International Journal of Smart Sensor and Adhoc Network

Volume 3 | Issue 3 Article 6

March 2022

Prevention of Phishing Attacks Using AI-Based Cybersecurity Awareness Training

Meraj Farheen Ansari
University of the Cumberlands, merajfarheenansari25@gmail.com

Pawan Kumar Sharma
University of the Cumberlands, spawankumar570@gmail.com

Bibhu Dash
University of the Cumberlands, dash.bibhuprasad@gmail.com

Recommended Citation

Ansari, Meraj Farheen; Sharma, Pawan Kumar; and Dash, Bibhu (2022) "Prevention of Phishing Attacks Using AI-Based Cybersecurity Awareness Training," *International Journal of Smart Sensor and Adhoc Network*: Vol. 3: Iss. 3, Article 6.
DOI: 10.47893/IJSSAN.2022.1221
Available at: https://www.interscience.in/ijssan/vol3/iss3/6

Prevention of Phishing Attacks Using AI-Based Cyber security Awareness Training

Meraj Farheen Ansari [1]
Pawan kumar Sharma[2]
Bibhu Dash[3]
[1] Dept. of Computer and Information Systems, University of the Cumberlands, Williamsburg, KY USA
[2] Dept. of Computer and Information Systems, University of the Cumberlands, Williamsburg, KY USA
[3] Dept. of Computer and Information Systems, University of the Cumberlands, Williamsburg, KY USA

Abstract

Machine learning has been described as an effective measure in avoiding most cyber attacks. The development of AI has therefore promoted increased security for most computer attacks. Phishing attacks are risky and can be prevented through AI-based solutions. This factor suggests the need for increased awareness of cyber security through AI. Developing awareness for most people will prevent these types of attacks. The research paper describeshow the awareness of AI-based cyber security could ensure a reduction of phishing attacks. The paper, therefore, showcases the effectiveness of AI-based cyber security awareness training and how it may influence cyber-attacks.

Keywords*:* Machine learning, AI, phishing, smishing, vishing pop-up attacks, impersonate, forward attacks social engineering, cyber security, cyber attacks, NICE.

1. Introduction

A phishing attack is among the most common types of cyber security attacks. This type of attack involves some type of social engineering where the attacker sends fraudulent messages tricking the victim into providing his credentials[1]. This attack may also be included in sending malicious software requiring ransom or impacting a person's computer. Phishing attacks are very common, requiring that people have been provided with essential training about this attack[1]. There are different ways through which phishing can be achieved. Attackers could also engage in a mass phishing attack which targets a group of people to directly impact the vulnerable individuals[2]. Remaining ready to avoid and detect this attack is considered an essential factor in avoiding these attacks. Cisco (2022) suggests that no single cyber security attack can prevent phishing attacks. Remaining aware of these attacks is an effective approach to remaining protected from scammers using this method to acquire sensitive information. AI-based awareness has especially been found to be relevant in avoiding these attacks. AI-based cyber security is

effective in preventing most types of attacks[3]. Therefore, the research proves a review of how AI-based awareness may prevent phishing attacks.

2. Background on Phishing Attacks

Hackers and scammers use different types of attacks to attack computer systems[4]. Most of these attacks include a specific set of software that completely takes over a user's system[5]. Cisco (2022) defines phishing as, "Phishing attacks are the practice of sending fraudulent communications that appear to come from a reputable source. It is usually done through email" [21]. The main goal of phishing attacks includes acquiring sensitive information such as login and credit card information[1]. The attacks could also include installing malware on users' machines and asking for ransom for removing the malware.

A good example of a phishing attack could involve a user being tricked into clicking a website link from his email[6]. The attacker's website would then ask for login information which the user would readily provide, believing that it is a trusted website he uses. This ensures that the attacker has obtained the main information he needed. Some common phishing attacks include email, spear, voice, and social media phishing[2]. Phishing is among the most common attacks used by hackers and scammers. A recent study by Verizon indicated that 36% of all breaching cases involved phishing[7]. The use of phishing has also been on the rise in recent years[8]. The increased use of the internet has made more people vulnerable to attacks. The concept of phishing is, therefore, a continued danger in the community today.

Phishing has also risen due to the development of AI technology. The approach has risen significantly from attackers, including AI and machine learning, in managing their attacks[6] [9]. Advanced technologies in AI have especially been adopted by phishing attackers[9]. The graph below shows that phishing attacks have been increasing in using AI to complete their objective.

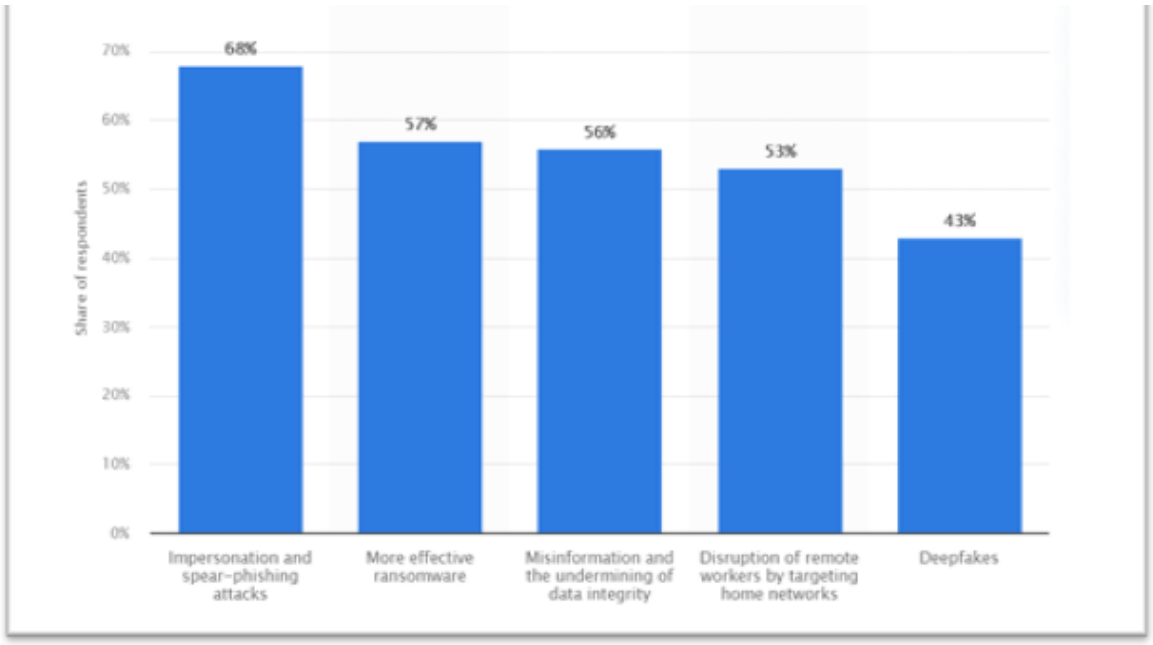

Figure 1: Potential scenarios of AI-enabled cyberattacks worldwide as of 2021; (Source: Statista.com)

Statista (2021) shows that around 245,771 phishing attacks were recorded in January 2021. Phishing is, therefore, a key problem around the globe today. Attackers are also getting more ideas and tricks for managing their attacks [22]. The information presented above shows the need to develop methods to promote security against attacks[10]. One of these approaches is AI-based cyber security. AI-based cyber security has been researched to have significant results in cyber security[2]. The results associated with cyber security through AI indicate that awareness would effectively promote security for most individual users.

3. How Phishing works

The phishing method usually begins with an impersonated email, impacting individuals to log in to their accounts by utilizing minted WebPages that glimpse like the official webpage of the legitimate service provider, such as a financial group or an online shop[24]. The spoofed emails continually look like valid emails because the phishers disseminate identical emblems and visual images as the actual website. In addition, the scam emails retain misleading URL addresses relating to a fraud website.

By clicking the link, the user will be directed to a false website that looks like the legitimate one. The information is captured as soon as the victim enters the username, password, or credit card number. Therefore, users should not forward unauthenticated emails, click on unusual links in an email, or use search engines to look for online donations and charitable organizations [24].

3.1 Phishing Techniques

AI-based Cyber security awareness training programs can help employees protect themselves and their organizations by following phishing techniques. These are five practical approaches to executing phishing attacks:

Impersonate: This is a standard technique. Merely, the phishing email falsely argues to be from a legitimate business where victims might have an account. The phisher transmits the symbols and illustrations with the original website so that the scam email seems to be an official email requesting the user to log in to decrypt specific issues[24]. This attack weakens the user's morale as it will be challenging for ordinary users to differentiate between legitimate and deceitful emails .**Figure 2**shows a scam email that reveals the graphic of a bank's website and a deceitful URL link up to a tricky website

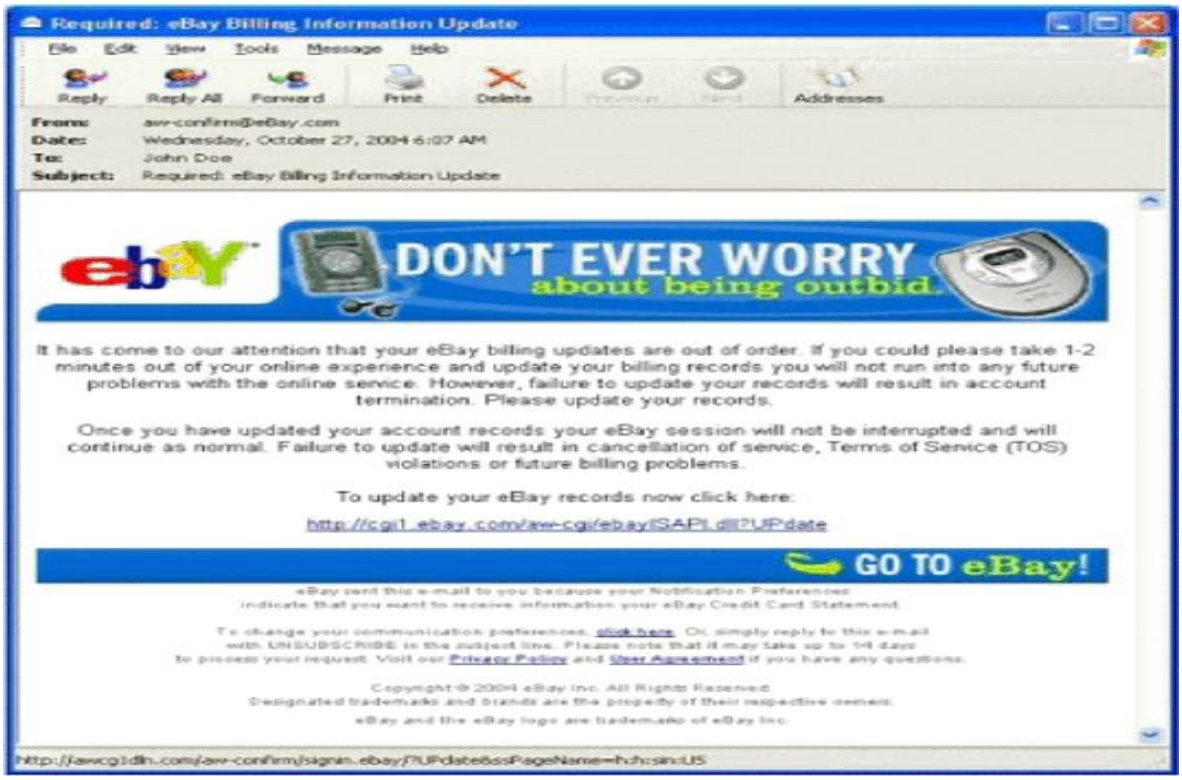

Figure 2: scam email shares graphics with legitimate website

Forward attack: This is a sophisticated approach where the phisher gathers confidential details through harmful code or script within a scam email.

Pop-up Attack: This method establishes a malicious pop-up in front of the authentic website requesting the target to log in via a barred pop-up window. Once the user logs in to the pop-up,

the phisher grabs the target's credentials and delivers them to the authorized website[24]. In this case, the pop-up window performs as a man-in-the-middle to gather confidential data.

Voice Phishing is known as Vishing: In this scenario, the victim is reached over the phone rather than by email. When the receiver responds to the fake call, an automated recording statement plays, alerting the victim about account infringements. The recorded information directs the victim to take action to save the account. The scheme after this scenario is that the victim accepts the call from a spoofed ID number of the monetary organization [24].

Mobile Phishing, known as Smishing: On the other hand, the word Smishing is the collaborative and abbreviated form of SMS and Phishing. Attackers plan to pinch the confidential data of the victims using the content they send in SMS messages instead of another media source. These contents are typically comprised of data such as smartphone applications, fraudulent website URLs, greeting notes, and mobile contact numbers [25]. A sample of the smishing message is shown in Fig.3

Figure 3: A sample of smishing message

4. NICE FRAMEWORK AND viCyber Model

In 2010, US President Barack Obama formed the National Initiative for Cyber security Education (NICE) to expand the Comprehensive National Cyber security Initiative (www.whitehouse.gov/Cyber security/comprehensive-national-Cyber security-initiative) from an internal, nationwide focus to a federal activity. NICE drives to complete an active, endurable, and continuously enhancing program for Cyber security awareness, teaching, training, and workforce evolution that measurably increases the United State's long-term Cyber security posture. Although NICE concentrates on the US, it identifies the global essence of cyberspace. It believes that by partnering with international organizations, global norms associations, and the international educational society, its movements can have favorable outcomes worldwide [26].

NICE was created with the view that an essential aid in the fight against cyber threats is individuals:

- People who can make the technologies that save data and resources.
- Individuals who can identify cyber threats and react to them.
- Individuals who comprehend how to safeguard themselves and others in cyberspace.

The NICE framework extensively guides curriculum evolution, but influential businesses face hardships using it due to the scarcity of domain specialists who can fully employ it. To develop a practical framework, organizations must consider AI-based Cyber security awareness competencies along with their relationships. To overcome this challenge, Amazon presents a cloud-based system: viCyber, an intelligent system capable of rapid Cyber security curriculum and training development using AI and visual mappings [23]. Organizations can use this service anytime and anywhere to evolve, prepare, and collaborate when protecting infrastructure from perils. The viCyber model design is controlled based on the NICE framework with feedback and suggestion engine regarding user perspective [23]. This AI-based model has a determination support strategy established on the human-computer dealings to explain the structure, which enables to adjust the conceptual experience of the user when proceeding via the training with real-time feedback. Figure 4 explains the NICE framework which consists of seven categories, 31 specialty areas, and 369 Knowledge. Skills and Abilities areas (KSAs), 65 competencies, and 444 tasks under various specialty areas

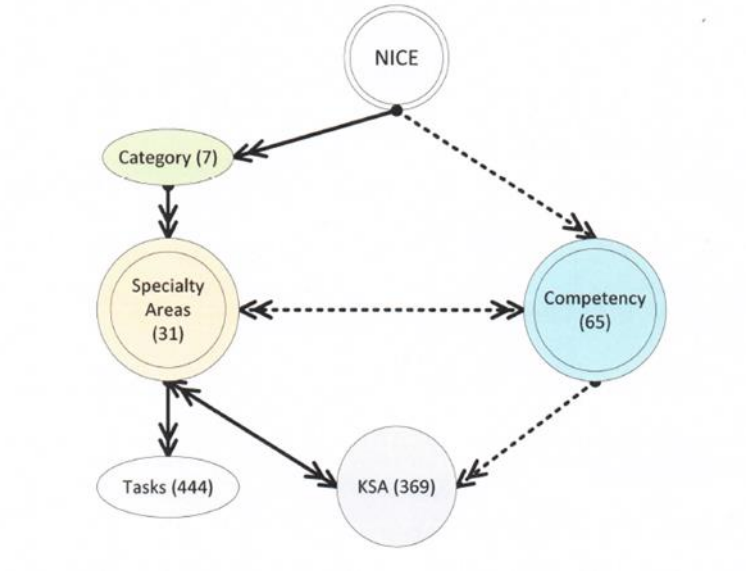

Figure 4.: NICE framework diagram

5. AI-Based Cyber security Systems' Benefits

There are many risks associated with phishing attacks. Brad (2021) indicates that AI technologies have significant results in avoiding most of these attacks. This factor has been associated with most organizations focusing on AI-based Cyber security in protecting their organizations' systems[10]. The approach ensures that the companies have avoided breaches within their organizations[3][9]. There has also been an increase in the development of AI-based Cyber security systems[9]. Google developed a system that could avoid email phishing for most of its users[1]. Other approaches and methods to prevent attacks include increased care and awareness when online and when emails are opened.

The capability of AI to avoid cyber attacks is promoted through AI reasoning. The knowledge offered to AI systems has been found to have significant results in avoiding attacks. The development of Machine learning technologies has also promoted Cyber security[11]. This is achieved from a system learning in real-time, ensuring the user's safety. AI in Cyber security has automated features which act at a fast response time, ensuring safety. The systems are therefore able to detect key threats and create ways through which these attacks could be avoided. The response time promotes this type of security compared to humans.

There are several benefits of using AI in Cyber security today. As showcased before, the faster response time is the main benefit of adopting AI in Cyber security. The second key benefit is that AI can learn more over time. Machine learning technology has enabled AI systems to improve by learning from their mistakes[11]. The systems can understand attack patterns and whats approaches would work to avoid these risks. The next advantage of AI-based Cyber security is that it can detect new attacks humans don't understand[6]. Attackers are always experimenting with new ideas[12]. AI technology has been found to offer better results in detecting new threats and attacks. AI can also handle large amounts of data due to modern technologies[3]. This factor has ensured that this system can offer better security and better vulnerability management. Including human and AI intervention in Cyber security has offered even better results. Therefore, this factor shows that increased awareness of AI-based Cyber security would effectively avoidphishing attacks.

6. AI-Based Cyber security Awareness Training

One of the key reasons phishing is always effective is a lack of awareness from public[4]. Most users do not understand the potential risk associated with internet use[1]. The continued rise of phishing attacks has been contributed by the public's lack of awareness of AI-based Cyber security[12]. The need for providing users with awareness can be seen in the rising number of phishing attacks and breaches being recorded. Providing people with essential knowledge of these types of attacks could significantly promote the awareness associated with most users[4]. Awareness includes providing people with the information they need to understand AI-based Cyber security and how they can use it to protect themselves[3]. Training users with this key information will act as an effective approach to reducing phishing-based attacks across the globe.

Training can be considered as being the act of providing lessons to different individuals. The training sessions would therefore entail the need to understand Cyber security and how AI achieves a significantly more helpful type of security[1]. These lessons would offer users an idea of what it meant to be protected[12]. The training on AI-based Cyber security would also involve lessons on phishing attacks, among other types. The lessons on phishing attacks could include a more understanding of phishing and the types of phishing[4]. The lessons on each of these factors could significantly promote increased awareness across the global community. Awareness has been considered a key prevention measure against hackers[4]. Most attacks can benefit from people's lack of awareness[4]. The training involved could therefore be significant in obtaining more results. It could ensure that people remain educated on ways to protect themselves against most types of attacks.

The first defense against phishing requires awareness of the meaning of phishing attacks and how they are achieved[13]. More information on this type of attack ensures that people can benefit from detecting attacks[1]. Social engineering includes simple steps which sometimes become effective in attaining sensitive information about some individuals[3]. The awareness of phishing attacks could therefore attain better results for most people.

Training on phishing attacks is considered an effective strategy due to the increased phishing attacks in the global community[3]. Brad (2021) finds that most of the attacks included in the past year were a result of a lack of awareness. The increased lessons on phishing attacks will show how social engineering is achieved and some factors to check in avoiding social engineering[5]. The awareness would also showcase the importance of factors such as two-factor authentication when placing passwords and the importance of backing up data[14]. This ensures people are protected against ransom ware attacks.

AI-based Cyber security has promised great results for most companies. Most companies that have benefited from AI-based Cyber security have invested millions in obtaining the best system in Cyber security[15]. The employees in these companies are also educated on phishing attacks and how AI-based security protects the company. Companies are always required to train their employees since the human factor remains the biggest vulnerability to a system[13]. Protecting against the human factor requires that employees have been provided with an awareness of ways that they could protect themselves and the company[15]. Training employees on Cyber security is practiced in organizations that keep users' sensitive information. This ensures that the information is always protected and the vulnerability likelihood has been reduced.

Training offered to employees ensures that they can better protect the systems in the company[16]. All employees within a company especially benefit when they understand how the company's system has been protected[5]. The information on developing these systems ensures that they can better protect the company[16]. Up-to-date training ensures that users can avoid real-life scenarios of attacks[2]. The focus on preventing attacks through awareness can be

observed in programs that companies like Amazon and Google have implemented for their employees. It has promoted high-end security for these companies[6].

Training on AI-based Cyber security ensures that individuals have protected themselves from the risk of providing secrets about the company[5]. Users are also provided information on how they can implement the same levels of security on their systems. Implementing this type of security requires that users remain educated on the latest type of security to include[17]. The AI society educates each other on new technologies that could be implemented to achieve security[1]. Training towards the public, therefore, ensures that they have also protected themselves from different types of attacks. AI-based security awareness, therefore, benefits public users.

An individual with training on AI-based Cyber security is difficult to social engineer compared to individuals who lack awareness[3]. AI-based Cyber security focuses on achieving security through engaging in being extra careful. Phishing attacks are especially avoided by being careful on the internet[3]. Social media and email phishing are all achieved through the internet. AI-based Cyber security can promote an extra sense of carefulness[13]. Promoting this type of awareness shows users the need to be careful in avoiding these attacks. When promoting this type of security, users are educated on the importance of being careful. Therefore, training on awareness can reduce the risk of social engineering to the users. Training on AI-based Cyber security is essential in promoting these types of security.

A lot of programs are available online to teach users about AI0-based Cyber security. The public can access these training programs at a cost. The most popular program is the ESET Cyber security awareness training[17]. ESET is a leading Cyber security provider that teaches the public about awareness. The training program included gamified training modules and phishing simulations to ensure users were educated[3]. These programs include AI systems which complete these programs. Users are therefore educated through AI, main them more aware of the ways hackers could use to acquire access to their programs.

Admins in these programs ensure that users have interacted with their AI systems in obtaining security. The information and lessons on security are included for all individuals, showcasing to them the importance of maintaining a similar level of security[18]. The AI systems can promote security by avoiding links sent through unverified emails and engaging in different types of security programs[19]. Users in the program by ESET are therefore advised to avoid mistakes that most users engage. The company has also included the overall need for awareness, which has recorded high results over the past few years.

7. Conclusion

The analysis indicates the need to promote AI-based Cyber security awareness training to prevent phishing attacks. The effectiveness of awareness can be seen in companies' success in engaging their employees in training. The training by employees ensures that they understand the

methods and ideas to avoid in promoting security. AI-based Cyber security awareness ensures that users understand how they can use AI to promote security against phishing attacks. The methods that AI-based Cyber security uses in avoiding Cyber security also ensures users can avoid phishing attacks such as social engineering. The level of security is also promoted through more information on types of AI-based Cyber security that they can implement. More companies have been seen to benefit from this type of awareness. Phishing attacks are shown to have arisen in the past few years. Including the same level of security will ensure that users can prevent phishing attacks on their systems. Cyber security training is therefore important to companies and users in general. The approach ensures that people avoid mistakes which result in them being attacked. Preventing phishing attacks using AI-based Cyber security awareness training should therefore be adopted by more organizations, thus reducing the number of global phishing attacks.

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.