2008

Anti-Phishing Models: Main Challenges

Edina Hatunic-Webster

Anti-Phishing Models: Main Challenges

Edina Hatunic-Webster

School of Computing
Dublin Institute of Technology
Kevin Street, Dublin 8, Ireland
Edina.Hatunic-Webster@dit.ie

Abstract

Phishing is a form of online identity theft in which the attacker attempts to fraudulently retrieve a legitimate user's account information, logon credentials or identity information in general. The compromised information is then used for withdrawing money online, taking out cash advances, or making purchases of goods and services on the accounts.

Various solutions have been proposed and developed in response to phishing. As phishing is a business problem, the solutions target both non-technical and technical areas. This paper investigates the current anti-phishing solutions and critically reviews their usage, security weaknesses and their effectiveness.

The analysis of these models points to a conclusion that technology alone will not completely stop phishing. What is necessary is a multi-tiered, organised approach: user awareness, technical and non-technical solutions should work together.

Keywords: Phishing, Security, E-commerce

1 INTRODUCTION

Phishing is a form of online scam with the aim of stealing or laundering money. In the simplest form, phishers use a replica of an existing web page to deceive a user into submitting personal or financial data, such as account usernames and passwords. There are different ways to get the user to visit the fake websites and the type of targeted websites also varies. The main targets are banks, but merchants, such as Amazon [2], payment sites (PayPal [21]), online auctions (eBay [7]) and even gambling websites (PartyPoker [20]) are attacked as well.

Becoming a victim of a phishing attack can lead to direct financial losses for the customer. The targeted financial institution will also suffer financial losses such as recovery and repair costs and their reputation may also be damaged. The phishing attacks are becoming so expensive that the Federal Deposit Insurance Corporation (FDIC) and the Federal Financial Institutions Examination Council (FFIEC) mandated that all online banks in the US would need to improve their authentication technologies, as single-factor authentication methodologies may not provide sufficient protection for Internet-based financial services [8]. Phishing has also become a major concern for Internet Service Providers (ISPs), with pressure coming from both users who demand that service providers do more to protect them from attacks, and from the financial institutions targeted by these attacks [16].

In the past, most of the security attacks were committed by single individuals out of curiosity, or to show that a system could be cracked. As the number of people using the Internet for financial applications increased, the reasons have changed. With financial gain as the primary reason, criminals, phishers, spammers and hackers closely cooperate with each other, in order to perform their attacks more efficiently. A study carried out by Abad [1] that involved monitoring chat rooms that phishers used, found that the phishing economy is comprised of many participants that play specialized roles that overlap with other online communities.

A typical phishing attack involves sending an email to multiple email addresses requesting some urgent update of user's existing account information. The email contains a convenient link to allow the user to perform the required task. The link usually leads to a spoofed website. This is known as *classical* or *deceptive* phishing attack [4]. However, new types of phishing attacks do not only exploit careless Internet users but also use the security flaws of the Internet and the underlying computing platforms [10].

2 ANTI-PHISHING MODELS

Most e-commerce applications are designed with the assumptions that the user should be educated to follow good security practices when using sensitive services. Phishers recognised this as the weakest point in the online business. The result is the fast increase in the number of successful phishing attacks.

As the number of phishing attacks is increasing and the potential negative impact on e-commerce has been recognised, many security companies, research institutions and university researchers are tackling the problem of phishing. The solutions offered vary in the same way that phishing methods vary.

There have been many proposals for adding security toolbars to web browsers to display warnings or security information if a phishing website is detected. Browser indicators such as location bar information, Secure Socket Layer (SSL) warnings or certificate information, tell the user whether to trust a server. Examples are:

- Microsoft Phishing Filter, the built in phishing filters in Microsoft Internet Explorer 7 [18] web browser.
- McAfee SiteAdvisor Plus [17], designed to detect not just phishing websites but any sites that send spam or offer downloads containing spyware.
- Netcraft Toolbar [19], displays trustworthiness of the accessed site, hosting country, the name of the organisations hosting the site and the domain registration date. Most phishing sites are short lived and a significant number of phishing sites are registered in a different country to where the spoofed site is based [3].
- Google Toolbar for Firefox [11] displays a popup if a phishing site is suspected.

These anti-phishing toolbars incorporate various methods to detect phishing sites. Most of the commercial products (e.g. Google Toolbar for Firefox) do not reveal the algorithms used. Wenyin et al. [26] propose a method to detect phishing web pages based on *visual similarity*. It compares legitimate and suspicious web pages in three metrics: block level similarity, layout similarity, and overall style similarity. If any of these metrics are higher than a preset threshold, the owner will be alerted and can then take action to prevent potential phishing attacks and hence protect its brand and reputation. Fu [9] proposes a phishing web page detection method using Earth Mover's Distance (EMD) based visual similarity of web pages. Both legitimate and suspected phishing pages are preprocessed into an image signature. The visual similarity of these images is calculated using the EMD method. When the visual similarity value is higher than a threshold, the suspected web page is classified as a phishing web page.

Another approach to differentiate the phishing sites from the spoofed legitimate sites is by using so called Dynamic Security Skins proposed by Dhamija [5]. Dhamija proposes to use a randomly generated visual hash to customize the browser window or web form elements to indicate successfully authenticated sites.

AntiPhish [15], is a browser extension that tracks the sensitive information of a user and generates warnings whenever the user attempts to give away this information to a web site that is considered untrusted. The user associates a set of credentials with a particular website. Whenever the user enters their protected credentials the extension checks to make sure the user is at the appropriate site. A warning message is issued if a registered credential does not match up with the appropriate site.

S*ite-specific passwords* authentication is based on the assumption that most users perform their financial transactions from the same machines. These authorised computers are registered together with the customer account, and their presence is used as a second factor authentication. Therefore, even if the phishers succeeds in taking the user's password, the transaction will fail, as it does not originate from a registered machine.

A similar approach is to authenticate the web server's domain by combining it with the user password. PwdHash [22] is a browser-extension that replaces a users password with a one way hash of the password and the domain name. As a result, the web server only receives a domain-specific hash of the password instead of the password itself.

The Passpet system [29] generates unique passwords for each site. The user only enters one password and Passpet generates different passports for each site/account. The user assigns site labels (petnames) to help securely identifies sites. It is implemented as browser extension and is available for public download [30].

Jakobsson [14] proposes a new authentication protocol called Delayed Password Disclosure that provides the user with dynamic visual feedback while entering password. It allows users to stop entering their password if they obtain feedback that they do not recognize. The protocol relies on the average user's ability to recognise or rather, notice an incorrect image returned. It is not proposed what type of user interface would be suitable. That is left to the user interface designer.

Gouda et al. [12] proposes an anti-phishing single password protocol that allows a user to securely use one single password and one single user name for multiple accounts. The protocol, which they named Single Password Protocol (SPP), uses two techniques: challenge/response and one-time server-specific tickets. This protocol also mitigates phishing attacks because what an attacker obtains is a one-time ticket that is specific to the malicious server (i.e., the

domain hosting the malicious web page), and this one-time server-specific ticket cannot be successfully played anywhere else.

Most *two-factor authentication* systems use shared secrets, tokens (USB token devices, smart cards, or password-generating tokens), or biometrics. Shared secrets are questions that are asked during the authentication process, which a fraudster would be unlikely be able to answer. Security of this approach depends on how unique it is relating to the user.

RSA Security [23] proposes that each website consumer be provided with an RSA SecurID authenticator which generates a new, unpredictable code every 60 seconds which can be combined with a Personal Identification Number (PIN) to implement strong, two-factor authentication. It provides protection against the majority of password phishing attempts because the one-time passcode changes every 60 seconds.

Wu et al. [28] designed a new solution, called Web Wallet that would allow a user to submit their sensitive information online. It deactivates all login forms in the browser and the user has to press a special security key to enter sensitive data. The wallet verifies the credibility of the website. It detects phishing attacks by determining where users intend to submit their information and suggests an alternative safe path to their intended site if the current site does not match it. The user has to choose the destination site from the offered list.

Some researchers are trying to find more comprehensive solutions. For example, Gajek et al. [10] propose a security architecture to protect against deception phishing and malware based phishing attacks.

3 ANTI-PHISHING MODELS SECURITY ANALYSIS

Various anti-phishing models are being proposed in order to prevent phishing attacks. Most of them concentrate on a specific aspect of how we use the Internet to conduct online business.

The most widely used countermeasure used to detect the ongoing attack is user awareness, i.e. understanding the technology. Unfortunately, an average user does not know how to find or interpret the browser's basic security indicators [5]. The user is required to learn not to click on links in an email, making sure that 'https' is being used or check the Uniform Resource Locators (URL) at the browsers toolbar. Even if they click on the lock icon indicating a Secure Socket Layer/ Transport Layer Security (SSL/TLS) session has been established, very few users would be able to determine if the server certificate is valid or fake, or whether is issued by reputable authority. The average user seems to rely on indicators used in the non-digital world, i.e. the logo, and familiar look and feel [14]. To make the problem worse, users are not aware how easy it is to create web pages that look exactly the same as the legitimate web page. Users are preoccupied with their main task, rather than deciphering security indicators. Especially, as some browser plug-ins show that something is wrong, but they do not suggest an alternative to finish the required task (e.g. AntiPhish [15]).

Models, such as [9, 26], that compare visual similarity between the legitimate and the spoofed site, require the crawling of websites to spot the spoofed ones. They also require fast update of the black lists of phishing websites. Judging by SPAM proliferation, which also uses black lists, the anti-phishing organisations need to be much faster than the phishers. The Anti-Phishing Working Group reported in April 2007 [13] that phishing websites were online for an average 3.8 days and the longest time online for a site was 27 days. So, discovering the phishing sites and updating blacklists needs to be done in a very short period of time.

Models that propose creating site-specific passwords are less costly and more usable than other hardware-based authentication. However, they are susceptible to a range of attacks. For example, the malware based phishing in which the dedicated computer becomes a botnet [24]. Also, transmitting the computer identity information is vulnerable to a Man-In-The-Middle (MITM) attack. PwdHash and Passpet systems can work against classical phishing, providing no Domain Name System (DNS) based attack is present.

Dynamic Security Skins [5] differentiates the phishing sites from the spoofed legitimate sites, but it does not provide security for scenarios where the user login is from a public terminal. It also does not protect against malware based attacks.

Models that utilise the creation of site-specific passwords, such as [28, 29] are vulnerable to attacks that emulate the user interface. To overcome possible security loopholes in an HTML page that has JavaScript, AntiPhish [15] deactivates JavaScript every time the focus is on an HTML text element and to reactivates it whenever the focus is lost.

Methods that generate tokens are vulnerable to phishing attacks in which the economic damage takes place while the token is valid. For example, if RSA SecurID [23] is used, even if the phisher has obtained the password and passcode, that combination will need to be used within 60 seconds.

The models analysed so far do not protect against malware based phishing. According to [10], for malware based phishing it is not difficult to fake security indicators (e.g. URL) or modify the system configuration. Key-loggers are used to record all keystrokes entered by a user. User's credentials used to access various online services are then altered. As the anti-key logging techniques were deployed by various organisations, screen-grabbers were invented. Screen-grabbers record the whole or a part of a screen image regularly. Gajek et al. [10] propose a compartmented security architecture which aims to protect against both classical and malware based phishing. The security of the proposed system seems to be efficient against current malware based attack. The problem with this model would be deployment. It builds up on the Trusted Computing Group [25] platform and would require hardware and software changes for mass deployment.

Table 1: Weaknesses of selected models

Model	Weaknesses
Security toolbars [17-19]	The browser indicators (e.g. URL, SSL lock) can be easily forged. Many users ignore warnings provided by anti-phishing toolbars [31], [6], [27]. Small area, users do not notice it on time as security is a secondary goal.
Detecting visual similarity of web pages [5, 26]	Crawling of websites to spot the spoofed ones, short period to update blacklists.
AntiPhish [15]	An HTML page that has JavaScript.
PwdHash [22]	Password reflection attacks can be used by a phisher to obtain a user's site-specific hashed password.
PassPet [29]	DNS based attack.
Dynamic Security Skins [5]	Does not provide security for scenarios where the user login is from a public terminal. Does not protect against malware.
Web Wallet [28]	Easy to emulate user interface.
Single Password Protocol [12]	Vulnerable to MITM attack in the time frame in which passcode/token is valid.
RSA SecurID [23]	Vulnerable to MITM attack in the time frame in which passcode/token is valid.
Trusted computing [10]	Significant software and hardware changes for massive deployment.
Delayed Password Disclosure [14]	Relies on average user's ability to recognise or rather, notice an incorrect image returned.

The weaknesses of the selected models are presented in the Table 1. Each of the analysed models has a security weakness which makes it just a matter of time before it is exploited. For example, a DNS based attack for PassPet [29], or a password reflection attack for PwdHash [22]. Others, like [10], are more robust, but unrealistic to deploy on large scale and protect the most vulnerable, average skilled users. The majority of the models rely heavily on the user to notice provided security indicators and then make the decision as whether to proceed with the intended task or not. However, phishing is an old type of scam adapted for the new cyber society and its weakest point is the user.

4 CONCLUSION

Current anti-phishing efforts concentrate on specific aspects of how we use the Internet to conduct online business: training users how to use the Internet safely; adding various plug-ins to the web browsers in order to warn the user if the phishing site is suspected; using stronger authentication protocols than just *userID* and *password*.

Various security policies and technical solutions which can help to protect against phishing should be available to the user by default. It is unrealistic to expect a user to decide whether a site is genuine or not. The user should also be educated about the general law pertaining to phishing and what steps he/she needs to take in case of being phished. Legislative institutions should also impose valid technology measures on to the service providers. As the laws are only as effective as the technology used to track suspects down, technology research bodies should work on the solutions that will help forensics to discover phishing websites faster, take them down and convict phishers.

Based on the analysis of the anti-phishing models, a conclusion is that technology alone will not completely stop phishing. An integrated approach on multiple levels should help to mitigate phishing effects. User awareness, technical and non-technical measures should be combined to reduce the success rate of phishing attacks.

REFERENCES

1. Abad, C. (2005), 'The economy of phishing: a survey of the operations of the phishing market', First Monday: p. Volume 10, number 9, September 2005.
2. Amazon.com (2008),Amazon.com, Inc., http://www.amazon.com (February 2008)
3. APWG (2007), *'Phishing activity trends: report for the month of June, 2007'*,Anti-Phishing Working Group, (October 2007)
4. Birk, D., Gajek, S., Grobert, F., et al. (2007), *'Phishing phishers - observing and tracing organized cybercrime'*,*Second International Conference on Internet Monitoring and Protection (ICIMP 2007)*, IEEE,
5. Dhamija, R. and Tygar, J.D. (2005), *'The battle against phishing: Dynamic Security Skins'*,*Symposium on Usable Privacy and Security (SOUPS) 2005*, Pittsburgh, PA, USA, ACM, 6-8 July 2005
6. Dhamija, R., Tygar, J.D. and Hearst, M. (2006), *'Why phishing works'*,*CHI Conference on Human Factors in Computing Systems*, Montréal, Québec, Canada, April 22-27, 2006
7. eBay (2008),eBay Inc., http://www.ebay.com (February 2008)
8. Federal Deposit Insurance Corporation, (2004), 'Putting an end to account-hijacking identity theft',
9. Fu, A.Y. (2006),*'Web identity security: advanced phishing attacks and countermeasures'*, *Computer Science*, City University: Hong Kong.
10. Gajek, S., Sadeghi, A.-R., Stuble, C., et al. (2007), *'Compartmented security for browsers – or how to thwart a phisher with Trusted Computing'*,*Second International Conference on Availability, Reliability and Security (ARES'07)*, IEEE Computer Society, 10-13 April
11. Google (2007), *'Google safe browsing for Firefox'*,Google, http://www.google.com/tools/firefox/safebrowsing (February 2008)
12. Gouda, M.G., Liu, A.X., Leung, L.M., et al. (2007), *'SPP: An anti-phishing single password protocol'*, Computer Networks.
13. Anti-Phishing Working Group, (2007), 'Phishing activity trends, report for the month of April 2007',http://www.antiphishing.org
14. Jakobsson, M. and Myers, S. (2007), *'Delayed password disclosure'*, ACM SIGACT News. **38**(3).
15. Kirda, E. and Kruegel, C. (2005), *'Protecting users against phishing attacks with AntiPhish'*,*Proceedings of the 29th Annual International Computer Software and Applications Conference (COMPSAC'05)*, IEEE,
16. Messaging Anti-Abuse Working Group (MAAWG), Anti-phishing Working Group (APWG), (2006), Anti-Phishing Best Practices for ISPs and Mailbox Providers,
17. McAfee, I. (2008), *'McAfee SiteAdvisor'*,McAfee, Inc., http://www.siteadvisor.com/download/ie.html (March 2008)
18. Microsoft (2007), *'Microsoft Phishing Filter at a glance'*,Microsoft Corporation, http://www.microsoft.com/mscorp/safety/technologies/antiphishing/at_glance.mspx (January 2007)
19. Netcraft (2007),*'Netcraft Toolbar'*, Netcraft Ltd.
20. PartyGaming (2006),WPC Productions Limited, http://www.partypoker.com (February 2008)
21. PayPal (2008), https://www.paypal.com (February 2008)
22. Ross, B., Jackson, C., Miyake, N., et al. (2005), *'Stronger password authentication using browser extensions'*,*14th Usenix Security Symposium*,
23. RSA Security Inc., (2004), 'Protecting against phishing by implementing strong two-factor authentication', PHISH WP 0904
24. RSA Security Inc., (2007), 'Phishing special report: what we can expect for 2007', PHISH2 WP 0107,www.rsa.com
25. TCG (2008), *Trusted Computing Group*, https://www.trustedcomputinggroup.org/home (February 2008)
26. Wenyin, L., Huang, G., Xiaoyue, L., et al. (2005), *'Detection of phishing webpages based on visual similarity'*,*14th international conference on World Wide Web*, Chiba, Japan, 10-14 May
27. Wu, M., Miller, R.C. and Garfinkel, S.L. (2006),*'Do security toolbars actually prevent phishing attacks?' CHI*, ACM: Montréal, Québec, Canada.
28. Wu, M., Miller, R.C. and Little, G. (2006), *'Web Wallet: preventing phishing attacks by revealing user intentions'*,*Symposium On Usable Privacy and Security (SOUPS)*, Pittsburgh, PA, USA, ACM, July 12-14
29. Yee, K. and Sitaker, K. (2006), *'Passpet: convenient password management and phishing protection'*,*Symposium On Usable Privacy and Security (SOUPS)*, Pittsburgh, PA, USA, July 12–14
30. Yee, K. and Sitaker, K. (2006), *'Passpet: Convenient Password Management and Phishing Protection'*, http://passpet.org (February 2008)
31. Zhang, Y., Egelman, S., Cranor, L., et al. (2007), *'Phinding phish: evaluating anti-phishing tools'*,*14th Annual Network & Distributed System Security Symposium (NDSS 2007)*, San Diego, CA, 28th February - 2nd March, 2007