International Conference on Information and Communication Technology and Its Applications (ICTA 2016)
Federal University of Technology, Minna, Nigeria
November 28 – 30, 2016

Survey of On-line Risks Faced by Internet Users in the Nigerian Telecommunication Space

Elizabeth. N. Onwuka[1], David O. Afolayan[2], Wasiu Abubakar[3], and Joshua. I. Ibrahim[1]
[1]Department of Telecommunications Engineering, Federal University of Technology, Minna, Nigeria
[2]Department of Cyber Security Science, Federal University of Technology, Minna, Nigeria
[3]Department of Computer Science, Federal University of Technology, Minna, Nigeria
onwukaliz@futminna.edu.ng, david.afolayan@st.futminna.edu.ng, wasiu.abubakar@st.futminna.edu.ng, joshua.ibrahim@st.futminna.edu.ng

***Abstract*—In the past ten years, mobile broadband has made an inroad into the country and just in the last six years a twenty-two percent leap has been gained with respect to Internet use penetration. To this end the use of Information and Communication Technology by Nigerians for their various daily activities has gradually but steadily grown. This has remarkably created new jobs, raised the national GDP, and has generally improved ways people live and do business. This advancement however has proven to be a double edged sword as a good number of Nigerians have reportedly fallen victim to different forms of threats online or might have heard about victims of such crimes, which has led to gross distrust in new and existing innovations in the world of ICT. The negative consequence of this on the potential economic alongside technological development that the country could enjoy from the ICT sector is quite obvious. This paper investigates the nature of threats posed at Nigerians as they go online via an online survey. The survey shows 95.2% of respondents are regular internet users with 14.4% as victims of online fraud.**

Keywords-cybercrime; cybersecurity; internet; Nigeria; online risk; telecommunication

I. INTRODUCTION

In the early days of telephony, telephone service comprised mainly voice and there were little or no worries about dangers to the user. However, as developments in the field of Information and Communication Technology began to emerge accompanied by the advent of Internet technology, electronic communication began to take a new face. The Internet, which is a network of networks, was designed to support data communications and has played a major role in the advancements recorded in digital technologies. It has resulted to the convergence of computing and telecommunications, and therefore the expansion of conventional telephony and data communications.

There has been an estimated 22% increase with respect to Internet use penetration in the Nigerian population just between 2010 and 2016, having the national Internet use penetration to be 46.1% in 2016, as opposed to 24% in 2010 [1]. This means that the Nigerian cyber space has experienced some growth over the past years with individual users seeing the Internet services to be quite an imperative aspect of their daily lives. This rapid escalation in users of Internet services as well as the varieties of services available online has, no doubt, contributed to the level of growth the Nigerian economy has experienced. However, this great feat is not without setbacks as it has given rise to diverse kinds of criminal activities including the very popular "419 attacks". Due to the various threats posed by the Internet coupled with the concept of online anonymity, a good number of Nigerians have little or no trust for online activities thereby leveraging the chances of Nigeria gaining possible advancements that could be acquired via exploiting the rich resources provided through telecommunication.

Nigeria currently ranks seventh amongst the top internet users globally with an Internet penetration of 46.1% of her population as at July 1st, 2016, consisting of persons who possess the capabilities to access Internet services from within the reach of their homes, with the aid of any form of device and mode of connection [1]. However, according to the report of G. Sesan *et al* [2] on the survey they carried out in the year 2013, 30% of the respondents affirmed to having been victims of cybercrime activities in the year 2012. Also recorded from a news report according to THISDAY newspaper, the estimated annual cost of cybercrime to the nation is roughly 0.08% of her Gross Domestic Product (GDP), equivalent to N127 billion cash worth[3]. To this end, it is therefore imperative to have a cybersecurity framework that is suitable to meet the evolving safety requirements in the field of telecommunication and cybersecurity as it concerns the nation. It is expected that with the aid of this framework an immense measure of confidence in the Nigerian telecommunication space will be instilled in her populace. This will boost the economy by making the nation connect to the world market via e-commerce. The moral development of the young will also be ensured. The rest of this paper is organized as follows: Section II presents various types of online risk, Section III discusses the methodology adopted for this on-going research, Section IV presents the results as well as relevant discussions, while Section V concludes the paper.

II. TYPOLOGY OF ONLINE RISK

Online Risk is any form of Internet related danger that internet users are prone to. Online risk can still mean the vulnerability of an organization's internal assets that emerges from the organization utilizing the Internet to conduct business [4]. All organizations that conduct some part of their business on the Internet encounter some type of online danger. Vulnerable data can incorporate individual information, data about ventures or information made by frameworks or procedures by which the association works. Online threat does not limit to only organizations rather it involves every internet consumer in one way or the other. Online risk typology is as shown Fig. 1 below.

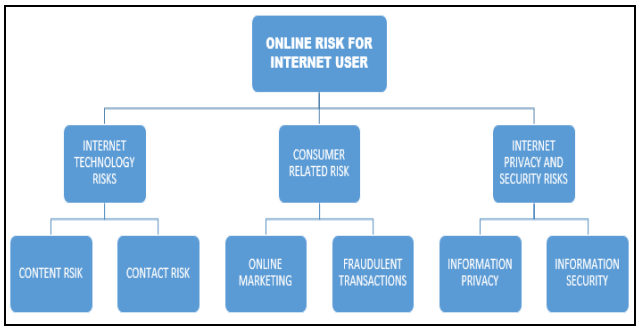

Figure 1. Typology of online risk for internet user. Adopted from OECD [5]

A. *Internet Technology Risk*

Internet technology risk can be grouped into two categories namely:

1) Content risk: Content risks comprise three main sub-categories: (i) illegal content; (ii) age-inappropriate or harmful content; (iii) harmful advice.

2) Contact risk: Contact risks comprises of (i) cybergrooming (ii) online harassment (iii) cyberbullying

B. *Consumer Related Risk*

Consumer related risk is a type of risk that occur to Internet user that engages in buying and selling of goods and services on the Internet [5]. Consumer related risk can be further broken down into two categories namely.

1) Online Marketing which is a category of consumer related risk that involves online advertisement for regulated or age-restricted products to minors such as alcohol, cigarettes and prescription medicines. It raises concerns that such marketing downplays risky lifestyles and links children to suppliers online.

2) Fraudulent Transactions occur when an Internet user enters into a distance sales contract but, having paid do not receive adequate value for money or find themselves tied into subscriptions. The fear of fraudulent transactions is very high in Nigeria which is one of the limitation affecting the growth of E-commerce in the country. Fraudulent transactions can be sub-categorized into 2 groups namely:

- Online fraud and
- Identity theft

C. *Internet Privacy and Security Risks (Mobile Devices and Malware)*

Over the years, smartphones and tablets have gained a worldwide penetration with over 1.4 billion smartphones bought in the year 2015. And it was observed that for every six new phones that were bought five of them ran on an android operating system [6]. From a survey carried out by S. Kempt et al it's observed that 82% of webpages viewed in Nigeria were served to mobile devices 66% of which were requested by users of android devices [7].

Over the past few years it has been observed that the different variants of malware that affect android devices have been on a very high increase even as they grow very much stealthy. Hackers all over the world have been working so hard to develop means by which malware can evade security software that make use of a signature-based solution. In the year 2015 there was a 40% increase in the volume of android malware variants present in cyberspace as against the volume in 2014 [6].

The possibility of having Trojan embedded apps on Google Play store, the official android app store as well as other intermediary app stores is a leading motivating factor why hackers are up and about coding up more sophisticated variants of these malware class [8]. In a report by Alcatel-Lucent [9], it was stated that in the bid to have users install malware infected apps, hackers run a social engineering campaign to gain the trust and confidence of such users. An instance was given of the Not Compatible proxy; whose name came about as a result of the events surrounding it being that prospective victims on visiting infected websites are notified that their browsers cannot view the site, the notification will further include recommendations about downloading and installing an update provided, which surely contained in it the intended to be propagated malware. The following are some of the most common categories of malware that affect mobile devices.

1) Madware: Basically the most prevalent of all the classes is the madware also known as aggressive mobile adware. The term aggressive emanates from the fact that madware are normally applications that make use of aggressive methods to put up advertisements on the notification bar, gallery, messaging application as well as other applications of an android phone user [10]. As at the first half of the year 2013, it was observed that madware had gained a well over 23% presence on the Google Play appstore and that of the sixty-five renowned ad libraries, over 50% were ranked as being aggressive [11].

2) Ransomware: The current rate at which people are faced with the challenge of extortion in Nigeria and ultimately the entire world is quite alarming, the trending utilities provided by Information and Communication Technology (ICT) made use of by almost everyone all over the world everyday aggravates the success-rate experienced by perpetrators of this appalling trend. Malicious persons often use this type of malware to commandeer victims' electronic resources as well as demand for a "ransom" in order that the resources be released [12]. There are currently two types of this malware in existence, the first of which is the crypto-ransomware designed with the intent of finding

and encrypting relevant data saved on a computer system rendering such data inaccessible to the user except he gets the decryption key. The next type of ransomware is the locker-ransomware with the aim of denying a legitimate user access to his computer or mobile device by locking it, leaving him with only the capability to relate with the ransomware so as to pay the demanded ransom [13]. A very renowned variant of ransomware is "CryptoWall", from the group of file-encrypting ransomware and came into limelight near the beginning of the year 2014 [14]. CryptoWall is famous for the fact that it makes use of a well-developed AES encryption scheme which is known to be impenetrable, a distinctive CHM infection mechanism and finally a quite robust C2 activity system running on dark web (i.e. the Tor Anonymous Network). This variant of ransomware is disseminated ubiquitously via spamming campaigns, malvertising schemes along with countless exploit kits [15].

3) Banking-Trojans: Over the years the battle between financial institutions and attackers have never ceased, the internet and various smart devices have also had their role to play in this tug-of-war both towards the positive as well as the negative axis [16]. One of the most illustrious weapons used by attackers against financial institutions is the Banking-Trojan, with the central purpose to gather relevant banking information from a certain victim so as to have adequate information to carry out sham transactions [17]. A good example of a Banking-Trojan is "Infostealer.Shifu" which is a quite sophisticated Trojan with the classic constituents of a well calculated financial fraud. It operates by pilfering a wide selection of authentication details made use of by an infected victim, this is made possible by virtue of a keylogging system that records keystrokes of authentication details typed into web forms, covert operations that harvest private certificates, rootkits that grant the attacker remote access and control over infected system and block channels for external authentication [18].

III. RESEARCH METHOD

A. Research Scope and Setting

The scope identifies the region or domain from which relevant data were gathered for the purpose of carrying out this research. The survey participants were basically obtained from all six geopolitical zones in the federation, having a substantial representation of residents from various parts of the country. The instrument of the survey was a web-based questionnaire administered via social media, e-mail as well as text-messages to various Internet users all over the country. The questionnaire was designed to consist of a six level categorization, category one handled general survey data (i.e. basic demographic data), the next category consisted of questions that cover general internet usage, category three comprised of questions on social media usage, the forth category included questions that compile email usage data, category five contained e-commerce questions and finally the last category probes the user on their level of awareness about online security.

B. Data Collection Instrument

For this study a web-based questionnaire platform served as the primary data collection instrument. The motivation behind selecting this method was as a result of:

- Its capacity to reach out to a larger geographical area as opposed to manually distributed questionnaires or interviews.
- The ease in processing data, being that responses can be automatically collected into a database for the purpose of storage, or directly sent to a data analysis application as well as a spreadsheet for further analysis of the data.
- The possibilities to make available audio and visual directives in order to simplify concepts.
- Existing provisions for sending out reminders to as many participants who are yet to respond to the questionnaire.

C. Proposed Framework Structure

The framework sought to highlight information security measures in the area of business confidentiality as well as modes of governmental security strategy implementation, and also processes put in place to maintain the protection of every Nigerian citizen's privacy and civil liberty.

With an understanding that telecommunication in Nigeria has the potential to cause a quantum leap in the level of development experienced as a nation and is being confronted with various threats present in cyber space that must be abated pronto, this framework is to be established on the basis of the following four areas, which were adopted from the model of the [4] Jamaican national cyber security strategy

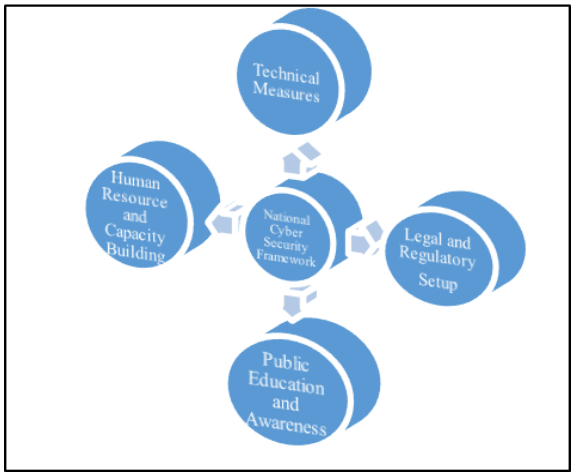

Figure 2. Proposed National Cyber Security Framework

*1) **Technical Measures**:* This makes sure that critical infrastructure remains in state of optimal operation by reason of maximum resilience to cyber threats. It adopts a risk based tactic having both private and public sectors of the federation carry out different levels of risk assessments as well as promoting the adoption of relevant precautionary

measures which will include proper utilization of best practises and standards.

2) ***Human Resource and Capacity Building****:* This section involves the institution alongside sustenance of a consortium of well-trained Cyber-Security experts who will be instrumental to the detection, response and recovery from whatever incidence of cyber-attack and would also be at the helm of developmental research in the area of National Cyber-Security.

3) ***Legal and Regulatory Setup****:* Here efforts are made to bring up existing policy documents and frameworks to ensure that the public is aware of them as well as possible reviews of such legislative documents in order to provide surety of resort for business stakeholders in cases where they stand as objects of a cybercrime incident.

4) Public ***Education and Awareness****:* Stands to be a pivotal part of this framework as it entails fostering educative campaigns targeted at Internet users in both the public and private sectors to retsrain them on matters concerning cyber risks and threats they are exposed to as well as apt actions they could possibly take to stay safe from such incidences.

IV. RESULTS AND DISCUSSION

A. *Description of Collated Data*

From the data collected under Category One: General survey data, Male gender has 89.1% while female gender has 10.9% of the total respondents as seen in Fig. 3, showing that male gender gave more responses as compared to female gender. Fig. 4 shows that, 56.2% of the respondents are aged between 21-30, 24% are aged between 11-20, 10.4% are aged between 31-40 while between age 41-50 we have 6.3% and respondents above age 50 take 3.1%. 83% of the respondents stays in urban area as compared to those respondents that stay in rural area of 17% as described in Fig. 5. This still shows that those in urban have more access to internet than those in rural area.

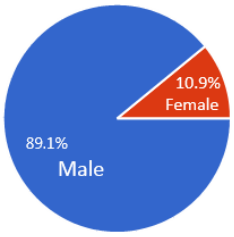

Figure 3. Gender of respondents

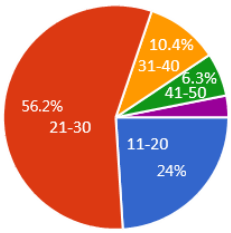

Figure 4. Age group of respondents

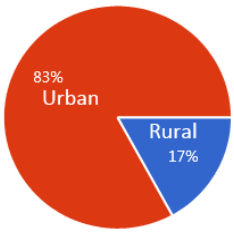

Figure 5. Respondents' locality

Category Two: General Internet Usage Data shows that, 95.2% of the respondents agree they use the internet regularly while 4.8% do not access the internet regularly as represented in Fig. 6. Fig. 7 shows 55.8%, 43.8%, 46.1%, 48%, 25.2%, 4.4% and 4.8% of respondents use Mozilla Firefox, Google Chrome, UC Browser, Opera, Internet Explorer, Safari and Other browser vendors respectively as means of accessing the internet. On devices used to access the internet seen in Fig. 8, 60.2% of all respondents use laptops, 18.8% use desktop devices, 13.3% use tablets, 66.5% use smartphones and 30% use mobile phones.

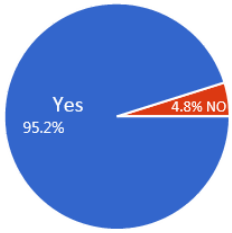

Figure 6. Respondents' internet use

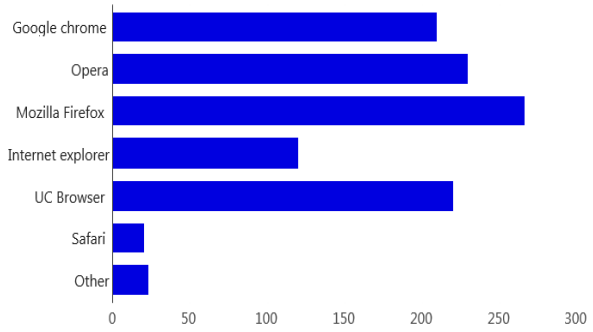

Figure 7. Applications used by respondents to access the internet

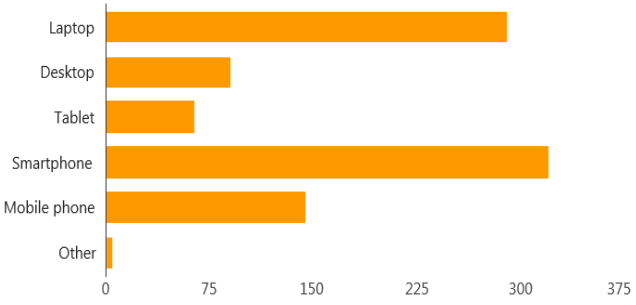

Figure 8. Devices used by respondents to access the internet

The responses collated from Category Three: Social Media Usage Data, showed that 97.5% of respondents are on social media while just 2.5% are not. This shows that quite a number of internet users in Nigerian are engaged in social networks making the social platform a wide and easy access to launch unscrupulous activities. Fig. 9 shows 91.2% use Facebook while 81.1% use Whatsapp with 43.5% of the respondents having very frequent access to these platforms and 41.4% accessing it often. Other platforms like Twitter (47.7%), Google+ (45.2%), Skype (20.4%) and 2go (12.8%) had below 50% access by the respondents. A total of 76.3% receive unwanted messages on their social platforms with 12.8% receiving these messages very often, 33.6% often, 31.1% not often and 22.5% rarely as depicted in Fig. 10.

This shows that quite a number of this users have privacy breaches not therefore ensuring the confidentiality of their data online. 14.4% have fallen victims of fraud via their social media accounts with 45.5% of this incident resulting to financial and money loss, 23.4% resulting to damaged reputation and a total of 6.5% leading to business discontinuities as seen in Fig. 12 below.

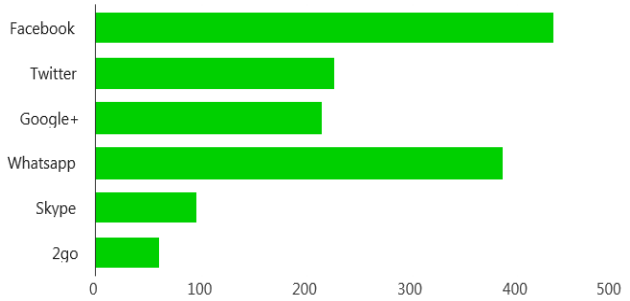

Figure 9. Social media platforms used by respondents

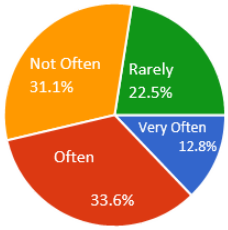

Figure 10. Frequency of unwanted messages received

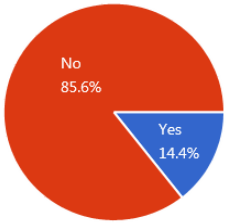

Figure 11. Respondents fallen victim of fraud via social media

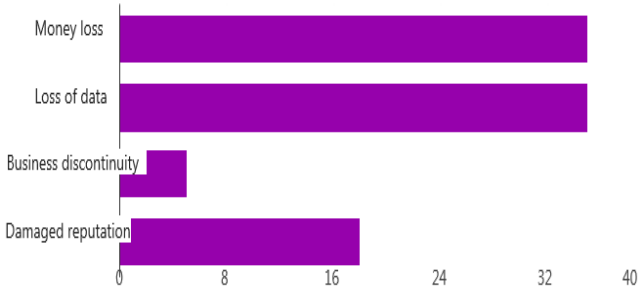

Figure 12. Forms of loss suffered by respondents

Results gotten from Category Four: Email Usage Data, reveal that 94.4% of respondents use electronic mail. Fig 13. Shows that only 53.3% checking their mails very often and 28.5% having often checks of their mails. 64.2% read all their mails while 35.8% do not. 8.2% do not go through spam messages, 10.9% go through them very often, 17.1% go through them often, 30% rarely go through them and 33.8% do not often go through them. This shows that quite a number of Nigerian internet users pay little or no attention to spam messages coupled with the 26.2% of respondents follow referral links provided in spam messages. 67.5% of respondents receive mails requesting their personal information through links and emails unknown to them with Fig. 14 showing 8.9% receiving such mails very often, 24.5% rarely, 27.3% often and 39.3% not often. Information such as personal bio data were requested from 63.2% of respondents, CV from 27.6% of the users and about 4.4% of the users had other information requested as seen in Fig. 15. 74% of the users took such mails to be a scam which shows quite a high sense and awareness of security, 22.8% considered it a beneficiary but uninteresting one and 12.9% took it to be a legitimate one.

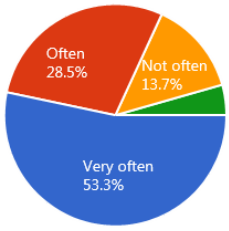

Figure 13. Frequency of how users check their mail

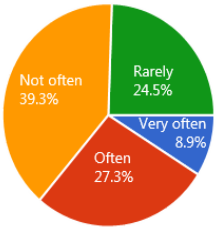

Figure 14. Frequency of users receing mails with requests for personal data

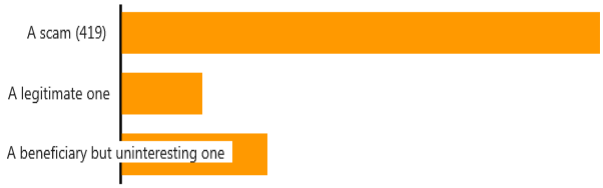

Figure 15. Thoughts of respondents about mails received

From the data collected under Category Five: e-commerce, 78.2% of the respondents indicated that they perform bank transactions online with 28.5% of them as users who utilize the services always, 54.2% perform transactions online once in a while and 17.3% only when they have no other choice. Of the various possible transactions online 79.5% of the respondents pay bills online, 44.2% purchase items individually while 11.1% make bulk purchases online and 64.7% take advantage of internet for money transfer purposes as shown in Fig. 16. This shows that a good number of Nigerians are knowledgeable about e-business portals which means they are also exposed to the various forms of fraudulent attacks by means of imposters posing to be legitimate online store outlets as well as persons who showcase inexistent products online for the sole purpose of duping gullible persons.

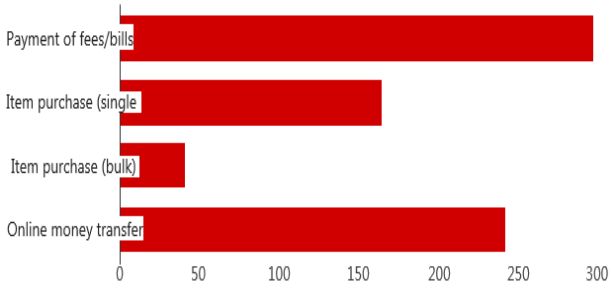

Figure 16. Forms of transactions respondents perform online

From Category Six: Security Awareness, 88.1% of respondents attested to using antivirus software which is an obvious indicator of the fact that Nigerians understand the importance of antivirus software for security over and above safety purposes, though for reasons best known to them

11.9% of the respondents do not use antivirus. However, 70.3 % of all respondents make use of free antivirus software mostly because of the cost-implications, 28.4% use paid versions while 22.1 % use cracked antivirus software. With only 28.4% of respondents making use of paid antivirus as depicted in Fig. 17. It is not far from the truth that only this percentage have full authentic protection from threats and various malware over the internet which leaves a tangible sum of the populace exposed. In mobile device use, 72.6% have devices running on android OS, 4% on iOS, 6.7% use Windows mobile devices, 9.9% use Blackberry devices, 0.4% and 4.9% still use devices running on Symbian and Java platforms while a striking 1.3% use other mobile device operating systems. For the category of desktop operating systems, 41.6% of respondents primarily use Windows 7, 3.9% still use Windows XP, 26.9% use Windows 8/8.1, 24.2% use Windows 10 while 1% and 2.4% use Linux and MacOS respectively. This shows that we have more of our respondents prone to various malware attacks as stated in Section II being that more of the respondents are on the android platform, however for the desktop users with no steady firewall protection would still be liable to suffer various threats online. On matters that concerned user awareness, as seen in Fig. 18, 2.5% of respondents classified their knowledge about applications and devices they use to access the internet as poor, 18% as excellent, 35.4% as satisfactory while 44.1% as good. 37.6% of respondents also indicated their knowledge of the settings and configuration of those devices and applications as good, 33.6% as satisfactory, 15.5% as excellent, with 8% and 5.3 as poor and having no knowledge of settings and configurations respectively shown in Fig. 19. Though a substantial amount of the respondents indicated to be aware of their devices and settings it is still important that a more of the Nigerian populace get acquainted with their devices and relevant settings as it is key to averting attacks such as social engineering. For those who look out for security indicators while surfing the internet 60.9% of respondents do while 39.1% do not look out for such indicators. Of the four security indicators specified in the questionnaire, 64.5% of respondents look out for HTTPS, 54.9% for the padlock icon, 23.9% for TRUSTe and 19.8% for Symantec Norton Secure.

V. CONCLUSION

This paper is posed to discover how vulnerable Nigerians are online. It started by discussing the various types and classes of online risks that users of the Internet are likely to encounter. It also highlighted on the methods of spreading these dangerous wares to unsuspecting users of the Internet. It then went ahead to report thoroughly on the survey carried out to discover how protected or not and how aware are Nigerian Internet users are of online risks. This is done in a bid develop a framework for protecting unsuspecting Nigerian citizens who carry out their daily legitimate businesses online. Doing this will give a boost to the Nigerian telecommunication space and strengthen ecommerce in the country. The paper also gave a brief highlight on the steps towards developing this online protection.

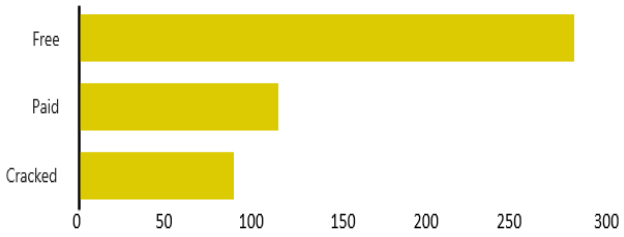

Figure 17. Classification of kinds of antivirus used by respondents

Figure 18. Respondents' knowledge about devices and applications they use

Figure 19. Respondents' knowledge about the settings of devices and applications they use

REFERENCES

[1] InternetLiveStats, "Statistics of Internet Users in Nigeria," 2016. [Online]. Available: http://www.internetlivestats.com/internet-users/nigeria/.

[2] G. Sesan, B. Soremi, and B. Oluwafemi, "Economic Cost of Cybercrime in Nigeria," 2013.

[3] THISDAY, "Nigeria Loses over N127bn Annually through Cybercrime," 2016. [Online]. Available: http://www.thisdaylive.com/index.php/2016/04/19/nigeria-loses-over-n127bn-annually-through-cybercrime/.

[4] TechTarget, "Risk managment in Business."

[5] OECD, "The Protection of Children Online," 2012.

[6] Symantec Corporation, "Internet Security Threat Report 2016," 2016.

[7] S. Kemp and wearesocial SG, "DIGITAL IN 2016," 2016.

[8] J. Gaines, E. Martin, F. Rieger, B. Rupp, M. Aukschlat, V. Jasny, S. Pirk, E. Bericht, M. Shahd, S. Dehmel, B. Datenschutz, P. Ruggiero, J. Foote, C. Reich, D. Wandel, M. Security, A. L. Ahead, R. O. Hornung, Kaspersky Lab, INTERPOL, F. Büllingen, and A. Hillebrand, "MOBILE CYBER THREATS," 2014.

[9] Alcatel-Lucent, "Mobile malware : A network view Black Hat Mobile Security Summit – London 2015," 2015.

[10] D. R. Tobergte and S. Curtis, "Norton Madware Fact Sheet," 2013.

[11] B. Uscilowski, "Mobile Adware and Malware Analysis," 2013.

[12] R. Lipovský, L. Štefanko, and G. Braniša, "The Rise of Android Ransomware," 2015.

[13] K. Savage, P. Coogan, and H. Lau, "The Evolution of Ransomware," 2015.

[14] C. Beek, C. Castillo, C. Cochin, A. Hinchliffe, J. Jarvis, H. Li, Q. Liu, D. Mandal, M. Rosenquist, R. Samani, R. Sherstobitoff, R. Simon, B. Snell, D. Sommer, B. Sun, J. Walter, C. Xu, and S. Zhu, "McAfee Labs 2016 Threats Predictions McAfee Labs offers a," 2016.

[15] J. Wyke and A. Ajjan, "The Current State of Ransomware," 2015.

[16] P. Krysiuk and S. Doherty, "The World of Financial Trojans," 2013.

[17] S. S. E. R. T. SERT, "BlackHole Exploit Kit , Banking Trojans and ACH Transfers," North America, 2012.

[18] C. Wueest, "Financial threats 2015," 2016.