A REVIEW PAPER ON PHISHING – A GROWING SCAM

[1]Md Rashid Hussain, [2]Garima Srivastava

[1]Associate Professor, ABESIT Ghaziabad, (India)

[2]B.Tech Scholar, ABESIT Ghaziabad, (India)

ABSTRACT

Phishing is a form of online identity theft in which cyber criminals tricks the victims to steal their sensitive information such as online banking passwords and credit card information from users. Spoofed emails that claim to be from legitimate source are crafted in a way to lead victims to reveal their personal, financial data by misdirecting them to the counterfeit website. It is affecting all the major sectors of industry day by day with a lot of misuse of user credentials.

In this paper we have studied phishing in detail and reviewed some of the existing anti-phishing techniques along with their advantages and disadvantages.

Keywords: Phishing Attacks, Anti-Phishing, Security, User-Protection.

I INTRODUCTION

Phishing is also known as "brand-spoofing". It is pronounced as fishing. The word has its origin from two words "Password harvesting" or "fishing for passwords". Phishing mostly uses spoofed e-mail messages that seem to come from legitimate source. Trojans, malware and other malicious software are also used for phishing attacks. A phisher may lure a victim into giving his/her Social Security Number, full name, & address, which can then be used to apply for a credit card on the victim's behalf [1].

Online services such as online shopping or online banking have brought us a great convenience yet at the same time new threats. One of these new threats is phishing whereby spoofed emails or instant messages purporting to be from trustworthy sources are used to lure recipients to click the contained URLs that lead to counterfeit websites to trick them into divulging sensitive information such as usernames and passwords, credit card information, social security numbers, etc.

Most methods of phishing use some form of technical deception designed to make a link in an e-mail (and the spoofed website it leads to) appear to belong to the spoofed organization. Misspelled URLs or the use of sub domains are common tricks used by phishers[17]. Example: www.gmail.com – original link, www.gmai1.com –

Fake link. Here are a few phrases that a phishing page may contain verify your account, businesses should not ask you to send passwords, login names, social security numbers, or other personal information through e-mail[17].

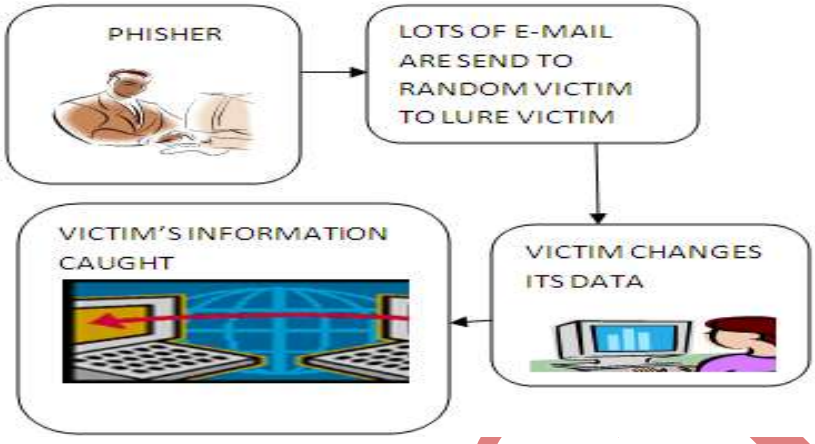

Fig 1: Process of Phishing

There are thousands of fake phishing websites established online every day, luring a number of customers. According to a phishing activity trend report published by Anti-phishing working group on 23 dec 2011, a lot of phishing attacks were done in first half of year 2011 as can be seen from fig 2. The number of unique phishing reports submitted to APWG in H1, 2011 reached a high of 26,402 in March, dropping to the half year low of 20,908 in April[2].

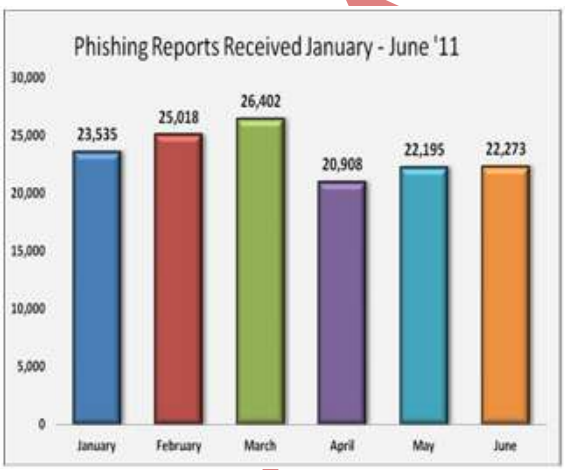

Fig 2: Phishing Activity Trend Report [2] **Fig 3: Industry Sector Area Wise Affect Of Phishing [2]**

The report also depicted that Financial Services continued to be the most targeted industry sector in the first half of 2011[2] as can be seen from figure 3.

II TYPES OF PHISHING ATTACKS

2.1 Deceptive Phishing

The term "phishing" originally referred to account theft using instant messaging but the most common broadcast method today is a deceptive email message. Messages about the need to verify account information, system failure requiring users to re-enter their information, fictitious account charges, undesirable account changes, new free services requiring quick action, and many other scams are broadcast to a wide group of recipients with the hope that the unwary will respond by clicking a link to or signing onto a bogus site where their confidential information can be collected.

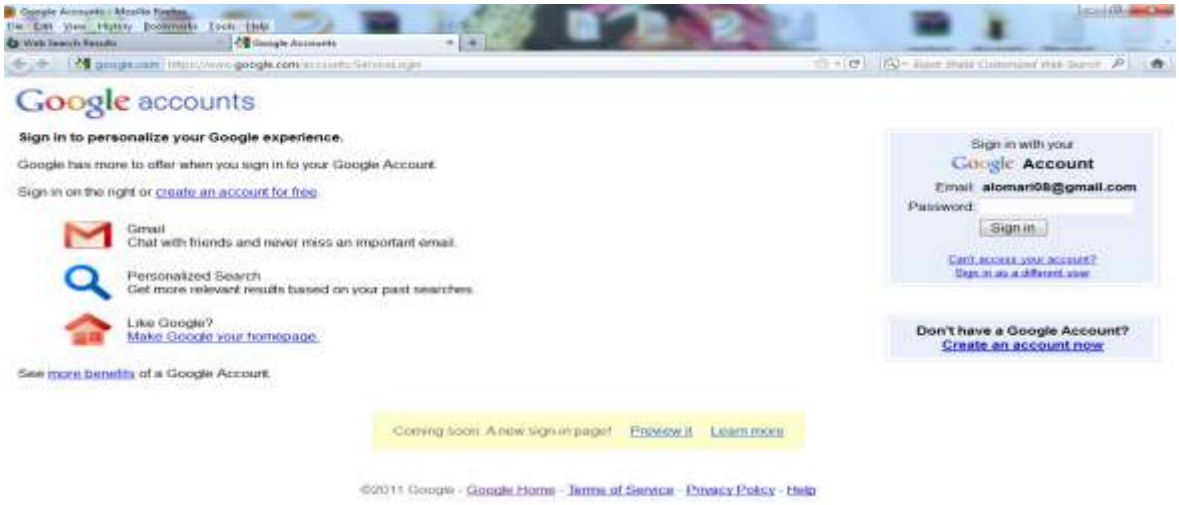

Fig 4: Phishing Page

2.2 Malware-Based Phishing

Refers to scams that involve running malicious software on users' PCs. Malware can be introduced as an email attachment, as a downloadable file from a web site, or by exploiting known security vulnerabilities--a particular issue for small and medium businesses (SMBs) who are not always able to keep their software applications up to date.

2.3 Keyloggers And Screenloggers

Are particular varieties of malware that track keyboard input and send relevant information to the hacker via the Internet. They can embed themselves into users' browsers as small utility programs known as helper objects that run automatically when the browser is started as well as into system files as device drivers or screen monitors.

2.4 Web Trojans

Pop up invisibly when users are attempting to log in. They collect the user's credentials locally and transmit them to the phisher.

2.5 Hosts File Poisoning

When a user types a URL to visit a website it must first be translated into an IP address before it's transmitted over the Internet. The majority of SMB users' PCs running a Microsoft Windows operating system first look up these "host names" in their "hosts" file before undertaking a Domain Name System (DNS) lookup. By "poisoning" the hosts file, hackers have a bogus address transmitted ,taking the user unwittingly to a fake "look alike" website where their information can be stolen.

2.6 Content-Injection Phishing

Describes the situation where hackers replace part of the content of a legitimate site with false content designed to mislead or misdirect the user into giving up their confidential information to the hacker. For example, hackers may insert malicious code to log user's credentials or an overlay which can secretly collect information and deliver it to the hacker's phishing server.

2.7 Session Hijacking

Describes an attack where users' activities are monitored until they sign in to a target account or transaction and establish their bona fide credentials. At that point the malicious software takes over and can undertake unauthorized actions, such as transferring funds, without the user's knowledge.

2.8 System Reconfiguration Attacks

Modify settings on a user's PC for malicious purposes. For example: URLs in a favorites file might be modified to direct users to look alike websites. For example: a bank website URL may be changed from "bankofabc.com" to "bancofabc.com".

2.9 Data Theft

Unsecured PCs often contain subsets of sensitive information stored elsewhere on secured servers. Certainly PCs are used to access such servers and can be more easily compromised. Data theft is a widely used approach to business espionage. By stealing confidential communications, design documents, legal opinions,employee related records, etc., thieves profit from selling to those who may want to embarrass or cause economic damage or to competitors.

2.10 DNS-Based Phishing ("Pharming")

Pharming is the term given to hosts file modification or Domain Name System (DNS)-based phishing. With a pharming scheme, hackers tamper with a company's hosts files or domain name system so that requests for URLs or name service return a bogus address and subsequent communications are directed to a fake site. The result: users are unaware that the website where they are entering confidential information is controlled by hackers and is probably not even in the same country as the legitimate website.

Fig 5 : Screenshot Of The Spoofed Hunting Online Banking Page. The Login Screen Closely Resembles The Legitimate Login Page [11].

2.11 Man-in-the-Middle Phishing

Is harder to detect than many other forms of phishing. In these attacks hackers position themselves between the user and the legitimate website or system. They record the information being entered but continue to pass it on so that users' transactions are not affected. Later they can sell or use the information or credentials collected when the user is not active on the system.

2.12 Search Engine Phishing

Occurs when phishers create websites with attractive (often too attractive) sounding offers and have them indexed legitimately with search engines. Users find the sites in the normal course of searching for products or services and are fooled into giving up their information. For example, scammers have set up false banking sites offering lower credit costs or better interest rates than other banks. Victims who use these sites to save or make more from interest charges are encouraged to transfer existing accounts and deceived into giving up their details.

III WHAT CAN BE DONE?

Many experts contend that phishing is less of a "technology problem" and more of a "user problem"; that the responsibility ultimately lies with the user being aware of where they are browsing, what information they are giving over the Internet, and to whom they are giving the information. Others are more concerned that the sophisticated techniques used by phishers are becoming more difficult to detect, even for experienced computer users; casual or less technical users are much less likely to be able to discern a legitimate e-mail, web address, or web site from a fake one. Social engineering ploys can be very effective in these situations.

3.1 Education

Education is a vital component of the phishing battle—as well as other online scams. The Federal Trade Commission suggests some things to remember:

- Don't reply to e-mails asking to confirm account information. Call or logon to the company's web site to confirm that the e-mail is legitimate.
- Don't e-mail personal information. When submitting information via a web site, make sure the security lock is displayed in the browser.
- Review credit card and bank account statements for suspicious activity
- Report suspicious activity.

3.2 Technology

Unfortunately, phishing usually involves social engineering tricks, and, thus, even the best defenses that a company might have in place to combat outside threats are sometimes useless against these types of attacks. Although education is likely the best defense against phishing scams, there are technologies that make phishing harder to accomplish. When implemented with a defense-in-depth approach, software and hardware can be installed to slow the phishers down.

IV ANTI-PHISHING

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. Most browsers such as Mozilla or the Internet Explorer have integrated functionality that allows form contents to be stored and automatically inserted if the user desires. This content is protected by a *master password*. Once this password is entered by the user, a login form that has previously been saved, for example, will automatically be filled by the browser whenever it is accessed. Antiphish takes this common functionality one step further and tracks *where* this information is sent.

As we are using the Mozilla firefox as browser it will give the warning as suspected web forgery , this is the first level of security that mozilla gives, but it is not enough to trace the phishing sites so there are many methods already exist for the detection of Phishing Attack.

4.1 Anti-Phishing Techniques

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 general anti-phishing techniques can be classified into following four categories [1].

Techniques	Advantages	Disadvantages
Attribute based anti-phishing techniques	It is able to detect more phished sites than other approaches as attribute based anti-phishing consider a lot of checks. It can detect known as well as unknown attacks.	This could result in slow response time as multiple checks perform to authenticate site.
Genetic Algorithm Based Anti Phishing Techniques	Before the user reads the mail it provides the feature of malicious status notification. It also provides malicious web link detection in addition of phishing detection.	Single rule for phishing detection like in case of url is far from enough, so we need multiple rule set for only one type of url based phishing detection. Likewise for other parameter we need to write other rule this leads to more complex algorithm.
An Identity Based Anti Phishing Techniques	It provide mutual authentication for server as well as client side. Using this techniques user does not to reveal his credential password in whole session except first time when the session is initialized.	In identity based anti-phishing if a hacker gain access to the client computer and disable the browser plug-in then method will be compromise against phishing detection .
Content Based Anti-Phishing Approach	Generally GoldPhish does not result in false positive and provides zero day phishing .	GoldPhish delays the rendering of a webpage. It is also vulnerable to attacks on Google's PageRank algorithm and Google's search service .

V CONCLUSION AND FUTURE WORK

Phishing emails and web site attacks have provided a faceless opportunity for fraudsters to reach millions of potential victims, with little cost outlay, in the hope of victims supplying their personal and financially sensitive information. This information is then used to hijack accounts and duplicate the victim's identity through the fastest growing crime in the world, Identity Theft. It is apparent that fraudsters perpetrating phishing scams are becoming more technologically efficient, utilizing smarter deception methods to create and implement their phishing scams.

In the above study we can conclude that most of the anti-phishing techniques focus on contents of web age, URL and email. Character based anti-phishing approach may result in false positive but content based approach never results in false positive. Attribute based approach consider almost all major areas vulnerable to phishing so it can be best anti-phishing approach that can detect known as well as unknown phishing attack. Identity based anti-phishing approach may fails if phisher gets physical access to client's computer.

Consumers need to become more educated concerning online threats and vulnerabilities. Companies need to make sure that online fraud and scams are reported and that their customers are kept apprised of scams that may affect them. The security community needs to work to find new ways to make e-mail and online commerce as bullet-proof as it can possibly be. This is a monumental task, but there are a great number of extremely talented people with many brilliant ideas out there. If something is not done, the way we do business online will change, and almost certainly not for the better.

As a future work on phishing we can do more work on server side security. In the server side security policy we use dual level of authentication for user by which only authentic user can get the access of his account, and to educate the user about this policy will results in avoiding user to give his sensitive information to phished web site.

REFERENCES

[1]. Hicham Tout, William Hafner "Phishpin: An identity-based anti-phishing approach" in proceedings of international conference on computational science and engineering, Vancouver, BC, pages 347-352, 2009 .

[2]. Phishing activity trend report 1st half /2011,http://www.antiphishing.org.

[3]. Mather Aburrous, M.A. Hossain, KeshavDahal, FadiThabtah "Prediction phishing websites using classification mining techniques with experimental case studies" in proceedings of Seventh International Conference on Information Technology, Las Vegas, NV, pages 176-181, 2010.

[4]. Michael Atighetchi, Partha Pal "Attribute-based prevention of phishing attacks" Eighth IEEE international symposium on network computing and application, 2009.

[5]. V.Shreeram, M.Suban, P.Shanthi, K.Manjula "Anti-phishing detection of phishing attacks using genetic algorithm" in proceedings of Communication control and computing technology(ICCCCT),IEEE international conference, Ramanathapuram , pages 447-450, 2010.

[6]. Juan Chen, ChuanxiongGuo-"Online Detection and Prevention of Phishing Attacks (Invited Paper)"in proceedings of Communicational and networking in china, first international conference, Beizing, pages 1-7, 2007.

[7]. Matthew Dunlop, Stephen Groat, and David Shelly" GoldPhish: Using Images for Content-Based Phishing Analysis", in proceedings of internet monitoring and protection(ICIMP),fifth international conference, Barcelona, Pages 123-128, 2010.

[8]. MiteshBargadiya, Vijay Chaudhary, Mohd. Ilyas Khan, BhupendraVerma "the web identity prevention: factors to considers in the anti-phishing design" internation journal of engineering science and technology vol. 2(7), 2010.

[9]. Huajun Huang Junshan Tan Lingxi Liu "Countermeasure Techniques for Deceptive Phishing Attack" International Conference on New Trends in Information and Service Science. NISS '09.June-2009.

[10].http://www.symantec.com/business/resources/articles/article.jsp?aid=phishers_targeting_the_government.

[11].TheAntiphishing Working Group. Home Page. http://www.anti-phishing.org, 2004.

[12]. A White Paper presented by FraudWatch International, the Internet's high profile Fraud Prevention Web Site. http://www.fraudwatchinternational.com, *Accessed: March 10, 2012*

[13]. The Anti-Phishing Working Group. "What is Phishing?" URL:http://www.antiphishing.org/(March 2004)