IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 1 Issue 6, August 2014.
www.ijiset.com
ISSN 2348 – 7968

Analysis of Issues in Phishing Attacks and Development of Prevention Mechanism

[1]Neelam Gupta, [2]Dr Vijay Singh

[1]Research Scholar, Mewar University, Chittorgarh(Raj.) deep.neel@gmail.com

[2]Rathore Professor & Director, Shree Karni Collge,

Absract

What is research design? Phishing scams have been used as a mode of online fraud over a long period. The attempts involve acquiring of individual sensitive information such as passwords, usernames and credit card information from the internet. A research design shows how information or data will be collected and the instruments that will be used to collect the data. It also shows how a given research or investigation will take place and the methods that will be used to analyze the data.. This paper aims at surveying many of the recently proposed phishing mitigation techniques. A high-level overview of various categories of phishing mitigation techniques is also presented, such as: detection, offensive defense, correction, and prevention.. The purpose of this study is to examine the available phishing literatures and phishing countermeasures, to determine how research has evolved and advanced in terms of quantity, content and publication outlets. The different approaches proposed so far are all preventive in nature. A Phisher will mainly target the innocent consumers who happen to be the weakest link in the security chain and it was found through various usability studies that neither server-side security indicators nor client-side toolbars and warnings are successful in preventing vulnerable users from being deceived. Educating the internet users about phishing, as well as the implementation and proper application of anti-phishing measures, are critical steps in protecting the identities of online consumers against phishing attacks. Further research is required to evaluate the effectiveness of the available countermeasures against fresh phishing attacks. Also there is the need to find out the factors which influence internet user's ability to correctly identify phishing websites. This paper gives brief information about phishing, its attacks, what are the negative economic , socail ,financial , corporate implications of phishing.on steps that users can take to safeguard their confidential information Anti-Phish that aims to protect users against spoofed web site-based phishing attacks. To this end, Anti-Phish tracks the sensitive information of a user and generates warnings whenever the user attempts to give away this information to a web site that is considered untrusted. Anti-Phish is based on the premise that for inexperienced, technically unsophisticated users, it is better for an application to attempt to check the trustworthiness of a web site on behalf of the user. Unlike a user, an application will not be fooled by obfuscation tricks such as a similar sounding domain name.

LITERATURE REVIEW

Historical perspective of phishing

An early form of computer hacking was to gain illicit access to other people's phone accounts and using them for illegal or expensive calls. This was called "phreaking", using the first two letters of the word "phone". It became fairly common hacker practice to replace the letter "f" with "ph" when talking about online or phone-based activities. *Phreaking* is a slang term coined to describe the activity of a culture of people who study, experiment with, or explore telecommunication systems, such as equipment and systems connected to public telephone networks. The term *phreak* is aportmanteau of the words *phone* and *freak*, and may also refer to the use of various audio frequencies to manipulate a phone system. *Phreak*, *phreaker*, or *phone phreak* are names used for and by individuals who participate in phreaking. Phreaking has since become closely linked with computer hacking. After that phishing on AOL(America Online) during the 1990s originally used fake, algorithmically generated credit card numbers to create accounts on AOL, which could last weeks or even months. After AOL brought in measures in late 1995 to prevent this, early AOL crackers resorted to phishing for legitimate accounts.

A phisher might pose as an AOL staff member and send an instant message to a potential victim, asking him to reveal his password. In order to lure the victim into giving up sensitive information the message might include text such as "verify your account" or "confirm billing information". Once

the victim had submitted his password, the attacker could access and use the victim's account for criminal purposes, such as spamming. After 1997, AOL's policy enforcement with respect to phishing became stricter and forced pirated software off AOL servers. AOL simultaneously developed a system to promptly deactivate accounts involved in phishing, often before the victims could respond. By 2004, phishing was recognized as fully industrialized, in the sense of an economy of crime: specializations emerged on a global scale and provided components for cash which were assembled into a finished attack.

The first way in which phishers conducted attacks was by using algorithms to create randomized credit card numbers. The random credit card numbers were used to open AOL accounts. Those accounts were then used to spam other users and for a wide range of other things. Phishers used email worm programs to send out spoofed emails to PayPal customers. Those customers were led to spoofed sites and asked to update their credit card information and other identifying information.By the beginning of 2004, phishers were riding a huge wave of success that included attacks on banking sites and their customers. Popup windows were used to acquire sensitive information from victims. Since that time, many other sophisticated methods have been developed. They are all on the same basic concept.

In the early days of AOL you could create a fake account as long as you had a credit card generator. AOL smartened up to this technique. AOL now uses banks to verify every credit card submitted. By 1996, hacked accounts were called “phish”. By the time 1997 rolled around phish were actively being traded between hackers as a form of currency. “The scam was called ‘phishing’ as in fishing for your password, but spelled differently” said Tatiana Gau, vice president of integrity assurance for AOL.

Current dynamics of modern day phishing scams

As the Internet has grown in popularity and convenience it is increasingly being used by people to shop, bank and carry out business online. The Internet provides access to resources and services that would be far more time-consuming and difficult to reach in person. Unfortunately though, there have been cases of the Internet and email being used for fraud – to trick people into revealing personal information in order to commit a crime. This information sheet contains information about a kind of online fraud called “phishing” and will give you some pointers on how to avoid being caught out by it. Phishing is a broadly launched social engineering attack in which an electronic identity is misrepresented in an attempt to trick individuals into revealing personal credentials that can be used fraudulently. . Phishing is a new type of network attack where the attacker creates a replica of an existing web page to fool users in to submitting personal, financial, or password data to what they think is their service provider’s website. . Phishing is a form of online identity theft that aims to steal sensitive information such as online banking passwords and credit card information from users. The effectiveness of this paper is too examined in a large-scale dataset collected from real phishing cases and to study. Different approaches for handling phishing activities. This article surveys the literature on the detection of phishing attacks. Phishing attacks target vulnerabilities that exist in systems due to the human factor. Many cyber attacks are spread via mechanisms that exploit weaknesses found in end-users, which makes users the weakest element in the security chain. The multiple techniques are often implemented to mitigate specific attacksUsing social networks, people behave more socially and are less discriminating with messages or comments they receive on their profiles. With social media, a core component of a successful phishing attack is already built-in trust. Users ‘follow’ people they know or trust, they receive messages from people or services In cases where a social network makes heavy use of URL shorteners, telling a suspicious hyperlink before browsing to it is very difficult.Avoid these Social Media Scams Social networking sites are getting much better at knowing their users and leveraging that information for more targeted marketing and sales More ways to phish, more data to steal more attacks and more successful phishing.

Another factor for encouraging phishing to come through social networks is enterprises going social. This new and increasingly ‘social’ nature of delivering phishing attacks is a reflection of user behavior – a factor that will always be the most significant driver for online crime trends.Growing use of social networking is going to make phishing via that media more popular with time, and just further supporting the need for ongoing and timely user-education and awareness campaigns to help consumers protect their online identities and accounts. As we post more and more information about ourselves on sites such as twitter and Facebook, scammers can increasingly find ways to steal not only our personal details, but also the company details of the organisations. New threat vectors have been well and truly opened with the rise of social media and its interconnectedness with our professional lives. Phishers can now access and infiltrate our corporate networks by tailoring fake emails from ‘business associates’ which actually contain malicious links and malware.

How to protect yourself

A simple way to prevent your identity from being stolen is to limit the amount of personal details you share. It is always a safer bet to get in touch with a contact personally via email. One way to beat the phishing scammers is to stay one step ahead of the game and to be aware of the new, emerging threats. Phishers can now hack into our systems with “Open Source Intelligence Collection”; this is a term used to describe when hackers or nation-state sponsored adversaries gather as much information as possible from information available on the internet or other sources to allow the attack to be launched

The chance to promote yourself and network online is great, but this shouldn’t be at the risk of your personal identity being stolen, or even your colleagues finding themselves are the receiving end of a phishing scam. Always remember there are cyber criminals and state-sponsored attackers who are prepared to exploit the data you are voluntarily uploading to social media to attack you and your employer.

Email Phishing scams are carried out online by tech-savvy con artists and identity theft criminals. They use spam, fake websites constructed to look identical to real sites, email and instant messages to trick you into divulging sensitive information, like bank account passwords and credit card numbers. Once you take the phisher's bait, they can use the information to create fake accounts in your name, ruin your credit, and steal your money or even your identity. Phishing scams often lure you with spam email and instant messages requesting you to "verify your account" or "confirm your billing address" through what is actually a malicious Web site. Be very cautious. Phishers can only find you if you respond.

Phishers often pretend to be legitimate companies. Their messages may sound genuine and their sites can look remarkably like the real thing. It can be hard to tell the difference, but you may be dealing with a phishing scam if you see the following:

-Requests for confidential information via email or instant message

-Emotional language using scare tactics or urgent requests to respond

-Misspelled URLs, spelling mistakes or the use of sub-domains

-Links within the body of a message

-Lack of a personal greeting or customized information within a message. Legitimate emails from banks and credit card companies will often include partial account numbers, user name or password.

-Do not provide personal information to any unsolicited requests for information

-Only provide personal information on sites that have "https" in the web address or have a lock icon at bottom of the browser

-If you suspect you've received phishing bait, contact the company that is the subject of the email by phone to check that the message is legitimate

-Type in a trusted URL for a company's site into the address bar of your browser to bypass the link in a suspected phishing message

-Use varied and complex passwords for all your accounts

-Continually check the accuracy of personal accounts and deal with any discrepancies right away

Make sure that you have the best security software products installed on your PC for better phishing protection:

- Use antivirus protection and a firewall
- Get antispyware software protection

Do *not* copy and paste text or links from the email to your web browser. What you might be able to do if the link is live and you're in an online email program, is hover your mouse over the link, *without* clicking and check the browser for confirmation of where that link will take you; if it's not legitimate, you'll soon see an odd address. This is simply more confirmation of your suspicions.

Banks do not send emails asking for you to input personal information from an email link. They're wise to the scams, so don't fall for any such emails. Visit or call the bank if you're worried and get reassurance from a teller or customer service officer (and use the Yellow Pages telephone number, not any number provided in an email).

Latest in phishing is application of Trojan horse program.Trojan horse" program insinuates itself into a user's computer via an email and directs the user of the system to website which is exactly similar to financial institution web site. Crooks pick up passwords and account numbers as soon

as customer logon to these sites. Phishing causes maximum loss to the customers/ institution in comparison to other similar techniques. Keeping in view, the serious threats of phishing attacks author analyzed the trends of major activities of the phishing across globe specifically in the banking sector. In addition, author analyzed the reasons for increase in fishng activities, types of phishing techniques, and process of phishing. Further author has presented recent cases of phishing specifically in banking/ financial sector. Towards the end it author has studied the measures to combat the fishing in online banking. Globally, about 30,000 phishing attacks are reported each month, of which over 80% are directed at financial institutions. Statistics presented in table 5 is an ample proof of sharp increase in phishing activities. Phishing attackers have targeted at financial entities such as Citibank, Wells Fargo, Halifax Bank, eBay, and Yahoo as reported by Secure Science Corporation eBAy and Paypal are favaorite of phisher during the last five years.

Phishing Identification mechanisms

To protect users against phishing,various anti-phishing techniques have been proposed that follows different strategies like client side and server side protection. In this we reviewed some of the existing antiphishing techniques along with their advantages and disadvantages.AntiPhish is an application that is integrated into the web browser. It keeps track of a user's sensitive information (e.g., a password) and prevents this information from being passed to a web site that is not considered "trusted" (i.e., "safe"). The development of AntiPhish was inspired by automated form-filler applications. The symmetric DES algorithm is used for the encryption and decryption. Anti-phishing refers to the method employed in order to detect and prevent phishing attacks. Anti-phishing protects users from phishing. A lot of work has been done on anti-phishing devising various anti-phishing techniques. Some techniques works on emails, some works on attributes of web sites and some on URL of the websites. Many of these techniques focus on enabling clients to recognize & filter various types of phishing attacks. In our current implementation, user interaction is needed to tell AntiPhish that a piece of information on a page is important and that it should be protected against phishing attempts.Besides storing the sensitive information, AntiPhish also stores a mapping of where this information "belongs" to. That is, the domain of the web site where this information was . The AntiPhish application menu integrated into the browser.nally entered is also stored. We use domains instead of web site addresses because some web sites are hosted on multiple servers with different addresses. Hence, if web server addresses or URLs are used instead of domains, false phishing alarms could be generated.In our prototype, we provide simple dialogs for the management of stored sensitive information.The user can see a list of web site domains from which sensitive information has been captured and has the possibility of clearing this cached information. Originally, the primary advantage for criminals conducting phishing-related fraud was the lack of education and awareness of a) the existence of financial crimes targeting internet users, and b) the policies and procedures of online sites for contacting their customers regarding account information and maintenance issues. The root of the phishing problem is that users are not able to identify if the website is original or fake. Looking at the URL and SSL certificate carefully can really help but not all users have the time or technical skill to analyze and make the correct judgement.

Although the best prevention technique against Phishing attacks is security awareness there is no warranty that the users can learn and use this knowledge and then always be up to date. Therefore, science of computer security creates some countermeasures against these attacks. Since types of Phishing attacks are variant, the prevention techniques should be diverse. Some of these techniquesare:

- "Signature based" techniques, similar to "spam protection" techniques
- "Model based" features which are actually statistical trainable filtering
- "PHONEY" which is mimicking the user's response to detect Phishing attacks
- A frame work to detect similar domain names and fraud action
- Domain Name Server
- Phishing-based keyloggers have tracking components which attempts to monitor specific actions
- Uniform resource locator (URL) confirmation in this Web address should be preceded by https:// instead of the usual http:// in the browser's Address bar.

The considerable progress in the prevention methods could lead to a huge change on phishing attacks in the near future. But, there is no doubt that this fight will be continued for many years between the security experts and the attackers similar to virus's technology, therefore people must have some knowledge about security to deal with these attacks. Phishers are getting better every day. The security industry has taken up the challenge and today we have multiple solutions to the problem. We need to move towards effective solutions without over-burdening the user -like personalised images during login or passwords through SMS. Only time will tell , which of these will meet both objectives - survive the latest attacks and find user acceptance.

ISSN 2348 – 7968

Negative implications of Phishing

The effects of phishing cannot be overstated - this criminal method of acquiring personal data via emails and webpages in order to fool a financial institution is a huge threat with shocking consequences. Providing private information to an unauthorized person (e.g., name, address, phone number, email, account etc.) ,Experiencing identity theft as a result of stolen personal information ,Lost money or property as a result of stolen personal information , Loss of use of a service, such as an email account , Reduced trust in people, Reduced trust in echnology, Unwillingness to use a service in the future are the losses due to phishing. Phishing affects us all it also steals identity.

Criminal organizations around the world use the technique known as phishing to extract information from innocent citizens in order to access their bank details, steal identities, launder money and more.Attempts can be difficult to spot with an untrained eye, and successful phishing affects everybody, from the bank manager to small children whose school, club or church group may be caught out by this type of scam.The effect of phishing on the economy is also powerful but rarely as long lasting, hard-hitting or just downright embarrassing as when they con you. The criminals perpetrating these thefts are clever, and skilled at deception. The effect of phishing scams can be swift, resulting in identity theft, the loss of thousands of pounds of savings, running up of huge debts and even repossession of vehicles and property.
It is estimated that businesses in the United States lose $2 billion dollars per year when their clients are targeted by phishing scams. While many banks and businesses are of the opinion that customers are also responsible for taking precautions, the truth is that many don't. As a result, many businesses that communicate regularly with their customers via email have taken steps to personalize their communications. Phishers often don't get information such as usernames or even first names when attempting to gain information via fake emails, so the genuine institutions have been able to gain an advantage by addressing customers directly either in emails or on their websites.

The increasing stealing information (both personal and corporate), malicious attacks all have serious business implications to the more traditional impacts to storage, bandwidth, infrastructure and other costs. Phisher can use data to access a victim's account and withdraw money or purchase or services. Phishers can use the data to open new bank or credit-card accounts in a victim's names, and use the new account to cash illegitimate checks or purchase merchandise. Phishers can install computer viruses and worms on a victim's computer.

-The impact of phishing is far more insidious than just an invasion of privacy. Phishing is used to compromise computer security through social engineering. It can be used to steal information, disrupt computer operations, steal money, ruin reputations, destroy important information or feed the ego of an attacker. The most destructive uses are probably to facilitate the theft of information from companies and governments and the theft of money from individuals and corporations. Hijack your usernames and passwords.

-Steal your money and open credit card and bank accounts in your name

-Request new account Personal Identification Numbers (PINs) or additional credit cards

-Make purchases

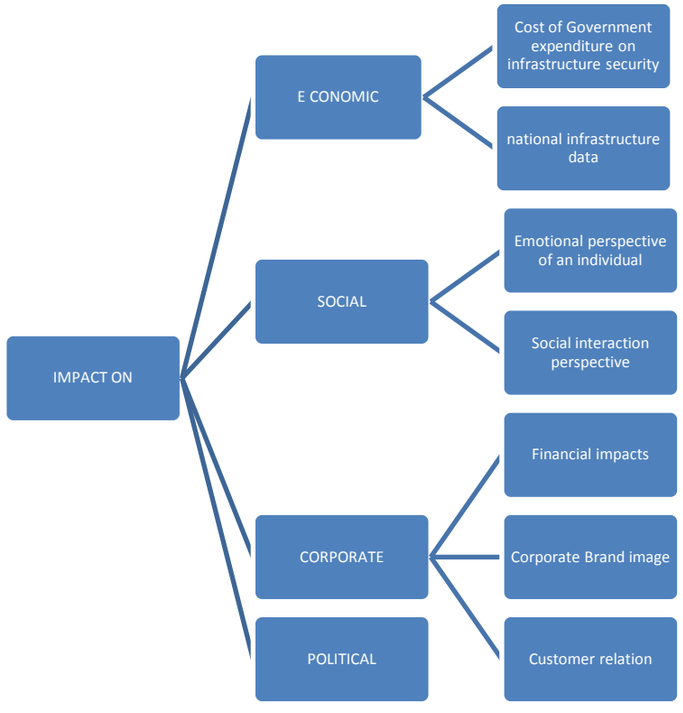

Figure 1 : Impact on Organization

-Add themselves or an alias that they control as an authorized user so it's easier to use your credit

-Obtain cash advances

-Use and abuse your Social Security number

-Sell your information to other parties who will use it for illicit or illegal purposes

Conclusion

Phishing is a highly profitable activity for criminals. Over the past two years, there has been an increase in the technology, diversity, and sophistication of these attacks in response to increased user awareness and countermeasures, in order to maintain profitability. Users have become more aware of phishing crimes and how to identify unsophisticated phishing sites. In response, criminals are using web browser vulnerabilities and obfuscation techniques to create phishing scam pages that are more difficult to differentiate from legitimate sites; thus users can become victims even if they are aware of phishing scams. In reaction to increasing response from service providers and law enforcement, criminals are using increasing technical sophistication to establish more survivable infrastructures that support phishing activities. The key building blocks for these infrastructures are the botnets that are used to send phishing emails and host phishing sites. We have also observed specialized malware that can be used to target sensitive information, with an increased potential to cause damage. Malware is providing the means for criminals to create more effective phishing attacks that can target multiple businesses at a time. Malware is also evolving to acquire particular sensitive information (e.g., TAN numbers) that was created especially for authorizing online commerce transactions. These trends are important to understand as they show the ability of criminals to recognize and adapt to increasing awareness of and response to phishing. By properly understanding the continual evolution of technical capabilities used by those who commit phishing and online financial fraud in general, more effective countermeasures and more secure online commerce systems can be developed. Based on the technological trends that phishing criminals are deploying to undertake their activities, phishing awareness is an integral element of the counter phishing strategies. Phishing awareness must be educated both to the customers and the employees of the organization. Vigilance and foresight should also be put into consideration during the development of online communication platform, whereby companies should take into account the risk associated with the unauthorized access of personal information.

Currently, reviews have shown that the widespread phishing attacks on government and private data is increasing at an alarming rate. Initially it had key insights on the general consumers within the public with the aim of stealing personal data such as credit card information, intellectual property, organizations' financial data, and other sensitive information about national infrastructure found online. The hacking world has witnessed an evolution in terms of the phishing attacks because most attacks no longer are being concentrated toward social basis like stealing social media passwords for online trolling, but are redirected toward stealing sensitive information such as intellectual property and support designs. Most attackers now employ spear phishing to steal information from selected individuals. It indicated that the increased level of selectiveness in the choice of target and increased advancement in the sophistication levels of phishing thus is becoming a serious concern . Most developers and organizations have shifted the blame to the users for not being aggressive enough in employing the recommended measures to prevent phishing attacks. As much as this is an issue of concern and is true. The developers should be focused on coming up with effective countermeasures that ensure protection of the user and organizations' sensitive data from such attacks (Oriyano and Shimonski, 142). Development of a prevention mechanism proves to be a challenge, given the increased shift in online activities in modern society. Developers can employ various strategies, such as providing adequate training, to a wide range of users, thus imparting awareness, development of high-level user interfaces that will restrain the phishing attacks, and finally making different things invisible because they will reduce chances of an attacker manipulating a given system or user information. This all includes enabling filtering phishing emails, blockage of phishing sites, and other alternative authentication measures.

References

1."Phishing" scams. (2007). Bismarck, ND: Office of Attorney General, Consumer Protection Division.

2.Geier, E. (2006). *Simple computer security: disinfect our PC ; [special version of CA Internet security suite for computers running MicrosoftÂ® WindowsÂ® included on two CD-ROMs; hacker attacks, identity theft, phishing scams, viruses, spam, spyware, and more ...]*. Indianapolis, Ind.: Wiley.

3.Hatton, L. (2011). *E-mail forensics: eliminating spam, scams and phishing*. New Malden: Bluespear Pub.

4.Miller, M. (2007). *Absolute beginner's guide to computer basics* (4th Ed.). Indianapolis, Ind.: Que.

5.Scams & swindles phishing, spoofing, ID theft, Nigerian

ISSN 2348 – 7968

advance schemes, investment frauds, false sweethearts: how to recognize and avoid financial rip-offs on the Internet age. (2006). Los Angeles, CA: Silver Lake.

6..http://www.historyofphonephreaking.org/faq.php Sterling 2002: 39

*7.History of Phishing*Written by Carl E. Reid on February 12, 2009

8. "GP4.3 - Growth and Fraud — Case #3 - Phishing". *Financial Cryptography*. December 30, 2005.

9. Journal of Internet Banking and Commerce, August 2007, vol. 12, no.2 (http://www.arraydev.com/commerce/jibc/) Online Frauds in Banks with Phishing First Author's Name: N. P. Singh, PhD

10.T. Hansen Request for Comments: 5585 AT&T Laboratories Category: Informational D. Crocker Brandenburg InternetWorking P. Hallam-Baker Default Deny Security, Inc. July 2009

11.The Critical Effects of Phishing Scams written by: Christian Cawley•edited by: Simon Hill•updated: 3/4/2010