Cyber Insecurity: End User Vulnerability Awareness and Perception Assessment

Dorothy E. Akpon-Ebiyonare, Ph.D.* and Susan Konyeha, Ph.D.

University of Benin, Nigeria.

E-mail: dorothy.akpon@uniben.edu*

ABSTRACT

Increasingly, cyber attackers are breaching computer systems security by targeting the weakest links in the information security chain – people. They are potential victims of most attacks and the role they play in successful cyber attacks is significant. The most effective counter measures against attacks in cyber space are awareness as well as training. This study investigates and evaluates respondents' information security perceptions, practices, and levels of awareness of the rules of staying safe in cyber space.

A survey was administered to 200 randomly selected users of web-based applications from a higher institution in Nigeria. The respondents were selected randomly from the population who engage in either or a combination of these: online shopping, operate email/social media accounts, and online financial transactions. The study used quantitative methods to analyze the gathered data. The data analysis was performed by using the statistical package for social scientist (SPSS). The result of the study identified the weakest point that is most vulnerable to cyber attacks; the categories of cyber users that are most vulnerable; and the common mistakes that expose them to possible attacks.

(Keywords: cyber security, threat, user awareness, vulnerability, cyber crime, security breach, social engineering)

INTRODUCTION

The cyberspace has made the process of doing business, governance, social networking, and communication quite seamless (Hansen and Nissenbaum, 2009). With the Internet able to handle almost every kind of activity, both old and new businesses have moved their trade online in order to deliver quality service and stay ahead of competition. In the same vein, the increasing services provided online has made individuals increasingly dependent on the Internet for their daily needs. These activities include online shopping, email communication, social interactions, health information searches, and financial transactions (Microsoft, 2014). These activities have attracted criminals who have equally moved their trade online.

To counter the activities of these criminals, organizations have had to device means of securing their critical infrastructure in cyber space (Hart, 2011). Cyber security is the protection of the network, information and software in cyber space. Regardless of the billions of dollars spent on cyber security infrastructural solutions, a simple action such as an erroneous click could render an organization's security efforts meaningless. Attackers have countless times preyed on the ignorance or vulnerability of cyber users to obtain information that is used to future attacks (Frumento et al, 2015).

An information system is said to be vulnerable to attacks when its defenses are weak. The weak defense could be from the human, machine, or software angle. The attacks could be in the form of content interception, interruption, modification, or fabrication (Hansen and Nissenbaum, 2009).

The goal of securing a network system in cyber space is to ensure that the three properties of data security (confidentiality, integrity and availability) are maintained. Any successful attack on an information system renders one or more of these properties questionable. With the ever-increasing number of people having one form of smart device or the other, Klimburg (2012) estimated that by 2020, fifty billion devices will be connected to the internet with an individual having more than one device with online connections. This can be translated to mean more user data online and more potential victims for cyber criminals unless they possess the security awareness to enable them to identify

potential threats and the skills to counter attacks (Pinola, 2014).

STATEMENT OF PROBLEM

Many individuals regularly use social network sites (SNS) for private or business communication (Ballagas, et al., 2004). With reports indicating that users are the weakest link in the IS security chain, cyber criminals have taken advantage of this weakness to target this category of security risk (Pinola, 2014; Frumento, et al., 2015; Compromise, 2017).

Security awareness as well as training on security is considered the most effective countermeasure against security attacks (Parsons, et al., 2010). Many studies have looked at the human element of cyber security from the employee or work force angle. Workshops and training are regularly organized for this category of users. What about the human elements external to organizations who access third party online platforms like bank customers, applicants to universities, social network site users, email account holders, and online shoppers. How cyber literate are they? Do they undergo any form of orientation before getting on platforms to access and interact with an organization's website?

With a prediction for 2019 by a cyber security group (https://www.cybersecurityintelligence.com) that there will be an increase in the number of attacks through smart phones and personal devices as the number of persons connecting to the internet continue to increase, This study is to understand the perception and awareness of security of these category of cyber users.

OBJECTIVE OF STUDY

The main objective of this study is to investigate the level of security vulnerabilities created by the various categories of cyber users who access the internet for work, social activities and for business. The study seeks to determine the extent of cyber users awareness of the likely threats they face in cyber space in the course of their using the web and providing business, family, financial, or health information as well as precautions they take to protect themselves and counter successful attacks.

METHODOLOGY

To evaluate the human factor in cyber security in Nigeria, the study employed the use of a survey which covered respondents' awareness, perceptions, and practices of cyber security issues. The survey instrument was administered randomly to 240 cyber users which comprised of university employees and students from a public university in Edo State Nigeria. Respondents are those who answer yes to at least one of these:

1. Holds at least one active social media account on Facebook, Twitter, Instagram, Linked-In, etc.),
2. Visit the cyber space for research purpose,
3. Engages in online banking,
4. Has an active email account,
5. Use Online shopping sites where personal information including financial information (credit/debit card details) are supplied, or,
6. Any other category of cyber user who has provided personal, health or financial information online to create an account, etc.

The survey comprised of 30 cyber security questions on basic knowledge of rules guiding one while on the internet. The questions are on user behavior, perception and practice on cyber space. Respondents are expected to tick a "Yes", "No" or "Don't Know" as response to each of the questions. The responses were then analyzed using the statistical package of social scientist (SPSS). The data collected were analyzed to show: responses by each gender; staff and students; and age group of respondents.

This study contributes quantitative evidence for the phenomena that shape perceptions and behavior of respondents on cyber security.

ANALYSIS

The data collected was validated and responses that didn't fulfill the requirements for the survey were excluded. This left a total of 142 acceptable respondents giving an overall response rate of 71%. Figure 1 shows the distribution of respondents by gender. Table 1 and Figure 1

indicate the age range of respondents and Table 2 shows the platform mostly visited by respondents.

Table 1: Distribution of Respondents by Gender.

RESPONDENT	GENDER	Total	%
Staff	Male	28	19
	Female	21	15
Students	Male	56	39
	Female	37	27
Total		142	100

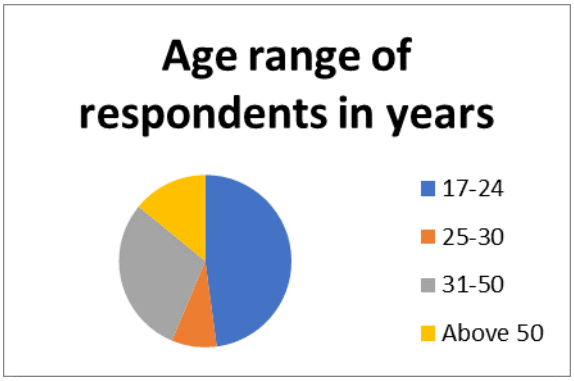

Figure 1: Age Range of Respondents.

Table 2: Regular Activity on the Web.

S/N	PURPOSE OF VISITING THE WEB		Total	%
1	Social Media Activity (Facebook, Twitter, Instagram, Linked-In)	Staff	37	75.5
		Students	72	77.4
2	Online banking	Staff	35	71.4
		Students	84	90.3
3	Email account activity	Staff	49	100
		Students	93	100
4	Information Search	Staff	49	100
		Students	93	100
5	Work related / education related search	Staff	49	100
		Students	93	100

Majority of the respondents are very active on the internet and carry out most of the common activities usually carried out on the internet by regular users. They include All respondents (both staff and students – 100%) have email accounts; carry out information search and are involved in work related or education related search. Over 70% of respondents are involved in online banking and social media activities.

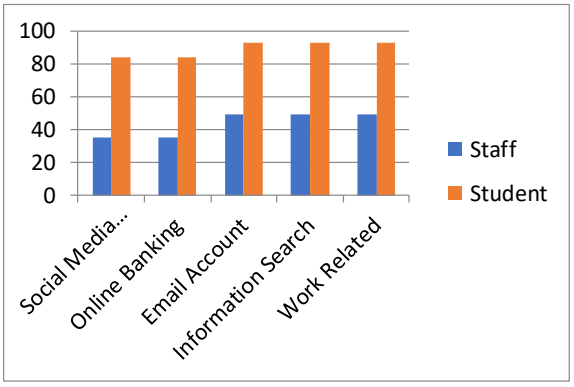

Figure 2: Respondents use of Social Media and On-Line Services.

Table 3 shows their major concern of respondents while online either for business or pleasure.

Table 3: Major Concern while on the Web.

S/N	Biggest Concern/Fear When Online	Respondents	Total
1	Identity theft/impersonation	Staff	35
		Students	62
2	Financial loss	Staff	49
		Students	93
3	Email account loss	Staff	15
		Students	32
4	Cyber bullying	Staff	12
		Student	22
5	Virus Attack on computer/phone	Staff	39
		Students	88

The major fear of cyber users is the fear of financial loss and all respondents agreed that that is their major fear as all the 104 respondents of the 142 who participated in the survey are involved in online money transactions. All of them have loss of money online as their biggest worry. This is followed by virus attack on their devices.

Table 4: Awareness of Online Attack Types.

ATTACK	NUMBER AWARE	%
Malware	38	27
Phishing	35	25
Worm	32	23
Trojan horses	37	26
Virus	142	100
Social engineering	20	14

As shown in Table 4, all respondents (100%) have heard or had experience of virus attack. Majority of them do not know anything or have never heard about malware, worm, Trojan horse or social engineering as Table 5 indicates. For example, only 14% understand what social engineering is; 23 know about worm and 23% know about Trojan horse. They may have been attacked by these but are not aware of their existence or do not understand the meaning of the term. Further investigation revealed that those who understand are mostly ICT students and staff.

Figure 3: Those Who Have been Affected by Cyber Attacks.

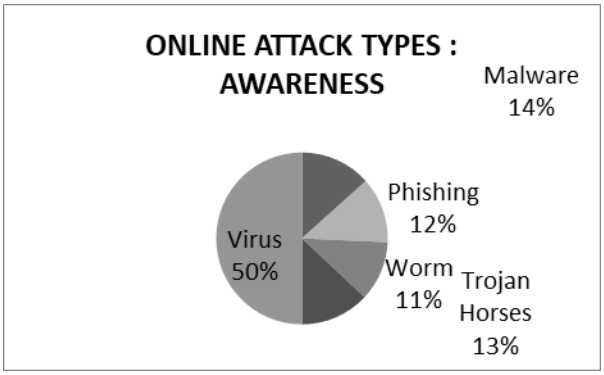

Table 5: Summary of the Responses of the Survey Participants.

S/N	USER BEHAVIOUR /PERCEPTION / PRACTICE	Yes	Yes %	No	No %	DK	DN %
1	I have received computer /information security awareness training	35	25	98	69	9	6
2	I know how to recognize unsecure website address	21	15	80	56	41	29
3	I had the opportunity to undertake computer security training, but I didn't participate	89	67	43	30	10	7
4	I have shared my password to my online account with friend/family	86	61	42	30	14	10
5	I sometimes forget to log off when my computer or phone is unattended to	101	71	31	22	10	7
6	Out of curiosity, I sometimes open unsolicited email attachment to know what it contains	76	54	45	37	21	15
7	I sometimes borrow USB stick (flash drive) from friends and colleagues	107	75	21	15	2	1
8	I have many times left printed sensitive documents exposed	93	65	29	20	20	14
9	The password to all my online accounts are written down somewhere in case I forget	58	41	69	49	16	11
10	I feel safe online even without up-to-date antivirus in my computer system	91	64	47	33	4	3
11	I make use of pirated software	114	80	8	6	20	14
12	I have personally experienced at least one cyber attack	75	53	21	15	46	32
13	It is okay to access my files from cyber cafes	83	58	19	13	30	21
14	I have been a victim of online fraud? (e.g. identity theft, ATM card fraud, online banking theft, phishing)	72	51	40	28	30	21
15	My work/home computer has been infected by malicious software (e.g. keylogger, spyware, virus)	59	42	51	36	32	23
16	I reuse the same password for several user accounts (e.g. personal email account, work email account, social media account, online shopping account)	87	61	34	24	21	15
17	I write down a password that is difficult to remember	56	39	67	47	19	13
18	My personal/home computer has no logon password	102	72	31	21	9	6
19	Have checked my bank account balance while logged into a public Wi-Fi network	102	72	25	18	15	11
20	Have made an online purchase or transferred money while logged into a public Wi-Fi network	88	62	47	33	9	6
21	Have entered my username and password on a web site whose address starts with "http://"	34	24	30	21	78	55
22	I have allowed someone else to use my home/private computer without my supervision?	88	62	29	20	25	18
23	I understand the difference between website addresses that start with http:// and https://	41	29	24	17	77	54
24	Have entered my ATM/credit card information on a web site whose address starts with http:// (e.g. http://www.example.com/)	34	24	26	18	82	58
25	Have you ever given your ATM / credit card information over the phone (text message, WhatsApp, or voice?	72	51	70	49	-	0
26	Before installing any mobile app, do you take time to read the condition for use?	27	19	89	63	26	18
27	Do you change your password regularly for security purpose?	20	14	101	71	21	15

FINDINGS

Finding from the analysis is summarized in Table 6.

Table 8: Summary of Survey Responses.

S/N	USER BEHAVIOUR/ PERCEPTION/ PRACTICE	FINDINGS
1	COMPUTER SECURITY TRAINING	All respondents have had the need to visit the web many times for the purpose of research, work or personal purpose. Their purposes of visiting the web are diverse. The security awareness of both students and staff who participated in the survey is relatively low. Only 35 (25 %) have had any form of information security training. A further investigation revealed that 30 (21%) of the 35 respondents who have had IT security training were either IT professionals or computer science students. For the rest of them (65%), they tend to learn on the go, in most cases after suffering a setback like credit card fraud or malware attack. This can be likened to driving a vehicle without driver's license. The absence of security awareness training has resulted in the many mistakes made by respondents while using the internet. Over 70% of respondent haven't received any form of information security training yet they navigate the internet without knowledge of the risk that they face.
2	SECURITY OF DEVICES AND SENSIVE FILE	71% have at one time or the other given their password to family or friend to access their account The risk faced when people forget to log off include loss of money, jobs and integrity. 78% of respondents are guilty of this activity. As many as 58% have accessed their sensitive file from cyber cafes while out of curiosity, some (54%) sometimes open unsolicited email attachment to know what they contain. 76% of respondents are exposed to virus attack as they use USB sticks borrowed from friend and colleagues.
3	SOFTWARE USAGE	81% of respondent do not bother or take note that they should read the condition for use of the apps that they install on their mobile devices. 67% feel comfortable on the internet with outdated antivirus or have non at all on their computer systems. Some of them are employees of the case organization and they use their system to carry out official duties as well as personal research work. 80% of respondents have at least one pirated software on their computer while 14% do not even know whether the software application on their device is pirated or not. This means these persons are exposed to having software embedded malware (Ransomware, Trojans and virus) in their computers. The risk these persons are exposed to include: access to personal records, access to financial and confidential information, identity theft and even destruction of data. What they don't understand is that most pirated software have Windows Update disabled and FireWall rules changed (Microsoft Australia). respondents do not see or understand the danger of using the internet without antivirus on their systems (computer or smart devices). 4 respondents don't even know whether they have antivirus installed. They have no idea of how to check whether their computer system or phones have antivirus yet they go online to shop and visit social media sites where they must have provided their personal information in order to create accounts on such platforms.
4	CYBER ATTACK EXPERIENCE	Over 53 % have experienced cyber attack; 32% didn't even know whether they have been attacked or not. The later just remembered that at some points, their systems were not functioning as usual or their hard disk crashed or the system wouldn't boot etc. 72% access their banking platform to Wifi networks to check account balance while 62% carry out financial transactions like online money transfers from public Wifi connections
5	PASSWORD PROTECTION	72% have mobile devises that are not passworded. This means anyone who has access to where the computer is can have access to it content. 62% have allowed some else to use their computers without supervision. Even of the ones that password their computers, 61% use the same password for several user accounts and/or write them down (39%) so that they would not forget. People still write down passwords to online accounts as this study indicates that 52% still engage in the act. As for the safe rule of regularly changing passwords, 71% are guilty of sticking to one password for a long time.
6	EMAIL ACCOUNT HANDLING	41 % have the email password written down somewhere
7	CREDIT CARD FRAUD	56% could not differentiate between an https:// and http://. As a result they do not know whether a site is safe or not. This means they could visit a cloned website and not even know the difference. Over 70% of the web visitors most likely are not aware of the importance of getting knowledgeable about the internet and the risks of navigating ignorantly. Some of them have confessed to being victims of credit card fraud. 58% have fallen victims of credit card fraud. 51% give out their financial information like credit card detail over the phone or as text messages to family members to enable them make payment for goods, services or pay school fees.

CONCLUSION

There will always be cyber illiterates as more and more organizations are pushing more of their services online. The study concluded that most of the commonplace actions that users take online are what lead them to data and financial loss. Except for IT professionals and a few IT students, majority of the respondents are uninformed of the many risks they face in cyber space. Also most of the respondents who have fallen victim to cyber criminals were as a result of social engineering, a situation where victims were lured into providing confidential information or clicking on fake links. Had they the simple tips of staying safe in cyber space, many of the mistakes would have been avoided.

The study reports that majority of cyber users have not been part of any form of security related training, workshop or seminar before entering the cyber space. This findings from the study is an indication that cyber users are not fully aware of the dangers that lurk in cyber space. They therefore learn the hard way through loss of valuable information or financial asset. There is therefore the urgent need to educate this category of human elements external to the organization as organizations tend to focus mainly on their workforce.

Organizations tend to spend a lot of funds on the acquisition of technology to protect and detect threats. Reports have established that the human factor is the weakest point in the cyber security chain and cyber criminals are focusing their attention on their direction. Users should be adequately sensitized on how to work, play and do business online in which case the cyber space will be protected from the end user point. That indeed will be a formidable force against cyber crime and criminals. Most educational institutions in Nigeria have platforms for online application, registration and payments. There is the need to provide workshops for fresh students as not all of them are cyber literate. Many respondents, especially students responded that they visit cyber cafes through which sensitive information like passwords and financial information are supplied during their numerous applications, registrations and online payment activities. These actions make them vulnerable to attacks. There is the need to provide information system security training to students at the secondary school level. This should cater for all potential cyber users. It could be part of their computer science curricular. It is at this age many of cyber users start using the internet to search for information to find answers to school assignments, open bank accounts, shop online and then apply for higher education. Organizations with online platforms need be constantly remind users of the risk they face online as many do not know the gravity of certain actions they take.

Attackers are always offering free software, free downloads etc. Organizations should find ways to provide information to their clients who use their online services about new strategies by cyber criminals. They need to understand the characteristics of social engineering attacks as new strategies are introduced by hackers.

REFERENCES

1. Ballagas, R., M. Rohs, J.G. Sheridan, and J. Borchers. 2004. “Bring Your Own Device (BYOD)”. *Proceedings of the Workshop on Ubiquitous Display Environments*. Ubicomp. 2004 .

2. Hansen, L. and H. Nissenbaum. 2009. “Digital Disaster, Cyber Security, and the Copenhagen School”. *International Studies Quarterly*.

3. Frumento, E., R. Puricelli, F. Freschi, D. Ariu, N. Weiss, C. Dambra, and I. Cotoi. 2015. “The Role of Social Engineering in Evolution of Attacks”. *Advanced Social Engineering and Vulnerability Assessment Framework*. Source: http://www.doganaproject.eu/images/

4. Hart, C. 2011. “Mobilizing the Cyberspace Race: the Securitization of the Internet and its Implications for Civil Liberties”. *Cyber - Surveillance in Everyday Life: An International Workshop*. May 12-15, 2011, University of Toronto.

5. Microsoft. 2014. “How to Recognize Phishing Email Messages, Links, or Phone Calls”. http://www.microsoft.com/security/ online-privacy/phishing-symptoms.aspx. Accessed 12/10/2018

6. Parsons, K., D. Calic, M. Pattinson, M. Butavicius, A. McCormac, and T. Zwaans. 2017. “The Human Aspects of Information Security Questionnaire (HAIS-Q): Two Further Validation Studies”. *Computers & Security*. 66: 40–51.

7. Pinola, M. 2014. “The Most Important Security Settings to Change on Your Router”. http://lifehacker.com/the-most-important-security-

settings-to-change-on-your-1573958554.
Retrieved: 25/11/2018.

SUGGESTED CITATION

Akpon-Ebiyonare, D.E. and S. Konyeha. 2019. “Cyber Insecurity: End User Vulnerability Awareness and Perception Assessment”. *Pacific Journal of Science and Technology*. 20(2):88-94.