Available online at www.elixirpublishers.com (Elixir International Journal)

Computer Science and Engineering

Elixir Comp. Sci. & Engg. 79 (2015) 30114-30117

ISSN: 2229-712X

A systematic approach and model generation for preventing phishing attacks

Jigar Patel
Department of MCA, Kalol Institute of Management, Kalol.

ARTICLE INFO

Article history:
Received: 10 April 2013;
Received in revised form:
16 January 2015;
Accepted: 30 February 2015;

Keywords
Court of Law,
Cyber Emergency Response Team,
Phishing,
Phishing Prevention Model.

ABSTRACT

Phishing is one kind of Cyber crime in which phisher is doing online theft of secret information like username, password, credit card numbers etc. from the user. This type of crime growing everyday and also creates lot of social and financial issues. Such type of crime causes the direct or indirect damage to the victim. There are number of anti-phishing solution available today, yet the cases of phishing attacks cannot be removed because of several reasons. Here in this paper the model generated namely Phishing Prevention Model which explain what the causes of phishing are, how the phishing attack has been taken place and how we can prevent it using Cyber law.

Introduction

Phishing is the act of attempting to acquire information such as usernames, passwords, and credit card details and sometimes, indirectly, money by masquerading as a trustworthy entity in an electronic communication [1]. Generally phishers hijack a web page of banks and send emails to the user in order to allure the victim to visit the malicious site which look and feel is same as the original web site in order to collect user bank account numbers and credit card numbers. Pharming is a hacker's attack aiming to redirect a Web site's traffic to another, bogus Web site. Pharming can be possible either by changing the hosts file on a user's computer or by changing in DNS server software.

Phishing occurred via fraud Emails and similar looking websites to trick the user to submit the secret personal information like bank account numbers, credit account, and social security numbers, login IDs and passwords of bank transaction. phisher will use such information to steal your money or identity or for any other malicious intention. For phishing criminals are generally use trusted logos of companies and sending large number of emails that appear to come from genuine reputed company or financial institution. The email generally ask user for the secret personal information or in order to verification of information what user has previously provided to establish online account. The chances that a recipient will respond, the phisher might employ all kind of such techniques to phish the Internet user [7].

According to RSA's October Online Fraud Report 2012 a hike in phishing attacks, up 19% in compare of second half of 2011. The firm revealed that it blocked around 200,000 phishing attacks during first half of 2012 and 60% of those attacks originated from U.S. servers. The U.S. is hit by 26% percent of the global volume of phishing attacks followed by U.K. at 46%.The total loss for various organizations comes to more than 2 billion dollar in the last one and a half year. RSA also estimates that there have been roughly 33,000 phishing attacks each month worldwide the year; in the country like Canada have registered an increase of 400 percent in the number of attacks.

All such data shows the strength of the bad intention and related damages to the various organizations and victims, RSA also reveals phishing is grows in the new channels like the mobile phones and social media due to its access use by the normal users. It has been found that these types of platforms are used daily by half of U.S. citizens, making them a privileged target. The other reason of increase of such crimes are that the lack of knowledge about cyber threats and poor awareness about the risks related to an improper use of new media represent critical factors that make possible the spread of malicious contents through social networks and mobile devices. According to a research study by Microsoft, phishing via social networks in early 2010 was only used in 8.3% of all attacks; by the end of 2011 that number stood at 84.5% of attacks delivered through social media. New fraud schemas take advantage of a fundamental aspect of the new social media, the trust. Infecting a node in these complex networks makes it possible to compromise entire groups of individuals, exploiting their mutual trust in contents and links they post.

As per RSA report it has been identified nearly 35 thousand phishing attacks launched worldwide last year, and among them U.S. brands continue to most targeted country of phishing attack followed by United Kingdome and Australia. U.S. is top hosting country nearly 77% attack while U.K., Canada, France and Poland combine 10 % of attacks in month. U.S. is the top hosting country for phishing, with 77% of attacks. Poland, the U.K., Canada, and France combined for hosting just over 10% of attacks in September. Organizations from the U.S. are the mostly targeted; Bank of America, Bay, PayPal, and J.P. Morgan are the principal targets of cyber attacks.

Similar data are published by McAfee in the "McAfee Threats Report: Third Quarter 2012", the financial sector is the most impacted by phishing activities, followed by Online Auction as shown in Figure 1 [25].

In this trend, it is difficult to distinguish private cyber criminals from state-sponsored hackers. Both are interested in getting private companies and government agencies to acquire private information that will allow them to conduct future cyber attacks [8].

Tele:
E-mail addresses: drjigarvpatel@gmail.com

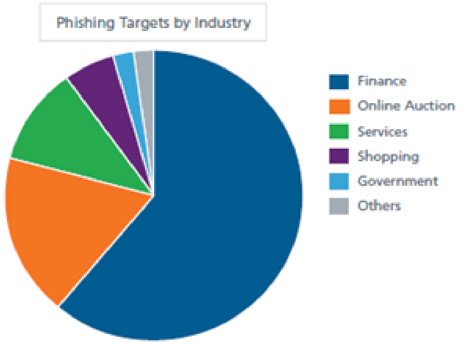

Figure 1: Phishing Target by Industry (McAfee source)

Related Work:

Lots of research has been done on the how phishing attack occurred and how to prevent it and also number of models have been developed by the researchers to protect the consumer trust [2] [3] [4] [5] [6]. Current literature deals with truth of contents in website, policies and interface design and customer support mechanism. The research also carried out to check the URLs which must be identical to genuine website address and making the white list of website which is the list of legitimate website but sometimes phisher can trespassing such security techniques and somehow able to phish the victim. Empirical research in online trust includes a study of how manipulating seller feedback ratings can influence consumer trust in eBay merchants [4]. Fogg. et al. conducted a number of large empirical studies on how users evaluate websites [10] [11] and developed guidelines for fostering credibility on websites, e.g., “Make it easy to verify the accuracy of the information on your site” [9].

Phishing Prevention Model:

Here in the phishing prevention model as shown in Figure 2 it is explained how the phishing take place and how it can be prevented and even after the phishing occurred then what is the remaining procedure that victim has to follow to get the justice from the court of law and punish the phisher using various Cyber Laws created by different countries around the globe. Here in the first part we will see what are the entities in the model while the second part contain how we can prevent the phishing using various techniques of network security. In the third part we will see if any person found that he has been attacked by the phisher then how he/she can go further using police, lawyer and court of law. At the end we will see that after successful prosecution what punishment given to the phisher of the phishing cases and also see how to spread awareness among the Internet user to reduce such types of crimes in future.

Entity:

1. User: Any user who is accessing the Internet.
2. Phisher: One type of Cyber criminal who is trying to access secret information such as usernames, passwords, and credit card details for malicious intention.
3. Victim: The victim is special kind of user who has been attacked by phisher.
4. Cyber Emergency Response Team (CERT): This is responsible body known as Cyber Cell which is looking after the investigation, evidence collection & representation as well as actively involved in the Cyber case prosecution process in the court of law.
5. Court of Law: This is responsible body containing judge, lawyer and supporting staff which is generally run by the government to perform judicial activity.

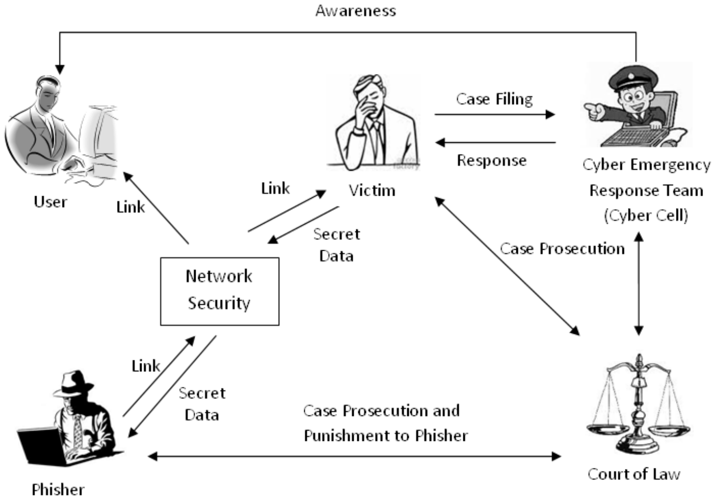

Figure 2: Phishing Prevention Model

Network Security:

This is the area where lots of worked already done by researcher to prevent the phishing attack through Network Security rather than to detect and prosecute the phishing attacks. There are several ideas and techniques proposed and implemented to preventing and detecting phishing attacks among them some techniques trying to prevent phishing emails from being delivered [10] [11], other techniques suggest to make blacklist URLs [12], and also analyzing user pages that user visits [13]. For instance it has been proposed a method called PILFER that depends on features extraction to distinguish between phishing email with 10 features denoted to phishing email for training data [14]. Abu-Nimeh compared six classifiers related to the machine learning technique for phishing prediction. He used 43 features for training and testing by six classifiers [15]. Similarly, Saberi [16] who proposed a new mechanism using three learning methods for phishing e-mail detection. The mechanism depends on binary classification which is either scam or non-scam. Saberi’s proposed method detected 94.4% of phishing e-mails accurately, with the FP reaching up to 0.08%. Islam [17] used another feature-based approach, which depends on three-tier classification method system to detect phishing e-mail. This technique proves that the Bayesian algorithm provide the best level of average accuracy, reaching up to 97% [18, 19].

Anti-phishing toolbars are far and wide available and commonly used by naive or nontechnical computer users to help pinpointing the phishing websites such as Spoofguard [13] and Netcraft [20] toolbars as reported [21]. AntiPhish is a Firefox anti-phishing browser plug-in developed in 2005 [22], It keeps track of a user’s sensitive information (e.g., a password) through binding this information of a user to domain names, thus, preventing this information from being passed to a web site that is not considered trusted. The antiPhish is similar to PwdHash [23] and SpoofGuard [13], where both solutions convert a user’s password into a domain-specific password.

Victim Responsibility:

Any internet user can be become victim of such phishing attack but timely action taken by victim can be very helpful to prevent future damage. Generally all Internet user getting phishing related spam Email everyday and most of users are aware of such Emails and ignoring the same but phishers nowadays making newer and smarter techniques to phish the user. It has been found sometimes civilians are not ready to complain of such crime due to having myth of he/she can be harassed by police and court prosecution and at the end they may not get justice or in other words they don’t have a time for investigation and prosecution process and that’s why number of cases even not registered in the Cyber world. Therefore, that is duties of victim to come forward and register the case in Cyber cell or whatever body has been formed in the native country. Here in the model victim can register his case in the Cyber cell in which CERT is always ready to tackle such cases in the court. In short, that is victim responsibility to cooperate the CERT in the evidence collection process. Generally phishers are sending the link of fake websites through the spam Email that victim has to produce to CERT.

Role of CERT:

Cyber Emergency Response Team (CERT) connects the victim and the court and also plying the dual role at the middle layer. First of all when any victim files the case in such Cyber Cell the first task of CERT to decide whether this attack is for specific victim or it can be attacked to other Internet user as well, if yes then CERT can spread the information of such attack via news channels or papers to prevent the further damage in the country. Other task of CERT is to collect the digital evidences from the victim computer and via Internet which can be produce in the court of law as proof or evidence. CERT can trace the spam Email and its origin as well as it can search the web URLs of fake websites and where it is hosted. It can produce the blacklist of such websites which are generally used as fishing sites.

Other task of CERT is to run the awareness program to Internet user and giving the guidelines to the financial or banking institution to prevent such attacks as follows.

1. Don’t include the personal and financial information like password, credit card number and account number in email because there is no security guaranties in the email.
2. Don’t trust email looking similar like bank web page including logos, picture and similar color scheme that looks original webpage of the bank website.
3. Don’t reply the emails request of your personal and financial information or updating of such information.
4. Don’t click the links comes in emails or copy it to web browser because it can redirect you to other bogus websites.
5. Don’t give any private information on telephone.
6. Check your financial credit report regularly and if you find something odd then contact the bank immediately.
7. Install and update quality anti-virus, firewall and anti-spyware software that can be helpful to restrict the phishing emails.
8. Check the “https” instead of “http” and closed padlock when accessing and transmitting any sensitive or bank transaction information online.
9. Report any suspected phishing scams to concern authority i.e. Cyber cell and contact your financial institution to freeze such account.

Prosecution in Court of Law:

Prevention and detection is not the end of the phishing because that will not affect to the criminal who has committed the phishing attacks. Therefore it is also important to prosecute the phisher in the court of law and give appropriate punishment that helps to create more powerful proactive Cyber laws infrastructure in future.

Lots of countries has drafted phishing related laws like in US the Anti-Phishing Act of 2005 which is specially drafted for scams involving fraudulently obtaining personal information from user. The bill also proposed a five-year imprisonment or fine or both for individuals who is committing identity theft by such falsified emails and websites. United Kingdome has also announced final version of its new fraud bill in which provision of the punishment up to 10 years of imprisonment.

Indian IT act has also some direct and indirect provisions for the phishing attack in which if victim compromised by phisher which is not possible unless & until the phisher fraudulently effects some changes by way of alteration or deletion of the information or data electronically for the victim residing in the any bank server. Therefore, Indian IT act is directly covered and punishable under section 66. Under the subsection of this act the fraudulent email having any fake link of the bank or organization is used for phishing attack of such email and therefore, it clearly attracts the provisions of Section 66A of Indian IT Act. In the phishing email, the fraudster claimed himself as the true banker and uses the identifying feature of the bank or organization like trademark or logo or look and feel of the webpages etc. and thus, clearly attracts the provision of Section 66C of Indian IT Act. Since, phisher trying to cheat the victim by email it is also punishable under Section 66D of the IT act.

Conclusion:

Since people are relying more and more on Internet for online fund transfer, online shopping through credit card inspire the phisher to commit phishing attack to get easy money every day. Therefore, that is important to aware the user how to use the Internet safely and protect themselves against such kind of phishing attacks. The implementation of strong IT infrastructure for register and prosecute Cyber crimes related cases and digital forensics for evidence collection poses the new challenges to the government due to borderless cyber world. To draft uniform policies and Cyber laws worldwide and its implementation is debatable issue nowadays.

References:

1. Wikimedia Foundation, Phishing, 2013. http://en.wikipedia.org/wiki/Phishing.
2. Gefen D, Reflections on the Dimensions of Trust and Trustworthiness Among Online Consumers, ACM SIGMIS Database, 33, 3 (2002), 38-53.
3. Fogg B J et al., How Do Users Evaluate the Credibility of Web Sites?: A Study with Over 2,500 Participants, Proceedings DUX (2003).
4. Kim D, Song Y, Braynov S, & Rao H, A B-to-C Trust Model for Online Exchange, Proceedings of Americas Conference on Information System (2001), 784-787.
5. Egger F N, Affective Design of E-commerce UserInterfaces: How to Maximize Perceived Trustworthiness:, Proceeding of International Conference on Affective Human Factors Design (2001), 317-324.
6. Ang L, Dubelaar C, Lee B, To Trust or Not to Trust? A Model of Internet Trust from the Customer's Point of View, Proceeding. 14th Bled E-Commerce Conference (2001), 25-26.
7. Phishermen P., “Phishing Fraud: How to Avoid Getting Fried”, published by U.S. Securities and Exchange Commission, http://www.sec.gov/investor/pubs/phishing.htm, 2013.
8. Pierluigi Paganini, Phishing: A Very Dangerous Cyber Threat, http://resources.infosecinstitute.com/ phishing-dangerous-cyber-threat/, 2013
9. McAfee Threats Report: Second Quarter 2012.
10. Microsoft. sender id framework overview, http://www.microsoft.com, 2005.
11. Yahoo. yahoo! anti-spam resource center, http://antispam.yahoo.com, 2006.
12. Microsoft. anti-phishing technologies, http://www.microsoft.com, 2005.
13. Chou N, Ledesma R, Teraguchi Y, Boneh D, and Mitchell JC, Client-side defense against web-based identity theft,

Proceedings of the 11th Annual Network and Distributed System Security Symposium (NDSSŠ04), 2004.

14. Fette I, Sadeh N, Tomasic A, Learning to detect phishing emails, in Proceedings of the 16th international conference on World Wide Web. ACM, 2007, 649–656.

15. Abu-Nimeh, Nappa D, Wang X, Nair S, A comparison of machine learning techniques for phishing detection, Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit, ACM, 2007, 60–69.

16. Saberi A, Vahidi M, Bidgoli BM, Learn to detect phishing scams using learning and ensemble? methods ,Web Intelligence and Intelligent Agent Technology Workshops, IEEE/WIC/ACM International Conferences, 2007, 311–314.

17. Islam MR, Abawajy J, Warren M, Multi-tier phishing email classification with an impact of classifier rescheduling Pervasive Systems, Algorithms, and Networks (ISPAN), 10th International Symposium. IEEE, 2009, 789–793.

18. Yearwood J, Mammadov M, and Banerjee A, Profiling phishing emails based on hyperlink information, Advances in Social Networks Analysis and Mining (ASONAM), International Conference. IEEE, 2010, 120–127.

19. Dazeley R, Yearwood J, Kang B, Kelarev A, Consensus clustering and supervised classification for profiling phishing emails in internet commerce security, Knowledge Management and Acquisition for Smart Systems and Services, 2011, 235–246.

20. Netcraft ltd. netcraft toolbar, 2011. http://toolbar.netcraft.com/.

21. Cranor L, Egelman S, Hong J, Zhang Y, Phinding phish: An evaluation of anti-phishing toolbars, CyLab, Carnegie Mellon University, 2006.

22. Raffetseder T, Kirda E, Kruegel C, Building anti-phishing browser plug-ins: An experience report, Proceedings of the Third International Workshop on Software Engineering for Secure Systems. IEEE Computer Society, 2007.

23. Ross B, Jackson C, Miyake N, Boneh D, Mitchell JC, Stronger password authentication using browser extensions, Proceedings of the 14th Usenix Security Symposium, 2005.

24. Phishing Scam Prevention Tips, Department of state, division of consumer protection, New York, http://www.dos.ny.gov/consumerprotection/identity_theft/protect_yourself_from_identity_theft/phishing.html, 2013.

25. McAfee Threats Report: Third Quarter 2012.