Copyright © 2020 International Journal of Cyber Criminology – ISSN: 0974–2891
July – December 2020. Vol. 14(2): 460–478. DOI: 10.5281/zenodo.4770111
Publisher & Editor-in-Chief – K. Jaishankar / Open Access (Authors / Readers No Pay Journal).

Rising Trend of Phishing Attacks on Corporate Organisations in Cross River State, Nigeria

John Thompson Okpa[1]
University of Calabar, Cross River State, Nigeria

Benjamin Okorie Ajah[2]
University of Nigeria, Nsukka, Nigeria

Joseph Egidi Igbe[3]
University of Calabar, Cross River State, Nigeria

Abstract

This study examines the rising incidence of phishing and its impact on the survival of corporate organisations in Cross River State, Nigeria. A cross-sectional survey research design which allows the triangulation of quantitative and qualitative methods is applied. Questionnaires were distributed to 1074 respondents purposively selected from 18 financial institutions, 4 telecommunication network providers and 2 manufacturing companies, while in-depth interviews were conducted on 13 participants across the selected corporate organisations. The presentation of data is done using frequency distribution tables and chart while the qualitative data were content analysized. The study concludes that phishing is on the increase and corporate organisations in Cross River State are losing fortunes to the activities of phishers. This development the study reveals has forced organisations to lose trade and competitiveness, destroying consumers' confidence in the organisations and their products/services, among others. Based on the findings of this study, it is recommended that corporate organisations should invest more resources and time in sensitizing staff and customers on how to stay safe from cybercriminals and their villainous activities. Also, customers should verify the authenticity of the correspondence between them and the various organisations they transact business with, before responding to such mails, especially when it involves divulging sensitive information about themselves.

Keywords: Corporate organisations, Cybercrime, Phishing, Smishing, Troubled waters.

[1] Lecturer in the Department of Sociology, University of Calabar, Cross River State, Nigeria. Email: okpajohntom@gmail.com
[2] Lecturer II in the Department of Sociology and Anthropology, University of Nigeria, Nsukka, Nigeria. Email: okorie.ajah@unn.edu.ng
[3] Lecturer in the Department of Sociology, University of Calabar, Cross River State, Nigeria. Email: igbejoe@unical.edu.ng

Introduction

The complexity of doing business in today's world has further been compounded by the introduction and subsequent adoption of information technology in the daily operations of corporate organisations globally (Alkadi & Alkadi, 2004; Brown, Howe, Ihbe, Prakash, & Borders, 2008). Historically, corporate organisations have been beset by a myriad of such challenges as insecurity, poor power supply, corruption, unfavourable government policies, inadequate infrastructure, paucity of capital, and scarcity of competent & trustworthy employees (Fette, Sadeh & Tomasic, 2007; Garera, Provos, Chew & Rubin, 2007). These challenges have exacerbated with the advent of modern technology, but the increase in cyber-attacks via phishing on corporate organisations, with its attendant negative consequences, has spread comprehensively in various aspects of the organisations' socio-economic life (Sheng, Magnien, Kumaraguru, Acquisti, Cranor, Hong & Nunge, 2007). There is substantial evidence in extant literature which demonstrates that phishing is an evolving enigma in the current global industry and poses a dynamic threat that adversely affects corporate organisations (Ohaya, 2006; Orgill, 2004; Safecode, 2008; Threat Insight Quarterly, 2005). Phishing has increased the dangers of doing business online by making corporate organisations vulnerable to new dimensions of risk, hitherto unknown to them. The impact of phishing attacks on corporate organisations is of obvious policy relevance, but little is empirically known about it.

Phishing is a prohibited cyber-related act that involves social engineering, facilitated through social media, spam e-mails and SMS, which aim at gaining unauthorized access to an individual's/organisation's secret information, that is then used for personal gain (Ragucci and Robila, 2006). Phishers exploit the natural desires of humans to trust others to send unsolicited electronic mails to unsuspecting victims, as though they originated from legitimate sources (Orgill, Romney, Bailey & Orgill, 2004). Phishers have intensified their operations by going beyond targeting individuals to attacking corporate organisations with larger wallets (Johnson, 2017). The phisher's goal is to "fish" for confidential information private to the phishes. This sensitive data can include bank account numbers, usernames, passwords and social security numbers (Duntemann, 2004; Ibikunle, 2005). Fundamentally, phishers obtain the essential information of their victims by either data mining any of the social networks and databases in the public domain, or retrieving the information from an end user's internet browser (Ragucci and Robila, 2006). Badra, Sawda and Hajjeh (2007) argue that there are other functional techniques applied by phishers during their operations. Common among these methods is the use of spoofed e-mails to lure phishes to counterfeit websites developed to compromise their personal data (Ohaya, 2006). A classic demonstration of the spoofed-e-mail technique could be a threat that the phishes bank account will be blocked within twenty-four hours if they fail to act on the message sent to them by the phisher. A successful phishing attack can have disastrous consequences for the victims leading to financial losses and identity theft (Paganini, 2013). Corporate organisations in Cross River State that have suffered phishing attacks frequently report substantial losses among previously loyal clientele, loss of revenues, massive loss of quality production time, overhead loss, as well as, immeasurable damages to their brand's corporate image and reputation.

Estimating the global financial impact of phishing is difficult. However, Ponemon Institute estimates that in the first quarter of 2016, successful phishing attacks collected up to $3.7 million per attack on a large organisation. The Austrian aircraft manufacturer FACC lost $54 million in January, 2016 to phishing (Johnson, 2017). According to

Akinsehinde (2011) and Olayemi (2014) the alarming rise in incidents of phishing and the resultant financial implications have exposed more than eighty per cent (80%) of e-businesses in Nigeria to phishing activities, which consequently threatens their existence and survival. These scholars argue that web portals and web-based applications of the Central Bank of Nigeria, Nigeria Stock Exchange, banks, shopping malls, pension fund administrators, and switching/electronic payment companies are vulnerable to phishing attacks due to inadequate security measures for safeguarding their platforms. The current economic downturn in Nigeria is pushing more and more young people across the federating units below the poverty line, thereby forcing them, especially the unemployed and underemployed youths, into cyber-related crimes like phishing and other related vices (Ibrahim, 2016). The situation in the country has been exacerbated by historic mismanagement of the nation's resources by successive regimes, which has contributed to the increasing level of cybercrimes such as phishing, hacking, cyber vandalism, and other heinous crimes like armed robbery, kidnapping, terrorist attacks and other forms of armed violence (Ogbeidi, 2012; Ola, Mohammed, & Audi, 2014). Phishing in Nigeria is largely perpetrated by both young and old adults; however, most of the young adults are students of higher institutions of learning across the country, as well as unemployed graduates and school dropouts (Hassan, Lass & Makinde, 2012). They explore the liberty offered by the cyberspace to defraud, steal and engage in mind-boggling atrocities which challenge the survival of corporate organisations in Nigeria.

Paganini (2013) summarizes the effects of phishing on the survival of corporate organisations to include – financial loss, loss of intellectual property and sensitive data. Others include opportunity costs, including service and employment disruptions, damage to the brand image and company reputation, penalties and compensatory payments to customers (for the inconvenience or the consequential loss), or contractual compensation (for delays), cost of counter-measures and insurance, cost of mitigation strategies and recovery from phishing attacks, the loss of trade and competitiveness, distortion of trade and job loss. The upsurge in this fraudulent activity negatively affects the productivity of corporate organisations in the Cross River State. Saini, Rao, and Panda (2012) posit that attacks from viruses take productive time away from staff who make use of these computers. Such attacks slow down the performance of IT equipment in organisations, makes servers inaccessible and causes network jam. Such instances of attacks affect the overall productivity of the users and the socio-economic development of the organisations. The activities of these fraudsters have aided other illicit activities in the State, including the disruption of public services, drug trafficking and kidnapping. The abuses of the cyber space by internet fraudsters portends great danger and has stalled the developmental contributions accruable from a well-harnessed ICT adoption, diffusion and utilisation by corporate organisations in Nigeria. This development has widened the digital divide, crumbled the information infrastructure and negatively affected the consumer's confidence in online transactions (Oumarou, 2007; Salifu, 2008; Longe, Ngwa, Wada, Mbarika & Kvasny, 2009).

Several attempts have been made by corporate organisations to check the threat of phishing in Nigeria over the past few years with minimal result. One of such attempts is the employment of e-mail filters or softwares that prevent some attachments from being opened (Fanawopo, 2004; Gercke, 2013; Frank & Odunayo, 2013). With more than 80% of e-businesses in Nigeria susceptible to phishing attacks, the effects of phishing activities on corporate organisations are indicators of the need for relevant policies to guard the

system, but little is empirically known about it. Similarly, the threats posed by phishing are widely reported in literature (Ragucci & Robila, 2006; Jaishankar, 2007; Kamini, 2011; Ndubueze, Igbo & Okoye, 2013; Folashade & Abimbola, 2013; Das & Nayak, 2013; Dzomira, 2014; Duah & Kwabena, 2015; Leukfeldt 2015; Karim, 2016; Ajah & Chukwuemeka, 2019; Ajah & Okpa, 2019; Nnam, Ajah, Arua, Okechukwu & Okorie, 2019; Okpa, Ilupeju & Eshiotse, 2020; Ugwuoke, Ajah & Onyejegbu, 2020; Nzeakor, Nwokeoma, & Ezeh, 2020). The extent of damage on the economic development of corporate organisations is often misrepresented because of the insufficiency of data. A common denominator in these studies is the acknowledgement of phishing as part of the loopholes of technology, which has fostered a new dimension of crime and risks. Nonetheless, the pace at which corporate organisations subscribe to e-commerce, irrespective of the dangers posed by cybercriminal activities, motivate the study to investigate the economic development impact of phishing on corporate organisations involved in e-commerce in Cross River State. This was premised on the assumption that the financial loss often reported does not adequately account for the cost of phishing and without an insight on how corporate organisations' overall economic development is impacted. Therefore, empirical knowledge of the impact of phishing cannot be absolute. Thus, the study examines the impact of phishing on corporate organisations in Cross River State, Nigeria. Specifically, (i) the study examines corporate organisation experiences of phishing, (ii) determines common types of phishing suffered by corporate organisations, (iii) determines phishers mode of operations, and (iv) finds out the effects of phishing on the survival of corporate organisation. This study is a part of an unpublished PhD thesis conducted on three major (3) institutions vulnerable to phishing attacks.

Conceptual clarifications

Phishing: A phishing e-mail is a fraudulent attempt to get sensitive data or information from people, like their usernames, passwords, financial information or credit card details, by disguising as legitimate well-known companies or an important personality. It is an unwholesome cyber-related act that involves social engineering, where a scammer requests for confidential information from an individual(s) through the social media, spam e-mails and SMS by disguising as legitimate well-known companies or an important personality for personal aggrandisement. Ragucci and Robila (2006) define phishing as sending e-mails claiming to be from a legitimate business and trying to entice the recipients into giving up confidential information. According to Kumaraguru, Rhee, Acquisti, Cranor, Hong and Nunge (2007), phishing is a social engineering technique through which scammers attempt to solicit and steal confidential information from a user or employee by masquerading as a legitimate entity.

Smishing: This refers to a cybersecurity lexicon, where deceptive text messages are used to trick victims to divulge sensitive information which the phisher uses to attack the individual or the organisation. The goal is to trick the victim into believing that a message has arrived from a trusted person or organization, and then convincing the victim to take action that gives the attacker exploitable information such as the bank account login credentials. Smishing is a text-message-centric variation of the e-mail-based phishing scams that direct the text message recipient to visit a website or call a phone number, at which point the person being scammed is enticed to provide sensitive information such as credit card details or passwords (Palan, 2019; Stroud, 2020).

Phish: It is an activity that attempt to steal financial or other confidential information or both from a victim, typically by sending an e-mail that looks as if it is from a legitimate organization, usually a financial institution, but contains a link to a fake website that replicates the real one.

Phisher: This refers to an individual who attempts to trick people into divulging sensitive data about their account details via e-mail so that the criminal can have an unauthorised access that allows him/her steal money from such compromised account. Phishers carry out their fraudulent activities by relying on forged e-mails and web pages to steal individual identity and defraud their victims.

Literature review

Phishing attacks: an overview

Saudi, Ismail, Tamil, and Idris (2007) carried out a study on phishing: challenges and issues in Malaysia. From the result of their study, it can be observed that users are aware of phishing threat. However, their knowledge of the identification and prevention of phishing is very poor. The study also reveals that phishing had cause serious problems to computer users and organisations that depend on the internet for their daily transactions. The study gathers that a number of forgery incidents, especially phishing cases in Malaysia has enormously increased. This social engineering act which tricks someone into giving out their confidential information, is becoming a major threat in securing a peoples' identity. In related study, Leukfeldt (2015) reveals that there are many similarities between phishing and malware attacks. First, he argues that both cyber infractions have almost the same crime script. Secondly, he points out that both criminal groups are happy with almost any victim they can get and do not discriminate between the rich and poor. In addition, Leukfeldt (2015) makes a distinction between high- and low-tech victimisation. First, he reports that almost none of the online visibility variables has any effect on the risk of becoming a victim to low-tech attacks. Victims of high-tech attacks tell a different story. There is a clear connection between victimisation and spending time in the online world. The second difference can be found within online accessibility. Both the phishing and malware analyses are based upon a secondary analysis of a Dutch cybercrime victim survey.

Similarly, Damodaram (2016) observes that the damage caused by phishing does not only apply to monetary property alone as it destroys and shatters the fragile bond of trust that organisations have built with their customers in the process of transacting business. Damodaram (2016) is of the view that as people loss faith in the reliability of electronic communication methods, companies also suffer a cut in their customer base. In the case of disasters, people can spend billions in preparation, to analyse weaknesses and improve recovery time, only to have their trust shattered by phishing attacks. This in turn causes a significant loss in money, resources and time. Based on current trends, the study predicts an increase in the frequency and precision of these attacks and suggests best practices for both user and business education such that the impact is minimized. In the same vein, Leukfeldt (2014) reports that crime script in Amsterdam reveals that criminals not only use fake e-mails and replicates websites that appears to be from the bank, but also make telephone calls to victims to obtain transaction codes. The study concludes thus; that the crime script consists of the formation of a criminal group, the capturing of login details

from the victims, the transfer of funds to money mule accounts and the withdrawal of the money from these accounts to avoid interception by the digital money trail.

Yeboah-Boateng and Amanor (2014) study on Phishing, Smishing and Vishing attacks against mobile devices in Ghana shows that men are more comfortable and trusting on the cyber-space and, thus, more susceptible to phishing attacks than women. The results also indicates that most users are either slightly aware or not aware at all of Phishing, Smishing and Vishing threats against their mobile devices.

Theoretical framework

The study is anchored on the risk society theory by Ulrich Beck (1992). The theory, although not specific to phishing attacks, took as its major focus, the various side effects of modernity as evident in the postmodern era. Consequently, it provides an in-depth insight on how increasing technological advancement could expose corporate organisations and their network of clients to a new dimension of risks/hazards. The theory argues that the risks associated with postmodern society are not limited in time and space as it is global in its consequences, and cyberspace, to a large extent, epitomizes the risk society (Beck, 1992; Jaishankar, 2010). Cyberspace currently features millions of e-business transactions involving buying, selling and exchange of huge financial information in the form of data from one location to another. Plausibly, this change has revolutionized the corporate organisations' approach to business offerings globally, unlimited market opportunity and client network. It has, however, exposed users (individuals and corporate organisations) to a global-based risk. As described by Jackson and Robert (2016), in such a society, every citizen is exposed to some degree of technological dangers of which phishing is inclusive. Deriving from Beck, Giddens and Lash (1994) analogy, this represents the case of technological advancement producing unintended risks with severe consequences for social organisations. It is an attempt to expatiate on impacts of such risks like phishing within the context of corporate organisations on which the study is centred.

Buttressing Beck's claims of the risk society, corporate organisations in Cross River State that are connected to cyberspace are found to be exposed to a series of potential and actual cyber-attack risks. These risks materialise in actual disruption of the organisations' businesses leading to socio-economic setbacks. Almost all the respondents confirm that their organisations have experienced one phishing attack or the other. The global nature of these attacks, as demonstrated in some of the narratives obtained qualitatively, is such that the actual perpetrators or collaborators could be from any part of the world because technology has made it easy for cybercriminal syndicates to operate from different regions of the world. This further supports Beck (2006) argument that science-tech further contributes to the intensity and range of the risks rather than abating it. Furthermore, within the context of risk analogy, the study from a criminological perspective establishes that corporate organisations who transacts on the cyberspace are exposed to risk, which could be checkmated through some awareness and technological education of staff in the organisations. This is where the findings of the study retracted a bit from the theory's pessimism that technology rather than addressing the risks heighten it as more than half of the respondents expressed the different ways through which technological advancements can be used in minimizing the risks. These include measures like regular updates of antivirus, strengthening of firewalls and cryptography security, two-factor authentication, among others.

Methods and materials

Cross sectional survey research design is adopted in this study. The study is conducted in Cross River State, Nigeria. The choice of Cross River State rests on the fact that reliable data on the incidence of cybercrime generally in the State is lacking, but news reports and statements by police and government agencies give credence to the increase of the problem in the State. Cross River State has three senatorial districts namely: Southern, Central, and Northern Senatorial Districts, with eighteen Local Government Areas and one hundred and ninety-three (193) wards (Ipole & Okpa, 2019).

Table 1. Spread of sample size

S/N	Organisations	Sample Proportion of Staff	Proportion of Staff	Sample Size (n)
Sample of financial institutions (Banks)				
1	Access Bank	37	0.03	20
2	Diamond Bank	54	0.05	30
3	Eco Bank	95	0.09	53
4	First City Monument Bank	80	0.08	44
5	Fidelity Bank	41	0.04	23
6	First Bank	308	0.29	171
7	Guarantee Trust Bank	37	0.04	20
8	Heritage Bank	17	0.02	9
9	Keystone Bank	22	0.02	12
10	Skye Bank	19	0.02	11
11	Stanbic Bank	32	0.03	18
12	Standard Chartered Bank	15	0.01	8
13	Sterling Bank	16	0.01	9
14	United Bank of Africa	54	0.05	30
15	Union Bank of Nigeria Plc	44	0.04	24
16	Unity Bank	14	0.01	8
17	Wema Bank	23	0.02	13
18	Zenith Bank	148	0.14	82
	Total	1056		585
Sample of manufacturing companies				
1	Flour mills	384	0.48	213
2	UniCem	409	0.52	226
	Total	793		439
Sample of telecommunication network providers				
1	9mobile	17	0.19	9
2	Airtel	15	0.16	8
3	Glo	19	0.21	11
4	MTN	40	0.44	22
	Total	91		50

Source: Field survey, 2019

The study population is limited to employees working in selected corporate organisations in Cross River State, Nigeria. These corporate organisations include

eighteen (18) financial institutions, four (4) telecommunication network providers and two (2) manufacturing companies, based in the three senatorial districts of Cross River State. The eighteen (18) financial institutions, four (4) telecommunication network providers and two (2) manufacturing companies were delineated into strata. Respondents were purposively selected from each of the strata. A sample size of one thousand and seventy-four (1074) respondents is drawn using Survey Monkey Sample Size calculator. The details are highlighted in Table 1.

Qualitative data was elicited using the in-depth interview guide. The in-depth interview is rich and insightful and is used to support the findings of the quantitative data. The in-depth interview is conducted among thirteen (13) purposively selected participants from selected corporate organisations. The inclusion criteria are that respondents must have a computer set connected to the internet attached to their desks and that they must be ICT staff and staff of information security unit of the banks, as well as, engineers of these selected organisations. IDI was thematically and contently analysed. The use of both quantitative and qualitative methods ensures complementarities of data and triangulation, which is emphasised in modern research. The study observes all known ethical principles guiding social research such as informed consent, specific permission required for audio or video recording, voluntary participation and no coercion, participant's right to withdraw and cultural sensitivity. The instruments were put through a pre-test. The pre-test is conducted using 5% of the sample size from respondents working in different corporate organisations from the ones studied. The essence is to ensure that the data and findings of the study reverberate their set target. These instruments were validated by three senior lecturers in the Department of Sociology and Anthropology, University of Nigeria, Nsukka. The reliability of the questionnaire is determined using Cronbach alpha, and a reliability coefficient of 0.86 is obtained. The analyses of quantitative data is done with descriptive statistics. The data were presented using tables and pie charts.

Results

In all, 1074 questionnaires were distributed, while 1002 were adequately completed, retrieved and used for the analysis. Majority of respondents (64.7%) of the respondents were males, while 35.3% were females. Again, the modal age of the respondents ranges as follows: 31-40 years 47%, followed by 43.2% who are below 30 years, next is ages 41-50 9.1%, while 0.7% of the respondents are 51 years and above. In terms of respondents' level of education, 0.5% of the respondents have only their First School Leaving Certificate (FSLC), followed by 9.1% of the respondents who have their General Certificate of Education (GCE) or Secondary School Certificate of Education (SSCE). Also, 14.9% have their National Certificate of Education (NCE) or Ordinary National Diploma (OND), while, 62.9% have their First Degrees in the forms of Higher National Diploma (HND) or Bachelor's Degree. In terms of the nature of respondents' organisation, 41.8% of the respondents work in manufacturing companies such as Flourmills and Lafarge cement company. Also, 4.5% of the respondents work in Telecommunication organisations such as 9mobile, Airtel, Glo and MTN. The remaining respondents (53.7%) work in financial institutions, which are 18 commercial banks that operate in Cross River State. In terms of respondents' job designations, 5.8% of the respondents indicate that their job designation is that of risk management, while 9.3% work indicate that they work with the Information and Communication Technology (ICT) units of their organisations. Furthermore, 31.5% indicate that they work as account officers in their organisations, while 55.4% work as

operational staff. It was observed that 42.1% of the respondents identified the primary function of their organisations as that of production, while 53.3% of the respondents indicate that their organisations render financial services. Also, 4.3% of the respondents indicate that their organisations' primary function is that of telecommunication services, while 0.3% of the respondents indicate others.

To enable deeper insight on the structure of the respondents considering their distinct organisations, key aspects of their socio-demographic characteristics is cross-tabulated with the nature of the organisations they work with, as well as the primary function of their organisations. Respondents' age and level of education were re-coded into two categories. Respondents who were below 31 years were re-coded as "younger respondents", while those that were 31 years and above were re-coded as "older respondents". The classification is informed by the structure of the respondents' age presented in socio-demographic section. Additionally, the respondents' level of education is re-coded into two groups; respondents who have their B.Sc./HND or Masters/PhD were re-coded as "higher education", while those with First School Leaving Certificate, GCE/SSCE and NCE/OND are classified as "lower education". The outcome of the cross tabulation is presented in Table 2, 3 and 4.

Table 2. Cross tabulation of respondents' gender and nature of organisation

Nature of Organization	Gender		Total
	Male	*Female*	
Financial Institution	338 (52.2%)	200 (56.5%)	538 (53.7%)
Telecommunication	33 (5.1%)	12 (3.4%)	45 (4.5%)
Manufacturing	277 (42.7%)	142 (40.1%)	419 (41.8%)
Total	**648 (100.0%)**	**354 (100.0%)**	**1002 (100.0%)**

Source: Field Survey, 2019

Table 2 shows that 52.2% of the male respondents work in financial institutions, which is 4.3% lesser than the proportion of female respondents that work in the same type of organisation. This is not the case with telecommunication organisation, as 5.1% of male respondents indicate that they work with telecommunication organisations, while only 3.4% of the female respondents work in similar organisation. With regards to respondents in the manufacturing institutions, the finding shows that 42.7% of the male respondents work in manufacturing company, while 40.1% of the female respondents work in similar organisations. This implies that there were relatively more males in the telecommunication and manufacturing organisations than female.

Table 3. Cross Tabulation of respondents' education and nature of organisation

Nature of Organization	Level of Education		Total
	Lower Education	*Higher Education*	
Financial institution	49 (20%)	489 (64.6%)	538 (53.7%)
Telecommunication	7 (2.9%)	38 (5.0%)	45 (4.5%)
Manufacturing	189 (77.1%)	230 (30.4%)	419 (41.8%)
Total	**245 (100.0%)**	**757 (100.0%)**	**1002 (100.0%)**

Source: Field Survey, 2019

Data presented in Table 3 shows that greater percentage of respondents with higher education (64.6%) works in financial institutions, while only 20% of respondents with lower education works with financial institutions. The reverse is the case with manufacturing companies, which shows that 77.1% of respondents with lower education work in manufacturing companies, while only 30.4% of respondents with higher education works in similar organisation. This further reiterates the fact that manufacturing organisations in Nigeria are largely labour intensive, and as a result relies more on personnel with lower education.

Table 4. Cross Tabulation of respondents' age and their organisations primary function

Organizations' Primary Function	Respondents' Age Groups		Total
	Younger	*Older*	
Production	240 (55.4%)	182 (32.0%)	422 (42.1%)
Financial Services	183 (42.3%)	351 (61.7%)	534 (53.3%)
Telecommunication Services	8 (1.8%)	35 (6.2%)	43 (4.3%)
Others	2 (0.5%)	1 (0.2%)	3 (0.3%)
Total	**433 (100.0%)**	**569 (100.0%)**	**1002 (100.0%)**

Source: Field Survey, 2019

Table 4 demonstrates the age disparity of respondents in the different organisations. It shows that majority of the younger respondents (55.4%) are in organisations whose primary function is that of production, while majority of older respondents (61.7%) are in organisations with financial services as their primary function. Also, a disparity was observed between younger respondents in organisations with telecommunication services as their primary function (1.8%), compared to older respondents in similar organisation (6.2%).

Phishing experience

Respondents were asked: "whether their organisations have fallen victim of phishing attacks in the past"? Majority (85.5%) of the respondents work in organisations that have experienced phishing in the past, while 14.5% indicate that their organisations have not experienced phishing in the past. This implies that majority of the respondents are of the view that their organisations have experienced cyber-attacks in the past. This goes further to suggest the high rate of phishing attacks on corporate organisations in Cross River State. However, it is possible that some of the respondents who claimed their organisations have not experienced phishing attacks in the past may have simply been unaware that the attacks occurred or exist. This is because in some of the organisations, especially the financial institutions, a specialized unit exists that manages cyber-attack related issues; consequently, an average staff in another department might not know that the various changes in the banks software or cyber platforms are practical response to anticipated or real phishing attacks. This is deduced from one of the participants in the qualitative interview. Responding to whether their organisation has been phished, the participant responds thus:

> Definitely, though a specialised unit in the bank known as Information Security Department manages the information about phishing attacks on the bank, If there is a phishing attack, staff are usually not informed of the incident, but are directed and compelled to take certain actions to mitigate future occurrence. Such actions include a change of password in the middle of the month or deploying a new software, which require staff to log in afresh. ***(IDI: Male Banker, 48, First Bank Plc).***

Another participant from a distinct financial institution who claimed that the activities of cyber criminals are routinely experienced by corporate organisations, especially the financial institutions, further corroborated his position. According to the participant, "banks on daily basis experience breaches on their security networks by cyber criminals" (**IDI: Male Banker, 39, GT Bank**).

Other corporate organisations in the State are not exempted from the wave of phishing attacks. Although, their own experience varies, some of them perceive themselves as the most prone targets of phishing attacks as they stand a chance of losing their organisations' biggest assets in the form of the intellectual property on which the organisation operates. One of the participants from a manufacturing organisation affirming that their organisation had experienced phishing attack in recent time expressed his views thus:

> Yes, we have been attacked and you see, manufacturing organisations like Lafarge are often at the biggest risk with phishing attacks because of the vast and easily transferable intellectual property they possess. This is contrary to the assumption that cyber threats are aimed only at financial institution or organisations, where data could be monetized ***(IDI: Male ICT Staff, 39, Cement Manufacturing Company).***

Another participant from a telecom organisation also confirmed that telecom corporations are exposed to a large number of cyber-attacks as they are the gateway to other organisations' access to the internet. According to the participant:

> Telecom companies like the one I work with experience a whole lot of phishing attacks. The reason why telecom industries suffer heavy phishing attacks is because they manage and operate data bank that is largely used to communicate and store large amounts of sensitive information, and they also serve as the connecting point for some organisations' network. The wide range of services offered and huge data in their custody make them attractive to cybercriminals ***(IDI: Female Staff, 36, Airtel Telecom).***

An integration of the quantitative and qualitative responses indicate the reality of phishing activities against corporate organisations in Cross River State. Again, while the attacks are dominantly perceived as revolving within financial organisations because they transact mostly on liquidity, other organisations are also having their share of the attacks. These organisations do not lose cash, but when vital information about the organisation is stolen through attacks like phishing, the cybercriminals could sell it to their rivals for a fortune or use it to bring down the organisation.

Common types of phishing suffered by corporate organisations

Table 5. Distribution of respondents on the common types of phishing suffered by corporate organisations

Common types of phishing	Frequency	Percentage (%)
Spear phishing	271	27.0
Smishing	412	41.1
Vishing	103	10.3
Search engine phishing	176	17.6
Whaling	25	2.5
Email phishing	15	1.5
Total	1002	100

Source: Field Survey, 2019

Aside identifying corporate organisations' phishing experiences, the study also inquires on the common types of phishing attacks suffered by these organisations. Data presented in table 5 shows that 41.1% of the respondents indicate smishing as the most common type of phishing attack suffered by their organisations, 27.0% indicate spear phishing, while 176 % indicate search engine phishing. Again, 10.3% of the respondents were of the view that vishing is the most common type of phishing attacks suffered by their organisations, 2.5 % indicate whaling, while 1.5% indicate e-mail phishing. This implies that majority of the respondents (41.1%) indicate smishing as the most common type of phishing attacks suffered by their organisations.

The qualitative data indicate that smishing is the most common type of phishing experienced by corporate organisations. However, it might not be regarded as the attack with the most direct devastating eco-development impact on the organisations, but it is the most reported and most talked about because it affects the customers a great deal. One of the participants who identified smishing as the most common type of cyber-attacks that their organisation has suffered the most in the past said:

> I think it is smishing. The target of cybercriminals is usually the bank customers. They impersonate the bank and send bulk SMS to bank customers' phone numbers requesting them to provide sensitive information, such as card number, passwords, ATM Pin etc. These fraudsters know very well that it is difficult to attack bank platforms, and that the easiest way of having access to the bank platforms is through the customer's account *(IDI: Male Banker, 48, First Bank Plc).*

Phishers mode of operations

Respondents were asked: "the commonly used techniques during phishing attacks in their organisation"? The research shows that 17.9% of the respondents identify the use of calls as the most frequent strategy adopted by phishers in defrauding their victims. Again, 19.8% of the respondents point out sending of false e-mails to people, 41.8% indicated sending of SMS, while 20.6% of the respondents are of the view that phishers adopt all the identified approaches (false e-mail, call and fraudulent SMS) in defrauding their victims. This finding implies that phishers in defrauding their victims apply strategies like sending of false e-mails, calling the victims with outrageous proposals and sending fraudulent SMS

to the victims. However, the most common as indicated by more than one-third of the respondents (41.8%) is that of fraudulent SMS.

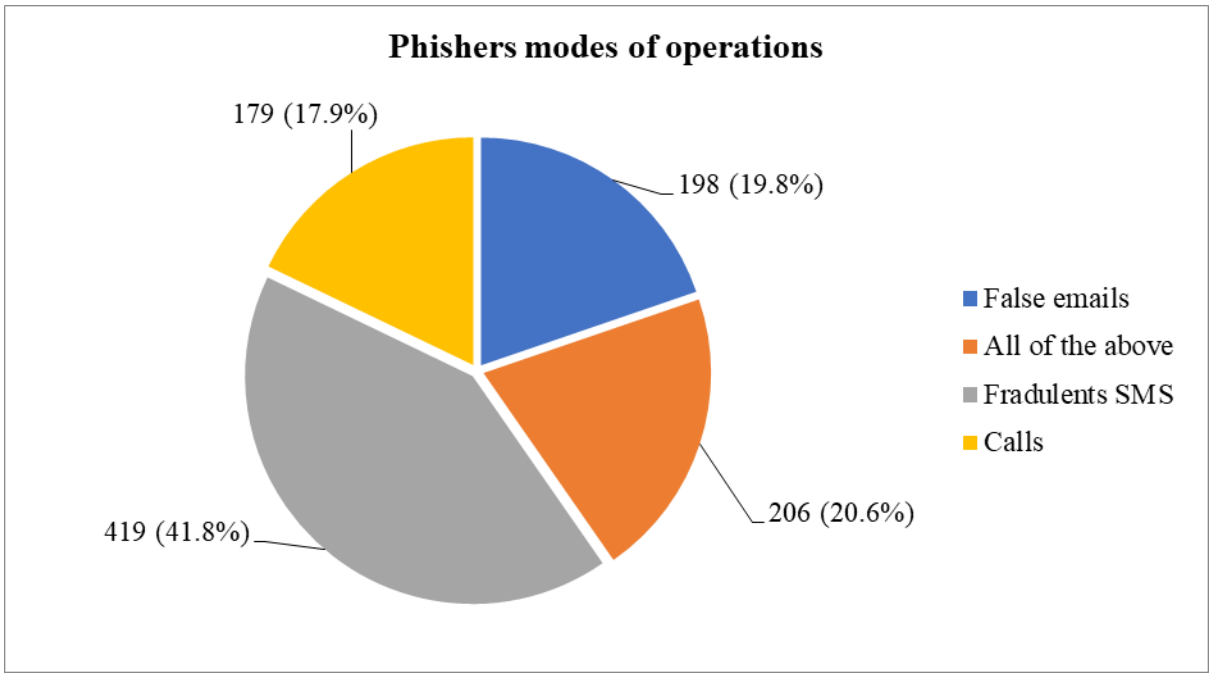

Table 6. Distribution of respondents by the financial and organisational implications of Phishing

Effects of phishing	Agree	Disagree	Total
It damages organisations brand image and reputation	963 (96.1%)	39 (3.9%)	1002 (100.0%)
It makes organisation to loss trade and competitiveness	951 (94.9%)	51 (5.1%)	1002 (100.0%)
It affects consumers' confidence in online transactions thus discouraging them from patronizing your organisations via the internet	938 (93.6%)	64 (6.4%)	1002 (100.0%)
It affect organisation from taking care of their staff welfare	867 (86.5%)	135 (13.5%)	1002 (100.0%)
It leads to penalties and compensatory payments to customers (for inconvenience or consequential loss) which affects the economy of your organisations	890 (88.8)	112 (11.2%)	1002 (100.0%)

Source: Field Survey, 2019

To understand the specific effects of phishing, respondents were asked to "agree", "strongly agree", "disagree" or "strongly disagree" with five likely financial and organisational impacts of phishing identified in extant literatures. Furthermore, in presenting the responses, "strongly agree" and "agree" options were merged and recoded as "agree", while "strongly disagree" and "disagree" responses were merged and presented as "disagree". The outcome presented in Table 6 shows that 96.1% of the respondents

agree that phishing damages their organisations' brand image and reputation, whereas 3.9% disagree.

In the second row, 94.9% of the respondents agree that phishing makes their organisation to suffer losses in trade volume and competitiveness, while 5.1% disagree. In the third row, it is identified by 93.6% of the respondents that phishing affects consumers' confidence in online transactions, thus discouraging them from patronizing their organisations via internet. On the contrary, 6.4% of the respondents disagree, noting that such is not applicable in their own organisations. On the fourth row, 86.5% of the respondents indicate that phishing affects their organisations' ability of taking care of their staff welfare, while 13.5% disagree with this notion. In addition, the last row shows that 88.7% of the respondents agree that phishing could lead to penalties and compensatory payments to customers, which in turn affects the organisations' economy. This was disagreed to by 11.2% of the respondents, who claim that phishing in their organization does not call for penalties and compensatory payments to customers. The implication of all the findings presented in Table 8 is that phishing impacts on more than half of the organisations by expanding their financial expenditures, impairing their brand competitiveness and reputation, among other things.

Discussion

Among the various types of phishing observed in the study, smishing stands out at 41.1% making it the most common type of phishing perpetrated against corporate organisations in Cross River State. It is also found to be a variant of phishing that is commonly reported by customers of these corporations. Quarshie and Martin-Odom (2012), although did not use the concept 'smishing', noted that deceitful e-mails, which is an aspect of phishing constitute one of the most prevailing aspects of cybercrimes in Africa's Internet landscape. For Longe, et al (2009), phishing in the form of sending deceitful, deceptive and spurious financial proposals all over the world is trending in most developing countries of the world of which Nigeria is an instance. Although this relates with the position of the study findings, it is however observed in this study that sending of fraudulent SMS is the most common mode of operation deployed by phishers in the area, followed by sending e-mails to millions of unknown users. Similarly, Leukfeldt (2014) observes that the nature of phishing in Amsterdam, apart from involving fake e-mails and replication of websites, the perpetrators often go as far as calling the victims using telephone to obtain transaction codes. Consequently, and in line with the research objective, the financial implication of phishing on corporate organisations is analyzed to show that phishing has five key effects on the organisations' management and finances.

On the organisation generally, phishing affects brand reputation and image of the organisations as indicated by the majority of the respondents (96.1%). Again, 94.9% of the respondents showed that organisations when exposed to phishing attacks experience loss of trade and competitiveness. Other financial impacts include a decrease in consumers' confidence in online transactions, thereby reducing patronage (93.6%) and also the huge finances carted away from the organisations as penalties and other compensatory payments made to customers by the organisations. This in some ways corroborates the position of extant studies which highlight various economic and other implications of phishing. Damodaram (2016), for example, notes that phishing poses a huge threat to the e-commerce industry by shifting the confidence of customers away from e-commerce activities thus causing a huge financial loss to electronic service providers. Additionally,

Ragucci and Rabila (2006) report that phishing impact goes beyond the monetary loss experienced by the affected organisations, as it also encompasses destruction of the bond of trust built by organisations over the years. Put differently, they observe that phishing damages the organisations' reputation and public confidence in the organisations.

Jansen and Leukfeldt (2016) in their study observe the incidence of phishing among bank customers in the Netherlands, of which one-third of the respondents who have been victims of the fraud were aware of it before their victimization. They, however, conclude that awareness and training on how to apply protective measures are critical factors in safeguarding online users from financial scams induced via phishing mechanism. In another study, Saudi, et al (2007) identities respondents who are likely to fall victim of phishing to include home users, persons with non-IT literacy backgrounds and people who are involved either directly or indirectly in the IT and computing industry.

Conclusion and recommendations

Phishing attacks have been a major cause of concern to all Internet users, especially those who rely on it for their businesses. Like other variants of cybercrime, phishing manipulates innocent people into taking various actions which lead to being defrauded of their finances. Governments, through relevant agencies in collaboration with corporate organisations, have made attempts to safeguard businesses and their clients from phishing attacks and other cyber-related crimes. However, reports of cyber victimization persist, with millions often lost to phishing. The analysis reveals that all the corporate organisations studied have been exposed to phishing, while more than three-quarters have in the past recorded different forms of phishing attacks like smishing, and vishing. The intensity of the attacks and the corresponding economic development impact, however varies as factors like employees' gender and a number of cyber platforms, among others, predict a high negative effect of phishing on the economic development of corporate organisations. The study recommends that corporate organisations should train their employees to recognize phishing schemes and encourage them to raise alarm when suspicious transactions are noticed. Similarly, organisations should ensure that they stay up-to-date with the latest scam trends so that they will be able to identify any different form of attack as it emerges. Customers should verify the authenticity of the messages they receive from the various organisations before responding to such messages, especially when it involves divulging sensitive information about the individual.

Strengths and limitations of the study

The major strength of this study lies in the triangulation of the quantitative and qualitative methods of data collection. This approach facilitates the authentication of research findings from two distinct sources, thus providing a more valid and reliable research findings.

However, the major limitation of this study is that the study focuses only on one state in Nigeria, consequently data gleaned only relies on information gathered from staff of selected corporate organisations in the state and supported by secondary sources such as internet-based materials, text books and journal articles. All the approaches used in data collection belong to the obtrusive measures which has its inherent flaws. Again, since respondents are selected from three corporate organisations in one state, caution should be applied in generalizing the findings of this study to other corporate organisations in other states in Nigeria and beyond.

Suggestions for further research

A dynamic issue such as "Phishing" cannot be exhausted in a single study like this. This study has been limited to a scope that could be handled within a timeframe, resources and ability of the researchers. However, considering the havoc phishers wreck on businesses and corporate entities on a daily bases, it becomes pertinent to suggest that further enquiry on "Phishing" should be replicated in different corporate organisations across Nigeria and indeed, the African continent for the purpose of ascertaining the consistency and refinement of results that should be adopted in enhancing cyber security in the African continent. Again, there is need to explore the effects of phishing on other institutions like education, health and judiciary, among others. In addition, there is also need for study with several identified variables that could explain the predisposing factors that push or pull individuals into phishing.

References

Ajah, B. O. & Chukwuemeka, O. D. (2019). Neo-economy and militating effects of Africa's profile on cybercrime. *International Journal of Cyber Criminology, 13*(2), 326-342

Ajah, B. O. & Okpa, J. T. (2019). Digitization as a solution to the problem of awaiting-trial inmates in Ebonyi State, Nigeria. *International Journal of Criminal Justice Sciences 14*(2), 199-20.

Akinsehinde, E. (2011, October 11). 80% of Nigerian businesses risk cyber-attacks. *The Punch Newspaper* Tue, pp. 19

Alkadi, I. & Alkadi, G., (2006). Grid computing: The past, now and future. *Human systems management*, *25*(3), 161-166

Badra, M., E-L Sawda, S., & Hajjeh, I, (2007). Phishing attacks and solutions, ACM International conference proceedings of the 3rd International conference on mobile multimedia communications, vol. 329, ICST (Institute for Computer sciences, social-informatics and telecommunications engineering, Nafpaktos, Greece

Beck, U. (2006). Living in the world risk. *Society Economy and Society, 35*(3), 329-345

Beck, U. Giddens, A. & Lash, S. (1994). *Reflexive modernization: Politics, tradition and aesthetics in the modern social order*. Cambridge: Polity Press

Brown, G., Howe, T., Ihbe, M., Prakash, A. & Borders, K., (2008). Social networks and context-aware spam, Proceedings of the ACM 2008 conference on computer supported cooperative work, ACM, San Diego, CA, USA, pp. 403-412

Damodaram, R. (2016). Study on phishing attacks and anti-phishing tools. *International Research Journal of Engineering and Technology (IRJET),* 03(01), 700- 705

Das, S. & Nayak, T. (2013). Impact of cybercrime: Issues and challenges. *International Journal of Engineering Sciences & Emerging Technologies*, *6*(2), 142-153.

Duah, F. A. & Kwabena, A. M. (2015). The impact of cybercrime on the development of electronic business in Ghana. *European Journal of Business and Social Sciences*, *4*(01), 22 – 34

Duntemann, J. (2004). Debunking Your Email, Spam, And Viruses.

Dzomira, S. (2014). Electronic fraud (cyber fraud) risk in the banking industry, Zimbabwe. Risk Governance & Control: *Financial Markets & Institutions*, *4*(2), 3-26

Fanawopo, S. (2004). FG moves to enforce cybercrime laws.

Fette, I., Sadeh, N. & Tomasic, A. (2007). Learning to detect phishing emails', Proceedings of the 16th International conference on World Wide Web, ACM, Banff, Alberta, Canada, pp 649-656

Folashade B. O. & Abimbola, K. A. (2013). The nature, causes and consequences of cybercrime in tertiary institutions in Zaria-Kaduna State, Nigeria. American *International Journal of Contemporary Research*, 3(9), 98-114

Frank, I. & Odunayo, E. (2013). Approach to cyber security issues in Nigeria: challenges and solution. *International Journal of Cognitive Research in science, engineering and education*, 1(1), 1-11

Garera, S., Provos, N., Chew, M., & Rubin, A. D. (2007). A framework for detection and measurement of phishing attacks', Proceedings of the ACM workshop on recurring malcode, ACM, Alexandria, Virginia, USA, pp. 1-8

Gercke, M. (2013). Training on cybercrime and discussion of the draft bill, special training on cybercrime. 2nd Workshop on Transposition of SADC Cyber security. Model Laws in National Laws for Namibia Windhoek, Namibia. Available from: http://www.itu.int/en/ITU-D/Projects/ITU-ECACP/HIPSSA/Documents/Special%20Training%20on%20Cybercrime%20%281%29.pdf.

Hassan, A. B., Lass, F. D., & Makinde, J. (2012). Cybercrime in Nigeria: Causes, effects and the way out. *ARPN Journal of Science and Technology*, *2*(7), 626-631

Ibikunle, A. (2005). Investigation of computer crime in information technology industry. (Unpublished Master's Thesis). Ladoke Akintola University of Technology, Ogbomoso, Oyo State.

Ibrahim, S. (2016). Causes of socio-economic cybercrime in Nigeria. In: Cybercrime and computer forensic (ICCCF), IEEE International Conference on (pp. 1-9). Vancouver: IEEE.

Ipole, P. A. & Okpa, J. T. (2019). Working Conditions and employees' productivity in Cross River State civil service, Nigeria. *European Scientific Journal (ESJ), 15*(8), 132-14.

Jackson T. C. B. J. & Robert W. E. (2016). Cybercrime and the challenges of socio-economic development in Nigeria. *JORIND, 14*(2), 42-49.

Jaishankar, K. (2007). Cyber criminology: Evolving a novel discipline with a new journal. *International Journal of Cyber Criminology*, *1*(1), 1–6

Jaishankar, K. (2010). The future of cyber criminology: Challenges and opportunities. *International Journal of Cyber Criminology* (IJCC),*1*(2), 26–31

Jansen, J. & Leukfeldt, R. (2016). Phishing and malware attacks on online banking customers in the Netherlands: A Qualitative Analysis of factors leading to victimization. *International Journal of Cyber Criminology, 10*(1), 79–91

Johnson, L. (2017). The risks of phishing to organizations. https://blog.eccouncil.org/the-risks-of-phishing-to-organizations/

Kamini, D. (2011). Cybercrime in the society: Problems and preventions. *Journal of Alternative Perspectives in the Social Sciences*, *3*(1), 240-259.

Karim, S. S. (2016). Cyber-crime scenario in banking sector of Bangladesh: An overview. *The Cost and Management*, *44*(2), 12-19

Kumaraguru, P., Rhee, Y., Acquisti, A., Cranor, L. F., Hong, J. & Nunge, E. (2007). Protecting people from phishing: The design and evaluation of an embedded training

email system, Proceedings of the SIGCHI conference on human factors in computing systems, ACM, San Jose, California, USA, pp. 905-914

Leukfeldt, E. R. (2014) Cybercrime and social ties: Phishing in Amsterdam. In: *Trends in Organized Crime*, *17*(4), 231-249.

Leukfeldt, E. R. (2015). *Comparing victims of phishing and malware attacks: Unravelling risk factors and possibilities for situational crime prevention*. Netherlands Institute for the Study of Crime and Law Enforcement (NSCR)

Longe, B. O., Ngwa, O., Wada, F., Mbarika, V. & Kvasny, L. (2009). Criminal use of information and communication technologies in sub-Saharan Africa: Trends, concerns and perspectives. *Journal of Information Technology Impact*, *9*(3), 155-165

Longe, B. O., Ngwa, O., Wada, F., Mbarika, V. & Kvasny, L. (2009). Criminal use of information and communication technologies in sub-Saharan Africa: Trends, concerns and perspectives. *Journal of Information Technology Impact*, *9*(3), 155-165.

Ndubueze, P. N., Igbo, E. U. M. & Okoye, U. O. (2013). Cybercrime victimization among internet active Nigerians: An analysis of socio-demographic correlates. *International Journal of Criminal Justice Sciences, 8*(2), 225-234.

Nnam, M. U., Ajah, B. O., Arua, C. C., Okechukwu, G. P., Okorie, C. O. (2019). The War must be Sustained: An Integrated Theoretical Perspective of the Cyberspace-Boko Haram Terrorism Nexus in Nigeria. *International Journal of Cyber Criminology, 13*(2), 379-395

Nzeakor, O. F., Nwokeoma, B. N., Ezeh, P. J. (2020). Pattern of Cybercrime Awareness in Imo State, Nigeria: An Empirical Assessment. *International Journal of Cyber Criminology, 14*(1), 283-299

Ogbeidi, M. M. (2012). Political Leadership and Corruption in Nigeria Since 1960: A Socio-economic Analysis. *Journal of Nigeria Studies*, *1*(2), 1-25

Ohaya, C. (2006). Managing phishing threats in an organization, Information Security Curriculum Development Conference, Proceedings of the 3rd annual conference on Information security curriculum development, ACM, Kennesaw, Georgia, pp 159-161

Okpa, J. T., Ilupeju, A. A., & Eshiotse, E. (2020). Cybercrime and socio-economic development of corporate organisations in Cross River State, Nigeria. *Asian J. Sci. Res*, *13*, 205-213

Ola, A. S., Mohammed, A. & Audi, M. S. (2014). Effects of corruption on economic development in Nigeria. *Global Journal Interdisciplinary Social Sciences, 3*(3), 209-215

Olayemi, O. J. (2014). A socio-technological analysis of cybercrime and cyber security in Nigeria. *International Journal of Sociology and Anthropology, 6*(3), 116-125

Orgill, G.L., Romney, G.W., Bailey, M.G. & Orgill, P.M. (2004). The urgency for effective user privacy-education to counter social engineering attacks on secure computer systems, Information Technology Education (Formerly CITC), ACM, New York, USA, Salt Lake City, UT, USA, pp. 177-181

Oumarou, M. (2007) Brainstorming advanced fee fraud: 'Faymania'–the Cameroonian experience. In: N. Ribadu, I. Lamorde and D. Tukura (Eds), Current trends in advance fee fraud in West Africa. EFCC, Nigeria, 33–34.

Paganini, P. (2013). Info Sec Institute 2013 Cost of cybercrimes. Retrieved from: http://resources.infosecinstitute.com/cybercrime-and-theunderground-market.

Palan, C. (2019). Smishing Explained: What It Is and How to Prevent It. Retrieved from: https://www.webroot.com/blog/2019/09/16/smishing-explained-what-it-is-and-how-you-can-prevent-it.

Quarshie, H. O. & Martin-Odoom, A. (2012). Fighting cybercrime in Africa. *Computer Science and Engineering, 2*(6), 98-100

Ragucci, J. W. & Robila, S. A. (2006). Societal aspects of phishing. Conference paper.

Robila, S. A. & Ragucci, J. W. (2006). Don't be a phish: Steps in user education', Annual Joint Conference Integrating Technology into Computer Science Education, Proceedings of the 11th annual SIGCSE conference on Innovation and technology in computer science education, ACM, Bologna, Italy, pp. 237-241

Saini, H., Rao, Y. S. & Panda, T. C. (2012). Cybercrimes and their impacts: A Review. International Journal of Engineering Research and Applications (IJERA), 2(2), 202-209.

Salifu, A. (2008). Impact of internet crime on development. *Journal of Financial Crime*, *15*(4), 432–444.

Saudi, M. M., Ismail, S., Tamil, E. M. & Idris, M.Y. I. (2007). Phishing: challenges and issues in Malaysia. *The International Journal of Learning*, *14*(8), 79-88

Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L.F., Hong, J. & Nunge, E. (2007). 'Anti-phishing Phil: The design and evaluation of a game that teaches people not to fall for phish', Proceedings of the 3rd symposium on usable privacy and security, vol.229, ACM, Pittsburgh, Pennsylvania, pp. 88-99

Stroud, F. (2020). Smishing. Retrieved from: https://www.webopedia.com/TERM/S/smishing_scams.html

Threat Insight Quarterly (2005). 'Phishing and other significant threats of 2004', Internet Security Systems, Retrieved from: http://documents.iss.net/ThreatIQ/ISS_XFIQ0205.pdf

Ugwuoke, C. O., Ajah, B. O., & Onyejegbu, C. D. (2020). Developing patterns of violent crimes in Nigerian democratic transitions. *Aggression and Violent Behavior, 53*, 1-8.