International Research Journal of Advanced Engineering and Science
ISSN (Online): 2455-9024

A Survey of Cyber-Security Practices in Nigeria

Ahmad Rufai[1], Salisu Modi[2], Buhari Wadata[3]
[1, 2, 3]Department of Computer Science, Sokoto State University, Nigeria
Email address: rufaiahmed5 @ gmail.com, salisumodi @ gmail.com

Abstract**—** *In recent years, developing countries have experienced fast growth in internet usage. As a result, there has been rapid development in the deployment of information and communication technologies in these countries. Information is often exchanged through these technologies by users. Over the years, this information has been under attack by those with malicious intent. While there is growing awareness about these threats in the Western world, awareness in developing countries is poor. Nigeria is a developing country in Africa that has experienced rapid growth in internet and mobile technology usage with a reported mobile phone teledensity of 97.47% and nearly 186 million active mobile internet subscriptions {NCC, 2019, Industry Statistics}. As these advancements are new, the citizens of this country may not be aware of the threats associated with them. This paper examines the level of cyber-security awareness amongst the general public using a quantitative online survey. A sample size of 176 Nigerians responded to the survey. The results from the survey indicate that the knowledge of cybersecurity is moderate although, several cases of poor practices such as choice of weak passwords, free anti-virus software, and password sharing were observed. It was also found that despite the presence of ngCERT, a body tasked with the responsibility of managing the risks of cyber threats in Nigeria and also the first point of contact for victims of cyber-crime, many of the respondents (77.84%) are not aware of this. Thus, there is an immediate need for concerned agencies to create more awareness programs to enlighten citizens on the dangers of poor cyber-security practices*.

I. INTRODUCTION

The world is in the so-called Information Age, characterized by rapid deployment of information and communication technologies. Organisations in this age rely heavily on information technology tools to interact with their customers and deliver services. Similarly, individuals utilize these tools to communicate with each other as well as to access services from both government and private organizations. Most of these interactions are made through the World Wide Web, emails and mobile applications. Thus, the use of these technologies has risen exponentially in recent years (Alotaibi, et al. 2016). According to the recent data from the International Telecommunication Union (ITU), there are 4.1 billion internet users worldwide, this represents 53.6% of the global population (ITU, 2019). Internet usage in Africa has also increased over the years, with data from ITU showing an increase from 2.1 in 2005 to 24.4% of the continent's population using the internet in 2018 (ITUnews, 2018). Nigeria's internet penetration rate was 27.7% in 2017 (ITU, 2019). These figures are expected to grow given the proliferation of mobile phones, the fast pace of internet penetration and technology deployment in both developed and developing countries.

Due to the rapid growth in communication technologies and the advantages they provide, organizations now rely heavily on them to improve the efficiency of their processes and to deliver effective services, thus further integrating technology in our daily lives. Daily activities such as shopping, banking, and entertainment are now carried out online using mobile devices. However, whilst these technologies provide easy access to information and a chance to conduct such activities anytime and anywhere, they also provide an avenue for those with malicious intent to misuse or destroy such information (Alarifi, Tootell, & Hyland, 2012). Over the last few years, crimes associated with these technologies have risen significantly. According to Symantec Corporation, 978 million people in 20 countries were affected by cybercrime in 2017 alone (Symantec, 2017). The cost of cybercrimes according to a 2018 study by McAfee and a think tank, the Centre for Strategic and International Studies (CSIS) is estimated at $600 billion, this figure is up from $500 billion the last time a similar study was conducted in 2014 (Lewis, 2018).

Lewis believed the reasons for this growth are largely due to the adoption of new attack technologies, an increase in internet users from countries with weak cybersecurity and increased ease of committing cybercrime with the growth of Cybercrime-as-a-Service.

Tackling cybercrimes is challenging for both developed and developing countries, this task is even more challenging for developing countries largely due to their weak cybersecurity frameworks. A study by (Kshetri, 2010), found that most organizations in developing economies adopt technologies without considering their security problems thus subjecting their technological infrastructure to cyber-attacks. Also, many internet users in the developing world are inexperienced and not technically savvy. This is a big problem especially with the rate of growth of Smartphone usage in these countries (Poushter, Bishop, & Chwe, 2018).

Nigeria, which is one of the fastest developing countries in Sub-Saharan Africa, has seen tremendous growth in internet usage and deployment of communication technologies in recent years. According to the Nigerian Communication Commission (NCC), the country's telecommunication regulatory agency, In January 2019, reported a mobile phone tele-density of 97.47% and nearly 186 million active mobile internet subscriptions. This shows that more than 90% of Nigeria's population which is currently around 195 million are connected to the internet. Online banking, electronic commerce and social media for communication are relatively new in Nigeria. The proliferation in the use of the internet in Nigeria began in 2008, when it was reported that for every 100 persons, 15 are connected (Vanguard, 2010). Therefore, it can be assumed that the importance of cybersecurity and the

Ahmad Rufai, Salisu Modi, and Buhari Wadata, "A Survey of Cyber-Security Practices in Nigeria," *International Research Journal of Advanced Engineering and Science*, Volume 5, Issue 3, pp. 222-226, 2020.

International Research Journal of Advanced Engineering and Science
ISSN (Online): 2455-9024

security measures to be taken against cyber-attacks are limited within the general public.

According to the country's National Information Technology Development Agency (NITDA), in 2018, 60% of Nigerian firms suffered cyber-attacks, 43% of which are small and medium enterprises which are the backbone of the country's economy (Osuagwu, 2019). Thus, it is very important to assess the level of cyber-security awareness in the country. Besides, most studies on cybersecurity awareness in the literature are carried out in western countries. Nigeria as a developing country is different from these countries, the culture, diversity and the understanding of cybersecurity differs. Thus, this paper seeks to feel this gap by focusing on the information security awareness of the people of Nigeria. To the best of the authors' knowledge, this study is the first to be carried out at this scale.

II. Materials and Methods

Surveys were used as the research approach for investigating and understanding the level of cybersecurity awareness among the people of Nigeria. This approach was adopted because we aim to gather data from a large sample of Nigerians. Thus, surveys in the form of questionnaires are the most suitable. Moreover, as the study seeks to get inputs from all over Nigeria, we decided that online surveys would be most appropriate. The language of the questionnaire was English and the questions were selected from questionnaires of similar studies in the literature notably, we selected questions from the studies by (Alarifi et al., 2012; Alotaibi et al., 2016). The questionnaire comprises of 13 questions. The first part of the questionnaire contains questions that aim to obtain general information such as users' demographics, level of education, internet skills, devices used to access the internet and purpose of internet usage. The second part of the questionnaire targets users' cybersecurity awareness. We used eSurv, a popular free online survey tool recommended by (Farmer, Oakman, & Rice, 2016) as the most appropriate when collecting non-personally identifiable data. We ensured a high response rate by distributing the link to the questionnaire on social media platforms such as Facebook, Twitter, and WhatsApp. As a result, we were able to obtain 176 responses. The period of the survey was between February and March 2019.

III. Results

176 Nigerians took part in the study, there was no null response as all questions were answered by the participants. The questionnaire result which is in two parts; user demographic/general information and cybersecurity awareness is presented below.

User Demographic and General Information

152 (86.6%) were male and 24 (13.6%) were female. This disproportionate female response confirmed findings in earlier studies particularly, the study by (Poushter, 2016) were gender gaps on many aspects of technology use, including the internet was observed in African nations. The percentage of the participants' age group to the nearest whole number (31%) were aged 18-29, (65%) were aged 30-39, (4%) were aged 40-49 and (1%) were aged 50 and over. Out of the 176 participants, (2%) had secondary or primary education and (98%) had tertiary education. With regards to the participants' internet access, (85%) said they had access to the internet throughout the day and (15%) said they access the internet only once or twice a day. In terms of internet skills, (3%) of the respondent had beginner skills, (51%) had intermediate and (46%) had expert skills. The popular devices used by respondents to access the internet are; pc/laptop (5%), smartphone (47%), tablet (2%). A significant number of the respondents, (46%) said they used pc/laptops, smartphones, and tablets to access the internet.

Cyber Security Practices/Awareness

In this section, we asked respondents about their cybersecurity practices. The first question asked if respondents physically secure their portable devices (e.g. laptops, mobile phones, etc.), (67%) of respondents indicated that they kept their devices in a secure place, (28%) said they sometimes physically secure their devices while (5%) said they do not physically secure their devices making them prone to theft or loss. Physically securing devices specifically those with sensitive data is an important practice in cybersecurity, as access to these devices by those with malicious intent can put organizations and individuals at risk.

The second question asked respondents if they secure their devices using passwords. Securing computing devices using passwords is an important practice in cybersecurity. Users are encouraged to do this to prevent unauthorized access, which if occurred can lead to data and information loss and sometimes financial loss Users' identities can also be stolen and used in conducting criminal activities which may put them into legal trouble. Thus, protecting devices using a password is an important practice in cybersecurity. The results from our survey show that most of the respondents (94.3%) use passwords to log into their devices. These findings are presented in Table I.

TABLE I: Password use

Do you secure your devices using login passwords? (N=176)		
	percentage	count
Yes	94.3%	166
No	5.7%	10

Though, most of the respondents said they used a password to protect their devices however, the strength of the passwords determines the level of security they can provide. Systems protected using weak passwords are susceptible to break-in attacks. Therefore, we asked the respondents their password creation practice, we wanted to find if they create passwords using personal information such as names, date of birth, mobile phone number, etc. Table II below shows that more than half of the respondents used personal information to create passwords. We believe this is a poor security practice and is a well-known problem in the security domain that including personal information in passwords aids attackers in passwords guessing or brute-force attack (Castelluccia, Chaabane, Dürmuth, & Perito, 2013). It is believed that the

Ahmad Rufai, Salisu Modi, and Buhari Wadata, "A Survey of Cyber-Security Practices in Nigeria," *International Research Journal of Advanced Engineering and Science*, Volume 5, Issue 3, pp. 222-226, 2020.

International Research Journal of Advanced Engineering and Science
ISSN (Online): 2455-9024

limitation of human memory is the reason why users tend to create passwords using personal information. The idea is that such passwords can be easily remembered (Li, Wang, & Sun, 2017). Nowadays, most personal information on users can be found online without much hassle, thanks to the exponential growth in social network sites such as Facebook and Twitter coupled with users' open attitudes of sharing personal information online, password cracking is now easier than ever.

TABLE II: Use of personal information to create passwords

Do you create passwords using your personal information such as names, DoB and phone number? (N=176)		
	Percent	Count(N)
Yes	48.86%	86
No	51.14%	90

Users can reduce their susceptibility to password guessing or brute-force attack by creating strong passwords. Experts believed strong passwords are those that are long, have at least 15 characters, contain a mix of characters and letters (both upper- and lower-case) (Empey, 2018). We asked the respondents how strong they believe their passwords were although we had to make sure the respondents know what is considered a strong password. Therefore, we included this explanation as part of the question, then we asked them to rate how strong they consider their passwords are based on the provided information. Figure 1, shows 58% of the respondents think their passwords were very strong, 39% believed their passwords were strong and 3% believed they have very weak passwords.

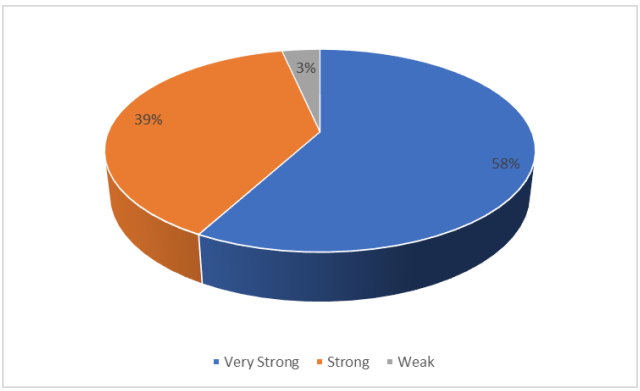

Figure 1: Respondents' password strength

Another important practice in cybersecurity is the regular change of passwords. Users are frequently advised to change their passwords regularly as part of a precautionary measure to ensure access is ended in case of account hijack. We asked respondents how often they changed their passwords. 12% said regularly, 66% said sometimes and 22% said never. When asked whether they share their passwords with someone, 15 respondents skipped this question. We believe this may be attributed to the sensitive nature of the question. Nevertheless, Table III presents the responses of 161 respondents that attempted this question.

The findings in Table III shows that 62% of the respondents do not share their passwords, perhaps for security concerns. However, it also shows that 24% of respondents share passwords with their families, 9% with friends and 5% with system administrators. This raises the question of why people share passwords with family and friends as opposed to system administrators. Our findings are similar to those of (Alarifi et al., 2012), where it was found that a high level of Saudi's (130 out of 363) share their passwords with family members. (Alarifi et al., 2012) believed it is due to the cultural beliefs in Saudi, where members of the family are considered more trustworthy than those who are not members of the family. We believed a similar case applies in the Nigerian context.

TABLE III: Password sharing

Do you share your passwords with any of the following? (N=161)		
	Percent	Count(N)
Family	24.31%	44
Friends	8.84%	16
System Administrators	4.97%	9
None	61.88%	112

Being safe online nowadays requires knowledge of existing cyber threats and the protection mechanism available. Aside from viruses, which most of the respondents are aware of, there are other cybersecurity threats including phishing, denial of service, identity theft, etc., that may lead to loss of data, confidentiality, and availability of services. We asked the respondents to indicate if they are aware of some popular cyber threats. We also compare the results from this question with the results of similar research conducted on Saudi Arabians by (Alarifi et al., 2012), Table IV presents our findings.

TABLE IV: Cybersecurity threats awareness

Knowledge of existing cyber threats		
	Saudi Arabia	Nigeria
Viruses	87.2%	92.1%
Spam emails	57.8%	86.9%
Phishing	29.7%	44%
Denial of Service (DoS)	7.4%	36.9%
Identity theft	25.5%	73.8%

The findings in Table IV show that most of the respondents are aware of the listed threats. Specifically, Viruses, Spam emails, and identity theft are the most known threats by respondents. The results from the survey also show that respondents from Nigeria tend to have a better knowledge of these threats. However, due to the differences in sample size, a conclusion cannot be made. We also found that Phishing, despite being a serious threat in cybersecurity is not widely known by respondents from both Nigeria and Saudi Arabia. Phishing which is the use of social engineering techniques and technical subterfuge to lure users to fake websites where their sensitive information such as credit cards are harvested is a major problem in cybersecurity today. According to a recent report by the Anti-Phishing Working Group (ATPWG), the total number of phishing sites detected rose to 266, 387 in the 3rd quarter of 2019 from 182, 465 in the 2nd quarter of the same year. This almost doubles the 138, 328 phishing sites detected in the 4th quarter of 2018 (APWG, 2019). The trend can be seen in Figure 2. The APWG also

Ahmad Rufai, Salisu Modi, and Buhari Wadata, "A Survey of Cyber-Security Practices in Nigeria," *International Research Journal of Advanced Engineering and Science*, Volume 5, Issue 3, pp. 222-226, 2020.

keeps a record of the number of unique phishing emails it receives from the general public and consumers, this emails also increases to 122,359 in the 3rd quarter of 2019, from 112,163 in the 2nd quarter of the same year. Thus, there is a need for internet users in these countries to be enlightened more about these attacks and ways to ensure they do not fall victim to such attacks.

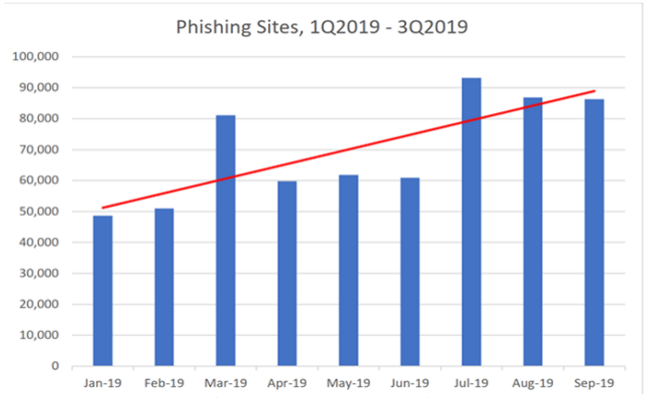

Figure 2: Total number of phishing sites detected from Jan 2019 to Sep 2019 (Source: Anti-Phishing Working Group).

While being aware of the existence of security threats is good, however, awareness and protection are two different things. Internet users are required to be both aware of the existing threats and to employ several defensive mechanisms to protect themselves. Thus, it is good to know what security mechanisms are used by the respondents to safeguard themselves against cyber threats. When asked this question, 51% of the respondents said they used Anti-virus software, 11% said they used Anti-spam software, 9% said they used Anti-spyware and 29% said they used internet security software. The results show that most of the respondents rely on Anti-virus and internet security software for protection. From the authors' experience, one of the reasons people in Nigeria rely on Anti-virus and internet security software for protection is because they are free. To confirm this, our next question asked respondents to select the category of software they used for protection. Majority of the respondents (48%) said they used freeware-a software that is freely distributed to users at no cost, (21%) said they used licensed protective software and (31%) indicated they used both free and licensed software as a protective mechanism. The fact that the majority of the respondents used Freeware is a big concern as software in this category tend to offer only the basic protection. (Mediati, 2010) compared free and paid anti-virus software in terms of their malware detection capability, and speed. Findings from the study found that paid antivirus products do slightly better than their free counterparts. Specifically, paid anti-virus was better at both detecting and removal of malware.

Cyber-criminals nowadays are very active and are frequently launching more sophisticated malicious software. It is often a race, between those providing the defensive mechanisms and the cybercriminals. Thus, anti-virus software vendors provide frequent updates to users as a response to these increasing number of threats. Users, therefore, are required to update their protection software regularly. In line with this, we asked respondents their software update practice, (46%) said they update their protection software regularly, (40%) said they do that every three months or more and (14%) said they do not update their protective software.

The internet today is full of threats, which can affect the integrity of data. Viruses and trojans do not just steal users' data but can also erase them. Users, therefore, are often advised to back-up their data regularly. There is also the increasing use and deployment of ransomware; a software that encrypts user's data and demands a ransom before it is decrypted. Thus, backing up data is an essential practice in cyber-security. We seek to find users' data back-up practice by asking them how often they back-up their data. (43%) said regularly, (49%) said sometimes and (8%) said never. This, therefore, implies that over 50% of our respondents do not have a good back-up practice, making them susceptible to data loss.

In an earlier question, we asked our respondents if were aware of the existence of some cyber threats, we presented the result of this question in Table IV. Equally, we also wanted to know the percentage of respondents who experienced such threats. Therefore, we asked respondents if they have experienced any cybercrime in the last few years. Our findings show that (43%) of our respondents have experienced cybercrime, while (57%) indicated they have not experienced such attacks. This result is alarming and shows that cyber-crimes are also prevalent in Nigeria. In contrast to what is believed by many, that cybercriminals only target developed countries, our results show that even countries in the developing world are being targeted by criminals. The prevalence of cyber-crime has resulted in many countries creating agencies and establishing dedicated lines for their citizens to contact in case they fall victim to such crimes. The idea is to provide enough information to the security agencies to aid in preventing future occurrences and to also lunch an investigation. The Nigerian Government established the Nigeria Computer Emergency Response Team (ngCERT). The agency is tasked with the responsibility of managing the risks of cyber threats in Nigeria's cyberspace through the coordination of incidence response and mitigation strategies (ngCERT, 2020). Unfortunately, Table V shows that 77.84% of the respondents were not aware of where and how to report security incidents. This low awareness would affect the rate at which cybersecurity incidences are dealt with, also, it would affect the overall function of ngCERT.

TABLE V: Incident Reporting

Are you aware of how and where to report cybersecurity incidences in Nigeria? (N=176)		
	Percent	Count(N)
Yes	22.16%	39
No	77.84%	137

Information Dissemination Channels

Table VI shows the responses of the respondents when asked to select which information dissemination channel should be used to create more awareness of cybersecurity in

Nigeria. The result shows that many of the respondents prefer awareness to be carried out using web portals (67.05%) and Advertisement (58.52%).

TABLE VI: Preferred information dissemination channels.

Which of the following do you think would be an effective mechanism to disseminate and create awareness of cybersecurity in Nigeria (N=176)		
	Percent	Count(N)
Web portals	67.05%	118
Newspapers	54.55%	96
Documentaries	36.93%	65
Advertisements	58.52%	103
Seminar/Workshops	53.41%	94
Billboards/Posters	54.55%	96
Other	15.34%	27

IV. CONCLUSIONS

Over the last few years, there has been a significant increase in internet usage and the deployment of information and communication technologies in Nigeria. While this has improved the overall digital outlook of the country, it has also increased the number of cyberattacks. The recent report by Nigeria's information technology body NITDA, confirms this increasing trend. It shows that businesses specifically SMEs are facing increasing cyber threats. We believe the lack of good cybersecurity practices amongst the country's general public as evidenced by our findings in this paper, is a contributing factor in the increased cybersecurity incidence in the country. Thus, there is a need for the country to strengthen its cybersecurity measures, including increasing awareness campaigns and programs.

Conflict of interests

The authors declare no conflict of interest.

REFERENCES

[1] Alarifi, A., Tootell, H., & Hyland, P. (2012). *A study of information security awareness and practices in Saudi Arabia.* Paper presented at the 2012 International Conference on Communications and Information Technology (ICCIT).

[2] Alotaibi, F., Furnell, S., Stengel, I., & Papadaki, M. (2016). *A survey of cyber-security awareness in Saudi Arabia*. Paper presented at the 2016 11th International Conference for Internet Technology and Secured Transactions (ICITST).

[3] APWG. (2019). *Phishing Activity Trends Report* Retrieved from https://docs.apwg.org/reports/apwg_trends_report_q3_2019.pdf

[4] Castelluccia, C., Chaabane, A., Dürmuth, M., & Perito, D. (2013). When privacy meets security: Leveraging personal information for password cracking. *arXiv preprint arXiv:1304.6584*.

[5] Empey, C. (2018). How to create a strong password. Retrieved from https://blog.avast.com/strong-password-ideas

[6] Farmer, R., Oakman, P., & Rice, P. (2016). A review of free online survey tools for undergraduate students. *MSOR Connections, 15*(1), 71-78.

[7] ITU. (2019). Statistics. Retrieved from https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

[8] ITUnews. (2018). New ITU statistics show more than half the world is now using the Internet Retrieved from https://news.itu.int/itu-statistics-leaving-no-one-offline/

[9] Kshetri, N. (2010). Diffusion and effects of cyber-crime in developing economies. *Third World Quarterly, 31*(7), 1057-1079.

[10] Lewis, J. (2018). *Economic Impact of Cybercrime No Slowing Down*. Retrieved from https://csis-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf?kab1HywrewRzH17N9wuE24soo1IdhuHd&utm_source=Press&utm_campaign=bb9303ae70-EMAIL_CAMPAIGN_2018_02_21&utm_medium=email&utm_term=0_7623d157be-bb9303ae70-1940938

[11] Mediati, N. (2010). Free vs. Fee: Free and Paid Antivirus Programs Compared. Retrieved from https://www.pcworld.com/article/210589/free_versus_fee_free_and_paid_antivirus_programs_compared.html

[12] NCC. (2018). *Industry Statistics*. Retrieved from Nigeria: https://www.ncc.gov.ng/stakeholder/statistics-reports/industry-overview#view-graphs-tables

[13] ngCERT. (2020). About Us. Retrieved from https://www.cert.gov.ng/about

[14] Osuagwu, P. (2019). CYBER ATTACK: 60% of Nigerian businesses attacked in 2018. Retrieved from https://www.vanguardngr.com/2019/03/cyber-attack-60-of-nigerian-businesses-attacked-in-2018/

[15] Poushter, J. (2016). Smartphone ownership and internet usage continues to climb in emerging economies. *Pew Research Center, 22*, 1-44.

[16] Poushter, J., Bishop, C., & Chwe, H. (2018). Smartphone ownership on the rise in emerging economies. Retrieved from https://www.pewresearch.org/global/2018/06/19/2-smartphone-ownership-on-the-rise-in-emerging-economies/

[17] Symantec. (2017). *2017 Norton Cyber Security Insights Report Global Results.* Retrieved from https://www.symantec.com/content/dam/symantec/docs/about/2017-ncsir-global-results-en.pdf

[18] Vanguard. (2010). Internet: 13 years of growth from ground zero in Nigeria from 1960- 1996. Retrieved from https://www.vanguardngr.com/2010/10/internet-13-years-of-growth-from-ground-zero-in-nigeria-from-1960-1996/