. Other companies that are trained in computer security are investigating other ways to report phishing issues; programs are being designed that can analyze web addresses for fraudulent behavior through new tactics, and cross-checking domain names for validity.

10. CONCLUSION

No single technology will completely stop phishing. However, a combination of good organization and practice, proper application of current technologies, and improvements in security technology has the potential to drastically reduce the prevalence of phishing and the losses suffered from it. In particular:

- .High-value targets should follow best practices and keep in touch with continuing evolution of them.
- Phishing attacks can be detected rapidly through a combination of customer reportage, bounce monitoring, image use monitoring, honeypots and other techniques.
- Email authentication technologies such as Sender-ID and cryptographic signing, when widely deployed, have the potential to prevent phishing emails from reaching users.
- Analysis of imagery is a promising area of future research to identify phishing emails.
- Personally identifiable information should be included in all email communications. Systems allowing the user to enter or select customized text and/or imagery are particularly promising.
- Browser security upgrades, such as distinctive display of potentially deceptive content and providing a warning when a potentially unsafe link is selected, could substantially reduce the efficacy of phishing attacks.
- Information sharing between the components involved in a phishing attack – spam filters, email clients and browsers – could improve identification of phishing messages and sites, and restrict risky behavior with suspicious content.
- Anti-phishing toolbars are promising tools for identifying phishing sites and heightening security when a potential phishing site is detected.
- Detection of outgoing confidential information, including password hashing, is a promising area of future work, with some technical challenges.
- An OS-level trusted path for secure data entry and transmission has the potential to dramatically reduce leakage of confidential data to unauthorized parties.

- Two-factor authentication is highly effective against phishing, and is recommended in situations in which a small number of users are involved with a high-value target. Device identifier based two-factor authentication offers the potential for cost savings.
- Cross-site scripting is a major vulnerability. All user content should be filtered using a let-in filter. Browser security enhancements could decrease the likelihood of cross-site scripting attacks.

11. REFERENCES

http://en.wikipedia.org/

http://webopedia.com/

http://computerworld.com/

http://www.anti-phishing.info/

http://lorrie.cranor.org/