Study on Security Policy Options for Responding to Phishing

Policy Development Division
Korea Information Security Agency
KISA, IT venture tower, Garakdong, Songpagu, Seoul
Korea

Phishing is targeted financial scam in which attacker uses social engineering and spyware, malicious code methods to steal personal data such as credit card numbers. Many companies are trying to protect themselves and customers by seeking solutions designed to stop phishing. However no safeguard is perfect. For a phishing attack, Phishers use a number of methods to trick internet users such as man-in-the-middle attacks, URL obfuscation, observing user data, cross-site scripting attacks, hidden attacks. Phishing countermeasures are technological, social, legal ones. And we propose political options. Government's security agencies should assess pishiing risk, and establish government-wide guidance, and improve citizen's phishing-awareness, and establish governmental collaboration system for coping with phishing, and revise legal system.

Key-Words: - Phishing, Threats, Security, Pharming, Attacks

1 Introduction

Lately law enforcement authorities, businesses, and Internet users have seen a remarkable increase in the use of "phishing. A growing number of phishing schemes are using for illegal purposes the names and logos of legitimate financial institutions, businesses, and government agencies. Phishing is a term coined by computer hackers, who use email Internet hoping to hook users into supplying them the loggins, passwords or credit card information.

Phishing is wide spread targeted financial scam in which attackers or scammers use social engineering and spyware, malicious code methods to steal personal and credential data such as credit card numbers, account usernames, password and other identification of Internet users[16].

Phishing employed social engineering technique to extract personal and financial data of the users and each phishing attack targeted a specific financial institution, further reducing the chances of success. But not all users can be bait of phishing. On the other hand, pharming can affect a far greater number of online banking users in which keylogger and malware/spyware get installed on a user's system. Pharming is a technique to redirect users from real websites to the fraudulent websites by using malware/spyware, typically DNS hijacking. Pharming uses modifications in the name resolution system, so as when a user clicks a financial institution web pages, it actually goes to the spoofed website[16].

2 The Phishing Threat

2.1 Social Engineering Factors

Phishing attacks rely on a mix of technical deceit and social engineering practices.

In general, the Phisher must persuade the victim to intentionally perform a series of actions that will provide access to confidential information[2].

In computer security, social engineering is a term that describes a non-technical kind of intrusion that relies on human interaction and often involves tricking other people to break normal security procedures[17].

Another aspect of social engineering relies on people's inability to keep up with culture that relies heavily on information technology. Social engineers rely on the fact that people are not aware of the value of the information they process, and so are careless about protecting it[17].

2.2 Financial Loss

Phishiers use the personal data such as credit card number, account user name and passwords and financial information, to charge goods onto the victim's credit card or steal money from the victim's bank account by using spoofed emails and websites.

On the Internet, phishing is a scam where the perpetrator sends out legitimate-looking emails appearing to come from the some of the Web's biggest sites including eBays, MSN, Citibank, America Online and so on.

Furthermore, phisher's email displayed AOL logos as well as legitimate links. But when recipients clicked on the "AOL Billing Center" link, they were taken to to a spoofed AOL web pages asking for personal identification information.

2.3 Dramatic Development of Phishing Skill

It is apparent that fraudsters perpetrating phishing scams are becoming more technologically efficient, utilizing smarter deception methods to create and implement their scams.

Trojan, worm viruses are sent to users as an email attachment. The attachment is a program that exploits vulnerabilities in Internet Browsing software to force a download from another computer on the Internet. The Trojan is designed to harvest personal information, which is then sent to a remote computer on the Internet.

Spyware which is planted on a user's computer, captured information entered at legitimate web sites and sent this information to fraudsters via a remote computer in the Internet.

2.4 Difficulties in Response

Many companies are trying to protect themselves and customers by seeking solutions designed to stop phishing. Because recovering from large scale phishing scam would be detrimental not only to the company's bottom line, but also to maintaining the trust of their customers.

However no safeguard is perfect. Whatever preventions white hat programmers cook up, lack hat programmers will eventually dismantle. It needs customer's attention to distinguish phishing email from others.

3 Phishing Cases

The word "phishing" originally comes from the analogy that early Internet criminals used email lures to fish(phish) for passwords and financial data from the Internet users. The term was coined in the 1996 timeframe by hackers who were stealing AOL accounts by scamming passwords from unsuspecting AOL users. The popularized first mention on the Internet of phishing was made in hacker newsgroup in January 1996.

By 1996, hacked accounts were called "phish" and by 1997 phish were actively being traded between hackers as form of electronic currency. There are instances where phishers would routinely trade 10 working AOL phish for a piece of hacking software. The earliest media citation referring to phishing wasn't made until 1997.

The term phish covers not only obtaining user account details, but also no includes access to all personal and financial data[2].

3.1 Phishing Cases in the World

On Nov. 2003, many eBay customers received email notification that their accounts had been compromised and were being restricted. In the message, was a link to what appear to be an eBay web page where they could re-register. The top of the page looked like eBay's homepage and incorporated all the eBay internal links. To re-register, the customers were told, they had to provide credit card data, personal identification numbers, social security number, date of birth and their mother's name. The problem was, eBay hadn't sent the original email, and the web page didn't belong to eBay. It was prime example of phishing.

In recent, 17-year-old male sent out messages purporting to be from AOL, stating a billion problem with recipients' AOL accounts.

Lloyds TSB scam which is sent to online banking community, asks customers to confirm account data by clicking on the link email. Some victims are taken to a spoof login page where sensitive account details are captures by the phishers.

On Feb. 2005, Harry Potter author J.K. Rowling warned her fans scammers attempting to sell e-book versions of her next release. Customers received and email which asks for bank account information so that an electronic copy of the novel can be bought. But she said those are all phishing scams.

On Jan. 2005, unsolicited email claiming to be from Red Cross International, the Netherlands asks recipients to donate money to tsunami victims by arranging a money transfer.

3.2 Phishing Cases in Korea

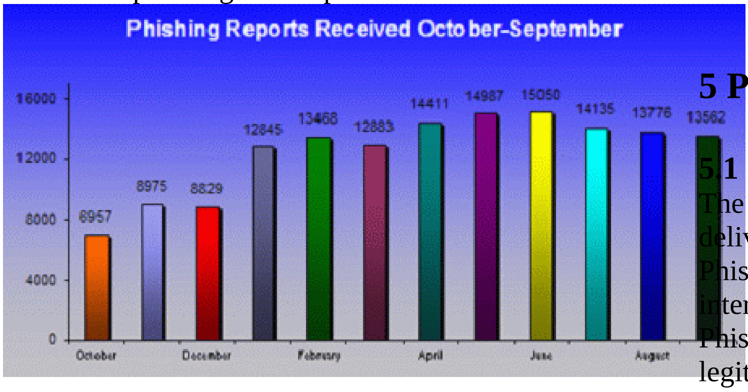
South Korea relatively has been safe from the phishing criminals as the mails were written in English. But since the first outbreak of the Korean bank-related phishing in July, alarm was raised among local firms, too.

In Aug. 2005, a group of five criminals also set up a fake banking site on the Web and enticed Internet users by offering a low-interest loan. The hackers even made phone calls to assure the victims and confirm their online banking ID and password. With the phished information, the gang drew 120 million won from 12 bank accounts until caught by police.

In Dec. 2005, police arrested two men for sending 170 million phishing spam mails by which they acquired personal information from some 150,000 people. As the mail carried a rather general questionnaire such as name, telephone number and home address, a large number of the recipients didn't hesitate to answer it.

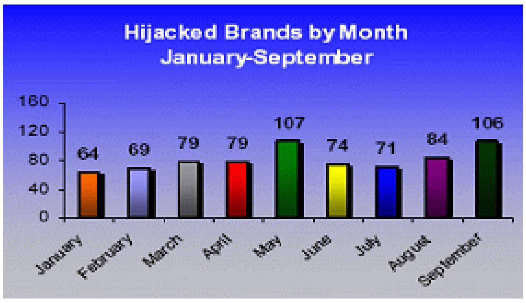
4 Phishing Statistics

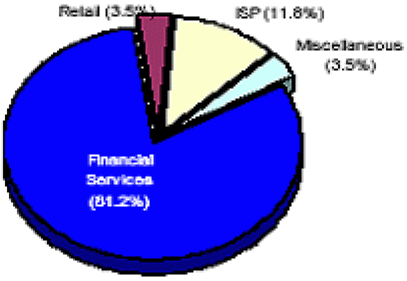
According to Anti-Phishing Working Group(APWG), the number of reports received in Sep. 2005 13,562 continuing a trend of dramatic growth for a year from Oct. 2004. In Sep. 2005, we can see a continuation of a trend of using cousin domain names to host phishing sites. Consequently, the use of alternate ports has decreased and the standard HTTP port 80 is in use 98% of all phishing sites reported.



In Sep. 2005, the number of phished brands grows to 106 brands by 26% compared to previous month. The visible trend is that brands in the "favorites" list tend to remain for a long time, and the ones in the "tail" frequently change.

The 81% of phished brands are financial companies and 11.8% are ISP such as AOL, then 3.5% are e-commerce site like eBay. The sector distribution is a function of the brand distribution, thus there is a large, stable share(the financial sector) and a small fluid share(everything sector)





5 Phishing Methods

5.1 Phishing Message Delivery

The most common method for phishing message delivery is phishing attacks initiated by email Phishers deliver specially crafted emails to millions of internet users within a few hours. Techniques used in Phishing emails use official looking emails, copies of legitimate corporate emails with minor URL changes, HTML based email used to obfuscate target URL, fake postings to popular message boards and mailing lists, etc.

Using IRC and Instant Messaging becomes a popular phishing ground. As these communication channels become more popular, and messenger's functionality improves, intelligent phishing attacks will increase. As many messengers allow for embedded dynamic content such as graphics, and multimedia to communicate among channel participants, it is considered a trivial task to employ the phishing techniques used in standard web-based attacks.

Phishing attacks initiated through malicious web-site content become an increasingly popular method. This content may be included in a web-site operated by the Phisher. Web-based delivery techniques include the inclusion of HTML disguised links within popular web-sites, the use of fake banner advertising graphics to lure customers to the Phishers web-site, the use of web-bugs to track a potential customer in preparation for a phishing attack etc.

The delivery source may be home PC's that have been previously compromised. A Trojan horse program has been installed which allows Phishers to use the PC as a message propagator.

5.2 Phishing Attack Methods

For a Phishing attack, Phishers use a number of methods to trick internet users. The most common methods are man-in-the-middle attacks, URL obfuscation, observing user data, cross-site scripting attacks, Hidden attacks etc.

In case of Man-in-the-Middle attack, the attacker situates themselves between the user and the real web-based application, and proxies all communications between the systems for gaining control of customer information and resources. From this, the attacker can observe and record all transactions.

In case of URL obfuscation attacks obfuscates the final destination of the user's web request using bad domain names, friendly login URL's, third-party shortened URL's, and host name obfuscation

Observing user Data is an old favorite hacking methods and becoming increasingly popular among phishers. Key-loggers and screen-grabbers is commonly used to observe confidential user data

In the Cross-site scripting attacks, attacks use custom URL or code injection into a valid web-based application URL or imbedded data field using web-application design vulnerabilities. Unfortunately, the user has no way of knowing that web page is legitimate or not.

In the hidden attacks, the attacker disguises fake content as coming from the real site using hidden frames, overriding page content, graphical substitution.

6 Phishing Countermeasures

6.1 Technical Countermeasures

Possible preventative technology solutions are "Strong Website Authentication", "Mail Server Authentication", and "Mail Authentication via Digital Signatures"

Strong Website Authentication would require all users of legitimate e-commerce and themselves to the site using a physical token such as a smart card. For this, enterprises must issue tokens to their customers, customers must install the necessary software on their desktops, and 3rd party trust authorities may have to issues certificates on behalf of the business. This approach has the positive aspects such as 1) even if a user falls for a phishing attack, a phisher can't log into real site without the right physical token and 2) users are given a stronger sense of trust in their transactions with business web site. But this approach down-sides such as user education, set up time delays, desktop software installation, high management costs, and potentially high cost per user

Mail Server Authentication uses authenticating sending mail. This approach have positive aspects such as easy configuration at senders mail servers, making it harder for phishers to be anonymous, better identification of legitimate business email. But this approach have down-sides such as requiring sender and recipient gateways to both use these methods, being a problem for anyone using a 3rd party emailing service, and not being capable of accommodating email forwarding

Digitally Signed Email with Desktop Verification uses the existing industry standard S/MIME. This approach would send emails with a digital signature attached. If an email arrives to a user that is either not signed, or the signature can not be verified, the user would know that it is not a genuine email from the sending bank or e-commerce provider. This approach have positives such as use of S/MIME, a standard in business email clients, phisher's registration of a certificate authority, and better identification of legitimate business email. But this approach has down-sides such as recipient's need to inspect the "From:" address for misleading domains, and email client's need to support S/MIME.

Similarly Digitally Signed Email With Gateway Verification uses the S/MIME standard. A gateway server at the mail relay level would verify the signatures before they were even received by the receiver's email server.

6.2 Social Countermeasures

The "best practices" can be effective countermeasures to address phishing issues. These fall into two general categories such as corporate best practices and customer ones

Corporate best practices are like:

1) Establish corporate policies and communicate them to consumers:

Create corporate policies for E-mail content so that legitimate E-mail cannot be confused with phishing. Communicate these policies to customers and follow them.

2) Provide a way for the consumer to validate that the E-mail is legitimate: The consumer should be able to identify that the E-mail is from the institution, not a phisher. To do that, the sending institution must establish a policy for embedding authentication information into every E-mail that it sends to consumers.

3) Stronger authentication at web sites: If institutions did not ask consumers for sensitive information when logging onto a web site (e.g., social security numbers or passwords), then it would be more difficult for phishers to extract such information from the consumer.

4) Monitor the Internet for potential phishing web sites: The phishing web site generally appears somewhere on the Internet prior to the launch of the phishing E-mails. These sites often misappropriate corporate trademarks to appear legitimate.

5) Implement good quality anti-virus, content filtering and anti-spam solutions at the Internet gateway: Gateway anti-virus scanning provides an additional layer of defense against desktop anti-virus scanning. Filter and block known phishing sites at the gateway. Gateway anti-spam filtering helps end users avoid unwanted spam and phishing emails.

Consumer Best Practices is like:

1) Automatically block malicious/fraudulent E-mail: Spam detectors can help keep the consumer from ever opening the suspicious E-mail, but they aren't foolproof.

2) Automatically detect and delete malicious software: Spyware is often part of a phishing attack, but can be removed by many commercial programs.

3) Automatically block outgoing delivery of sensitive information to malicious parties: Even if the consumer can't visually identify the true web site that will receive sensitive information, there are software products that can.

4) Be suspicious: If you aren't sure if an E-mail is legitimate, call the apparent sending institution to verify the authenticity.

6.3 Legal Countermeasures

On February 28, 2005, Senator Patrick Leahy (D-VT) introduced the Anti-Phishing Act of 2005 ("the Act") in the United States Senate. The Act, if passed, will add two crimes to the current federal law: It would criminalize the act of sending a phishing email regardless of whether any recipients of the email suffered any actual damages[14]. It would criminalize the act of creating a phishing website regardless of whether any visitors to the website suffered any actual damages[10].

The UK government is proposing changes to a fraud law that would mean scammers behind phishing attacks could face up to 10 years in jail.

Under the proposal, the offence could be committed in three ways: by false representation, such as phishing scams; by failing to disclose information for financial gain; or by abuse of position. The Home Office is also planning to criminalize obtaining services dishonestly, possessing articles for use in fraud and participating in fraudulent business[12].

The Korea government changed a law (Promoting use of information and network and information security) that would mean scammers behind phishing attacks could face up to 3 years in jail or punishable with a fine of about $ 30,000.

Any legislation aimed at punishing Internet-related offenses faces three formidable hurdles: (1) difficulty inherent in finding the perpetrator of an on-line crime, (2) obtaining personal jurisdiction, and (3) collecting the judgment. Unless these can be overcome, the net impact of bills such as the Anti-Phishing Act will be limited, at best.

The first problem, finding the perpetrator, is like this. Internet allows anonymous communications that are virtually impossible to trace through Internet nodes. Cyber-tortfeasors frequently use false e-mail headers and anonymous remailers to make it difficult to retrace the steps of wrongdoing. Computer records are easy to alter and it is likely that spoliation of electronic evidence is widespread.

The second hurdle, obtaining jurisdiction over the phisher, stems from the fact that "cybercrime has always been a cross-border enterprise." Even if the perpetrator can be located, it is very possible that the person is located in a foreign country outside of the legislation's jurisdictional reach. Indeed, "countries where cybercrime flourishes tend to have weak laws dealing with computer crime, law enforcement agencies that lack computer forensic capabilities and an underdeveloped apparatus for collaborating with law enforcement agencies in other countries."

The third problem is that even if the first two hurdles are overcome the perpetrator will very often be found to be "judgment proof."46 This phenomenon is explained as follows: Even when a prevailing plaintiff wins a large punitive damages award, collecting it is a different matter. Collecting a punitive damages award is difficult because a number of wily Internet mice either fail to make an appearance, file bankruptcy, or simply disappear after the plaintiff obtains a judgment. Default judgments outnumbered cases decided by juries in the larger cybertort dataset. The large number of default judgments in cyberlaw reflects the reality that it is easy for web sites to disappear or assets to be transferred[10].

7 Policy Options

In order to more effectively prepare for and address emerging phishing threats, We recommend the following five political options:

Firstly, government's security agencies should address the risk of emerging phishing threats, including performing periodic risk assessments; implementing risk-based policies and procedures to mitigate identified risks; providing security-awareness training; and establishing procedures for detecting, reporting, and responding to incidents of emerging phishing threats[14].

Secondly, government's security agencies should establish government-wide guidance on how to address emerging phishing threats and report incidents to a single government entity, including clarifying the respective roles, responsibilities, processes, and procedures for government entities—including national security and law enforcement entities[14].

Thirdly, government's security agencies should improve citizen's phishing-awareness. They should assess actual situation by means of surveying citizen's phishing-awareness about its risk and incidents. In addition, promotion of phishing-awareness should be expanded into targets which could be damaged by cyber-crime such as individuals, companies legally responsible for cyber-crime, law-enforcing organization. For this individuals should raise awareness of current e-mail or web-mail phishing methods and their damage risk, and of need of PC security and private data protection. Companies should be aware of methods for design of application with less risk, and need awareness of several phishing types in order to identify phishing attacks and respond them respond rapidly. Companies, also, should educate their customers about phishing attacks and their risk, and countermeasures against them. Law-enforcing organization should have methods for promotion of phishing methods and effective countermeasures.

Fourthly, governmental collaboration system should be prepared for coping with phishing. Single reporting channel should be established for detection of phishing and reporting, and each organization's roles should be defined clearly. Collaboration with APWG, representative international organization to respond phishing, should be reinforced to exchange incident information, and help investigate cyber –crime. In addition, regular communication channels with agencies for superintending national financial system, agencies for customer protection, and agencies for prosecution would be recommendable. Industrial autonomous communities can be effective for responding to phishing.

In parallel with these, legal system should be revised on a continual basis. The way to overcome the limitation of legal system such as difficulties in detection of phishier, achievement of jurisdiction over phishing crimes, and verification of them should be prepared

8 Conclusion

The main objective of this paper was to survey phishing attacks and countermeasures against them, and to propose political options for designing an effective responding system to them in order to provide secure and safe cyberspace.

We conclude that government's security agencies should assess the risk of emerging phishing threats, and establish government-wide guidance on how to respond phishing, and improve citizen's phishing-awareness, and establish governmental collaboration system for coping with phishing, and revise legal system continually.

References:

[1] McAfee, *Phishing & Pharming*, 2005. 8.

[2] Gunter Ollmann., *The Phishing Guide*

[3] FSTC, *FSTC Counter-Phishing Initiative*, 2004.

[4] Anti-Phishing Working Group, *Phishing Activity Trends Report*, 2005. 9.

[5]KrCert/CC, *Korea Phishing Activity Trends Report*, 2005.10.

[6]Demopoulos Associates, *User Phishing Awareness Surve*y, 2005.10.

[7] Anti-Phishing *Working Group, Proposed Solutions to Address the Threat of Email Spoofing Scams*, 2003. 12.

[8] McAfee, *Anti-Phishing:Best Practices for Institutions and Consumers*, 2004. 3

[9] FDIC, *Putting and End to Account-Hijacking Identity Theft*, 2004. 12.

[10]Robert Louis B. *Stevenson, Plugging the Phishing Hole*, 2005. 3.

[11]IT Pro, *Launching Korea Phishing Countermeasure Association*, 2005. 5. 2.

[12]ZDNet, *Government moves to tackel phishing*, 2005. 11. 25.

[13]ITTC, *Report on Online Identity Theft Technology and Countermeasures*, 2005. 10.

[14]GAO, *Emerging Security Issues Threaten Federal Information Systems*, 2005. 5.

[15]Gregg Tally. et., *Anti-Phishing: Best Practices for Institutions and Consumers*, 2004. 3.

[16]Anil Sagar, *Phishing Attacks and countermeasures*, 2005. 3.

[17]Kathleen Ting, *Phishing*, 2005. 2.

[18]Department of Justice, *Special Report on Phishing*

[18] Jason Milletary, *Technical Trends in Phishing Attacks*

[20]Princeton Survey Research Associates International, *Spyware Survey Final Topline,* 2005. 6.

[21]OECD, *Scoping Study for the Measurement of Trust in the Online*