The Phishing Hook: Issues and Reality

Journal of Internet Banking and Commerce, December 2004, vol. 10, no.3
(http://www.arraydev.com/commerce/jibc/)

By Qinyu Liao, Ph.D. Candidate, Department of Management & Information Systems
College of Business & Industry, Mississippi State University, USA

Web: http://misweb.cbi.msstate.edu/~COBI/faculty/professor.shtml?qliao
Email: ql1@cobilan.msstate.edu

Qinyu Liao, is currently a PhD candidate major in Management Information Systems at Mississippi State University. Her research interest is in human computer interaction, e-commerce, and cultural issues in information systems management.

By Xin Luo, Ph.D. Student, Department of Management & Information Systems
College of Business & Industry, Mississippi State University, USA

Web: http://misweb.cbi.msstate.edu/~COBI/faculty/professor.shtml?rluo
Email: xl96@msstate.edu

Xin Luo is currently a PhD student majoring in Information Systems at Mississippi State University, USA. He has a undergraduate degree in International Business, a Master's degree in Business Administration in CIS, and a Master's degree in Business Information Systems. His research interests center around Information Security, M-commerce, and global IT adoption. He is a member of The Mississippi State University Center for Computer Security Research (CCSR).

Abstract

Phishing attacks has become increasingly serious and spread more rapidly because of its ease of launching, difficulties to be caught and the monetary benefit behind it. As currently there is no single technology that has been effective in deterring phishing, the authors pointed out the trends in prevention of phishing and emphasized the importance of preventive measures, such as awareness education, collaboration in information sharing and standardization, legal enforcement etc.

Keywords: security, Internet crime, identity theft, phishing

Introduction

Phishing has become one of the most widespread and insidious forms of Internet crime challenging the financial institutions, health companies, and other online business as well. The concept of phishing has actually been around for years. Original phishing was a term coined around 1996 by hackers to describe stealing America Online accounts by acquiring usernames and passwords[1]. With the ubiquitous spread of email use and internet access, the ability of criminals to take advantage of the technology has increased significantly since the past several years, with an almost exponential increase in incidents since the second half of 2003, according to many organizations that are trying to track this trend[2].

Microsoft defines phishing as any type of attack that attempts to lure users to a fraudulent website to enter sensitive information that is then used for identity and banking theft. This normally occurs via an email, directing users to a phishing web site [3]. By hijacking the trusted brands of well-known banks, online retailers, and credit card companies, phishers convince up to 5% of recipients to respond to them[4].

Identity theft is the endgame for many phishing schemes and has been the No. 1 consumer complaint to the Federal Trade Commission in the past four years. It has been stated as a significant step in the transition of spam from nuisance and productivity speed bump to a potentially huge fraud problem[5]. Reports of phishing attacks has become a weekly event targeting popular trusted sources such as VISA, US Bank, CitiBank, eBay, PayPal and many others[3].

The purpose of this paper is to pinpoint current issues concerning phishing and provide practical suggestions for consumers and financial institutions.

Why Phishing works

Increased enterprise security

Phishing is on the rise because increased security measures are making it harder for attackers to directly breach enterprise networks and the consumer has become the weakest link in the trust chain[6]. According to a report by the Anti-Phishing Working Group (AWP), the number of reported phishes reaches 1,974 in July 2004, which is a 39% increase over June (1422).

Time and cost

The costs associated with spam are low compared with the payoff [5]. Phishing messages and scam sites don't have to be around for long to do damages. Often, scammers shut their phishing sites down after only a few hours, since they can bring in credit card information in a matter of minutes[7] and work on them offline. It takes about eight days from the establishment of a web address to the time a phishing attack can be launched using that address. However, monitoring online phishing attacks, trading of account numbers, identity theft, and so on requires companies to be on a 24-by-7 basis.

Technology savvier

Most typical phishing email messages are poorly constructed and rife with misspelled words and are easily identifiable as fakes, but the sophistication of the new attacks is high and keeps growing. The phishers are starting to cooperate with crackers and virus writers to swap ideas and methods, which unlike previous scams, victims would likely have no idea they had done anything wrong[8]. In some case, victims are directed to the real bank's website while a pop-up window is overlaid to capture details. In other cases, the surfer's toolbar is taken over. One of the latest attacks against Berclays goes even further by tricking people into going to a web site that sneakily downloads a 'Trojan horse' program to their PC. Once installed, the Trojan horse watches keystrokes and thus snaffles the customers identifier and pass code [9]. The latest Trojan horse can even uninstall itself after a designed period and remove tags from windows registry, making it very difficult for users to detect and track. Therefore, even if the user is smart enough not to enter any personal information into the web form, his or her data still could be at risk [8].

Threats of phishing

The natural targets of phishing are prominent corporations that keep sensitive financial and other personal information: banks, brokerages and credit card companies, as well as popular e-commerce firms such as eBay, Amazon, PayPal and large internet service providers. Companies whose names are used in scams can incur substantial operational costs if they have to change passwords and PINs for thousands of customers[6], reissuing cards, reassuring customers and so on. According to a Gartner report, phishing-related fraud cost banks more than $1.2 billion dollars in direct losses in the US [7] and some £60 million in the UK[2] in 2003. In Sep.2003, the Federal Trade Commission reported that 9.9 million U.S. residents have been victims of identity theft during the past years, costing business and financial institutions $48 billion and consumers $5 billion in out-of-pocket expenses[1].

The companies' concern is more for their organizational reputations than the actual financial losses. They're dealing with people's trust [8]. Those corporations spend hundreds of millions of dollars infusing their brand with positive associations and entrenching them in the public consciousness. That hard work is quickly eroded when the name and logo get used to dupe consumers. On the Internet, a company can quickly lose control of its own brand [10]. According to The Identity Theft Resource Center, the average time spent repairing the damage caused by a stolen identity is approximately 600 hours and can take years to completely recover[11]. The consequence of the dilemma is that many institutions have stopped communicating with customers via email to help eliminate the possibility that the user may become a victim of phishing[12].

Consumers go to great lengths to protect their personal information, yet any breach of that protection can open one up to many potential threats, including credit card fraud, having an identity used for other criminal activity, or stolen money. There are also various intangible threats, such as damage to credibility, loss of trust, or embarrassment; having personal information stolen can cost a great deal more than merely losing cash. In a recent online survey of 650 U.S. respondents, 75% said they are less likely to respond to emails from their bank because of the fear of phishing.

Organizations are walking a fine line with phishing. They want people to be aware, but they don't want them to be so paranoid that they stop doing business or communicating with them [8]. This could lead to a change in the way online banking is implemented if not handled properly.

The reality of the phishing fighting

Awareness education

It has been suggested that end user education, technology solutions, information sharing with law enforcement are the best practice fighting phishing [13]. Some of the rule of thumb for users include: be suspicious of requests for personal information; don't click the link in email but instead enter URLs manually; try some of the new web tools that unmask fake sites; contact the credit-card company, bank, or the web site immediately if suspect being hooded in a phishing attack; warn family and friends who may be new to the Internet and susceptible to scams; lobby ISP to do something about the problem[14].

Suggestions for the financial institutions are on the technology and planning side, such as adopting technology that certifies legitimate mail, incorporating toolbars that warn users that they may be entering shady parts of the Internet, using software that can help react when targeted by tainted mail, blunting the damage to customers[15]. Others also pointed out that financial institutions need to be consistent in online dealings with customers so that customers can tell the difference between a real email and a phishing attack.

Lack of technical standards

Some of the technologies suggested to avoid phishing are authentication, validation, blocking and monitoring [4]. These are basically computer software/technologies that could authenticate and validate legitimate emails, block users from going to fraudulent web sites, and alert companies when someone registers for a copycat brand. For example, eBay has added a new service to its tool bar called Account Guard, which alerts users when they're at legitimate eBay and PayPal sites and spoofed eBay and PayPal sites. Software called Spoofstick by CoreStreet can validates a web site by using the browser's internal read-only variables to display the top and the second level domain name that the user is browsing. Companies such as Cyveilliance can monitor the web on behalf of large companies so that the phishing sites can be detected and shut down nearly within hours instead of two days. Birch et al. [9] also recommended using Smart Cards to fix the phishing problem.

The focus of phishing prevention technology is identity authentication. The SMTP (Simple Mail Transfer Protocol), which is widely implemented to forward the majority of email on the Internet, does not require any authentication from the sender. This enables phishers and other cyber criminals to spoof the sending address of a message and to make it appear to be legitimate. As such, a solid authentication mechanism is needed to ensure that the email originates only from valid mail servers, which will require revamped changes to the email protocol standard as well as an added layer of authentication to the messaging infrastructure. The new email system doesn't require action on the part of end users because it is an entirely server-based approach. It will require that administrators install and manage yet-to-be-released open-source public-key software on the mail server [16]. It will reduce the amount of spams but not entirely eliminate it [16]. One recent proposal of this new system is the Sender ID technology by the Internet Engineering Task Force. It claims to inspect email at the server level to ensure it comes from where it claims to come from and inspect it at the header level to look for domain spoofing [17].

However, revising email standards could be effective to fight against phishing but changing the way email works could take years and it's not feasible to completely depend on this for solving phishing problems.

Legal enforcement

Without the involvement of legal enforcement to further strengthen relevant juristic policies, the war against phishing would not become a possible success. The House of representatives has passed the Identity Theft Penalty Enhancement Act, which increases the sentences for ID theft via phishing and creates a new crime of aggravated ID theft, defined as using a stolen ID to commit certain crimes[18]. Another proposed legislation *The Anti-Phishing Act 2004* by the Democrat from Vermont will target "*a rapid growing class of identity theft scams on the internet that is causing short-term losses and long-term economic damage.*"

It has been argued that the proposed law "*will allow the authorities to get involved a lot more quickly and proactively.*" [19] Yet it has been criticized being strictly reactive and providing nothing helpful for preventing identity theft.

Collaboration in information sharing

Companies are also needed to team up to tackle the problem of phishing. The Trusted Electronic Communications Forum (TECF) is an organization representative of leading retail, telecommunications, financial services, and technology companies to work with the U.S. and other global governments, as well as standards organizations and companies, to fix problems such as email and web site spoofing, which contribute to a fast-growing online identity theft problem. The TECF describes itself as "*a cross-industry, cross-geographic consortium dedicated to the standardization of technologies, techniques and best practices in the fighting against phishing, spoofing and identity theft.*"[20] It also intends to develop long-term and short-term strategies to combat the phishing problem.

Additionally, The Anti-Phishing Working Group (APWG) is another industry consortium made up of financial institutions, online retailers, Internet service providers, and law enforcement. While APWG tracks and reports on phishing scams, the TECF focuses more on developing and promoting standards that companies can use to combat phishing and to prevent the erosion of online commerce[21].

As the internet can reach users beyond the geographical boarder and facilitate phishing to the same extent, it's not always easy to shut down a phishing web site, especially if it's in another country. And "*once you catch them, you cannot necessarily stop them*" [7]. Therefore, it's necessary to call for collaborations in information sharing, in terms of anti-phishing strategies and development, among companies and countries.

Conclusion

Phishing attacks have become increasingly serious and spread more rapidly because of how easy they are to launch via the globally connected networks, how easy it is to not get perceived by computer users, and the dilemma that attackers gain monetarily without being caught. The sophistication of such attacks will likely increase over time and become less likely to be discerned from a legitimate email, web address, or web site, even for experienced computer users. Online system vulnerabilities only exacerbate this situation, making it difficult for users to battle against such attacks.

New technologies and standards are becoming more important than ever to deter and detect phishing attacks but we have to be realistic in how long it will take. No single technology can keep phishing at bay but there are ways to make phishing harder to accomplish and less appealing for the would-be phishers. Legislation is necessary for prosecution of a crime after the fact. However, prevention is the better way to fight the problem [22].

Importantly, companies should have disaster recovery plan in place to cover phishing attacks. Consumer education can arouse and increase the awareness of the phishing threat and online vulnerabilities. Security insiders should applaud the growing public-private partnership and the increased attention to phishing issues so that information can be shared within the network of allies to expand incident-response capabilities to deal with the spike in phishing attacks. This is also a need for government leadership to commit to fighting the online menace [23] by giving more investigators, more funding, and more attention from lawmakers and upper management.

References

1. Kay, R., Phishing. Computerworld, 2004. 38(3): p. 44.

2. Roberts, P., Gartner: phishing attacks up against U. S. consumers. IDG News Service, 2004.

3. Dunham, K., Phishing isn't so sophisticated: scary! Information Systems Security, 2004(May/June).

4. Radcliff, D., Phear of phishing. Network World, 2004. 21(22): p. 35-37.

5. Sturdevant, C., Communication can take the bite out of phishing. eweek, 2004: p. 45.

6. Vijayan, J., IT, Vendors' scramble to combat phishing. Computerworld, 2004. 38(3): p. 12.

7. Claburn, T., and Marlin, S., Saving Email. Informationweek, 2004.

8. Fisher, D., Phishing gets savvier. eweek, 2004: p. 14.

9. Birth, D., and Pannifer, S., Phish and Chips: We're with Bill Gates-- We'll never fix this problem without smart cards. Journal of Internet Banking and Commerce, 2004. 9(2).

10. Wahl, A., Gone phishin'. Canadian Business, 2004. 77(12): p. 13.

11. Identity Theft Facts and Statistics. The Identity Theft Resource Center, 2004.

12. Elledge, A., Phishing: an analysis of a growing problem. 2004.

13. Savage, M., This threat could kill e-commerce. SC Magazine, 2004.

14. Stone, A., How to avoid the 'phish' hook. Business Week Online, 2004.

15. Stone, A., Tangled in the phishing lines. Business Week Online, 2004.

16. Caton, M., Revising standards could slow spam. eweek, 2004: p. 46-47.

17. anonymus, A cure for malware. eweek, 2004.

18. Fisher, D., and Carlson, C., Phishing under the gun. eweek, 2004.

19. Sterlicchi, J., Industry body welcomes anti-phishing proposals. SC Magazine, 2004.

20. Rosencrance, L., 17 companies form group to fight phishing, spoofing. Computerworld, 2004.

21. Roberts, P., Companies team to reel in phishing. Network World, 2004.

22. Musthaler, L., How to avoid the phish hook. Network World Technology Executive Newsletter, 2004.

23. Fisher, D., Fighting back. eweek, 2004.