ISSN 2250-3153

E-Mail Phishing - An open threat to everyone

Gori Mohamed .J, M. Mohammed Mohideen, Mrs.Shahira Banu. N

Assistant Professor, Department of Information Technology, Mohamed Sathak A.J College of Engineering, Chennai, TamilNadu, India

Abstract- We cannot imagine a day without a computer especially without Internet. E-Mail is one of the primary ways through which we communicate. We not only use it every day for official communication but also to be in touch with our friends and relatives. As E-Mail plays a vital role in communication globally for communication and sharing of data as well. The security issues also have increased. The major problem or the attack on E-Mail by the hackers nowadays is known as E-Mail Phishing. It is the right time to secure the data communicated over mail even on trusted network. Cyber criminals craft these emails to look convincing, sending them out to literally millions of people around the world. The criminals do not have a specific target in mind, nor do they know exactly who will fall victim. They simply know the more emails they send out, the more people they may be able to fool. In this paper we are analyzing the various ways in which the Phishing is achieved, the possible solutions and the awareness along with some tips to be away from a victim of Phishing attacks are discussed.

Index Terms- *Phishing, Cyber Security, E-Governance, Cyber Crime*

I. INTRODUCTION

Email is one of the most widely and commonly used internet services. We not only use it everyday for official communication but also to be in touch with our friends and relatives. Phishing was a term originally used to describe email attacks that were designed to steal your online banking username and password. However, the term has evolved and now refers to almost any email-based attack. Phishing uses social engineering, a technique where cyber attackers attempt to fool you into taking an action. These attacks often begin with a cyber criminal sending you an email pretending to be from someone or something you know or trust, such as a friend, your bank or your favorite online store. These emails then entice you into taking an action, such as clicking on a link, opening an attachment or responding to a message. As E-Mail plays a vital role in communication globally for communication and sharing of data as well. The security issues also have increased. The mail infrastructure employed on the internet primarily consists of email servers using SMTP to accept messages from clients, transport those messages to other servers, and deposit them into a user's server-based inbox. In addition to email servers, the infrastructure includes email clients. Clients retrieve email from their server-based inboxes using POP3 or IMAP. A client communicates with email servers using SMTP. Basically the basic email system is not secure as the protocols used to support email do not employ encryption. Thus, all the messages are transmitted in the form in which they are submitted to the email server. In addition to this email phishing problem, password cracking is also a problem in email system, crackers try to indulge into email system by compromising the password using well known attacks such as dictionary attacks and others.

Phishing websites can be achieved easily by sending a spoofed link. It impersonates legitimate counterparts to lure users into visiting their websites. Once users visit a phishing website then the phishing website may steal users' private information or cause drive-by downloads. Here the main problem we have to address is not only the website phishing but also the root cause i.e Email Phishing. This paper will strive to identify the phishing mail at the maximum level by implementing some added security layers.

Phishing has becoming a serious network security problem, causing finical lose of billions of dollars to both consumers and e-commerce companies. And perhaps more fundamentally, phishing has made e-commerce distrusted and less attractive to normal consumers

In addition, email itself can be used as an attack mechanism using DoS attack known mail-bombing resulting the legitimate messages can not be delivered. Spam: sending unwanted, inappropriate, or irrelevant messages. It is often difficult to stop spam because the source of the messages is usually spoofed. These attacks often begin with a cyber criminal sending you an email pretending to be from someone or something you know or trust, such as a friend, your bank or your favorite online store. These emails then entice you into taking an action, such as clicking on a link, opening an attachment or responding to a message. Cyber criminals craft these emails to look convincing, sending them out to literally millions of people around the world. The criminals do not have a specific target in mind, nor do they know exactly who will fall victim. They simply know the more emails they send out, the more people they may be able to fool.

II. RELATED WORK

1. Dr.anthony yingjie fu in Ph.D thesis titled "web identity security: advanced phishing attacks and counter measures-2006. He has mentioned that it is possible to detect phishing web pages by evaluating the visual similarity of web pages.
Visual assessment approach, semantic assessment approach, human computer interaction enforcement, and web page originality verification.

2. Mr.Shalendra Chhabra in his MS thesis titled "Fighting Spam, Phishing and Email Fraud" has mentioned that He illustrated and explained CRM114 usage for small-, medium-, and large-scale enterprises (for filtering up to one million client email accounts). He presented the internals of a system using CRM114, implementing the concept of Internet postage known as the CAMRAM. He described a unified model of spam filtration followed by all the spam filters currently available in the market. He also presented the Markov Random Field model

and Nick Littlestone's Winnow-based machine learning techniques for spam-filtering, which have shown significant improvements in accuracy over the Na¨ive Bayesian filtering technique.

3. Mr.Madhusudhanan and co in their research paper titled "Phishing Email detection based on structural properties" have illustrated that phishing mails can be classified easily before it reaches the inbox using their prototype.

III. PROPOSED WORK

Upon researching on all the existing method to classify phishing emails before it reaches the users' inbox we have been planning to match original emails website image with the suspected email's webpage image using image processing concept in future.

Phishing attacks work one of four ways:

• **Harvesting Information:** The cyber attacker's goal is to fool you into clicking on a link and taking you to a website that asks for your login and password, or perhaps your credit card or ATM number. These websites look legitimate, with exactly the same look, imagery and feel of your online bank or store, but they are fake websites designed by the cyber attacker to steal your information.

• **Infecting your computer with malicious links:** Once again, the cyber attacker's goal is for you to click on a link. However, instead of harvesting your information, their goal is to infect your computer**.** If you click on the link, you are directed to a website that silently launches an attack against your computer that if successful, will infect your system.

• **Infecting your computer with malicious attachments**:

These are phishing emails that have malicious attachments, such as infected PDF files or Microsoft Office documents. If you open these attachments they attack your computer and, if successful, give the attacker complete control.

• **Scams:** These are attempts by criminals to defraud you. Classic examples include notices that you've won the lottery, charities requesting donations after a recent disaster or a dignitary that needs to transfer millions of dollars into your country and would like to pay you to help them with the transfer. Don't be fooled, these are scams created by criminals who are after your money.

List of phishing techniques

Phishing

Phishing is a way of attempting to acquire information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in an electronic communication.

Spear phishing

Phishing attempts directed at specific individuals or companies have been termed spear phishing Attackers may gather personal information about their target to increase their probability of success.

Clone phishing

A type of phishing attack whereby a legitimate, and previously delivered, email containing an attachment or link has had its content and recipient address(es) taken and used to create an almost identical or cloned email. The attachment or Link within the email is replaced with a malicious version and then sent from an email address spoofed to appear to come from the original sender. It may claim to be a resend of the original or an updated version to the original. This technique could be used to pivot (indirectly) from a previously infected machine and gain a foothold on another machine, by exploiting the social trust associated with the inferred connection due to both parties receiving the original email.

Whaling

Several recent phishing attacks have been directed specifically at senior executives and other high profile targets within businesses, and the term **whaling** has been coined for these kinds of attacks.

Link Text in Email Differs From Link Destination

In fraudulent email, the link that was present in the email is usually different than the actual destination. For example, the email looks as though it is going to send the user to "http://account-registration.com," but instead sends the user to http://www.membership.com. http://account.earthlink.com

Reply Address Differs From the Claimed Sender

In some fraudulent emails messages, the email claims to be from a credible reputable company, but the email is set to reply to a fraudulent reply address. The following are some examples from fraudulent emails:

From: Greenland Security Dept. From: IobBank
Reply-To: greenland80@1-base.com
Reply-To: Iobbank41@collegeclub.com

Approaches to Prevent Phishing Attacks

There are several (technical or non-technical) ways to prevent phishing attacks:

1)Educate users to understand how phishing attacks work and be alert when phishing-alike e-mails are received.

2) use legal methods to punish phishing attackers

3) Use technical methods to stop phishing attackers. In this paper,

4) Detect and block the phishing Web sites in time

5) Enhance the security of the web sites

6) Block the phishing e-mails by various spam filters:

IV. PROTECTING YOURSELF

In most cases, simply opening an email is safe. For most attacks to work you have to do something after reading the email (such as opening the attachment, clicking on the link or responding to the request for information). But to be safer if you are using GMAIL then follow this.

Always use 2-factor authentication if are a Gmail user which prevents unauthorized access to your email inbox also forbids legal issues on which the crackers will make in your name if your mail password is compromised. Recently gmail has released an android application called "Google Authenticator"

Which does not require internet connection. We can add n number of accounts. It generates verification code for every 60 seconds. When you sign in to Google, you will have to enter your username and password as usual. Then another screen appears asking for another level of securing your mail for OTP like verification code which usually will be sent to our registered mobile number but due to network failure we may face some difficulties in getting this verification code. To avoid this only they have introduced these Google authenticator apps on android market. When you are asked for code you will able to get one from this apps.

This apps is very useful at the initial level to prevent illegal mails sent /read from our mail.

Here are some indications if an email is an attack:

• Be suspicious of any email that requires "immediate action" or creates a sense of urgency. This is a common technique used by criminals to rush people into making a mistake.

• Be suspicious of emails addressed to "Dear Customer" or some other generic salutation. If it is your bank they will know your name.

• Be suspicious of grammar or spelling mistakes; most businesses proofread their messages carefully before sending them.

• Do not click on links. Instead, copy the URL from the email and paste it into your browser. Even better is to simply type the destination name into your browser.

• However your mouse over the link. This will show you the true destination where you would go if you actually clicked on it. If the true destination of the link is different than what is shown in the email, this may be an indication of fraud.

• Be suspicious of attachments and only open those that you were expecting.

• Just because you got an email from your friend does not mean they sent it. Your friend's computer may have been infected or their account may have been compromised, and malware is sending the email to all of your friend's contacts. If you get a suspicious email from a trusted friend or colleague, call them to confirm that they sent it. Always use a telephone number that you already know or can independently verify, not one that was included in the message. If after reading an email you think it is a phishing attack or scam, simply delete the email. Ultimately, using email safely is all about common sense. If something seems suspicious or too good to be true, it is most likely an attack. Simply delete the email.

Computer Related Crimes Covered under IPC and Special Laws:

1. Email spoofing Sec 463 IPC
2. Web-Jacking Sec. 383 IPC
3. E-Mail Abuse Sec.500 IPC

A Growing Problem in Phishing

The phish attack volume increased 33% in April to 36,557 attacks, continuing the growth trend from March. Phish attacks had been in general decline from August 2009 to February 2010, but now look set to return to the seasonal growth trend that has historically peaked in late Summer/early Fall . In August 2009, for example, the high point of fast-flux phish attacks Produced 60,678 incidents. As shown in Figure. 1, the monthly attacks from April 2009 to April 2010 averaged 45,605. Phish attack volume has not returned to the level seen in April 2009, but note that this chart does not include branded malware attacks, which cybercriminals are likely to have launched during periods of lower phish volumes.

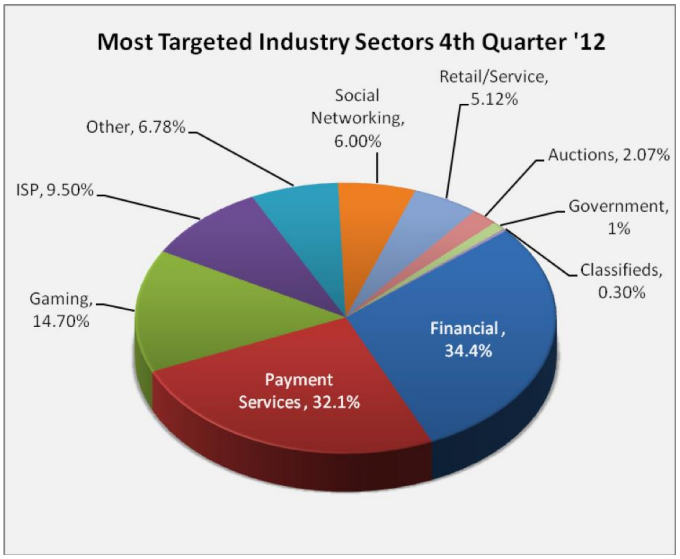
Table 1: Phishing statistics for year 2006

YEAR-2006	Valid Phishes	Invalid Phishes
Oct	3678	7061
Nov	10044	18130
Dec	11309	20352

Table 2: Phishing statistics for year 2007

YEAR-2007	Valid Phishes	Invalid Phishes
Jan	18077	30509
Feb	19947	25647
Mar	10515	11620

Phishers Shift to Target Online Game Players



Phishing attacks against online game players saw a massive increase, from 2.7 percent of all phishing attacks in Q3 to 14.7 percent in Q4. Financial services continued to be the most-targeted industry sector in the fourth quarter of 2012 with payment services close behind.

4th Quarter '12 Phishing Activity Trends Summary

● During Q4, about 30 percent of personal computers worldwide were infected with malware. More than 57 percent of PCs in China may have been infected, while PCs in European nations were infected least often.

● Except for October 2012, the number of phishing sites declined every month from April 2012 through December 2012.

April 2012 saw 63,253 unique phishing sites detected, falling to 45,628 in December 2012.

● The APWG received reports of 28,195 unique phishing sites in December. December's total was 31 percent lower than the high of 40,621 reports in August 2009.

● Use of crime ware dipped slightly in this quarter from the previous, as did the use of data stealing malware. The use of other malware has increased by a statistically significant amount from the previous quarter.

V. CONCLUSION

As communication mode in this IT era is EMAIL. All kinds of communication made must be ensured. To address this problem we have given an awareness to let the common people about the Phishing issues and its consequences. Many researchers have provided various solutions to find, prevent and avoid phishing. We are on the process of developing new method which overcomes all the demerits of the existing phishing solutions. In addition to providing new solutions it is very important to give the awareness of this issue. In this paper we have given awareness with a demonstration. For security reason we have not given any phishing mail in detail but will demonstrate on the day of presentation. There we can show you the mails having come from Barack Obama, George bush and from anyone we want to receive. These are to name few only. Actually these people have been taken only for the education purpose. Also we will show you some methods to identify their originality. Soon we will implement our own prototype to distinguish phishing mails using classification and clustering technique before it reaches the inbox using their prototype. Our research presently focuses on developing a search engine that would find the phishing link.

VI. FUTURE ENHANCEMENT

In future as research moves further will show the world that all kinds of phishing mails are eradicated. In email server itself these kinds of mails are ignored and corresponding actions will be taken by corresponding officials.

REFERENCES

[1] Guidelines on Electronic Mail Security Recommendations of the National Institute of Standards and Technology Special Publication 800-45 Version 2.

[2] M. Delany, "Domain-based email authentication using DNS , May 2007. http://ietf.org.html

[3] A countermeasure to email sender address spoofing by Toshiyuki Tanaka, Akihiro Sakai, Yoshiaki Hori, Kouichi.

[4] Techniques and tools for forensic Investigation of e-mail International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.6, November 2011

[5] Cyber crime – prevention & detection by v.shiva kumar, Asst.director A.P.Police Academy.

[6] http://www.antiphishing.org.

[7] New Filtering Approaches for Phishing Email by Mrs.P.Lalitha and , Sumalatha.Udutha International Journal of Computer Trends and Technology (IJCTT) – volume 4 Issue 6–June 2013

[8] C. E. Drake, J. J. Oliver, and E. J. Koontz, "Anatomy of Phishing Email",MailFrontier Inc.,CA,USA.

[9] M.Chandrashekaran, K.Narayana, S.Upadhyaya, "Phishing Email Detection Based on Structural Properties",Symposium on Information Assurance: Intrusion Detection and Prevention, New York, 2006

[10] Phishing Secrets: History, Effects, and Countermeasures Antonio San Martino and Xavier Perramon International Journal of Network Security, Vol.11, No.3, PP.163–171, Nov. 2010

[11] Phishing: An Analysis of a Growing Problem SANS Institute InfoSec Reading Room January 2007

AUTHORS

First Author – Gori Mohamed J., B.Tech(IT)., M.Tech (CSE)., LMISTE., MCSTA., Assistant Professor, Department of Information Technology, Mohamed Sathak A.J College of Engineering, Chennai., Email:drgorimohamed@gmail.com
Second Author – Mohammed Mohideen.M., B.Tech (IT)., M.Tech (IT)., CCNA Assistant Professor, Department of Information Technology, Mohamed Sathak A.J College of Engineering, Chennai., Email:farukmmm@gmail.com
Third Author – Mrs.Shahira Banu N B.Tech(IT)., Email:nskbanu@gmail.com