International Conference on Recent Innovations in Science, Agriculture, Engineering and Management
University College of Computer Applications Guru Kashi University, Bathinda, Punjab (India)
20th November 2017, www.conferenceworld.in ISBN: 978-93-86171-80-1

A Review: Phishing and its Impact

Sunita[1], Sunny Sharma [2], Dr. Vijay Rana[3]

[1,2]Research Scholar) Arni University (HP), India

[3]Assistant Professor & HOD SBBS University (PB), India

ABSTRACT

In cyber crime phishing is a major crime. Phishing attack is a method of tricking users into unknowingly providing personal and financial information or sending funds to attackers. The most common phishing attacks use some form of electronic messaging such as email to provide a link to what appears to be a legitimate site but is actually a malicious site controlled by the attacker. Phishing is a hybrid attack combining both social engineering and technological aspects and combating phishing attacks requires dealing with both aspects.

Keywords: Phishing, cyber security, community computing, cybercrime

I. INTRODUCTION

Phishing is a form of cybercrime that aims to deceive users into providing personal and/or financial information or to send money directly to the attacker. A phishing attack is generally initiated via some form of message which includes a link to a deceptive domain name which appears to be a legitimate site but is actually controlled by the attacker. Phishing is no longer limited to email to but may also be carried out through voice messaging, SMS, instant messaging, social networking sites, and even multiplayer games [4]. The aim is to deceive the victim into visiting the spoofed site, which appears identical to the original one, and make the user feel comfortable entering a username and password or other personal information. A phishing site is generally created to acquire personal information such as credit card numbers; personal identification numbers (PINs), social security numbers, banking numbers, passwords, etc. or to install malware on the victims computer Phishing began as email. It has since spread to include SMS and instant messaging, message boards, banner ads on websites, voice messaging, social media sites such as Facebook, Banks and even multiplayer games.

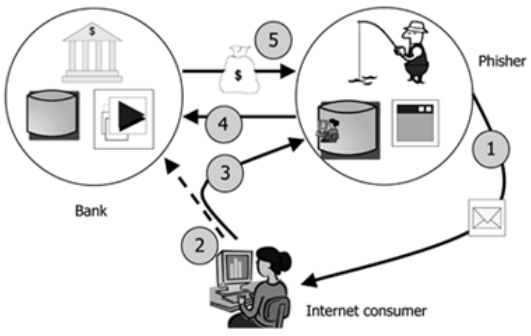

Figure 1 Bank Phishing Process

 ISBN: 978-93-86171-80-1

II. RELATED WORK

Phishing victims often do not realize that they have been tricked. The first phase in combating phishing problem is the detection of a phishing attack. We classify these detection methods in two categories: human detection and machine detection. Human Detection All technology users are not the same. Some are more knowledgeable about security issues and some think longer before they click on a suspicious link. Users may receive training at work but otherwise most internet users are not particularly knowledgeable. Within an organizational setting common operational procedure, knowledge sharing, and double verification processes can reduce problems. Most technology workers are not familiar with the user interaction model of the information systems that they use. Hence it becomes easier for the phishing attackers to mimic the web interface of some familiar webpage and lure the user to enter their private information that is then transmitted to the attackers an overview of phishing education is presented in [13]. This work focuses on context aware attacks and introduces a strategy for educating users by combining phishing IQ tests and class discussions. However not all potential victims have the advantage of formal classroom training and simply presenting the information in an email or a webpage is of limited effectiveness [14] To explore the effectiveness of embedded training, researchers conducted a large-scale experiment that tracked workers' reactions to a series of carefully crafted spear phishing emails and a variety of immediate training and awareness activities [16]. Based on behavioral science findings, the experiment included four different training conditions, each of which used a different type of message framing. The results from three trials showed that framing had no significant effect on the likelihood that a participant would click a subsequent spear phishing email and that many participants either clicked all links or none regardless of whether they received training. The study was unable to determine whether the embedded training materials created framing changes on susceptibility to spear phishing attacks because employees failed to read the training materials. Anti-Phishing Phil [15] is an online game that teaches users good habits to help avoid phishing attacks. It was designed according to learning science principles. During a study participants who played the game were better able to identify fraudulent web sites. Again, however, such training approaches are only useful if potential victims take the training [17].

III. PHISHING COUNTERMEASURES

There is no silver bullet to tackle the issue of phishing. However, we can adapt to better cyber hygiene that will make phishing harder to achieve. Bringing maturity into information sharing protocols will also go a long way in minimizing the damages inflicted by phishing campaigns. In the following passages, we identify the critical areas of improvements and recommend immediate and gradual development practices. We divide our discussion into client-side tools and policies that help protect users from phish attacks and server-side tools and policies that web sites can apply.

 ISBN: 978-93-86171-80-1

Client-Side tools Password Management

Users commonly choose passwords casually to be easy to remember and often use the same password across multiple sites. Users should be encouraged to use different passwords generated and managed by a password management system. The password generation system could check for password reuse. While this will not prevent capture of login credentials for a single site it should limit the damage.

Electronic Communication Filtering

Electronic content filtering should be adopted which filters the contents of the data exchanged on corporate networks. The data should be encrypted as a mandatory practice in order to ensure integrity of the data, prevent data poisoning, and to reinforce the trust on own data. Anti-phishing systems should be set up that filter messages and make recommendations about the trustworthiness of a message.

Firewalls and Filters

Firewalls and filters go a long way in reducing the volume of the "known" phishing scams. They can be an effective tool in reducing the number of phishing messages the user receives. Antivirus and Anti-malware Technologies In many ways, phishing can be achieved with an "anchor" at the user terminal in the form of malware. Antivirus technologies are somewhat effective in eradicating phishing payloads from the end user terminal and strengthening endpoint security. Many anti-virus programs also provide warnings about suspicious websites. Browsers are also more likely to warn users when they are entering data into a website that is not secured by SSL. This makes it much more difficult phishers to set up bogus websites to collect information. Unfortunately, because SSL allows any certificate authority to certify any website it is not impossible for bogus websites to have legitimate security certificates. Some browsers also warn about links that have been reported as malicious.

Secure Email Protocols

It is of utmost importance that the email protocols among the organizations be revised so that the identity of the sender of the email is somewhat ensured to the receiver because without it both the user training and the technological revisions shall be of little use. Due to flaws in email protocols, it is not hard to fake identity of anyone. There have been some solutions that heuristically verify the identification of email senders but email spoofers devise newer ways to trick those systems. Organizations should use cryptographically signed email internally.

Communication

Once a phishing scam is exposed, the related companies whose identity is used in that scam should communicate with their customers and stakeholders about the scam. This is to contain the proliferation of the scams and prevent the users of information systems at the stakeholder's end from giving up their credentials to the attackers. Preparedness: In the modern cyber world, security breaches can happen to any organization.

Education and Training

By far the most important components of fight against fishing measures are education and training. The end users of the corporate systems should be trained in identification of phishing messages. This will help in not only in identification of phishing messages, it will also provide priority feed to the information security knowledge sharing portal that we highly recommended be set up for secure knowledge sharing.

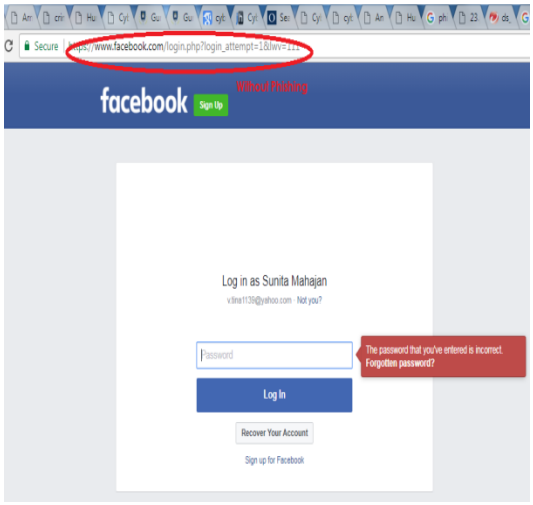

Figure 2 without Phishing Social Site

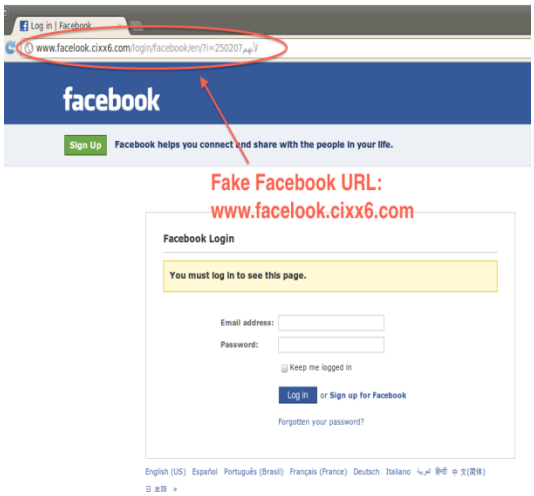

Figure 3 after Phishing Social Site

Server-Side Protection Authentication Procedures

Single factor authentication needs to be replaced with either two-factor authentication or with multi-factor authentication (whichever is cost effective). Unfortunately, there is a risk that overly intrusive security procedures may alienate users. These procedures should be revised and renewed frequently in order to match the pace of the anti-security research and development industry. Site Personalization: One simple technique that websites can use to help safeguard users is personalization. Users can select an image that is shown after their username is entered and before they enter passwords. Facebook Phishing example to identify by domain.

IV. CONCLUSION

Phishing will never be completely eradicated. However, the threat can be reduced through a combination of user and corporate safeguards and server-side measures. User education remains the strongest and at the same time, the weakest link to phishing countermeasures. It is also an intellectual contribution to the employee career growth and ultimately to the evolution of the host organizations as safer, phishing free workplaces. Organizations providing web services also have a role to play.

REFERENCES

[1] J.A Chaudhry, S.A Chaudhry, R.G Rittenhouse, R.G, "Phishing: Classification and Countermeasures", In: The 7th International Conference on Multimedia, Computer Graphics and Broadcasting. SERSC, Jeju, South Korea (2015).

[2] G. Ollmann, "The Phishing Guide--Understanding & Preventing Phishing Attacks", (2007).

[3] M. Jakobsson , S. Myers, "Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft", Wiley, Hoboken, NJ, USA (2006).

[4] J. Hong, "The state of phishing attacks. Commun", ACM. vol. 55, no. 74, (2012).

[5] Anti-Phishing Working Group: Phishing Activity Trends Report. (2014).

[6] A. Litan, "Phishing attack victims likely targets for identity theft", Gartner First Take FT-22. (2004).

[7] R. Dhamija, J.D Tygar, M. Hearst, "Why phishing works. In: Proceedings of the SIGCHI conference on Human Factors in computing systems" - CHI '06. p. 581. ACM Press, New York, New York, USA (2006).

[8] S. Sheng, M. Holbrook, P. Kumaraguru, L.F Cranor, J. Downs,"Who falls for phish? In: Proceedings of the 28th international conference on Human factors in computing systems" - CHI ' ACM Press, New York, New York, USA , vol. 10, (2010), p. 373.

[9] E. Earley, "Understanding social engineering", http://www.net-security.org/article.php?id=1403.

[10] T.N. Jagatic, N.A Johnson, M. Jakobsson, F. Menczer, "Social phishing", Commun. ACM. vol. 50, (2007), pp. 94–100.

[11] F. Zhou, "Phishing Sites and Prevention Measures", Int. J. Secur. Its Appl.vol. 9, (2015), pp. 1–10. [12] F. Howard, O. Komili, "Poisoned search results: How hackers have automated search engine poisoning attacks to distribute malware", Sophos Tech. Pap. (2010).

[13] S.A Robila, J.W Ragucci, "Don't be a phish", ACM SIGCSE Bull. vol. 38, no. 237, (2006).

[14] P. Kumaraguru, S. Sheng, A. Acquisti, L.F Cranor, J. Hong, "Teaching Johnny not to fall for phish", ACM Trans. Internet Technol. vol. 10, (2010), pp. 1–31.

[15] Caputo, D.D., Pfleeger, S.L., Freeman, J.D., Johnson, M.E.: Going Spear Phishing: Exploring Embedded Training and Awareness. IEEE Secur. Priv. vol. 12, (2014), pp. 28–38.

[16] Mahajan, S., & Rana, V. (2017). Spam Detection on Social Network through Sentiment Analysis. *Advances in Computational Sciences and Technology*, *10*(8), 2225-2231.

[17] Mahajan, S., Sharma, S., & Rana, V. (2017). Design a Perception Based Semantics Model for Knowledge Extraction. *International Journal of Computational Intelligence Research*, *13*(6), 1547-1556.