Assistance with University Projects? Research Reports? Writing Skills?

We've got you covered!

www.assignmentstudio.net

WhatsApp: +61-424-295050

Toll Free: 1-800-794-425

Email: contact@assignmentstudio.net

Follow us on Social Media

Facebook:

https://www.facebook.com/AssignmentStudio

Twitter:

https://twitter.com/AssignmentStudi

LinkedIn:

https://au.linkedin.com/company/assignment-studio

Pinterest:

http://pinterest.com/assignmentstudi

INTERNET FRAUD

Research Report on Spear-Phishing

(2070 words)

Student Name:

Student Id:

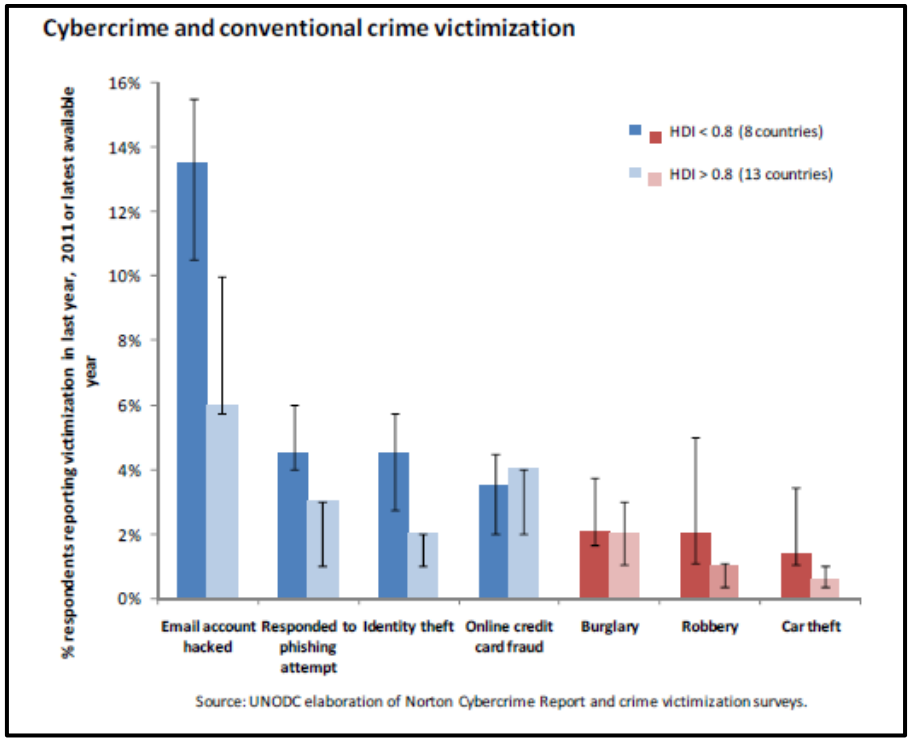
Contents

1.0 INTRODUCTION

1.1 Background

Internet usage has increased significantly over the years. According to UNODC (2013), 2.3 billion people had access to internet in 2011, and in 2017, the number of networked devices will be six times the population. The enhanced proliferation has led to a significant increase in cybercrimes. Since the crime occurs around all around the world (real and virtual), is not easy to put together a standard definition of cybercrime. However, a limited number of acts against the confidentiality, integrity and availability of computer data or systems represent the core of cybercrime. Hacking of email accounts tops the list of victimization, and many cybercrimes involve ***fraud*** committed over internet, like online credit card fraud and illegal funds transfer using ***phishing*** (figure 1) (p. xvii).

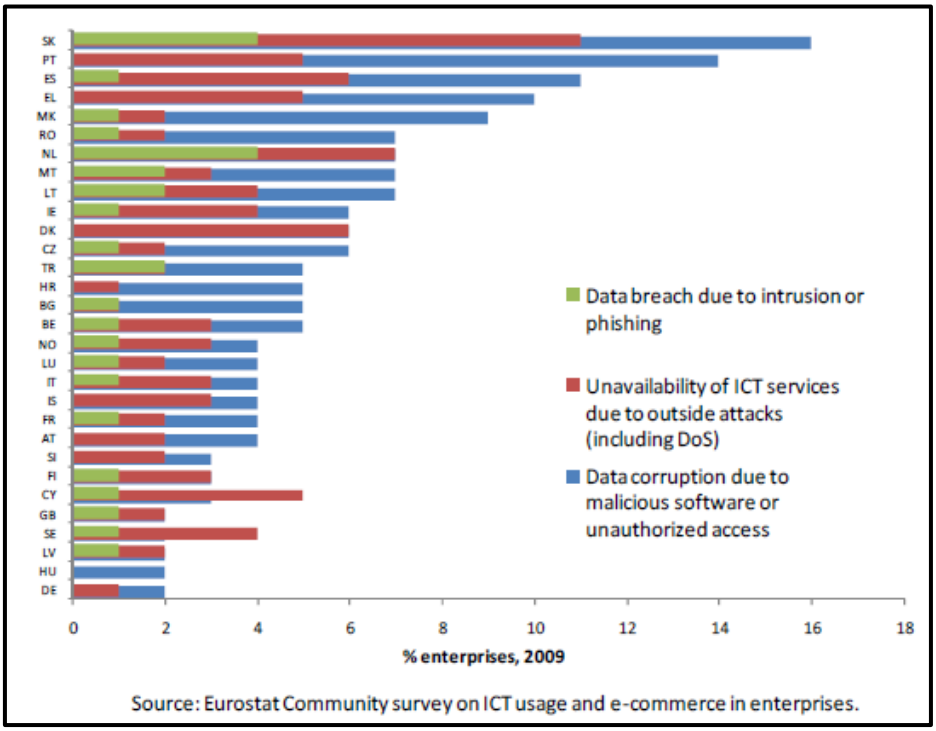
Figure 1



Source: UNODC (2013, p. 28)

According to ECC-Net (2013), Europol estimates that victims lose around €290 billion each year globally due to cybercrime. This makes cybercrime more profitable for criminals than the combined value of global trade in marijuana, cocaine and heroin (p. 5). Private sector organizations are also susceptible to cybercrime, and data breach due to intrusion or phishing is a major problem (pp. 30-31). Merchants in North America alone lost an estimated 1% of their online revenue or $3.4 billion due to fraud (Cybersource, 2012).

Figure 2: Cybercrime and Enterprise Victimization



Source: UNODC (2013, p. 31)

1.2 Internet Fraud & its Common Types

AGD (2011) defines ***fraud*** as dishonestly obtaining a benefit or causing a losses by deception or by using other means. When applied to internet crimes, AFP (2013) defines ***'internet fraud and scams'*** or ***'online fraud'*** as any type of fraud scheme that uses any of the components of internet (email, web sites, chat rooms or message boards) to present fraudulent solicitations, to conduct fraudulent transactions or to transmit the proceeds obtained through such fraud to financial institutions or to others involved in the scheme. According to Kerr, Owen, Nicholls & Button (2013), online frauds include confidence fraud (e.g. mass marketing & romance scams); possessing, making or supplying articles for use in fraud (e.g. computer programs for skimming credit card numbers); phishing and pharming (getting users to transmit personal details or financial information to a fraudulent website); use of malware; SMishing (personal information obtained via SMS); vishing (personal information obtained on telephone); spear-phishing (highly targeted spam emails) and Koobface (messages containing viruses are sent to users via their social media site) (p. 3).

1.3 Internet Fraud - Impact & methods

Apart from financial loss, online fraud causes damage to participants' relationships with others, physical and psychological impact, change in long-term online behavior (e.g. lesser purchases), loss of time and convenience, and reduced trust in society on legitimate online businesses (p. 6). According to KPMG (2013), criminals are using botnets, malware, phishing services, criminal cloud services and hackers available for hire in the cyber underground (p. 18). According to ECC-Net (2013), many frauds which are now committed over Internet have existed in one form or another for many years (p. 23). Online fraud can be related to fake auctions, intentional non-delivery of products, credit and debit card fraud, check fraud, identity theft and phishing (p. 3). According to the survey conducted by KPMG, increased connectivity and use of social media has made Australian businesses more susceptible to cyber-attacks (Stafford, 2013).

This report highlights the dangers posed to businesses by ***spear-phishing***. It examines a real incident involving internet fraud in MOHO, a company in China (Ma, 2013). The incident brings to focus the causes, problems, effects and possible solutions to the menace of Phishing.

2.0 CASE STUDY – SPEAR-PHISHING ATTACK ON MOHO

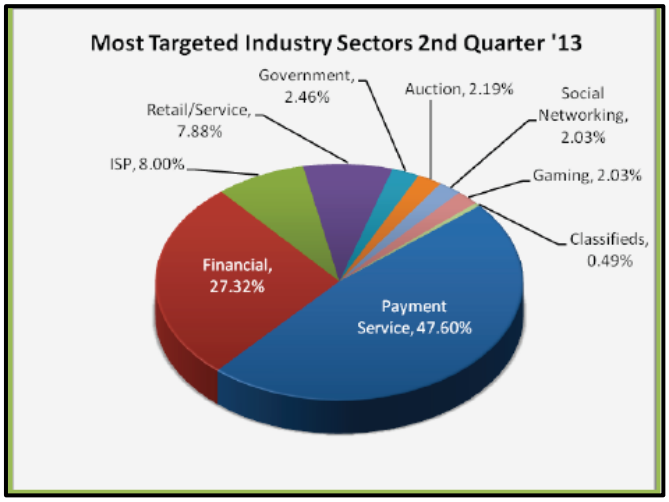
The case of spear-phishing attack on MOHO has appeared in the Journal of Technology Research. Before delving into the details, some basic information about phishing is discussed below.

2.1 Phishing – History, Definition & Statistics

Phishing is a common form of internet fraud which affects consumers and businesses around the world. The term originated in 1996 and referred to the practice of tricking users to disclose information related to America On-Line (AOL) accounts. The information was used to distribute malware. While it disappeared by 2000, a new form of phishing, as we know today, surfaced in 2002 (McCombie, 2008). APWG (2013) defines phishing as a criminal mechanism which uses both social engineering and technical subterfuge to steal data related to consumers' personal identity and financial accounts. Social engineering schemes use deceptive emails purporting to be from legitimate organizations (e.g. banks). These emails are designed to lead consumers to counterfeit websites which trick the recipients into disclosing vital information such as usernames and passwords of their bank accounts. Phishing also uses technical subterfuge schemes by planting malicious software in computers to steal the data directly and

lead users to fake websites. Even authentic websites can be used by the phisher. In such cases he uses proxies controlled by him to monitor and intercept user's keystrokes. USA hosts the most number of phishing websites (pp. 2-3). In April-June 2013, 75% of the phishing attacks were directed towards payment services and the financial sector (figure 3) (pp. 7-8).

Figure 3



Source: APWG (2013, p. 7)

2.2 Spear-phishing

Spear-phishing emails are being increasingly used, and may refer to the targets by their specific name, rank, or position (Trend Micro, 2012, p. 4). Spear-Phishing has a 70% open rate compared to 3% for mass phishing, and half of those who open the email also click on the malicious link. The value of loss per victim is also significantly higher. Such attacks on organizations damage its reputation, and many attacks are not reported to avoid this consequence. Apart from money, phishers target businesses to steal employee personal identity details, intellectual Property, and business partnership relationships information. The geographical area is selected, then profitable industries are identified, and finally the target organization is chosen (Ma, 2013).

2.3 Why MOHO was chosen by the fraudsters?

As mentioned in Ma (2013), MOHO is a small Chinese manufacturer / trader of construction chemicals and also provides professional services like technology know-how transfer and process design. Its sells its products and services to businesses (B2B). International customers make payments to the company using wire transfer (the preferred mode) and letter of credits. The minimum value of the orders is around $30,000. To expand its international presence, the

company advertised itself in B2B marketplaces and other websites. MOHO attracted the attention of spear-phishing fraudsters because small businesses are more vulnerable to such attacks due to weaker internet security. Further, developing countries are also preferred because of weaker security systems. High level of English is not required in the phishing email content to lure the users from these nations. B2B companies, working in competitive environment are preferred. MOHO met all these prerequisites.

2.4 The Steps followed

According to Ma (2013), spear-Phishing of businesses involves a professionally planned, carefully orchestrated, globally distributed, collusive and multistage process. The emails are contextually and technically sound, and hence involve experts from different fields. They use disguised email addresses and hyperlinks. The emails may contain multiple domain names in the header, and the body contains the link which leads to the fake website. The DNS name is similar to the genuine website. The website presents the form in which the unsuspecting users fill their personal or financial details. The filled information is sent to the fraudster's database for subsequent use. The content in the email body is the bait. It usually contains promise for a job or a new sales order or some 'urgent' information for the user or some 'immediate' action required by the user.

In MOHO's case, the phishers, pretending to be a new customer requiring technology transfer services, sent an email to the sales department. The email had fake contact information and the misleading link. Phishers had already created the fake website. The email asked the salesperson to click on the link and fill in his email login information. This was supposed to 'help' him to access the design specimen for which the technology transfer services were required. English was the salesperson's second language, and he was not so knowledgeable about security matters. He took the email on face value and considered it as a sales opportunity. He filled in the information on the innocuous looking fake website, and did not notice issues like long sub-domain name and some inconsistencies in company information. He could not login, so he reported to the phisher about this 'technical' issue. He did not realize that his login details had already been captured by the phisher (Ma, 2013).

As part of the usual modus-operandi, once a higher level partner in a supply chain is phished, lower level are also phished. Business spear-phishing involves exchanges of emails over a longer time, unlike a one-time attempt in the case of phishing of individual accounts. Once the

data is collected through this website, email settings of the user are manipulated for long term access and for searching of other targets in the contacts or correspondence of the emails of the first victim. For this, the 'reply-to' and 'from' settings are changed to suit the fraud plan execution of the phisher. This is exactly what was done in MOHO's case. The Phishers accessed the emails and contacts of the salesperson, and configured the settings to facilitate repeated misuse. The correspondence and the email addresses provided vital details, and the phishers could send fraudulent emails to MOHO's business partners. During normal course of business, the MOHO salesperson contacted a particular customer with whom the company was discussing a $100,000 order. Once the order was finalized, the salesperson's sent an email containing the Proforma Invoice. This was intercepted by the phishers. The customer's account was also phished, and fraudulent emails were sent to him to finalize the order and send the payment to a new bank account (belonging to the phishers). So the phishers received the real emails sent by both parties and send fraudulent emails to both, thereby manipulating the whole system to their advantage. The real parties (MOHO salesperson and the customer), however, believed that they were in direct contact with each other. As with such spear-phishing cases, money was defrauded by the phishers. When the fraud was discovered, and the emails analyzed, it was found that the emails from phishers originated from various countries. This made tracking and detection of the fraud difficult (Ma, 2013).

3.0 DISCUSSION & CONCLUSION

This case highlights that spear-phishers select soft targets, plan in detail, and use highly contextual and targeted content based on the information gathered about the company. The phishers knew that it would be easier to attack a small Chinese business which is trying hard to increase its international presence. They gathered information about the company's business and pretended to be a customer for their services rather than their products. This gave them a reason to ask the salesperson to click on the link to understand the fake customer's requirement (design specification). The average size of the order made the exercise worth the effort. A multi-stage and multi-level process was followed to target MOHO's customers. The existing trust between the parties was exploited.

The above discussion involves understanding internet fraud and gaining a practical perspective by analyzing the case of a Chinese company MOHO which was subjected to a targeted phishing attack. Based on above, it is concluded that internet fraud presents a real threat to businesses. It leads to financial loss, loss of reputation and lowers the trust amongst business partners. It

can also have an adverse impact on employees' morale and health. It is important to educate the members of the organization about the various prevalent methods of internet fraud. Methods like phishing require active participation of the personnel to be successful. So education can definitely reduce the success rate of the phishers. As mentioned in Chhikara, Dahiya, Garg & Rani (2013) corporations should establish corporate policies and communicate them to consumers, provide a way for the consumer to validate that the E-mail is genuine, develop stronger authentication at web sites, monitor the Internet for potential phishing web sites, and use good quality anti-virus, content filtering and anti-spam solutions at the internet gateway (p. 465). To summarize, fighting internet fraud is a continuous and a collaborative effort involving members of the business community, technology experts and society at large. Since internet usage is expected to increase significantly, it is important for all to remain aware of the threats posed by cybercriminals.

References

AFP. (2013). *Internet fraud and scams.* Australian Federal Police (AFP). Canberra. Retrieved from http://www.afp.gov.au/policing/cybercrime/internet-fraud-and-scams.aspx.

AGD. (2011). *Commonwealth Fraud Control Guidelines 2011.* Attorney-General's Department. Australian Capital Territory. Retrieved from http://www.ag.gov.au/Publications/Documents/CommonwealthFraudControlGuidelinesMay2002/Commonwealth%20Fraud%20Control%20Guidelines%20March%202011.pdf.

APWG. (2013). *Phishing Activity Trends Report 2nd Quarter 2013.* Anti-Phishing Working Group (APWG). USA. Retrieved from http://docs.apwg.org/reports/apwg_trends_report_q2_2013.pdf.

Chhikara, J., Dahiya, R., Garg, N., & Rani, M. (2013). Phishing & Anti-Phishing Techniques: Case Study. *International Journal of Advanced Research in Computer Science and Software Engineering, 3*(5), 458-465. Retrieved from http://www.ijarcsse.com/docs/papers/Volume_3/5_May2013/V3I3-0315.pdf.

CyberSource. (2012). *2012 Online Fraud Report - Online Payment Fraud Trends, Merchant Practices and Benchmarks.* CyberSource Corporation. California. Retrieved from https://www.jpmorgan.com/cm/BlobServer/13th_Annual_2012_Online_Fraud_Report.pdf?blobkey=id&blobwhere=1320571432216&blobheader=application/pdf&blobheadername1=Cache-Control&blobheadervalue1=private&blobcol=urldata&blobtable=MungoBlobs.

ECC-Net. (2013). *Fraud in cross-border e-commerce.* European Consumer Centres Network (ECC-Net). Luxembourg. Retrieved from http://ec.europa.eu/dgs/health_consumer/docs/news_20131206_ecc-report-cross-border-e-commerce_en.pdf.

Kerr, J., Owen, R., Nicholls, C. M., & Button, M. (2013). *Research on Sentencing Online Fraud Offences.* Sentencing Council. London. Retrieved from http://www.natcen.ac.uk/media/205369/research_on_sentencing_online_fraud_offences.pdf

KPMG. (2013). *Global profiles of the fraudster White-collar crime – present and future.* KPMG International Cooperative. Switzerland. Retrieved from http://www.kpmg.com/AU/en/IssuesAndInsights/ArticlesPublications/Documents/fraudster-global-profiles.pdf.

Ma, Q. (2013). The process and characteristics of phishing attacks - A small international trading company case study. *Journal of Technology Research*, *4*, 1-16. Retrieved from http://www.aabri.com/manuscripts/131446.pdf.

McCombie, S. (2008). *Trouble in Florida: The Genesis of Phishing attacks on Australian Banks.* Proceedings of the 6th Australian Digital Forensics Conference. Edith Cowan University. Perth Western Australia. December 3rd 2008. Retrieved from http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1047&context=adf.

Patrick Stafford, P. (2013). *Australian businesses have lost $373 million to fraud: Five ways to make sure you're not a victim.* SmartCompany. Victoria. Retrieved from http://www.smartcompany.com.au/finance/30514-australian-businesses-have-lost--373-million-to-fraud-five-ways-to-make-sure-you-re-not-a-victim.html#.

Trend Micro. (2012). *Spear-Phishing Email: Most Favored APT Attack Bait.* Trend Micro, Inc. California. Retrieved from http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-spear-phishing-email-most-favored-apt-attack-bait.pdf.

UNODC. (2013). *Comprehensive Study on Cybercrime*. United Nations Office on Drugs and Crime (UNODC). Vienna. Retrieved from http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf.

Other References – Not Cited

Baker, C. R. (1999). An analysis of fraud on the Internet. *Internet Research: Electronic Networking Applications and Policy, 9* (5). 348-359.

EMC. (2013). *Phishing Kits – The Same Wolf, Just a different sheep's clothing.* EMC Corporation. Retrieved from http://www.emc.com/collateral/fraud-report/rsa-online-fraud-report-012013.pdf.

Experian. (2012). *Fraudster case studies Understanding the mind of a fraudster.* Experian Limited. Nottingham. Retrieved from http://www.experian.co.uk/assets/identity-and-fraud/fraudsters-case-study.pdf.

Kalige, E., & Burkey, D. (2012). *A Case Study of Eurograbber: How 36 Million Euros was Stolen via Malware.* Versafe. Israel. Retrieved from www.cs.stevens.edu/~spock/Eurograbber_White_Paper.pdf.

NW3C. (2013). *2012 Internet Crime Report.* National White Collar Crime Centre. Virginia. Retrieved from http://www.ic3.gov/media/annualreport/2012_IC3Report.pdf.