UNDERSTANDING PHISHING AND SETTING-UP DEFENSIVE MECHANISM AGAINST THE ATTACKERS

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
This paper begins with a background exposition on phishing trends and highlights previous findings in relation to 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.

Keywords: Security, Phishing, Social Engineering

INTRODUCTION

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 apparently originates from a widely trusted entity like a bank, utilities company, or web portal. (Cyberisk 2016 USA). 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

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 2008). 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 (Jaccobson 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 on 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. Afterward, we close with countermeasures against phishing.

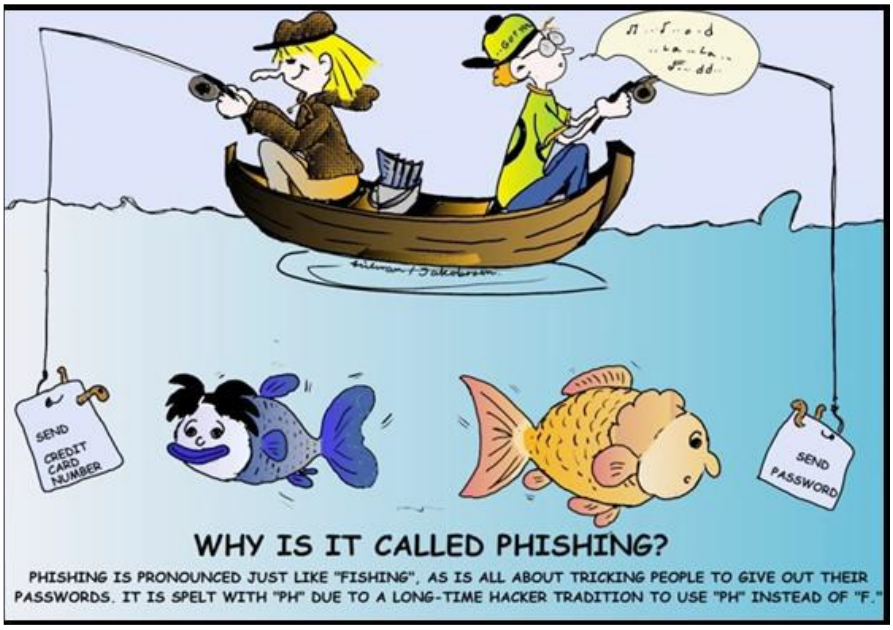


Fig 1: Phishing Example

LITERATURE REVIEW

The past decade saw a great deal of research activities in the area of phishing. See the excellent survey of Hong (2012) 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 the findings of Dhamija et al. continue to hold and users remain vulnerable to phishing (Hong, 2012)

Phishing trend

While phishing started out with attacking America Online (AOL) users, it is a common facet in today's society. Typical phishing attempts target customers of banks, online payment services and

auction sites, to name a few (Ramzan, 2007). Phishing activities have continued to thrive in spite of the technological measures put in place by organizations, campaign by the target industry sectors and the advent of anti-phishing organizations. According to Anti-Phishing Working Group (2019), The total number of phishing sites detected by APWG in 2Q was 182,465, up slightly from the 180,768 seen in 1Q2019, and up notably from the 138,328 seen in 4Q 2018 and the 151,014 seen in 3Q 2018. (APGW 2019)

Types of Phishing

Phishing has been categorized by many researchers from different perspective (Bagarawa, 2019), 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 (Bagarawa, 2019)

Mariam Khalid Al-Hamar (2010) categorized the phishing by considering the communication channels of which phishing is carried out as follows:

Pharming

Pharmers attempt to redirect the URL to a forged site which looks similar to the legitimate one. Once the user gets into the forged site, pharmers can capture the login information the user has provided. In essence, pharmers direct the user to another bogus website instead of a requested legitimate website, this is done by inserting 'wicked' code into a PC or DNS (Domain Name System) server on the Internet. (APWG, 2006; Fox, 2005; Hubbard, 2005; Pandit, 2006; Radcliff, 2005b).

Google phishing

Attackers have used the Google search engine to assist their attacks by using it to drive users to their fake website. As phishers do not aim to make any legitimate sales, they will design a fake website which will usually attract online users by claiming to sell a product or provide a service at incredibly low prices. In order to carry out the transaction, users have to enter their private details. Once the information is submitted, an error message will usually be displayed, informing the user of a problem which has occurred which results in an unsuccessful transaction. However, the phisher has already gained the disclosed information (Corrons, 2005; Radcliff, 2005b).

Wi-phishing

Phishers may use wireless technology and Bluetooth facilities to carry out their crime. This could be done by setting up a wi-fi network in public places that looks like the legitimate networks at designated hotspots in order to trick the user of a wireless broadband connection. Wi-phishing could thus harvest the user's personal information (Der Hovanesian, 2005; Radcliff, 2005b).

Vishing

Vishing is a criminal attack over the telephone system to gain access to private information from the users of the system; it abuses user trust in landline telephone or cellular services. Banking

clients were targeted by vishing and the first reported incident was in April 2006 (Patterson, 2006; Sausner, 2006). The attackers sent out an email message in bulk, alerting the user to a security risk and asking the potential victim to phone the bank's call center to resolve the matter. Once the victims called the number given in the email/SMS, they were asked to verify bank details, such as bank account numbers and PINs through an automated system set up by the phisher (Patterson, 2006; Sausner, 2006).

SMishing

This phishing technique attacks cell phone users; it was identified in September 2006 (Hickey, 2006). The attacker uses the technology of the cellular short message service (SMS) to steal the victim's identity. Phishers capture the required information by sending a misleading SMS to victims asking them to disclose it. The deceptive SMS may refer the victim to visit a fraudulent web site to disclose the information; sometimes the victim is encouraged to download a program that is actually a Trojan horse which allows the hacker to have control of the victim's cellular phone (Hickey, 2006).

Phishing scams

This is a type of phishing which targets Internet users, where phishers send a deceptive email/SMS to the user, posing as a trusted and legitimate entity, but attempting to trick the victim to reveal sensitive information or private information such as username, password and account number. Misleading phishing scams attacks are one of the most successful and common methods of identity theft (Emigh, 2005; Ollmann, 2004). Popular companies such as PayPal or eBay are frequent targets.

Spear phishing

Usually phishing scams are designed to steal information from individuals in general, whereas, in spear phishing scams, the target is highly specific individuals or groups. Instead of sending a huge volume of email/SMS to large numbers of people, a spear phishing attack is usually to gain access to a specific organization's system (Microsoft, 2006). Spear phishing can be carried out by telephone, the phishers appearing as legitimate to the victims. The attack uses authority to commit the crime by impersonating a communication from HR (Human Resources), the manager or any other authoritative figure. It might require the victims to give their user names or passwords or it might contain malicious software such as a Trojan horse or virus (Der Hovanesian, 2005; Pandit, 2006; Radcliff, 2005a, 2005b).

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 behaviour of users, clever tricks by phishers and ignorance factor that influence the vulnerabilities of students to phishing.

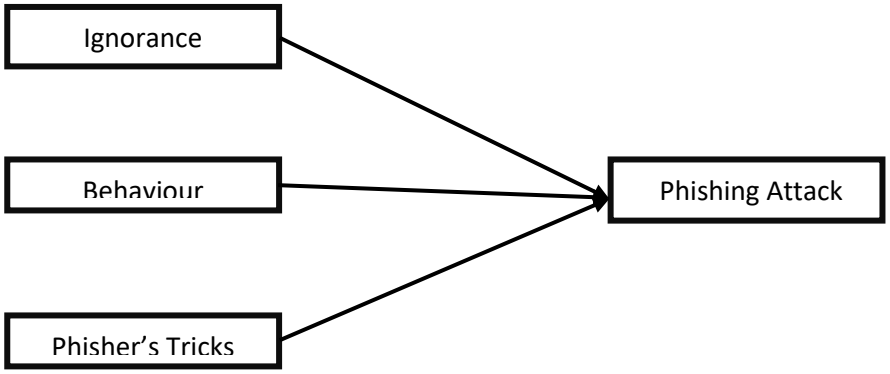


Fig 2 Proposed Research model

RESEARCH METHOD

Research Instrument

The instrument for this study was developed from the existing literature above. In order 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, reword some items, as well as restructure the overall instrument.

A structured questionnaire was used to collect data to 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 defense against this attack. Therefore, the questionnaire consisted of six sections, each contributing to the aim of the whole questionnaire.

Research Respondents

142 respondents were selected for this study from Ummaru Ali Shinkafi Polytechnic most of whom are students from computer departments and Mass Communication

RESULTS AND FINDINGS

Table 1: Respondents' Demographic Characteristics and Phishing Knowledge.

Demographic Characteristics		N	%	Phishing Knowledge		N	%
Gender	Male	81	57	Awareness on Ant phishing Software	Yes	50	35
	Females	61	43		No	82	65
Age	18-24	85	60				
	25-31	50	35	Phishing Victimization	Yes	135	95
	32-38	7	4		No	7	5
Educational Level	HND	19	13				
	Diploma	96	68				
	Certificate	27	19				
Smartphone Usage	Smartphone	128	90				
	Other means	14	10				

The following question tries to investigate the frequency at which respondent receive the email/SMS they suspect to be phishing. Its unfortunate to note that more than 38% of them received email/SMS they suspect to be phishing message in their lifetime.

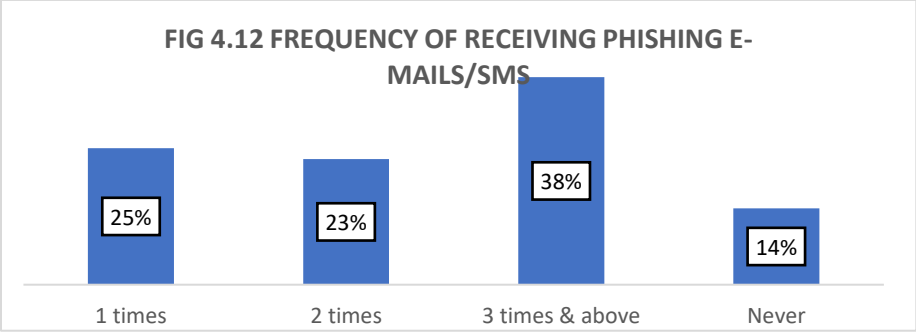
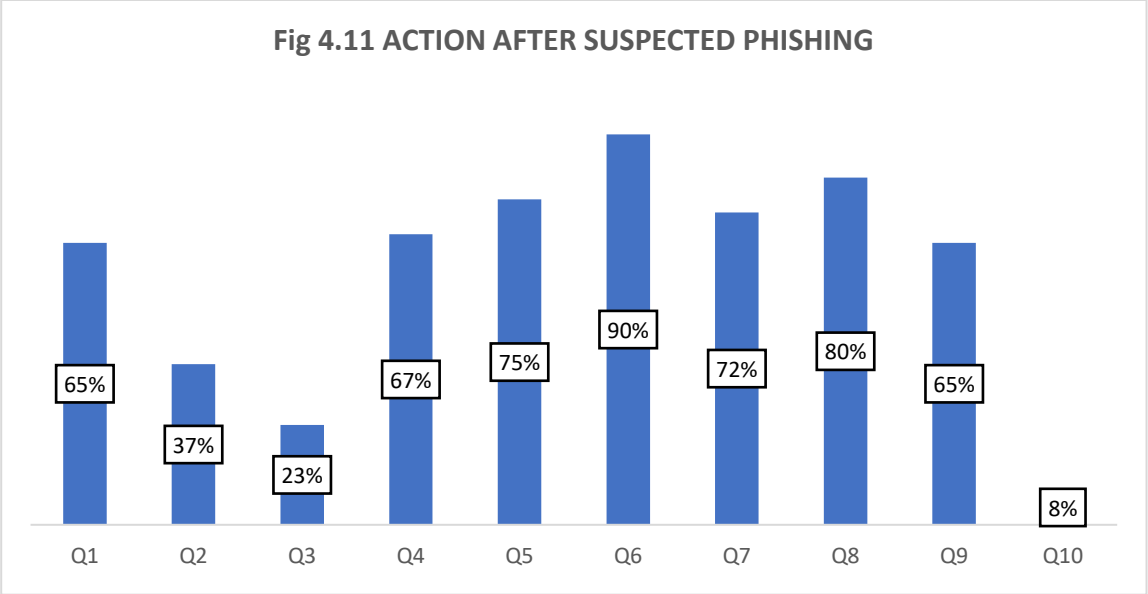


Fig 3

This implies that when adequate awareness was not put in place to guide the students on do and don't when phishing messages are received and how to effectively classified the messages, many students will fall prey to the phishers in the near future.



Q1: Ignore the message and immediately delete it
Q2: Open the message and read it
Q3: Read the message and respond to it/ reply phisher
Q4: Report the message to the bank or company whose website/name or was faked
Q5: Report to the police or institution that specializes in dealing with such cases
Q6: Report 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)
Q12 Others

Regarding the actions which would be taken by victims on being tricked, fewer than half of the participants change their account details, check their financial statement 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 experience with other as they believe that they will be seen as fools. However, for an ideal situation, victims of such attack should apply all of the above actions in order 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.

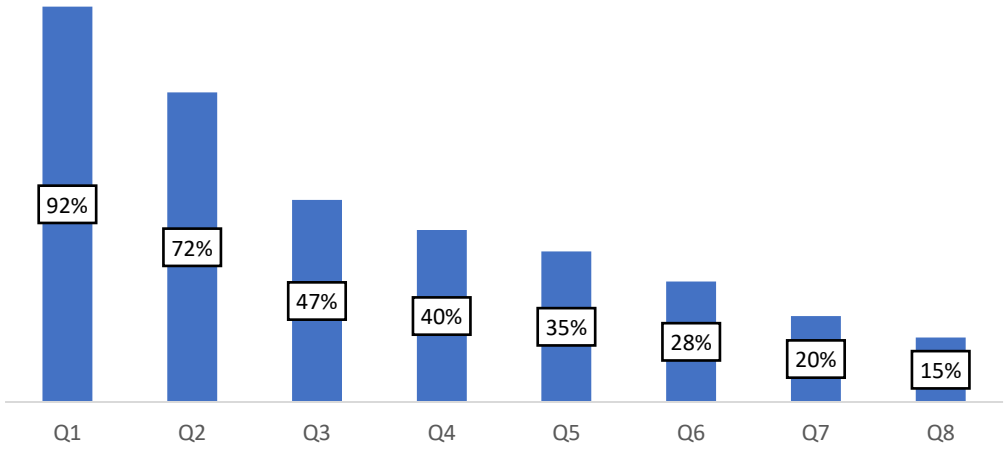
Conclusively, many students in tertiary institutions are not much aware of simple tricks phishers take in duping the victims, most of them were not aware of simple ways to defend themselves nor that they use apps that can defend them against some sorts of phishing. Even the most straightforward phishing 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.

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 percentage of responses:

- They did not believe they would be tricked
- Phishers come up with smarter tricks which make it difficult to identify phishing
- The fake website looked almost identical to a legitimate one
- They lacked awareness and training about phishing
- They trusted the e-mail because they did not know about phishing (this confirms the response in the previous question)
- The e-mail came up with sense of urgency and surprise
- They were not aware of the importance of the information they had divulged.
- They did not install software to protect against phishing e-mails and websites

FIG 4.13 REASONS FOR FALLING PREY



Q1 They did not believe they would be tricked

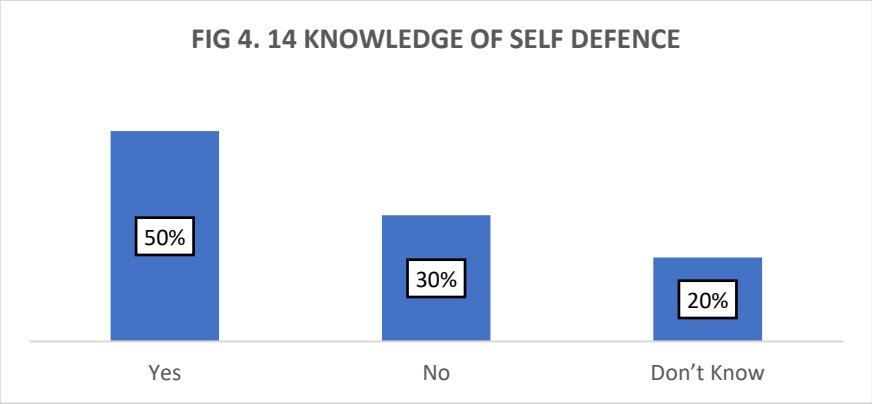
Q2 Phishers come up with smarter tricks which make it difficult to identify phishing

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 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

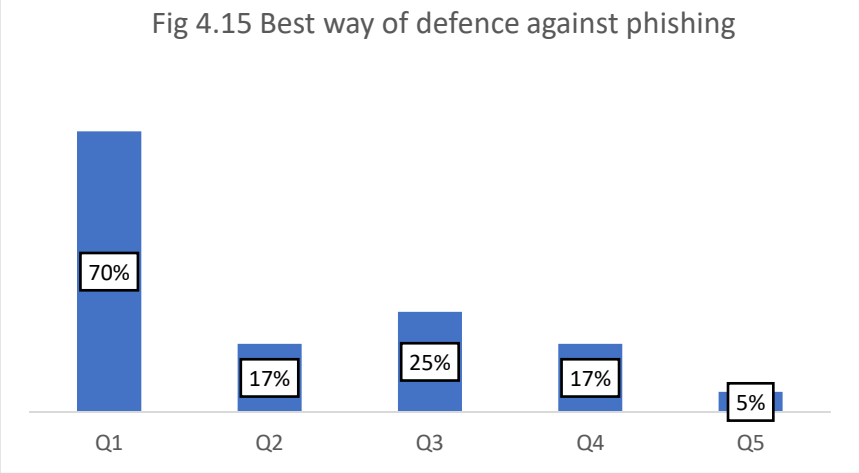
The above responses indicate all of the above reasons were significant causes of participants' falling prey to SMS/e-mail phishing attacks. In conclusion, the extent of the e-mail phishing threat in tertiary institution is high in view of the regular quantity of phishing e-mails/SMS received in participants'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

Defense against phishing

Even though Nigerian cybercrime act has come into law since 2015 which includes among others death penalty down to 5 years imprisonment, many participants are of the opinion that Government is not doing enough in defending its citizens against the fraudsters. According to figure 4.23, 50% of the participants had clearly said that Government is not doing what its supposes to do, while 30% doesn't even know whether there are measures on ground to fight the act, despite the fact that most of them believes 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 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% (see Figure below).

CONCLUSION

As stated in the articles, Phishers always and everyday create additional means of reaching their potential victims as soon as on out of their hundred ways is exposed. As such the field of phishing will need a continues research that will help to avert te activities the criminals in question. It is also likely we will see an increase in spear-phishing and whaling attacks, as phishers continue to look for vulnerable targets with valuable information.

Phishing also causes new problems for organizations, as they blur traditional security perimeters. One's lawyers and accountants may be attacked to surreptitiously gain access to documents. Facebook and other social media provide more contextual details that can be used for spear-phishing attacks. An employee falling for a phish in one context may cause a headache for your organization because of reused passwords. Finally, instant messaging, VOIP, SMS, and other new ways of communicating offer criminals new vectors for sending attacks.

On the positive side, law enforcement, industry, and academics are becoming better organized, in terms of reporting phishing attacks, sharing information, analyzing 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

RECOMMENDATIONS

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 different;
2. Provide better user interfaces that either make things more obvious to users or offer additional protection; and
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.

Make it Invisible

The first line of defense 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, in part because phishing is a relatively new phenomenon, but also because phishing emails look legitimate. 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 web sites. 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 in 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*

There are several companies that 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 web sites. 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 *(ECRS 2007).*

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 today). Many web sites offer advice on how to identify phishing sites. Past studies by Kumaraguru et al (Kumaraguru, 2010) have shown that this kind of information is useful in helping people identify fake web sites, but only if you can get people to read the material.

REFERENCES

APWG. APWG & CMU's Phishing Education Landing Page. 2008. http://education.apwg.org

Anti-Phishing Working Group. *Phishing Activity Trends Report: 4th Quarter Report*.

Bagarawa, M.U. *Investigating the risk of phishing among students in tertiary institutions.* 2019

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., and Hearst, M.A. Why phishing works. *Conference on Human Factors in Computing Systems (CHI 2006)*, (2006), 581.

Downs, J.S., Holbrook, M.B., and Cranor, L.F. Decision strategies and susceptibility to phishing. *Symposium on Usable Privacy and Security (SOUPS 2006)*, (2006).

Fette, I., Sadeh, N., and Tomasic, A. Learning to Detect Phishing Emails. *Proceedings of the 16th International World Wide Web Conference (WWW2007)*, (2007).

Garera, S., Provos, N., Chew, M., and Rubin, A.D. A framework for detection and measurement of phishing ttacks. *Workshop On Rapid Malcode*, (2007), 1.

Görling, S. An overview of the Sender Policy Framework (SPF) as an anti-phishing mechanism.*Internet Research 17*, 2 (2007), 169 - 179.

Herley, C. and Florencio, D. Nobody Sell Gold for the Price of Silver: Dishonesty Uncertainty and the Underground Economy. *Workshop on the Economics of Information Security (WEIS 2009)*, (2009).

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.

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.

Jagatic, T.N., Johnson, N.A., Jakobsson, M., and Menczer, F. Social phishing. *Communications of the ACM 50*, 10 (2007), 94.

Jakobsson, M. and Myers, S. *Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft*. Wiley- Interscience, 2006.

Keizer, G. California Enacts Tough Anti-Phishing Law. *Information Week*, 2005.http://informationweek.com/news/171202672.

Krastev, N. U.S. Indicts Dozens From Eastern Europe In Internet Theft Scheme. *Radio Free Europe*, 2010. http://www.rferl.org/content/US_Indicts_Dozens_From_Eastern_Europe_In_Internet_Theft_Scheme/2173545.html.

Kumaraguru, P., Rhee, Y., Sheng, S., et al. Getting users to pay attention to anti-phishing education: evaluation of retention and transfer. *The Anti-Phishing Working Group's 2nd Annual eCrimeResearchers Summit (ECRS 2007)*, (2007), 70.

Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L.F., and Hong, J.I. Teaching Johnny not to fall for phish. *ACM Transactions on Internet Technology (TOIT) 10*, 2 (2010).

Moore, T. and Clayton, R. Examining the impact of website take-down on phishing. *The Anti-Phishing Working Group's 2nd Annual eCrime Researchers Summit (ECRS 2007)*, (2007).

PhishTank. PhishTank Stats. 2011.http://www.phishtank.com/stats.php.

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.

Wu, M., Miller, R.C., and Garfinkel, S. Do Security Toolbars Actually Prevent Phishing Attacks? *Human Factors in Computing Systems (CHI 2006)*, 601–610.

Xiang, G. and Hong, J.I. A hybrid phish detection approach by identity discovery and keywords retrieval. *International World Wide Web Conference*, (2009), 571-580.

Xiang, G., Rose, C., Hong, J.I., and Pendleton, B. A Hierarchical Adaptive Probabilistic Approach for Zero Hour Phish Detection. *15th European Symposium on Research in Computer Security (ESORICS 2010)*, (2010).

Zhang, Y., Hong, J.I., and Cranor, L.F. Cantina: a content-based approach to detecting phishing websites. *International World Wide Web Conference*,(2007), 639.