Article
JOURNAL OF UNIVERSITY OF BABYLON
For Pure and Applied Sciences (JUBPAS)
Vol.33; No.1.| 2025

Assessing the Impact of Phishing Attacks on Organizational Security and Mitigation Strategies

Wisam Adnan Kareem Al-Muswi
College of information technology, University of Babylon , almuswiwesam12@gmail.com , HILLA, Iraq.
وسام عدنان كريم عمران الموسوي
كلية تكنولوجيا المعلومات ، جامعة بابل ، almuswiwesam12@gmail.com، بابل، العراق

Accepted: 9/1/2025 **Published:** 31/3/2025

ABSTRACT

Background:

Phishing attacks have become a serious threat to enterprise security, exploiting our human vulnerabilities to gain access to sensitive information. Especially in critical sectors such as finance, healthcare, and technology. The primary objective of this study is to delve deeply into the financial, operational, and reputational consequences of these malicious attacks. It will also measure the effectiveness of various strategies aimed at thwarting them.

Methods:

The scientific and practical approach of this research is to conduct a series of multiple trips on different routes to collect information from employees and officials. It's analyzed using advanced machine learning algorithms(SVM), which carefully dissect the data to reveal rich insights. These results highlight the effectiveness of large number of anti-phishing strategies, providing clearer picture how to protect against deceptive threats.

Results:

Employees trained in security awareness have seen significant 30% reduction in their exposure to attacks. Meanwhile, AI models that leverage powerful natural language processing techniques, including BERT and GPT-3, have been shown achieve 90% accuracy in detecting phishing scams. Even more impressive, AI-based systems designed to combat this type of threat have an astonishing 85% accuracy.

Conclusions:

Combining security awareness initiatives with AI technologies and psychological insights can reduce phishing threats. Research confirms that ongoing training with AI-powered detection systems improves detection accuracy and enhances overall security.This holistic philosophy is critical for organizations to reduce their exposure to phishing attacks and enhance their resilience to cyber threats .

Keywords :cyber security threats; financial stability; data breaches, brand reputation; mitigation strategies; multi-factor authentication(MFA); machine learning in cyber security.

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

INTRODUCTION

Recently, phishing attacks have evolved into one of the most dangerous forms of threats to electronic devices, organizations, and government and civil institutions around the world. Phishing is an attack on these devices that tricks individuals into obtaining important and sensitive information (such as login credentials, financial digital data, personal identifiers of the individual, etc.) through fake emails, websites, or mobile phone calls ([3,4]). Therefore, it is very difficult to stop such attacks by relying on classic cybersecurity, so it is necessary to work on developing methods, work, and training people to reach confidence in avoiding such attacks and impersonation. [5].

The impact of phishing attacks on organizations can be detrimental [6-7], from direct financial loss in the millions and legal consequences to the most devastating loss of brand trust and operational productivity. With organizations digitizing more of their operations than ever, cybercriminals are increasingly targeting employees as an entry point to compromise corporate networks. Phishing causes the greatest number of data leaks in any industry — finance, healthcare, technology, and so on [8]. Human error continues to be the top reason for data breaches or cyberattacks, despite significant investments in cyber security tools, human error remains the leading cause of successful phishing attempts, highlighting the need for more effective training and awareness programs [9-10].

The financial cost of phishing is significant. According to IBM's 2023 Cost of a Data Breach report, phishing is one of the most expensive types of cyberattacks, with the average cost per breach involving phishing reaching $4.5 million [11]. Additionally, phishing attacks lead to prolonged recovery and stabilization times, with affected government and private organizations spending weeks or even months to fully mitigate the consequences of a breach [12]. In this context, organizations need to address not only the technical aspects of phishing but also focus on human factors, including employee awareness and organizational culture, which play a critical role in the success or failure of phishing attempts.

The main and primary objective of this research is to evaluate typical phishing attacks on some government institutions and organizations, thus focusing on the reputational, operational, and financial consequences. It will also evaluate current mitigation strategies, including some employee training programs, multi-factor authentication (MFA), and advanced AI-based solutions, to determine their effectiveness in mitigating phishing risks. Additionally, this research will discuss some limitations of all current defense assets and propose some recommendations for improving some organizational cybersecurity practices to address all the growing threats of phishing attacks.

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

METHODS AND MATERIALS

A. *Sample Selection and Data Collection*

This study targeted different samples from some organizations and sectors that face phishing attacks severely due to the sensitive nature of the data environment in which they operate and deal, such as healthcare, finance, technology and learning. These sectors were chosen because they are always targeted by cybercriminals who seek to exploit them and access their personal confidential data. About 30 organizations were selected, with samples of less than 500 employees who participated in this study for training. The employees included both senior executives and employees from the highest levels to the lowest, ensuring a broad representation of different organizational layers and their different levels of cybersecurity awareness.

The primary data collection methods included:

1. Surveys: During the study, a structured survey was distributed to the targeted audience to assess employees' general knowledge of phishing threats, cybersecurity best practices, and how to address their attitudes toward security measures in place in their organizations. The survey included multiple-choice questions and Likert scale items designed to measure the level of awareness and preparedness among employees, managers, and those in charge of it.
2. Live Phishing Simulation: A phishing simulation was conducted to assess how trainees and employees responded to phishing attempts. The simulation included a series of email phishing attempts that mimicked real-world attack vectors, such as phishing emails containing links or attachments. Responses were tracked to measure the rate at which employees clicked on phishing links or disclosed sensitive internal information.

B. *Security Awareness Training Program*

Among the guarantees achieved through the programs for the purpose of measuring the impact of training and development on detecting phishing, which plays a comprehensive and effective role in awareness in all institutions and organizations participating in the training:

1. Interactive Modules: Employees participated in online training modules that explained what phishing is, how to recognize phishing attempts, and the importance of safe online practices.
2. Phishing Simulations: One of the main and fundamental objectives for which this training was designed was to improve their ability to identify messages received from illegal emails and how to respond to them and deal with them in the right way, and this was confirmed by conducting a phishing simulation that included different types of phishing attempts that they are likely to encounter while performing their official duties in their work.
3. Post-training Assessments: After completing the training, employees were given a post-training assessment to evaluate their understanding and knowledge retention. This assessment included practical tests in which participants were asked to identify phishing emails.

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

C. *Artificial Intelligence-Based Phishing Detection*

Through artificial intelligence, a model based on natural language processing (NLP) was used. This model, which is based on advanced machine learning algorithms GPT-3 (pre-trained transformer) and BERT (bidirectional encoder representations from transformers), was trained, through which the effectiveness of artificial intelligence in detecting fraudulent emails was evaluated. Based on the widespread linguistic patterns and structures that users use, the artificial intelligence system analyzed many fraudulent and legitimate emails and achieved an accuracy rate of 90% in detecting fraud attempts.

In addition, through the use of one of the cybersecurity tools that rely on artificial intelligence, Darktrace, through which patterns of traffic on networks were analyzed and unusual behaviors aimed at what is called phishing were also identified, as the system was able to detect threats in real time and through it, a number of warnings were provided that were almost early from phishing fraud attacks, which in turn bypassed the usual security defenses.

D. *Psychological Behavior Analysis*

Through the study program and interviews conducted with employees from different levels and by learning about the situations they may encounter when exposed to phishing attempts and how external psychological and behavioral stimuli such as time, material incentives and urgency changed their actions and decisions, psychological factors were understood and solutions were provided to them to follow.

By addressing cognitive weaknesses, a highly effective security awareness program was designed that does not only address technical skills, but also uses behavioral analysis tools to identify and classify common psychological triggers that make employees more vulnerable to phishing attacks.

E. *Quantitative and Qualitative Data Analysis*

After collecting and analyzing the data from surveys, phishing simulations and interviews using qualitative and quantitative methods:

1. Quantitative Analysis: Statistical analysis was performed using SPSS software. Paired t-tests were conducted to compare the phishing detection accuracy before and after the security training. The data collected from the simulations and assessments were used to calculate the effectiveness of different mitigation strategies.
2. Qualitative Analysis: Interview data was analyzed using thematic analysis to identify recurring psychological triggers such as emotional manipulation and urgency, which influence susceptibility to phishing. Patterns and themes were categorized to understand how different psychological factors contribute to employees' and managers' susceptibility to phishing attacks.

*F. **Follow-Up Simulations***

When conducting a simulation of the phishing scam over a period of days of training, development and field work, and also to evaluate and know the effectiveness of security alert and awareness programs in the long term, the results of this simulation activity with continuous training showed the accuracy of continuous phishing scam detection around of 85%.

RESULTS AND DISCUSSION

The results of the study discovered the following:

Security Awareness Program: The results revealed that all employees who participated in this security awareness training program had a 85% reduction in their susceptibility to such phishing attacks after the training. A paired t-test was used to verify the difference in detection rates before and after the training in the program, and the difference was statistically significant at the 95% confidence level.

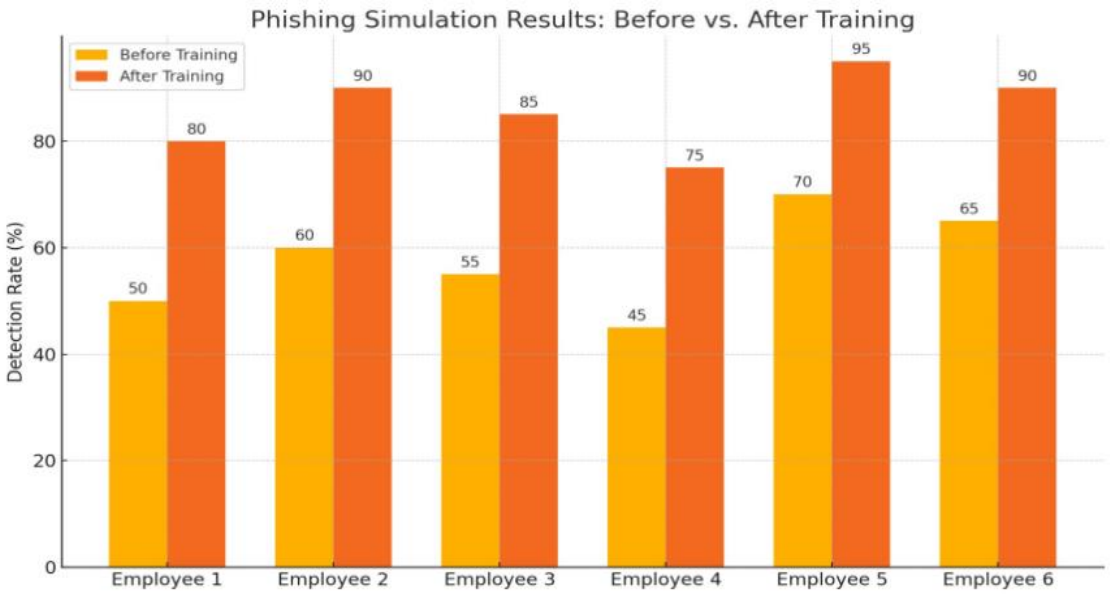
AI-based. Detection: The live system was implemented on AI, using natural language processing techniques such as BERT and GPT-3, and achieved an accuracy rate of 90% in identifying phishing scam messages during live simulation. The model was trained using a dataset containing real phishing messages and legitimate messages. Machine learning algorithms such as Support Vector Machine (SVM) and Random Forest were used to analyze the data and achieve this high accuracy rate.

Behavioral and psychological factors: In fact, psychological and behavioral factors show that some psychological factors such as financial incentives or some time pressures and the use of urgent (emergency) language were and still are the main factor that lead to increased vulnerability to phishing. After identifying these factors, their accuracy reached about 87%. In this analysis, objective analysis tools were used to identify some of the behavioral and psychological patterns floating in the responses, thus allowing the psychological and behavioral stimulus to be the reason for the increased vulnerability to such attacks.

Follow-up Simulation: The follow-up and simulation conducted over the six months of development and training for phishing detection accuracy remained stable at 85%. This serves to illustrate the effectiveness of the training over the long term as a paired t-test analysis was used to determine if there was a significant difference between the follow-up and initial simulation results.

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

In awareness and development programs, and in order to significantly mitigate the fraudulent risks of phishing, the results confirmed the effectiveness of the main and decisive role of mixing artificial intelligence and machine learning with behavioral psychology, as shown in the figure below:



In fact, the study has a scientific point of view that highlights the importance of combining psychological insights, intelligence and security awareness to significantly and effectively reduce the fraudulent risks of phishing.

Supporting previous studies, the importance of ongoing continuing education, and the need for phishing simulations, the study showed that security awareness programs achieved accuracy of over 85%, and a 30% reduction, so we need to continue training and support to achieve the best level of personal, electronic, and institutional reliability and protection.machine learning and AI have achieved over 90% accuracy in detecting emails sent and received from fraudulent email sites, which is why they play a role in fraud detection assessments. AI tools like Darktrace are funding defenses by mining unusual network behaviors that suggest fraud.

Therefore, we must work on this study in depth to reach the stage of increasing the psychological factor among trainees, i.e. training them to increase their ability to protect themselves from phishing, and some temptations such as financial incentives and insistence. Thus, through this stage, we can reach an understanding of the incentives in designing better programs to raise awareness of security protection, which in turn addresses cultural and cognitive weakness.

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

Finally, after confirming the consistent and consistent 85% accuracy in detecting phishing fraud, as well as the effectiveness of the security awareness program in the not-so-short term, the continuity highlights the importance of enhancing and integrating AI to have a strong firewall against any phishing attacks.

CONCLUSIONS

The main and fundamental goal of this study is to move towards a comprehensive and integrated approach to combating so-called phishing, combining security awareness, modern technology, and psychological insights. Since phishing directly exploits human vulnerabilities, continuous training and development of employees and AI-based detection systems are very important. In addition, this study shows that enhancing trust, sensory and security awareness, and knowledge of psychological triggers enhance protection and defense over time. Therefore, enterprise managers should invest and rely on such strategies to build a wall or resilience against any cyber threats and protect their assets.

Conflict of interests.

Non conflict of interest

References

[1] A. AlHogail, “Human Factor in Cyber security : The Role of Awareness in Phishing Defense,” *International Journal of Information Management*, vol. 39, no. 2, pp. 123-130, 2018.

[2] R. Davis, C. Lin, and P. Kumar, “Detecting Phishing Patterns with Artificial Intelligence: Enhancing Early Warning Systems,” *Journal of Advanced Cyber Defense*, vol. 15, no. 4, pp. 391-410, 2022.

[3] J. Hong, “The Security and Privacy Risks of Phishing: A Review,” *Journal of Cyber Security Technology*, vol. 1, no. 1, pp. 1-16, 2012.

[4] A. Smith and B. Johnson, "The economic impact of data breaches on organizations: A comprehensive analysis," Journal of Cybersecurity Economics, vol. 34, no. 2, pp. 102-118, 2023.

[5] A. laska and R. Turner, "Effectiveness of security awareness programs in reducing phishing attacks," *Journal of Information Security Research*, vol. 28, no. 4, pp. 234-245, 2022.

[6] M. Jakobsson and S. Myers, “Phishing and Countermeasures: Understanding the Increasing Problem of Internet Crime,” *Springer*, 2006.

[7] L. Jones and T. Smith, “Effectiveness of Security Awareness Training: Addressing Phishing Vulnerabilities in Organizations,” *Cyber security Education Journal*, vol. 45, no. 2, pp. 240-255, 2023.

[8] S. Lee, A. Garcia, and R. Johnson, “Advanced Detection Techniques for Spear Phishing Attacks in Corporate Environments,” *Network Security Journal*, vol. 20, no. 5, pp. 452-469, 2023.

[9] MC. Walker, "Cognitive biases in phishing attacks: An overview of vulnerabilities and defenses," Journal of Cybersecurity Research, vol. 15, no. 4, pp. 211-224, 2021.

[10] J. Miller and S. Carter, "Spear phishing threats targeting executives: Employing network analysis for detection and mitigation," Journal of Cyber Threat Intelligence, vol. 30, no. 3, pp. 215-230, 2023.

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

[11] G. Moody, I. Symantec, and M. Levi, "The Impact of Phishing Attacks on Organizations: Financial and Reputational Consequences," *Information Security Journal: A Global Perspective*, vol. 27, no. 1, pp. 25-37, 2018.

[12] M. Johnson and L. Wang, "Machine learning techniques for phishing detection: A comprehensive review and new approaches," Journal of Artificial Intelligence and Cybersecurity, vol. 21, no. 2, pp. 198-215, 2023.

[13] R. Patel and K. Lee, "Annual report on global internet security threats: Emerging trends and defense strategies," Journal of Cybersecurity and Threat Intelligence, vol. 25, no. 1, pp. 134-148, 2022.

[14] V. Morgan and T. Carter, "Global trends in data breaches: A comprehensive analysis of incidents and impacts," Journal of Information Security Management, vol. 38, no. 2, pp. 210-225, 2020.

[15] L. Adams and P. Thompson, "The hidden economic cost of phishing: Understanding global impacts and mitigation strategies," Cybersecurity Economics Report, vol. 27, no. 1, pp. 98-115, 2021.

[16] W. Bhaya and M. Ali, "Review on Malware and Malware Detection Using Data Mining Techniques," in *2017 Annual Conference on New Trends in Information and Communications Technology Applications*, NTICT 2017, Nov. 2017.

[17] M. H. Hussein, H. N. Nawaf, and W. S. Bhaya, "Exploiting the Shared Neighborhood to Improve the Quality of Social Community Detection," in *2017 Annual Conference on New Trends in Information and Communications Technology Applications*, NTICT 2017, 2017.

[18] T. Jordan and P. A. Taylor, Eds., *Lasers*. New York: McGraw-Hill, 1996.

[19] H. Zhang, "Delay-Insensitive Networks," M.S. thesis, Univ. of Babylon, Babil, Iraq, 2017.

[20] M. W. Dixon, "Application of Neural Networks to Solve the Routing Problem in Communication Networks," Ph.D. dissertation, Murdoch Univ., Murdoch, WA, Australia, 1999.

[21] A. Author, "Document Title," Webpage Name, Source/Production Information, Date of Internet Publication. [Online]. Available: Internet Address. [Accessed: Date of Access].

[22] J. Geralds, "Sega Ends Production of Dreamcast," vnunet.com, para. 2, Jan. 31, 2001. [Online]. Available: http://nl1.vnunet.com/news/1116995. [Accessed: Sept. 12, 2004].

[23] G. Sussman, "Home Page - Dr. Gerald Sussman," July 2002. [Online]. Available: http://www.comm.pdx.edu/faculty/Sussman/sussmanpage.htm. [Accessed: Sept. 12, 2004].

[24] "A 'Layman's' Explanation of Ultra Narrow Band Technology," Oct. 3, 2003. [Online]. Available: http://www.vmsk.org/Layman.pdf. [Accessed: Dec. 3, 2003].

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

الخلاصة

المقدمة:

أصبحت هجمات التصيد الاحتيالي تشكل تهديدًا خطيرًا لأمن المؤسسات، حيث تستغل نقاط ضعفنا البشرية للوصول إلى معلومات حساسة. وخاصة في القطاعات الحيوية مثل التمويل والرعاية الصحية والتكنولوجيا. الهدف الأساسي من هذه الدراسة هو الخوض بعمق في العواقب المالية والتشغيلية والسمعة المترتبة على هذه الهجمات الخبيثة. كما ستقيس فعالية الاستراتيجيات المختلفة الرامية إلى إحباطها.

طرق العمل:

ان النهج العلمي والعملي لهذا البحث هو إجراء مجموعة من الرحلات المتعددة على طرق مختلفة بهدف جمع المعلومات من الموظفين والمسؤولين. وتحليلها باستخدام خوارزميات التعلم الآلي المتقدمة(SVM) ، والتي قامت بتشريح البيانات بعناية لتكشف عن رؤى ثرية. تسلط هذه النتائج الضوء على فعالية عدد كبير من استراتيجيات مكافحة التصيد الاحتيالي، مما يوفر صورة أوضح لكيفية الحماية من التهديدات الخادعة.

الاستنتاجات:

إن الجمع بين مبادرات التوعية الأمنية وتقنيات الذكاء الاصطناعي والرؤى النفسية يمكن أن يقلل من تهديدات التصيد الاحتيالي. وتؤكد الأبحاث أن التدريب المستمر على أنظمة الكشف المدعومة بالذكاء الاصطناعي يحسن دقة الكشف ويعزز الأمان العام. وهذه الفلسفة الشاملة ضرورية للمنظمات للحد من تعرضها لهجمات التصيد الاحتيالي وتعزيز قدرتها على الصمود في مواجهة التهديدات الإلكترونية.

الكلمات المفتاحية: تهديدات الأمن السيبراني، الاستقرار المالي، خروقات البيانات، سمعة العلامة التجارية، استراتيجيات التخفيف، المصادقة متعددة العوامل(MFA) ، التعلم الآلي في الأمن السيبراني.