Caliphate Journal of Science & Technology (CaJoST)

ISSN: 2705-313X (**PRINT**); 2705-3121 (**ONLINE**) **Research Article**

Open Access Journal available at: https://cajost.com.ng/index.php/files and https://www.ajol.info/index.php/cajost/index

DOI: https://dx.doi.org/10.4314/cajost.v5i1.4

Article Info

Received: 4th March 2022

Revised: 26th July 2022

Accepted: 27th July 2022

[1]Computer Science Department, Sokoto State University, Sokoto
[2]Computer Science Department, National Open University of Nigeria.
[3]Computer Science Department, Umaru Ali Shinkafi Polytechnic, Sokoto State.

***Corresponding author's email:**

mansur.aliyu@ssu.edu.ng

Cite this: *CaJoST*, 2023, 1, 22-31

Understanding phishing awareness among students in tertiary institutions and setting-up defensive mechanisms against the attackers

Mansur Aliyu[1*], Mukhtar U. Bagarawa[2], Abba N. Mu'azu[2] and Muhammad T. Umar[3]

The average loss by companies to phishing in 2021 is $14.8 million, more than triple what it was in 2015. That translates to hundreds of billions of dollars in total losses from phishing attacks on global businesses, and the vulnerability of these attacks is every day increasing, particularly among the younger generation less than 40 years of age. This paper begins with a background exposition on phishing trends and highlights previous findings concerning users' susceptibility to phishing attacks. It however explores the term Phishing itself, its kinds, types and some basic measures necessary for defense against phishing activities. The research was employed with a major focus on the email aspect of phishing. Alongside the website aspect of phishing, the certificate of a website was also considered. 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.

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

1. 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 perpetuating their attacks. Therefore, those thieves have thought of ways of bypassing the sophisticated security controls and measures by shifting their focus on the people to commit their crimes.

Since thieves believe that people are the weakest link in the security chain of any organization, no matter how sophisticated its security controls, cybercriminals are currently moving to exploit people in committing their offenses (Schechter, 2007). 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, 2008), Hence, several kinds of attack against people have emerged, of which phishing is a paradigm. This research was designed to answer the following questions:

a. What is the level of awareness of college students regarding phishing attacks?
b. How do students react to specific phishing attacks?
c. Is there a difference in the ways students of different demographics react to specific phishing attacks?

2. Literature Review

The past decade saw plenty of research activities in the area of phishing. See the excellent survey of Hong (2010) for the state of phishing. 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. Many participants did not verify the correctness of the sites' URLs or were not able to distinguish between legitimate and fraudulent URLs. Even fewer understood the SSL security indicators, such as 'HTTPS' in the URL, the padlock icon, and the certificate.

Many participants incorrectly based their decisions on how professional the content of the viewed web pages look, failing to understand that the content of a web page can be easily copied. Moreover, visual deception attacks successfully fooled even the most experienced participants. Examples of visual deception include using visually deceptive text in closely mimicked URLs (e.g. using the number '1' in place of the letter 'l', or using two 'v's for a 'w'), hiding a hyperlink to a rogue site inside an image of a legitimate hyperlink, and using an image of a real site in the content of a phishing page. Following the work of Dhamija et al., many other researchers led similar studies which show that their findings continue to hold and users remain vulnerable to phishing (Hong, 2011; 2012)

2.1 Phishing Attacks

Phishing: is a type of social engineering attack and takes the form of an online identity theft that 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 (Litan, 2007). Phishing is an attempt by an individual or organization to gain valued information such as usernames, passwords, credit card details, or financial records by luring or tricking a target into divulging his data through a communication (email, instant message, etc.) that originates from a widely trusted entity like a bank, utility company, or web portal. (Cavalli, 2009). With the development of new communication channels, phishers have found new means to carry out their attacks. Consequently, different categories of phishing have been discovered such as Vishing, SMishing, Pharming, Google phishing, Wi-phishing, Phishing scam and Spear phishing

Moreover, phishing attacks are also becoming increasingly pervasive and sophisticated. Phishing has spread beyond email to now include VOIP, SMS, instant messaging, social networking sites, and even massively multiplayer games (Herley and Florencio, 2009). Criminals are also shifting from sending out mass emails in the hopes of tricking anyone, to more selective "spear-phishing" attacks that use relevant contextual information to trick specific victims. Academic and commercial work in phishing is a dynamic area that combines elements of social psychology, economics, distributed systems, machine learning, human-computer interaction, and public policy. In 2006, Jakobsson and Myers (2006) provided an overview of how phishing works and what countermeasures were available at that time. This article serves as an introduction as well as an overview of the current state of phishing. We start by examining how phishing attacks work. We then discuss why people fall for phishing attacks. We follow with the debate over the damage caused by phishing attacks.

2.2 Types of Phishing

Phishing has been categorized by many researchers from a different perspective, but the most common types are the ones adopted by Al-Hamar (2010) in their various research categorized 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, Malware, Keyloggers, Screen loggers, Session Hijacking, Web Trojans, Hosts File Poisoning, System Reconfiguration Attacks, Content-Injection and Man-in-the-Middle. 1997 was the first occasion when the media demonstrated phishing and its threat, since then, phishing attacks have subsequently increased dramatically. The majority of researchers have considered phishing as a formidable attack facing online consumers (Herzberg and Jbara, 2008; APWG, 2006. Accordingly, this has motivated me 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. 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.

2.3 Financial Damages Caused by Phishing

Phishing exerts both direct and indirect costs on society. Examples of direct loss include consumers losing money, banking fraud, etc. Examples of indirect costs include erosion of consumer trust in the Internet, negative impact on businesses' brands, an increase in service call center 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 to estimate direct costs. Gartner Research surveyed 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 the economic loss to be 2.8 billion dollars in 2006 (Gartner Inc, 2008). A follow-up survey in 2007 with a similar methodology estimated that 3.2 billion dollars is lost in 2007 (Litan, 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 8 users per day afterward. The total cost to consumers per year was estimated at around 320 million dollars (Moore and Clayton, 2007).

3. Research Model

Based on previous research, this study proposes a model for evaluating the Reasons for students' vulnerabilities to phishing. The preliminary block research model is created based on the literature. This model contains three main dimensions which identified the behavior of users, clever tricks by phishers and ignorance factors that influence the vulnerabilities of students to phishing.

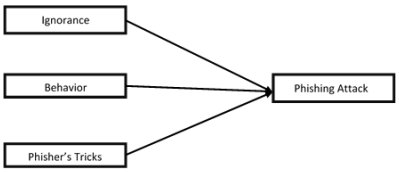

Fig 1: Proposed Research model

4. Research Method

This study was designed to identify the current level of students' knowledge of phishing to determine their vulnerability. Students, in other words as a youth, 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 whether to visit a web or not on its fantasy and beautiful vie as established in other research (Dhamija 2006). Therefore understanding the level of awareness among this class of people and the factors that guide their actions will help in designing a better awareness program that will help in reducing the phishing vulnerability.

4.1 Research Instrument

The instrument for this study was developed from the existing literature above. To confirm the clarity and identify any possible ambiguity in the wording of the instrument, a pilot study with 10 students was conducted. The results provide valuable suggestions to add, remove, and reword some items, as well as restructure the overall instrument.

A structured questionnaire was used to collect data for the research model. The questionnaire consisted of 18 simple questions relating to phishing which were all closed-ended, that is yes/no, multiple choices. The ultimate aim of the questionnaire was to draw a profile of people's awareness of phishing and their views on the best method of defence against this attack. Therefore, the questionnaire consisted of six sections, each contributing to the aim of the whole questionnaire.

One Hundred and Forty-Two (142) questionnaires were distributed among students of Umaru 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).

5. Results

5.1 Demographic profile of respondents

The following question tries to investigate the frequency at which respondents receive the

email/SMS they suspect to be phishing. It's unfortunate to note that more than 38% of them received email/SMS they suspect to be phishing messages in their lifetime.

Table 1: Respondents' Demographic Characteristics and Phishing Knowledge

Demographic Data		N	%	Phishing Awareness		N	%
Gender	Male	81	57	Phishing Software	YES	50	35
	Female	61	43		NO	82	65
Age	18-24	85	60	Phishing	YES	135	95
	25-31	50	35	Victimization	NO	7	5
	32-38	7	4				
Educational	HND	19	13	Frequency of	Once		25
level	ND	96	68	receiving phishing	2 times		23
	Certificate	27	19	e-mails/SMS	3 times+		38
Usage	Smartphone	128	90		Never		14
	Email	14	10				

This implies that when adequate awareness was not put in place to guide the students on dose and don'ts when phishing messages are received and how to effectively classify the messages, many students will fall prey to the phishers shortly.

5.2 Smartphones Use for Phishing

The following tables present the finding for the group as a whole. The percentages in the response column for the first questions indicate the percentage 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 2: Smartphone use

S/N	QUESTION	%
1	Smartphones as a means of accessing the Internet	90
2	Students with email Addresses	100
3	Students that know at least 3 ways of defense against Phishing	36

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

1. Question 1 indicates that 52% of the students will voluntarily render their information to an email or SMS that asks 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 it's hard to gather the necessary information to achieve that, it's agreed by most of the respondents that it's usually legitimate.

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

4. It was expected that students will understand the simplest characteristics of phishing messages, which are urgency and the need for a 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 have some security concern attached to them. But unfortunately, only 50% of the students classified it as phishing.

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

7. HTTPS with padlock signs are two common signs 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.

6. Findings

Regarding the actions which would be taken by victims of being tricked, fewer than half of the participants change their account details, check their financial statements immediately, cancel their credit cards, or report the incident to their banks or organizations concerned. Few report the incident to the police or any relevant body dealing with such cases or to the company whose address or website was faked. Also, it was believed that reporting the case to the company whose address or website was faked will not make any difference to what happens, as most think that it will not take the matter seriously. Furthermore, some stated they did not know that there is a specialized body to deal with such cases, like NITDA or EFCC. Most of the participants were even shame to share their experiences with others as they believe that they will be seen as fools. However, in an ideal situation, victims of such an attack should apply all of the above actions to protect themselves from its further consequences. Fewer than 10% of the participants would take all of the above steps and about a seventh of them would do nothing once they have been tricked by phishing, which means most are vulnerable to huge consequences as a result.

Conclusively, many students in tertiary institutions are not much aware of the simple tricks phishers take in duping the victims, most of them were not aware of simple ways to defend themselves nor that they use apps that can defend them against some sorts of phishing. Even the most straightforward phishing attacks which ask users to disclose their confidential information and usually convey a sense of urgency and surprise were not distinguished by a large percentage of the students, which makes them vulnerable even to such basic phishing attacks. In addition, the majority do not take enough or even any action to diminish the possible consequences of successful phishing. In brief, this means that students in tertiary institutions are generally vulnerable to phishing threats.

6.1 Action after receiving suspected Phishing massage.

Q1: Ignore the message and immediately delete it
Q2: Open the message and read it
Q3: Read the message and respond to it/ reply to the phisher
Q4: Report the message to the bank or company whose website/name was faked
Q5: Report to the police or institution that specializes in dealing with such cases
Q6: Report the incident to the bank or other organization for which you disclosed your details
Q7: Check your financial statement immediately
Q8: Block off your ATM card
Q9: Change the account details (e.g. Pin, User name, Password you have disclosed)
Q10: Others

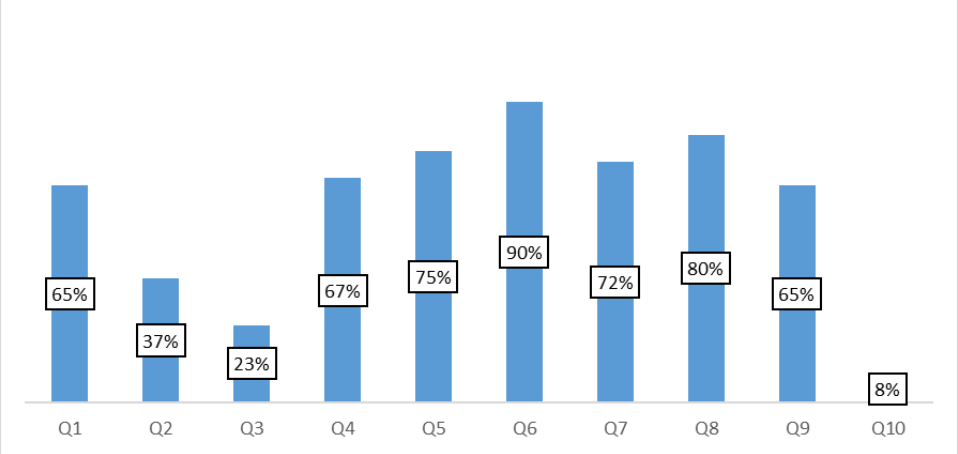

Fig 2: Action after suspected phishing

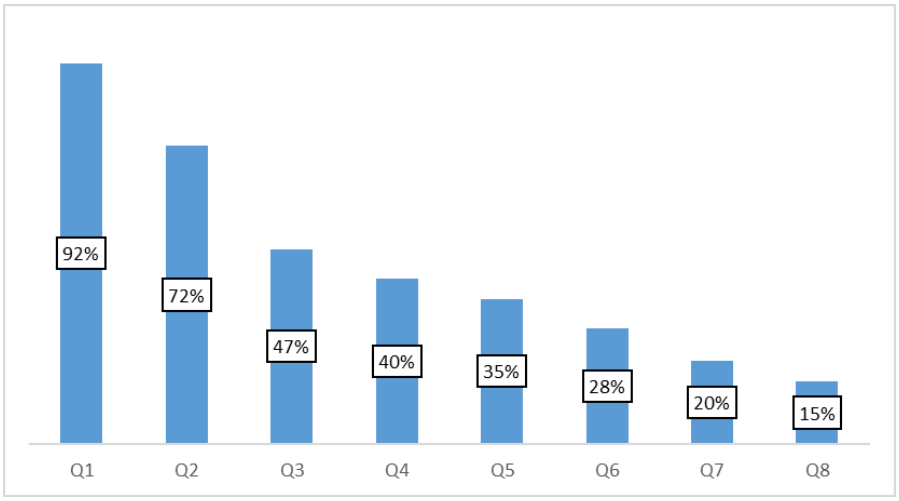

Fig 3: Reasons for falling prey

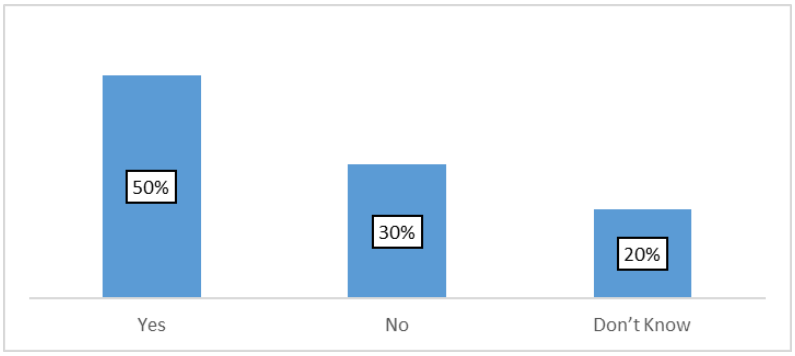

Fig 4: Knowledge of self-defence

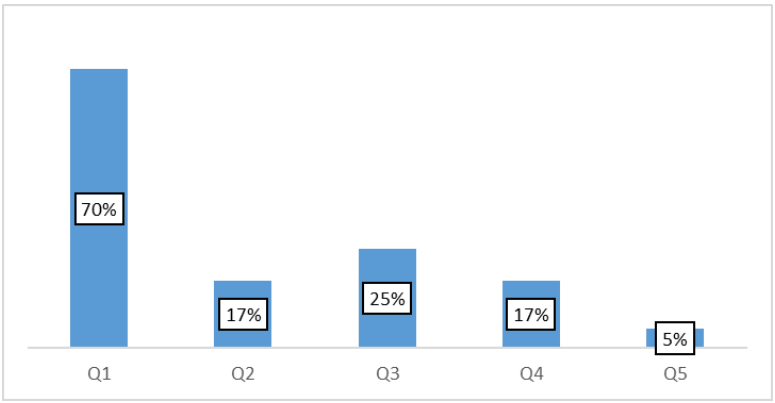

Fig 5: Best way of defence against phishing

6.2 Reasons why people are involved in phishing

The participants refer to the reason for their being tricked as being the following, arranged in descending order by the percentage of responses:

Q1 They did not believe they would be tricked
Q2 Phishers come up with smarter tricks which make it difficult to identify phishing
Q3 The fake website looked almost identical to a legitimate one
Q4 They lacked awareness and training about phishing
Q5 They trusted the e-mail because they did not know about phishing
Q6 The e-mail came up with a sense of urgency and surprise
Q7 They were not aware of the importance of the information they had divulged.

Q8 They did not install software to protect against phishing e-mails and websites.

The above responses indicate all of the above reasons were significant causes of participants' falling prey to SMS/e-mail phishing attacks. In conclusion, the extent of the e-mail phishing threat in tertiary institutions is high in view of the regular quantity of phishing e-mails/SMS received in participants' inboxes and the rate of successful phishing attacks.

6.3 Defence against phishing

Even though the Nigerian cybercrime act has come into law in 2015 which includes among others death penalty down to 5 years imprisonment, many participants think that Government is not doing enough in defending its citizens against the fraudsters. According to figure 4, 50% of the participants had clearly said that Government is not doing what it supposes to do, while 30% don't even know whether there are measures on the ground to fight the act, even though most of them believe that the trend of phishing in Nigeria is increasing, this means that even if Government is doing something, there is no awareness among citizens about the punishment of phishing or cybercrime in general.

Although there are lots of ways to protect against phishing attacks, it was of interest to discover participants' outlook on the best way to defend themselves. The responses were positive since most (70%) considered awareness to be the best defence, then came the experience of getting infected by phishing with 25% and, finally, fewer than 20% think that the use of technological solutions, guidelines, or installation of effective anti-virus software.

Q1 Be aware and be educated about Phishing
Q2 Allow clear guidelines addressing Phishing
Q3 Install effective anti-Phishing software
Q4 Get infected by Phishing so that I will learn more
Q5 Others

Most participants, about 50%, preferred to be educated about phishing through seminars, media, or interactive games. Others prefer other tools ranging from posters, videos and documents. Cartoons are the less preferred method of learning among participants with about 3%.

6.4 Summary of Findings

The study found that the level of phishing awareness among college students is very low at about 22.85% this literary means over 70% of the student may not be able to differentiate between phishing emails/SMS and legitimate ones. It's found that only 25.9% (36% male and 15.8% females) of the student correctly classify phishing attacks and 39.6% (19.6 males and 20% females) were able to correctly classify legitimate messages, therefore there is a need for continuous awareness on phishing among students of tertiary institutions. This result emphasizes the need for education on phishing, but in order to adequately prepare and motivate students to increase their level of awareness, there is a need for sensitization agenda not only on how to recognize phishing emails and fraudulent websites but also on the cost and magnitude of the phishing problem. Since over-reliance on technical solutions for protection is dangerous, the best defense is therefore a continuing education program. Sometimes the latest scam is 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 76% 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 Kumaraguru et al. (2010) found that lack of knowledge is the primary reason why users fall for phishing good educational materials reduced participants' chance of falling for phishing by 40%. Kumaraguru et al. (2010) further studied the effects of these educational materials and training in helping users prevent phishing and found that simplifying anti-phishing materials to users is ineffective, as people are used to receiving and ignoring such warnings. They found that users learn more effectively in embedded training, where users have 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. The study showed that with this approach, participants' chance of falling for phishing was reduced by 45%, even one month after the training. The authors 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 (Kumaraguru (2010). Studies showed that this approach improved novices' ability to identify phishing by 61%.

This study further revealed that 95% of the respondent received at least 3 phishing messages and are below the age of 30 years, furthermore,

the demographic difference in classifying the suspected attacks found that male student has a better chance of correctly identifying phishing attacks than female students.

7. Conclusion

As stated in the articles, Phishers always and every day create additional means of reaching their potential victims. As such the field of phishing will need continuous research that will help to avert the activities of the criminals in question. It is also likely we will see an increase in spear-phishing, as phishers continue to look for vulnerable targets with valuable information. Phishing also causes new problems for organizations, as they blur traditional security perimeters. An employee falling for a phish in one context may cause a headache for the entire organization.

On the positive side, law enforcement, industry, and academics are becoming better organized, in terms of reporting phishing attacks, sharing information, analysing data to identify trends, and focusing resources. There are more organizations now devoted to combating online fraud, including the APWG, the National Cyber-Forensics and Training Alliance (NCFTA), and NITDA as far as Nigeria is concerned. There are also initiatives for educating people about phishing scams, for example, StaySafeOnline.com. Law enforcement has been stepping up efforts in gathering evidence and cooperating with international partners in shutting down phishing sites and phishing gangs. Legislators have also been passing new laws to explicitly spell out what phishing is and what the penalties are for committing this crime.

7.1 Phishing Countermeasures

Given the risks of phishing, what can individuals and organizations do to protect themselves from the end user's perspective, there are three strategies:

1. Make it invisible, so that users do not have to do anything differently;
2. Provide better user interfaces that either make things more obvious to users or offer additional protection;
3. Train end-users to recognize and avoid phishing attacks. All three of these approaches are needed to offer the strongest possible protection against phishing attacks.

7.2 Make it Invisible

The first line of defence is to prevent phishing attacks from reaching end-users. The solutions in this space include filtering phishing emails, blocking fake sites, and taking down fake sites.

- *Filtering Phishing Emails*

There is a large body of research on detecting spam. However, research on detecting phishing emails is sparse because phishing is relatively a new phenomenon. Fette et al. developed the first email phishing filter, identifying several features that are highly indicative of phishing, for example, having URLs that use different domain names.

- *Blocking Phishing Sites*

Currently, there are two ways of detecting phishing websites. The first is to use heuristics that examine the URL, HTML, and server characteristics to classify sites. The second is to use manually verified blacklists. For heuristics, researchers have investigated a large number of ideas using machine learning. Some examples include looking for patterns in URLs (Grera 2007) words on the web page and using search engines. Researchers have also looked at linguistic characteristics of web pages, identifying the brand name that a web page claims to be (Xiang 2009)

- *Taking Down Phishing Sites*

Several companies identify and take down phishing sites. There are also private mailing lists used for sharing information about fake sites as well as finding contact information for specific ISPs and websites. Typically, when phishing sites are taken down, end-users who click on a phish are shown a “page not found” error. One innovation developed by APWG and Carnegie Mellon University is to have ISPs and takedown providers replace the phishing page with a training message, thus teaching people who click on phishing emails about these kinds of attacks. The APWG landing page (APGW, 2008) has been in use since Sept 2008 and is available in several languages. As of April 2010, it has been displayed in place of 1285 phishing pages and viewed about 200,000 times.

7.3 Train the Users

The third way of protecting people from phishing scams is to train them. Training is an essential part of computer security but arguably the least popular approach, given the inherent challenges in motivating people to be secure, as well as the fact that training does not guarantee complete protection (though in reality, neither do other solutions). Many websites offer advice on how to identify phishing sites. Past studies by Kumaraguru (2010) have shown that this kind of information is useful in helping people identify fake websites, but only if you can get people to read the material.

8. Recommendations

The result of this study reveals that many students are not that aware of simple tactics for self-defence against phishing that is why we prepare the following recommendations and suggestions:

1. Things to look for in scam emails 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 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 the status bar, not the website 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 recent 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 displays fake URL in the address bar on the browser
- Type addresses directly into the browser or uses personal bookmarks
- Verify security certificates by double-clicking on the 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 can't 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)

Conflict of Interest

The author declares that there is no conflict of interest.

Acknowledgements

We acknowledged the efforts of all those who contributed to the completion of this study. We are thankful to the CaJoST Team and Peer Reviewers for their painstaking editorship and review of our paper.

References

Al-Hamar, M. K. (2010). *Reducing the risk of e-mail phishing in the state of Qatar through an effective awareness framework* (Doctoral dissertation, Loughborough University).

APWG & CMU's Phishing Education Landing Page. 2008. http://education.apwg.org Anti-Phishing Working Group. *Phishing Activity Trends Report: 4th Quarter Report*.

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

Cavalli, E. World of Warcraft Phishing Attempts on the Rise. *Wired Magazine*, 2009. http://www.wired.com/gamelife/2009/04/world-ofwarcraft-phishing-attempts-on-the-rise/.

Dhamija, R., Tygar, J. D., & Hearst, M. (2006, April). Why phishing works. In *Proceedings of the SIGCHI conference on Human Factors in computing systems* (pp. 581-590). Doi: 10.1145/1124772.1124861.

Downs, J. S., Holbrook, M. B., & Cranor, L. F. (2006, July). Decision strategies and susceptibility to phishing. In *Proceedings of the second symposium on Usable privacy and security* (pp. 79-90). DOI: 10.1145/1143120.1143131.

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

Herley, C., & Florêncio, D. (2010). Nobody sells gold for the price of silver: Dishonesty, uncertainty and the underground economy. In *Economics of information security and privacy* (pp. 33-53). Springer, Boston, MA. DOI: 10.1007/978-1-4419-6967-5_3

Herzberg, A., & Jbara, A. (2008). Security and identification indicators for browsers against spoofing and phishing attacks. *ACM Transactions on Internet Technology (TOIT)*, *8*(4), 1-36. DOI: 10.1145/1391949.1391950.

Hong, J. I. Statistical Analysis of Phished Email Users, Intercepted by the APWG/CMU Phishing Education Landing Page. *APWG CeCOS*, 2010. http://www.antiphishing.org/events/2010_opSummit.html.

Hong, J. I. Why Have There Been So Many Security Breaches Recently? *Blog@CACM*, 2011. http://cacm.acm.org/blogs/blog-cacm/107800-whyhave-there-been-so-many-security-breachesrecently/fulltext.

Jagatic, T. N., Johnson, N. A., Jakobsson, M., and Menezer, F. (2007) Social Phishing. *Communications of the ACM, 50,* 10, 94-100. DOI: 10.1145/1290958.1290968.

Jakobsson, M., & Myers, S. (Eds.). (2006). *Phishing and countermeasures: understanding the increasing problem of electronic identity theft*. John Wiley & Sons.

Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L. F., & Hong, J. (2010). Teaching Johnny not to fall for phish. *ACM Transactions on Internet Technology (TOIT)*, *10*(2), 1-31. DOI: 10.1145/1754393.1754396.

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.

Moore, T., & Clayton, R. (2007, October). Examining the impact of website take-down on phishing. In *Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit* (pp. 1-13). DOI: 10.1145/1299015.1299016.

Schechter, S.E., Dhamija, R., Ozment, A., and Fischer, I. The Emperor's New Security Indicators: An evaluation of website authentication and the effect of role-playing on usability studies. *IEEE Symposium on Security and Privacy*, (2007). Verisign. *Fraud Alert: Phishing — the Latest Tactics and Potential Business Impact*. 2009.

