International Journal of Computer and Information Technology (ISSN: 2279 – 0764)
Volume 12– Issue 01, March 2023

Evaluation of Phishing Attack Strategies on Mobile Device Users

Adekola A. Ajayi*, Michael Segun Olajide, Oluwagboyega Peter Afolabi, Oladoyin Anthony Abiodun

Department of Computer Science,
Adeyemi College of Education,
Ondo, Nigeria
**Corresponding author's email: ajayiaa [AT] aceondo.edu.ng*

Abstract **-–- Phishing is one of the most common types of hostile internet attacks, which are on the rise on a daily basis. Phishing is a deliberate act that uses deception to trick unsuspecting individuals into disclosing their personal information online. Phishing attacks change in size and shape over time as they all have unique characteristics. Therefore, this paper attempts to evaluate phishing attack strategies on mobile device users by taking into account new techniques such as phishing attacks on videoconferencing services, SMS, voice calls, emails, and social media. The study also carried out a survey with the use of a questionnaire (via google form) to gather data from 122 mobile device users across Nigeria to elicit their awareness and experience, as well as responses to phishing attacks. The aim of this paper is to bring to light, phishing attacks techniques targeted at mobile device users, to sensitize the populace and provide information on how to avoid them.**

Keywords – *Phishing, attacks, mobile devices*

I. INTRODUCTION

The Internet without doubt has been of tremendous help to humanity and has eased the burden of transactions such as shopping, paying bills, transferring funds between different bank accounts and many more, allowing seamless transactions from the comfort of people's homes and any other chosen location.

As most businesses shift sections of their operations onto the Internet, business owners and consumers are necessitated and compelled to take trading of goods and services on the Internet. This has been attributed to the increase in the number of Internet users in the world, which according to statistics as of the start of 2022 is reported to be about 4.95 billion Internet users [10]. Economic activities are now possible without physical contacts and rather through electronic super highway, that is, the Internet. So electronic contacts have replaced the traditional face-to-face (physical) contacts. There are also sufficient software and hardware resources required to facilitate electronic transactions be it financial, industrial, social, economic and political [11].

Internet users with varying levels of needs and availability of infrastructure access the Internet with devices other than the computer, one of which is mobile devices. Presently, with mobile devices having robust functionalities almost equal to that of computers, it has afforded people the privilege of using these mobile devices for many of the same purposes as that of computers. On this note, a lot of people tend to use mobile devices for various online transactions and are therefore not excluded from the enormous security threats associated with the internet. These Internet malicious threats include malware attack, spyware attack, botnet attacks, email bombing and spamming, identity theft, virus and worm attack, adware, key logging, denial-of-service attack (DOS attack), phishing, man-in-the middle attack and so on with phishing being the most common amongst them all [8].

Phishing refers to a premeditated act that is employed as a deceptive tool to lure unwary users into giving out their personal information over the Internet. However, with various countermeasures put in place for phishing attacks by computer and Internet security experts, phishing seems to be on the increasing side every day. In spite of the fact that phishing that targeted webmail and software-as-a-service (SaaS) customers remained the biggest category of phishing, sources claim that the number of phishing sites detected in the first quarter of 2020 increased from the 162,155 seen in the fourth quarter of 2019, as stated in [3]. It is startling to see that 75% of phishing sites nowadays use SSL (Secured Socket Layer) protection as the methods used by phishers to carry out/or execute their phishing attacks [3]. This is done to further conceal their dishonest behavior and deceive unsuspecting victims into thinking they are interacting with a reliable and reputable entity.

This paper examined numerous phishing attack methods for mobile devices and in addition, the profile of the phishing attacks was analyzed based on the responses from mobile device users. The avoidance of phishing attacks on mobile device users was also considered as measures aimed at protecting them from such attacks. Section 2 describes the mobile device attacks while section 3 reviews some existing literatures and methodology of the work considered in section 4. The results obtained from data collected from the responses were appraised in section 5 and the various steps, which mobile device users should observe always was also given prominence. Section 6 concludes the work.

II. MOBILE DEVICE ATTACKS

Mobile devices are generally regarded as a computer small enough to hold and operate in the hand and are thus also called “hand-held devices”. Examples include smartphones, tablets, laptops, cell phones, smart watches and other portable devices. They are often described as electronic communication devices used to facilitate interaction between few persons or several people seamlessly in real-time manner. The devices are veritable tools which enhance Internet communication amongst systems (digital devices) on the global network

Despite the ease of use and beneficial capabilities of mobile devices, using them for sensitive online transactions has made them vulnerable to attackers. The top seven vulnerabilities to mobile devices in 2020, according to Kaspersky mobile security threat reports [9], are data leakage, unprotected Wi-Fi, network spoofing, phishing assaults, spyware, broken encryption, and incorrect session handling.

Data Leakage: Often times, some mobile applications intentionally cause data leakage. When these applications are given broad access rights, both private and business information is transported to remote servers where it may be harvested by cybercriminals for all manners of evil activities.

Unsecured Wi-Fi: Hackers find it easy to make their way through unsecured Wi-Fi networks as confidential and personal information of users on these networks are not safe and are consequently harnessed for malicious purposes or intents.

Network Spoofing: In this instance, attackers frequently establish a phony access point that resembles Wi-Fi networks in public places and assign the access points popular names like "Free Airport Wi-Fi" to entice consumers to connect. Since it is common for many users to use a login combination of username and password for multiple accounts, the attackers use the details of users who connect to their network in accessing other accounts where such details could have been used. This is feasible if attackers demand that users create "an account" in order to access the free Wi-Fi [9].

Phishing: According to a Civil Society Organization (CSO) on cyber security in the United States [5], mobile users are the most susceptible to phishing attacks since they often monitor their emails in real-time, which offers them the opportunity to open and read their emails as soon as they receive them. Attackers use this situation to their advantage by sending email links to users, demanding quick response by users who in turn get directed to fake websites (phishing websites) as they click on the link(s) they received and then fall victim of phishing attacks.

Spyware: Spyware is unwanted software known for infiltrating computing and mobile devices, stealing away sensitive information without the knowledge of the users of these devices. This type of software sniffs personal details for malicious intent.

Broken Cryptography: When app developers apply powerful encryption techniques insecurely or employ weak encryption algorithms, hashed sensitive data from the app thus pose a threat when attackers gain access to the hashed sensitive data [7].

Improper Session Handling: In cases where a person neglects the practice of logging out from a site or when a browser or app improperly handles a session and tokens from such sessions are unintentionally shared, malicious attackers impersonate the legitimate users. In addition, information and details of other users on the website remains unsecured and could be harnessed by the attackers.

In addition to the mobile device attacks earlier explained, other known computing and mobile device attacks include the following: malware, mobile botnets, adware, ad and click fraud, Dead apps and so on.

Mobile Malware: These are malicious software targeted specifically to attack mobile devices; mobile phones in particular. As the number of mobile phone users are increasing, so is mobile malware rapidly becoming a point of concern. Today, attacks on mobile devices are escalating, and no one is safe [5]. Examples of mobile malware are described in the table below

TABLE I. TABLE SHOWING EXAMPLES OF MOBILE MALWARE

Malware	**Devices Affected**	**Date first discovered**	**How it works**
AceDeceiver	iOS	Early 2016	Hides in downloaded apps and steals Apple IDs and passwords
Ghost Push	Android	Late 2015	Gains root access to push advertising or download malicious code
Gooligan	Android	Mid 2016	Ghost Push variant that downloads malicious codes
Hummingbad	Android	Mid 2016	Disguises ad clicks to generate revenue for perpetrator
Pegasus	iOS, Android	August 2016	Masquerades as an app to gain root access and harvest data or do surveillance
Viking Hoard	Android	Mid 2016	Creates a botnet on any rooted or non-rooted device that uses proxied IP address to disguise ad clicks
Xcode Ghost	iOS	Late 2015	Used to develop apps that can be remotely controlled to steal information or direct users to malicious websites

Mobile Botnets: A "bot," commonly referred to as a "web robot," is a sort of malware that allows an attacker to take control of a compromised mobile device, according to [1]. They are a component of the "botnet," a global network of infected machines that is often composed of all victim mobile devices. The first mobile botnet for android devices, known as Viking Horde, was reportedly unveiled around 2016 as stated in [5]. Botnet functions do not need a lot of compute power to be a danger to mobile devices because they do not have the bandwidth and processing throughput of a desktop computer. Due to the frequent use of mobile devices, a large number of potential zombie bots are available to botnet owners around-the-clock scavenging for mobile devices to predate.

III. REVIEW OF EXISTING LITERATURE ON PHISHING ATTACKS

In the mid ’90s, the term phishing was first coined from the instance of hackers that is to mean stealing online accounts and passwords of Americans. Since then, a lot of literature has surfaced from research carried out by various researches on phishing attacks and techniques. According to [16], phishing is a deceitful conduct done to trick consumers online in order to obtain their personal information. Due to a number of factors, including mobile browsers' weaker security capabilities and light weight, phishing attacks are well facilitated on mobile devices [16]. It was also mentioned that since mobile devices have limited screens, it is challenging to identify phishing websites by their appearance or through security indicators. Thus, screen characteristics is not a serious indicator for phishing websites.

According to [4], phishing is one of the more well-known social engineering attacks that aims to take advantage of flaws in system operations brought on by users' behavior, particularly in situations where a gullible user jeopardizes the security of a system by disclosing his or her password to a fake website reached. Another type of computer attack known as "phishing" targets people by sending them socially engineered communications over electronic communication channels and convincing them to take specific activities that will benefit the attacker [14].

In addition, the idea of phishing was simply defined as a form of online fraud that tries to steal users' credentials from swindling websites by using an attacker's email, website, and URL to directly steal users' usernames, passwords, and credit card information [12]. According to [2], phishing attacks may take the form of direct attacks in which the sender or perpetrator is a harmful application that sends the user (victim) to a spoof version of the target application rather than the actual one. A phishing attempt could alternatively take the form of a "man-in-the-middle attack," in which the sender or attacker is good, but a third party intercepts the link and loads a faked target application instead of the original target application.

Another definition of phishing attack in [8] describes it as a fraudulent action when the attacker appears to be an authorized person or organization in order to obtain sensitive information like usernames, passwords, credit card numbers, and so on. Usually, the individual who is being attacked will get a message or email that either installs malware on their computer or directs them to a harmful website where they are easily attacked.

IV. PHISHING TECHNIQUES

Phishing attacks which is one of the most prominent Internet attack takes several form in its usage by attackers. The end goal of all phishing techniques is to rip off confidential information of online users and consequently extort unsuspecting victims of valuable assets and resources

A. Videoconference Service Phishing Attack

In the year 2020, phishing attacks against videoconference service became conspicuous as a result of the COVID-19 pandemic which necessitated a lot of cloud meetings. According to phishing activity trends report for 1st quarter of 2020, there were reports of 1,054 attacks against zoom (a videoconference service brand) in April. Some of the attacks highlighted in the report involved phishing, in which the perpetrators sent phony meeting notifications for zoom videoconferencing through email [3]. Victims of such mails were directed to webpages that had been set up by the phishers, primarily with the purpose of stealing zoom account usernames and passwords from ignorant users. This afforded phishers the opportunity to use these credentials as login details to corporate videoconferencing accounts. The harvested passwords can as well be used by phishers on other sites and services.

B. SMiShing

It was noted in [15] that the word "SMiShing" originated from the text messaging protocol SMS (Short Messaging Service). This type of phishing involves a text message or phone number. It is particularly frightening in the sense that people sometimes have a high tendency to trust on text message’s genuineness than an email, though this could be less true. They feel that they are safe from the security risks involved with clicking on links that appear in emails. Similar to phishing, smishing involves sending a victim a text message asking for their banking information or prize claim information instead of an email [13]. Smishing takes two forms; one involves a text message received by a victim whereby such message appears to have originated from a trusted and known source, such as from a system administrator or a bank official. In the second, the victim receives a very significant text message informing them that their identity has been compromised or stolen. The victim is then instructed to visit a fraudulent website or contact a phone number to confirm the allegedly compromised account or identity, as applicable. Upon receiving the divulged information, the smisher proceeds immediately to the stage of using the victim’s information for fraudulent activities or withdrawing money from the victim’s account and possibly open a new credit card in the name of the victim.

C. Email Phishing

This form of phishing is one of the earliest forms of phishing recorded. It involves sending of a malicious and fraudulent email message to the victim by a phisher who appears or poses to be a person or company that is known to the victim. Typically, a phishing email will include at least one link to a false website that have been designed to have the appearance of a legitimate website. Phishers mostly use the technique of making the message look enticing to the recipient who in turn falls victim of providing sensitive information that can be used by phishers for either online financial theft or identity theft.

D. Vishing – Voice Call Phishing

Vishing is the practice of using voice over Internet Protocol (VoIP)-based voice messaging services to manipulate the intended victim into divulging personal, financial, or other sensitive information in exchange for financial gain [15]. "Vishing" has the potential to be a very effective attack vector since it combines the ease of Voice over Internet Protocol (VoIP) with email phishing methods. Victims of vishing are at risk of financial fraud and/or identity theft [6]. Vishing as a phishing method takes advantage of society's trust in telephone service because most targets are typically unaware that con artists may employ caller ID spoofing and sophisticated automated systems to perpetrate this type of scam. In some cases, scammers obtain user details (majorly name, phone number and any other details available) on any social media platform or even business or organizational websites where such information is available. In a situation when a scammer puts a call through to the target using the user details obtained, the unwary target falls victim to the scam, except in some cases where the target is extra careful and asks the caller some questions to verify the genuineness of the call before any sensitive information is provided or before any further action is taken, which could be required of the target by the scammer.

V. METHODOLOGY

In this section, we describe the research methods and approaches used in the study to investigate phishing attacks on end-users. Specifically, it involves the investigation into the various forms of phishing attacks. The samples cut across friends, colleagues and family at different locations in Nigeria. The operating system of the mobile devices for the selected samples include the common ones, which are Andriod, iOS and Windows. The data gathering technique used was questionnaire, in which google form was used as a tool in this regards.

About 122 end-users responded to survey questions posed in the questionnaire. The introduction section of the google form had a brief description of what phishing is, to enable the responders understand the term “phishing” as the term itself may be new to some people, though they may be familiar to the meaning. Thereafter, an in-depth and extensive literature review was done on the reliable sources such as journals, documents and online databases for issues relating to phishing, the research questions were thoroughly refined to reflect our objectives clearly.

VI. FINDINGS AND DISCUSSION

This section presents a systemic results of the study. The organization of the texts and figures are done in such a manner that makes it easy to interpret the findings. The data gathered from the survey were processed and analyzed to create a unified dataset which consists of 69 males and 53 females.

A. User's Level of Proficiency on the Use of Internet-related Facilities

Here, the assessment is aimed at ascertaining the level of proficiency of mobile users on how to use the Internet, web browsers, filling of forms online and responding to online-related activities. The result is shown in Fig. 1 below

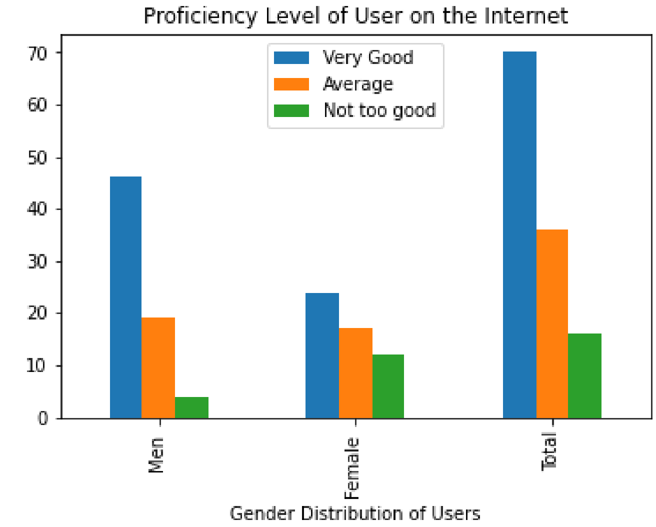

Figure 1. Internet activities proficiency

The level of individual proficiency on Internet usage could form a good determinant to avert any form of phishing attacks. On this premise, the result in Fig. 1 shows that men in larger proportion are more proficient than their female counterparts which leaves the latter at a higher level of susceptibility to operational phishing attacks.

B. Phishing Attack per Technique

Pertaining to the techniques on which attacks were carried out, Fig. 2 shows that attackers used more of email and text message to reach out to their targets. So a total of six platforms are considered for our study.

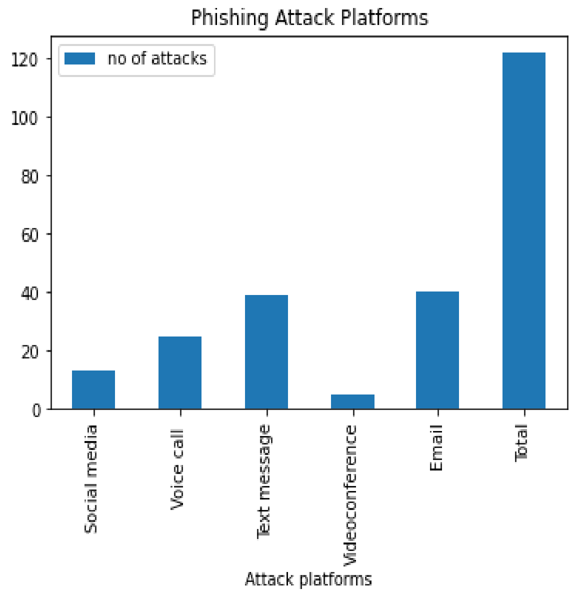

Figure 2. Phishing attacks per technique

C. User's Response to Fraudulent and Phishing Attacks

From the survey, most mobile device users with a high level of proficiency on the use of Internet-related facilities are already aware of phishing techniques and as such pay rapt attention to messages and information from a perceived unknown source. Due to this level of awareness, the question "do you respond to messages from unknown or suspicious sources?" showed more people refusing to respond to such messages and Fig. 3 presents this information

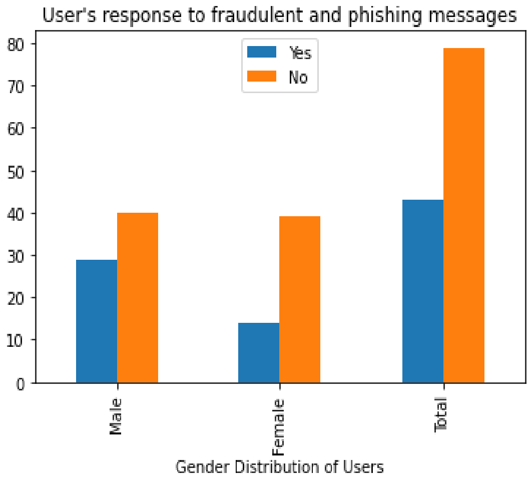

Figure 3. Response to Phishing Attacks

D. Information Search on Perceived Threat

So as not to fall victim of phishing attacks, Fig. 4 shows the percentage of users who felt that it was necessary to run a cross check and verify the information received before providing sensitive information. However, with the Internet as a viable tool, yet only a few number of the responders carefully searched online to know the genuineness of the sender of messages received.

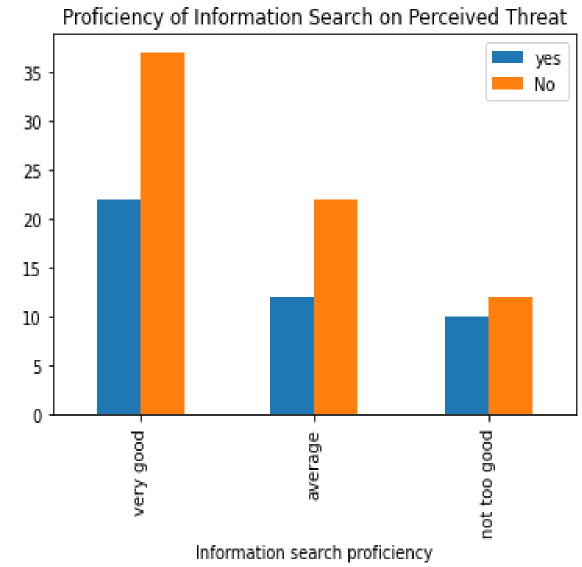

Figure 4. Information Search on perceived threats

E. Suspicion Level

Fig. 5 considers the level of suspicion by the targets of phishing attacks. The urgency of response demanded by the attackers for their targets to provide the needed information often raise a lot of suspicion for those who are sensitive to the divulging of personal information.

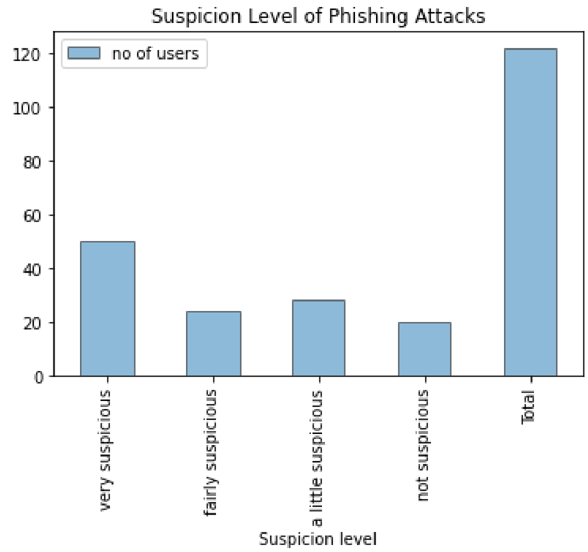

Figure 5: Suspicion level of users on phishing attacks

F. Avoidance of Phishing Attacks

From available results on phishing attacks, it is paramount for mobile device users to be conscious of the avoidance of such attacks while using their devices. Naïve and old users of mobile devices consciously or unconsciously had fallen victim of scammers at different times as a result of their ignorance on their nefarious activities. However, certain measures can be put in place to avert the susceptibility of mobile users to the interlopers and these includes

- Sensitization of phishing attacks on mobile devices using short, crisp and captivating messages for mobile device users.
- Mobile device users generally should be mindful of their interactions for unsolicited messages traced to URLs and other options in form of baits.
- Mobile device users should refrain from disclosing their personal security information to an unknown site.
- Software (anti-phishing) which are designed to avert phishing attacks should be installed on mobile devices as a means of protection from attacks.
- Periodic review of personal data particularly the passwords of mobile device users for more protection.
- Updating of browsers should be encouraged amongst mobile device users.

VII. CONCLUSION

This section concludes with the summary of findings, limitations of the study and direction for further research work.

The focal point and main thrust of this study was to investigate the phishing attacks and techniques that are particular or peculiar to mobile users as well as the level of attacks on victims. In general, it was perceived that men have more technical know-how on Internet-related activities and therefore, have a good level of awareness of tricks and techniques used by attackers to carry out phishing attack. It was also obtained that email and text message were the major tools or platforms used by these attackers to perpetrate their evil deeds. Also examined is the behavior and response of users to messages from unknown sources, especially ones that requires urgency or looks suspicious. However, users who are not oblivious of phishing attacks and techniques often neglect messages from unknown or suspicious sources. It was established that most users find messages from unknown sources suspicious and would not respond to such messages nor divulge sensitive information. Although, an empirical approach was used to deduce the findings of this study, we were however not able to get lots of sample which would have been used to generalize the findings. To this end, further studies would be appreciated to further establish any links between the vulnerability of mobile users and phishing attacks. Further studies on the new trends of phishing attacks targeted at mobile users can also be carried out for emergence of new discoveries.

REFERENCES

[1] Amro, B. (2017). Malware Detection Techniques for Mobile Devices. *International Journal of Mobile Network Communication & Telematics*, 7(4) 28 – 34

[2] Amro, B. (2018). Phishing techniques in mobile devices. *Journal of Computer and Communications*, 2018(6), 27-35

[3] APWG (2020). Phishing Activity trends Report 1st Quarter 2020 https://docs.apwg.org/reports/apwg_trends_report_q1_2020.pdf?_gl=1*1mx8oug*_ga*MTI1NTE5MTA5Ny4xNjU3MjY4NTE3*_ga_55RF0RHXSR*MTY1NzI2ODUxNi4xLjAuMTY1NzI2ODUxNi4w&_ga=2.204149143.605371871.1657268519-1255191097.1657268517 Retrieved 22 July 2020

[4] Bottazzi, G., Casalicchio, E., Cingolani, D., Marturana, F., & Piu, M. (2015, October). MP-shield: A framework for phishing detection in mobile devices. In *2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing* (pp. 1977-1983). IEEE.

[5] CSO (2020). Five New Threats to Your Mobile Security. From https://www.csoonline.com/article/2157785/five-new-threats-to-your-mobile-security.html. Retrieved 26 July 2020

[6] Griffin, S. E., & Rackley, C. C. (2008, September). Vishing. In *Proceedings of the 5th annual conference on Information security curriculum development* (pp. 33-35).

[7] Srinivas, (2014). Broken cryptography. From https://resources.infosecinstitute.com/android-hacking-security-part-16-broken-cryptography/ Retrieved 26 October 2022.

[8] Joshi, R. (2015). "Interactive Phishing Filter". Unpublished Master's Projects. 430. From https://scholarworks.sjsu.edu/etd_projects/430 Retrieved 22 July 2020

[9] Kaspersky (2020) Top 7 Mobile Security Threats. From https://www.kaspersky.com/resource-center/threats/top-seven-mobile-security-threats-smart-phones-tablets-and-mobile-internet-devices-what-the-future-has-in-store Retrieved 23 July 2020

[10] Kemp, S. (2022). Digital 2022: Global Overview Report. From https://datareportal.com/reports/digital-2022-global-overview-report#:~:text=Global%20internet%20users%3A%20Global%20internet,of%20the%20world's%20total%20population . Retrieved 26 October 2022

[11] Lawrence, J. E., & Tar, U. A. (2010). Barriers to e-commerce in developing countries. *Information, society and justice journal*, *3*(1), 23-35.

[12] Odeh, A., Keshta, I., & Abdelfattah, E. (2020). Efficient detection of phishing websites using multilayer perceptron. *International Journal of Interactive Mobile Technologies*, 14(11), 22-31

[13] Shahriar, H., Klintic, T., & Clincy, V. (2015). Mobile phishing attacks and mitigation techniques. *Journal of Information Security*, *6*(03), 206 – 212.

[14] Whittaker, C., Ryner, B., & Nazif, M. (2010). Large-scale automatic classification of phishing pages. Available at https://storage.googleapis.com/pub-tools-public-publication-data/pdf/35580.pdf

[15] Yeboah-Boateng, E. O., & Amanor, P. M. (2014). Phishing, SMiShing & Vishing: an assessment of threats against mobile devices. *Journal of Emerging Trends in Computing and Information Sciences*, *5*(4), 297-307.

[16] Yousif, H., Al-saedi, K. H., & Al-Hassani, M. D. (2019). Mobile Phishing Websites Detection and Prevention Using Data Mining Techniques. *International Journal of Interactive Mobile Technologies*, *13*(10), 205 – 213.