How to prevent phishing attacks?

- In 3 Pages -

Author: Soroush Dalili
Email: irsdl {4t[yahoo }d0t] com
Website: Soroush.SecProject.Com

March 2009

How to prevent phishing attacks?

1. Introduction

"Phishing" has several definitions; however, all of them are common in the main idea of misleading people to divulge their sensitive information such as their credit card number. In fact, Phishers[1] apply "social engineering" techniques to deceive their victims, and exploit the vulnerabilities of the system to conceal their attack completely. Two terms of "*brand spoofing*" or "*carding*" refer to Phishing attack [1] that shows one pervasive type of Phishing attack in which an attacker shows a masquerading website instead of the legitimate one to the users to steal their confidential data.

The term of Phishing was used for the first time in 1996 in relation to stealing AOL[2] accounts [2] [3]. And nowadays, this type of attack is the most common kind of stealing users' data. Statistic shows that Phishing attacks are growing very fast each month and they become more and more serious and sophisticated during the time [1] [4]. On the other hand, there are some techniques and methods to prevent Phishing attacks which are called anti-phishing techniques. In this article, several types of Phishing attacks and effective prevention techniques are introduced briefly.

2. Phishing Attacks in Detail

In order to prevent Phishing attacks, it is vital to comprehend their behaviour first. As this article is in the field of computer security, it does not want to speak about the Phishing techniques which are not directly related to this area, such as "*phone caller ID spoofing*" and so on[3].

Phishing scam does not have a specific schema and it might be seen in different places with dissimilar behaviours. Popular forms of Phishing attacks are:

1. A malicious email (or an instant message) which pretends it is from a legitimate company but it contains some links which are from the attacker website. In most cases, the attacker manipulates the email header to change the sender to a legitimate one. (Figure A.1 in appendix A)
2. A malicious email (or an instant message) that deceives people into sending their information for the attacker. (Figure A.2 in appendix A)
3. A fake website which accepts donation for charities but it is actually the Phisher's website [5].

[1] The person who performs Phishing
[2] American Online
[3] More details of these attacks are in reference [1]

4. A fake website with the similar content as the legitimate website and a homogeneous domain name address such as “payepal.com” or “secure-paypal.com” instead of “paypal.com”.

Moreover, there are some other types of Phishing attacks which are widely used these days.

5. A malicious message which guides the victim to one page of the legitimate website which has a vulnerability such as “*XSS*[4]”. And by using that page, the attacker steals the victim’s confidential information. (Figure A.3 appendix A)
6. Attacker fools the victim to setup a malware which is called “*crimeware*” [4]. This program redirects the important websites, such as “ebay.com”, to the attacker website (for instance by changing the local DNS[5]) or steals the user’s information via the web browsing directly (for instance by adding a small JavaScript to all of the web pages)[6].

Although at first sight it seems that 5 and 6 are not types of Phishing attacks, according to the definition of Phishing and the purpose of these attacks, it is obvious that they can be mentioned in Phishing group.

In order to have more success, Phishers usually use the hybrid of these methods.

3. Anti-Phishing Techniques

Although the best prevention technique against Phishing attacks is security awareness [6] [7], there is no warranty that the users can learn and use this knowledge and then always be up to date. Therefore, science of computer security creates some countermeasures against these attacks. Since types of Phishing attacks are variant, the prevention techniques should be diverse. Some of these techniques are:

1. “Signature based” techniques, similar to “spam protection” techniques [8] [9]. In some forms of this kind of protection, system can learn during the time [16]. For instance in figure A.2 (appendix A) “Authentication-Results” can be used as a signature to recognise a Phishing attack (or spamming) (Type 1 and 2)
2. “Model based” features which are actually statistical trainable filtering [10]. (Type 1 and2)
3. “PHONEY” which is mimicking the user’s response to detect Phishing attacks [11]. In this method, server tries to answer the email automatically, and through the answer, a signature-based algorithm is applied to detect a Phishing attack. (Type 1 and 2)
4. A frame work to detect similar domain names and fraud action [12]. (Type 2 and 4)
5. Page similarity recognition techniques in order to find the fake websites [13] [14]. (Type 2 and 4)

[4] Cross Site Scripting
[5] Domain Name Server
[6] “*Unlike most generic keyloggers, Phishing-based keyloggers have tracking components which attempts to monitor specific actions (and specific organizations, most importantly financial institutions retailers, and e-commerce merchants) in order to target specific information.*” [4]

6. Client side tools (sometimes special for a website of a company) in order to check the safe web pages by some signature based algorithm and also perform harmful website filtering. [15] (Depends on algorithm can apply for all types)
7. Using SSL/TLS or more sophisticated algorithms which use SSL/TLS.[17] [18] (Type 2 and 4)
8. Using some "sign-in seal" during the login process of the user. "sign-in seal" should be secret between the user and the specific server, and can consist of some letters, pictures, or a media which must be shown whenever the user opens the login page. For instance, Yahoo! uses this technology on the login page. (Type 2 and 4)
9. Using updated antivirus to detect "*crimeware*" applications. (Type 6)
10. Secure the websites to have no vulnerability such as XSS. (Type 5)
11. A technique, which no one has spoken about, can be searching the captured image of the website in a powerful search engine. The algorithm of this method can be similar to face detection one, but this time it is for a website. (Type 4)

Despite the high cost of implementing these methods which requires a lot of investment, phishing techniques vary during the time and their cost is very cheap:

1. A Phisher can bypass many of these prevention methods by putting his/her messages inside a picture.
2. A Phisher can hide the source code of a websites by using a simple obfuscation technique.
3. A user who does not care about the pad lock of SSL/TLS or the warning messages can still be a victim of Phishing action.
4. A new Phishing website can bypass the Phishing filtering without any problem.
5. Sign-seal method can also be circumvented when the website has a simple XSS vulnerability.

4. Conclusion

Phishing attacks have become more popular in recent years. As the rates of the crimes in this area have been increased, in this article, several types of Phishing attacks and their prevention ways were introduced. However, this does not mean that there will be no phishing attack in future as phishers can still find some ways of attacking the World Wide Web. Statistics show Phishers use the "botnet"s to vastly disperse their Phishing emails and get more victims. On the other hand, there have been lots of researches on protecting users from these kinds of attacks which may lead to decrease the phishing attacks.

The considerable progress in the prevention methods could lead to a huge change on phishing attacks in the near future. But, there is no doubt that this fight will be continued for many years between the security experts and the attackers similar to virus's technology, therefore people must have some knowledge about security to deal with these attacks.

Appendix

A. Figures

Figure A.1 – Phishing by the email (type 1)

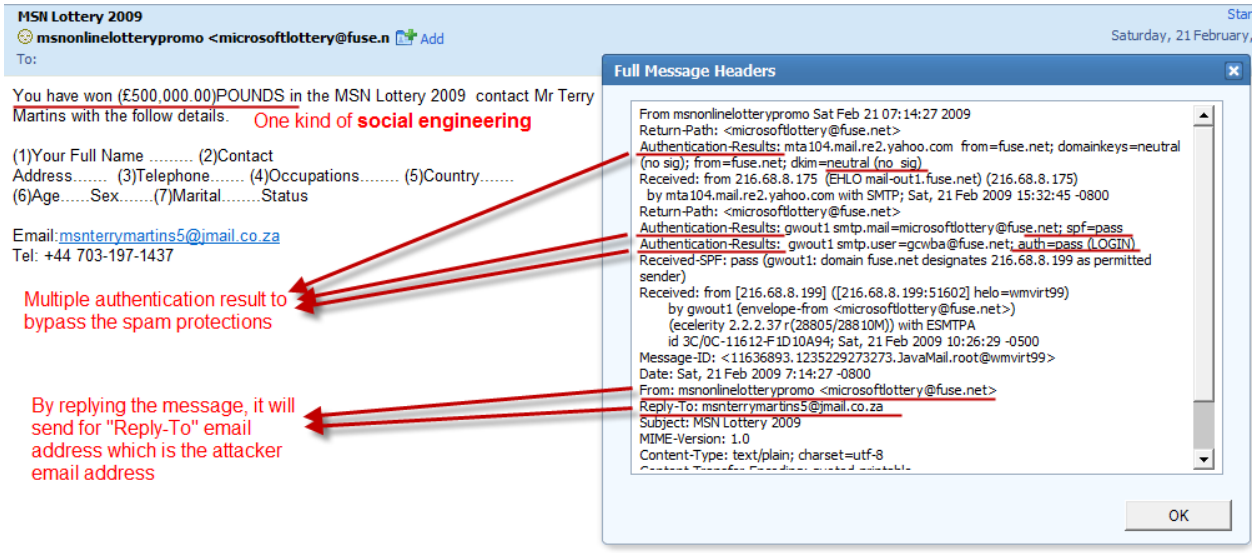

Figure A.2 – Phishing by the email (type 2)

Figure A.3 – Phishing by the website vulnerability (type 5)

References:

[1] A. Williams. “Phishing Exposed”. Syngress Publishing Inc.; 2005.

[2] G. Ollmann. "The Phishing Guide: Understanding and Preventing Phishing Attacks". (URL: http://www.technicalinfo.net/papers/Phishing.html)

[3] "phish, v.". Oxford English Dictionary Online; Dec. 2008. (URL: http://dictionary.oed.com/cgi/entry/30004303/)

[4] The Anti-Phishing Working Group (APWG). “Phishing Activity Trends Report Q2/2008”. (URL: http://www.antiphishing.org/reports/apwg_report_Q2_2008.pdf)

[5] “Recognize phishing scams and fraudulent e-mail”. Microsoft Co.. Oct. 2008 (URL: http://www.microsoft.com/protect/yourself/phishing/identify.mspx)

[6] The Anti-Phishing Working Group (APWG), “Consumer Advice: How to Avoid Phishing Scams”. (URL: http://www.antiphishing.org/consumer_recs.html)

[7] Ronald C. Dodge Jr., Curtis Carver, Aaron J. Ferguson. “Phishing for user security awareness”. Department of Electrical Engineering and Computer Science, United States Military Academy, West Point, NY, USA; 2007.

[8] Michael Edward Edge, Pedro R. Falcone Sampaio.“A survey of signature based methods for financial fraud detection”. Manchester Business School, University of Manchester, Booth Street East, Manchester M16 6PB, United Kingdom; 2009.

[9] T. Beardsley. “Phishing Detection and Prevention - Practical Counter-Fraud Solutions”. TippingPoint; 2005.

[10] A. Bergholz, G. Paab, F. Reichartz, et al. “Improved Phishing Detection using Model-Based Features”; 2008.

[11] M. Chandrasekaran, R. Chinchani, S. Upadhyaya. “PHONEY: Mimicking User Response to Detect Phishing Attacks”; 2006.

[12] S. Garera, N. Provos, M. Chew, et al. “A Framework for Detection and Measurement of Phishing Attacks”. ACM; 2007.

[13] L. Wenyin, G. Huang, L. Xiaoyue, et al. “Phishing Webpage Detection”. IEEE; 2005.

[14] R. Dhamija, J.D. Tygar. “The Battle Against Phishing: Dynamic Security Skins”.

[15] D. Florencio, C. Herley. “Stopping a Phishing Attack, Even when the Victims Ignore Warnings”. Microsoft Research, One Microsoft Way, Redmond, W. 2005

[16] Y. Pan, Xu. Ding. “Anomaly Based Web Phishing Page Detection”. School of Information Systems, Singapore Management University. ACM; 2006.

[17] C. How Tan, J. C. Ming Teo. “Protection Against Web-based Password Phishing”. IEEE.

[18] “Preventing Man in the Middle Phishing Attacks with Multi-Factor Authentication”. TriCipher, Inc.