PHISHING AWARENESS AMONG STUDENTS IN TERTIARY INSTITUTION

Mukhtar Umar Bagarawa
Ummaru Ali Shinkafi Polytechnic Sokoto
Mukhtar.bgw@gmail.com
Abba Nasir Mu'azu
Nigeria Deposit Insurance Corporation (NDIC)
Mansur Aliyu
Sokoto State University

ABSTRACT

There was reportedly $13.2 billion dollar in losses to phishing attacks during 2018 and the number of attacks is everyday increasing particularly among the younger generation of less than 40 years of age. The purpose of this study was to identify the level of student awareness related to specific phishing tactics. Findings revealed that while students are unlikely to provide personal information in response to an email/SMS request, they can be easily tricked by numerous other tactics. This paper reports the findings of the study in addition to listing suggested points to employ for creating phishing awareness. According to Kumaraguru et al; Education is the most powerful tool available for combating the growing phishing security threat and student vulnerability.

Keywords: Phishing, Awareness, Students, Tertiary, Institution, Nigeria.

INTRODUCTION

There has been a rapid growth of knowledge and technology over the past centuries. During the twenty-first century, information handling has become more important, as the technology of collecting, processing and distributing information has become important. In addition to these innovations, including large telecommunication networks. Meanwhile the Internet is no longer simply a means of gathering and sharing information, serving economic needs and providing education and entertainment, but is now an indispensable part of the daily life of people in their public and private affairs, assisting them in crucial day-to-day decisions, often with financial links.

As a result, thieves have quickly found that the Internet offers them a superior environment in which to carry out their attacks on a still vulnerable society and this has led to the appearance of electronic fraud, the so-called e-fraud. However, with the massive development in security and countermeasures, e-fraud fraudsters have found difficulties in perpetrating their attacks. Therefore, those thieves have thought of ways of bypassing the sophisticated security controls and measures by shifting their focus on people to commit their crimes.

Since thieves believe that people are the weakest link in the security chain of any organisation, no matter how sophisticated its security controls, cyber criminals are currently moving to exploit people in committing their offences (Symantec, 2006). Thieves have always known that the best way around any security system is to manipulate a human being into giving them what they want, and this is what people in the IT field refer to as ‘social engineering’ (Gartner, 2002a), Hence, several kinds of attack against people have emerged, of which phishing is a paradigm.

This research was designed answer the following questions:

1. What is the level of awareness of college students regarding phishing tactics and results?
2. How do students react to specific phishing tactics?
3. Is there difference in ways students of differing demographics react to specific phishing tactics?

PREVIOUS RESEARCH ON PHISHING ATTACKS

Phishing: is a type of social engineering attack and takes the form of an online identity theft which targets people to gather personal and confidential information such as username and password to commit a crime in the name of the true owner which could cause the victim negative consequences (Bielski, 2004; Litan, 2004).

Types of Phishing

Phishing has been categorised by many researchers from different perspective, but the most common types are the ones adopted by Mariam Khalid Al-Hamar 2010 and Pranit R. Thite1, Ganesh Suryawanshi2, Prof. A. M. Ingole in their various research Mariam Khalid Al-Hamar (2010) categorised the phishing by considering the communication channels of which phishing is carried out as follows: Pharming, Google phishing, Wi-phishing, Vishing, SMishing, Phishing scams and Spear phishing, Phishing could also be executed through Deception, Malwares, Keyloggers, Screen loggers, Session Hijacking, Web Trojans, Hosts File Poisoning, System Reconfiguration Attacks, Content-Injection, Man-in-the-Middle and Search Engine 1997 was the first occasion when the media demonstrated phishing and its threat (Ollmann, 2004), Since then, phishing attacks have subsequently increased dramatically. The majority of researchers have considered phishing as a formidable attack facing online consumers (Herzberg, 2008; APWG, 2006; Consumer Reports, 2006; Gartner, 2005; Pruitt, 2005). Accordingly, this has provided the motivation to focus on phishing as a research area.

Dhamija et al. (2006) conducted the first published study of phishing. In the study, each participant was shown 20 websites, some real and some fake, and was asked to determine whether each given site was legitimate or fraudulent. For sites that they determined to be fraudulent, the participants were also asked to give their reasons for their decisions. The study found that well designed phishing sites fooled over 90% of the participants. Following the work of Dhamija et al. many other researchers led similar studies which show that the findings of Dhamija et al. continue to hold and users remain vulnerable to phishing (Hong, 2012). Downs et al. (2006) conducted the first study of phishing messages (as opposed to phishing websites) and how users respond to them. Just as in the case of judging websites (Dhamija et al., 2006), the study of Downs et al. found that users often base their judgments of messages on incorrect heuristics. Users fall particularly for spear phishing, which involves messages sent to a specifically targeted group, such as members of a community, employees of an organization, or customers of a business. The findings of Downs et al. were confirmed in the work of Jagatic et al.

(2007), which showed that people were 4.5 times more likely to fall for social phishing, i.e. phishing sent from an existing contact, than standard phishing attacks, and it is for this reason that criminals heavily target online social networking sites.

Financial Damages Caused by Phishing

Phishing exerts both direct and indirect cost to the society. Examples of direct loss include consumers losing money, and banking fraud, etc. Examples of indirect cost include erosion of consumer trust of the Internet, negative impact to businesses' brand, an increase in service call centre complaints volume etc. Estimating either cost is hard, as there are many stages of the attack and it is difficult to collect good data. Three reports attempted estimating direct costs. Gartner Research conducted a survey of 5000 Internet users in August 2006 asking whether consumers have received, clicked or given information in phishing emails. Based on this survey, they estimated that 24.4 million Americans have clicked on a phishing e-mail in 2006, while 3.5 million have given sensitive information. They calculated that the economic loss be 2.8 billion dollars in 2006 (Gartner 2006). A follow up survey in 2007 with similar methodology estimated that 3.2 billion dollars is lost in 2007 (Gartner 2007). The above studies rely on people's survey responses. Psychology literature has shown that there is often a wide discrepancy between people's stated choices and their actual behaviour. Moore and Clayton empirically studied phishing websites using Phish Tank data. They found that a phishing site lives for 61 hours on average. Using the web log data of some of these phishing sites, they estimated that on average 18 users would fall for phishing on the first day when the site was up, and subsequently 8 users per day afterwards. The total cost to consumers per year was estimated around 320 million dollars (Moore, and Clayton, r. 2007).

RESEARCH METHODS

This study was designed to identify the current level students' knowledge of phishing in order to determine their vulnerability. Students, in other words youth as established by other researchers- see excellent research of Gibson (Gibson 2013)-, are viewed as easy prey by phishers which makes them vulnerable at a time when finances are generally stretched thin. Furthermore, students based their decision on to visit a web or not on its fantasy and beautiful vie as established other research (Dhamija 2006). Therefore understanding the level of awareness among this class of people and their the factors that guid their actions will help in designing better awareness program which will help in reducing the phishing vulnerability

One Hundred and Forty-Two questionnaires were distributed among students of Ummaru Ali Shinkafi Polytechnic Out of which 137 were retrieved and 8 were discarded because of their incompleteness the questionnaire contained demographic data and awareness questions rated on a five-point Likert scale ranging from very unlikely (1) to very likely (5).

RESULTS AND FINDINGS

The following tables presents the finding for the group as a whole. The percentages in the response column for the first questions indicate the percent of students who would engage in risky behavior based on the occurrence of the event described in the "Item" column. Risky behavior was defined as not being very likely or likely to have engaged in safe behavior. Thus, the higher the percentage, the greater the risk to the individual and to the organizations with which the student has a relationship.

Table 1: Smartphone use

S/N	QUESTION	
1	Smartphone as a means of accessing Internet	90%
2	Students with email Address	100%
3	Students that knows at least 3 ways of defense against Phishing	36%

Smartphone in this part of country is mostly the means of accessing internet and emails particularly among students in tertiary with 90% of smartphone reliability in accessing internet and email. But unfortunately, only around 1/3 of them can mention three ways of defence against phishing even if they never apply for them. Below is the interpretation of the results from Table 2.

1. Question 1 indicate that 52% of the students will voluntarily render their information to an email or SMS that ask for their account information, an action that can pose a big threat to the security of cyber.

2. Spear Phishing which is addressed to the potential victim is known to be among the highest means of phishing in the world, even though its hard to gather the necessary information to achieve that, its agreed by most of the respondents that its usually legitimate.

3. 62% of the respondents agreed that when the email or SMS directs to a website with SSL certificate and the name of the sending organisations, then its legitimate. But the name and the https must be meticulously checked to verify its certainty. Because fraudsters use other means to manipulate those security barriers.

4. It was expected that students will understand the simplest characters of phishing messages, which is urgency and need for quick response. But only 45% of them consider a message with some urgency as a phishing message.

5. in most cases messages classified as junked or spam by email providers has some security concern attached to it. But unfortunately, only 50% of the students classified it phishing

6. 20% are sceptical on whether or not to visit the link which their browser warned them that it may contain some virus attachments. The worst is that 30% of them do even consider it as legitimate. Only 49% of them classified it as phishing related messages

7. https with padlock signs are two common sign one should pay attention to when visiting any website but only 56% of the respondents were aware of that. Meaning the remaining 44% are vulnerable to unsophisticated phishing attacks.

8. Some phishing SMS supplied phone numbers whom they claim are representative that will help the victim rectify their issue but they instead dupe the victims to either send them money or supply them with confidential information about their financial addresses.

Table 2: Phishing vs Legitimate

S/N	Question	Real Situation	% indicating its phishing	%indicating its legitimate	% Not sure
1	If an SMS/email Asks you to enter information about your account	Phishing	48%	52%	Nil
2	If an SMS/email addresses you by your first and last names	Legitimate	63%	30%	7%
3	If an SMS/email directs you to a website containing a security certificate matching the name of the website.	Legitimate	62%	33%	5%
4	If an SMS/email conveys sense of urgency and surprise	Phishing	45%	55%	Nil
5	If an SMS/email classified as junk or spam mail by your e-mail system (e.g Yahoo, Gmail or Hotmail)	Phishing	50%	42%	8%
6	If an SMS/email contains attachment of which your browser is notifying you that it might contain viruses that could harm your computer.	Phishing	49%	31%	20%
7	If an SMS/email directs you to website with URL starting with https	Legitimate	36%	56%	8%
8	If an SMS/email asks you to call the phone number supplied in the e-mail.	Phishing	62%	30%	8%

Table 3 reports the differences between male and female respondents. On all items except number 3 and 7, males are more cautious although, once again, they tend to make poor decisions that make them vulnerable. F do not come into play in the differences found in this table.

Table 3: differences between male and female respondents

S/N	Question	Real Situation	% indicating its phishing		%indicating its legitimate		Right
	GENDER OF RESPONDENT		M	F	M	F	
1	If an SMS/email Asks you to enter information about your account	Phishing	28%	20%	22%	30%	M
2	If an SMS/email addresses you by your first and last names	Legitimate	33%	30%	20%	10%	M
3	If an SMS/email directs you to a website containing a security certificate matching the name of the website.	Legitimate	32%	30%	13%	20%	F
4	If an SMS/email conveys sense of urgency and surprise	Phishing	35%	10%	25%	30%	M
5	If an SMS/email classified as junk or spam mail by your e-mail system (e.g Yahoo, Gmail or Hotmail)	Phishing	40%	10%	22%	20%	M
6	If an SMS/email contains attachment of which your browser is notifying you that it might contain viruses that could harm your computer.	Phishing	29%	29%	13%	20%	M
7	If an SMS/email directs you to website with URL starting with https	Legitimate	26%	10%	26%	30%	F
8	If an SMS/email asks you to call the phone number supplied in the e-mail.	Phishing	52%	10%	20%	10%	M

CONCLUSION

The respondents of this study did not demonstrate a good understanding of the inadvisability of responding to emails from what appears to be a financial organization. These results emphasize the need for education on phishing. Academicians have the opportunity to send informed consumers into the workforce where they can protect not only themselves but their organizations. In order to adequately prepare and motivate students to increase their level of awareness, there need to be sensitization agenda not only on how to recognize phishing emails and fraudulent websites but also on the cost and magnitude of the phishing problem. Students need to understand the ripple effect caused by this phenomenon. Students need to understand the significance of the types of information that can be obtained by phishers. Over-reliance on technical solutions for protection is dangerous but common. The best defense is a continuing education program. Phishers will not stop generating new ideas nor will they cease to communicate or sell information to each other over the web; thus, greater numbers of attacks are facilitated. Money is readily available by defrauding those foolish enough to fall prey to the latest scam. Sometimes the latest scam is actually an old trick revamped for a new purpose. Take, for example an email attachment. Anti-virus software has become sophisticated enough to catch and eliminate infected attachments as a major concern but now the same scheme is being used to deliver spyware and key-loggers to systems. The results of this study revealed that 51% of the respondents may open an attachment they were not expecting without verifying that it had been sent by a friend

In the meantime, many authors such as Sheng and Kumaraguru found that good educational materials reduced participants' chance of falling for phishing by 40%. Since lack of knowledge is the primary reason why users fall for phishing, many researchers studied the effects of education and training in helping users prevent phishing. Kumaraguru et al. found that simplifying anti-phishing materials to users is ineffective, as people are used to receiving and ignoring such warning. They found that users learn more effectively in embedded training, where users are presented training materials after they fall for an attack. they developed an embedded training system called PhishGuru which periodically sends simulated phishing messages to users in training, and when users fall for such a message, they receive an intervention message that explains to them that they are at risk for phishing attacks and teaches them how to protect themselves against phishing. Study showed that with this approach, participants' chance of falling for phishing reduced by 45%, even one month after the training. Sheng et al. developed an educational game called Anti-Phishing Phil that teaches users basic security concepts related to phishing, and then tests users on what they learned (Sheng et al., 2007; Kumaraguru et al., 2010). Studies showed that this approach improved novices' ability to identify phishing by 61%.

RECOMMENDATIONS

The result this study reveals that students are not that aware of simple tactics for self defence against phishing, that is we prepare the following recommendations.

1 Things to look for in scam email and websites

- An "official" looking sender's email address which is easily altered
- Generic email greeting – Dear User indicates mass mailing
- False sense of urgency – threats that your account is in "danger" are typically fraudulent
- Key phrases such as "Verify your account"
- Fake links – move the mouse over the link to see if the URL changes
- Slightly altered URLs – i.e. www.micosoft.com instead of www.microsoft.com
- Links containing the @ symbol – characters preceding the @ will be ignored
- Out-of-place lock icon – should appear on status bar not the web site window

Security certificate – double click on the lock icon to display the security certificate. If the certificate does not appear, the lock is counterfeit. (Recognize Phishing Scams and Fraudulent Emails, 2008)

2. How to handle suspicious email

- Do not respond
- Check http://www.millersmiles.co.uk/ to search for the email
- Report it to
    - The Anti-Phishing Working Group at http://www.antiphishing.org/

- NITDA, EFCC, ICPC and other related agencies
- The organization that the email appears to be from – i.e. Bank, Jumia, etc.

3. What to do after responding to a phishing email

- Report the incident
- Change passwords on all online accounts
- Routinely review credit card and bank statements for fraudulent activity
- Use the latest anti-phishing products and services.

(Recognize Phishing Scams and Fraudulent Emails,2008)

4. Take a proactive defense

- Check http://www.millersmiles.co.uk/
- Review daily scam updates
- Search for specific emails
- Read the latest news regarding phishing
- Implement a combination of the most current security technology and safe user practices
- Install, update, and maintain firewalls and intrusion detection software
- Use the latest browser and security patches
- Practice awareness
- Never email financial or personal data
- Open attachments only from trusted sources – verify

(Botnet threats and solutions: Phishing, 2006)

- Don't click links – phishers can display a fake URL in the address bar on the browser
- Type addresses directly into the browser or use personal bookmarks
- Verify security certificates by double clicking on yellow lock (Recognize Phishing Scams and Fraudulent Emails, 2008)
- Know Internet Explorer 7 colors
  - Red – phishing site that has been reported to Microsoft
  - White – page that is not supposed to ask for or display personal information
  - Yellow – suspicious website – may be fraudulent
  - Green – certified safe
- Remember that technology alone cannot protect users and organizations from phishing
- Educate family, friends, and coworkers

Phishing attacks are growing more numerous each day. As long as there are artists and people foolish enough to fall for their scams, phishing will be a problem. In other words, phishing is likely here to stay and the most powerful tool for combating the threat is education. It is up to educators to stem the phishing tide. (Bailey, et al 2018)

REFERENCES

Alun, M., Potter, C., and Beard, A. (2006) *Information security breaches survey 2006,* Retrieved February 26, 2008, from http://www.pwc.co.uk/pdf/pwc_dti-fullsurveyresults06.pdf

Bagarawa M. U. (2019). Investigating the risk of phishing among students in tertiary institutions

Berghel, H. (2006). Phishing mongers and posers, *Communications of the ACM* , 49,4, 21-25.

Botnet threats and solutions: Phishing. (2006) Retrieved February 25 from http://us.trendmicro.com/imperia/md/content/us/pdf/threats/securitylibrary/wp01_phishingfinalproof.pdf

Desman, M. (2003) the ten commandments of information security awareness training, *Information Systems Security, 11,* 6, 39-44.

Jagatic, T. N., Johnson, N. A., Jakobsson, M., and Menezer, F. (2007) Social Phishing. *Communications of the ACM, 50,* 10, 94-100.

Keizer, G. (2007) *Phishers pinch billions from consumer' pockets,* Retrieved February 25, 2008, from www.computerworlduk.com/management/security/cybercrime/news-analysis/index

Kenney, B. (2007) From ID to IP theft. *Industry Week/IW , 256,* 7, 49.

Krebs, B. (2006) *Flaws in financial sites aid scammers,* Retrieved February 25, 2008, http://blog.washingtonpost.com/securityfix/2006/06/flaws_in_financial_sites_aid_s.html

Lemos, R. (2008) *Universities fend off phishing attacks*, Retrieved February 25, 2008, from http://www.securityfocus.com/print/news/11504

Litan, A. (2007) *Phishing attacks escalate, morph and cause considerable damage,* Stamford: Connecticut: Gartner, Inc.

National Cyber Alert System Cyber Security Tip ST04-014. (2007) Retrieved February 25, 2008, from http://www.us-cert.gov/cas/tips/ST04-01`4.html

Quarterly Trends and Analysis Report. (2008) Retrieved February 25, 2008, from http://www.uscert. gov/press room/trendsandanalysisQ108.pdf