The International Journal Of Engineering And Science (IJES)
|| Volume || 3 || Issue || 3 || Pages || 35-40 || 2014 ||
ISSN (e): 2319 – 1813 ISSN (p): 2319 – 1805

Exposing Ways and Means of Carrying out Phishing attacks towards Ensuring Confidence in the use of University Portals

[1,] Joshua John, [2,] Dr. S. Z. Bugi
[1, 2,] *Department of Information Technology, National Open University of Nigeria (NOUN)*

ABSTRACT

The Internet was originally developed with little or no security. As governments run test bed for academic research, the user community was co-operative and nobody considered the possibility that one user or group of users would undertake operations harmful to others. The commercialization of the Internet in the early to mid-1990s resulted in the rise of the potential for adversarial interactions. Phishing is a form of online identity theft. Phishers use social engineering to steal victims' personal identity data and financial account credentials. Social engineering schemes use spoofed e-mails to lure unsuspecting victims into counterfeit websites designed to trick recipients into divulging financial data such as credit card numbers, account usernames, passwords and social security numbers. This is called a deceptive phishing attack. In this paper, a thorough overview of Exposing Ways and Means of Carrying out Phishing attacks towards Ensuring Confidence in the use of University Portals, the ways and means by which phishers carry out phishing attacks.

Keywords*- crackers, cybercrime, hackers, identity theft, phishing*

Date of Submission: 13 March 2014 Date of Publication: 30 March 2014

I. INTRODUCTION

Phishing is the electronic means of obtaining personal information by disguising oneself as a legitimate online entity. More specifically phishing is the process of creating a fraudulent email or website that appears to originate from a legitimate source. Phishers, who are authors of phishing websites, create a fraudulent website in hopes that visitors will divulge sensitive information such as account numbers, usernames, passwords, pins, social security numbers, etc. [1]

Phishers mostly target e-commerce websites. Electronic Commerce is defined as "the buying and selling of products or services over electronic systems such as the Internet and other computer networks" [3]. E-Commerce is thus an online application that enables the buying and selling of products or services. This largely occurs between two businesses (called B2B) or between a business and a consumer (B2C). Commerce and business transactions conducted over the Internet make use of supporting technologies such as the World Wide Web, Electronic Data Interchange, Online Transaction Processing, and E-mail to name a few. [11]

As modern E-Commerce continues to evolve, common trends can be identified, such as, the move of the web into more of a collaborative social marketplace facilitating online transactions, increasing user interaction through a more digital or 'virtual' online environment, and the increasing focus on enhancing business services through personalised product and customer information.

However, there are a number of threats that exploit these technologies thereby increasing the risk of conducting business online. Such threats include money theft, fraud, information and identity theft, threats to the system from malicious software, spam e-mail and the invasion of consumer privacy, as well as the theft of intellectual property. [11].

The rapid adaptation of mobile devices and wireless networks has increased the grounds for newer and much more organized forms of cybercrime. With highly sophisticated and targeted security attacks becoming the norm, 'Phishing' has become one of the most commonly employed techniques to spread malware. Unlike other popular attack vectors, phishing requires very little technological capital. Today phishing is quite a serious problem as it affects not only people but also the organization that the victims work for. Phishing attackers can target unsuspecting employees to access the critical company details. [5]

II. LITERATURE REVIEW

From the beginning, Internet lives on indirect monetization through advertisement on the portals of the services being offered. Starting from Search, Internet Mail, News, Blog, Social Networking, VoIP, File Sharing all and every services had been on offer for absolutely zero cost to end user other than cost to buy the bandwidth for the Internet, It must be noted, here that many effort to offer Internet services e.g., News service as paid subscription did not find much taker.[7]

As with the normal, non-fraudulent user, privacy is also important to the fraudster. The internet is an excellent platform to be anonymous or pseudo-anonymous. Most of the online hackers/crackers/Phishers maintain their anonymity/pseudo-anonymity, which is of a major concern since this makes tracking them virtually impossible. There are 3 major aspects to this:

- Identity abundance
- Identity confusion
- Location neutrality [13]

2.1 Identity abundance – opportunity to have as many identities**:** The motivation of internet was such that it allowed any one to be connected to the network, without actually verifying the identity of the user. This was seen as a major step in getting the world together, on the platform called web, where users from any background could interact. Since monetization on the internet is through advertisement, the service providers like Hotmail to Skype to Facebook - all had their valuations tied to the registered number of subscribers in their database. This economic model obviously does not promote any reasonable degree of subscriber identification mechanism beyond what is needed for running the basic services. On the contrary, this model encourages end users to open and use as many account as they prefer, as that inflates the possible valuation of that service provider.[18] This situation where user is allowed to have as many identities leads to what is called "Identity Abundance" and is surely a new security problem that will bother the security professional for quite some time. Some of the major issues with identity abundance are to map each online identity of a person with the real life identity is almost impossible.

2.2 Identity Confusion: Opportunity to have any identity**:** One inherent problem of services on the internet is that they don't have strong method for user identification. For example in Skype any user can assume any identity without any problem so long that identity is available in that service provider's domain. This capability of user to assume such arbitrary identity (say GoodluckJonathan@Skype.com, PresidentOfNigeria@skype.com, etc.) of their choice may confuse any remote party in conversation or transactions with the users of such assumed identity. This is what is called identity confusion. Nevertheless, this model allows one to assume any other identity of one's preference creating a situation of virtual-identity-theft. This in particular may cause serious problem in context of communication based services e.g. Gmail, IM, Facebook, Skype etc. convincing remote party through the assumed identity forcing into acts of disgrace. This " Identity Confusion" is a serious problem and may retard the growth of Internet services beyond certain level.

2.3 Location neutrality: On the internet, the unique source of tracing a PC is by its Internet Protocol (IP) address. This appears to be a fool proof way of tracing anyone on the internet, but as with other crime areas, internet criminals are smart enough to find ways to beat this security aspect by leaving multiple traces of different IP addresses. Moreover, Even though the IP mapped location databases are reasonably accurate, they are far from deterministic as we are used to in case of legacy telephone network [PSTN or GSM/CDMA].

Moreover, cybercrimes encompass a broad range of activities. Generally they can be classified as the ones that target the computer devices or networks directly and the ones whose prime target is independent of the computer device or network. The types of crimes that target particular network or devices are Denial of Service attacks (DoS), Malware or malicious code, computer viruses, Trojans and so on. Apart from such a classification there are several methods of attacks such as,

Web Vandalism**:** I s the willful, voluntary, and malicious destruction or damage of the property of others. In this attack a cyber- criminal gets the access to the target website, and changes the visual appearance of the target website. This is also known as website defacement, and is generally harmless; however it can be used to cover up more evil actions like uploading malware.[16]

Cyber Espionage**:** Is the act or practice of obtaining secrets without the permission of the holder of the information. This is an act of acquiring secret from individuals, rivals, governments, rivals and so on using certain exploitation methods. It is usually carried out for unethical and illegal strategic advantage and or psychological, political and physical subversion activities and sabotage.

Denial of Service Attack (DoS): DoS or Distributed DoS (is an effort to make one or more computer systems unavailable) an attempt to make a computer resource unavailable to the intended user. The most common method of carrying out this attack involves saturating the victim machine with excessive external communication requests, so that it cannot respond to legitimate traffic or responds so slowly that is rendered effectively unavailable. The most common victims of such an attack are servers hosted on high profile web servers such as banks, credit card payment gateways and even root name servers.[14]

Spams: Unsolicited means that the Recipient has not granted verifiable permission for the message to be sent. Spam accounts for over 100 billion messages each day, which is approximately 85 percent of email sent worldwide. Such a huge number definitely eats up a lot of computer resources. Spammers continue to improve the design and content of the spam e-mails, to make it appear more legitimate and professional. Spammers hardly use computers in their physical possession to send out the bulk of spam, instead they rent botnets.[13]

Malware/Crimeware: Computer programs designed to infiltrate and damage computers without the users consent. Most modern malware is designed to help attacker gain control over victim's computer, device or a network. Certain malware changes the way the infected computer works. It might force the terminal to connect to the internet and download additional malware. In addition it might also search for sensitive information. [7]

Botnets: Is a large number of compromised computers that are used to generate spam, relay viruses or flood a network or Web server with excessive requests to cause it to fail. Most of the current malware is used to deploy the huge botnets. Botnets consist of thousands of compromised computers and have become the basis of the of large scale online criminal activity. People controlling the botnets typically rent out the botnets to send out bulk of spam or carry out other online crimes.[8]

The above mentioned are a few categories of crimes on the internet. This study shall highlight the impact of one of the crimes, 'Phishing', which can be classified as cyber espionage or as spam, since the attack typically begins with a fake e-mail. Online applications have been plagued with problems since their inception and this study examines one of these problems: The lack of user trust in online applications created by the risk of phishing.[9] The growth and advancement of technology has not only benefitted honest Internet users, but has enabled criminals to increase their effectiveness which has caused considerable damage to this budding area of commerce. Moreover, it has negatively impacted both the user and online business, by breaking down the trust relationship between them.

The severity of this problem can be seen in the statement that phishing has increased by 8000% over the period January 2005 to September 2006 (APACS, 2007). Also, the Anti- Phishing Working Group (the leading, worldwide, anti-phishing law enforcement association) reported that in August 2009, the number of unique phishing websites detected by the Anti-Phishing Working Group reached an all-time high of 56,362, this being a 1.3 percent increase on the previous record of 55,643 in April 2007 [11].

III. OBJECTIVE

This research project aims to investigate a problem within E-Commerce as there is a significant lack of user trust and confidence between both the user and the E-Commerce business created by escalating information security breaches such as phishing attacks or its modifications, such as pharming. The study attempts to firstly, provide a better understanding of the threat of phishing that creates online risk and a lack of confidence in E- Commerce. Secondly, it hopes to contribute to the efforts of reducing this risk by building confidence and enhancing the user's protection.

IV. METHODOLOGY

This study was a descriptive survey type where interviews were conducted with some stake holders who are selected members of academic and non-academic staff, students ICT staff of Ahmadu Bello University, Zaria, as well as questionnaires administered on same stakeholders of the same University. The population of the research comprises of the above listed stake holders of the portal for Ahmadu Bello University, Zaria who are directly involved in either the design and development, or usage, of the Students' Registration Portal.The sample for the study is 250 comprising of 120 male students and 100 female students selected from the faculties of the University where the study was conducted, 10 members of academic and non-academic staff who are not working in the ICT section and 20 ICT staff. A Purposive Random sampling Technique was used to select among males and females.

The selection of the students was based on computer and internet literacy in order to actually involve those students who have the capacity to use the Internet. This is because a good number of students interact with the portal by proxy, since they do not have the requisite computer knowledge to use the portal. As for the ICT staff, only those involved in the design and development of the portal were included in the sample. The sample size for students was limited to 220 students for easy administration of the questionnaire. Ten (10) members of staff involved in the design and development of the portal were also interviewed and likewise, 20 ICT staff were interviewed.

Purposive sampling was utilized for the purpose of this research, as it targets a particular group of people (those that use computers and the internet). This is a form of non-probability sampling in which decisions concerning the individuals to be included in the sample are taken by the researcher, based upon a variety of criteria which may include specialist knowledge of the research issue, or capacity and willingness to participate in the research. Some types of research design necessitate researchers taking a decision about the individual participants who would be most likely to contribute appropriate data, both in terms of relevance and depth as already explained in the section above. In selecting the sample for the students, (male & Female) simple purposive random sampling technique was used. In this method, each member of the population, has equal chances of been selected in the sample.

A Structured Questionnaire which is a series of written questions a researcher supplies to subjects, requesting their response was used for soliciting information from respondents regarding Exposing Ways and Means of Carrying out Phishing attacks towards Ensuring Confidence in the use of University Portals. . It is an inexpensive method that is useful where literacy rates are high and respondents are co-operative. Questionnaires can be open or close ended. Open ended questions allow for a space for the respondent to make any comments he or she wishes to make on the course while a close ended question restrict responses to prescribed ones. A second method that was employed along with structured questionnaire was **Interview Guide which** is a form that is completed through an oral interview with the respondent. More expensive than questionnaires, but they are better for more complex questions, low literacy or less co-operation.

V. RESULTS

What are the ways and means by which phishers carry out phishing attacks?
Phishing attacks according to the result of this study are carried out through several ways, however the prominent ones comprise:

5.1 Emails

Often victims fall prey to phishing due to spam emails, these being most common methods of luring a victim to the fake website. Phishers generally send out such specially crafted emails to millions of legitimate users, having live email accounts, within a few hours. Most of these addresses are purchased from the same source as the conventional spam (Gunter, 2009). Many of the recipients of these emails are not even the customers of the spoofed companies and may realize that that the email is a fraudulent one and ignore it; however the Phishers rely on the few naive users, who are the customers of the spoofed organization and fall prey to the attack. To make sure that the innocent user doesn't suspect the email to be fraudulent one, the text of the email should be legitimate. The attacker create these plausible conditions by a message such as account suspension, failed transaction or even upgrading of the user account to the newly installed security feature (Christine et al, 2004). Along with the challenge of convincing the user about the genuineness of the email another challenge is that the email should also pass the spam filters of the mailboxes.Once the user clicks the link in the email, he is automatically taken to the fake, phishing, and site. The site may or may not be displayed by the browser depending upon a number of heuristics used by the browser to detect phishing. These heuristics rely on a lot of parameters. If the browser fails to identify the fake website or if the user overrides the browsers decision and continues with the process, he is tricked into entering his credentials. The credentials might be stored as a plain text file or can be sent as an email to the attacker. These attackers usually sell these credentials to other agents commonly referred to as cashiers who empty the bank accounts of the users [16].

We demonstrate a step by step phishing attack.

As mentioned previously the first step in Phishing is to successfully send an email which is convincing enough for the user as well as it escapes the spam filter.

Phishing is to successfully send an email which is convincing enough for the user as well as it escapes the spam filter. Once the user clicks on the link in the email he is taken to a spoofed webpage. i.e. fake web site. The phisher then ask the credentials (information of the victim) finally, after getting the victim’s information, then, the crime is carried out.

5.2 Identity abundance – opportunity to have as many identities: The motivation of internet was such that it allowed any one to be connected to the network, without actually verifying the identity of the user. This was seen as a major step in getting the world together, on the platform called web, where users from any background could interact. Since monetization on the internet is through advertisement, the service providers like Hotmail to Skype to Facebook - all had their valuations tied to the registered number of subscribers in their database. This economic model obviously does not promote any reasonable degree of subscriber identification mechanism beyond what is needed for running the basic services. On the contrary, this model encourages end users to open and use as many account as they prefer, as that inflates the possible valuation of that service provider. This situation where user is allowed to have as many identities leads to what is called “Identity Abundance” and is surely a new security problem that will bother the security professional for quite some time. Some of the major issues with identity abundance are to map each online identity of a person with the real life identity is almost impossible.

5.3 Identity Confusion: Opportunity to have any identity: One inherent problem of services on the internet is that they don’t have strong method for user identification. For example in Skype any user can assume any identity without any problem so long that identity is available in that service provider’s domain. This capability of user to assume such arbitrary identity (say GoodluckJonathan@Skype.com, PresidentOfNigeria@skype.com, etc.) of their choice may confuse any remote party in conversation or transactions with the users of such assumed identity. This is what is called identity confusion. Nevertheless, this model allows one to assume any other identity of one’s preference creating a situation of virtual-identity-theft. This in particular may cause serious problem in context of communication based services e.g. Gmail, IM, Facebook, Skype etc. convincing remote party through the assumed identity forcing into acts of disgrace. This “ Identity Confusion” is a serious problem and may retard the growth of Internet services beyond certain level.

5.3 Location neutrality**:** On the internet, the unique source of tracing a PC is by its Internet Protocol (IP) address. This appears to be a fool proof way of tracing anyone on the internet, but as with other crime areas, internet criminals are smart enough to find ways to beat this security aspect by leaving multiple traces of different IP addresses. Moreover, Even though the IP mapped location databases are reasonably accurate, they are far from deterministic as we are used to in case of legacy telephone network [PSTN or GSM/CDMA].

VI. CONCLUSION

Phishing is the electronic means of obtaining personal information by disguising oneself as a legitimate online entity. More specifically phishing is the process of creating a fraudulent email or website that appears to originate from a legitimate source. As with the normal, non-fraudulent user, privacy is also important to the fraudster. The internet is an excellent platform to be anonymous or pseudo-anonymous. Most of the online hackers/crackers/Phishers maintain their anonymity/pseudo-anonymity, which is of a major concern since this makes tracking them virtually impossible. They do this through 3 major aspects means:

E-mails
Identity abundance
Identity confusion
Location neutrality

VII. RECOMMENDATIONS

7.1 Emails:

Once there is a spam user should not click on the link in the email because he will be taken to a spoofed webpage. i.e. fake web site. The phisher then ask the credentials (information of the victim) at this juncture the user should not supply any personal information because the final action by the phisher will be, getting the victim’s information, to use for the purpose of carrying out the crime.

7.2 Identity abundance

First and foremost every portal should be protected from Identity abundance, It is observed that a good number of students have their registration done to them by others, mostly in public internet cafés where they sublet some key information about themselves and their records to people they do not know and whose character they cannot vouch for. The University should do more to make all students computer literate and also provide internet services to all nooks and crannies of the University.

Portals should educate all users about Identity confusion that is often created by the phishers.

7.3 Identity Confusion:

This means opportunity to have any identity One inherent problem of services on the internet is that they don't have strong method for user identification. For example in Skype any user can assume any identity without any problem so long that identity is available in that service provider's domain. This capability of user to assume such arbitrary identity (say GoodluckJonathan@Skype.com, PresidentOfNigeria@skype.com, etc.) of their choice may confuse any remote party in conversation or transactions with the users of such assumed identity. This is what is called identity confusion. Nevertheless, this model allows one to assume any other identity of one's preference creating a situation of virtual-identity-theft. This in particular may cause serious problem in context of communication based services e.g. Gmail, IM, Facebook, Skype etc. convincing remote party through the assumed identity forcing into acts of disgrace. This " Identity Confusion" is a serious problem and may retard the growth of Internet services beyond certain level.

7.4 Maintain Location neutrality on the portal:

On the internet, the unique source of tracing a PC is by its Internet Protocol (IP) address. This appears to be a fool proof way of tracing anyone on the internet, but as with other crime areas, internet criminals are smart enough to find ways to beat this security aspect by leaving multiple traces of different IP addresses. Moreover, Even though the IP mapped location databases are reasonably accurate, they are far from deterministic as we are used to in case of legacy telephone network [PSTN or GSM/CDMA].

VIII. FURTHER STUDIES

A study on how to identify spam emails that are fake should be carried out to educate portal users properly.

REFERENCES

[1] Christine E. D., Jonathan J. O. and Eugene J. K. (2004). "Anatomy of a Phishing mail", First Conference on Email and Anti-Spam (CEAS). *2004* Proceedings

[2] FBI (2007). *Something Vishy, Be Aware of a New Online Scam* 2007

[3] Gunter, O. (2009). "The Phishing Guide, Understanding & Preventing Phishing Attacks", Next Generation Security Software

[4] http://cloudmark.com/en/home.html

[5] http://crypto.stanford.edu/SpoofGuard/

[6] http://en.wikipedia.org /wiki/Malware# Characteristics_of_data- stealing_ malware

[7] http://en.wikipedia.org/wiki/Pretty_Good_ Privacy

[8] http://en.wikipedia.org/wiki/Two-factor_ authentication

[9] http://pages.ebay.com/eBay_toolbar/index.html

[10] http://toolbar.netcraft.com/

[11] Anti-Phishing Working Group. http://www.antiphishing.org/, 2009

[12] http://www.passmark.com/

[13] IETF RFC: The TLS Protocol, http://www.ietf.org/rfc/rfc2246.txt

[14] James, L. (2005) *Phishing Exposed*. Oct., Syngress

[15] Rachna, D., Tygar, J. D. (2005). **"**Phish and HIPs: Human Interactive Proofs to Detect Phishing Attacks", In Human Interactive Proofs: Second International Workshop (HIP 2005)

[16] Rob T., and Jerry, M. (2010). "The underground economy: priceless"

[17] Shah, J. (2007) *Online Crime Migrates to Mobile Phones.* Sage, April. **1**(2).

[18] Yue Zhang, S.E., Lorrie C., and Jason H. (2007). *Phinding Phish Evaluating Anti-Phishing Tools*. In *14th Annual Network & Distributed System Security Symposium (NDSS 2007).* San Diego, CA.