https://doi.org/10.31871/WJIR.10.1.9
World Journal of Innovative Research (WJIR)
ISSN: 2454-8236, Volume-10, Issue-1, January 2021 Pages 34-44

The Current Phishing Techniques – Perspective of the Nigerian Environment

Palang Nicolyn Mangut, Kalamba Aristarkus Datukun

***Abstract*— Phishing has continued to be a tool in the hands of the cybercriminals. APWG (Anti-Phishing Working Group) trend report of 2020 first quarter revealed a rise in phishing websites particularly in the month of March, taking advantage of the COVID-19 pandemic to affect the most vulnerable of the times. Likewise second quarter reports attackers deploying more sophisticated measures to deceive users and having 78% of phishing sites using SSL (Secure Socket Layer) protection. This shows continuity in perpetration and sophistication of phishing attacks. This paper explored recent phishing trends, reviewed some work carried out by the research community, identifying methods to detect and mitigate the scourge. A particular focus was analysing the Nigerian environment putting into considerations some of the factors that affect the society to determine common phishing approaches used by actors and most targeted community. Data from World Bank, ITU (International Telecommunication Union) and Nigerian regulatory institutions were used. The study identified Vishing and Smishing categories as most popular attack vectors in contrast to developed economies experiencing high incidences reported in email and other similar mediums. This knowledge will create better understanding to factors that can make phishing attack types more unique to certain regions and thus tailor researchers' direction for finding solutions in the areas most needed.**

***Index Terms*—Phishing, Phishing in Nigeria, Smishing, Social Engineering, Vishing**

I. INTRODUCTION

In recent times internet security has come to be the most crucial thing for most organisation as businesses and services have continued to span using many forms of electronic communication. Little wonder, the perpetration of evil has also drifted towards that direction. Cybercriminals have constantly worked to improve their game and thereby causing tremendous havoc to ordinary Internet user, institutions such as Banks and its customers. Phishing is a cybercrime whereby a user is targeted with fraudulent messages from an illegitimate source that mimics the looks and feel of a legitimate source, in order to get valuable and confidential information of the user. This process can be in a form of an email spoofing, counterfeit webpage, using a malware and many more recent methods [1]. The earliest Phishing activity was linked to the American Online (AOL) group in the early 1990s. The group was attacked with multiple fake AOL accounts that was sending messages and emails to its users asking them to verify their account or billing information [2]. The Anti-phishing Working Group (APWG), saddled with the task of analysing all reported phishing activities from its member institutions defined Phishing as "a crime employing both social engineering (SE) and technical subterfuge to steal consumers' personal identity data and financial account credentials"[3]. Overtime this attack has gotten more sophisticated not with so much technology to execute but breadth of SE to lure targets into compromise. Social engineering is dependent on human interaction and works at tricking the human psychology to get them to do some certain unacceptable actions such as disclosing their pin or passwords. The human behaviour and user orientation has largely contributed to the successes of SE tricks. SE also takes advantage of the human lack of knowledge in security matters [4]. It is seen by other researchers as a science that uses social interaction as a way to persuade individuals or an organisation to act on a request using a computer related entity [5]. Reviewing other past work on human behaviour, [6] related the inability of participants to pay attention to security indicators of websites even after gaining little awareness. Such and much older works of [7] have shown phishing success due to human behaviours which has inevitably put man as the weakest link to the security chain. It is likewise noted that the Nigerian spammers with an old known tale of a prince who needs ten million out of his country have also grown executing more sophisticated phishing attacks using social engineering says Sjouwerman CEO of KnowBe4 [8]. These Nigerian attackers without use of any malware can pharm data from sites like LinkedIn and know who the CEO is and carryout a more targeted attack.

This paper reviewed related literature and identified various recommendations made towards solving phishing problem. It seems phishing attack is ubiquitous across the globe but one noticeable argument is its prevalence of some certain attack methods in specific regions of the world. What this paper has been able to show are factors that determine phishing attack trend in Nigeria and calls for conscientious effort made by research community to work in finding solutions that deter attacks affecting populated low income persons around the globe.

The rest of the paper is arranged in into five sections. Section two presents related findings of existing phishing methods, approaches detection and mitigations. Section three identifies possible phishing targets while section four enumerates determining influences to phishing methods deployed by attackers in the Nigerian society. Section five gives specific example to attack scenarios emanating from

Palang Nicolyn Mangut, Computer Science Department, Plateau State University, Bokkos, Nigeria.
Kalamba Aristarkus Datukun, Computer Science Department, Plateau State University, Bokkos, Nigeria.

Nigeria and section six concludes the paper.

II. Review of Phishing Trend

Because phishing has been around for a while and studies does show that it is not going to be extinguished any time soon, this raises questions researchers and the public deserve to be familiar with so as to strategically position themselves to ways to overcome these attacks. What are the recent trends used in phishing? Ross in [9] identified recent approaches adopted by criminals to perpetuate phishing attacks around the world and proffered ways to identify and investigate these attacks. The writer showed examples of six methods; here we present same trend and included two more methods (smishing and Vishing). We examined works relating to these categories in addition to highlighting proposed solutions for detecting and mitigating these attacks.

A. The Money Scam

Attackers in this category try to scam users of money, sometimes offering a small fee to entice the user to trust the scammer and so they can later send money to scammer. Or scammer gets confidential information of the target using malware when the user falls victim of initiating a dialogue or clicks on a link or attachment or submits information in a provided link [12]. Money scam is a common attack, over the years it has continued to evolved with many tactics and have also transformed to other types of attack like BEC (Business Email Compromise). One of the earliest identified in the list of money scam is the Nigerian prince tale, who claims to have a large sum of money to get out of Nigeria [10], [11]. A word of caution on Money scam is for users to take note of poor grammar in phishing emails says Ross [9], this is also widely reported by many researchers [1], [12]. Secondly, users are not to fall gullible for offers that look too good to be true, which aren't most time [12].

B. Information scam

The attacker's intent is to collect confidential data from the user and later use it for other malicious purposes. The scammer provides a link in the message to lure the target to surrender their credentials. Recently, samples of such attacks shows the email portrayed to be from a security outfit of a reputable organisation such as the bank. The email can claim a compromise on user account status and will require the user to make changes so that problem with the account can be resolved. This is becoming more difficult for users as the make believe for integral service of securing one's account is also put at risk. Users are advised not to click on links found in emails or enter their credentials on such links whether they believe the source is legitimate or not, rather type out known web address of the organisation from user web browser. Users are to take note of such strong action words that pose to threaten or create fear and points to clues of a phishing mail [9], [13], [14]. [15] Studies highlighted some word characteristics used in a Phishing emails.

C. Malware distribution

Here the scammers basically want the recipient to open the mail attachment, all with the aim of perpetuating further attacks. This malware could be in form of ransomware, virus, worms, bots, password stealers and more. Malwares are used to compromise organisations network where scammers execute insidious attack on the network [16]. This malicious malware can be software that is targeted to take advantage of security vulnerability [17] and also used as a pre-emptive attack for BEC when used in whaling phishing attack [18]. [19] Relates how the GandCrab ransomware is spread by use of a word document attachment in simple and innocent looking mails. These word documents attachments when opened download and run an executable with capability of encrypting system files.

Ross does suggest caution be taken when dealing with attachment in mail or messages. Opening a single attachment can affect the computer in use and network as a whole. Industry email filters can warn off a malicious attachment if the extension is suspicious but other measures taken can be users' enlightenment to check email header and making phone calls for further verification if source is suspicious [16]. It is common that emails with malicious attachment can pass through end point threat systems, a recent work by [20], tested five webmail service providers used widely by the public (note, names were not revealed but services were connoted with letters S1, S2, S3, S4 and S5) . Their test was conducted in two stages using hundred well known phishing mails, passing twenty each to identified accounts of the providers. The messages were ensured to have characteristics of being a phishing mail, having phrases such as verify account, including links, poor grammar and likes of it. Twenty messages without links where sent in the first stage to users account and stage two had links left in the massages and sent to users account. It turned out that two out of the five providers (S3 and S5) did not filter a single message of the two stages. S1 and S4 did fairly better with 6 and 8 messages consecutively sent to spam folder of each of the twenty messages with links, while only 1 message each of theirs was spammed in the first phase test. Of all the five service providers only S2, had a good acceptable result. S2 was able to spam 19 emails of those with links and 1 message missing, while it spammed all 20 messages of the no links phase. This test portrayed the realistic state of what the ordinary user would encounter on a daily bases using some of the known public web services available in the open domain, as such security of phishing attacks has escalated beyond technology to place man as the first human firewall.

D. Multiple file extensions

Though similar to malware distribution, here the scammers use attachment with different file types, deceiving the user from knowing the actual file extension of the attachment [21] shares report on how attackers use the control panel extension (cpl.) needed for icons to be on Windows Control Panel to successfully bypass threat controls and install other second stage payload on endpoint device. Though this attack was commonly targeted at the South American bank users other similar campaigns used to hide file extensions in another is Steganography – a method that hides file or image inside an unsuspecting file type [1]. This complicates operations in strong defence business environment as it becomes difficult for threats to be spotted

when employees pass around innocent looking pictures or emails that could infiltrate the network and leave a backdoor says Rutherford.

E. Disguised links

Moving away from email attachment to scammers using links, here the intent also is to capture user credentials and use links to spread malwares. These links in messages often times do not look suspicious but are used for redirecting target to a different URL setup by the criminals [9]. Attackers have been successful using obscure links to infiltrate networks and system devices. Past works by [7] studied more of website security and its authenticity rather than the phishing mails that lure users to these sites. Identifying strategies used by actors in making users fall for a successful phishing attack, numerous forms of these websites methods were analysed by [7], [17], these examples include; Redirected links, Cloaked links, Obfuscated links, Misleading named links, Programmatically obscured links, Map links and Homograph URLs. Users are easily deceived when they are unable to differentiate domain names based on syntax to know legitimate and fraudulent URL (example, www.google.com and www.google-play-account.com) and identifying forged email headers from legitimate ones. So also, understanding security indicators such as the use of Secure Socket Layer (SSL) and Transport Layer Security (TLS), padlock icon within the web browser and knowing how to verify these SSL certificates in the browsers. Attackers use phishing cue in many ways which include visual deception that uses text, known as "typjacking" or "homoglyph". Others are mimicking domain name syntax by substituting some letters to slip the human scrutiny (example, replacing letter "l" with number 1 in domain name www.paypa1.com). More include using image hyperlink to mask a fraudulent site, image mimicking windows, windows masking, placing rogue window on top of a legitimate window and website deceptive looks and feel that could constitutes tone of language, misspellings and typeface. Phishers tend to use typefaces that mimic original typeface of a website among other features [6], [7]. Dhamja et al. acknowledged that, protective indicators do not hinder users from being phished from above mentioned deception methods used by attackers particularly when users lack attention in noticing security indicator and lack attention to the absence of these security indicators. Their findings did show that the protective indicators do not still hinder users from being phished [7].

In combating the menace of phishing links the task becomes that of discovering ways for users to identify fraudulent links or putting technologies in place to stop these links since it is impractical to ask users to stop clicking on all links in emails [22]. How does a user treat or determine the eligibility of a link within or outside the email message? Email authentication technologies and related research works have been proposed by researchers and some are now in use to authenticate email sources to stop forging return addresses, and help track phishing domain via domain registration [17]. Gupta, Arachchilage and Psannis [23], build a taxonomy of phishing attacks for both spoofed email and fake websites. They authors also build taxonomy of solutions in spoofed email filtering and fake websites category. Some of these solution classifications include; User education, Protection from phishing emails, Link features-LinkGuard algorithm, Structural features-Support Vector Machine (SVM), Word list features (based on machine-learning algorithm)-k-Nearest Neighbour (k-NN), Naïve bays classifiers and Protection from Phishing Websites that include, Black and Whitelist, Heuristic solutions, Visual similarity methods and others.

Phishing detection methods rely on specific features of the webpage to gather information about the status of the page, as seen in the work carried out by [23]. Reference [24] also identified features and classified them based on URL, Domain Name System (DNS) and content features. They also further categorised detection tools into 1) Education, 2) URL Blacklist/Whitelist, 3) Heuristic Rule and 4) Machine Learning. The researchers proposed the SHLR (Search & Heuristic & Logistic Regression) method which uses Baidu search engine, a rule-based detection method and logistic regression classifier which showed to reduce false positive. Their work [24] basically leveraged on these methods in three folds (apart from education), the use of search tool utilizes the search engine technology (such as Google Safe Browsing blacklist) using the title tag as search key. This step certified legitimacy of the WebPages and not their phishing status yet. Further screening of search results with heuristic rules is applied to detect complex anomalies of phishing URL obfuscation techniques where the black-list/whitelist method is limited in identifying zero hour attack. Rules applied included; use of hidden phishing target words, many identification name, un-standardized naming system, IP address used as domain name, URL having protocol in a wrong field, Top Level Domain (TLD) in non-domain and more. The search engine also does provide a limited data set for the rule to analyse and results obtained from this analysis gives machine learning method a much better sample size to further analyse. This is able to give the process a real-time detection capability and high accuracy of detection, a limitation known with machine-learning techniques when detecting phishing WebPages. The logistic regression classifier analysed webpage features of DNS, Whois, place of phishing vocabulary, lexical features and HTML.

More work in this area targeted analysing structure of hyperlinks in an ego network (adopting graph theory approach to retrieve features and linking data of a webpage and its interconnected webpages that form the ego network) to detect phishing websites [25]. The researchers argued the poor reliability and inconsistency of other phishing detection methods that focus on use of surface content of the webpages and of third party data such as WHOis, hence they proposed the new detection technique using graph theoretic approach. Working with a dataset of 1000 samples used to build their classifier for phish detection, the technique utilises deeper level features (not easily obtained from queried webpage) to extract patterns on phishing websites. They used 17 graph features extracted for machine learning test and found performance of 97.8% accuracy on C4.5, a better performance recorded for graph

features compared to conventional features utilised for similar set. Testing against SVM (Support Vector Macnine), Naïve Bayes, C4.5 and Random Forest classifiers, there results showed outstanding accuracy values of performance with C4.5 and Random Forest algorithms.

In another study similar to [23], Khonji Iraqi and Jones [26] carried out an in-depth survey of phishing literature, identifying attack categories and analysing some anti-phishing software approaches. This study considered detection accuracy in respect to zero-day achievement and rate of low false positive as criteria for measurement. They researchers also classified software detection solutions into Blacklists, Rule-based heuristic, visual similarity and Machine-based classifiers. Their findings revealed a higher accuracy of phish detection amongst Machine-Learning based methods compared to the rule-based heuristic methods. Due to the draw backs of each of the other methods, such as inability of Blacklists technique in addressing zero-hour attacks, heuristic technique though able to achieve zero hour detection test has a tendency of producing high FP(false positives), likewise the visual similarity test techniques do give high FP as well as high computational cost. Based on these findings, the researchers suggested an approach that takes advantage of the helpful attributes of these techniques to produce an effective result in large classifiers, for example taking in an output of some classifiers to be used as input of another classifier. This suggestion could be seen applied in the work of [24] discussed above.

A more recent work by [27], investigated the properties that machine learning technique use for the detection of malicious URL. This includes features used for classification, and the writers grouped the features into Blacklist, Lexical, Host-based, Content-based and others such as Context and Popularity features. These features are studied and quality features are selected for prediction model (quality of feature representation does affect quality of URL prediction model testing). The researchers also analysed learning algorithms used and categorised them into Batch learning algorithms, Online learning algorithms, Representation learning and others. These categories make up some of the most used algorithms in detection systems. A basic process in machine learning performs the task of extracting features from URL (URL crawling of relevant information e.g. lexical information such as length of URL, words used on the URL and more). Other extractions are host-based information such as WHOIS information, IP address, location and more. After extract, features are formatted and stored into a numerical vector and passed through machine learning algorithm (for learning the prediction). Often the numerical data can be used as fetched or stored as Bag-of-words (a dictionary made of words that appear in a URL and used as a feature) approach. Sahoo, Liu and Hoi's work reviewed limitations of blacklist technique thereby presenting machine learning techniques for Malicious URL Detection. Their work reviewed machine learning techniques already in use and they proposed systematic formulation of Malicious URL for machine learning approach as well as addressing feature representation and designing new algorithms. Concluding, the researchers identified some design principles required for developing a Malicious URL Detection as a service, which considers accuracy, speed of detection, scalability, adaptation and flexibility. Notable challenges identified by [27] despite success recorded in the area of machine learning of Malicious URL detection include, effective data sampling with efficient algorithms, ways to get labelled data or new ways in using unsupervised learning, challenges in feature collection used for creating training datasets, issue of feature representation and high dimensionality, adapting to concept drifts, interpretability of models particularly of deep learning model, preparing for advance adversarial attacks and more. These and many more are examples of techniques investigated by researchers establishing ways to counter attackers' revolutionised phishing methods.

F. Spear-phishing

This attack targets an individual, group of individuals or specific organisation in order to obtain confidential or financial data of users, heavily deploying impersonation tactics to influence target on authenticity of the message they receive [4], [9], [16], [23]. "Whaling" attack a form of Spear phishing attack on the other hand targets top executives of an organisation [23]. Spear phishing attack does require attackers carrying out reconnaissance on the target to have an effective attack, they go to all extend of registering a deceptive domain with similar identity of a real one to deceive victims [9]. In comparing mass phishing against spear phishing, Aleroud and Zhou [4] showed that the overall cost implication of a spear phishing attack is more substantial than that of mass attack. [28] Were able to determine the feasibility of targeted attack success by exploiting some known ID caller applications like True-Caller ID to get first-hand knowledge about targets name, location, email, phone number etc. and other sources include information fetched from social networking sites. Many researchers have shown the success of spear phishing attacks where a victim is tricked by an identity of someone that is familiar to them or an organisation with known business relationship, examples of emails send with user name instead of a generic salutation like "Dear customer" has high chances of phish success. The survey [18] also indicates how Spear Phishing is attackers most preferred method of launching Advanced Persistent Threat (APTT) and other Cloud computing attacks that require login credentials. And more recently, Spear Phishing is an identified ground setting activity for BEC attacks that scammers use when email accounts are compromised to steal identity [3]. An early susceptibility test conducted by [29] showed female gender more susceptible to phishing attacks. Other studies [30] showed spear-phishing emails used in a training simulation tool (PhishGuru) targeted at participants and able to make users less victims of phish attacks if they are trained at least twice. The researchers also found the age range 18-25 more susceptible to fall for a

phishing attack. A study by [31] examined the susceptibility of most rational personality class of persons (conscientious) by sending targeted messages with conscientiousness and known phishing cues to participants. Despite high level of personality traits, the results showed 62% of participants clicked on phishing link, invariably implying emotional tendencies can rule rationality in decision making points, and hence a need for custom defences with specific designs needed. Because spear phishing attacks are not easy to detect, neither is user level of technicality an exception, user training has been proposed by most researchers [24], [26], [32].

G. BEC

Most BEC/EAC (Business Email Compromise and Email Account Compromise) attacks will demand a wire transfer from the victim [9]. BEC attack a next level of spear-phishing attack is carried out by the target lured to respond to an email and thereby set a ground for conversation. The scammer goes after individuals (in organisations) who handle huge finances and sends them emails using an account that has been compromised or spoofed [3]. BEC attacks have shown to be successful without the target clicking on a URL but merely acting to fool the target to execute a wire transfer or give out confidential information [9]. Reference [3] report for first quarter 2020 had 66% BEC cash-out method on Gift Cards, 18% for Direct Debits and 16% for Payroll Diversion. Gift cards has had much success, due to the nature of the amount of money involved, small amount requested could go unnoticed thus having a greater use. Likewise BEC wire transfer has also recorded one of the highest cybercrime losses with a first quarter attempt made for the sum of $976,522 [3] and a total of BEC losses amounting to more than $1.7 billion in 2019 [33]. Instances of attacks reported to [33] included cases of victims receiving instruction from a compromised management staff ID requesting a (lower level) staff to make gift card purchase for some work related reason and thereafter the scammer makes use of it. Or in the case of a wire transfer, an email coming from the CFO, can instruct a staff to carry out a transaction with the guise that he (the CFO) is held up on some reasons and is unable to make the transaction at that point[Ever-changing face]. Where does the scammer know who to impersonate? LinkedIn tells the attacker who is who in the organization with their various job schedules [8].

Email of a BEC attack is not any different from an everyday email; it is simple and has properties of a real account thereby making it difficult for email defence systems to detect such attacks. Individuals (organisations) are encouraged to have a policy that allow measures such as phone call verification before carrying out wire transfers (not with contacts supplied in emails), more than one person authorisation of wire-transfer [9]. Since old school security training does not work, organizations are advised to train using simulated phishing attacks and testing users performance and susceptibility says industry experts, thereby producing a 'human firewall' on-top its defence. Tools suggested for authenticating sources of emails include DMARC (Domain-based Message Authentication, Reporting & Conformance) but expert warn of a no fit all solution currently in the market [8], [34].

H. Smishing

This phishing method got its name from the acronym created for text messaging service SMS which means Short Message Service. The attacks is perpetuated with criminals sending text messages to mobile phone lines with a likely instance of claiming to be someone the target personally knows or does business with, such as the Bank or offers for some services and freebees. In another case the criminals will send messages about the targets identity being compromised and asked the target to supply vital information to that effect to solve the problem. This message will indicate a website or link directing the target to go along to give in the information they required [35]. Reference [36] reported how messages in a smishing text also contained notable signs of phishing bait or threat sent to the target, examples of such phrases include, call a number, click a link and other request to pass confidential information or install malicious software unknown to the target. [37] Advices victims to report to cell phone carriers when they receive phishing text, which the carrier can identify if the text message was sent from an email or a cell phone. In a study conducted by [38], investigating SMS fraud in Pakistan revealed the rural area most vulnerable to SMS fraud attacks. The researchers used an application to categorise messages received from participants and further use a simple classifier to labelled messages as spam, ok and fraud, based on some identified fraud vocabulary. The study showed that applying some level of filtering from Telco companies can reduce the amount of fraudulent messages that citizens receive [38]. Smishing attack is gaining more populace even though a survey in [39] showed more awareness of vishing attacks compared to smishing. But just like phishing email attacks, detection mechanisms for smishing can yield more results when message context is used in contrasts to vishing attack.

I. Vishing

The vishing word is a blend of the words "Voice" and "phishing". The same as phishing except the attack uses voice technology. The attack aims at getting the target to provide confidential information over the phone [40], most demanded data are credit card details, birthdays, social security numbers, passport numbers, account numbers and account PINs, to mention but a few [41]. Vishing attack can be conducted in any of the following scenarios, using a voice message, automated voice simulation technology (and speech synthesis) or direct call as seen nowadays [40]. Examples of such ploy could have the criminal spoofing a Caller ID of a legitimate institution like the bank and the caller asking the potential victim to call a certain number to clear a suspicious activity that might have taken place in their account. Early vishing attacks were common on the VoIP networks, it is used because the operation on VoIP can be connected and disconnected in a short given time, it

can either connect or disconnect on a computer wherever in the world and a decrease in cost of making a call was another advantage [41]. Other attractive reason for vishing include attackers ability to, obfuscate real source of calls by use of proxies to send traffic anywhere, knowing how to spoof a Caller ID credential of company and more [41]. Vishing attack is not restricted to VoIP technology alone; recently other voice technologies such as the cellular network have also been deployed to phish users. Ways used by phishers to execute this attack include, Internet email, mobile text messaging, Voicemail and live telephone call [41]. Each of the mentioned can be a vector in itself for a full launch of phishing attack but can also be a pre attack vector for vishing to be successfully accomplished. The following are common examples of vishing attack categories reported by victims, Bank account or credit card compromise, Telemarketing (unsolicited investment deals), social security scam, Tax scam (IRS for US), Tech support, freebees offers and many more [40], [42].

Attackers gather Caller IDs available on the internet and sound like staff of a legitimate company, thereby luring the customers to reveal confidential data. Innocent people have parted with large sums due to these attacks, a case of a woman is told in [36] who parted with £100,000 when fraudsters made her transfer her entire money into their account claiming they were her Bank's fraud team informing her of a compromise on her account and demanding she makes the transfer to a new account opened in her name to sort the problem. The security group [43] have blogged samples of vishing latest schemes reported by victims who had spoofed direct calls, automated and a hybrid of both. Just like the case of phishing emails, these vishing attacks are crafted with degree of urgency pressed on the victim. The writer indicates 800-numbers of big technological companies are being polluted on popular search engines with spoofed versions of customer support of these companies [43]. There are a number of identified reasons why vishing can be the most exploitable phishing attack, two of which is it does permit high level of personalisation that allows social engineering to occur and ability of a wider population to be reached through phone call rather than email system [41].

Much work has been done in respect to attacks on VoIP technology. While early works of [44], demonstrated a requirement of callee feedback to determine the call as spam. [45] On the contrary build detection on some characteristics of call such as day, time of call and duration of call to streamline call behaviour and were able to detect bulk spam calls. Though there are not much literature in specific attacks of smishing and vishing, some efforts have been made by researchers. A model proposed by [39], detects vishing attack by analysing technical vulnerability of mobile systems, psychological states of emotions and attack script as well as sensitivity of data requested by attacker. But this model works relying heavily on targets awareness to ploys and scripts played by phishers, as well as soundness with technology of device. Detection systems as that presented by [46], monitors activities that attacker make victims do during a telephone vishing conversation. Attackers lure and mandate victims to carry out transaction and other operations in an unusual manner sensed to detect as being under duress. The systems detects if movement exhibited by the victim are in any form of an earlier known pattern of vishing attack (referred to as the 'playbook'). The system senses the victim being under pressure with unusual data entry pace, typographical error pace, changes to victim's unique posture, changes to device orientation and many other irregularities that would be detected. [28] Showed how vishing attack among other related attacks can be conducted via voice, SMS and OTT ((over-the-top) applications like WhatsApp) against 722, 696 users taking advantage of applications like Truecaller and other social networking applications to retrieve targets data and connected network data. Because of poor verification process with Truecaller, the researchers showed how fake true caller registration and Caller ID spoofing can elevate the chances of an attacker appearing legit when vishing targets.

III. PHISHING TARGET

Data theft, financial gain, political war has been some of the identified reasons to why phishing attacks are being conducted by criminals. It is of interest to note that financial gain weighs as a global force particularly among individuals or acting criminal groups. Cybercrime actors even when found acting for other reasons like identity hiding, also sell their cyber loots in the dark web market [26].

In terms of impact, the banking and financial institutions have over the past years fallen as the most targeted sector in general cybercrime, and recently still trending among the most hit institutions. Phishing attacks in particular, have also reflected these same readings. The graph in figure 1 shows financial institution as the second most-targeted in first

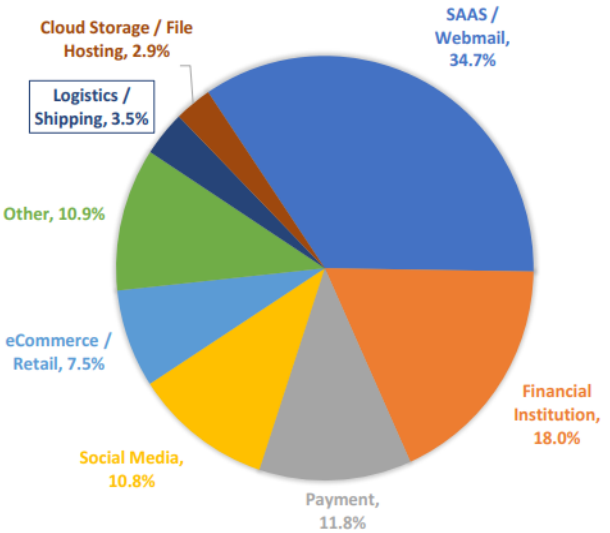

Figure 1: Most-Targeted Phishing Sectors, 2Q2020 –Source [47]

quarter and second quarter of 2020 report [3], [4], [7], while SAAS (Software As A Service) and Webmail top the targets. It is known that webmail services are a lucrative platform used by attackers to direct their phishing attacks so as to exploit other services in the categories listed [20].

Reference [33] Consistently reports losses incurred for various types of cyber-attack. The year 2019 alone, the organisation recorded 3.5 billion dollars of victim losses of over 340,000 complaints received per year average for the last five years. And in an all crime type victim table, Phishing, Vishing, Smishing and Pharming topped the table with a total number of victim loss of $57,836,379 [33]. In a study by [39], the researchers were able to establish the consequences of vishing attacks to financial loss and loss of data. The state of Brazil has experienced the highest attack on Banks and financial Institutions from last quarter of 2019 to first quarter of 2020. Likewise, financial sector companies have been the prey to hosted phishing domains in this year's first quarter [3]. This will mean that most cybercriminal activities like phishing are mostly driven for financial motive. We can then infer that financial sector and financial gain stands as the most targeted and most stipulated motive. Therefore, any representation of individuals or cooperate institutions with any form of financial activity are attractive to criminals, and any form of online financial activity is attractive for cybercrime.

Premise: All financial account holders or active Internet participants are targets to phishing attack.

IV. Phishing Attacks in Nigeria

The world may consider Nigeria as a centre of some of the described cybercrimes in recent times. Unfortunately, this premise is not far reached as shown by [47]. These criminals have damaged the country's reputation and as rightly stated by [48], such actions from a little few has had great consequences on individuals, businesses, institutions and country as a whole. Nigeria has an estimated population of over 200 million people [49] as at 2019, see figure 2 and table1.

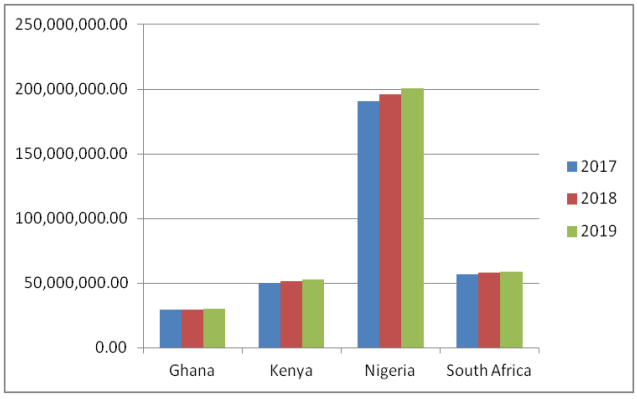

Figure 2: Country Population, Source: World Development Indicators

Table 1: Country Population

	2017	2018	2019
Ghana	29,121,471.0	29,767,108.0	30,417,856.0
Kenya	50,221,473.0	51,393,010.0	52,573,973.0
Nigeria	190,873,311.0	195,874,740.0	200,963,599.0
South Africa	57,000,451.0	57,779,622.0	58,558,270.0

Created from: World Development Indicators
Series: Population, total

Nigeria is the most populated African country and 7th largest in the world [50]. The chart shows Nigeria with a population three times bigger than the next populated country to her. In identifying phishing attack trend within Nigeria, it is important to recognize methods deployed by criminals to perpetuate attacks; therefore a number of factors are discussed below.

A. Nigeria's Population with Internet inclusion

Number Africa is the least region with use of the Internet. The 2020 Report of UN E-Government Development Index (EGDI) (EGDI uses metrics such as provision of online services, telecoms connection and human capability on countries to measure e-government development activities), survey report showed Africa with an estimate of 27% of individuals using Internet in the region [EGDI 2020]. The region experienced an increase of 5% from previous record of 2017 survey [51].

Nigeria's local statistics of Internet users as at 2020 is 99.05 million, with a penetration of 46.6% of its large population as reported by [52]. But other sources like World Development Indicator data reported this as seen in figure 3 and table 1. Altogether, the number of active subscribers by various technologies listed for the period (October 2019 to September 2020) is a total of 151,512,122 million [53]. Generally, Nigeria tops as an African country ranked with high use of mobile internet traffic. Refernce [54] Provided an estimate of mobile internet users of almost 85 million in Nigeria, indicating 14.05 million of Internet users with traffic from non-mobile medium. These statistics render a below average Internet participation in contrast to its population, implying less of the population engaging in Internet activities such as having email accounts to become victims of phishing attacks conducted via web email services.

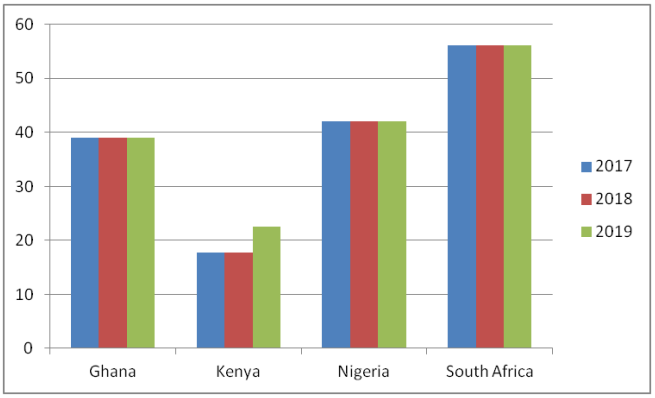

Figure 3: Individuals using the Internet (% of population), Source: World Development Indicators

Table 2: Individuals using the Internet (% of population)

	Ghana	Kenya	Nigeria	South Africa
2017	39.0	17.8	42.0	56.2
2018	39.0	17.8	42.0	56.2
2019	39.0	22.6	42.0	56.2

Created from: World Development Indicators
Series: Individuals using the Internet (% of population)

Premise 2: Less Nigerians have email accounts and less Nigerians use the Internet.

B. Telecommunication Advantage

Though, the last two decades have seen a rise in the provision of telecommunication, other countries have moved in a much faster pace than some. Nigeria, a country with a large population has experienced slower growth in telecommunication sector compared to some of its African counterpart; see figure 4 and table 3. Refernce [48] Compared Nigeria's yearly Mobile Cellular subscription against four countries, namely, Ghana, Kenya and South-Africa using World Bank dataset for the years 2005 to 2015. Their report showed these countries with less population than Nigeria growing consistently higher than Nigeria particularly Ghana and South Africa [48]. Recent data from the same source has not revealed any changes to Nigeria's pace matched with indicated countries as seen in figure 4 and table 3. A two year record of Cellular Subscription per 100 people has Nigeria with the list number of subscription for the years 2017, 2018, 2019 (75.9, 88.2, 88.2 consecutively). A telecommunication infrastructure report of [55] indicates Nigeria's mobile cellular telephone subscriptions per 100 inhabitants to be 88.18 for the year 2020, stationary level of three years..

Growth in telecommunication sector invariably affects development in other sectors of life such as education, health, businesses and more, [55] have continued to monitor growth with technological indictors. As at 2019, more developing nations are seen to embrace mobile cellular solutions as numbers of subscribers' increases globally, particularly when income levels are considered in pricing structure, with possible influence of recent ITU expert group review of price baskets made in 2018 (low and high consumption based on countries usage patterns) [56]. The low-income economies have shown a trend of preferences to mobile-cellular subscription, though a large margin exists in developed and developing countries Internet consumption.

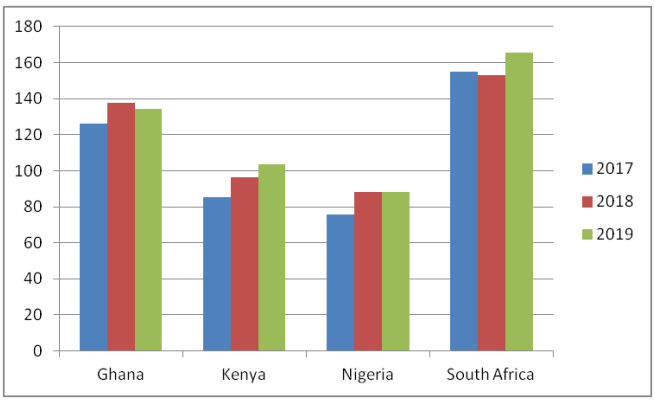

Figure 4: Mobile Cellular Subscription (per 100 people), Source: World Development Indicator

Table 3: Mobile Cellular Subscription (per 100 people)

Country	2017	2018	2019
Ghana	126.2	137.5	134.3
Kenya	85.3	96.3	103.8
Nigeria	75.9	88.2	88.2
South Africa	155.2	159.9	165.6

Created from: World Development Indicators
Series: Mobile cellular subscriptions (per 100 people) Subscriber

This can be traced to affordability but other factors such as poor Internet connectivity, low-level of education, lack of skills and absence of relevant content have notably been attributed to this trend [56]. Where fixed telephone services is available in the urban regions, the mobile-cellular services overrides limitations of infrastructures and thus many developing countries have enjoyed this method of communication alongside benefiting from universal services funds made possible from some governments, obliging service operators to give basic services at minimal price to remote area or poor income areas. This signifies more use of mobile cellular services as for Internet usage for most developing African countries like Nigeria. This statistics narrows the most popular medium of communication used by majority of users found in countries like Nigeria. The Global System for Mobile (GSM) Telecommunication technology has the highest share of service rendered in Nigeria [57], [58].

Premise 3: Larger population of Nigerians have access to GSM communication network, as such enjoy calls and SMS services that are used by criminals to perpetuate smishing and vishing attacks.

C. Banking Inclusion

Users become vulnerable to attacks when engaged in online activities, interaction with financial service providers and institutions because phishing actors attack targets for monetary reasons, impersonation and many more as seen in section 3. The Nigerian financial inclusion rate is still growing while efforts are being made by the government and stakeholders to meet the global recommendations required to foster growth. Nigeria is committed to achieving set objectives and targets an inclusion rate of 80% by 2020, a shift from its past data of 2016 which had 41.6% of adult population financially excluded of its 96.4 million population. And of 58.4% that is included, only 36.9million is banked [59]. Analysing these figures gives a picture of the size of most targeted sectors of phishing attacks like the banks. Where data is easily available, the number of bank customers opting for SMS or email for preferred communication method can further reveal insight to most targeted category of banked customers. Bank holders are more likely to fall for phishing attacks, we can assume over 36.9 million persons receive messages/calls from their Bank regarding their account and may be susceptible to fall for any phishing message/call placed to them concerning their account.

Premise 4: Bank account holders are a good target for phishing and more likely to be targeted via SMS messages and phone calls.

V. Smishing and Vishing in Nigeria

Availability of data emanating from Nigeria to this threat has been difficult to access for this survey but some Internet media have identified and reported cases of vishing and smishing attacks. In Nigeria vishing and smishing which is a form of phishing attack is punishable under Section 32 of the Cybercrime Act of 2015. Other financial crimes laws like the Economic and Financial Crimes Commission act of 2004 and Advance Fee Fraud and Related Offences Act 2006 have served its purpose in handling fraud related cybercrimes [60], [61].

In a survey conducted by [62], while examining e-banking fraud prevention and its detection in Nigerian banks, the researchers identified vishing and smishing amongst other methods used for perpetuating e-banking frauds in Nigerian banks. Nigeria was not left alone with the high numbers of COVID-19 phishing messages received by phone users. This constituted messages with all kinds of offers, particularly government offers as palliatives to entice vulnerable persons needing assistance as result of the pandemic. Figure 5 is an example of such messages. In an NCC related smishing message, the regulator intervened and cautioned the public on attackers offer of free Internet bundle as a stay at home package of COVID-19 and warned of visiting the fake URL which demands victims to fill in some personal data (https://covid-19-fg-grant.blogspot.com/?=1) [63]. The most reachable phishing data (attributed to either smishing and vishing or phishing attack as a whole) is that given by a US based multinational cybersecurity company which monitored activities of a certain Nigerian cybercriminal group coded "SilverTerrier" for more than six years. The group (SilverTerrier) grew with over 400 actors involved in BEC schemes that is recognized with 51,000 thousand malwares and 1.1 million attacks reached in 2017 [64]. Social profiles of these actors have pointed to the malwares, tools and fraudulent domains registered by Nigerian threat actors [10]. Though most of the victims of perpetuated crime ranged across the globe from Middle East, Asia and fewer numbers in Europe and North America, little or no data has been forwarded from security agencies to losses affecting local victims in Nigeria. An Interpol report also linked a Nigerian actor responsible for a single victim's loss of $15.4m and a worldwide loss of more than $60m in 2016 [10], other reported cases involving Nigerians is seen in [65]. These groups have used simple tools,

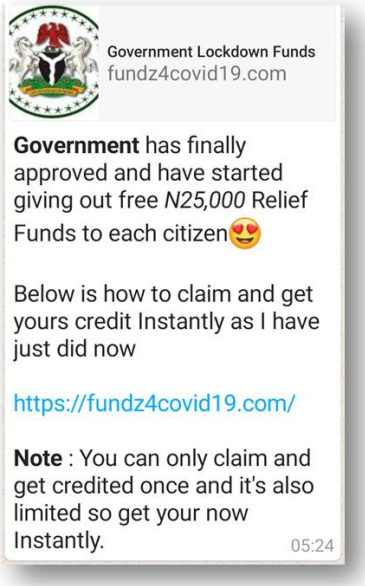

Figure 5: Sample of COVID-19 Smishing Message (Message Retrieved from author's OTT platform)

taking advantage of social media platforms to organise their activities. The impact of these syndicate groups is what citizens in Nigeria have continued to receive as bombardment of phishing messages targeted at in every platform (WhatsApp, SMS, Facebook, email, phone contact etc.).

VI. Conclusion

The phishing problem has seen quite a number of investigations, proposals and working solutions put in the market. And newer approaches using machine learning as discovered in earlier sections have shown to have better promising results to deterring phishing attacks. Unfortunately because no single solution has proved to have a total elimination of phishing attacks even with most commonly used technologies such as ant-spam, anti-virus, content filters and URL filtering, file sandboxing and secure web gateways are ways phishing is controlled. Yet the best security practice is when people are trained as a defence. User education is important; they need to know about latest phishing scams and techniques used by actors. Putting in place comfortable policies to allow employees and users report incidents can also position organisations to aptly deal with rising cases. In Nigeria, security, regulatory and non-governmental cybersecurity agencies can rise up to the task of educating and providing the general public on phishing threats and reporting incidences that will provide valuable data on methods and approaches attacks can be mitigated.

This paper has tried to reflect on most recent phishing attacks, focusing on the Nigerian environment by identifying nature and facets of tactics deployed by attackers within its setting. Phishing is still prevalent but getting more sophistication with BEC threats seen targeted not just at Nigerians but more so to other parts of the world by Nigerian actors. Most common is the assault targeted through messaging platform at mobile phone users and

non-Smartphone users as well, affecting a great majority in the country who will not necessarily have email accounts based on figures seen in countries Internet growth index. An even more generalised method is vishing which is growing at a higher scale and also affecting a wider population of Nigerians, taking advantage of wide coverage of GSM network across the country. More research work is needed in the areas of smishing and vishing attacks to tailor attacks that are targeted even to the most common remote user of cellular and Internet networks. Detection and mitigation solutions for smishing and vishing are very much needed to curb the annoying and misleading request thrown particularly over OTT applications, not undermining efforts from Telecom companies as well. Future work on this paper is to research more on the premises established here and deliver empirical data to vishing and smishing attacks claims in addition to an inside into threat analysis of various deployed techniques.

REFERENCES

[1] R. Rutherford, "The changing face of phishing," *Comput. Fraud Secur.*, vol. 2018, no. 11, pp. 6–8, Nov. 2018, doi: 10.1016/S1361-3723(18)30107-6.

[2] KnowBe4, "Phishing | History of Phishing," *Phishing.org*. https://www.phishing.org/history-of-phishing (accessed Aug. 28, 2020).

[3] "apwg_trends_report_q1_2020.pdf," *www.apwg.org*, May 11, 2020. https://docs.apwg.org/reports/apwg_trends_report_q1_2020.pdf (accessed Aug. 28, 2020).

[4] A. Aleroud and L. Zhou, "Phishing environments, techniques, and countermeasures: A survey," *Comput. Secur.*, vol. 68, pp. 160–196, Jul. 2017, doi: 10.1016/j.cose.2017.04.006.

[5] F. Mouton, L. Leenen, and H. S. Venter, "Social engineering attack examples, templates and scenarios," *Comput. Secur.*, vol. 59, pp. 186–209, 2016.

[6] M. M. Moreno-Fernández, F. Blanco, P. Garaizar, and H. Matute, "Fishing for phishers. Improving Internet users' sensitivity to visual deception cues to prevent electronic fraud," *Comput. Hum. Behav.*, vol. 69, pp. 421–436, Apr. 2017, doi: 10.1016/j.chb.2016.12.044.

[7] R. Dhamija, J. D. Tygar, and M. Hearst, "Why phishing works," in *Proceedings of the SIGCHI conference on Human Factors in computing systems*, 2006, pp. 581–590.

[8] S. Mansfield-Devine, "The ever-changing face of phishing," *Comput. Fraud Secur.*, vol. 2018, no. 11, pp. 17–19, Nov. 2018, doi: 10.1016/S1361-3723(18)30111-8.

[9] C. Ross, "The latest attacks and how to stop them," *Comput. Fraud Secur.*, vol. 2018, no. 11, pp. 11–14, Nov. 2018, doi: 10.1016/S1361-3723(18)30109-X.

[10] A. Hinchliffe, "Nigerian princes to kings of malware: the next evolution in Nigerian cybercrime," *Comput. Fraud Secur.*, vol. 2017, no. 5, pp. 5–9, May 2017, doi: 10.1016/S1361-3723(17)30040-4.

[11] P. Kumaraguru, Y. Rhee, A. Acquisti, L. F. Cranor, J. Hong, and E. Nunge, "Protecting People from Phishing: The Design and Evaluation of an Embedded Training Email System," in *School of Computer Science at Research Showcase @ CMU*, 2007, p. 12, [Online]. Available: http://repository.cmu.edu/hcii/63.

[12] A. Binks, "The art of phishing: past, present and future," *Comput. Fraud Secur.*, vol. 2019, no. 4, pp. 9–11, Apr. 2019, doi: 10.1016/S1361-3723(19)30040-5.

[13] S. F. Verkijika, "'If you know what to do, will you take action to avoid mobile phishing attacks': Self-efficacy, anticipated regret, and gender," *Comput. Hum. Behav.*, vol. 101, pp. 286–296, Dec. 2019, doi: 10.1016/j.chb.2019.07.034.

[14] M. Blythe, H. Petrie, and J. A. Clark, "F for fake: four studies on how we fall for phish," in *Proceedings of the 2011 annual conference on Human factors in computing systems - CHI '11*, Vancouver, BC, Canada, 2011, p. 3469, doi: 10.1145/1978942.1979459.

[15] L. De Kimpe, M. Walrave, W. Hardyns, L. Pauwels, and K. Ponnet, "You've got mail! Explaining individual differences in becoming a phishing target," *Telemat. Inform.*, vol. 35, no. 5, pp. 1277–1287, Aug. 2018, doi: 10.1016/j.tele.2018.02.009.

[16] F. Salahdine and N. Kaabouch, "Social Engineering Attacks: A Survey," *Future Internet*, vol. 11, no. 4, p. 89, Apr. 2019, doi: 10.3390/fi11040089.

[17] A. Emigh, "Online Identity Theft: Phishing Technology, Chokepoints and Countermeasures," Oct. 2005.

[18] K. L. Chiew, K. S. C. Yong, and C. L. Tan, "A survey of phishing attacks: Their types, vectors and technical approaches," *Expert Syst. Appl.*, vol. 106, pp. 1–20, Sep. 2018, doi: 10.1016/j.eswa.2018.03.050.

[19] M. Boddy, "Phishing 2.0: the new evolution in cybercrime," *Comput. Fraud Secur.*, vol. 2018, no. 11, pp. 8–10, Nov. 2018, doi: 10.1016/S1361-3723(18)30108-8.

[20] S. Furnell, K. Millet, and M. Papadaki, "Fifteen years of phishing: can technology save us?," *Comput. Fraud Secur.*, vol. 2019, no. 7, pp. 11–16, Jul. 2019, doi: 10.1016/S1361-3723(19)30074-0.

[21] A. Riley and M. Feller, "Phishing Campaigns are Manipulating the Windows Control Panel Extension to Deliver Banking Trojans," *Cofense*, Jan. 17, 2019. https://cofense.com/phishing-campaigns-manipulating-windows-control-panel-extension-deliver-banking-trojans/ (accessed Sep. 17, 2020).

[22] P. Kumaraguru, S. Sheng, A. Acquisti, L. F. Cranor, and J. Hong, "Teaching Johnny not to fall for phish," *ACM Trans. Internet Technol.*, vol. 10, no. 2, pp. 1–31, May 2010, doi: 10.1145/1754393.1754396.

[23] B. B. Gupta, N. A. G. Arachchilage, and K. E. Psannis, "Defending against phishing attacks: taxonomy of methods, current issues and future directions," *Telecommun. Syst.*, vol. 67, no. 2, pp. 247–267, Feb. 2018, doi: 10.1007/s11235-017-0334-z.

[24] Y. Ding, N. Luktarhan, K. Li, and W. Slamu, "A keyword-based combination approach for detecting phishing webpages," *Comput. Secur.*, vol. 84, pp. 256–275, Jul. 2019, doi: 10.1016/j.cose.2019.03.018.

[25] C. L. Tan, K. L. Chiew, K. S. C. Yong, S. N. Sze, J. Abdullah, and Y. Sebastian, "A graph-theoretic approach for the detection of phishing webpages," *Comput. Secur.*, vol. 95, p. 101793, Aug. 2020, doi: 10.1016/j.cose.2020.101793.

[26] M. Khonji, Y. Iraqi, and A. Jones, "Phishing Detection: A Literature Survey," *IEEE Commun. Surv. Tutor.*, vol. 15, no. 4, pp. 2091–2121, 2013, doi: 10.1109/SURV.2013.032213.00009.

[27] D. Sahoo, C. Liu, and S. C. H. Hoi, "Malicious URL Detection using Machine Learning: A Survey," *ArXiv170107179 Cs*, Aug. 2019, Accessed: Aug. 27, 2020. [Online]. Available: http://arxiv.org/abs/1701.07179.

[28] S. Gupta, P. Gupta, M. Ahamad, and P. Kumaraguru, "Abusing Phone Numbers and Cross-Application Features for Crafting Targeted Attacks," *ArXiv151207330 Cs*, Dec. 2015, Accessed: Dec. 29, 2020. [Online]. Available: http://arxiv.org/abs/1512.07330.

[29] S. Sheng, M. Holbrook, P. Kumaraguru, L. F. Cranor, and J. Downs, "Who falls for phish?: a demographic analysis of phishing susceptibility and effectiveness of interventions," in *Proceedings of the 28th international conference on Human factors in computing systems - CHI '10*, Atlanta, Georgia, USA, 2010, p. 373, doi: 10.1145/1753326.1753383.

[30] P. Kumaraguru *et al.*, "School of phish: a real-word evaluation of anti-phishing training," in *Proceedings of the 5th Symposium on Usable Privacy and Security - SOUPS '09*, Mountain View, California, 2009, p. 1, doi: 10.1145/1572532.1572536.

[31] T. Halevi, N. Memon, and O. Nov, "Spear-Phishing in the Wild: A Real-World Study of Personality, Phishing Self-Efficacy and Vulnerability to Spear-Phishing Attacks," *SSRN Electron. J.*, 2015, doi: 10.2139/ssrn.2544742.

[32] A. Bhardwaj, V. Sapra, A. Kumar, N. Kumar, and S. Arthi, "Why is phishing still successful?," *Comput. Fraud Secur.*, vol. 2020, no. 9, pp. 15–19, Sep. 2020, doi: 10.1016/S1361-3723(20)30098-1.

[33] "2019 INTERNET CRIME REPORT," FBI's Internet Crime Complaint Center (IC3). Accessed: Sep. 05, 2020. [Online]. Available: https://pdf.ic3.gov/2019_IC3Report.pdf.

[34] E. Derouet, "Fighting phishing and securing data with email authentication," *Comput. Fraud Secur.*, vol. 2016, no. 10, pp. 5–8, Oct. 2016, doi: 10.1016/S1361-3723(16)30079-3.

[35] E. O. Yeboah-Boateng and P. M. Amanor, "Phishing, SMiShing & Vishing: An Assessment of Threats against Mobile Devices," *J. Emerg. Trends Comput. Inf. Sci.*, vol. 5, no. 4, p. 11, 2014.

[36] M. K. Cellan-Jones Rory, "Vishing and smishing: Social engineering fraud," *BBC News*, Jan. 01, 2016.

[37] H. Shahriar, T. Klintic, and V. Clincy, "Mobile phishing attacks and mitigation techniques," *J. Inf. Secur.*, vol. 6, no. 03, p. 206, 2015.

[38] F. Pervaiz *et al.*, "An assessment of SMS fraud in Pakistan," in *Proceedings of the Conference on Computing & Sustainable*

Societies - COMPASS 19, Accra, Ghana, 2019, pp. 195–205, doi: 10.1145/3314344.3332500.
[39] E. M. Maseno, "Vishing Attack Detection Model For Mobile Users.," PhD Thesis, KCA University, 2017.
[40] J. Fruhlinger, "Vishing explained: How voice phishing attacks scam victims," *CSO Online*, May 18, 2020. https://www.csoonline.com/article/3543771/vishing-explained-how-voice-phishing-attacks-scam-victims.html (accessed Sep. 02, 2020).
[41] G. Ollmann, "The vishing guide." IBM Global Technology Services, 2007, [Online]. Available: http://www.infosecwriters.com/text_resources/pdf/IBM_ISS_vishing_guide_GOllmann.pdf.
[42] J. Van der Kleut, "What is vishing? Tips for spotting and avoiding voice scams," *NortonLifeLock*. https://us.norton.com/internetsecurity-online-scams-vishing.html (accessed Jan. 07, 2021).
[43] "Voice Phishing Scams Are Getting More Clever — Krebs on Security," Oct. 01, 2018. https://krebsonsecurity.com/2018/10/voice-phishing-scams-are-getting-more-clever/ (accessed Jan. 02, 2021).
[44] R. Dantu and P. Kolan, "Detecting Spam in VoIP Networks," in *SRUTI '05: Steps to Reducing Unwanted Traffic on the Internet Workshop*, p. 7.
[45] H. Sengar, X. Wang, and A. Nichols, "Call Behavioral Analysis to Thwart SPIT Attacks on VoIP Networks," 2011, [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.717.4780.
[46] O. Kedem and T. Aviv, "(71) Applicant: BioCatch Ltd., Tel Aviv (IL)," US 2019 / 0158535 A1, 2019.
[47] S. L. Abdul-Rasheed, I. Lateef, M. A. Yinusa, and R. Abdullateef, "Cybercrime and Nigeria's External Image: A Critical Assessment," p. 14, 2016.
[48] U. Ibrahim, "The Impact of Cybercrime on the Nigerian Economy and Banking System," *NDIC-Q.*, vol. Vol-34, no. No-12, p. 20, 2019.
[49] "Population, total - Nigeria | Data." https://data.worldbank.org/indicator/SP.POP.TOTL?locations=NG (accessed Sep. 13, 2020).
[50] H. Plecher, "Countries with the largest population 2019," *Statista*, Mar. 31, 2020. https://www.statista.com/statistics/262879/countries-with-the-largest-population/ (accessed Nov. 17, 2020).
[51] United Nations department for economic and social affairs, *United nations e-government survey 2018*. Place of publication not identified: UNITED NATIONS, 2019.
[52] C. J, "Nigeria: number of internet users 2025," *Statista*, Nov. 09, 2020. https://www.statista.com/statistics/183849/internet-users-nigeria/ (accessed Nov. 09, 2020).
[53] "Industry Statistics," *Nigerian Communications Commision*, Nov. 09, 2020. https://www.ncc.gov.ng/statistics-reports/industry-overview#view-graphs-tables (accessed Nov. 17, 2020).
[54] J. Clement, "Nigeria mobile internet users 2025," *Statista*, Nov. 09, 2020. https://www.statista.com/statistics/972896/nigeria-mobile-internet-users/ (accessed Nov. 17, 2020).
[55] United Nations department for economic and social affairs. Desa, *United nations e-government survey 2020: digital government in the decade of action for... sustainable development*. S.l.: UNITED NATIONS, 2020.
[56] M. Schaaper and P. Biggs, "Measuring Digital Development: ICT Price Trends 2019," International Telecommunication Union (ITU), Publication, 2019. [Online]. Available: https://www.itu.int/en/ITU-D/Statistics/Documents/publications/prices2019/ITU_ICTpriceTrends_2019.pdf.
[57] Policy Competition and Economic Analysis Department, "2018 subscriber/network data report," Nigerian Communications Commision. Accessed: Sep. 10, 2020. [Online]. Available: https://www.ncc.gov.ng/docman-main/industry-statistics/policies-reports/832-2018-year-end-subscriber-network-data-report/file.
[58] Policy competition and economic analysis department, "2019 subscriber/network data report," NCC (Nigerian Communications Commission). [Online]. Available: https://www.ncc.gov.ng/docman-main/industry-statistics/policies-reports/915-2019-year-end-subscriber-network-data-report/file.
[59] "National financial inclusion strategy.pdf," Central Bank of Ngeria, Oct. 2018. Accessed: Nov. 24, 2020. [Online]. Available: https://www.cbn.gov.ng/out/2019/ccd/national%20financial%20inclusion%20strategy.pdf.
[60] *CyberCrime__Prohibition_Prevention_etc__Act__2015.pdf*. .
[61] *Advance-fee-fraud-and-other-related-offences-act.pdf*. .
[62] O. M. Fadayo, "An Examination of E-Banking Fraud Prevention and Detection in Nigerian Banks," p. 350.
[63] "DISCLAIMER - Press Statement: NCC Alerts Nigerians about Fake Website Spreading False Free Internet Claim." https://www.ncc.gov.ng/media-centre/news-headlines/809-disclaimer-press-statement-ncc-alerts-nigerians-about-fake-website-spreading-false-free-internet-claim (accessed Dec. 12, 2020).
[64] "SilverTerrier: 2018 Nigerian Business Email Compromise Update," *Unit42*, May 09, 2019. https://unit42.paloaltonetworks.com/silverterrier-2018-nigerian-business-email-compromise/ (accessed Sep. 01, 2020).
[65] "281 Arrested Worldwide in Coordinated International Enforcement Operation Targeting Hundreds of Individuals in Business Email Compromise Schemes," Sep. 10, 2019. https://www.justice.gov/opa/pr/281-arrested-worldwide-coordinated-international-enforcement-operation-targeting-hundreds (accessed Sep. 01, 2020).