CHAPTER 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.
Phishing

Fig 1.1 the simplified flow of information in a Phishing attack

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.
CHAPTER 2

PHISHING TECHNIQUES

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

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.

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.

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
Phishing

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.

![Image of a website which does not show the real address bar]

Fig 2.1 An website which does not shows real address bar

**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.
A hacker sends a fake or "spoofed" email that appears to be from a trusted company.

The email usually instructs the user to login to verify information, and contains a link.

The link in the email directs the user's web browser to a fake website operated by the hacker.

The fake website looks exactly like a company's real website, and requires the user to login.

Any information the user enters into the fake website is immediately delivered to the hacker, which they can use to access the user's accounts.

Fig 2.2 How Phishing Attack can take place
CHAPTER 3

REASONS OF PHISHING

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

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.

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
Phishing

from FedEx overnight packages. Political advertisements are adorned with all manner of patriotic symbols to help us link the candidate with our nationalistic feelings.

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
CHAPTER 4

ANTI PHISHING TECHNIQUES

To counter the phishing threat, a number of anti-phishing solutions have been proposed, both by industry and academic world. The anti phishing techniques can in general be divided into three categories.

1. Spam Filters
2. Anti-phishing tool bars and
3. Password protection mechanism

Spam Filters

A class of anti-phishing approaches aims to solve the phishing problem at the email level. The key idea is that when a phishing email does not reach its victims, they cannot fall for the scam. Hence, filters and content analysis techniques are often used to attempt to identify phishing emails before these emails are delivered to users. Clearly, this line of research is closely related to anti-spam research [10]. By continuously training filters (e.g., Bayesian filters), a large number of phishing emails can be blocked. This is because such emails often contain words that may be identified as suspicious tokens that do not frequently occur in legitimate emails (e.g., —update‖, —login‖, etc.). The main disadvantage of anti-spam techniques is that their success depends on the availability of these filters and their proper training. That is, when the user does not actively help in training the filter, the filter typically does not perform as expected. Furthermore, even when filters are trained well and a user rarely receives any spam or phishing emails, once a phishing email bypasses the filter, the user’s belief of the legitimacy of this mail is strengthened.
Anti-Phishing Toolbars

To identify a page as a phishing site, there are a variety of methods that can be used, such as white lists (lists of known safe sites), blacklists (lists of known fraudulent sites), various heuristics to see if a URL is similar to a well-known URL, and community ratings. The toolbars examined here employ different combinations of these methods. By using publicly available information provided on the toolbar download web sites as well as observations from using each toolbar we get a basic understanding of how each toolbar functions. Some of the toolbars that are used for anti-phishing are

1) eBay Toolbar

The eBay Toolbar uses a combination of heuristics and blacklists. The toolbar also gives users the ability to report phishing sites, which will then be verified before being blacklisted.

2) GeoTrust TrustWatch Toolbar

GeoTrust’s web site provides no information about how TrustWatch determines if a site is fraudulent; however, it is suspect that the company compiles a blacklist that includes sites reported by users through a button provided on the toolbar.

3) Google Safe Browsing

Google provides the source code for the Safe Browsing feature and says that it checks URLs against a blacklist

4) McAfee SiteAdvisor
Phishing

SiteAdvisor claims to detect not just phishing websites, but any sites that send spam, offer downloads containing spyware, or engage in other similar bad practices. The determination is made by a combination of automated heuristics and manual verification.

5) Microsoft Phishing Filter in Windows Internet Explorer

This toolbar largely relies on a blacklist hosted by Microsoft. However, it also uses some heuristics when it encounters a site that is not in the blacklist. Users also have the option of using this feature to report suspected phishing sites.

6) Netcraft Anti-Phishing Toolbar

The Netcraft toolbar also uses a blacklist, which consists of fraudulent sites identified by Netcraft as well as sites submitted by users and verified by the company. The toolbar also displays a risk rating between one and ten as well as the hosting location of the site.

7) Netscape Browser 8.1

It appears that the functionality of Netscape Browser relies solely on a blacklist, which is maintained by AOL and updated frequently. When a suspected phishing site is encountered, the user is redirected to a built-in warning page. Users are shown the original URL and are asked whether or not they would like to proceed.
8) Spoofguard

Spoofguard does not use white lists or blacklists. Instead, the toolbar employs a series of heuristics to identify phishing pages.

9) AntiPhish

AntiPhish is an academic solution which keeps track of where sensitive information is being submitted to.

10) Dynamic security skins

Dynamic security skins is also an academis solution which allow a remote server to prove its identity in a way that is easy for humans to verify.

Most of the tools that were tested used blacklists, but only half of them were able to identify the majority of phishing web sites. We don’t know the size of the blacklists used by each toolbar, nor do we know what heuristics are used by any of the toolbars other than Spoofguard. We suspect that the toolbars that performed best use larger and more frequently updated black lists. They may also use heuristics that allow them to detect phishing sites that haven’t yet been put on the blacklist. The only toolbar known to make no use of blacklists was Spoofguard. While it was able to identify the majority of phishing sites using only heuristics, it still missed some phishing sites and it had a very high false positive rate. Spoofguard could potentially be improved through the use of a whitelist, which would prevent the problems that occurred when phishing sites were visited before their corresponding legitimate sites. The whitelist would not necessarily need to be extremely large or updated frequently to be effective.

Password Protection Mechanism

A password is a secret word or string of characters that is used for authentication, to prove identity or gain access to a resource. The password should be kept secret from
those who are not allowed for access. So, the major concern for any user is to safeguard his/her password. The password can be cracked with the attacks such as Guessing attack, Brute-force attack, Dictionary attack, Phishing attack etc.,.

Another problem regarding password is single password problem where the user uses a single password for both vulnerable sites and financial sites. The hackers can break into the vulnerable sites that simply stores username and password and apply those retrieved combination of username and password on high security sites such as banking sites.

All these problems at a single stroke can be solved by hashing the master password using domain name as key on client side. Some of the applications/tools that use this powerful technique are

1) Password Composer

This extension [25] puts a tiny red icon to the left of a password entry field. If one clicks on this icon, the password field is overlaid with a replacement input, where one can supply a single, secure password (Master Password).

2) Magic Password Generator

This extension combines master password and the domain name of the site to make another unique password for that site. For advanced users, with a catchall address at a domain, just put "@example.com" (whatever one’s domain is) for the address, and MPWGen will make a different email for every site too. Alternately, use "foo+@…" and the value will be inserted after the + sign, for email accounts that support this feature, like gmail.

3) Password generator

Password Generator gets the hostname from the page's URL and mixes it together with one’s personal master password using a little cryptographic magic MD5. It always gets the same result if given that hostname and master password, but will never get that result if either changes.
4) Hassapass

Hassapass automatically generates strong passwords from a master password and a parameter like domain name. The password generation is performed inside this very browser window in JavaScript.

5) Genpass

GenPass is a JavaScript/MD5 bookmarklet-based password generator. GenPass is no longer being updated. Presently consider using SuperGenPass; however, note that SuperGenPass is not compatible with GenPass—given the same input, they generate different passwords.

6) Password Hasher

When the master key is given to Password Hasher and it enters the hash word into the site's password field. A hash word is the result of scrambling the master key with a site tag. Click on a # marker next to a password field or press the Control-F6 key combination when in a password field or choose Password Hasher from either the Tools menu or the right-click popup menu on a password field to enter the master key.

7) Pwdhash

Pwdhash is a browser extension that transparently converts a user's password into a domain-specific password. The user can activate this hashing by choosing passwords that start with a special prefix (@@) or by pressing a special password key (F2). Pwdhash automatically replaces the contents of these password fields with a one-way hash of the pair (password, domain-name).
Phishing

Based on the features like application type, hashing algorithm, security, password strength, spoof proof, visibility to webpage, visibility to user etc., Pwdhash is the best among the above mentioned applications. But some of its disadvantages are as follows:

a) **Invisible to user** - Password hashing done by Pwdhash is invisible to user. If this extension stops working, user will not know about this, i.e., passwords will not be hashed.

b) **Visibility of activation to webpage** - Webpage gets the intimation about the activation of Pwdhash. This made Pwdhash vulnerable for JavaScript attacks. So webpage can put some efforts to know the original master password.

c) **Password availability as plain text** – The master password is directly filled in password field given by webpage. i.e., password is available in plain text.

d) **Easily spoof-able** – As activation is visible to webpage and by using Alex’s corner method it is very easy to know the master password of user by fake webpage.

e) **Affect on others / Affecting webpage** - Pwdhash have some side-effects on websites. Any JavaScript attached with password fields will not work properly. For ex. keyPress event will not work properly.

f) **Not secure** – Finally, Pwdhash is not looking so secured.
CHAPTER 5

ANTI-PHISHING

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

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
Phishing

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.

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.

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
Phishing

meaningful to the user. Simply displaying the domain name for the visited website as 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

**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.

**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
Phishing

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.

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.

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.

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.
CHAPTER 6

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 they 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. Microsoft 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
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 valuable 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.

The best and in most using Anti-Phishing Software is **Netcraft Anti-Phishing Toolbar**

Netcraft is an Internet Services Company located in the United Kingdom and is devoted to tracking online technology. Additionally, Netcraft has actively taken up the sole of patrolling the cyberspace to sniff out phishing emails. The *antiphising toolbar from Netcraft* not only protects you and your savings from phishing attacks but also lets you check the hosting location and Risk Rating of every site you visit. Once you download and install the toolbar, you join a *giant neighbourhood watch scheme* whose most alert and most expert members defend everyone in the community against phishing frauds. This *antiphising group working* to protect you is one of the finest ways to fight phishing.
Phishing

This could be downloaded through internet
Advantages

- Protect your savings from Phishing attacks.
- When a Phishing website or phishing email appears it will informs to the user.
- Some Anti-Phishing software's also allows seeing the hosting location and Risk Rating of every site you visit.
- 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.
Phishing

Disadvantages

• No single technology will completely stop phishing. So Phishing attacks can not be completely stopped
• Even Anti-Phishing software's should be upgraded with respect to the Phishing attacks.

CHAPTER 8

FEW SNAPSHOTs OF PHISHING WEBSITES
Dear People member,
We ask you to confirm immediately of your parity the account to given e-mail.

www.people-onlinebank.net

Otherwise we stop temporarily service of your account.
Thank you for using Suntrust Bank!

Please do not reapply this letter.
Again, thank you for using People.com

Fig 8.1 Phishing Peoples Bank Web site
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. 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.

BIBLIOGRAPHY


