PHISHING

Nishan.A.H[1], Mari Selvi.K[2]
[1,2]UG Scholars, B.Tech III Year, Department of Information Technology, Francis Xavier Engineering College,Tirunelveli.627003

ABSTRACT

In the field of computers security, phishing is the criminally fraudulent process of attempting to acquire sensitive information such as user names, passwords and credit card details, by masquerading as a trustworthy entity in an electronic attempting to acquire sensitive information such as username, password 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 user names and passwords such as credit card numbers, bank account numbers, social security numbers and mother's maiden names. Phishing presents direct risk 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 that are created specially 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 improvement 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 reported and even reviewed as a report after a period of time

This also includes detecting phishing attacks, how to prevent and avoid being scanned, how to react when your suspect or or reveal a phishing attack and what you can do to help stop phishers.

1.1 INTRODUCTION

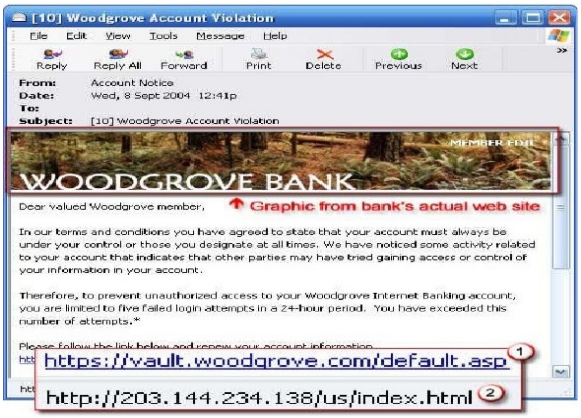
In the field of computers security, phishing is the criminally fraudulent process of attempting to acquire sensitive information such as user names, passwords and credit card details, by masquerading as a trustworthy entity in an electronic attempting to acquire sensitive information such as username, password 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 user names and

passwords such as credit card numbers, bank account numbers, social security numbers and mother's maiden names. Phishing presents direct risk 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.

There are several different techniques to combat phishing, including legislation and technology. Created specially 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 improvement 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 reported and even reviewed as a report after a period of time

This also includes detecting phishing attacks, how to prevent and avoid being scanned, how to react when your suspector or reveal a phishing attack and what you can do to help stop phishers.



1. A deceptive message is sent from the phishers to user.
2. A user provides confidential information to a phishing server (normally after some interaction with the server).
3. The phishers contains the confidential information from the server.
4. The confidential information is used to impersonate the user.
5. The phishers obtain illicit momentary again.

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

1.2 PHISHING TECHNIQUES

Phishers use a wide variety of techniques with one common thread

1.2.1 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 theURL will take you to the example section of the yourbank website;actually this URL points to the "your bank"(ie. Phishing) section of the example website.

An old method of spoofing used links containing the '@' symbol,originally intented 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 of members.tripod.com, using a username of www.google.com : the page opens normally,regardless of the username supplied.

1.2.2 FILTER EVATION

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

1.2.3 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.

1.2.4 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(ownrd by the phishers) was dialed,prompts told user to enter their account numbers and PIN. Vishing(voice Phishing) sometimes users fake caller-ID data to give the appearance that calls come from a trusted organization.

1.3 PHISING EXAMPLE

1.3.1 PAYPAL PUBLISHING

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 give a way is the lack of personal greeting, although the presence of personal details would not be a gurantee 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 Account holder". Other signs that the message is a fraud or misspelling of simple words,bad grammar and the thread of consequence such as account suspecision if the receipent fails to comply with the message request.

Note that many phishing e-mails will include, as a real e-mail from Paypal would,large warnings about never giving out your password incase of a phishing attack. Warning users of the possibility of the phishing attack as well as providing links to sites explaining how to avoid or spot such attacks are part of what makes the phishing e-mails so deceptive. In this example the phishing e-mail warns the users that e-mail from Paypal will never ask for sensitive information. True to this word, it is instead invities the user to follow a link to "Verify"their account, this will take them to a further phishing websites engineered to look like Paypals websites and will there ask for their sensitive information.

1.3.2 RAPID SHARE PHISHING

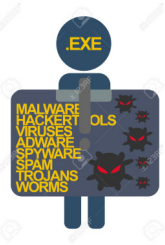
On the rapid share web hosts, phishing is common in order to get a premium account, which removes speed caps on downloads, auto removal of uploads, waits on downloads, and cool down times between downloads.

Phishers will obtain premium accounts for rapid share by hosting at warez sites with links to files on rapid shares. However, using link aliases like tiny URL, they can disguise the real pages URL, which is hosted somewhere else, and is a look alike of rapid shares"free user or premium users" pages. If the victim select free user, the phisher just passes them along to the real rapid share sites. But if they select premium, then the phishing sites records their login before passing them to the download. Thus, the phishers has lifted the premium account information from the victim.

1.3.3 EXAMPLES OF PHISHING

Phishing e-mails messages take a 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 sites.

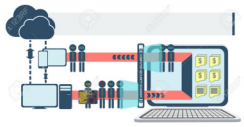
The main thing phishing e-mail messages have in common is that they ask for your personal data,or direct you to websites or phones numbers to call where they ask you to provide personal data. The following is an example of what a phishing scam in an e-mail message might look like.



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 appear to go to the legitimate website(1),but actually takes you to a phony scam site(2) or possibility a pop-up window that looks exactly like the official sites .

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



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 yellow back ground. The string of cryptic numbers looks nothing like companies web address, which is the suspicious sign.

1.4 REASONS OF PHISHING

Some of the reasons people fall victim to the phishing scams are

1.4.1 TRUST OF AUTHORITY

When a phishing e-mail arrives marked as "High priority" that threatened to close our bank account unless the update our data immediately, it engages the same authority response mechanism that we have obey for millennia. In our modern culture, the old marker of authority-physical strength, aggressiveness, ruthlessness-have largely given way to sign of economic power. "He is richer than I am,so he must be a better man". If you equate market capitalization with GDP then the bank of America is the 28th most powerful country in the world. If you receive a personal e-mail purported to come from BOA questioning the validity of our account data, you will have a strong compaltion to respond, and respond quickly.

1.4.2 TEXTUAL AND GRAPHIC REPRESENTATION LACKS TRADITIONAL CLUES OF VALIDITY

Most people feel that can tell an honest man by looking him in the eye.you can spot a "professional" panhandler before he gets to the fourth world in his spiel.without clues from the verbal and physical realms,our ability to determine the validity of business transaction is diminished.this is a cornerstone of the direct mail advertising business.if a piece of mail resembles some type of official correspondences,you are much more likely to open it.car dealers send sales flyers in manila envelopes stamped" official business" that look like the envelops tax refund checks are mailed in.bank send credit card offers in large cardboard envelops that are almost indistinguishable from Fedex over my pakage.political adverdisements are adomed with all manner of patriotic symbols to help us link the candidate with our nationalistic feelings.

1.4.3 E-MAIL AND WEB PAGES CAN LOOK REAL

The use of symbol laden with familiarity and repute lend legitimacy(or the illusion of legitimacy)

To information-whether accurate or fraudulent –that is placed on the imitating page. Reception is possible because the symbol that represents a trusted company or no more'Real' that the symbols that are reproduced for a fictitious company. Certain elements of dynamic web content can be difficult to copy

Directly or often easy enough to fake,especially when 100% accuracy is not required. E-mail messages are usually easier to replicate that web pages since their elements are pre-dominatly text or statics HTML and associated images. Hyper links are easily subverted since the visible tag does not have to match the URL that you click with actually re-direct 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

1.5 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 if 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 also fears that identify 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 victim's credit, or even the victims access of their own accounts.

It is estimated between May 2004 and May 2005,approximately 1.2 million computer users in the united states suffered losses caused by phishing, totally approximately Us $ 929 million

1.6 **ANTI-PHISHING**

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

1.6.1 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 individual 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 topic used by Phishers),it is a sensibke precaution to contact the company from which the e-mail apparently orginates to check the e-mail is legitimate. Alternatively, the e-mail apparently orginates to check 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 message from companies to their customers contain an item of information that is not really available to Phishers. Some companies, for example PayPal, always address their customers by their username in e-mails, so if an e-mail address the receipent in a generic fashion("Dear PayPal customer")

It is likely topartial account number. However, recent research has shown that the public do not typically distinguishable between the first few digits and the last few digits of an account number-a significant problem sice the first few digits are often the same for all clients of a financial institutions. People can be trained to have their suspicion aroused if the message does not contain any specifie=c personal information. Phishing attempts in early 2006, however, used personalized information, which makes it unsafe to assume that the presence of personal information alone gurantees that a message is legitimate.Further more, another recent study concluded in part that the presence of personalinformation does not significantly affect the success rate of Phishing attacks, which suggests that most people do not pay attention to such details.

1.6.2 TECHNICAL RESPONSES

Anti-phishing measure have been implemented as features embedded in browsers, as extensions or toolbars for browsers, and as part of website login procedures.

1.6.3 LEGAL RESPONSES

On January 26, 2004, the U.S. Federal Trade Commission field the fist lawsuit against a suspected Phisher. The defendant, a Californian teenager, allegedly created a webpage 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.

1.7 DEFEND AGAINST PHISHING ATTACK

1.7.1 PREVENTING 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 e-mail authenciation could become a valuable preventive measure by preventing forged or misleading email return address. Some services attempt to search the web and identity new phishing sites before they go"Live",but phishing sites may not be accessible to searc spiders, and do not need to be up for long, as most of the revenues are gained in the earliest.

1.7.2 DEFECTING PHISHING ATTACKS

Many different technologies may be employed todetect a phishing track, including:

Providing a spoof reporting e-mail address that customers may send spoof e-mail address that customers may send spoof emails to. This may both provide feed back 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 nonexistence email address, using return addresses belonging to the targeted institution

Establishing "honeypots" and monitoring for email purporting to be from the institution.

1.7.3 PREVENT DELEVERY 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.

1.7.4 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 of lightweight message authenciation may be very valuable in the further in combating phishing. For the potential value to be added, Sender-Id or a similar technology must become sufficiently widespread that invalid prejudicially, and security issues surrounding the use of mail forwards need to be resolved.

1.7.5 PREVENTING DECEPTION IN PHISHING MESSAGES AND SITES 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 gate way. However, current email clients simply displays an indication of whether an email is signed. A typical user is unlikely to notice that 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 message, which today constitute the vast majority of email messages. If critical mass builds up for signed emails, such measures may become feasible.

1.7.6 PERSONALLY IDENTIFIABLE INFORMATION

The simplest way to reduce the deceptiveness of phishing message is to include personally identifiable information with all legitimate communications. For example, if every email from bank. Comeducates the 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 measures.

Personalized imagery may also be used to transmit messages. For example , when a user creates to 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.

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

COUNTER MEASURES

INTERFERING WITH THE CALL TO ACTION

A phishing attack using email and abrowser asks a user to perform an action, such as clicking on a link.one class of counter measures focuses on disrupting the initial call to action.

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 bounded 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 alink 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 would enable many new ways to combat phishing.

WARNING ABOUT UNSAFE ACTION

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 informated 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.

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.

OUTGOING DATA MONITORING

One class of technology to interceptthe 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 keystrockes 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 attacks do not include effective countermeasures.

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 inti IP addresses>A simple example of this in which a phishers controles the DNS server for phisher. com and wants to transmit" credit-acrd- 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 responses from innocent third-party DNS servers.

DOMAIN-SPECIFIC PASSWORD 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 website.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 built-in mechanism that is automatically performed for password files. This provides excellent data security for the compromised sites as long as passwords are difficult to guess through the 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.

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 is 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.

CONVENTIONAL TWO-FACTOR AUTHENTICATION

The most prevalent approach to reducing the impact of data compromise is know as " two – factor authentication." This refers to requiring proof of two out of thefollwing 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. smartcard or dongle)
- What you know (e.g. an account name and password)

Phishing attacks typically compromise what a usere 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 a addition to account information. In order for this to be effective, two- factor authentication must be required for every transation. For example , a user must have a USB dingle, 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 not taken root in the United States for typical consumer applications.

LIGHT-WEIGHT TWO-FACTOR AUTHENTICATION

A less costly approach to two-factor authentications 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.

CROSS SITE SCRIPTING PROBLEM

Cross-site scripting, in which rather than sending an email, a phisher inserts malicious xode into a web page of a target 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 belives he or she is communicating with the targeted institution, but actually is providing confidential information to a phisher.

FILTERING OUT CROSS SITE SCRIPTING

Any user data that is every displayed on the screen should be filtered for the 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.

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 inadvertentkly 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 listing, 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 keys 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 for the key, it would lack the information required to re-enable scripting privilages. 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]

HOW ANTI-PHISING SOFTWARE WORKS

Anti-phishing software consists of computer programs that attempt to identify phishing content contained in websites and email. It is often integrated with web browsers and emails 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 need to e verified.many banking and financial institution become targets for this type of scams, and they can be 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 earth link scamBlocker are just a few programs that have reduced the risks involved.

In firefox 2.0, phishing protection is always turned on and check sites automatically for any potential risks or hazards. The list of reviewed on a regular basis, and can be configured to firefox security setting for maximum control. When phishing protection in enabled, the suites 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 neede. This option also allows you to review all suspected sites and find out which ones use SSL technology. Earthlink toolbar with scamBloker 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 behavior can be automatically reported,and even reviewed as areport after a period of time. Anti-phishing toolsbar 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 threads can be reduced considerably when they aremanaged by the browser program. Other companies that are trained in computer security are investing other ways to report phising issues; programs are being designed that can analyze web addresses for fraudulents behavior through new tactics, and cross-checking domain names validity.

CONCLUSION

No single technology will completely stop phishing. However, a combination of good organization and practice, proper application of current technologies, andimprovements 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, honey pots and other techniques. E-mails authentication technologies such as sender-ID and cryptographic singing, 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, inching password hashing,is a promising area of future work, witnsome 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 recommented in a situation in which a small number of users are involved with a high value target. Device identifier based two-factor authentication offers the potential for coast 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 script attacks.

REFERENCE

1. www.wikipedia.com
2. www.w3schools.com