ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 9, September 2017

Review of Phishing attacks and Anti Phishing Tools

Deepashree K. Mehendale, Reshma S. Masurekar, Neeta Takawale, Shibani Kulkarni

Assistant Professor, Department of Computer Science, Dr. D. Y. Patil A.C.S College, Pimpri, Pune, India

Assistant Professor, Department of Computer Science, Dr. D. Y. Patil A.C.S College, Pimpri, Pune, India

Assistant Professor, Department of Computer Science, Dr. D. Y. Patil A.C.S College, Pimpri, Pune, India

Assistant Professor, Department of Computer Science, Dr. D. Y. Patil A.C.S College, Pimpri, Pune, India

ABSTRACT: The use of internet has grown tremendously in our lives. Almost all services are offered online.Customers of banks enormously use the E-banking services. E-banking services suffer from many attacks one of the most common being Phishing. It is an attempt to obtain sensitive information such as username, password, and credit card details by disguising as a trustworthy entity. Malicious applications that steal financial account information have increased dramatically over the last few years, probably resulting in a direct loss of money to affected victims. While the primary target continues to be online financial systems, the methods used to gather the sensitive information vary. Attacks spread from simply spamming e-mails with links to fake web sites, which is known as phishing, to Trojans that monitor attempts to log on to online account web services and then begin recording the pressed key strokes, take screen shots, or even redirect the whole network traffic to a malicious site. Thus security is of main concern to both user and bank.This research paper focuses on phishing attacks and anti - phishing tools.

KEYWORDS: : E-banking, Phishing, Anti-Phishing, detection, prevention

I. INTRODUCTION

E-banking

Internet has not only brought the world together but has also made many reforms in it. The main reform is E-Commerce. E-commerce is the facilitation of trading in products or services using computer networks, such as the Internet.This change has attracted more cyber attackers.

E-banking means providing banking products and services directly to customers through electronic, interactive communication channels.E-banking provides extensive benefits to customers in terms of ease and cost of transactions through Internet. E-banking is a result of growing expectations of bank's customers. This system involves direct interface with the customers. The customers do not have to visit the bank's premises. E-banking offers the convenience of conducting most of banking transactions at a time that are suitable to customer. The rapid advancement in electronic distribution channels has produced tremendous changes in the financial industry in recent years, with an increasing rate of change in technology, competition among players and consumer needs. E-banking has become a part of life among many customers.

Now a day's E-banking means 24X7 services to customers. Any user with a personal computer and a browser get connected to his bank's website to perform any of the virtual banking functions. In E-banking system the bank has a centralized database that is web-enabled. All the services that the bank has permitted on the internet are displayed in menu.

Obtaining safe and secure environment of computer technology is the most important concern for all financial service organizations. Security of online banking transactions is one of the most important challenges to the banking sector. Billions of financial data transactions are conducted online every day, and bank cyber-crimes take place every day by skilled criminal hackers through manipulating the bank's online information system. Threats can come from inside or outside the system, which threatens customers' information and transactions, where bankadministrators must

DOI: 10.15680/IJIRCCE.2017. 0509049

ensure that banks have the appropriate practices in place to guarantee the confidentiality of customers' data, as well as the integrity of the e-banking system and the transactions conducted. The responsibility of secure online banking is not only on the banks but also on the customers, because the customers, to operate the online banking, have to have a certain level of knowledge and technical competence and awareness.

E-banking services suffer from various attacks one of the important being Phishing. Phishing is a new word produced from 'fishing', it refers to the act that the attacker attracts users to visit a fake Web site by sending them fake e-mails , and secretively obtains victim's personal information such as user name, password, and national security ID, etc. This information then can be used for future target advertisements or even identity theft attacks (e.g., transfer money from victims' bank account). The frequently used attack method is to send e-mails to potential victims, which seemed to be sent by banks, online organizations, or ISPs. In these e-mails, they will make up some causes, e.g. the password of your credit card had been miss-entered for many times, or they are providing upgrading services, to allure you visit their Web site to conform or modify your account number and password through the hyperlink provided in the e-mail. Phishers can even breach the security of a bank after they access user's financial information; then, they conduct a wide range of illegal activities. Online banking users are more vulnerable to e-banking frauds, when they conduct any financial activity through the web, such as money transfer.

Phishing Attacks on E-banking

Amongst most of the attacks, Phishing has become common attack for E-banking.Phishing is defined as "a criminal activity using social engineering techniques that enables phishers to attempt fraudulently acquire sensitive information, such as passwords, credit card details, by masquerading as a trustworthy person or business in an electronic communication. There are different type of phishing attacks classified as follows:-

1.*Deceptive phishing:* It refers to an attack where fraudsters pretend to be a legitimate company and attempt to steal personal information of users.For example, PayPal scammersmight send out an attack email that instructs them to click on a link in order to rectify a discrepancy with their account. In actuality, the link leads to a fake PayPal login page that collects a user's login credentials and delivers them to the attackers. The success of a deceptive phish depends on how closely the attack email resembles a legitimate company's official correspondence. As a result, users should inspect all URLs carefully to see if they redirect to an unknown website. They should also look out for generic salutations, grammar mistakes, and spelling errors scattered throughout the email.

2. *Spear Phishing*: For instance, in spear phishing scams, fraudsters customize their attack emails with the target's name, position, company, work phone number and other information in an attempt to trick the recipient into believing that they have a connection with the sender.The goal is the same as deceptive phishing, lure the victim into clicking on a malicious URL or email attachment, so that they will hand over their personal data. Spear-phishing is especially commonplace on social media sites like LinkedIn, where attackers can use multiple sources of information to craft a targeted attack email.

3. *Dropbox Phishing:* As millions of people use Dropbox every day to back up, access and share their files. Therefore, the attackers would try to capitalize on the platform's popularity by targeting users with phishing emails. One attack campaign, for example, tried to lure users into entering their login credentials on a fake Dropbox sign-in page hosted on Dropbox itself.

4. *Google Docs Phishing:* Fraudsters could choose to target Google Drive similar to the way they might prey upon Dropbox users. Specifically, as Google Drive supports documents, spreadsheets, presentations, photos and even entire websites, phishers can misuse the service to create a web page that mimics the Google account log-in screen and harvests user credentials.

5. *Malware-based Phishing:*Malware-based phishing refers to software programs that hackers install on customers' computers. This kind of phishing attack can happen when customers or bank employees visit an unauthorized website or download some infected software programs into their computers. The Phishing attackers use many techniques, such

as keyloggers to gain credential information of bank user. Keyloggers are programs that install themselves onto bank users' computers when customers visit any websites with a keylogger or download a piece of software with a keylogger. Hackers install these types of malware-based phishing software on users' computers without their knowledge or permission. Therefore, phishing attackers find this type of malicious software easy to use for fraudulent activities, since the victims are often unaware that such software even exist on their computers.

6.*DNS-Based Phishing:*DNS-based phishing, is another type of phishing attack in which an online deceptive agent gains control of the bank users' data. During the pharming technique, attackers are tampering with the bank's host files or domain name system (DNS). This form of attack redirects users to a fake website when they attempt to type in the domain name of their bank's web address. The hackers can perform the pharming attack in two ways. They can install a virus on the user's computer or tamper with the bank's web domain. Regardless of the method, the result is that the users type the correct URLs of their financial institutions on their browsers, but then they are directed to fraudulent but legitimate-looking websites. Therefore, users remain unaware that the websites into which they are typing their credentials are under the hackers' control.

II. LITERATURE REVIEW

The research paper [1] reveals that online banking involves many kinds of risks. Phishing attacks can cause damage to both banks and users. Since phishing hackers use several sophisticated methods, ranging from deceptive attacks to DNS attacks, banks must update their security measures regularly. Banks must use, two-factor authentication, along with other protection software programs. Educating customer is one of the top priority which should be considered. There are some signs to identify an attack sent by email. In phishing attack, attacker may duplicate an image of a real company, copy the name of a company or use the actual name of an employee which is used to assure you that you are receiving email from the company or bank. Also, bank users must check the source of information from incoming mails so that they could make sure whether it is a phishing attack. Moreover, users should know that banks never send their users an email request asking for usernames and passwords.

In research paper[2] an anti-phishing algorithm, Link-Guard, is discussed. This algorithm is characteristic based it can not only detect known attacks, but also is effective to the unknown ones. The experiment showed that Link Guard is light-weighted and can detect up to 96% unknown phishing attacks in real-time. Link Guard is not only useful for detecting phishing attacks, but also can shield users from malicious or unsolicited links in Web pages and Instant messages. When a user visits a Web site, the anti-phishing tool searches the address of that site in a blacklist stored in the database. If the visited site is on the list, the anti-phishing tool then warns the users. This category of tools uses certain rules in their software, and checks the security of a Web site according to these rules. Examples of this type of tools include Spoof Guard developed by Stanford, Trust Watch of the Geo Trust, etc. Spoof Guard checks the domain name, URL (includes the port number) of Web site, it also checks whether the browser is directed to the current URL via the links in the contents of e-mails. If it finds that the domain name of the visited Web site is similar to a well-known domain name, or if they are not using the standard port, Spoof Guard will warn the users. In Trust Watch, the security of a Web site is determined by whether it has been reviewed by an independent trusted third party organization. Both Spoof Guard and Trust Watch provide a toolbar in the browsers to notify their users whether the Web site is verified and trusted.

In research paper [3] titled, "A survey on phishing detection and prevention technique" a new model for detection and prevention of phishing is introduced. This model crosschecks the entered URL with Phish tank database, this database contains user feedbacks of the URL's. Thus the affected URL's can be detected.

In research paper [4] a higher level security model is proposed. In this system an email is send to the customer on the given mail address.The customer has to download the image which is in .png format and then give the path to the banks website for authentication purpose. The image is less than 2 ^ 64 bits in length. The last 16 bits of the image will be used to pass the security code for verification. This code is generated by using MD5 algorithm. Thus two factor authentication used in this model helps to provide higher level of security, one by login id and password authorization and other done with the help of email id given by the customer.

The research [5] critically analyses and discusses the effects of cyber threats whendealing with online banking services. It is concluded that by the research that there is a need to increase customer's awareness about available

DOI: 10.15680/IJIRCCE.2017. 0509049

cybercrimes when dealing with online banking and sensitive financial data. The research paper is beneficial for those financial organizations looking to develop awareness among individuals from security perspective and facilitate them with the recommendations that must be considered when dealing with online threats. The scope of the research could be measured through the scope of security and its implementation in online banking sectors. The novelty of this research is based on the comprehensive approach adopted to understand the seriousness of online cyber threats available to online banking industry. The research is unique due to the nature that it detailswith the effects of cybercrimes on customer's behaviour when dealing with online banking services through different digital devices such as personal computers, laptops, iPads and mobiles.

Research paper [6] proposes different anti-phishing approaches to avoid the stealing of personal information online and also shows the pros and cons of these approaches. The various anti-phishing approaches discussed are Content Base Approach, Black listing Heuristic based approach, Further the pros and cons of these approaches are discussed in detail.

In research paper [7] Fuzzy Data Mining Techniques are used which can be an effective tool in assessing and identifying e-banking phishing websites since it offers a more natural way of dealing with quality factors rather than exact values. In this paper, the researcher has presented a novel approach to overcome thefuzziness‟ in the e-banking phishing website assessment and propose an intelligent resilient and effective model for detecting e-banking phishing websites. The proposed model is based on Fuzzy logic combined with Data Mining algorithms to characterize the e-banking phishing website factors and to investigate its techniques by classifying there phishing types and defining six e-banking phishing website attack criteria's with a layer structure. A Case study was applied to illustrate and simulate the phishing process. Our experimental results showed the significanceand importance of the e-banking phishing website criteria (URL & Domain Identity) represented by layer one, and the variety influence of the phishing characteristic layers on the final e-banking phishing website rate.

III. ANTI-PHISHING TECHNIQUES

.

Anti-Phishing techniques focus on the methods of detecting and preventing phishing attacks. Some anti-phishing techniques are summarized as follows:-

1. *Content Filtering:* This technique is also known as Information filtering in which Content/email are filtered as it enters in the victim's mail box using machine learning methods. Content filtering usually works by specifying character strings that, if matched, indicate undesirable content that is to be screened out.

2. *Black Listing:* Blacklist is collection of known phishing Web sites/addresses published by trusted entities like Google's and Microsoft's black list. It requires both a client & a server component. The client component is implemented as either an email or browser plug-in that interacts with a server component, which in this case is a public Web site that provides a list of known phishing.

3. *Symptom-Based Prevention:* Symptom-based prevention analyses the content of each Web page the user visits and generates phishing alerts according to the type and number of symptoms detected[1]. Domain Binding- It is an client's browser based techniques where sensitive information (eg. name, password) is bind to a particular domains. It warns the user when he visits a domain to which user credential is not bind.

IV. ANTI-PHISHING TOOLS

Anti-phishing software consists of computer programs that attempt to identify phishing content contained in websites and e-mail or block users from being tricked. It is often integrated with web browsers and email clients as a toolbar that displays the real domain name for the website the viewer is visiting, in an attempt to prevent fraudulent websites from masquerading as other legitimate web sites.Most popular web browsers comes with built-in anti-phishing and anti-malware protection services, but almost none of the alternate web browsers have such protections.

1. *Anti-Phishing Database:* Mail-Secure maintain a data base which is updated on a daily basis. This database features millions of known Phishing URLs and domain names. If one of the listed URLs appears in a mail, it is blocked.

2. *SURBL:*An RBL which is designed to block or tag Phishing attempts based on URI's (usually their domain names) scattered in the body of the message. In this case, the RBL is not intended to block the source of the spam message. Instead, SURBL is used to block spam based on its message content. Even if a spammer uses new domains, they may point to the old, blocked IPs and will therefore be blocked, right from the first spam message received.

3. *Commtouch RPD:* Commtouch's Recurrent Pattern Detection (RPD™) is based on the fundamental characteristic of Phishing, spam and email-born Malware - its mass distribution over the Internet. Sniffers located worldwide, lookout for real traffic in over 60 million operational mailboxes. They then extract patterns to detect recurring patterns and examine the number of sources to determine if they are Trojan-based outbreaks. Commtouch RPD™ differentiates between bulk mail (which can be a mailing list), and confirmed spam.

4. *Heuristic Fraud detection sets of rules:* Mail-Secure uses Heuristic rules in order to detect possible new Phishing attempts. Mail-SeCure has over 2,500 sets of rules to detect characteristics of Phishing. The heuristic engine uses a score-based system to identify Phishing.

5. *Zombie detection:* Most Phishers use zombie computers to distribute their mail. Zombie computers are computers that were involuntarily hacked (whether by Trojan horses or by direct hacking) and used for mail distribution. Mail-SeCure has a unique Zombie Detection System – ZDS. It identifies zombies and automatically blocks them at the session level (similar to RBL). PineApp has a central ZDS, RBL-like server, which dynamically blocks identified IPs. Since a zombie computer owner can change his IP, ZDS automatically adds or removes IP addresses from blacklists.

6. *IP Reputation:*A powerful additional layer used to block Zombies at the SMTP session level. The IP Reputation mechanism is based on sniffers located at various points of the world, monitoring traffic of hundreds of millions of email messages daily. IP Reputation centredynamically classifies IPs, according to a profile built from parameters such as: volume, percentage of spam & viruses and elevations. When an SMTP session is established, Mail-SeCure queries the IP Reputation system (or uses local cache) and performs various actions according to the IP classification, such as: permanently reject the mail, respond with a temporary error to be able to re-evaluate the IP on the retry time, activate greylisting, activate Rate limit, etc.

7. *Browser Integrated Tools:* A browser-integrated tool usually relies on a blacklist, which contains the URLs of malicious sites, to determine whether a URL corresponds to a phishing page or not. In Microsoft Internet Explorer 7, for example, the address bar turns red when a malicious page is loaded. The effectiveness of a blacklist is strongly influenced by its coverage, credibility, and update frequency. At present, the most well-known blacklists are those maintained by Google and Microsoft, which are used by the most popular browsers, Mozilla Firefox and Microsoft Internet Explorer, respectively.

V. CONCLUSION

Phishing is a serious problem related to E-banking that results in threat and risk. Based on the discussion above, this research recommends the followings:-

1. There should be a system to monitor the act of fraudsters.
2. Customer awareness of Phishing attacks should be done properly.
3. To ensure high level of security, layers of authentication should be added to the process of E-banking transactions.
4. The confidence level of the online banking users must be developed by educating them about the tools andtechniques used when dealing with online banking services.

5. There should be awareness of available online threats among the customers who use E-banking.
6. Online banking users should use strong passwords and different user name combinations for different sites andaccounts.

REFERENCES

1. Alhuseen O. Alsayed, Anwar L. Bilgrami, E-Banking Security: Internet Hacking, Phishing Attacks, Analysis and Prevention of Fraudulent Activities, International Journal of Emerging Technology and Advanced Engineering (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 7, Issue 1, January 2017)
2. E.Konda Reddy, Dr. Rajamani and Dr. M. V. Vijaya Saradhi, Detection of E-banking Phishing Websites, International Journal of Modern Engineering Research (IJMER) Vol.2, Issue.1.
3. Archit Shukla , LalitGehlod, A survey on phishing detection and prevention technique,
   International Journal Of Engineering And Computer Science ISSN: 2319-7242 Volume 3 Issue 5 may, 2014 Page No. 6255-6259.
4. Gunjan Pathak, RiddhiNishar, Harnish Shah, PoojaGajera, Study of Anti Phishing on Internet Banking, International Journal of Innovative and Emerging Research in Engineering.
5. Liaqat Ali, Faisal Ali, PriyankaSurendran, Bindhya Thomas
   The Effects of Cyber Threats on Customer's Behaviour in e-Banking Services,
   International Journal of e-Education, e-Business, e-Management and e-Learning.
6. KanchanMeena, TusharKanti A Review of Exposure and Avoidance Techniques for Phishing Attacks.International Journal of Computer Applications (0975 – 8887) Volume 107 – No 5, December 2014
7. Maher Aburrous, M. A. Hossain, FadiThabatah, KeshavDahal , Intelligent Detection System for e-banking Phishing websites using Fuzzy Data Mining