Internet Fraud through Phishing: A High Tech Cybercrime

Student Name

Instructor's Name

Date

Introduction

Internet fraud is a common high tech crime that is difficult to solve because of its rapid evolution and broad categories. For instance, internet fraud occurs in various forms like online auctions, retail fraud, money laundering, and investment fraud. Moreover, Internet fraud continues to evolve making it difficult for the authorities to determine what online mediums cybercriminals use to defraud users and how (Newton, 2003). The World Wide Web's open platform also makes it easy for cybercriminals to look for various methods to defraud users, while the continued and growing use of the Internet for small- to large-scale businesses and consumers worldwide entice cybercriminals to take advantage of user information to embezzle money. Internet fraud "will continue to grow because of the ripe conditions that exist on the World Wide Web for fraudulent activities" and worsened by the "lack of a common set of international laws and the difficulty related to enforcing existing laws" (Kranacher, Riley & Wells, 2010, p. 127). The following discussion will be about Internet fraud and the various issues surrounding it. However, due to the broad nature of the topic, the discussion will focus on a specific means of Internet fraud – phishing. In addition, the discussion will also cover a discussion of actual cases of phishing and steps on how online users could prevent being defrauded by cybercriminals.

What is Phishing?

Phishing is a high tech crime committed by cybercriminals in their attempt to steal sensitive information from regular users and use private data to perform identity theft and Internet fraud. Cybercriminals obtain personal information from online users by sending them electronic messages or creating online websites where users will be asked to provide their usernames and passwords as well as other personal information. Cybercriminals are often

successful in doing so because they pose as legitimate and familiar organizations. As a result, online users are compelled to submit personal information thinking they would be doing so for a trusted business or organization. Online users often receive phishing messages that ask them to validate their accounts by entering personal information like credit card numbers, Social Security numbers, and passwords. Aside from being defrauded, cybercriminals also use phishing e-mails as a means to send viruses and malicious programs. (Boone & Kurtz, 2009) In recent years, phishing methods evolved allowing cybercriminals to obtain sensitive information in various ways. Instead of sending electronic messages and creating websites with pop-up pages, cybercriminals also use other techniques like voice messaging. Vishing (voice phishing), for instance, is conducted via text messaging or telephone calls. Cybercriminals pose as legitimate companies and ask users to validate their accounts by revealing their credit card numbers (Boone & Kurtz, 2009).

Actual Cases of Phishing

In 1996, a group of American cybercriminals hacked into the system of America Online (AOL) by scamming AOL users into revealing their usernames, passwords, and credit card information. The cybercriminals themselves coined the term ‘phishing’, which essentially means a “luring method that thieves use to fish for unsuspecting Internet users’ personal identifying information through e-mails and mirror-websites which look like those coming from legitimate businesses” (Acoca, 2008, p. 17). In 2009, Egypt and the United States filed charges against one hundred cybercriminals for phishing and defrauding online users for approximately $1.5 million. The perpetrators targeted major financial institutions, taking advantage of their account holders to gain access to personal accounts. Due to the efforts of the Federal Bureau of Investigation (FBI), the perpetrators were identified and charged. “American authorities charged 53 people,

while Egypt charged 47, with offences including conspiracy to commit bank fraud, computer fraud, money laundering and aggravated identity theft" (Wattanajantra, 2009). Another case of phishing involved online users who were victimized during the HM Revenue & Custom's (HMRC) data loss in the United Kingdom. Employees at the HMRC sent sensitive information via computer discs, which resulted to a massive data loss for the organization. Cybercriminals jumped at the opportunity to scam online users by sending phishing messages to the people involved in the case. The e-mails informed the users that to compensate for the outcomes of the data loss, they would be receiving a tax refund from the government and in order for them to claim their refunds, they must validate their accounts using personal information (Ec-Council, 2009).

Cybercrimes like phishing are difficult to eradicate because cybercriminals change their techniques often. Moreover, cybercriminals "have learned to narrow their focus on their victims and never stay in the same place for long" (Perlroth, 2012). They continue to target online users by spreading malicious content all over the World Wide Web. According to Google, cybercriminals create over 300,000 phishing websites every month and the number of websites allows them to target a large percentage of online users. Although there are various organizations that monitor online cybercrime trends and attempt to eradicate these crimes like the Anti-Phising Working Group (Jaishankar, 2008), the absence of a standard international anti-cybercrime laws prevent authorities from addressing the problem on a larger scale. The victimization of other online users will continue despite efforts from financial and security institutions in the United States like Barclays, American Express, and Citigroup, for instance (Seidman, 2012) to protect their users from Internet fraud and phishing scams and the government to implement strict laws to counter cybercrimes (Worthen, 2012) if those standards and laws do not exist outside the U.S.

"International cooperation is essential to address the unique challenges that the Internet presents" and "international treaties also have a significant role in combating international cybercime" (Ferrera, et. al., 2011, p. 436).

Prevention

Although international cooperation is highly significant in solving cybercrimes like Internet fraud and phishing, online users should also take precautionary measures to prevent being scammed by cybercriminals. Standard international laws to eradicate cybercrimes may seem to have a massive influence on the abolition of these crimes but online users could also use prevention techniques to help them detect scammers from legitimate organizations. Online users are advised to be vigilant especially when it comes to responding to electronic messages sent by suspicious sources. Despite electronic messages appearing to be legitimate, online users should remember that real organizations like financial institutions do not ask for sensitive information such as passwords and credit card numbers. Before responding to suspicious emails, online users should contact their banks or the institution to inquire whether they send the messages or not. Financial institutions like Barclays have also taken measures to ensure that their account holders can easily identify legitimate messages and websites from fake ones. By adopting private domains like .barclays, online users can easily determine legitimate websites and messages (Seidman, 2012). Online users could also use assistance from network security companies to ensure that they do not receive suspicious messages on their computer. Network security companies offer sophisticated softwares, programs, and systems that online users could use. These programs, softwares, and systems are programmed to detect malicious content and warn users to verify the identity of senders or authenticity of websites before accessing them. Overall, most business and organizations advise consumers to remain informed to prevent victimization.

References

Acoca, B. (2008). *Scoping paper on online identity theft of OECD.* Presentation at OECD Ministerial Meeting on the Future of the Internet Economy during 17-18 June 2008 at Seoul, Korea.

Boone, L. E. & Kurtz, D. L. (2009). *Contemporary business 2010 update.* Hoboken, NJ: John Wiley and Sons.

Ferrera, G. R. et al. (2011). *CyberLaw: Text and cases.* Florence, KY: Cengage Learning.

Jaishankar, K. (2008). Identity related crime in the cyberspace: Examining Phishing and its impact. *International Journal of Cyber Criminology,* Vol. 2 (1), pp. 10-15.

Kranacher, M., Riley, R., & Wells, J. T. (2010). *Forensic accounting and fraud examination.* Hoboken, NJ: John Wiley and Sons.

Newton, M. (2003). *The encyclopedia of high-tech crime and crime-fighting.* InfoBase Publishing.

Perlroth, N. (2012). *Cybercriminals getting quicker and craftier, Google says.* Retrieved 19 Aug 2012, from: http://bits.blogs.nytimes.com/2012/06/19/cybercriminals-getting-quicker-and-craftier-google-says/

Seidman, A. (2012). *No 'phishing': Banks try to sink scammers.* Retrieved 19 Aug2012, from http://online.wsj.com/article/SB10000872396390444508504577593243972975650.html

Wattanajantra, A. (2009). *The FBI cracks the 'largest phishing case ever'.* Retrieved 19 Aug 2012, from: http://www.itpro.co.uk/616069/the-fbi-cracks-the-largest-phishing-case-ever

Worthen, B. (2012). *Email giants move to slash 'phishing.'* Retrieved 19 August 2012, from: http://online.wsj.com/article/SB10001424052970204652904577191360158848618.html