Scientific and Practical Cyber Security Journal (SPCSJ) 8(3): 21 – 34 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

MITIGATING THE IMPACT OF PHISHING ATTACKS ON THE E-LEARNING INFRASTRUCTURE

Mamman Ojima John[1], Onoja Emmanuel Oche[2], Enoch Blessing Toyin[3]

[1]Department of Mathematics, Federal University of Agriculture Makurdi

[2]Department of Cyber Security, Federal University of Technology Minna

[3]Department of Mathematics, Federal University of Lafia

ABSTRACT: An essential component of the educational system is e-learning. this study delves into the potential risks and threats that e-learning systems face from unauthorized access by third parties and ways to protect data from unauthorized use, alteration, and reuse in a variety of e-learning-related circumstances, this work presents a systematic literature review on phishing techniques. it also takes mitigation techniques for phishing into account. as a result, the component and the threat posed by the information security component are presented in this study. in addition, important information security techniques for safeguarding e-learning systems are suggested at the conclusion of this paper. today, cybercrime remains a continuous danger. this paper gives an overview of the different types of phishing attempts and how they work. we come across new forms of cybercrime every day, along with its dire repercussions. as a result, there are numerous ways for hackers to pilfer sensitive and important data in addition to money. we also provide ideas and tactics that should be taken into account while creating mitigation plans. mitigation strategies primarily rely on human-centric approaches, secure e-learning systems, machine learning and neural networks, deep learning, and cryptography. as new phishing attacks emerge, new strategies will continue to develop to counter them.

KEYWORDS. E-Learning; Phishing; cybercrime; threat; Security, Cryptography.

1.0 INTRODUCTION

There is seldom a week that goes by without news about hackers assaulting companies, governments, colleges, and people all across the world. If we were to learn about all these online crimes, we might decide to quit using the internet altogether, which would be extremely inconvenient for us. The current study's review is likewise predicated on (Das et al., n.d.) where the hazards are actual, albeit it can be challenging to gauge their scope. It's not always about stealing money; sometimes it's about stealing ideas. The scope of intellectual property (IP) theft on a global scale is unprecedented (Eze et al., 2018). E-learning platform have a particular issue with IP theft. Since educational systems frequently fall behind in terms of technology and qualified employees, they are soft targets for cybercriminals (Ennu et al., 2018). Security breaches of E-learning networks can have serious repercussions, costing colleges millions. This study's aim was to identify cyberthreats and the most likely places where online learning systems would be vulnerable to attack. Instead of fully avoiding the internet, it is crucial that we understand the many kinds of cybercrimes and how to prevent becoming a victim of them. According to (Drzani, 2014) a fundamental definition of cyber crime is any criminal activity involving the use of the internet or cyberspace as a means to carry out the intended dishonest conduct for financial gain or other forms of dishonesty. Cybercriminals target particular computers, the most prevalent cybercrimes today include pharming, phishing, skimming, eavesdropping, and DOS attacks. Phishing is a form of online fraud in which the attacker poses as a reliable source (Catal et al., 2022). The attacker uses temptations that the victim is likely to succumb to in an attempt to seduce them and sensitive information about the victims, including credit card numbers or login credentials is typically stolen by these attackers (Das et al., n.d.) and (Desolda et al., 2021). This occurs when the victim clicks on a link sent by an attacker posing as a legitimate entity or when they give information to the attacker over the phone. The intrusive party collects user information and utilizes it maliciously against the victim by seducing the victim and promising false rewards. Annually, there is a rise in security events and breaches that target the human aspect of cybersecurity. Phishing attacks are a popular type of cyberattack that prey on people's ignorance of

cybersecurity. Phishing occurs when a perpetrator deceives a target into doing an action that is detrimental to both the victim and the system. It also involves attempts made without authorization to pose as a reliable source in order to gain sensitive information. These definitions make it evident that phishing is a fraudulent endeavor, albeit the attackers' motivations differ. Typically, its goal is to obtain financial information, steal sensitive data, and get access to system credentials. Phishing is additionally utilized as a vector for other assaults, including ransomware attacks. Recently, phishing attacks have targeted businesses, with malware containment costs, lost productivity costs, credential containment costs, and ransomware costs looming in its path (Abdillah et al., 2022).

This paper is organized as follows. First, the introduction gives a brief summary of the significance of cybersecurity in today's digital world, with a focus on e-learning platforms. It increases public awareness of the frequency of cybercrimes and their possible impacts on people and businesses. To emphasize the importance of the issue, it also cites pertinent studies.

Materials and Methods contains a list of the selection criteria for research publications, databases consulted, search terms utilized, and platforms or frameworks for data extraction and analysis.

The meaning of our results and how they relate to earlier research are covered in the results and discussion section.

The conclusion highlights the importance of phishing attacks and summarizes the major findings of the research.

2.0 MATERIALS AND METHODS

This approach describes the systematic literature reviews (SLRs) of phishing techniques, Risks and threats associated with e-learning systems and mitigation strategies against phishing attacks. As phishing attacks become one of the top cyberattack trends, the research community has worked hard in order to lesson the difficulties caused by phishing assaults (Chen et al., 2022) and (Alaubaci et al., 2024). Consequently, numerous research publications have emerged, shedding light on various aspects of phishing phenomena, user responses, and potential remedies (Prosen et al., 2022) and (Nadeem et al., 2023). In recent years, a series of literature reviews (SLRs) have been conducted and published, serving as comprehensive summaries of existing knowledge and guiding future studies in this field (Dima et al., 2022) and (Altaher, 2021). Notably, the selection of research papers for this study employed the VOSviewer tool, which considers word clusters, frequency, and impact factors to facilitate data extraction. VOSviewer's user-friendly interface enables the identification of significant clusters of key terms, which in turn inform the grouping of research activities and subsequent publications exploring various data relationships. The sources utilized for bibliometric information include Web of Science, Pubmed, digital libraries, Scopus, and search engines like Google, all of which are highly reputable.

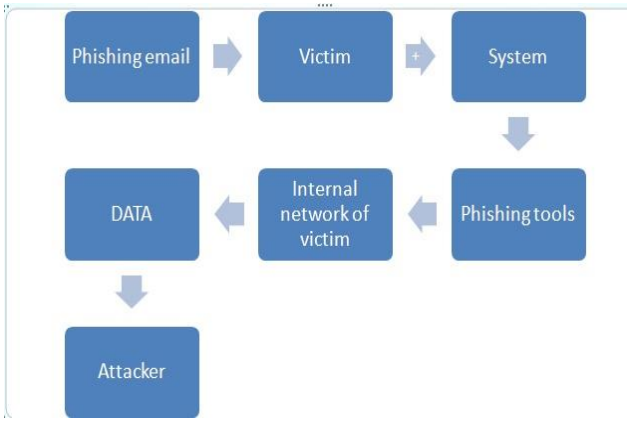

Fig. 1. *Process of phishing*

While numerous evaluations have recently been published, providing comprehensive descriptions of phishing attempts and encompassing both non-technical and technical protective measures, not all assessments have focused on the types and underlying reasons behind these attacks. The review

conducted by (Catal et al., 2022) highlights machine learning-based phishing detection techniques as its primary finding. This review thoroughly examines and evaluates strategies, information sources, records, feature selection methods, deep learning (DL) algorithms, assessment factors, verification methods, and the execution structures employed throughout the system's learning model life cycle. Additionally, the review identifies challenges associated with phishing detection and proposes potential solutions. The challenges and potential solutions are discussed in the review conducted by (Abdillah et al., 2022). The review focuses on the most common phishing assault vectors, sources of data, and detection methods employed to counteract phishing attempts. Additionally, the review examines the techniques utilized for rating performance in phishing attacks. The findings are presented in Table 1, which represents the Phishing Attack Incident from 2020 to 2022, as reported by Wise Online. The table provides information on the targeted industries and the percentage of phishing attacks in each industry for the years 2020, 2021, and 2022. Furthermore, Figure 2 illustrates the phishing attacks in the industry.

Tab.1. *Online report by Wise*

Targeted industry	2020	*2021*	*2022*
Webmail	29.80%	29%	29%
Financial	14.20%	15%	14.20%
Payment	33%	32.90%	33.90%
Logistics/Shipping	3%	3.20%	3.20%
Telecommunication	3.20%	3%	3%
Cloud Storage	4%	4.10%	4%
Others	12.80%	12.80%	12.70%

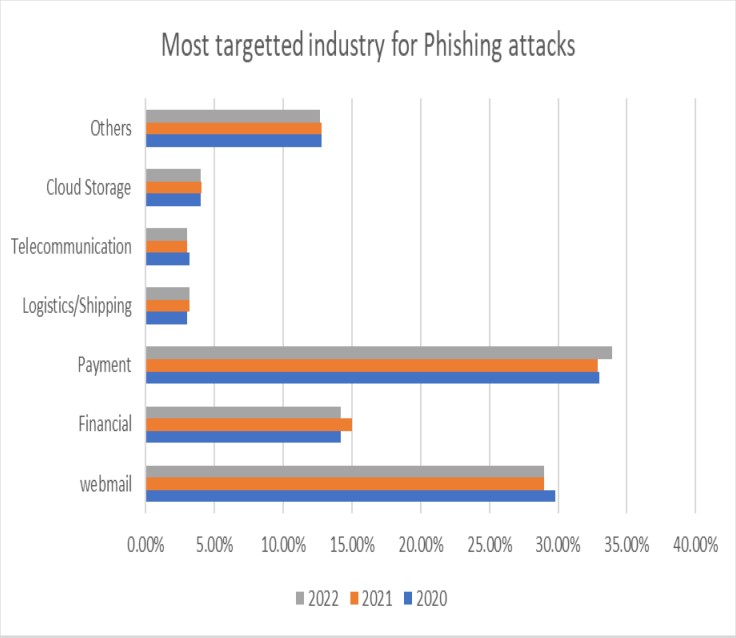

Fig. 2. *Wise online report of phishing attack incident from 2020 to 2022*

(Safi & Singh, 2013) conducted an examination of the literature on various methods for detecting phishing websites, information sets, and quantitative assessments of performance, including machine

learning-based methodologies. They also explored the use of natural language processing (NLP) to identify phishing emails and NLP-based methods for this purpose. (Desolda et al., 2021) and (Arshad et al., 2021) reviewed the literature on phishing and anti-phishing techniques, with a particular focus on the human element in phishing assaults. They discussed human-based ways to mitigate phishing attempts and user-based interventions.

Fig. 3*. Utilizing VOSviewer, a word cloud was created based on keywords from authors and index terms*

It is worth noting that the current classification schemes proposed by (Chanti & Chithralekha, 2019) and (Apandi et al., 2020) were not utilized in this literature review. These classification methods have limitations in classifying a wide range of data and are restricted to specific attack vectors. As a result, they are not applicable in the context of anti-phishing strategies. Furthermore, we examined the author keywords and index phrases for every publisher in order to find trends for categorizing anti-phishing tactics. To see the terms ranked by frequency, make a word cloud similar to the one shown in Figure 3. Figure 3 depicts the introduction of pertinent terminology for categorizing mitigation, including "algorithm," "system," "tool," and "learning." with regard to categorizing mitigation tactics. Still, they do not represent the entire taxonomy of mitigation techniques taken into account.

2.1 TECHNIQUES OF PHISHING

Middle-Man

This form of attack involves an unauthorized individual, known as the attacker, covertly intercepting the communication between the parties involved. The attacker gains illicit access to the transmitted information, manipulates it, and then forwards it to the intended recipient. As a result, the message is altered, and its original content is neither authentic nor genuine.

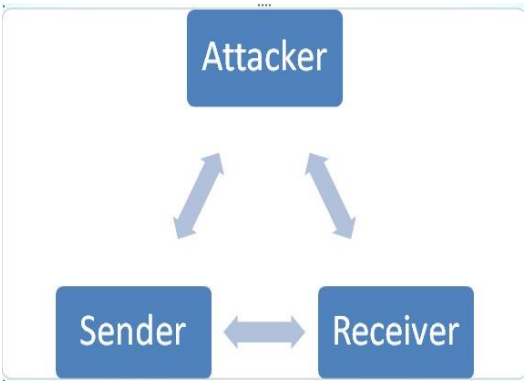

Fig. 4. *Middle-Man*

Email Phishing

Scams Attackers may go to great lengths to craft seemingly genuine emails to trick victims into providing the requested data (Sallaum et al., 2022). The attacker uses the original logo of the fake company and her signature to appear valid (Muutode & Parwe, 2019). Attackers also manipulate victims by mentioning urgency. For example, a phishing email could indicate that something is going on to pressure user to take necessary action as soon as possible. This leaves victims vulnerable and gradually becoming victims. Example as seen in fig. 5 below:

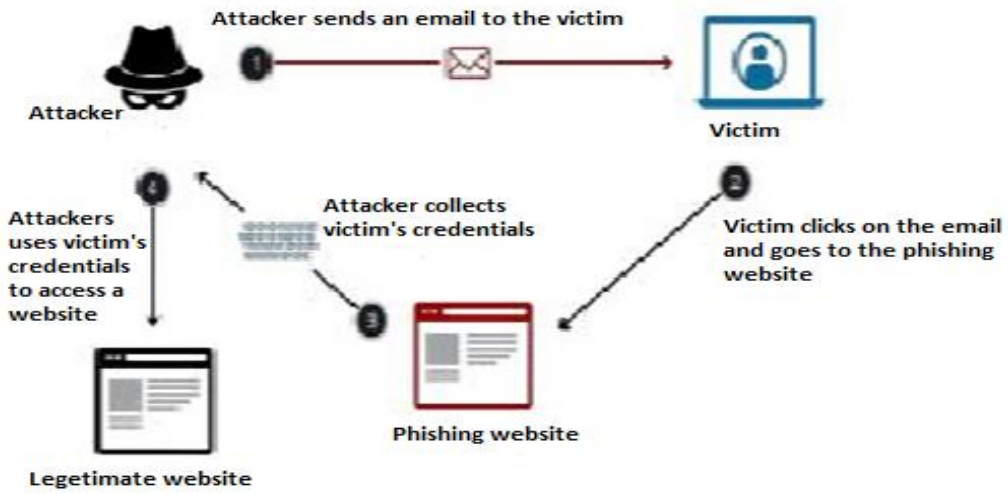

Fig. 5. *Example of e-mail Phishing*

Spear Phishing

Spear phishing involves targeted attacks directed at specific organizations or individuals for predetermined purposes (Ciangaxatapu et al., 2020). This technique requires in-depth knowledge of the target, including their operational structure. By tailoring the phishing attempt to the specific characteristics of the target.

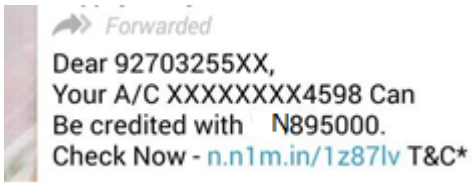

Fig. 6. *Spear Phishing example*

Phone Phishing

Phone phishing encompasses fraudulent messages that appear to originate from banks or network operators. Victims may receive SMS notifications claiming that their SIM card has expired, urgent updates to their bank details are required, or a new service has been activated on their device (Ibrahim et al., 2020). These messages often prompt the recipient to access a specific webpage, thereby exposing them to potential attacks.

Fig. 7. *Phone Phishing example*

Pharming (Domain Name Server-based Phishing)

Another form of phishing is pharming, which involves the manipulation of domain name servers to redirect victims to fraudulent websites. This can result in data or financial loss for the victim (Ibrahim et al., 2020).

Search engine indexing phishing

Search engine indexing phishing is another type of phishing that involves the use of attractive advertisements and offers to mislead victims with broken links or IP addresses.

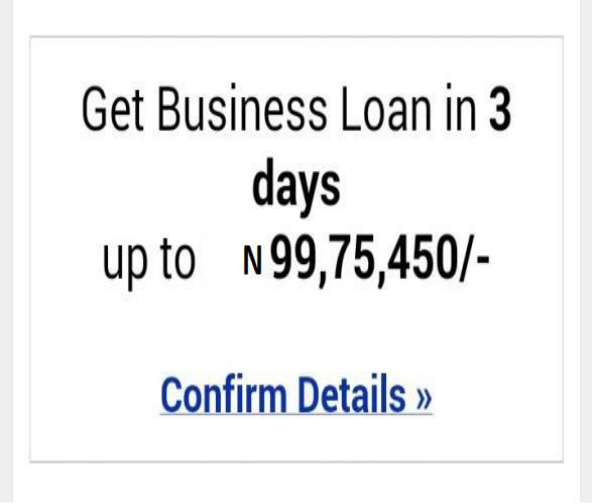

Fig.8. *Search engine indexing phishing*

Games, Social Networks, and Prizes

Games elements on certain websites encourage users to play particular games, ssimilar to "wheel games" or "three questions games" (Eze et al., 2018).

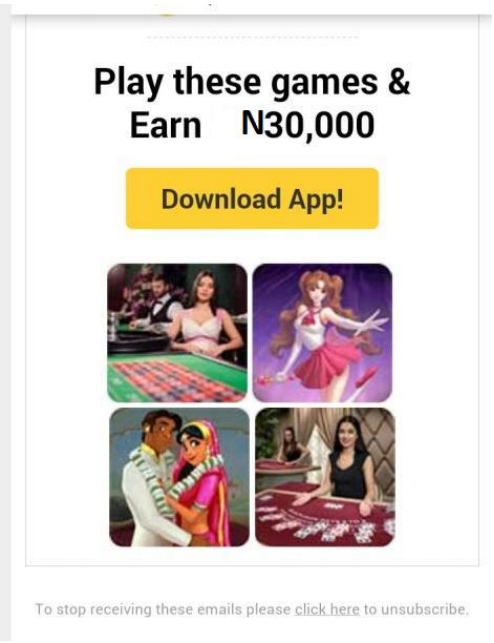

Fig.9. *Example of games, Social Networks, and Prizes*

Impersonation by creating a fake user

Creating fake users and using them as a way to make offers look genuine and gain the victim's trust is another way to carry out phishing attacks. These fake user accounts are essentially JavaScript code embedded as plugins on these phishing sites (Luminita, 2011). They trick victims into believing that someone has won the prize, and then take further steps.

Fig.10. *Fake user*

Sharing and Spreading

When you "earn" these games and rewards, the Website invites you to share more links with your social contacts through various social networks such as WhatsApp, Facebook. This is done to increase the attack's propagation range and increase the size of the target network.

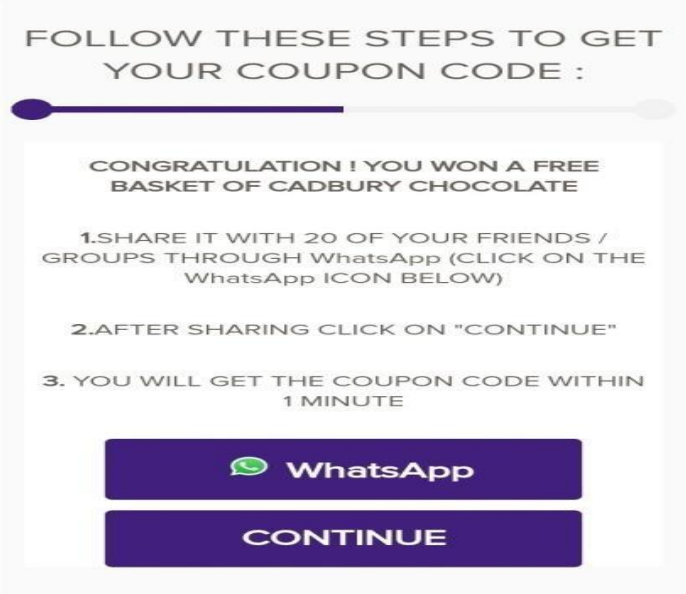

Fig.11. *Sharing and Spreading example*

2.2 RISKS AND THREATS ASSOCIATED WITH E-LEARNING SYSTEMS

This section provides an overview of the main cybersecurity risks associated with online systems and distributed e-learning systems. Important participants in the e-learning system are (Li et al., 2020):

Writer

As you know, writers can provide access to books and journal articles to a wide range of students. you can evolve to iimplement the content of these documents. Only registered students have access to these lecture notes, term papers and exam papers, so it is the writer's duty to protect the data from unauthorized use, alteration and reuse in various e-learning related situations.

Educators

Discussions are an important part of each course lesson. One form of discussion is an online forum. An advantage of online forum discussions over oral discussions is that all documents are stored electronically on a server. However, storing discussion, digitally poses a significant risk to the privacy of students and educators, but in any educational system, maximal interaction helps clarify understanding for both students and educators. In the long run, only robust security mechanisms can trigger this kind of interaction. In the examination system, the examination questions and questionnaires are standardized, and the academic freedom of individual faculty members may be restricted, and the risk of the examination is directly linked to misconduct. Additionally, educators should be concerned about assessment availability and non-repudiation prevention, and the risk of students receiving unaltered questionnaires.

Entry

All entry must be aware of all documents they receive from the Institute, educators, or other students. Because if an intruder has processed a questionnaire or other important documents, it must be considered that a problem occurred during the inspection. User IDs and passwords, in many attacks, provide an excellent opportunity for attackers to prevent authorized learners from accessing eLearning servers. Phishing tricks learners into entering sensitive information into fake websites that look like genuine e-learning websites.

Administrator

There are many risks associated with e-learning platforms, including fraudulent individuals impersonating students and creating tests on behalf of registered students, or assisting in the creation of online exams without authorization. Legal issues such as copyrights, online tests, and sending official documents can therefore be a big problem for these participants. In this case, the administrator must handle course enrolment and, if necessary, cancellation of enrolment. Enrolling a given student in multiple courses poses a risk to the entire organization. You should have a plan for testing your backup and recovery processes. Otherwise, it will be difficult to create a plan.

2.3 STRATEGIES OF MITIGATION AGAINST PHISHING ATTACKS

To combat phishing attacks effectively, it is essential to incorporate interpretations of terms developed through literature analysis. Anti-phishing systems encompass software and tool-based strategies, including standalone systems, programmatic design approaches, and mitigation tools. Models and frameworks play a crucial role in defending against phishing attacks, encompassing activities to mitigate such attacks and machine learning-based models to enhance anti-phishing capabilities. Additionally, human-centered mitigation strategies focus on improving the ability of individuals to identify and respond to phishing attempts.

By considering these modifiers, a comprehensive solution can be developed to address the challenges and risks associated with e-learning platforms and phishing attacks.

This text provides guidelines and recommendations for enhancing skills related to e-learning security. These include organizing anti-phishing training sessions and conducting assessment quizzes. Additionally, key concepts and techniques that should be considered when developing strategies to mitigate security risks. The study revealed that the main concepts and technologies utilized in mitigation strategies are machine learning, neural networks, deep learning, cryptography, human-centric approaches, and secure e-learning systems (Chiew et al., 2019).

In response to growing threats, researchers have developed a number of measures and solutions to improve e-learning security. This section summarizes relevant discussions in the literature (Chang, 2016). Thanks to new technologies, e-learning has become more user-centric and secure.

Biometrics

Despite the availability of authentication technologies such as passwords, smart cards, digital signatures, and digital certificates, there is still a risk of unauthorized access by malicious individuals. For instance, rogue students may misuse passwords while submitting assignments, participating in surveys, or downloading course materials. Biometric authentication offers an additional layer of security in such scenarios. The advantage of biometric computer authentication lies in its reliance on unique personal characteristics, making it difficult to replicate or steal (Ciangaxatapu et al., 2020).

Digital Rights Management

Digital Rights Management (DRM) is a crucial aspect of managing intellectual property rights in the digital realm. Various stakeholders, such as writers, artists, scholars, for-profit companies, and consumers, have distinct motivations for implementing DRM. Writers and artists seek control over the usage of their creative works, scholars aim to ensure proper attribution, for-profit companies support business models that rely on licenses and fees, and consumers desire a legal and cost-free environment. It is important to note that rights themselves are not inherently technical but are shaped by laws, beliefs, and practices. However, technology plays a pivotal role in facilitating the transmission, verification, interpretation, and enforcement of digital rights (Ibrahim et al., 2020)

Watermarking

One effective solution for implementing DRM is watermarking. This technique allows for the inclusion of hidden copyright notices, as well as audio, video, and image signals within digital content (Chang, 2016). For instance, in the context of e-learning systems, watermarking can safeguard the multimedia database server from unauthorized use. By employing watermarking, certain e-learning information remains invisible to viewers, the risk of hacking is significantly reduced. E-learning platforms typically consist of diverse web-based applications that exhibit high interoperability and share similar authentication models. In a typical scenario, a student accessing an e-learning application is required to provide a "shared secret," such as a password or PIN number, along with their student ID. The password is securely stored in the database through a one-way hash function during registration. During the verification process, the student's submitted password is hashed and compared with the stored hash value. This authentication mechanism ensures the legitimacy of the student.

Distributed Firewall Solution

Software application that protects corporate network servers and end-user computers from unwanted intrusions such as distributed firewalls is considered server-based security. The difference between personal firewalls and distributed firewalls is that the latter have important advantages such as centralized management, logging, and sometimes granular access control (Muutode & Parwe, 2019). These features are necessary for implementing corporate security policies in large organizations.

Encryption

The purpose of confidentiality is to prevent disclosure of information or data to unauthorized individuals or organizations. One of the techniques in this aspect is encryption (Drzani, 2014). Cryptography plays an important role in the design and implementation of almost every kind of electronic system. Various cryptographic tools are required to implement security in Internet-based transactions. Encryption is a technology of data transformation Applications in inconsistent, encrypted, or unintelligible formats. This includes research into mathematical algorithms related to information security such as data integrity and authentication. Symmetric key cryptography and asymmetric key cryptography are two other important encryption types.

Tab.2. *Suggested policies based on preventative and detection techniques for people and organizations*

Principal Category	***Directives***
Put endpoint security in place.	- Install endpoint protection. - Develop a technique for identifying threats to intelligent networking. Update computers' hardware and software on a regular basis. Use firewalls, email blocks, browser extensions, and the most recent version of antivirus software. Make use of intrusion detection systems for hosts (HIDS). Follow the security instructions provided by the vendor.
Put access restrictions in place.	Put limitations on access in place. Install tripwires for websites. Use administrator authentication that requires several factors, such as Microsoft Multi-Factor Authentication (MFA). Employ email authentication with DMARC. Observe login instructions.
Observe security guidelines	Respect security protocols. Adjust company policy to allow for anti-phishing and targeted security training, especially for individuals who pose a risk to others. Establish reporting protocols.
Preserve efficiency.	- Create and maintain password protection guidelines. - Discuss potential threats, compromise indicators, and internal best practices. - Establish backup plans - Provide privacy-respecting data processing and sharing. - Provide a Standard Solution (SS) that would enable an experienced writer to draft several sets of guidelines and then utilize them again.
Put device policies into action.	- Establish and set aside money for life-cycle management so that aging equipment can be retired and not easily replaced. - To maintain an up-to-date list of all allowed and illegal devices on the network. Create a policy in collaboration with internal and external manufacturing stakeholders to enable timely updates. - Develop a patching plan to minimize equipment failures. Before buying, take into account how long you think the devices will last.
Remember the guidance.	Verify every call that is received for the authority. - Refrain from sharing information unless you expected to

> hear from the other person.
> - Employ cybersecurity specialists.

Given the dynamic nature of attackers and the possible sensitivity of data, a key issue for future exploration will be the difficulty in giving comparable evaluations among various phishing detection algorithms due to the lack of established benchmarks and reference datasets (Ozcan et al., 2023).

3.0 RESULTS AND DISCUSSION

The discussion revolved around the techniques employed by attackers to carry out phishing attacks, wherein a third party covertly intercepts data exchanged between parties and gains unauthorized access to valuable information within e-learning systems. The risks and threats associated with key participants in the e-learning system were also examined, along with strategies to safeguard data from unauthorized use, alteration, and reuse in diverse e-learning scenarios. Additionally, mitigation measures against phishing attacks, particularly those relying on software and tools, were explored. These measures encompassed stand-alone systems, programmatically designed methods, and tools aimed at mitigating the impact of such attacks.

Numerous researchers have endeavoured to develop different approaches for detecting and protecting against phishing attacks, yet these efforts have often resulted in significant losses. Systematic literature reviews (SLRs) were conducted to assess the effectiveness of various countermeasures against phishing attempts, given the gravity of the situation.

The research on phishing has witnessed a notable surge, particularly in terms of the methods employed by attackers and the domains they target (Bhavsar et al., 2018). According to Table 1 and Figure 2 of a comprehensive online study conducted between 2020 and 2022, phishing attacks were most prevalent in areas such as payments, webmail, and finance. This observation suggests a consistent increase in the frequency of phishing attacks each year, with certain areas exhibiting a heightened vulnerability and concentration of attacks.

4.0 CONCLUSION

Phishing attacks can be launched through various means. However, this study primarily focuses on the detection and prevention techniques applicable to e-learning environments, aiming to empower clients and learners to take necessary precautions against such attacks in the future. The work presented here encompasses an exploration of different types of attacks, along with their prevention and detection mechanisms.

We provide a brief overview of the extensive utilization of email and digital media, highlighting their susceptibility to cybercrime when used without caution. Furthermore, we delve into the various techniques employed in phishing, focusing solely on the phishing process. This document presents an outline of well-known phishing scams. Additionally, we present measures that can aid in the identification of phishing attacks and safeguard individuals from falling victim to such malicious activities. Phishing stands as one of the most prevalent and rapidly expanding forms of cybercrime. Failure to exercise proper precautions and care when engaging in digital and electronic communication can result in significant financial and data losses. Given the ever-evolving nature of phishing assaults, there is an urgent need for effective strategies to mitigate these attacks, which is a major problem for further research and the difficulty in providing comparable evaluations among different phishing detection algorithms due to the lack of established benchmarks and reference datasets, given the dynamic nature of attackers and the potential sensitivity of data. Lastly, the target audience for this paper includes but not limited to academics and business professionals as well as anybody with an interest in cyber security. To assist researchers in organizing their next steps, it offers existing solutions, and current trends. Apart from offering guidelines and recommendations that are specifically crafted with the organization's viewpoint in mind, it provides industry practitioners with an up-to-date summary of the most recent research on phishing attacks and could prove beneficial to incorporate in their respective environments. This paper presents the state of the art in mitigation strategies and highlights current phishing trends for a general audience interested in cyber security.

DECLARATION OF COMPETING INTEREST

The authors affirm that they possess no known competing financial interests or personal relationships that could have potentially influenced the findings presented in this paper.

REFERENCES

Abdillah, R., Shukur, Z., Mohd, M., & Murah, M. Z. (2022). Phishing classification techniques: A systematic literature review. *IEEE Access*, 10, 41574-41591.

Alaubaci, F. S., Almazros, A. A., & Ayub, N. (2024). Enhancing phishing detection: A novel hybrid deep learning framework for cybercrime forensics. *IEEE Access*, 12, 8373-8389. https://doi.org/10.1109/access.2024.3351946

Altaher, A. (2021). Intelligent ensemble learning approach for phishing website detection based on weighted soft voting. *Mathematics*, 9(21), 2799. https://doi.org/10.3390/math9212799

Apandi, S. H., Sallim, J., & Sidek, R. M. (2020). Types of anti-phishing solutions for phishing attacks. IOP Conference Series: *Materials Science and Engineering*, 769, 012072.

Arshad, A., Rehman, A. U., Javaid, S., Ali, T. M., Sheikh, J. A., & Azeem, M. W. (2021). A systematic literature review on phishing and anti-phishing techniques. arXiv. https://doi.org/10.48550/arXiv.2104.01255

Bhavsar, V., Kadlak, A., & Sharma, S. (2018). Study on phishing attacks. *International Journal of Computer Applications*, 182(33), 27-29. https://doi.org/10.5120/ijca2018918266

Catal, C., Giray, G., Iskinenlagan, B., Kumar, S., & Shukla. (2022). Applications of deep learning for phishing detection: A systematic literature review. *Knowledge and Information Systems*, 64(6), 1457-1500. https://doi.org/10.1007/s10115-022-01672-

Chang, V. (2016). Review and discussion: E-learning for academia and industry. *International Journal of Information Management*, 36(3), 476-485. https://doi.org/10.1016/j.infomgt.2015.12.007

Chanti, S., & Chithralekha, T. (2019). Classification of anti-phishing solutions. *SN Computer Science*, 1(1). https://doi.org/10.1007/s42979-019-0011-2

Chen, S., Lu, Y.-X., & Lim, D. J. (2022). Phishing target identification based on neural networks using category features and images. *Security and Communication Networks*, 2022, 1-12. https://doi.org/10.1155/2022/5653270

Chiew, K. L., Tan, C. L., Wong, K. S., Yong, K. S. C., & Trong, W. K. (2019). A new hybrid ensemble feature selection framework for machine learning-based phishing detection system. *Information Sciences*, 484, 153-166. https://doi.org/10.1016/j.ins.2019.01.064

Ciangaxatapu, T., Jaidhat, C. D., & Chanduka, B. (2020). Applicability of machine learning in spam and phishing email filtering: Review and approaches. *Artificial Intelligence Review*, 53(7), 5019-5081. https://doi.org/10.1007/s10462-020-09814-9

Desolda, G., Ferro, L. S., Marrella, A., Catarsi, T., & Costabile, M. F. (2021). Human factors in phishing attacks: A systematic literature review. *ACM Computing Surveys*, 54(8), 1-35. https://doi.org/10.1145/3469886

Das, A. S., Baki, A., El Aassal, & Vetm. (n.d.). Phishing research from the society perspective: A comprehensive re-examination of BEE Common Surveys Tuts. *Journal*, 22(1), 671-704. Available at https://1911.00953

Dima, A., Bugheanu, A. M., Boghian, R., & Madsen, D. O. (2022). Mapping knowledge area analysis in e-learning systems based on cloud computing. *Electronics*, 12(1), 62. https://doi.org/10.3390/electronics12010062

Drzani, M. (2014). Securing e-learning platforms. 2014 International Conference on Web and Open Access to Learning (ICWOAL), *Dubai, United Arab Emirates*, 1-4. https://doi.org/10.1109/ICWOAL.2014.7009237

Eze, S. C., Chinedu-Ere, V. C., & Belle, A. O. (2018). The utilisation of e-learning facilities in the educational delivery system of Nigeria: *A study of M-University. International Journal of Educational Technology in Higher Education*, 15(1). https://doi.org/10.1186/41239-2018-0116-2

Ennu, G., Martes, M., & Boratto, L. (2018). A multi-brometne system for continuous student authentication in e-learning platforms. *Pattern Recognition Letters*, 113, 83-92. https://doi.org/10.1016/j.patrec.2017.03.027

Ibrahim, H., Karabatak, S., & Abdullahi, A. A. (2020). A study on cybersecurity challenges in e-learning and database management systems. *2020 8th International Symposium on Digital Forensics and Security (ISDFS)*. https://doi.org/10.1109/isdfs49300.2020.9116415

Li, T., Kou, G., & Peng, Y. (2020). Improving malicious URLs detection via feature engineering: Linear and nonlinear space transformation methods. *Information Systems*, 91, 101494. https://doi.org/10.1016/j.is.2020.101494

Luminita, D. C. (2011). Information security in e-learning platforms. Procedia - *Social and Behavioral Sciences*, 15, 2689-2693. https://doi.org/10.1016/j.sbspro.2011.04.171

Muutode, A. R., & Parwe, S. S. (2019). An overview on phishing, its types and countermeasures. *International Journal of Engineering Research and Technology*, 8(12). https://doi.org/10.17577/ijertv8is120260

Nadeem, M., Zahra, S., Abbasi, M., Arshad, A., Riaz, S., & Ahmed, W. (2023). Phishing attack, its detections and prevention techniques. *International Journal of Wireless Information Networks.* https://doi.org/10.37591/gwan

Ozcan, A., Catal, C., Demmez, E., & Senturk, B. (2023). A hybrid DNN-LSTM model for detecting phishing URLs. *Neural Computing & Applications*, 35, 4957-4973. https://doi.org/10.1007/s00521-02

Prosen, M., Kamuž, I., & Ličen, S. (2022). Evaluation of e-learning experience among health and allied health professions students during the COVID-19 pandemic in Slovenia: An instrument development and validation study. *International Journal of Environmental Research and Public Health*, 19(8), 4777. https://doi.org/10.3390/ijerph19084777

Safi, A., & Singh, S. (2013). A systematic literature review on phishing website detection techniques. *Journal of King Saud University - Computer and Information Sciences*, 35(2), 590-611. https://doi.org/10.1016/j.jksuci.2025.01.004

Sallaum, A., Gaber, T., Vaderz, & Shaalan, K. (2022). A systematic literature review on phishing email detection using natural language processing techniques. *IEEE Access*, 10, 65703-65727. https://doi.org/10.1109/access.2022.31830838918286.