Internet Phishing and Current Trend-Ghana

Edward Danso Ansong[1#], J. B. Hayfron-Acquah[2#], Dominic Damoah[3 #], Amponsah-Kaakyire K[4#], G. Nagappan[5#]
[#134] Faculty of Science, Valley View University, Accra-Ghana
[#2]Department of Computer Science, Kwame Nkrumah University of Science & Technology
[#5] Department of Computer Science, Saveetha Engineering College, Chennai-India
[1]*edkan20002002@yahoo.com*, [2]*kwddamoah@yahoo.com*, [3]*jbha@yahoo.com*, [4] *kamponsah-kaakyire@st.vvu.edu.gh*, [5] *nagappan_g@yahoo.co.in*

ABSTRACTE-commerce has made it so convenient to do business from almost anywhere and at any time. With the rising popularity and use of e-commerce increases the number and techniques of cybercrime relating to business. But of what benefit is e-commerce if it is insecure from criminals? Phishing is the act of stealing credentials from people through electronic means by posing as a legitimate body the victim has a connection with whilst the attacker really has no such identity. Phishing has caused great losses to businesses and some individuals. In this paper, phishing techniques and a few counter measures will be discussed. This is to raise people's awareness about phishing scams to enable them identify and combat such scams.

*****

INTRODUCTION

Phishing is defined by (Junxiao & Sara, 2012) as "a form of social engineering in which an attacker, also known as a phisher, attempts to fraudulently retrieve legitimate users' confidential or sensitive credentials by mimicking electronic communications from a trustworthy or public organization in an automated fashion." Simply, phishing can be defined as using fallacious means to try to collect confidential information or credentials from licit users by falsely posing as an authentic public organisation through electronic means. Phishers use social engineering coupled with their technical knowledge in attempting to collect the credentials of victims.

Because of phishing scams organisations fear that their reputation is at stake and that, customers will lose trust in electronic commerce which will adversely affect their business (Kruegel & Kirda, 2005).

The focus of this article is to increase people's awareness about phishing and to suggest methods by which one can identify and combat phishing scams. According to (Junxiao & Sara, 2012), "a study of demographic factors suggests that women are more susceptible to phishing than men and users between the ages of 18 and 25 are more susceptible to phishing than other age groups." This study will also aim at suggesting methods by which these vulnerable groups in society can be protected against phishing scams.

According to (Anti-Phishing Workgroup (APWG), 2013), "the following are the phishing activity trend summary for the 1st quarter of the year 2013:

- 'Phishing attack numbers declined 20 percent from Q4 2012 to Q1 2013, due to a precipitous drop in virtual server phishing attacks.'
- 'Trends indicate phishing levels returning to the levels seen prior to the record-setting highs of 2012.'
- 'The significant drop in the number of phishing-based Trojans and downloaders hosted in the USA, with an increase in Canada, illustrates the migratory patterns of cyber-criminals.'
- After reaching an all-time high in November 2012, the number of brands targeted by phishers dropped as low as 348, in February 2013.'
- 'Payment Services jumped back on top as the most-targeted industry sector, after being surpassed by financial services during the fourth quarter of 2012.'
- Trojan infections have reached record levels, accounting for almost 80 percent of all infections.'"

Phishing Techniques

"Vulnerability searches are intended to pick out a particular program or version of a program, which the attacker can subvert" (Moore & Clayton, 2009).

Spear phishing is a phishing attempt aimed at specific individuals or companies normally suspected to have access to valuable assets.

Clone phishing is a phishing attack where an attacker replaces links or attachments in a previously delivered legitimate mail with malicious ones. An almost identical (cloned) email is then sent to the receiver with the spoofed email address of the original sender making it seem authentic and claiming to be a resend or an updated version of the original mail (Wikipedia, 2013).

Whaling is phishing attacks aimed at high profile targets within business (Wikipedia, 2013).

Link manipulation is a technique where a link in an email is made to seem to belong to an authentic organization. The URL may be misspelt or subdomains will be used. For instance, www.legitimatesite.home.com appears to take you to the homepage of the legitimate site while it actually points to the legitimate site section of the home website of the phisher. Also the displayed link text could be set by phishers to appear to take the victim to a legitimate site (Wikipedia, 2013).

In the filter evasion technique, phishers use images instead of text making it harder for anti-phishing filters to detect commonly used phishing text in emails (Wikipedia, 2013).

Website forgery is also another phishing technique where the attacker creates a forgery of a legitimate website. Using the vulnerabilities in the legitimate website's scripts, the attacker attempts to redirect users to his forged site. Once a victim visits the phishing site and enters his details, they are captured by the phisher (Wikipedia, 2013).

Phone phishing is an attempt by an attacker to collect legitimate information from a person through phone calls or messages by using fake caller ID to pose as a legitimate organization.

'Evil twin' is a phishing technique where attackers create a fake wireless network with similar SSID and other network information to a legitimate public network. When a victim logs in to an account on the fake network their credentials are captured (Wikipedia, 2013).

Another method is to forward the user to a legitimate website, then to place a popup window requesting credentials on top of the page in a way that makes many users think the site is requesting this sensitive information. When the victim enters the credentials, they are captured by the attacker (Wikipedia, 2013).

Tabnabbing takes advantage of tabbed browsing, which uses multiple open tabs, that users use and silently redirects a user to the affected site. This technique doesn't redirect you to sign in at a fake website, but instead loads the fake page in one of your open tabs. If the user is not aware and minimizes the window or moves to another tab and tries to get back to the legitimate site's tab, he might end up selecting the tab with the fake site. Attackers then prey upon information entered by the victim (Wikipedia, 2013).

Counter Measures against Phishing as a Country

"Dynamic Security Skins seems to be a good method. The idea is that the website server generates a unique abstract image for each user, and the web browser also independently computes the same image. The algorithm ensures that a phisher cannot predict this image. The user just needs to compare these two images; if they are identical, the server is legitimate" (Junxiao & Sara, 2012).

Users can also verify phishing attacks by checking for digitally signed certificates though certificates can be hacked and replicated. The padlock icon in the https address bar can be used to check for certificates. Sometimes users

may have difficulties identifying an https padlock from a normal padlock icon in a browser.

User education is one major way of protecting people against phishing attacks. According to (Junxiao & Sara, 2012), "a study on the effectiveness of several anti-phishing educational materials suggests that educational materials reduced users' tendency to enter information into phishing webpages by 40%, however, some of the educational materials also slightly decreased participants' tendency to click on legitimate links." Phishing scams have become sophisticated and advanced. Users have to use their discretion carefully when they are on sites that request for useful information.

There has to be legislative measures according to each country's laws to deal with phishers. The laws have to be detailed to specify which actions can be classified under phishing and which cannot. It has to help to deal with the grey area so people do not find mild ways of phishing and get away with such acts.

Also businesses need to have specific ways by which their clients can identify that certain mails, other information and requests coming from them are very legitimate. Just as businesses have trade secrets, these measures should be very difficult to imitate.

Users should be discouraged from following ads that claim to bring users fortune for which they have to do very little or no work.

Unfortunately, Ghana is still challenged with policies to implement against cyber security. Politics, bureaucracy, and lack of cooperation between the Universities, Research Institutions and State Security Agencies have not helped in the implementation of these policies. Universities still train students on US and UK laws on cyber security when those laws do not apply in Ghana. The Ghana police is mostly unable to prosecute cases effectively against criminals and in some cases go for a reduce sentences because of lack of knowledge in these laws on cyber security but charge such criminals with conventional laws, thereby escaping with lesser punishment [6].

CONCLUSION

Phishing has a number of harmful effects on society, business and individuals. Phishing results in excessive use of network resources such as bandwidth. It results in loss of sensitive information which can be stolen and accessed by phishers with stolen credentials. Phishing can therefore be a doorway to hacking with the stolen credentials of a victim. It also results in financial loss to individuals and business. Phishing could result in loss of reputation and trust in a business therefore reducing its market. With these effects and others, phishing is something that internet users have to be aware of and everyone must engage in helping to combat it.

References

[1] Anti-Phishing Workgroup (APWG). (2013, 1st Quarter). *Phishing Activity Trends Report.* Retrieved from http://www.apwg.org

[2] Junxiao, S., & Sara, S. (2012). Phishing. Retrieved from http://www.cs.arizona.edu/~collberg/Teaching/466-566/2012/Resources/presentations/2012/topic5-final/report.pdf

[3] Kruegel, C., & Kirda, E. (2005). Protecting Users Against Phishing Attacks. *The Computer Journal Vol. 00 No. 0*. Retrieved from http://www.cs.ucsb.edu/~chris/research/doc/cj06_phish.pdf

[4] Moore, T., & Clayton, R. (2009). Evil Searching: Compromise and Recompromise of Internet Hosts for Phishing. Retrieved from http://www.cl.cam.ac.uk/~rnc1/fc09evil.pdf

[5] Wikipedia. (2013). *Phishing*. Retrieved from Wikipedia: http://en.wikipedia.org/w/index.php?title=Phishing&oldid=484977983,%202012#Recent_phishing_attempts

[6] Digital Family Forum - Workshop, Ministry of Communication, Ghana. 12 March 2014, International Conference Centre – Ghana.