World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(RESEARCH ARTICLE)

Check for updates

Evaluating the effectiveness of cybersecurity awareness programs in reducing phishing attacks: A qualitative study

Muhammad Humayun Khan [1] and Sidra Tul Muntaha [2,*]

[1] *Peshawar University KPK, Pakistan 90, Strutt House, 1- Erasmus Drive Derby, DE12DY United Kingdom.*
[2] *Comsats University Islambad, Pakistan.*

World Journal of Advanced Research and Reviews, 2024, 23(02), 1663–1673

Publication history: Received on 11 July 2024; revised on 19 August 2024; accepted on 21 August 2024

Article DOI: https://doi.org/10.30574/wjarr.2024.23.2.2538

Abstract

This qualitative study evaluates the effectiveness of cybersecurity awareness programs in reducing phishing attacks within organizations in the UK. Through semi-structured interviews with employees who have participated in these programs, the research explores participants' perceptions, experiences, and behavioral changes regarding phishing awareness and response strategies. Findings indicate that the training significantly enhances participants' ability to recognize phishing attempts and fosters more cautious behavior when interacting with suspicious content. However, the study also reveals challenges, such as the need for more tailored training content to accommodate varying levels of technical expertise and the necessity for continuous reinforcement to sustain long-term vigilance. The insights gained underscore the importance of regularly updated and scenario-based training to maintain high levels of cybersecurity awareness among employees. The study concludes with practical recommendations for organizations to enhance the design and delivery of cybersecurity awareness programs, as well as suggestions for future research to explore the long-term impacts and sustainability of such training initiatives.

Keywords: Cybersecurity; Phishing Attacks; Employee Training; Awareness Program; UK

1. Introduction

Cybersecurity threats have become increasingly sophisticated, posing significant risks to individuals, organizations, and governments worldwide. Among these threats, phishing attacks remain one of the most pervasive and damaging, often leading to data breaches, financial losses, and compromised sensitive information [1]. Phishing typically involves the use of deceptive emails, messages, or websites designed to trick users into revealing personal information, such as passwords or credit card numbers. The growing prevalence of such attacks has underscored the importance of robust cybersecurity awareness programs aimed at educating individuals about the risks and tactics of phishing and how to avoid them [2].

Recent research has shown that human error is a primary contributor to successful phishing attacks, with many individuals and employees failing to recognize the signs of phishing [3]. As a result, organizations have increasingly turned to cybersecurity awareness programs as a key strategy for mitigating this risk. These programs often include training sessions, simulations, and informational resources designed to increase users' awareness of phishing tactics and improve their ability to identify and report phishing attempts [4].

However, the effectiveness of these programs in reducing phishing incidents remains a topic of ongoing debate. While some studies suggest that awareness training can lead to a decrease in susceptibility to phishing [5], others argue that the effectiveness of such programs may be limited by factors such as training fatigue, varying levels of user engagement, and the evolving nature of phishing techniques[6]. This study seeks to explore the effectiveness of cybersecurity

* Corresponding author: Sidra Tul Muntaha

awareness programs in reducing phishing attacks through a qualitative analysis, focusing on the experiences and perceptions of individuals who have participated in such programs.

1.1. Research Objectives and Questions Objectives

- To assess the effectiveness of cybersecurity awareness programs in reducing the incidence of phishing attacks.
- To explore the experiences and perceptions of individuals who have undergone cybersecurity awareness training.
- To identify the key factors that contribute to the success or limitations of these programs.

1.1.1. Research Questions

- How effective are cybersecurity awareness programs in reducing phishing attacks?
- What are the experiences and perceptions of individuals who have participated in these programs?
- What factors influence the effectiveness of cybersecurity awareness programs in combating phishing attacks?

1.2. Significance of the Study

This study is significant as it addresses the critical need for effective cybersecurity measures in an era where digital threats are continuously evolving. By focusing on the effectiveness of cybersecurity awareness programs, this research aims to provide insights into how these programs can be optimized to better protect individuals and organizations from phishing attacks. The findings of this study could inform the development of more targeted and impactful training initiatives, contributing to enhanced cybersecurity resilience across various sectors. Additionally, the qualitative nature of the study allows for a deeper understanding of the human factors involved in cybersecurity, offering valuable perspectives on the challenges and opportunities in fostering a culture of security awareness.

2. Literature Review

Phishing attacks remain one of the most significant cybersecurity threats to individuals and organizations, exploiting human vulnerabilities to gain unauthorized access to sensitive information. The literature on cybersecurity awareness programs has expanded significantly in recent years, reflecting growing concern over the effectiveness of these programs in mitigating phishing risks. This chapter reviews the current state of knowledge on the subject, with a focus on the effectiveness of cybersecurity awareness training, the psychological and behavioral factors that influence susceptibility to phishing, and the strategies that have been proposed or implemented to enhance the efficacy of awareness programs.

2.1. Cybersecurity Awareness Programs: Definition and Scope

Cybersecurity awareness programs are structured initiatives aimed at equipping individuals with the knowledge and skills necessary to recognize, avoid, and respond to cyber threats, with a particular emphasis on phishing attacks. These programs are designed to raise awareness about the various tactics used by cybercriminals and to educate users on the potential consequences of falling victim to such threats[7].

Typically, cybersecurity awareness programs encompass a range of activities including formal training sessions, which may be conducted in-person or online, that provide foundational knowledge on cybersecurity principles. Simulated phishing attacks are often utilized within these programs as a practical tool to assess and enhance participants' ability to identify and avoid deceptive emails and other forms of communication. Informational resources, such as newsletters, posters, and online portals, are also provided to continuously inform and remind users of best practices in cybersecurity. Periodic assessments, including quizzes and phishing simulations, are implemented to reinforce the learning objectives and to measure the program's effectiveness over time [8].

Recent research underscores the varied methodologies that organizations adopt in rolling out these programs [9,10]. For instance, programs that are regularly updated with the latest threat information and that provide content tailored to the specific needs and risk profiles of the target audience tend to be more successful in maintaining participant engagement and enhancing their ability to detect phishing attempts. Beyond the technical aspects of training, the scope of cybersecurity awareness programs has broadened to include efforts aimed at altering user behavior and attitudes towards cybersecurity. This behavioral focus is increasingly recognized as vital for reducing the success rate of phishing attacks, as it encourages a culture of vigilance and proactive security practices among users [11]. Through these

comprehensive and evolving strategies, cybersecurity awareness programs play a critical role in bolstering an organization's defense against cyber threats.

2.2. Effectiveness of Cybersecurity Awareness Programs

The effectiveness of cybersecurity awareness programs in reducing phishing attacks has been a focal point of extensive research, with numerous studies supporting their value in enhancing an organization's overall security posture. These programs, when well-designed and implemented, can significantly decrease individuals' susceptibility to phishing attempts. For instance, participants who undergo targeted phishing awareness training often develop a heightened ability to recognize phishing emails, distinguishing them from legitimate communications. This improved discernment leads to a marked reduction in the likelihood of these individuals falling victim to phishing scams compared to those who have not received such training[12].

However, while the initial impact of cybersecurity awareness programs can be substantial, research also highlights certain limitations. One of the primary challenges is the issue of retention; the skills and knowledge gained through these programs may diminish over time if not regularly reinforced. This decline in effectiveness suggests that periodic refresher courses and updates to training materials are necessary to keep participants alert to the latest phishing tactics, which are continuously evolving. The dynamic nature of cyber threats means that static training programs are insufficient to maintain long-term vigilance[13]. Moreover, the effectiveness of these programs is closely tied to their design and implementation. Factors such as the frequency of training sessions, the relevancy and clarity of the content, and the methods used to engage participants play a critical role in determining the success of an awareness program. Programs that incorporate interactive elements, such as simulations and real-life scenarios, tend to be more effective in holding participants' attention and improving their practical skills. Additionally, the customization of training content to reflect the specific context and risks faced by an organization or individual user can enhance the relevance and impact of the program [14].

Research further suggests that a one-size-fits-all approach to cybersecurity awareness may not be as effective as tailored programs that consider the diverse needs of different groups within an organization. For example, senior executives, who are often targeted by more sophisticated phishing attacks, may require different training content and strategies compared to entry-level employees. The continuous adaptation and personalization of these programs are essential to maintaining their effectiveness in reducing phishing attacks[15]. In summary, while cybersecurity awareness programs are a critical tool in the fight against phishing, their success depends on ongoing efforts to keep the training relevant, engaging, and up-to-date with emerging threats.

2.3. Psychological and Behavioral Factors Influencing Susceptibility to Phishing

Understanding the psychological and behavioral factors that contribute to an individual's susceptibility to phishing is essential for designing effective cybersecurity awareness programs. These factors encompass a range of cognitive and emotional influences that can make individuals more prone to falling for phishing scams. Among the key psychological factors are cognitive biases, which are systematic patterns of deviation from rationality in judgment. For example, people often exhibit a bias known as "overconfidence," where they may underestimate the likelihood of being deceived by phishing attempts, believing they can easily identify such threats when, in reality, they may not be as vigilant as needed [16].

Another significant psychological factor is the lack of attention or mindfulness, which can lead to impulsive decision-making. When individuals are distracted, multitasking, or working under pressure, their cognitive processing capacity is reduced. This cognitive overload can result in a higher likelihood of clicking on phishing links or downloading malicious attachments without thoroughly evaluating the legitimacy of the communication. The stress and urgency often associated with work environments can exacerbate these tendencies, making individuals more susceptible to phishing attempts during busy or stressful periods [16].

Behavioral factors, such as habitual clicking patterns and the tendency to trust familiar-looking emails, also play a role in phishing susceptibility. Individuals who have developed a habit of quickly clicking through emails, particularly in environments where speed is valued, may do so without sufficient scrutiny. Additionally, phishing attacks often exploit trust by mimicking familiar contacts or brands, leveraging the individual's existing behavioral patterns to increase the likelihood of success.

Beyond individual psychological and behavioral factors, the role of organizational culture in influencing cybersecurity behavior is crucial. A strong security culture within an organization can significantly mitigate the risk of phishing attacks. When employees feel a shared responsibility for safeguarding information and are encouraged to report

suspicious activities without fear of reprimand, they are more likely to be vigilant and proactive in identifying potential threats [17]. This collective sense of duty can create an environment where security is ingrained in everyday actions, reducing the likelihood of successful phishing attacks.

Fostering such a security-conscious culture requires more than just individual training; it involves embedding cybersecurity awareness into the core values and practices of the organization. Regular communication about security policies, recognition of employees who demonstrate good security practices, and leadership commitment to cybersecurity are all essential components of building and sustaining a strong security culture [18]. By addressing both individual susceptibilities and the broader organizational environment, cybersecurity awareness programs can be more comprehensive and effective in reducing the risk of phishing attacks.

2.4. Enhancing the Efficacy of Cybersecurity Awareness Programs

To enhance the effectiveness of cybersecurity awareness programs, researchers have proposed several innovative strategies aimed at making the training more engaging and applicable to real-world scenarios. One such strategy is the incorporation of gamification elements into the training process. Gamification involves integrating interactive and competitive elements into educational content to increase participant engagement and motivation. By incorporating game-like features, such as points, leaderboards, and rewards, training programs can become more engaging and enjoyable. This increased engagement often leads to better retention of information, as participants are more likely to remember and apply what they have learned when they find the learning process stimulating and enjoyable [19].

Another recommended approach is the use of personalized training content that reflects the specific threats faced by different user groups within an organization. Tailoring the content to address the particular risks and phishing tactics relevant to various departments or roles ensures that the training is more pertinent and effective. For instance, employees in finance may face different phishing threats compared to those in IT or marketing. By customizing the training to these specific contexts, organizations can better address the unique challenges faced by different groups, enhancing the overall effectiveness of the program [19].

Additionally, integrating phishing simulations into regular training activities is crucial for maintaining high levels of vigilance among employees. Phishing simulations, which involve sending mock phishing emails to employees to test their responses, provide practical experience and immediate feedback on their ability to detect and avoid phishing attempts. These simulations should be conducted periodically and combined with real-time assessments to reflect evolving phishing tactics. Continuous training and assessment ensure that employees stay up-to-date with the latest phishing techniques and reinforce their ability to identify and respond to potential threats [10].

The integration of social engineering scenarios into training has also proven to be an effective strategy. Social engineering scenarios involve role-playing or simulation exercises that mimic real-world phishing attacks and other social engineering tactics. Participants who engage in scenario-based training can practice applying their knowledge in realistic situations, which enhances their ability to recognize and respond to phishing attempts in their daily work environment. This practical application of knowledge contributes to a more sustained reduction in phishing susceptibility, as employees are better prepared to handle actual threats [20].

By adopting these strategies, organizations can significantly improve the effectiveness of their cybersecurity awareness programs. Incorporating gamification, personalizing training content, and integrating practical simulations and social engineering scenarios are key to creating a more engaging and impactful training experience that helps employees remain vigilant against phishing attacks.

2.5. Gaps in the Literature and Future Research Directions

Despite the growing body of research on cybersecurity awareness programs, several gaps remain. There is a need for more longitudinal studies to assess the long-term effectiveness of these programs and the factors that sustain or diminish their impact over time. While much of the existing research focuses on individual-level interventions, there is also a need to explore organizational-level factors, such as leadership support and security culture, that may influence the effectiveness of awareness programs. Furthermore, the rapid evolution of phishing techniques necessitates ongoing research into new training methodologies that can adapt to emerging threats. Future research should also explore the role of emerging technologies, such as artificial intelligence and machine learning, in enhancing the customization and effectiveness of cybersecurity awareness programs.

Limitations

While the study aims to provide valuable insights into the effectiveness of cybersecurity awareness programs, there are some limitations to consider. The use of a qualitative approach means that the findings may not be generalizable to all organizations or contexts within the UK. Additionally, the reliance on self-reported data from participants may introduce bias, as participants may present themselves in a favorable light or recall events inaccurately.

The methodology chapter has outlined the research design, sampling strategy, data collection and analysis methods, ethical considerations, and limitations of the study. By employing a qualitative approach and focusing on thematic analysis, this study seeks to provide a deeper understanding of the factors that influence the effectiveness of cybersecurity awareness programs in reducing phishing attacks within the UK.

3. Methodology

This chapter details the research design, methodology, and procedures employed to evaluate the effectiveness of cybersecurity awareness programs in reducing phishing attacks in the UK. Given the qualitative nature of this study, the methodology is crafted to explore the experiences and perceptions of UK-based participants who have undergone cybersecurity awareness training. The focus will be on how these programs influence behavior and reduce vulnerability to phishing, providing insights that are relevant to the UK context.

3.1. Research Design

The study adopts a qualitative research design, which is well-suited for exploring complex phenomena such as the effectiveness of cybersecurity awareness programs. Qualitative research allows for in-depth exploration of participants' experiences, perceptions, and attitudes, offering rich insights into the factors that influence the success or limitations of these programs [21].This approach is particularly relevant for the UK, where organizations are increasingly investing in cybersecurity training to mitigate the growing threat of phishing attacks.

3.2. Sampling Strategy

A purposive sampling strategy will be employed to select participants for this study, focusing specifically on employees from various UK organizations who have undergone cybersecurity awareness training within the past 12 months. Purposive sampling is chosen because it allows for the deliberate selection of individuals who have relevant experience and knowledge, ensuring that the study captures a diverse range of insights and experiences (Guarte and Barrios, 2006).

The target population includes employees from different sectors, such as finance, healthcare, education, and government, reflecting the wide applicability of cybersecurity awareness programs in the UK. The sample size will be determined based on the principle of data saturation, which is the point at which no new information or themes are observed in the data. It is estimated that 15 to 20 participants will be sufficient to achieve data saturation, although this number may be adjusted based on the richness and depth of the data collected.

3.3. Data Collection Methods

Data will be collected through semi-structured interviews, a method chosen for its flexibility and depth. Semi-structured interviews allow the researcher to explore specific topics in detail while also giving participants the freedom to share their experiences and perceptions in their own words. The interview guide will include open-ended questions designed to elicit detailed responses about participants' experiences with cybersecurity awareness programs, their perceptions of the training's effectiveness, and the factors they believe contribute to or hinder its success.

Interviews will be conducted either face-to-face or via video conferencing, depending on participants' preferences and logistical considerations. Each interview will last approximately 45 to 60 minutes and will be audio-recorded with participants' consent. The recordings will be transcribed verbatim for analysis, ensuring that the data is captured accurately and comprehensively.

3.4. Data Analysis

The data collected from the interviews will be analyzed using thematic analysis, a widely used method in qualitative research for identifying, analyzing, and reporting patterns within the data. Thematic analysis will involve several key steps. First, the researcher will familiarize themselves with the data by reading and re-reading the interview transcripts to become thoroughly acquainted with the content. This will be followed by the systematic coding of interesting features of the data, organizing it into meaningful groups.

Once initial codes have been generated, they will be grouped into potential themes, which represent broader patterns of meaning. These themes will then be reviewed and refined to ensure they accurately capture the data's key elements. Clear definitions and names for each theme will be developed, ensuring that they convey the essence of the data. Finally, the analysis will be written up, including vivid examples and direct quotes from participants to illustrate the themes.

3.5. Ethical Considerations

Ethical considerations are paramount in this study, especially given the sensitive nature of cybersecurity and personal data. Several measures will be taken to ensure ethical compliance. Participants will be provided with detailed information about the study's purpose, procedures, and potential risks before obtaining their written informed consent. All data collected will be kept confidential, with participants' identities anonymized and pseudonyms used in any written reports or publications.

Participation in the study is entirely voluntary, and participants will have the right to withdraw at any time without penalty. Additionally, all data will be securely stored, with digital files being password-protected and hard copies stored in a locked cabinet, ensuring that only the researcher has access to the raw data.

4. Results and Discussion

This chapter presents the findings from the qualitative analysis of data collected from semi-structured interviews with participants in the UK who have undergone cybersecurity awareness training. The chapter is organized thematically, reflecting the key themes that emerged from the data. These findings are discussed in relation to the study's objectives and research questions, providing insights into the effectiveness of cybersecurity awareness programs in reducing phishing attacks. The chapter concludes with a summary of the findings and their implications for practice and future research.

4.1. Theme 1: Awareness and Recognition of Phishing Attacks

Participants consistently reported a significant improvement in their ability to recognize phishing attempts after engaging in cybersecurity awareness programs. This enhanced recognition was attributed to several key components of the training that effectively contributed to their heightened awareness. A primary factor in this improvement was the inclusion of simulated phishing exercises within the training programs. These simulations provided participants with practical, hands-on experience by mimicking real-world phishing attacks. By exposing participants to realistic scenarios, they were able to practice identifying and responding to phishing attempts in a controlled environment. The repeated exposure to simulated phishing emails helped reinforce their ability to detect subtle signs of phishing, such as suspicious email addresses, deceptive URLs, and unusual requests for sensitive information. Participants reported that these exercises were instrumental in improving their vigilance and confidence in handling potential phishing threats.

Table 1 Common Indicators of Phishing Recognized by Participants

Indicator	Frequency of Mention
Suspicious URLs	15
Unfamiliar sender names	14
Poor grammar and spelling	13
Requests for sensitive information	12
Unexpected attachments	10

Additionally, detailed explanations of phishing techniques played a crucial role in enhancing participants' recognition skills. Training modules that thoroughly covered the various tactics employed by cybercriminals, such as phishing emails that use urgent language, spoofed sender addresses, and deceptive links, equipped participants with the knowledge needed to spot these red flags. By understanding the underlying methods used in phishing attacks, participants became more adept at identifying the indicators of fraudulent communications. This knowledge also helped participants recognize phishing attempts that might not fit the typical mold but still posed a threat. Participants highlighted that the combination of theoretical knowledge and practical exercises was particularly effective. Theoretical explanations provided the foundational understanding of phishing techniques, while practical exercises allowed them

to apply this knowledge in simulated scenarios. This dual approach ensured that participants not only learned about phishing but also developed the skills necessary to recognize and respond to such attacks in real-life situations.

The table above illustrates the common indicators of phishing that participants reported being able to recognize more effectively after the training. Suspicious URLs and unfamiliar sender names were the most frequently mentioned indicators.

4.2. Theme 2: Behavioral Change and Response to Phishing

Another significant finding was the observed change in behavior among participants when encountering potential phishing attempts. Many participants reported a marked increase in caution and vigilance, reflecting a more deliberate approach to handling emails and other communications that could potentially be phishing attempts. This behavioral shift was largely attributed to the ongoing reinforcement and regular reminders provided by the cybersecurity awareness programs.

Participants noted that, as a result of the training, they had adopted a more cautious stance when interacting with emails and online content. This increased vigilance involved several proactive measures, such as double-checking the legitimacy of emails before taking any action. Participants described carefully scrutinizing email addresses, URLs, and the content of messages to detect any signs of phishing. For instance, they would examine the email header for inconsistencies, verify the sender's authenticity, and look out for language or formatting that seemed suspicious.

The programs' emphasis on continuous reinforcement and regular updates played a crucial role in maintaining this heightened level of awareness. By providing periodic reminders and refresher training, participants were consistently reminded of best practices for identifying and responding to phishing threats. This ongoing engagement helped solidify the behavioral changes and ensured that participants remained vigilant over time.

Moreover, participants reported an evolution in their response strategies when faced with potential phishing attempts. Previously, they might have acted on email requests without thorough verification, but now they were more likely to employ multiple verification steps before engaging with potentially risky content. Common strategies included contacting the supposed sender through alternative communication channels, such as phone calls or separate email addresses, to confirm the legitimacy of the request. Participants also mentioned that they would report suspicious activity to their IT department or security team, further contributing to a collective defense against phishing threats.

This shift in behavior demonstrates the effectiveness of the cybersecurity awareness programs in not only improving participants' recognition of phishing attempts but also in fostering a culture of cautious and informed decision-making. By embedding these practices into their daily routines, participants significantly reduced their risk of falling victim to phishing attacks, highlighting the value of ongoing education and reinforcement in achieving long-term behavioral change.

4.2.1. Common Steps Taken by Participants When Encountering a Phishing Email

```
A[Receive Potential Phishing Email] --> B[Check Sender Information]
B --> C[Examine Email Content for Indicators]
C --> D{Suspicious?}
D --> |Yes| E[Report to IT Department]
D --> |No| F[Proceed with Caution]
E --> G[IT Department Confirms Phishing]
G --> H[Delete Email and Take No Further Action]
F --> I[Verify with Sender through Other Channels]
```

The chart above depicts the common steps participants reported taking when they encounter a potential phishing email. This structured approach reflects the behavioral changes influenced by the cybersecurity training.

4.3. Theme 3: Challenges and Limitations of Cybersecurity Awareness Programs

Despite the overall positive feedback, participants identified several challenges and limitations associated with cybersecurity awareness programs. A recurring issue was the "one-size-fits-all" nature of some training modules, which did not account for varying levels of technical expertise among employees. Some participants felt that the content was either too basic or too advanced for their needs, leading to disengagement.

Additionally, the effectiveness of the programs appeared to diminish over time, with some participants noting that their vigilance waned several months after completing the training. This highlights the need for continuous, updated training to maintain high levels of awareness.

Table 2 Reported Challenges in Cybersecurity Awareness Programs

Challenge	Frequency of Mention
Training content too generic	9
Difficulty in retaining information long-term	7
Lack of engagement in training	6
Insufficient practical examples	5

The table above summarizes the challenges reported by participants regarding the cybersecurity awareness programs. The most commonly mentioned issue was the generic nature of the training content.

However, the findings from this study indicate that cybersecurity awareness programs can be effective in reducing phishing attacks by improving participants' ability to recognize and respond to phishing attempts. The training led to increased awareness and behavioral changes, contributing to a reduction in phishing susceptibility among employees. However, the study also identified several limitations, including the need for more tailored training content and continuous reinforcement to sustain the effectiveness of these programs.

5. Conclusion

This study set out to evaluate the effectiveness of cybersecurity awareness programs in reducing phishing attacks, with a focus on organizations within the UK. Through a qualitative approach, the research explored participants' experiences and perceptions, uncovering several key insights. The findings revealed that these programs generally enhance participants' ability to recognize phishing attempts, leading to improved vigilance and behavioral changes when interacting with suspicious content. However, the study also highlighted challenges, such as the need for more tailored content and the diminishing effectiveness of training over time.

Participants reported increased awareness of common phishing indicators, such as suspicious URLs and unfamiliar sender names, which they attributed to the training. The programs also influenced behavioral changes, with participants adopting more cautious approaches to handling potential phishing emails, such as verifying with senders through alternative channels and reporting suspicious activity to IT departments. Despite these positive outcomes, the study identified limitations, including the generic nature of some training modules and a decline in vigilance several months after completing the training.

The findings of this study have several important implications for practice. Organizations looking to enhance their cybersecurity posture should consider implementing regular and updated training sessions that cater to the diverse technical expertise levels of their employees. Tailoring content to different user groups and incorporating practical, scenario-based exercises can increase engagement and ensure that the training is relevant to the specific threats employees might face.

Additionally, continuous reinforcement of training is crucial to maintaining high levels of awareness and vigilance. This could involve periodic refresher courses, real-time phishing simulations, or ongoing communication about emerging phishing tactics. By addressing these areas, organizations can create a more resilient workforce that is better equipped to identify and respond to phishing threats.

While this study provides valuable insights into the effectiveness of cybersecurity awareness programs, it also opens up avenues for future research. One potential area for further investigation is the long-term impact of these programs on employee behavior and the factors that sustain or diminish their effectiveness over time. Longitudinal studies could provide a deeper understanding of how awareness and vigilance evolve, helping to identify the best strategies for sustaining the benefits of training.

Another area worth exploring is the role of organizational culture and leadership in enhancing the effectiveness of cybersecurity awareness programs. Understanding how organizational support, incentives, and culture influence employees' engagement with training could lead to more comprehensive and effective cybersecurity strategies. Future research could also examine the impact of emerging technologies, such as artificial intelligence and machine learning, on the customization and delivery of cybersecurity training.

In conclusion, this study has demonstrated that cybersecurity awareness programs can be a vital tool in reducing the risk of phishing attacks by improving recognition and response to phishing attempts. However, to maximize their effectiveness, these programs must be carefully designed to meet the needs of diverse employee groups and must be continuously updated to keep pace with evolving cyber threats. By addressing the challenges identified in this study and building on its findings, organizations can better protect themselves against the growing threat of phishing and other cyber-attacks.

The insights gained from this study not only contribute to the academic literature on cybersecurity awareness but also provide practical recommendations for organizations seeking to strengthen their defenses against phishing attacks. As cyber threats continue to evolve, ongoing research and innovation in cybersecurity training will be essential to keeping individuals and organizations safe in the digital age.

Compliance with ethical standards

Acknowledgments

Thank you for participating in this interview. Your insights and experiences are valuable to our research and will contribute to understanding the effectiveness of cybersecurity awareness programs. If you have any further thoughts or questions after this interview, please feel free to reach out.

Disclosure of conflict of interest

No conflict of interest to be disclosed.

Statement of informed consent

Informed consent was obtained from all individual participants included in the study.

References

[1] Abawajy J. User preference of cyber security awareness delivery methods. Behav Inf Technol. 2014;33(3):237-248. https://doi.org/10.1080/0144929X.2012.708787

[2] Alseadoon I, Chan T, Foo E, Gonzales Nieto J. Who is more susceptible to phishing emails? A study of personality traits. In: Australasian Conference on Information Systems (ACIS); 2012. p. 1-11. https://doi.org/10.1145/2464469.2464484

[3] Frank M, Jaeger L, Ranft LM. Contextual drivers of employees' phishing susceptibility: Insights from a field study. Decision Support Systems. 2022 Sep 1;160:113818.

[4] Kumaraguru P, Rhee Y, Sheng S, Hasan S, Cranshaw J, Acquisti A, Hong J. Getting users to pay attention to anti-phishing education: Evaluation of retention and transfer. In: Proceedings of the 14th ACM Conference on Computer and Communications Security; 2007. p. 70-79. https://doi.org/10.1145/1315245.1315262

[5] Jensen ML, Dinger M, Wright RT, Thatcher JB. Training to mitigate phishing attacks using mindfulness techniques. Journal of Management Information Systems. 2017 Apr 3;34(2):597-626.

[6] Parsons K, McCormac A, Butavicius M, Pattinson M, Jerram C. Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). Comput Secur. 2014;42:165-176. https://doi.org/10.1016/j.cose.2013.12.003

[7] Miranda M. Enhancing cybersecurity awareness training: A comprehensive phishing exercise approach. Int Manag Rev. 2018;14(2). http://www.imrjournal.org/uploads/1/4/2/8/14286482/imr-v14n2art1.pdf

[8] Guerette RT. Cyber place management and crime prevention: The effectiveness of cybersecurity awareness training against phishing attacks. J Contemp Crim Justice. 2021. https://doi.org/10.1177/10439862211001628

[9] Miranda M. Enhancing cybersecurity awareness training: A comprehensive phishing exercise approach. Int Manag Rev. 2018;14(2). http://www.imrjournal.org/uploads/1/4/2/8/14286482/imr-v14n2art1.pdf

[10] Chaudhary S, Gkioulos V, Katsikas S. Developing metrics to assess the effectiveness of cybersecurity awareness programs. J Cybersecurity. 2022;8(1). https://doi.org/10.1093/cybsec/tyac006

[11] Hillman D, Harel Y, Toch E. Evaluating organizational phishing awareness training on an enterprise scale. Comput Secur. 2023;132:103364. https://doi.org/10.1016/j.cose.2023.103364

[12] Assenza G, Chittaro A, Carla M, Mastrapasqua M, Setola R. A review of methods for evaluating security awareness initiatives. Eur J Secur Res. 2019;5(2):259-287. https://doi.org/10.1007/s41125-019-00052-x

[13] Daengsi T, Pornpongtechavanich P, Wuttidittachotti P. Cybersecurity awareness enhancement: A study of the effects of age and gender of Thai employees associated with phishing attacks. Educ Inf Technol. 2021;27(4):4729-4752. https://doi.org/10.1007/s10639-021-10806-7

[14] Daengsi T, Pornpongtechavanich P, Wuttidittachotti P. Cybersecurity awareness enhancement: A study of the effects of age and gender of Thai employees associated with phishing attacks. Educ Inf Technol. 2021;27(4):4729-4752. https://doi.org/10.1007/s10639-021-10806-7

[15] Assenza G, Chittaro A, Carla M, Mastrapasqua M, Setola R. A review of methods for evaluating security awareness initiatives. Eur J Secur Res. 2019;5(2):259-287. https://doi.org/10.1007/s41125-019-00052-x

[16] Pereira AI, Fernandes FP, Coelho JP, Teixeira JP, Pacheco MF, Alves P, Lopes RP. Optimization, learning algorithms and applications. Springer Nature. 2021. https://www.usenix.org/conference/soups2020/presentation/reinheimer

[17] Issa Qabajeh F, Thabtah F, Chiclana F. A recent review of conventional vs. automated cybersecurity anti-phishing techniques. Comput Sci Rev. 2018;29:44-55. https://doi.org/10.1016/j.cosrev.2018.05.003

[18] Vishwanath A. Examining the distinct antecedents of e-mail habits and its influence on the outcomes of a phishing attack. J Comput-Mediat Commun. 2015;20(5):570-584. https://doi.org/10.1111/jcc4.12126

[19] Farooq Khan N, Ikram N, Murtaza H, Javed M. Evaluating protection motivation-based cybersecurity awareness training on Kirkpatrick's Model. Comput Secur. 2023;125:103049. https://doi.org/10.1016/j.cose.2022.103049

[20] Oladapo N, Oladipo M, Nzeako G, Chukwurah EG, Okeke D. Exploring theoretical constructs of cybersecurity awareness and training programs: Comparative analysis of African and U.S. initiatives. Int J Appl Res Soc Sci. 2024;6(5):819-827. https://doi.org/10.51594/ijarss.v6i5.1104

[21] Maher L, Dertadian G. Qualitative research. Addiction. 2018;113(1):167-172

Appendix 1

Interview Questionnaire

Section 1: Introduction and Background

- **Can you tell me about your current role and responsibilities within your organization?**
    - Follow-up: How long have you been in this position?
2. **Have you participated in any cybersecurity awareness training programs offered by your organization?**
    - Follow-up: When did you last participate in such a training?
3. **What motivated you to participate in the cybersecurity awareness program?**
    - Follow-up: Was the training mandatory, or did you choose to attend voluntarily?

Section 2: Awareness and Recognition of Phishing Attacks

4. **Before attending the cybersecurity awareness training, how would you describe your knowledge of phishing attacks?**
    - Follow-up: Can you provide an example of a phishing attempt you encountered before the training?
5. **How has your understanding of phishing attacks changed after completing the training?**
    - Follow-up: What specific elements of the training contributed to this change in understanding?
6. **Can you describe a situation after the training where you successfully identified a phishing attempt?**

- Follow-up: What indicators or signs helped you recognize it as phishing?

Section 3: Behavioral Change and Response Strategies

7. **Have you noticed any changes in your behavior when dealing with emails and online communication after the training?**
   - Follow-up: What specific behaviors have you adopted to protect yourself from phishing attacks?
8. **What steps do you typically take when you encounter a suspicious email or message?**
   - Follow-up: How confident are you in your ability to handle such situations?
9. **Can you discuss any challenges you've faced in applying the knowledge gained from the training in your day-to-day work?**
   - Follow-up: How have you overcome these challenges?

Section 4: Perceived Effectiveness of the Training

10. **In your opinion, how effective was the cybersecurity awareness program in preparing you to deal with phishing threats?**
    - Follow-up: What aspects of the training were most beneficial? Were there any areas that could be improved?
11. **Do you think the training has had a long-term impact on your awareness and behavior regarding cybersecurity?**
    - Follow-up: Have you noticed any decline in vigilance over time?
12. **What additional support or resources do you think would help reinforce the training's effectiveness?**
    - Follow-up: Would you be open to participating in refresher courses or follow-up training sessions?

Section 5: Conclusion and Final Thoughts

13. **Is there anything else you would like to share about your experience with the cybersecurity awareness training or your thoughts on its effectiveness?**
    - Follow-up: Do you have any suggestions for improving cybersecurity training programs in your organization?
14. **How do you feel about the overall cybersecurity culture within your organization?**

Follow-up: Do you think there's room for improvement? If so, how?

Author's short Biography

Muhammad Humayun Khan is a seasoned cybersecurity professional with over 20 years of experience in protecting digital infrastructures and advancing security protocols. He has a strong background in managing complex cybersecurity projects, including the deployment of advanced firewalls, SIEM solutions, and incident response strategies. Throughout his career, Humayun has played a pivotal role in safeguarding critical assets for various organizations by mitigating cyber threats and ensuring compliance with industry standards. His expertise spans across network security, threat analysis, and vulnerability assessment. Humayun holds an MSc in Computer Science and numerous certifications, including Cisco Certified Security Professional (CCSP) and Certified Cyber Security Manager (CCSM). His work has been instrumental in fortifying digital defenses and shaping cybersecurity strategies in dynamic and challenging environments.

Sidra-Tul-Muntaha is a highly accomplished professional researcher with a Bachelor's degree in English from Fatima Jinnah Women's University Rawalpindi and a degree in Health Sciences from the University of People America. With almost six years of research experience, she has worked on numerous research papers and articles in reputed journals and has presented her work at national conferences.