Toward Eradication of Phishing Attacks in E-government Systems

Musa Midila Ahmed

***Abstract*—E-government has revolutionized social and economic activities of societies making human life easier. However, despite the numerous benefits of E-government system, the main challenge that accompanied the adoption of this novel innovation is phishing attack, a subset of social engineering attack (SEA). Phishing attackers psychologically manipulate citizens to disclose confidential information. The purpose of this study is to propose solution for eradication of phishing attacks in E-government system. To analyse business activities on the E-government system; information, communication, distribution and transaction (ICDT) model was used to systematically acquire sound knowledge and understanding of internet business activities. This study identified seven types of phishing attacks; standard email phishing, spear phishing, clone phishing, whaling, voice phishing, text-message phishing and angler phishing. in addition, gainful employment of citizens, legislative enactment for punishing phishing scammers as well as enforcement of the law to compel compliance with the law are among the recommendations for eradication of phishing attacks in E-government systems. The author abridged security awareness education, accurate citizens' authentication, phishing filter, MALWARE detection and prevention. Others are artificial intelligence, machine learning and deep learning methods of anti-phishing attacks in E-government systems. Recommendations for eradication of phishing attacks in E-government system include compliance with the suggested anti-phishing attacks.**

Keywords— Eradication Phishing Attack, Anti-Phishing Attack. E-government, Social Engineering Attack,

I. Introduction

The increase in the popularity of information and communication technologies (ICTs) and the internet services nowadays has revolutionized public service provision generally. ICTs greatly impacted on the social and economic activities of societies making all aspect of human life easier, efficient and transparent. Consequently, E-government is define as the use of ICT facilities for enhancing the efficiency, effectiveness, transparency and citizens' participation in governance. Alshaher [1] identified ICT's capabilities among the factors responsible for providing decision-makers with novel ways for the success of E-government systems. E-government system modernized public service delivery by providing digital services among government agencies and between government and citizens. According to Burlacu, et al. [2], E-government serves as a tool for integrating electronic services and systems among government and government organizations (G2G), government and citizens (G2C) as well as government and business (G2B) in a convenient, efficient and transparent manner. Therefore, E-government system improves efficiency of governance processes and procedures by promoting the effectiveness of interactions between governmental organizations and businesses with citizens. This ultimately leads to enhanced quality of public services and decision-making in governance.

Despite the numerous benefits of E-government system towards good governance, this innovation increases cybersecurity threats. One of the most popular and challenging category of threats is the social engineering attack (SEA). Social engineering is a psychological manipulation of human interactions to deceive citizens disclose sensitive information. The main challenge faced with SEA is that it exploits human error, irrespective of the tight technical security formation in software and operating system. Ahmed [3] identified Baiting, Pretexting, Quid Pro Quo, Honey Trap, Tail Gating, Pharming and Phishing as the most popular type of social engineering attackers uses to exploit E-government systems. Baiting attackers entice victims with gift or valuable promise to exploit victims' curiosity and greed for spreading malware. Whereas, Honey trap attackers impersonate attractive person to entice victim with romantic or sexual advances to get secret information. Pretexting attackers impersonate an authorised user to deceive citizens' to release confidential information. Quid Pro Quo hackers sought for critical information such as bank details or login credentials by pretending to be technical service provider. While Tail gating hackers closely follows an authorised users to gain access to restricted information. Pharming hackers automatically redirects users to fake websites that looks like the legitimate sites. However, according to Salahdine and Kaabouch [4], the most common SEA is the Phishing attack. Phishing attackers fraudulently mislead citizens to acquire private and confidential information through phone calls, SMS, or E-mail.

Phishing attack is a type of social engineering by sending

fraudulent communication to victims claiming it is from reliable source. Phishing attackers trick victims by sending fake messages to get credit card information or account details that can facilitate access to online accounts. Phishing attacks has a devastating effect on E-government network by bypassing the security controls to gain access to secured data, steal public fund or identity theft. Consequently, this attacks leads to huge financial losses, declined E-government systems' reputation and loss of citizens' thrust in E-government systems. Therefore, adequate measures to protect E-government system users from subtle mistake of exposing confidential information. Although, according to Rathee and Mann [5], technological means such as machine learning and deep learning can mitigate Phishing attack. Such approach proves to be unreliable. The best approach according to Ahmed [4] is citizens' ability to detect fraudulent communications appropriately. A study by Abroshan, et al. [6] shows that human factors such as education-level, fear, anxiety and risk-taking have increase phishing attack attempts after COVID-19 pandemic. These human factors are also responsible for the success of phishing attack in the pre-COVID-19 pandemic. Therefore, studies toward understand the different types of phishing attacks, ways of identifying potential phishing attack as well as propose solution to halt the success of phishing attacks in E-government system.

The remaining part of the paper is organise as follow; section, section 2 is for related work. Sector 3 present the objective of the study, Section 4 provide research methodology and section 5 report the results and discussion of the study. Finally, section 6 conclude the paper.

II. Related Works

Phishing attack is one of most popular, tricky and challenging category of SEA. The challenge in tackling this cyberattack is the increasing sophisticated approaches and techniques fraudsters' uses to disguise for assessing secret information from users or redirect users open malicious sites. Aljeaid, et al. [7] evaluated the level of Saudi Arabians knowledge and awareness by simulating phishing attacks. The results shows that about 77% of the samples fall victims of phishing attacks. Therefore, it is crucial to enhance the level of knowledge and awareness of citizens' on security risks and the consequences of privacy violation. Similarly approach on undergraduate population by Rahim and Azman [8] shows that demographic factors such as age and gender has no effect on the susceptibility of victim to phishing attacks. Similar quantitative research by Alguliyev, et al. [9] evaluated the role of social media on the security of E-government system. The outcome shows that confidentiality of messages is the greatest threat on social network in E-government systems.

Basit, et al. [11] conducted machine learning phishing attack detection by three machine language classifiers. The result shows that assembled RFC detects phishing attacks with about 97% accuracy. A similar machine learning experiment by Ravi [15] to improve phishing attack detection accuracy using deep machine learning (DML) CANTINA approach. The DML information retrieval algorithm proved to enhance phishing attack detection accuracy. An automated filtering experiment conducted by Rahim, et al. [14] proposed phishing attack identification technique by analysis of Emails and content of web services. The anti-phishing method gains about 98% malicious E-mails and web services detection accuracy. Similarly, Rastenis, et al. [10] proposed six phases E-mail based phishing taxonomy. The taxonomy enhances the description of Phishing attacks. Odeh, et al. [13] proposed a new feature selection model based on machine learning. According to the author, the strength of both deep learning and supervised machine learning detection approach depends on features selection and classification algorithm used.

Nemane and Pahurkar [18] defined phishing as an online identity to steal confidential information such as login credentials and credit card information of system users. The author classified phishing into six (6) categories; deceptive, malware, Trojan, system configuration, man-in-middle and search engine phishing. The author proposed a two (2) phases; login and registration phishing detection and prevention method that uses visual cryptography. Whereas, Chen [19] identified strong allure, chaotic information, clear goal, urgency and automated change of attack source as some phishing attacks' characteristics. The author discovered some technical means of mobile phone phishing including disguised websites sending short message service (SMS) and email from fake sites as well as exploiting vulnerability in mobile phone systems. In this study, timely installation and update of software on mobile phone, use of anti-spam technologies as well as disclosure of sensitive information on social media platforms as some of the anti-mobile phishing techniques.

III. Objectives

The objective of this study are;

i) To identify the types of phishing attacks in E-government systems.

ii) To identify anti-phishing attacks in E-government system.

iii) To propose solution for eradication of phishing attacks in E-government system

IV. METHODOLOGY

To adequately leverage on new opportunities and challenges to expand activities on the internet, there is the need for analysing online business strategies in E-government system. Moreover, evidence-based decisions on detection and prevention of phishing attack requires sound knowledge and understanding of technological development on internet business activities on the E-government system. In order to leverage on the vitality of the internet, Angehrn [20] of INSEAN developed the ICDT model.

A. Information, Communication, Distribution and Transaction (ICDT) Model

The ICDT model analyzed and classified activities in the virtual establishments into four segments in a systematic manner, the model's segment internet technology business

into information, communication, distribution and transaction (ICDT) virtual spaces. These virtual spaces represents strategies on which citizens can engage themselves in the E-government systems. To resolve security issues in the E-government space, careful analysis and classification of online channels can alleviate the possibility of Phishing attacks in the system. Each of these virtual spaces will be examined in relation to the legitimate business strategies in order to provide direction for eradication of Phishing attacks.

i) Information in E-government System

E-government is the use of information and communication technology (ICT) to promote the effectiveness, efficiency and transparency of governance. E-government system enables integration of different operational databases of government organizations and segments into a data warehouse. A data warehouse allows citizens get access to data at a central repository by queries to retrieve information for business analysis and decision making purposes. Furthermore, E-government integration merges information systems to ease governance processes by facilitating exchange of information and services among citizens, businesses and other agencies of government. This enables citizens participate transparently in governance by making significant contribution to E-government service delivery. However, one of the major challenge in E-government system nowadays is the phishing attack, a type of software engineering attack where attackers fraudulently steal confidential information. Phishing attackers can targets citizens from any sectors of E-government system. Phishing attackers can defraud numerous categories of citizens such as the chief executives of government and non-governmental organization, social network users or online banking customers. Therefore, effort toward eradication of this attack on the information system is crucial, timely and decisive.

ii) Communication in E-government System

Communication is an exchange of information from sender and the receiver transmitted through a medium. Modern technological development in telecommunication and internet such as social media, websites and other internet-based applications greatly simplifies communication nowadays. However, secured communication requires successful and accurate transmission of messages across all intermediaries from sender to the receiver. Therefore, communication has three parts; the sender, the receiver and the message transmitted through a medium. An effective communication should ensure that the message is formed appropriately, transmitted through a secured channel and the legitimate receiver correctly decodes the message. A secured communication should prevent hackers' attempts to access the transmitted data by pretending as authorized users. Although, advances in technology increasingly renders information systems protections obsolete and ineffective this days. Identity of the communicating parties must be authenticated by both sender and receiver. In addition, there should be mechanism to protect the integrity of messages exchange between sender and receiver transmitted across the medium.

iii) Distribution in E-government System

Precisely, information in E-government system is an integrated set of data in a form of messages that describes goods and services provided by public or private organization. Whereas, communication is the exchange messages between producers and consumers of goods and services in the E-government ecosystem. Distribution in E-government is the process of making goods and services available to the consumers. Basically, distribution is concerned with ensuring that goods and services reach target users in a secure and efficient manner. Distribution can be effected in either direct or indirect channels. The direct distribution channel does not have intermediaries. It means the producer of goods and services sells directly to the end user. The indirect distribution in the other hand has one or more intermediaries in order to transmit goods and services from its producers to the end users. For instance, one-level distribution channels transmits the goods and services from the producer to the consumers through the retailers. Similarly, two-level distribution channel transmit the goods and services through wholesalers and retailers to the end users. Knowledge and understanding of these distribution channels is important to easily detect any potential fraud in the process of transaction for supplying goods and services in E-government system.

iv) Transaction in E-government System

Transaction is an agreement between two parties especially s seller and a buyer to exchange goods, services or assets for funds. Transaction is a critical aspect of E-government system to build a steady revenue generation for public and private organizations. Therefore, accurate recording of transaction is a vital of E-government system for accountability and transparency in governance. There are two basic categories of transaction; cash method of transaction and accrual of transaction. In cash method of transaction, revenue is recognized only when cash is received by the organization. Whereas, accrual method of transaction recognizes revenue when they are earned, even if payment is deferred to future date. To reduce the fear of trust violation in pay-in-advance nature of online transaction design, customers may choice pay-on-delivery transaction, where customers pay only when goods or services are received as specified in the trade agreement. Nowadays, fraudsters exploits online transactions in e-commerce as well as digital financial services targeting e-payments and other confidential information. The popularity of digital channels of transaction has now created a new opportunity for phishing attack fraudsters. Therefore, identity of transacting parties need to be authenticated in order to eradicate fraud.

V. RESULTS AND DISCUSSIONS

A Types of Phishing Attacks in E-Government System

E-government system is a novel public service provision platform that promote efficiency and transparency in governance. However, despite the increase in migration to E-government system globally. Phishing attack, a type of social engineering is one of the information security challenge that proved to be difficult to eradicate. The

difficulty lie on human weaknesses, whereby attackers leverage on people's trust and lack of awareness to overriding the technical security mechanisms of the system. The best ways to avoid phishing attack is the knowledge of common techniques that scammer use to exploit their victims.

i) Standard Email Phishing

This is arguably the most popular type of phishing attack, whereby the attacker simply send emails to many people that appears to have a link with a trusted business organization. In this category of phishing attack, the attacker send emails to thousands of people with possibility that some unsuspecting recipient will respond to the attackers' demand. The demand usually are confidential information of the target victim, such as login credentials, PIN, financial credentials, bank card details, etc. Modern application and site has features for free email communication services. Consequently, email phishing is the cheapest and most common phishing attack. The attacker simply gather list of people's email and send messages with a probability that some recipient will respond to the mail in the scammers, advantage.

ii) Spear Phishing

This is a category of phishing attack that target specific individuals, business or organizations. The attacker uses email, or instant messages platforms to deceive people release confidential information or perform actions that leads to data loss, financial loss or destabilise the network. While phishing attack generally targets anyone in the population, spear phishing attacks targets particular people in a business or organization to get access to the business or organization itself. Spear phishing targets high profile system users such as an executive, network administrator accountant, and the like. This category of targets gives the attacker high privilege access with the ability to manipulate the network in an elevated authority.

iii) Clone Phishing

As business organizations intensifies training and awareness for public enlightenment on information security in general and phishing attack in particular. Attackers develops more sophisticated means of stealing people's credentials. Clone phishing attacks is a new category of email phishing attack, where attackers make identical copy of a real email message with attachment to resend it later as the trusted sender after replacement of the attachment with malware. In a nutshell, the attacker switches the legitimate attachment with a malicious email attachment to install malware on targets' machine. Sometimes, a successful compromise of a single target leads to taking-over the entire organizations' network.

iv) Whaling

Whaling is a category of spear phishing attack where the attacker targets high value individuals such as CEO, public figure, or senior employees to get sensitive information or funds. Both whaling and spear phishing know about the target's identity. However, personalized knowledge of target in whaling makes it more convincing, as such fool the victim believing the attacker is a legitimate entity. The goal of whaling attacker ranges from tricking a high-ranking individuals disclose sensitive or corporate information to manipulating the victim into authorizing huge-value electronic transfer to the scammer.

v) Voice Phishing

This kind of phishing attack is performed over phone call or voice message send by the attacker as it is from a legitimate organization to trick victims into releasing sensitive information, bank details or smart card details to the scammer. The scammer normally use threats and persuasive language to make victims feel that the response required is necessary and urgent. In a nutshell, vishing is a verbal scam that trick victims release sensitive details to the attacker.

vi) Text-Message Phishing

This is a category of phishing attack whereby the attacker uses short message services (SMS) and other chat-based message to commit fraud or other cybercrimes. Typically, scammers use text messages purported to be from a legitimate organization such as bank requesting for personal or financial information to steal money. Obviously, disclosing some of these information is the same with handing the key of your bank account to thieves. Text messages are naturally a private communication channel, which lowers victims' scepticism. Furthermore, attackers override targets' critical thinking capacity by the need of urgency for the recipient to take action.

vii) Angler Phishing

This is one of the latest phishing attack technique, whereby the target is tricked to disclose confidential information, financial details or other sensitive details through social media accounts of victims. In this type of phishing attack, scammer masquerade as a customer support staff on the social media platforms. The goal is to divulge aggrieved customers to disclose their confidential details. The attacker creates a hoax social media accounts of large organization, especially financial institutions. Dissatisfied customers are tricked to contact the fake social media handles to complete specific tasks, which redirect victims to malicious site under the attackers' control.

B. Anti-Phishing Attacks in E-Government System

i) Security Awareness Education

Security awareness education (SAE) is obtained by formal training for citizens, employees and other E-government systems' business partners on protection of organizations' resource from threats and other forms of violations. This is an essential measures to enable citizens recognise potential security problems and take preventive actions. In view of the dynamic nature of phishing attack techniques used by cybercriminals to deceive people, training should be done regularly and focused on contemporary measures for the protection of E-government systems, its citizens and its

workforce. The SAE should be dedicated to increasing nation-wide education on the importance of data confidentiality for the corporate security of the entire E-government system. Also, citizens need to be educated on how to keep confidential information and physical assets secure for successful protection of the entire E-government system.

ii) Accurate Authentication of Identities

Citizens' identification refers to the means of proving that a person is an indigene of a particular country, state or community. It serves as a trusted means of protecting unauthorized access to E-government systems' resources. Accurate authentication of identities lay solid foundation for establishing trust and privacy of citizens' data as well as security of material resources in E-government system. Citizen identification can be for general purpose with a broad coverage especially citizens' identity at a global scale. It can also be for a specific purpose, for instance, to identify citizens that are eligible to vote, drive or get access to the system. Authentication is the process of verifying citizens' identity. Acceptance of identification depends on the level of restriction and security requirement of the system. Authentication is implemented to accept one factor, two factors or multiple factors as in Single Factor Authentication (SFA), Two Factor Authentication (2FA) or Multi-Factor Authentication (MFA) respectively depending on the security level of the system. A highly secured implementation may impose MFA to get access to the system. However, a less secured implementation may require SFA for accessing the system. Consequently, MFA authentication is recommended for E-government system to prevent phishing attack, since citizen may detect the unnecessity and ill motives for the too much demands to withhold response.

iii) Phishing Filter

Phishing filter is a software features that offers protection from phishing activities. There are many phishing filters plugins available for websites and applications. However, most phishing filters are implemented, set up and activated in the same manner. Particularly, Domain-Name-Server (DNS) based content filters prevent users' access to the scammers controlled websites. Whereas, Domain-Based Message Authentication, Reporting and Conformance (DMARC) uses the combination of digital signature with public key cryptography and DNS verification at the recipient end to accept only valid email send by legitimate sender. These domain binding techniques link sensitive information to a particular domain for easy identification and evaluation blacklisted phishing attacks by the recipients. Phishing attacks are highly dynamic and increases in complexity. Therefore, one of the most effective way to protect against phishing attacks is by a modern and robust phishing filter security solution. Nowadays, phishing attack is a powerful and continue to be the most common cyberattacks criminals use to steal data and demand ransom extortion.

iv) MALWARE Detection and Prevention

Malicious software (Malware) is a software system designed to distort or monitor the normal operation of computer system. Malware is a broad name for numerous computer systems' infection methods. It refers to all types of malicious software including Ransomware, Worms, Trojans, Spyware, Adware, Botnets, Backdoors and Rootkits. Precisely, Ransomware uses malicious software to seize critical information, data or files for ransom. While, Worms are self-duplicating viruses that automatically spread among computer systems and networks. Also, Trojans disguise as legitimate software to carry-out criminal actions. Whereas, Spyware includes adware, Botnets and Backdoor are malware that collects information about the victim for the attacker. Lastly, Rootkits hide in the operating system to get root-level privileges access to the computer. Ultimately, the main goal of phishing attack is either to take control of the victims machine, send a spam to unsuspecting target or spying to steal sensitive data. Indeed, naïve computer system users cannot distinguish genuine application from malicious software. Therefore, computer systems and mobile applications should include plugins to detect malware using novel procedures in artificial intelligence, machine learning and deep learning algorithms.

v) Artificial Intelligence Methods

Artificial Intelligence (AI) is the ability of computer system perform tasks just like an intelligent human being. It is used to develop intelligent system with characteristics of human being such as reasoning, generalization or evaluate past experience to predict future occurrence. Simply put, AI simulates human intelligence processes with the ability to solve arbitrary problems. Application of AI is broad found in almost all business sector and other human real life endeavours. Nowadays, social engineers use AI as a tool to exploit human psychology and gain access to data and systems. With AI tools, hackers creates automated social engineering attacks (SEA) on social media accounts and public systems. These emerging technologies are also design to manipulate peoples' intelligence aiming at downplaying emotions and prompt actions. However, AI-based SEA use machine to enhance efficiency. Therefore, all the suggestions for eradication of Non-AI SEA is also applicable to AI based SEA.

AI-based SEAs require the same AI eradication technique. Manya [21] identified voice spoofing, deep fakes and automated bots as some of the impact of AI on SEA. First, AI offers automated voice cloning tools that rapidly clone voice sample. Attacker leverage on the fact that human brain does not significantly differentiate between real and artificial sound. These AI tool requires a sample of voice to create an artificial voice that sound like a specific person's speech style and tone. Second, deep fake manipulate image or video by AI to spread false information so that people will believe it is true. Finally, an automated AI-based SE bots is a program that performs specific task and interaction with no human intervention. Manyan [21] proposed safety precaution to the AI-based SEAs. The author suggested that careful observation for abnormalities such as unusual blinks,

facial, skin and hair on the deep fake software. Voice liveness detection software can be embedded to detect clone voice from the real human voice. In addition, if voice clone is a caller, ask challenging and diverse questions to determine the ideal posture, adequacy and tone of response to detect cloned voice. Generally, avoid responding to unknown or automated callers. Never release personal information such as username, password, PIN, or any identity information to unknown or automated callers. Scammers normally coerce victims by need for urgency in releasing information. Therefore, hang-up or suspend the conversation until after confirmation with the authentic source through legitimate means.

vi) Machine Learning Methods

Machine Learning (ML) is a subset of AI that focuses on statistical predictive techniques for building intelligent computer system.AI algorithm broadly refers to the capability of computer system simulates human cognitive function including learning and problem solving. Whereas ML algorithms takes historic data as input to accurately predict outcome that was not specifically programmed to do. ML has become an important computer systems' tool, particularly in social engineering fraud detection, spam filtering and Malware detection. ML are categorized into supervised learning, unsupervised learning and reinforcement learning. Supervised ML generally classifies dataset for making prediction of outcome. Unsupervised ML is generally to understand the relationships between datasets. Whereas reinforcement ML is the science of decision-making for optimal behaviour to get maximum rewards from dataset.

Advancement in ML technology nowadays leads to the creation of automated tools for gathering public information on people for phishing. Deshpande, et al. [22] discovered by using ML technology that phishing attack is the most popular SEA used to hack emails. ML tools are used to forge voice, or video of people done at large scale and automatically. The automated nature of this fraud is the most disturbing aspect of ML enhanced SEA. However, ML is identified as a feasible SEA detection techniques. The potential of ML for detecting SEA was explored by many researchers (Wang, et al. [23]; Basit, et al. [11]; Peng, et al. [24]; Alam, et al. [25]; & Garves, et al. [26]). Wang, et al. [23] proposed an ML techniques for detecting SEA in general. The author discovered that ML is an effective techniques for SEA detection. Furthermore, Ripa, et al. [27] used ML for detection of URL, Email and websites phishing attacks. Similarly, Hossain, et al. [28] used ML-based method for phishing website detection by features extraction and analysis to discover that application of basic ML algorithm improves defence against phishing attacks.

vii) Deep Learning Methods

Deep learning is a subset of machine learning method that comprised of multiple layers in the network to progressively extract high-level features from the raw input data. At each level, the system learn to transform the input data into a composite representation. Nowadays, attackers use creative means of exploiting human weaknesses to penetrate secured systems. However, Saha, et al. [29] presented deep learning approach of identifying phishing websites. Both the multilayer and feed-forward neural network architecture was used to detect phishing webpages. A similar approach by Yao, et al. [17] used improved convolutional neural network (CNN) deep learning to identify and evaluate datasets features for detection of phishing URL. The study shows that deep learning logo recognition can be used for detection of phishing attacks. According to Maurya and Jain [30], many solution exist for detection and prevention of phishing attacks, research for eradication of phishing attacks is far from existed especially with the increased in sophistication of phishing attacks to discover a proactive solution.

C. Recommendation for Eradication of Phishing Attacks in E-Government System

i) Anti-Phishing Attacks in E-government

Anti-Phishing attacks are security measures that can be taken by people in both private and government organizations to eradicate phishing attacks. In order to defend both private and public organizations I E-government systems, the anti-phishing attack measures outlined in section 5.2 above provide resilience and defence against phishing attacks. However, effective mitigation of phishing attacks requires combination of people, process and technological approaches. Therefore, typical defence against phishing attacks by technical measures will only have limited success. Consequently, some recommendations to address the prevalence and success of phishing attacks in E-government system include educational awareness campaign, gainful employment of citizens, legislative enactment and law enforcement.

ii) Education, Training and Awareness Campaigns

Despite the fact that anti-phishing technologies helps in mitigation of phishing attacks, phishing scam still get through security boundaries due to low level of education and security awareness of citizens. Therefore, Burita, et al. [31] proposed a training system that helps in enhancing users ability to differentiate between phishing and legitimate emails. Policy and awareness and public education by process of training to acquire knowledge on phishing scam and other SEA enhance citizens' power of reasoning and judgement is a fundamental means of phishing attacks' eradication.

iii) Gainful Employment of Citizens

Citizens that are gainfully employed mostly become responsible and law abiding citizens compared to unemployed ones. Overall, employed citizens' powerful and attractive benefits provided by the employers on top of compensation including insurance, learning and development opportunities, retirement benefits and more are catalysts for job satisfaction. A satisfied gainfully employed individuals tend to be productive, honest and dedicated citizens. Therefore, citizens' right to work and good working condition leads to social protection and responsible citizenship. Although, both employed and unemployed can

be victims of phishing scam. However, satisfied individual engaged in both private and public businesses will not want to lose their job as such will not partake in any fraudulent activities.

iv) Legislative Enactment

Legislative enactment is the law agreed by the parliament and made an official law of the country. However, the constitution is supreme, it is the basis for enactment of any laws. It means any law that contradicts the constitution is null and void. Nowadays, eradication is phishing attack is challenging because new threats are rising while the old threat is still being battled. Anti-phishing law and regulation can help to ensure that businesses in both private and public enterprises are safeguarded. The anti-phishing law should imposed serious penalty on anyone convicted of phishing activities. This will serve as deterrent to others thinking to partake in such scam. The stringent level of the anti-phishing law is an important factor in the security protection of E-government systems.

v) Law Enforcement

Law enforcement is an act of governance that compels citizens and non-citizens comply with the law. The duty of law enforcement agencies and officers is to ensure that people obey the law. Citizens benefit from the enforcement of laws since it prevents criminal activities. However, enforcement of law on phishing and SEA generally requires technical technological knowledge to effectively identify cybercriminals. Ultimately, special training for law enforcement agents on cybercrime investigation is sacrosanct.

VI. CONCLUSION

E-government system is globally identified as an approach for enhancing quality of public services and decision-making that promote effective interactions between governmental and private organizations with citizens. The numerous benefits of E-government systems leads to increase in adoption of the novel technology worldwide. However, as the reliance on E-government matures, this is accompanied with increase in creative phishing scams. To avoid phishing attack, seven common techniques use by scammers to exploit victims in E-government system are identified as standard email phishing, spear phishing, clone phishing, whaling, voice phishing, text-message phishing, and angler phishing. This paper abridged seven anti-phishing attacks for protection of E-government system. They are security awareness education, accurate authentication of citizens, phishing filter, MALWARE detection and prevention, artificial intelligence methods, machine learning and deep learning methods. The author recommend use of anti-phishing attacks, gainful employment of citizens as well as law enactment and enforcement for eradication of phishing attacks in E-government systems.

ACKNOWLEDGMENT

The support and encouragement of the council and management of Modibbo Adama University Yola is acknowledged.

REFERENCES

[1] Alshaher, A. (2021), "IT Capabilities as a Fundamental of Electronic Government System Success in Developing Countries from Users Perspectives", Transforming Government: People, Process and Policy, 15 (1), 129-149.

[2] Burlacu, S., Patarlageanu, S. R., Diaconu, A., & Ciobanu, G. (2021). E-government in the Era of Globalization and The Health Crisis Caused by the Covid-19 Pandemic, Between Standards And Innovation. In SHS Web of Conferences, EDP Sciences. 92(1), 1-8.

[3] Ahmed, M. M. (2022). Social Engineering Attacks in E-Government System: Detection and Prevention. International Journal of Applied Engineering and Management Letters (IJAEML), 6(1), 6.

[4] Salahdine, F., & Kaabouch, N. (2019). Social Engineering Attacks: A Survey. Future Internt, 11(4), 89-106.

[5] Rathee, D., & Mann, S. (2022). Detection of E-mail Phishing Attacks–Using Machine Learning and Deep Learning. International Journal of Computer Applications, 183(47), 1-7.

[6] Abroshan, H., Devos, J., Poels, G., & Laermans, E. (2021). COVID-19 and Phishing: Effects of Human Emotions, Behavior, and Demographics on the Success of Phishing Attempts during the Pandemic. IEEE Access, 9(1), 121916-121929.

[7] Aljeaid, D., Alzhrani, A., Alrougi, M., & Almalki, O. (2020). Assessment of End-User Susceptibility to Cybersecurity Threats in Saudi Arabia by Simulating Phishing Attacks. Information, 11(12), 547.

[8] Rahim, F. A., & Azman, F. (2020, August). Phishing Attack Simulation: Measuring Susceptibility among Undergraduate Students. In 2020 8th International Conference on Information Technology and Multimedia (ICIMU) IEEE, (pp. 132-137).

[9] Alguliyev, R., Aliguliyev, R., & Yusifov, F. (2018). Role of social networks in E-government: Risks and security threats. Online Journal of Communication and Media Technologies, 8(4), 363-376.

[10] Rastenis, J., Ramanauskaitė, S., Janulevičius, J., Čenys, A., Slotkienė, A., & Pakrijauskas, K. (2020). E-mail-based phishing attack taxonomy. Applied Sciences, 10(7), 1-15.

[11] Basit, A., Zafar, M., Javed, A. R., & Jalil, Z. (2020, November). A novel ensemble machine learning method to detect phishing attack. In 2020 IEEE 23rd International Multitopic Conference (INMIC) IEEE. 1(1). 1-5.

[12] Zabihimayvan, M., & Doran, D. (2019, June). Fuzzy rough set feature selection to enhance phishing attack detection. In 2019 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE), 1(1), 1-6.

[13] Odeh, A., Keshta, I., & Abdelfattah, E. (2021). PHIBOOST-a novel phishing detection model using Adaptive boosting approach. Jordanian Journal of Computers and Information Technology (JJCIT), 7(1), 64-73.

[14] Rahim, R., Murugan, S., Mostafa, R. R., Dubey, A. K., Regin, R., Kulkarni, V., & Dhanalakshmi, K. S. (2020). Detecting the Phishing Attack Using Collaborative Approach and Secure Login through Dynamic Virtual Passwords. Webology, 17(2), 524-535.

[15] Ravi, R. (2020). A performance analysis of Software Defined Network based prevention on phishing attack in cyberspace using a deep machine learning with CANTINA approach (DMLCA). Computer Communications, 153(1), 375-381.

[16] Kara, I. (2021). Don't bite the bait: phishing attack for internet banking (e-banking). The Journal of Digital Forensics, Security and Law: JDFSL, 16, 1-12.

[17] Yao, W., Ding, Y., & Li, X. (2018, December). Deep learning for phishing detection. In 2018 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Ubiquitous Computing & Communications, Big Data & Cloud Computing, Social Computing & Networking, Sustainable Computing & Communications, ISPA/IUCC/BDCloud/SocialCom/SustainCom, IEEE, 1(1), 645-650.

[18] Nemane, M. B. S., & Pahurkar, M. R. D. (2021). An Anti-Phishing Strategy Based on Visual Cryptography. International Research Journal of Engineering and Technology (IRJET), 8(2), 1035-1038.

[19] Chen, L. (2019, October). Research on Anti-phishing Strategy of Smart Phone. In Journal of Physics: Conference Series, IOP Publishing, 1314(1), 1-4.

[20] Angehrn, A. (1997). Designing Mature Internet Business Strategies: the ICDT Model. European Management Journal, 15(4), 361-369.

[21] Maurya, S., & Jain, A. (2020). Deep learning to combat phishing. Journal of Statistics and Management Systems,23(6), 945-957.

[22] Deshpande, A., Pedamkar, O., Chaudhary, N., & Borde, S. (2021). Detection of phishing websites using Machine Learning. International Journal of Engineering Research & Technology (IJERT), 10(05), 430-434.

[23] Wang, Z., Ren, Y., Zhu, H., & Sun, L. (2022). Threat detection for general social engineering attack using machine learning techniques. arXiv preprint arXiv:2203.07933, 1(1), 1-16.

[24] Peng, T., Harris, I., & Sawa, Y. (2018, January). Detecting phishing attacks using natural language processing and machine learning. In 2018 ieee 12th international conference on semantic computing (icsc) IEEE. 1(1), 300-301.

[25] Alam, M. N., Sarma, D., Lima, F. F., Saha, I., & Hossain, S. (2020, August). Phishing attacks detection using machine learning approach. In 2020 third international conference on smart systems and inventive technology (ICSSIT) IEEE, 1(1), 1173-1179.

[26] Garvés, I. O., Cazares, M. F., & Andrade, R. O. (2019, December). Detection of phishing attacks with machine learning techniques in cognitive security architecture. In 2019 International Conference on Computational Science and Computational Intelligence (CSCI) IEEE, 1(1), 366-370.

[27] Ripa, S. P., Islam, F., & Arifuzzaman, M. (2021, July). The emergence threat of phishing attack and the detection techniques using machine learning models. In 2021 International Conference on Automation, Control and Mechatronics for Industry 4.0 (ACMI) IEEE, (11). 1-6.

[28] Hussain, S., Sarma, D., & Chakma, R. J. (2020). Machine learning-based phishing attack detection. International Journal of Advanced Computer Science and Applications, 11(9), 378-388.

[29] Saha, I., Sarma, D., Chakma, R. J., Alam, M. N., Sultana, A., & Hossain, S. (2020, August). Phishing attacks detection using deep learning approach. In 2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT), IEEE, I (1), 1180-1185.

[30] Maurya, S., & Jain, A. (2020). Deep learning to combat phishing. Journal of Statistics and Management Systems, 23(6), 945-957.

[31] Burita, L., Matoulek, P., Halouzka, K., & Kozak, P. (2021). Analysis of phishing emails. AIMS Electronics and Electrical Engineering, 5(1), 93-116.

Received: 18/04/2024

Ahmed Midila Musa
Physical Sciences Education Department,
Faculty of Education, Modibbo Adama University, Yola, Nigeria
ahmedmm4me@yahoo.com