cognizancejournal.com
Adzmer W. Basir *et al*, Cognizance Journal of Multidisciplinary Studies, Vol.4, Issue.12, December 2024, pg. 520-524
(An Open Accessible, Multidisciplinary, Fully Refereed and Peer Reviewed Journal)
ISSN: 0976-7797
Impact Factor: 4.843
Index Copernicus Value (ICV) = 77.57

THE ROLE OF EMPLOYEE AWARENESS IN MITIGATING PHISHING RISKS IN THE WORKPLACE

Adzmer W. Basir; Jimmy R. Jumadil; Jul-Yasar A. Dasid; Jamraida H. Halilul; Fatima Nadine H. Saiyadi; Fatima Karwina H. Jumadil; Shiela S. Abdurajan; Parisa H. Habibi; Farhana G. Hussin; Mosri B. Mondares; Prof. Shernahar K. Tahil

BSIT Student, College of Computer Studies, Mindanao State University-Sulu, Philippines
Faculty, College of Computer Studies, Mindanao State University-Sulu, Philippines

DOI: 10.47760/cognizance.2024.v04i12.047

Abstract: This paper investigates the essential role of employee awareness in mitigating phishing risks within the workplace. Through an analysis of educational aspects of phishing awareness training, the study emphasizes the importance of equipping employees with the knowledge and skills necessary to recognize and respond to phishing attempts effectively. It further explores the integration of technological solutions to enhance employee training and improve the organization's overall security posture. The research highlights the significance of risk management in proactively identifying and addressing phishing threats. Findings indicate that a comprehensive approach combining thorough training, advanced technology, and proactive risk management strategies significantly reduces the likelihood of phishing attacks. By reinforcing employee understanding of cyber threats, organizations can minimize potential damages and strengthen their overall cyber-security defenses. This study underscores the need for continuous engagement and training to adapt to the evolving landscape of cybercrime.
Keywords: Phishing, Employee Awareness, Cybercrime

Introduction

Employee awareness is essential in mitigating phishing attacks because their knowledge and understanding of this cybercrime help combat the threats posed by cybercriminals. Phishing is a form of cybercrime where attackers use different tactics to trick their victims by impersonating a trustworthy entity to exploit sensitive information. Phishing awareness training

cognizancejournal.com
Adzmer W. Basir *et al*, Cognizance Journal of Multidisciplinary Studies, Vol.4, Issue.12, December 2024, pg. 520-524
(An Open Accessible, Multidisciplinary, Fully Refereed and Peer Reviewed Journal)
ISSN: 0976-7797
Impact Factor: 4.843
Index Copernicus Value (ICV) = 77.57

in the workplace can reduce the number of victims by reinforcing employee knowledge and understanding, allowing them to detect and avoid phishing attacks (Desai & Ansurkar, 2022).

Workplace phishing attacks test an organization's security awareness maturity. A research study emphasizes that many businesses conduct regular phishing awareness training to equip employees with knowledge about the different forms of cybercrime (Desai & Ansurkar, 2022). Employees equipped with knowledge about phishing tactics are less likely to fall victim to such attacks (Hadnagy & Fincher, 2018).

Employees are often the victims of these attacks. Organizations should dedicate time, effort, and resources to training their employees. By establishing effective organizational awareness and providing guidelines to information security officers the number of phishing attack victims can be reduced (Hillman et al., 2023).

Subtopic

1. Employee Engagement and Training

Phishing attacks are one method attackers use to breach organizational information systems; however, most related studies focus on individual susceptibility. A research study defined employee engagement as an effective strategy to secure organization growth and survival (Jose, 2012). Many businesses increasingly rely on digital ecosystems, and most become exposed to malicious actors—a serious concern. (Aslan, 2023).

Employees play the pivotal role in strengthening cyber-security defenses. Cyber-security awareness and training programs have become crucial components in every organization as they aim to mitigate the increasing risks in the cyber world (Cheng & Wang, 2022).

Cyber-security awareness programs cover a wide area of educational methodologies made to engage employees effectively. The training must have activities that involve hands-on participation and real world application. Given the flexible nature of the cyber threat, successful awareness training programs integrate with regular updates to maintain employee awareness about the emerging threats and recommended best practices in the cyberspace (Sharma & Thapa, 2023).

2. Risk Management and Mitigation

Today, in the 21st century, the issue about data breaches and security incidents continue to rise annually. The data breach investigations report (DBIR) by Verizon highlights that 82% of the analyzed breaches involved the human element (Verizon, 2022). according to Venkatesha et al. (2021). Users should be more attentive to computer security. For example, they should avoid connecting their computers in public Wi-Fi when handling confidential information.

Lim et al. (2021) propose one mitigation strategy: actively sending phishing emails to users. When users respond, provide them with concise training materials demonstrating how to

cognizancejournal.com
Adzmer W. Basir *et al*, Cognizance Journal of Multidisciplinary Studies, Vol.4, Issue.12, December 2024, pg. 520-524
(An Open Accessible, Multidisciplinary, Fully Refereed and Peer Reviewed Journal)
ISSN: 0976-7797
Impact Factor: 4.843
Index Copernicus Value (ICV) = 77.57

recognize phishing attacks. Furthermore, Sadiq (2021) suggests that users should think before clicking, use firewalls, and use antivirus software to minimize damage if an attack occurs.

3. Educational Aspects

Educating users about phishing attacks is vital for mitigating the risk of victimization; by teaching users to identify phishing attempts, they become more vigilant and better able to avoid them. As phishing techniques have diversified, attackers employing increasingly sophisticated methods to deceive victims have rapidly increased the frequency of successful attacks. This necessitates a proactive approach to education and awareness. A study explored the use of gamified learning experiences to teach users about phishing; the findings showed that gamification not only increased user engagement but also significantly improved knowledge retention regarding phishing tactics (Krombholz et al., 2015).

Moreover, continuous employee learning about phishing is crucial given the constantly evolving nature of cyber threats. Continuous learning and periodic refresher courses are essential to keep users informed about emerging tactics (Tso et al., 2020). In addition, Ifinedo's (2014) research indicates that organizations fostering a culture of security awareness experience significantly lower rates of successful phishing attacks because employees are more likely to report suspicious activities and adhere to organizational security protocols.

Finally, Wombat Security Technologies (2022) found that regular phishing awareness training decreased the success rate of phishing attacks by a remarkable 70%. Their research also showed that programs incorporating simulations of phishing attacks provide employees with valuable hands-on experience in identifying and responding to potential threats.

4. Technological Integration

Organizations face a serious threat from phishing attacks, which exploit human weaknesses to steal sensitive data. Effective countermeasures require a comprehensive strategy integrating technological defenses with strong employee training programs focused on security awareness. Studies consistently show that human error plays a major role in successful phishing attacks, accounting for a significant number of data breaches (Verizon, 2022).

Phishing is a major cyber-attack targeting individuals and organizations worldwide. Cybercriminals exploit human weaknesses to steal sensitive information, causing significant harm. Various strategies and techniques have been developed to prevent phishing attacks, including advanced email filtering and other technologies that detect and prevent phishing attempts. Enhancing employee education and awareness programs significantly reduces individual vulnerability to these attacks (Ayun, Shah, & Badi, 2024). Ahid (2024) highlights the potential of emerging technologies such as machine learning, behavioral biometrics, and block

ISSN: 0976-7797
Impact Factor: 4.843
Index Copernicus Value (ICV) = 77.57

chain to improve detection and prevention, emphasizing the persistent nature of phishing as a major cyber-security threat.

Finally, phishing attacks represent a major cyber-security threat, exploiting both human error and technological vulnerabilities. Fasial Sharif (2024) advocates for a cyber-security strategy combining technological defenses, such as advanced email filtering and AI-powered threat detection, with comprehensive employee training to prevent phishing attacks. Furthermore, Fasial Sharif (2024) stresses the importance of regularly measuring the effectiveness of these defenses to ensure ongoing protection against the ever-evolving tactics of phishers.

Conclusion

In conclusion, to minimize workplace phishing threats, employee security awareness is paramount. Equipping employees with the ability to recognize and handle phishing attempts significantly reduces organizational vulnerability. A successful strategy requires a multi-pronged approach: strong training, advanced technology, and proactive risk management to counter the ever-changing threat landscape. Ongoing training and updates are vital to maintain employee vigilance against increasingly complex phishing schemes. Finally, cultivating a security conscious culture improves both individual employee preparedness and the organization's overall security.

References:

1. Abrahams, T. O., Farayola, O. A., Kaggwa, S., Uwaoma, P. U., Hassan, A. O., & Dawodu, S. O. (2024). CYBERSECURITY AWARENESS AND EDUCATION PROGRAMS: A REVIEW OF EMPLOYEE ENGAGEMENT AND ACCOUNTABILITY. Computer Science & IT Research Journal, 5(1), 100-119. doi.org/10.51594/csitrj.v5i1.708
2. Abid, N. (2024). An Analysis of Phishing Attacks: Information Technology Security: Cybercrime and Its Solutions. BULLET: Jurnal Multidisiplin Ilmu, 3(5), 696–712. https://www.journal.mediapublikasi.id/index.php/bullet/article/view/4811
3. Sharif, F. (2024). Enhancing Cyber Security Resilience: Phishing Defense and the Importance of Measurement Strategies. https://www.researchgate.net/profile/Fasial-Sharif/publication/384367096
4. Damaraju, A. (2024). Mitigating phishing attacks: Tools, techniques, and user education. https://redc.revista-csic.com
5. E., L., I., M., & H., M. (2024). A multi-layered security model to counter social engineering attacks: a learning-based approach. Journal of Cybersecurity, 5(1), 313–336. https://link.springer.com/article/10.1365/s43439-024-00119-z
6. Naqvi, B., Perova, K., Farooq, A., Makhdoom, I., Oyedeji, S., & Porras, J. (2023). Mitigation strategies against the phishing attacks: A Systematic Literature Review. Computers & Security, 132, 103364. https://doi.org/10.1016/j.cose.2023.103364
7. Hillman, D., Harel, Y., & Toch, E. (2023). Evaluating organizational phishing awareness training on an enterprise scale. Computers & Security, 132, 103364. https://www.sciencedirect.com/science/article/abs/pii/S0167404823002742
8. Aslan, Ö. (2023). A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. Electronics, 12(6), 1333. https://doi.org/10.3390/electronics12061333
9. Sharma, R., & Thapa, S. (2023). Cybersecurity Awareness, Education, and Behavioral Change: Strategies for Promoting Secure Online Practices Among End Users. Journal of Cybersecurity, 8(1), 1–17. https://doi.org/10.1016/j.jocs.2022.100110
10. Li, S., Zhou, J., MO, C., LI, J., Tso, G. K. F., & Tian, Y. (2022). Motif-aware temporal GCN for fraud detection in signed cryptocurrency trust networks. arXiv preprint arXiv:2211.13123. https://doi.org/10.48550/arXiv.2211.13123

ISSN: 0976-7797
Impact Factor: 4.843
Index Copernicus Value (ICV) = 77.57

11. Stu, S. (2022). Train Employees and Cut Cyber Risks Up To 70 Percent. KnowBe4 Blog. https://blog.knowbe4.com/train-employees-and-cut-cyber-risks-up-to-70-percent
12. Werner, M. J. (2021). The effect on employee engagement after experiencing a phishing attack. ProQuest. https://www.proquest.com/openview/12e3f13c061a56c3bb027d03e75a703d/1?pq-origsite=gscholar&cbl=2026366&diss=y
13. Sushruth, V., Reddy, K. R., & Chandavarkar, B. R. (2021). Social Engineering Attacks During the COVID-19 Pandemic. SN Computer Science, 2(1), 78. https://doi.org/10.1007/s42979-020-00443-1
14. Sadiq, M. A., Butt, R. A., Masud, F., Shahzad, M. K., Naseem, S., & Younas, M. (2021). A review of phishing attacks and countermeasures for internet of things-based smart business applications in industry 4.0. Journal of King Saud University - Engineering Sciences, 33(1), 101–115. https://doi.org/10.1016/j.jksues.2020.06.002
15. Holdsworth, J., & Apeh, E. (2017). An Effective Immersive Cyber Security Awareness Learning Platform for Businesses in the Hospitality Sector. 2017 IEEE 25th International Requirements Engineering Conference Workshops (REW). https://ieeexplore.ieee.org/abstract/document/8054838
16. Alghamdi, H. (2017). Can phishing education enable users to recognize phishing attacks? https://arrow.tudublin.ie
17. Dias Angelo, F., Bartocci Liboni Amui, L., Ferreira Caldana, A.C., & Jose Chiappetta Jabbour, C. (2012). Towards a strategic CSR: a Brazilian case study. Business Strategy Series, 13(5), 224–238. https://doi.org/10.1108/17515631211264104

