IDENTIFYING PHISHING AS A FORM OF CYBERCRIME IN NIGERIA*

Abstract

Phishing is one of the oldest and most flexible types of social engineering attacks and could be used in many ways, and for different purposes, to lure unwary users to sites and trick them into entering personal information. This paper is written with the purpose of educating the public about phishing as a form of cybercrime. It adopts the use of doctrinal research methodology in analyzing phishing as a form of cybercrime, discussing its historical development, techniques and its criminalization under the Cybercrime Act in Nigeria. The paper further highlights the various ways of identifying messages that are phishing in nature. Aside from the general conclusion, the paper enumerates some of the things which a person can do when confronted with an attempted phishing scam. The paper recommends that the general public should be more suspicious of all electronic communications and websites especially those communications which were not initiated by them.

Keywords: 'Phishing', 'Scam', 'Email', 'Cybercrime', 'Phishing Techniques', 'Email Communications'.

1. Introduction

The Internet has created a marketplace for businesses and consumers to come together and interact in new and exciting ways. Unfortunately, it has also provided criminals and the unscrupulous with a new venue.[1] Phishing is a social engineering technique that is used to bypass technical controls implemented to mitigate security risks in information systems.[2] Phishing is a scam that has evolved many years ago and it has been growing ever since. Phishing refers to the process where a targeted individual is contacted by email or telephone by someone posing as a legitimate institution to lure the individual into providing sensitive information such as banking information, credit card details and passwords. The personal information is then used to access the individual's account and can result in identity theft and financial loss.[3] Phishing requires functional and effective countermeasures, as does any crime that result in financial loses. Many financial institutions currently combat phishing by contracting takedown companies that remove relevant phishing websites as soon as possible after they are detected.[4]

2. Meaning of Phishing

'Phishing' is the criminal and fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication through e- mails or instant messaging. They masquerade in form of an email from what appears from your bank asking a user to change his or her password or reveal his or her identity so that such information can later be used to defraud the user.[5] Phishing can be defined as an attempt by hackers

* **ABIODUN ASHIRU** (LL.B, B.L, LL.M) is a lecturer, Department of Public and Private Law, Lagos State University, Lagos-Badagry Expressway, Lagos.His email address is ashiruabiodun@gmail.com.

[1] R L B Stevenson, 'Plugging the "Phishing" Hole: Legislation versus Technology', 5 *Duke Law & Technology Review,* (2005) 1-14.

[2] A M Rader and M. Rahman, 'Exploring Historical and Emerging Phishing Techniques and Mitigating the Associated Security Risks', 5 (4) *International Journal of Network Security & Its Applications*, (2013) pp 24-41.

[3] Phishing. org, 'What is Phishing?' Available at https://www.phishing.org/what-is-phishing, accessed March 21, 2021.

[4] J P J Nero and Ors, 'Phishing: Crime that Pays', available at https://www.researchgate.net/publication/254052287_Phishing_Crime_that_pays, accessed August 2 2021.

[5] The Cybercrime (Prohibition, Prevention, etc) Act 2015, section 58.

or cyber criminals in which they try to lure computer or internet users into divulging their personal or sensitive financial information through a maliciously crafted message or an e-mail.[6] This sensitive or confidential information may include birthdates, passwords, credit card details, and social security numbers.[7] The hackers disguise themselves as an official entity such as authorities from the tax department or employees of a bank to gain the victim's trust.

Phishing scams are attempts by scammers to trick you into giving out personal information such as your bank account numbers, passwords and credit card numbers.[8] Phishing is the fraudulent attempt to obtain sensitive information or data, such as usernames, passwords and credit card details, by disguising oneself as a trustworthy entity in an electronic communication.[9]It is typically carried out by email spoofing, instant messaging, and text messaging. Phishing often directs users to enter personal information at a fake website which matches the look and feel of the legitimate site. Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers.[10]It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message. The recipient is then tricked into clicking a malicious link, which can lead to the installation of malware, the freezing of the system as part of a ransomware attack or the revealing of sensitive information. Phishing is a cyber-attack that uses disguised email as a weapon. The goal is to trick the email recipient into believing that the message is something they want or need — a request from their bank, for instance, or a note from someone in their company — and to click a link or download an attachment. Phishing is often used to gain a foothold in corporate or governmental networks as a part of a larger attack, such as an advanced persistent threat (APT) event.[11]

3. Historical Development of Phishing

Some say the term "phishing" got influences from the word "fishing". Analogous to "fishing", "phishing" is also a technique to "fish" for usernames, passwords, and other sensitive information, from a "sea" of users. Hackers generally use the letter "ph" instead of "f" and therefore initially they were known as phreaks.[12]The creator of the infamous Blue Box, John Draper, aka Captain Crunch, coined the term Phreaking. Phreaking refers to the technique of hacking telecommunication systems. The term "phishing" and its concept can be traced back to the 90s through America Online (AOL). A group of hackers called themselves as "warez community". They impersonated as "AOL employees". This group is also known as the first "phishers." They collected login credentials and personal information from AOL users. During the 90s, AOL was one of the leading internet service providers and had over a million customers subscribed to their service.

This massive popularity of AOL grabbed the attention of hackers. People trading with pirated and illegal software and tools used AOL for their communication. They formed a group called "the warez

[6] 'What is Phishing? How This Cyber-attack Works and How to Prevent It', available at https://www.csoonline.com/article/2117843/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it.html, accessed October 21, 2020.
[7] *ibid*
[8] Phishing: How does this Scam Work, available at https://www.scamwatch.gov.au/types-of-scams/attempts-to-gain-your-personal-information/phishing, accessed October 30, 2020.
[9] R Zulfikar; 'Phishing Attacks and Countermeasures', In S M Stavroulakis, Peter (eds.). *Handbook of Information and Communication Security*. Springer. 2010p23-55.
[10] *ibid.*
[11] V D Merwe, A J, Loock, M, Dabrowski, M. *Characteristics and Responsibilities involved in a Phishing Attack, Winter International Symposium on Information and Communication Technologies*, Cape Town, January 2005, pp98.
[12] *ibid*

community", thus sowing the first seeds of phishing.[13] Back in the early to mid-1990s, the only Internet option was 'dial-up' access for a fee. For those that were reluctant to pay for Internet access, the alternative was a thirty days' free trial to access to the Internet via an AOL floppy disk. Rather than face life without the Internet after the trial period expired, some found a way to change their screen names to make it appear as if they were AOL administrators. Using these phony screen names, they would "phish" for log-in credentials to continue accessing the internet for free.

As internet use increased in popularity, scammers adapted these tactics to disguise themselves as administrators from an ISP, emailing the accounts of the ISP's customers to elicit user login credentials. Having spoofed someone, the hacker could access the Internet from that user's account with the bonus of sending spam from the user's email address. The Love Bug of 2000. A change in tactics saw the world fall victim to the Love Bug on May 4 2000. Starting in the Philippines, mailboxes around the globe were filled with a message titled "ILOVEYOU". The message body simply said "Kindly check the attached LOVELETTER coming from me".

Those who could not resist unearthing their secret crush, opened what they thought was a harmless file, only to unleash a worm that did damage on the local machine. The worm overwrote image files and sent a copy of itself to all the user´s contacts in their outlook address book. 'Love Bug' showed how to get spam to send itself and that, with a cleverly designed virus that preyed on human psychology and technical failings; malware could rack up enormous numbers of victims. In all about forty-five million Windows PCs were thought to have been hit. The history of phishing shows that, although delivery methods have evolved over two decades to evade detection by spam filters and other technology, the tactics employed by phishers have remained fairly consistent. It would seem logical that people should have learned to avoid the trap of surrendering login credentials, clicking links or even opening attachments. Yet this is still an effective tactic for hackers.[14]

4. Techniques of Phishing

There are a number of different techniques used to obtain personal information from users. As technology becomes more advanced, the cybercriminals' techniques being used are also more advanced. To prevent Internet phishing, users of the internet should have knowledge of how the bad guys do this and they should also be aware of anti-phishing techniques to protect themselves from becoming victims.

4.1 Email Phishing Scams

This is the most common phishing technique. By this, the same email is sent to millions of users with a request to fill in personal details. These details will be used by the phishers for their illegal activities. Most of the messages have an urgent note which requires the user to enter credentials to update account information, change details, or verify accounts. Sometimes, they may be asked to fill out a form to access a new service through a link which is provided in the email. Email phishing is a numbers game. An attacker sending out thousands of fraudulent messages can access significant information and sums of money, even if only a small percentage of recipients fall for the scam. As seen above, there are some techniques attackers use to increase their success rates. For one, they will go to great lengths in designing phishing messages to mimic actual emails from a spoofed organization. Using the same

[13] History of Phishing: How Phishing Attacks Evolved from Poorly Constructed Attempts to Highly Sophisticated Attacks, available at https://www.phishprotection.com/resources/history-of-phishing/, accessed November 5, 2020.

[14] M A Rader and Syed (Shawon) M. Rahman, supra note 2 at 26.

phrasing, typefaces, logos, and signatures makes the messages appear legitimate. In addition, attackers will usually try to push users into action by creating a sense of urgency.[15]

4.2 Spear Phishing

Spear phishing targets a specific person or enterprise, as opposed to random application users. It's a more in-depth version of phishing that requires special knowledge about an organization, including its power structure. While traditional phishing uses a 'spray and pray' approach, meaning mass emails are sent to as many people as possible, spear phishing is a much more targeted attack in which the hacker knows which specific individual or organization they are after.[16]They do research on the target in order to make the attack more personalized and increase the likelihood of the target falling into their trap.[17]

4.3 Pharming

Pharming is a cyberattack intended to redirect a website's traffic to another fake site. [18]Pharming can be conducted either by changing the hosts file on a victim's computer or by exploitation of a vulnerability in Domain Name System Server (DNS) server software.[19] DNS servers are computers responsible for resolving Internet names into their real IP addresses. Compromised DNS servers are sometimes referred to as "poisoned". Pharming requires unprotected access to target a computer, such as altering a customer's home computer, rather than a corporate business server. The term "pharming" is a neologism based on the words "farming" and "phishing". Phishing is a type of social-engineering attack to obtain access credentials, such as user names and passwords. In recent years, both pharming and phishing have been used to gain information for online identity theft. Pharming has become of major concern to businesses hosting e-commerce and online banking websites. Sophisticated measures known as anti-pharming are required to protect against this serious threat. Antivirus software and spyware removal software cannot protect against pharming.[20]

4.4 Smishing

Smishing is phishing conducted *via* Short Message Service (SMS), a telephone-based text messaging service. A smishing text, for example, attempts to entice a victim into revealing personal information via a link that leads to a phishing website. It is a phishing method where users receive text messages containing malicious links.[21] Clicking the link leads to a phishing website where they are asked to reveal personal information.[22]

5. Criminalization of Phishing in Nigeria

The Cybercrime (Prohibition, Prevention, etc.) Act 2015 (CPPA) stipulates that:

> any person, who intentionally and without authorization, intercepts by technical means, non---public transmissions of computer data, content, or traffic data, including electromagnetic emissions or signals from a computer, computer system or

[15]L Irwin, 'Phishing Techniques', *available* at https://www.phishing.org/phishing-techniques, accessed November 6, 2020.
[16] *ibid*
[17] *Ibid.*
[18] *ibid*
[19] *ibid*
[20] *Ibid.*
[21] L Irwin, 'The 5 Most Common Types of Phishing Attack', available at <https://www.itgovernance.eu/blog/en/the-5-most-common-types-of-phishing-attack> Accessed November 5, 2020.
[22] *ibid*

> network carrying or emitting signals, to or from a computer, computer system or connected system or network; commits an offence and shall be liable on conviction to imprisonment for a term of not more than 2 years or to a fine of not more than N5,000,000.00 or to both such fine and imprisonment.[23]

This offence is known as 'Unlawful interceptions'. Although this offence is statutorily different from Phishing, their ingredients are nevertheless similar. Phishing which is the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers shares similar ingredient with the offence of unlawful interception.[24]The Act provides that any person who knowingly or intentionally engages in computer phishing shall be liable upon conviction to 3 years' imprisonment or a fine of N1, 000,000.00 or both.[25] This section merely provides for the criminalization of phishing without providing the element thereof. This is however provided for under section 58 of the Act. A close look at the section 32 reveals that the word 'phishing' as used under the Act may also be replaced with 'spamming'.

Section 58 of the CPPA defined 'Phishing' as the criminal and fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication through e-mails or instant messaging either in form of an email from what appears from your bank asking a user to change his or her password or reveal his or her identity so that such information can later be used to defraud the user.

To be guilty of the offence of phishing under the CPPA, the accused must have made a fraudulent representation parading himself as a trustworthy with the use of a computer and an internet network facility. The main reason this is done is to gain the trust of the victim, so that the victim may divulge sensitive and confidential information relating to his finances to the accused. Under the traditional criminal justice system, the perpetrator of this act may have been properly charged with the offence of obtaining by false pretences.[26]The offence of obtaining by false pretences is proscribed by the Code, and may be found in sections 419, 419A, 419B, 420, 421, 422, and 423 of the Criminal Code Act. In summary, the sections state that:

> where any person, by false pretence, and with the intent to defraud another person, obtains from that other person anything capable of being stolen, or advises any other person to deliver to any other person anything capable of being stolen, or obtains credit by false pretences or by some other kind of fraud, commits an offence and is liable on conviction to imprisonment for a term of three to seven years.[27]

The only defence or debate for this charge would have been whether or not the piece of information obtained is a thing capable of being stolen. In summary, the Nigerian society has been faced with several forms of scam and fraud in the past and the introduction of computer and computer network has made the commission of these atrocities smoother and easier. One of the commonly committed internet related crime is phishing. Section 12 of the CPPA criminalizes phishing by providing that any person, who intentionally and without authorization, intercepts by technical means, non--public transmissions of

[23] The Cybercrime (Prohibition, Prevention, etc.) Act 2015 (CPPA) section 12
[24] This has been criminalized by section 12 of the CPPA
[25] The Cybercrime (Prohibition, Prevention, etc.) Act 2015 (CPPA) section 32
[26] See the Criminal Code Act 1990, s.419.
[27] The Criminal Code Act 1990, ss 419, 419A, 419B, 420, 421, 422, and 423

computer data, content, or traffic data, including electromagnetic emissions or signals from a computer, computer system or network carrying or emitting signals, to or from a computer, computer system or connected system or network; commits an offence and shall be liable upon conviction. The punishment for the offence is imprisonment for a term of not more than 2 years or to a fine of not more than N5, 000,000.00 or to both such fine and imprisonment.[28]

6. Phishing Laws in Other Jurisdictions

6.1 The United States

Phishing uses deceptive spam that appears to be coming from legitimate, well-known sources to trick consumers into divulging sensitive or personal information, such as credit card numbers, other financial data, or passwords, either through a reply email or a link to a copycat of the purported source's website. Just like Nigeria, the United States had also had its own share of internet frauds. However, unlike Nigeria, in the United States, phishing is covered under various State laws, there is no single federal statute that directly criminalizes this type of activity. However, there are broader federal criminal laws that do apply to phishing and other identity theft crimes. For example, because phishing involves solicitations that are usually sent over the internet, the federal law against wire fraud is often used to punish phishing crime on a federal level.

Wire fraud is a type of fraud that involves the use of some form of telecommunications or the internet. These can include a phone call, a fax, an email, a text, or social media messaging, among many other forms.[29]According to the U.S. Department of Justice Criminal Resource Manual, the key elements of wire fraud include:

1) that the defendant voluntarily and intentionally devised or participated in a scheme to defraud another out of money;
2) that the defendant did so with the intent to defraud;
3) that it was reasonably foreseeable that interstate wire communications would be used; and
4) that interstate wire communications were in fact used.[30]

Wire fraud is a federal crime that carries a sentence of not more than 20 years' imprisonment and fines of up to $250,000 for individuals and $500,000 for organizations. The statute of limitations to bring a charge is five years unless the wire fraud targeted a financial institution, in which case the statute of limitations is 10 years. If the wire fraud is related to special circumstances, such as a presidentially declared state of emergency or targets a financial institution, it can carry a prison sentence of up to 30 years and a fine of up to $1 million. A person need not have actually defrauded someone or personally sent a fraudulent communication to be convicted of wire fraud.[31]The elements of wire fraud under section 1343 directly parallel those of the mail fraud statute, but require the use of an interstate telephone call or electronic communication made in furtherance of the scheme.

[28] The Cybercrime (Prohibition, Prevention, etc.) Act 2015 (CPPA) section 12

[29] 'What is Wire Fraud?' Available at https://www.investopedia.com/terms/w/wirefraud.asp, accessed August 3 2021.

[30] Section 941.18 U.S.C. 1343

[31] Every CRS Report. 'Mail and Wire Fraud: A Brief Overview of Federal Criminal Law.' Accessed August 2 2021.

This was properly explained by the court in the case of *United States v Bristcoe.*[32]Just as a person charged with the offence of phishing under the CPPA in Nigeria may also be charged with the offence of obtaining by false pretence, a person charged with phishing under the federal statute in the United States may also be charged with wire fraud. But while all States have laws that prohibit fraudulently acquiring someone else's personal information, not all States have laws that specifically address phishing. According to the National Conference of State Legislatures, a minority of States currently have specific phishing laws. However, even in those States that do not have specific phishing laws, other criminal laws can apply to phishing activity (computer crimes, identity theft). The implication of this position is that the activity is a crime in every State. States without these laws may also adapt phishing laws as the crime becomes more common. In the United States, twenty-three States and Guam have laws specifically aimed at phishing schemes. Other States have laws that address computer crime, fraudulent or deceptive practices or identity theft, which could also apply to phishing crimes.[33]The States with laws on phishing are Alabama, Arkansas, Arizona, California, Connecticut, Florida, Georgia, Illinois, Kentucky, Louisiana, Michigan, Minnesota, Montana, New Mexico, New York, Oklahoma, Oregon, Rhode Island, Tennessee, Texas, Utah, Virginia, Washington, and Guam.

6.2 The United Kingdom

According to the Government's Cyber Security Breaches Survey 2020 in the UK, Phishing is the most common form of cyber-attack in the UK. Five times more businesses now face phishing than attacks from viruses.[34]The law in the UK is gradually adapting to address phishing and other forms of cyber-crime. Forthcoming amendments to the Computer Misuse Act 1990 (in the Police and Justice Act 2006) aim to bring it up to date with developments in computer crime and to increase penalties for breach (up to 10 years imprisonment). Meanwhile, the Fraud Act 2006[35]resolves uncertainty over whether statutory offences under earlier anti-fraud law applied to activities like phishing and introduces new offences to better equip police and prosecutors to deal with the challenge of combating fraud in the 21st century. It addresses phishing by establishing the offence of making a false representation (including via email or the internet) with a view to making a gain for oneself or another, or to causing loss to another or exposing another to a risk of loss. The Fraud Act also addresses other aspects of cyber-crime, for example by introducing an offence of possessing software or data for use in fraud and of creating

[32] 65 F. 3d 576; see also the United States Department of Justice Archives, Elements of Wire Fraud, available at https://www.justice.gov/archives/jm/criminal-resourcce-manual-951-18-usc-1343-elements-wire-fraud, accessed August 3 2021.

[33] National Conference of State Legislatures, State Laws Addressing Phishing, available at https://www.ncsl.org/research/telecommunications-and-information-technology/state-phishing-laws.aspx, accessed November 10, 2020. See also State Spyware Laws and Computer Crime Statutes.

[34] L Hiscox, What is a Phishing Attack, available at https://www.hiscox.co.uk/business-insurance/cyber-and-data-insurance/faq/what-is-a-phishing-attack, accessed August 3 2021.

[35] The Act provides for a general offence of fraud with three ways of committing it, which are by false representation, by failing to disclose information and by abuse of position. It creates new offences of obtaining services dishonestly and of possessing, making and supplying articles for use in frauds. It also contains a new offence of fraudulent trading applicable to non-corporate traders. This offence parallels the offences in section 458 of the Companies Act 1985 (c. 6) and Article 451 of the Companies (Northern Ireland) Order 1986 (SI 1986/1032 (N.I. 6)), which apply to companies and certain other corporate bodies. The Act repeals the deception offences in sections 15, 15A, 16, and 20(2) of the Theft Act 1968 (c. 60), sections 15, 15A, 16 and 19(2) of the Theft Act (Northern Ireland) 1969 (c. 16 (N.I.)), sections 1 and 2 of the Theft Act 1978 (c. 31) and Articles 3 and 4 of the Theft (Northern Ireland) Order 1978 (SI 1978/1407 (N.I. 23)); see also legislation.gov.uk, Fraud Act 2006, available at https://www.legislation.gov.uk/ukpga/2006/35/notes, accessed August 7 2021.

software knowing that it is designed or adapted for use in connection with fraud. Offences under these Acts are punishable by fines and / or imprisonment up to 10 years.[36]

Section 2 of the Fraud Act may be the most appropriate provision to contain the criminalization of phishing. For the purpose of clarity, section 2 of the Fraud Act is reproduced hereunder:

> (1) A person is in breach of this section if he—
> (a) dishonestly makes a false representation, and
> (b) intends, by making the representation—
> (i) to make a gain for himself or another, or
> (ii) to cause loss to another or to expose another to a risk of loss.
> (2) A representation is false if—
> (a) it is untrue or misleading, and
> (b) the person making it knows that it is, or might be, untrue or misleading.
> (3) "Representation" means any representation as to fact or law, including a representation as to the state of mind of—
> (a) the person making the representation, or
> (b) any other person.
> (4) A representation may be express or implied.
> (5) For the purposes of this section a representation may be regarded as made if it (or anything implying it) is submitted in any form to any system or device designed to receive, convey or respond to communications (with or without human intervention). [37]

From the above provision, for a person to be guilty of phishing or fraud by representation as properly coined, the person must have a dishonest or misleading representation with the aid of any system which representation intends to make gain to himself or another or cause a loss to another or expose another to a risk of loss.

7. How to Recognize Phishing

Scammers use email or text messages to trick their victim into giving them their personal information. They may try to steal the passwords, account numbers, or social security numbers. If they get that information, they could gain access to the email, bank, or other accounts. Scammers launch thousands of phishing attacks like every day and they're often successful. The FBI's[38]Internet Crime Complaint Center reported that people lost $57 million to phishing schemes in one year.[39]Scammers often update

[36] Bcs.org, Legal Net Tightens on Phishing, available at https://www.bcs.org/content-hub/legal-net-tightens-on-phishing/, accessed August 5 2021.

[37] Fraud Act 2006, section 2

[38]The Federal Bureau of Investigation (FBI) is an intelligence-driven and threat-focused national security organization with both intelligence and law enforcement responsibilities. It is the principal investigative arm of the U.S. Department of Justice and a full member of the U.S. Intelligence Community. The FBI has the authority and responsibility to investigate specific crimes assigned to it and to provide other law enforcement agencies with cooperative services, such as fingerprint identification, laboratory examinations, and training. The FBI also gathers, shares, and analyzes intelligence, both to support its own investigations and those of its partners and to better understand and combat the security threats facing the United States; see also What is the FBI? Available at https://www.fbi.gov/about/faqs/what-is-the-fbi#:~:text=The%20FBI%20is%20an%20intelligence,of%20the%20U.S.%20Intelligence%20Community accessed 10 January 2021.

[39] Federal Trade Commission Consumer Information, 'How to Recognize Phishing', available at https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams, accessed 10 January 2021.

their tactics, but there are some signs that will help one recognize a phishing email or text message. Phishing emails and text messages may look like they're from a reputable company. They may look like they're from a bank, a credit card company, a social networking site, an online payment website or app, or an online store.

a**. Legit companies don't request your sensitive information via email**

Chances are if you receive an unsolicited email from an institution that provides a link or attachment and asks you to provide sensitive information, it's a scam. Most companies will not send you an email asking for passwords, credit card information, credit scores, or tax numbers, nor will they send you a link from which you need to login.[40]

b. **Legit companies usually call you by your name**

Phishing emails typically use generic salutations such as "Dear valued member," "Dear account holder," or "Dear customer." If a company you deal with required information about your account, the email would call you by name and probably direct you to contact them via phone. But, some hackers simply avoid the salutation altogether. This is especially common with advertisements. The phishing email below is an excellent example. Everything in it is nearly perfect. It will no doubt be difficult to spot a potentially malicious email message.[41]

c. **Legit companies have domain emails**

It is not enough to check the name of the person sending the email. It is needful to check their email address by hovering your mouse over the 'from' address. Make sure no alterations (like additional numbers or letters) have been made. Check out the difference between these two email addresses as an example of altered emails: michelle@paypal.com michelle@paypal23.com. This however is not a foolproof method. Sometimes companies make use of unique or varied domains to send emails, and some smaller companies use third party email providers.[42]

d. **Legit companies know how to spell**

The easiest possible way to recognize a scammy email is bad grammar. An email from a legitimate organization should be well written. Hackers do prey on the uneducated believing them to be less observant and thus, easier targets.[43]

e. **Legit companies don't force you to their website**

Sometimes phishing emails are coded entirely as a hyperlink. Therefore, clicking accidentally or deliberately anywhere in the email will open a fake web page, or download spam onto your computer.[44]

f. **Legit companies don't send unsolicited attachments**

Unsolicited emails that contain attachments reek of hackers. Typically, authentic institutions do not randomly send you emails with attachments, but instead direct you to download documents or files on their own website. This method is however foolproof. Sometimes companies that already have your email will send you information, such as a white paper, that may require a download. In that case, be

[40] D Ellis, 'Seven Ways to recognize a Phishing Email: Email Phishing Examples', available at https://www.securitymetrics.com/blog/7-ways-recognize-phishing-email, accessed 11 January 2021.
[41] *Ibid.*
[42] *Ibid.*
[43] *Ibid.*
[44] *Ibid.*

on the lookout for high-risk attachment file types include .exe, .scr, and .zip. (When in doubt, contact the company directly using contact information obtained from their actual website.).[45]

g. **Legit company links match legitimate URLs**

When a link claims it will send one to a place, it is needful that the URLs be Double checked. If the link in the text is not identical to the URL displayed as the cursor hovers over the link, it is a sure sign one will be taken to an unsolicited site. If a hyperlink's URL is not correct, or failed to match the context of the email, then it is should not be relied upon. One can ensure additional security by hovering the mouse over embedded links (without clicking!) and ensure the link begins with https://.[46] Phishing emails and text messages often tell a story to trick you into clicking on a link or opening an attachment.

8. Tips on how to Prevent Phishing Attack

This part of the paper shall enumerate the tips on preventing phishing. This is without prejudice to a criminal charge which may be brought against the perpetrator of the act under the Cybercrime Act.

a. **Learn to Identify Suspected Phishing Emails**

New phishing attack methods are being developed all the time, but they share commonalities that can be identified if you know what to look for. There are many sites online that will keep you informed of the latest phishing attacks and their key identifiers. The earlier you find out about the latest attack methods and share them with your users through regular security awareness training, the more likely you are to avoid a potential attack. There are some qualities that identify an attack through an email: They duplicate the image of a real company; Copy the name of a company or an actual employee of the company; Include sites that are visually similar to a real business; Promote gifts, or the loss of an existing account.[47]

b. **Check the Source of Information from Incoming Mail**

Your bank will never ask you to send your passwords or personal information by mail. Never respond to these questions, and if you have the slightest doubt, call your bank directly for clarification.[48]

c. **Never Go to Your Bank's Website by Clicking on Links Included in Emails**

Do not click on hyperlinks or links attached in the email, as it might direct you to a fraudulent website. Type in the URL directly into your browser or use bookmarks / favorites if you want to go faster. If the URL of the website doesn't start with "https" or you cannot see a closed padlock icon next to the URL, do not enter any sensitive information or download files from that site. Site's without security certificates may not be intended for phishing scams, but it's better to be safe than sorry.[49]

d. **Enhance the Security of Your Computer**

Common sense and good judgement is as vital as keeping your computer protected with a good antivirus to block this type of attack. In addition, you should always have the most recent update on your operating system and web browsers. If you've got online accounts, you should get into the habit of regularly rotating your passwords so that you prevent an attacker from gaining unlimited access. Your

[45] *Ibid.*
[46] *Ibid.*
[47] S Panda, 'Ten Tips to Prevent Phishing Attacks', available at https://www.pandasecurity.com/en/mediacenter/security/10-tips-prevent-phishing-attacks/, accessed 15 January 2021.
[48] *Ibid.*
[49] *Ibid.*

accounts may have been compromised without you knowing, so adding that extra layer of protection through password rotation can prevent ongoing attacks and lock out potential attackers.[50]

e. **Have a Data Security Platform to spot signs of an attack**

If you are unfortunate enough to be the victim of a successful phishing attack, then it's important you are able to detect and react in a timely manner. Having a data security platform in place helps take some of the pressure off the IT/Security team by automatically alerting on anomalous user behavior and unwanted changes to files. If an attacker has access to your sensitive information, data security platforms can help to identify the affected account so that you can take actions to prevent further damage.[51]

f. **Have the Slightest Doubt, Do Not Risk It**

The best way to prevent phishing is to consistently reject any email or news that asks you to provide confidential data. Delete these emails and call your bank to clarify any doubts.[52]

g. **Check Back Frequently to Read About the Evolution of Malware**

If you want to keep up to date with the latest malware attacks, recommendations or advice to avoid any danger on the net, etc. You can always read our blog or follow us on Twitter and Facebook. It will also be wise to answer any questions you may have.[53]

9. Conclusion

Phishing is a social engineering technique that is used to bypass technical controls implemented to mitigate security risks in information systems. Phishing is real and dangerous. Everyone needs to watch out for it because it happens to people every day, and getting scammed can be costly. It is a growing crime in the Nigerian society and it is indeed one that we must be aware of. Although laws have been enacted to curb the vice, education of the general populace seems to be the best defence against phishing attacks; after all, prevention is better than cure. This paper has however identified the techniques of phishing and the ways to recognize the scam are presented in the paper. The paper also outlined ways to prevent the scam.

10. Recommendations

This paper hereby recommends thus:

1. The general public should be more suspicious of all electronic communications and websites especially those communications which were not initiated by the person.
2. The general public should also adopt the habit of comparing URLs, spellings etc. For example: if you usually receive your banking alert from ZENITH BANK, be wary of any message which comes from Zenith bank or Zenith Bank or ZENITHBANK.
3. There should be promotion of digital signature especially for transactions relating to the financial institutions
4. Banks should develop softwares which when installed on customers' mobile and computer devices, it will be able to filter messages having phishing indications.
5. The general public should employ common sense before handing over sensitive information.

---

[50] *Ibid.*

[51] A Simister, 'Ten Ways to Prevent Phishing Attacks', available at https://www.lepide.com/blog/10-ways-to-prevent-phishing-attacks/, accessed 15 January 2021.

[52] *Ibid.*

[53] *Ibid.*