Phishing Attacks Prevention using Smart Based Artificial Intelligence Algorithms for Cyber Security Awareness

Nwokoro Ifeanyi Stanly[1], Okesola Olatunji Julius[2], Sambo Muhammad Qaim-Aliyu[3], Oshodin Osakpamwan George[4], Akinfenwa Timothy Ola[5], Adom-Oduro Zacciah Kwaku[6], Ahmed Sanusi Yusuf[7], Eze Ifeanyi Friday[8], Nwatu Augustina Nebechi[9]
[1]*Member, Rhema University Nigeria*
[2]*Member, First Technical University Ibadan Nigeria*
[3]*Member, Five Stars ICT Ltd Nigeria*
[4]*Member, Addbeams Nigeria Ltd*
[5]*Member, Osun State University Nigeria*
[6]*Member, University of Professional Studies Accra Ghana*
[7]*Member, Bank of Industry Nigeria*
[8]*Member, First Bank of Nigeria*
[9]*Member, Alex-Ekwueme Federal University Ndufu-Alike Ikwo*

***Abstract*- It has been said that machine learning is a useful defense against the majority of cyber-attacks. Therefore, the majority of computer attacks now have greater security thanks to the development of Artificial Intelligence (AI). Phishing assaults are dangerous, but they may be avoided using AI-powered solutions. This element points to the necessity of raising awareness of cyber security using AI. Most people's awareness will help to stop these kinds of attacks. The study explains how phishing attempts could be decreased if people were aware of AI-based cyber protection. Thus, the study illustrates the efficacy of AI-driven cyber security awareness education and its potential to impact cyber-attacks.**

Keywords: **Phishing, Artificial Intelligence, Machine Learning, Cyber Attacks, Social Engineering, Cyber Security.**

I. INTRODUCTION

One of the most prevalent kinds of cyber security threats is a phishing attack. This kind of attack uses social engineering in which the attacker sends phony messages to the target in an attempt to coerce him into giving his credentials [1]. This attack could potentially involve infecting a person's computer or sending ransom-ware software. Since phishing assaults are so frequent, people must have received the necessary training about them. There are various methods available for carrying out phishing attacks. A mass phishing assault is another tactic that attackers may use to directly affect vulnerable individuals by focusing on a group of people [2].

One of the most important things in preventing these attacks is being prepared to recognize and prevent them. According to Cisco (2022), phishing attempts cannot be stopped by a single cyber security attack. Being aware of these attacks is a good way to defend oneself from con artists that use this technique to obtain private information. It has been discovered that AI-based awareness is very important for preventing these threats. The majority of threats can be effectively stopped by AI-based cyber security [3]. Thus, the study supports an assessment of the potential for AI-based awareness to stop phishing attempts.

II. AN OVERVIEW OF PHISHING ATTACKS

Different attack types are used by scammers and hackers to target computer systems [4]. A particular collection of software that fully commandeers a user's system is a component of the majority of these attacks [5]. "Phishing attacks are the practice of sending fraudulent communications that appear to come from a reputable source," according to Cisco (2022). Typically, email is used for this [21]. Phishing attacks aim to get sensitive data, including credit card numbers and login credentials [1]. In addition, the attacks might involve placing malware on users'

computers and requesting a ransom to have the infection removed.

A person who is duped into clicking on a website link from his email is a prime example of a phishing attack [6]. After that, the attacker's website would request login credentials, to which the user would obligingly respond because he thought it was a reliable website. This guarantees that the assailant has acquired the primary data required. Phishing via email, spear, audio, and social media are a few popular techniques [2]. One of the most popular methods employed by hackers and con artists is phishing.

According to a recent Verizon research, phishing was implicated in 36% of all breaching cases [7]. In recent years, phishing has also become more popular [8]. People are increasingly susceptible to attacks due to the rise in internet usage. Thus, the idea of phishing remains a threat in today's world. Phishing has increased as a result of AI technology advancement. Attackers are now using AI and machine learning among other advanced techniques to manage their attacks [6] [9]. Phishing attackers have specifically embraced advanced AI technologies [9]. The graph below demonstrates how phishing attempts are becoming more and more dependent on AI to accomplish their goal.

According to Statista (2021), there were approximately 245,771 phishing attacks reported in January 2021. Thus, phishing is one of the major issues facing the world today. Additionally, attackers are learning additional strategies and tactics for controlling their attacks [22]. The data above demonstrates the necessity of creating strategies to support security against intrusions [10]. The use of AI in cyber security is one of these strategies. Research has shown that AI-based cyber security can have a major impact on cyber security [2]. According to the findings of the AI-based cyber security study, most individual users' security would be effectively promoted by awareness.

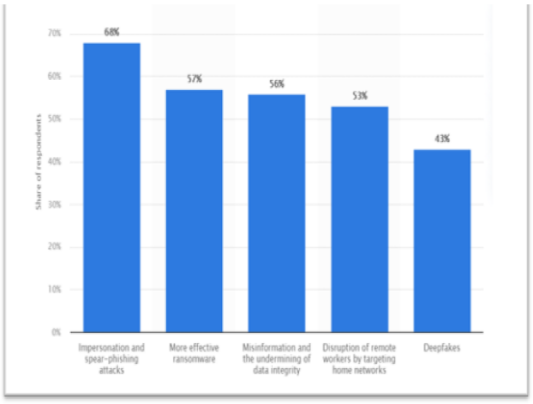

Figure 1: Possible global scenarios for cyber-attacks enabled by AI as at 2021 (Source: Statista.com).

2.1: How Phishing Operates

The phishing technique typically starts with a spoof email that persuades victims to use fake websites to access their accounts. These websites mimic the official website of a reputable service provider, like a financial institution or an online retailer [24]. Because the phishers spread the same logos and visuals as the real website, the spoof emails always appear to be legitimate emails. Furthermore, the fraudulent emails contain false URLs that point to a phony website.

The user will be taken to a fraudulent website that imitates the genuine one upon clicking the link. As soon as the victim enters their credit card number, username, or password, the information is recorded. As a result, users should refrain from forwarding unsolicited emails, clicking on odd links in emails, and using search engines to find charitable organizations and online donations [24].

2.2: Techniques for Phishing

By adhering to phishing strategies, employees can defend themselves and their businesses with the aid of AI-based Cyber security awareness training packages. Here are five useful methods for carrying out phishing attacks:

Pose as: This is a common method. All that is happening here is that the phishing email pretends to be from a reputable company where the victims may have an account. In order to make the scam email appear legitimate and ask the recipient to check in to

decrypt certain difficulties, the phisher transfers the symbols and drawings along with the genuine website [24]. The attack lowers user morale because it will be difficult for regular users to distinguish between reputable and fraudulent emails. Figure 2 illustrates a fraudulent email that displays a picture from a bank's website along with a phony URL that leads to a challenging webpage.

Figure 2: Scam email shares images with a genuine website (Source: Verizon research, 2023).

Forward attack: This is a cunning tactic where a phisher uses malicious code or a script inside a phony email to obtain personal information.

Pop-up Attack: This technique places a malicious pop-up window in front of the legitimate website, asking the target to log in through a pop-up window that is prohibited. The phisher obtains the target's login credentials when the user logs in to the pop-up and sends them to the approved website [24]. Here, the pop-up window acts as a man-in-the-middle to obtain private information.

Vishing, also referred to as voice phishing, occurs when a call is placed to the victim instead of an email. An automated recording statement notifying the victim about account violations plays when the recipient answers the fictitious call. The victim is directed to take action in order to save the account by the recorded information. Following this scenario, the victim is supposed to answer a call with a fictitious identification number from the financial institution [24].

Smishing, another name for mobile phishing: However, the combined and shortened form of SMS and Phishing is called Smishing. Instead of using another media source, the attackers intend to steal the victims' private information through the content they transmit in SMS texts. Usually, these contents consist of information like cellphone contact numbers, fake website URLs, greeting cards, and smartphone applications [25]. Fig. 3 shows an example of a smishing message.

Figure 3: An example of smishing message (Source: Walmart 2024).

III. NICE STRUCTURE AND *vi*CYBER MODEL

In order to transform the Comprehensive National Cyber Security Initiative (www.whitehouse.gov/Cybersecurity/comprehensive-national-Cybersecurity-initiative) from an internal, national focus to a federal activity, former US President Barack Obama established the National Initiative for Cyber Security Education (NICE) in 2010. In order to significantly improve the United States' long-term cyber security posture, NICE aims to finish an active, durable, and constantly improving program for workforce evolution, education, training, and awareness of cyber security. Despite focusing on the US, NICE recognizes the universal nature of internet. It feels that its movements may achieve positive results globally by collaborating with international organizations, global standards groups, and the international educational society [26].

NICE was founded on the belief that people are a vital resource in the battle against cyber risks:

• People who can design the technologies that preserve data and resources;

• People who can recognize and respond to cyber threats.
• People who understand how to protect others and themselves online.

The NICE framework heavily influences curriculum evolution, but because there aren't enough domain experts who can fully utilize it, powerful companies find it difficult to use. Organizations must take into account the relationships between AI-based cyber security awareness abilities in order to establish a workable framework. In order to address this issue, Amazon offers a cloud-based solution called viCyber, an intelligent system that uses artificial intelligence (AI) and visual mappings to quickly build cyber security curricula and training [23].

Businesses can utilize this service at any time and from any location to adapt, get ready and work together to safeguard infrastructure from threats. The NICE framework serves as the basis for controlling the viCyber model design, which incorporates a user viewpoint feedback and recommendation engine [23]. This AI-based model features a decision support technique based on human-computer interactions to explain the structure and allows the user to modify their conceptual experience while moving through the training process with instantaneous feedback. The NICE framework, which has seven categories, 31 specialty areas, and 369 Knowledge, is explained in Figure 4. There are 444 tasks under different specialized areas, 65 competencies, and Skills and Abilities areas (KSAs).

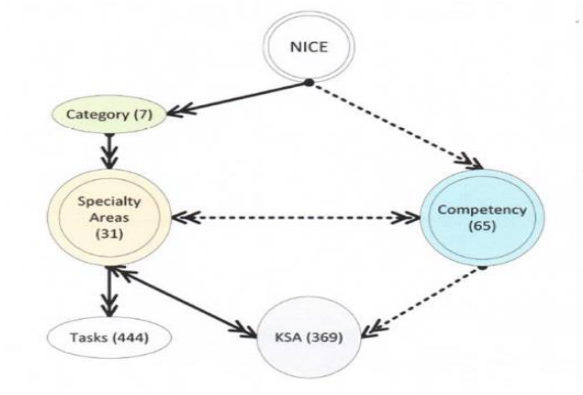

Figure 4: NICE Design framework (Source: whitehouse.gov)

IV. THE ADVANTAGES OF AI-BASED CYBER SECURITY SYSTEMS

Phishing assaults come with a number of concerns. According to Brad (2021), AI technologies significantly contribute to preventing the majority of these attacks. This element has been linked to the majority of firms prioritizing AI-based cyber security to safeguard their systems [10]. The strategy guarantees that the businesses have not had breaches within their own structures [3][9]. Additionally, there has been a rise in the creation of cyber security solutions powered by AI [9]. For the majority of its users, Google created a mechanism that could prevent email phishing [1]. Using more caution and awareness when using the internet and opening emails are some more strategies and tactics to stop assaults.

Through AI reasoning, the capacity of AI to prevent cyber attacks is enhanced. It has been discovered that providing AI systems with information significantly increases their ability to fend off threats. Cyber security has benefited from the advancement of machine learning technology as well [11]. This is made possible by a system that learns in real time while protecting the user. AI in cyber security has automated functions that respond quickly to ensure user safety. As a result, the systems are able to identify major risks and develop defense mechanisms against such assaults. Compared to people, the response time encourages this kind of security.

Today's use of AI in cyber security has many advantages. As previously demonstrated, the primary advantage of using AI in cyber security is faster response times. The ability of AI to learn more over time is the second major advantage. AI systems can now learn from their errors and get better thanks to machine learning technology [11]. The systems are able to recognize attack patterns and effective countermeasures. The ability of AI-based cyber security to identify novel threats that humans are unaware of is its next benefit [6]. Attackers never stop trying out novel concepts [12].

It has been discovered that AI technology performs better when it comes to spotting fresh threats and attacks. Large data sets can be handled by AI thanks to current technological advancements [3]. This element has made it possible for the system to provide

improved vulnerability management and security. Better outcomes have been obtained when human and artificial intelligence are involved in cyber security. This element thus demonstrates that a greater understanding of AI-based cyber security would successfully prevent phishing attempts.

4.1 AI-Powered training for Cyber Security Awareness

A major contributing factor to phishing's constant effectiveness is the general public's ignorance [4]. The majority of users are unaware of the possible risks connected to using the internet [1]. The public's ignorance about AI-based cyber security has contributed to the ongoing surge in phishing attacks [12]. The increasing number of phishing attacks and breaches that are being reported highlights the necessity of raising user awareness. Giving people the basic information they need to recognize these kinds of attacks could greatly increase user awareness [4]. Giving individuals the knowledge they need to comprehend AI-based cyber security and how they may utilize it to defend themselves is part of raising awareness [3].

Equipping people with this crucial knowledge will serve as a successful strategy in decreasing phishing-related attacks worldwide. One way to define training is the process of imparting knowledge to various people. As a result, the training sessions would require an understanding of cyber security and how artificial intelligence (AI) creates a far more beneficial sort of protection [1]. Users would gain an understanding of what it means to be sheltered from these lessons [12]. Phishing assaults would be one of the topics covered in the AI-based cyber security training, among others. A deeper comprehension of phishing and its various forms could be covered in the courses on phishing attacks [4].

The instruction on each of these elements has the potential to greatly advance global community understanding. One of the most important defenses against hackers is awareness [4]. The majority of attacks can profit from people's ignorance [4]. Hence, the training required might be crucial to getting better outcomes. It might guarantee that individuals always know how to defend themselves against the majority of attackers.

Understanding what phishing attacks are and how they work is the first line of defense against them [13]. To ensure that people can profit from identifying attacks, more information on this kind of attack is necessary [1]. Simple techniques used in social engineering can occasionally be successful in obtaining private information about certain people [3]. Therefore, raising people's awareness of phishing assaults could benefit the majority of people.

Given the rise in phishing attempts worldwide, training on these tactics is thought to be a successful tactic [3]. According to Brad (2021), ignorance was the primary cause of the majority of the attacks that occurred in the previous year. More phishing attack lessons will demonstrate how social engineering works as well as some things to look out for to prevent it [5]. Additionally, raising awareness would highlight the significance of data backups and two-factor authentication when creating passwords [14]. By doing this, people are guaranteed protection from ransomware assaults.

For the majority of businesses, AI-based cyber security has fantastic results promised. The majority of businesses that have profited from AI-based cyber security have spent millions to get the top cyber security system [15]. These organizations also train their staff on phishing attempts and how AI-based security safeguards the business. Employers must always provide training for their staff because people continue to be a system's greatest weakness [13]. In order to mitigate the impact of human error, it is imperative that staff receive training in self-defense and company policy [15]. Cyber security training is a common practice in companies that handle sensitive consumer data. By doing this, the possibility of vulnerability has decreased and the information is always safeguarded.

Employee training makes sure they can better safeguard the company's systems [16]. Understanding how the company's system has been safeguarded is very beneficial to all personnel inside the organization [5]. It is ensured that they can better secure the corporation with the information on constructing these systems [16]. Users can avoid assault scenarios in real life when they receive up-to-date training [2]. The emphasis on raising awareness to prevent assaults is

seen in the employee awareness initiatives that major corporations like Google and Amazon have put in place. It has encouraged these businesses to use premium security [6].

Instruction in AI-based Cyber security guarantees that people have shielded themselves against the possibility of disclosing firm secrets [5]. Additionally, users receive instructions on how to apply the same security measures to their own systems. Users must stay informed on the newest security measures to incorporate in order to implement this kind of security [17]. The AI community informs one another on emerging technologies that may be used to enhance security [1]. Hence, public education guarantees that individuals have safeguarded themselves from various forms of assaults. Thus, the general population benefits from AI-based security consciousness. Encouraging users to be mindful of these attacks, demonstrates to them the importance of exercising caution. Users are taught the value of exercising caution when this kind of security is promoted. As a result, awareness training can lessen the chance that users will fall victim to social engineering. Promoting these kinds of security requires training in AI-based cybercrime.

VII. CONCLUSION

To stop phishing assaults, the report suggests that AI-based cyber security awareness training should be promoted. The success of businesses in getting their staff to participate in training is indicative of the efficacy of awareness. Employee training guarantees that they are aware of the strategies and concepts to steer clear of when marketing security. Users that are knowledgeable with AI-based cyber security awareness are guaranteed to know how to use AI to strengthen security against phishing assaults. The techniques that AI-based cyber security employs to prevent cyber security also guarantee that users can stay away from social engineering and other phishing assaults. More knowledge about the many AI-based cyber security solutions that they can use also helps to raise the bar for security. It has been observed that more businesses gain from this kind of awareness. It has been demonstrated that phishing assaults have increased in recent years. By incorporating an equivalent degree of protection, users can guarantee that their systems are safe against phishing attempts. Thus, cyber security training is crucial for businesses and users alike. This strategy makes sure that people don't make mistakes that lead to attacks. Therefore, more enterprises should implement AI-based cyber security awareness training to prevent phishing attacks, which will lower the number of phishing attacks worldwide.

REFERENCES

[1] S. Back and R. Guerette, "Cyber Place Management and Crime Prevention: TheEffectiveness of Cyber security Awareness Training Against Phishing Attacks", *Journal of Contemporary Criminal Justice*, p. 104398622110016, 2021. Available: 10.1177/10439862211001628.

[2]"Reviewing Cyber security Awareness Training Tools Used to Address Phishing Attack at the Workplace", *Information Sciences Letters*, vol. 11, no. 2, pp. 391-398, 2022. Available: 10.18576/isl/110210.

[3] M. Ansari, "A Quantitative Study of Risk Scores and the Effectiveness of AI-Based Cyber security Awareness Training Programs", *International Journal of Smart Sensor and Adhoc Network.*, pp. 1-8, 2022. Available: 10.47893/ijssan.2022.1212.

[4] T.Daengsi, P. Pornpongtechavanich and P. Wuttidittachotti, "Cyber security Awareness Enhancement: A Study of the Effects of Age and Gender of Thai Employees Associated with Phishing Attacks", *Education and Information Technologies*, vol. 27, no. 4, pp. 4729-4752, 2021. Available: 10.1007/s10639-021-10806-7.

[5] S.Chatchalermpun and T. Daengsi, "Improving Cyber security awareness using phishing attack simulation", *IOP Conference Series: Materials Science and Engineering*, vol. 1088, no. 1, p. 012015, 2021. Available: 10.1088/1757-899x/1088/1/012015.

[6]"PREVENTION OF PHISHING ATTACKS: A THREE-PILLARED APPROACH", *Issues In Information Systems*, 2020. Available: 10.48009/2_iis_2020_1-8.

[7] D.Aljeaid, A. Alzhrani, M. Alrougi and O. Almalki, "Assessment of End-User Susceptibility to Cyber security Threats in Saudi Arabia by Simulating Phishing Attacks",

Information, vol. 11, no. 12, p. 547, 2020. Available: 10.3390/info11120547.

[8] E.Alamri, A. Alnajim and S. Alsuhibany, "Investigation of Using CAPTCHA Keystroke Dynamics to Enhance the Prevention of Phishing Attacks", *Future Internet*, vol. 14, no. 3, p. 82, 2022. Available: 10.3390/fi14030082.

[9] S.Purkait, "Examining the effectiveness of phishing filters against DNS based phishing attacks", *Information & Computer Security*, vol. 23, no. 3, pp. 333-346, 2015. Available: 10.1108/ics-02-2013-0009.

[10] S.Purkait, "Examining the effectiveness of phishing filters against DNS based phishing attacks", *Information & Computer Security*, vol. 23, no. 3, pp. 333-346, 2015. Available: 10.1108/ics-02-2013-0009.

[11] D.Glăvan, "Detection of phishing attacks using the anti-phishing framework", *Scientific Bulletin of Naval Academy*, vol., no. 1, pp. 208-212, 2020. Available: 10.21279/1454-864x-20-i1-028.

[12] R.Sabillon, J. Serra-Ruiz, V. Cavaller and Jeimy J. Cano M., "An Effective Cyber security Training Model to Support an Organizational Awareness Program", *Journal of Cases on Information Technology*, vol. 21, no. 3, pp. 26-39, 2019. Available: 10.4018/jcit.2019070102.

[13] J. Song and A. Kunz, "Towards Standardized Prevention of Unsolicited Communications and Phishing Attacks", *Journal of ICT Standardization*, pp. 109-122, 2021. Available: 10.13052/jicts2245-800x.126.

[14] S.Nasiri, M. TahghighiSharabian and M. Aajami, "Using Combined One-Time Password for Prevention of Phishing Attacks", *Engineering, Technology & Applied Science Research*, vol. 7, no. 6, pp. 2328-2333, 2017. Available: 10.48084/etasr.1510.

[15] A.Alhashmi, A. Darem and J. Abawajy, "Taxonomy of Cyber security Awareness Delivery Methods: A Countermeasure for Phishing Threats", *International Journal of Advanced Computer Science and Applications*, vol. 12, no. 10, 2021. Available: 10.14569/ijacsa.2021.0121004.

[16] A.Baiomy, M. Mostafa and A. Youssif, "Anti-Phishing Game Framework to Educate Arabic Users: Avoidance of URLs Phishing Attacks", *Indian Journal of Science and Technology*, vol. 12, no. 44, pp. 01-10, 2019. Available: 10.17485/ijst/2019/v12i44/147850.

[17] M. Jensen, M. Dinger, R. Wright and J. Thatcher, "Training to Mitigate Phishing Attacks Using Mindfulness Techniques", *Journal of Management Information Systems*, vol. 34, no. 2, pp. 597-626, 2017. Available: 10.1080/07421222.2017.1334499.

[18] T.Tagarev, N. Stoianov, G. Sharkov and Y. Yanakiev, "AI-driven Cyber security Solutions, Cyber Ranges for Education & Training, and ICT Applications for Military Purposes", *Information & Security: An International Journal*, vol. 50, pp. 5-8, 2021. Available: 10.11610/isij.5000.

[19] T. Gupta, S. Kumar, A. Tomar and K. Verma, "DNS Prevention Using 64-Bit Time Synchronized Public Key Encryption to Isolate Phishing Attacks", *International Journal of Security and Its Applications*, vol. 10, no. 8, pp. 395-406, 2016. Available: 10.14257/ijsia.2016.10.8.35.

[20] Brad. K. How Machine Learning Helps in Fighting Phishing Attacks. (2021).*Phish protection.https://www.phishprotection.com/blog/machine-learning-helps-fighting-phishing-attacks/*

[21] Cisco. What Is Phishing?2022. https://www.cisco.com/c/en_ae/products/security/email-security/what-is-phishing.html

[22] Statista. Potential scenarios of AI-enabled cyberattacks worldwide as of 2021. 2021. https://www.statista.com/statistics/1235395/worldwide-ai-enabled-cyberattacks-companies/

[23] Dash, B., & Ansari, M. F. (2022, April). " An Effective Cyber security Awareness Training Model: First Defense of an Organizational Security Strategy". Retrieved April 8, 2022, from https://www.irjet.net/volume9-issue4

[24] O. Salem, A. Hossain and M. Kamala, "Awareness Program and AI based Tool to Reduce Risk of Phishing Attacks," 2010 10th IEEE International Conference on Computer and Information Technology, 2010, pp. 1418-1423, doi: 10.1109/CIT.2010.254.

[25] C. Balim and E. S. Gunal, "Automatic Detection of Smishing Attacks by Machine Learning Methods," 2019 1st International Informatics and

Software Engineering Conference (UBMYK), 2019, pp. 1-3, doi: 10.1109/UBMYK48245.2019.8965429.

[26] C. Paulsen, E. McDuffie, W. Newhouse and P. Toth, "NICE: Creating a Cyber security Workforce and Aware Public," in IEEE Security & Privacy, vol. 10, no. 3, pp. 76-79, May-June 2012, doi: 10.1109/MSP.2012.73.