CyberWise: Virtual Security Learning Platform

Payton Howard, Mark Ferraro and Sajal Bhatia[a]
School of Computer Science and Engineering, Sacred Heart University, Fairfield, CT, U.S.A.

Keywords: Cybersecurity, Awareness, Training, Learning Platform.

Abstract: Security awareness training is a crucial aspect of ensuring and upholding the confidentiality, integrity, and availability of systems. This project addresses the need for improved security awareness training among staff and faculty members at the university. Our learning platform, CyberWise, leverages a virtual machine in conjunction with a Blackboard course to provide hands-on training modules for email security, secure browsing techniques, viruses, and password best practices. Participants in the CyberWise learning platform engage in realistic scenarios designed to improve learning comprehension about security best practices. The results of CyberWise demonstrated significant improvements in participants' confidence and skills in key areas of cybersecurity. Participants also indicated a high likelihood of applying the training to their daily work, with 90% feeling very or extremely likely to do so. CyberWise contributes to the field of cybersecurity by providing an effective, hands-on solution for security awareness training that allows staff and faculty members of the university to learn about security-related topics in an environment that looks and feels familiar to them. The interactive and simulation-based approach used in CyberWise not only serves to enhance user engagement, but also ensures a better application of security best practices compared to traditional training methods. This project underscores the value of immersive and practical training environments in the development of a robust security culture within higher educational institutions.

1 INTRODUCTION

In today's digital landscape, cybersecurity awareness is more important than ever. As cyber threats continue to evolve and become increasingly sophisticated, the need for robust security practices within organizations has never been greater. Employees are often the first line of defense against cyber-attacks, making it crucial that they are equipped with the knowledge and skills to recognize and respond to potential threats. Despite this, many organizations face a significant gap in security awareness, leaving them vulnerable to phishing attacks, malware, and other security breaches.

This project addresses the critical need for enhanced security awareness training among staff and faculty members at the university. Traditional security training methods, often consisting of passive learning through boring videos or lectures, fail to engage users effectively and do not provide the hands-on experience needed to develop practical skills. As a result, there is a pressing need for a more interactive and immersive training platform that can bridge this gap.

The primary objective of this project is to develop CyberWise, an innovative learning platform that leverages virtual machine technology to deliver comprehensive, hands-on security awareness training to the staff and faculty members of the university. CyberWise is specifically created for a university project and aims to improve participants' understanding and application of security best practices through realistic scenarios and interactive modules. By focusing on key areas such as email security, secure browsing techniques, virus recognition and response, and password best practices, the platform seeks to equip users with the necessary skills to protect themselves and their organization from cyber threats.

Through the development and implementation of CyberWise, this project aims to demonstrate the effectiveness of immersive, simulation-based training in enhancing cybersecurity awareness and preparedness among university staff and faculty members.

The rest of the article is organized as follows. Section 2 gives background of this research along with a summary of recent pertinent previous work. Section 3 provides the methodology and implementation details of the proposed training platform. Section 4 gives a summary of the metrics used to evaluate the effectiveness of CyberWise. Section 5 provides the challenges encountered in implementing and evaluating CyberWise. Section 6 summarizes and discusses the ob-

[a] https://orcid.org/0000-0002-0380-0623

Howard, P., Ferraro, M. and Bhatia, S.
CyberWise: Virtual Security Learning Platform.
DOI: 10.5220/0013378400003899
Paper published under CC license (CC BY-NC-ND 4.0)
In *Proceedings of the 11th International Conference on Information Systems Security and Privacy (ICISSP 2025) - Volume 1*, pages 416-425
ISBN: 978-989-758-735-1; ISSN: 2184-4356

tained results. Finally, Section 7 concludes the article by providing a summary of the work and directions for future work in this area.

2 BACKGROUND AND LITERATURE REVIEW

As previously mentioned, security awareness training can be found in a variety of flavors across different institutional and enterprise environments. Most of the common security awareness training methods used today tend to be similar to one another, and are often implemented just to meet compliance requirements (Mikova et al., 2021). This approach can be dangerous, as training programs that simply "check the box" (Haney and Lutters, 2020) are not designed to ensure that training and skills stick with individuals who complete the training. Employees need to have a reason to care about security; training should communicate the business value of security best practices to the organization. Typical training methods often focus on videos followed by multiple-choice tests, which can cause individuals to pay less attention if the training itself is not engaging. This, in turn, can result in participants gaining minimal skills and knowledge, and even less in terms of long-term retention.

Although there were limited direct comparisons between our research and others, we identified specific and relevant elements in each case study that we reviewed and decided to apply said elements to CyberWise. One relevant research paper emphasized the importance of using a virtual environment, "Towards an Automated Security Awareness System in a Virtualized Environment" (Labuschagne and Eloff, 2012). In this study, an automated and virtualized environment was created to allow users to safely access the internet through a virtual machine. This virtual environment would restart to its original save state to ensure that each new user had a fresh, malware-free environment. Additionally, the study included a survey to collect data on users' security awareness, and the system analyzed user behavior and malware to assess security threats.

When comparing the aforementioned study to CyberWise, it is clear that there are some related aspects. The use of a virtual environment is a core part of each research project. However, CyberWise focuses more on using the virtual environment as a general overarching training tool, rather than as a tool used solely to improve internet safety. Additionally, the use of surveys is similar, as CyberWise also includes a survey in the first learning module to establish a baseline of a user's security awareness and a post-training survey to measure improvement. During the initial research phase of CyberWise, a priority was building a virtual security learning platform that would effectively improve the cybersecurity skills of staff and faculty at an institution. (Vykopal et al., 2022) proposed Smart Learning Environment (SLE) focused on strengthening cybersecurity skills of its users by implementation of adaptive training methods. This was accomplished using a digital training environment that allowed for proficiency of cybersecurity skills to be tested and for additional complexity to be implemented to enhance learning. The SLE was setup by instructors and allowed them to "supervise training activities in the virtual learning environment for students who perform these activities". Lee et. al (Lee et al., 2022) proposed a novel cybersecurity training platform called ICSTASY (Integrated Cybersecurity Training System) that focused on "scenario-based, interactive, and immersive cybersecurity training". ICSTASY would focus on editable scenarios, autonomous agents for realistic interactions, and robust evaluation processes. Each of these systems was limited in overall scope, complexity, and scale.

Another relevant research paper that was useful is (Alkhazi et al., 2022) "Assessment of the Impact of Information Security Awareness Training Methods on Knowledge, Attitude, and Behavior". This study examined four groups using a variety of different training methods, with a common denominator being that all groups received a lecture as part of their training. One group only received a lecture to serve as a baseline, while the remaining three groups had additional training methods: a video, a reading, or a game. Each group was assessed on three categories of improvement: knowledge, attitude, and behavior. All groups showed noticeable improvement in these three areas. The categories of improvement for each group were calculated to collect the overall median improvement and range of improvement for each group. The baseline group had a median improvement of 17.52% with a range of 12.01. The group that included a game in their training showed the greatest improvement and the lowest overall range, with a median improvement of 32.31% and a range of 4.52.

3 METHODOLOGY AND IMPLEMENTATION

A variety of platforms and software were used to build and complete the CyberWise virtual security learning platform. These technologies include Blackboard, Azure, RDP, Windows 10, Outlook, Python, and Chrome. Blackboard was chosen as the learning

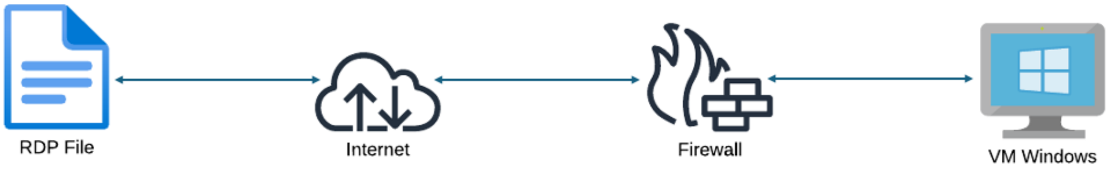

Figure 1: CyberWise Environment Setup.

platform because it is widely used by the university and many educational institutions for coursework and information accessibility. It provided an accessible platform for training participants to access learning modules, as all university staff and faculty have access to the software.

Azure was utilized to create and host the CyberWise Virtual Security Learning Platform. This allowed for streamlined management of the virtual environment, ensuring performance adjacent to that of a native system. RDP (Remote Desktop Protocol) was employed to enable participants to connect to the virtual training environment. Participants could run a provided RDP file and enter a password to access the virtual environment, which was based on a Windows 10 virtual machine. Windows 10 was selected due to its widespread use, ensuring that most participants would have some basic familiarity with the operating system.

Within the Windows environment, the Outlook desktop app was used for phishing training, allowing participants to access a realistic and live mailbox. Some training modules required customized scripts to properly explain and demonstrate concepts. For these purposes, CyberWise included customized Python scripts for simulating viruses and managing passwords. Finally, the Chrome browser was used for an internet-based module. Chrome was chosen because it is the most popular browser on Windows devices, providing a familiar interface for participants.

3.1 Environment Setup

When designing the CyberWise virtual lab environment, multiple key factors were considered, including ease of access, low cost, 24/7 availability, and a near-native experience. The options considered were a locally hosted device, Amazon AWS, and Microsoft Azure. The locally hosted option met all key factors except for providing a near-native experience, as the available hardware, being almost eight years old, did not offer sufficient performance. Therefore, while a locally hosted solution was useful for initial platform testing, it was not suited for long-term use by participants in the virtual training environment.

Midway through the CyberWise project, the decision was made to move to a cloud-based environment, and Microsoft Azure was chosen as it met all the key factors required. Azure offered ease of access, low cost, 24/7 availability, and a near-native experience.

The native Azure virtual machine resource was used to host the virtual environment. To keep costs relatively low while still providing a near-native virtual environment, the virtual machine was allocated 2 CPUs and 8GB of memory. The Windows 10 operating system was selected because it was less expensive than Windows 11 and most users were likely more familiar with Windows 10, given the ongoing transition between the two operating systems. The virtual environment was hosted in a data center located in Virginia to ensure that the environment was geographically close to CyberWise users, enhancing usability and responsiveness.

Once the virtual machine was created and running, firewall rules were configured. By default, Azure denies all inbound and outbound traffic. To secure the CyberWise environment, connections were restricted to the IP address space owned and operated by university. Specifically, connections from the 148.166.0.0/16 address space were allowed, and only port 3389 was open, with all other traffic denied by default. Port 3389 was chosen because it is the default port for Remote Desktop Protocol (RDP), which was used to connect to the virtual environment. RDP was selected as the ideal protocol/connection method because it provided CyberWise users with a graphical user interface (GUI) environment. Additionally, using RDP allowed users to access the virtual environment by simply opening an RDP file and entering the provided password.

3.2 Training Modules

For CyberWise training modules, we focused on four main areas: E-Mail Security, Password Best Practices, Secure Browsing Techniques, and Virus / Malware Awareness. Each learning module is broken down into two folders, a Concepts & Theory folder, and a Practical Application folder. In the Concepts & Theory folder, participants will find a variety of resources that will aid their overall comprehension of the respective learning module. In the Practical Application folder, participants will find a brief lab to complete within the learning environment, and a brief "exit" quiz to ensure adequate comprehension of the labs prior to moving onto the next module.

3.2.1 E-Mail Security

The e-mail security module equips participants with the knowledge and skills to identify and handle phishing attempts through a combination of theoretical resources and practical exercises (mic, b). Participants will explore fundamental concepts of e-mail security, learn best practices, and engage in hands-on activities within a virtual environment to apply their knowledge.

In the Concepts & Theory folder for the e-mail security module, participants will find valuable resources to understand the fundamentals of e-mail security. The first resource is a link to a comprehensive post on the Microsoft Security forum that covers the basics of email security, including its importance, benefits, best practices, and various types of email threats (mic, c). Following this, another link directs participants to a Microsoft page that offers guidance on protecting against phishing attacks. This page features a brief video overview of phishing and various dropdown menus covering topics such as identifying phishing messages and steps to take if they fall victim to a phishing attack. The final resource in this section is a document that explains how to report phishing emails using the Phish Alert feature in Outlook, tailored specifically for the university.

In the Practical Application folder, participants will find a detailed guide for a hands-on lab exercise and the practical assessment assignment. These activities are designed to enhance interaction with the training environment. Participants will follow step-by-step instructions to complete a lab within the virtual environment. They will use Outlook to examine a mailbox populated with emails created using an email spoofing tool. Among the 12 emails in the inbox, some are legitimate while others are designed as phishing examples (Emkei,). Participants will identify which emails they believe to be phishing attempts, applying the concepts learned in the theory section.

By engaging with both the theoretical resources and practical exercises, participants will gain a thorough understanding of e-mail security and be better equipped to recognize and respond to potential email threats.

3.2.2 Password Best Practices

The Password Best Practices module teaches participants how to create, manage, and protect strong passwords through theoretical resources and practical exercises. Participants will learn company policies and best practices, use a custom password manager to generate and store passwords securely, and understand encryption through hands-on activities.

In the Concepts & Theory folder for the Password Best Practices module, participants will find essential resources to understand the importance of secure password best practices. The first resource is a company document outlining the organization's password policy, which includes guidelines on creating robust passwords, the recommended frequency of password changes, and the importance of password uniqueness. Additionally, participants will have access to a CISA article titled ”Use Strong Passwords” (cis,) that discusses various password best practices and common pitfalls to avoid. This article covers topics such as the importance of creating complex passwords, the use of password managers, and avoiding password reuse. Another important resource is an Okta article that explains the significance of multi-factor authentication (MFA) and its role in enhancing security (okt,). This article provides a comprehensive overview of why MFA is crucial and how it works.

In the Practical Application folder, participants will engage with hands-on exercises designed to reinforce their understanding of password security. They will use a custom-programmed password manager within the virtual environment to create and store secure passwords. This manager generates strong passwords and saves them in an encrypted file (passwords.json), emphasizing the importance of encryption in password storage. Participants will then use a custom-programmed password decrypter to decrypt the stored passwords using a key file, providing a practical demonstration of encryption and decryption processes. Additionally, participants will complete a practical assessment where they evaluate the strength of various passwords and improve weak ones based on the best practices learned. By combining theoretical knowledge with practical application, the Password Best Practices module ensures participants are well-equipped to create, manage, and protect their passwords effectively.

3.2.3 Secure Browsing Techniques

The Secure Browsing Techniques module educates participants on safe web browsing practices through a combination of theoretical resources and practical exercises. Participants learn about key security concepts, the importance of HTTPS, and the benefits of AdBlockers, and engage in hands-on activities to recognize and respond to online threats effectively.

In the Concepts & Theory folder for the Secure Browsing Techniques module, participants will find four essential resources. The first resource is an article from HowToGeek titled ”9 Tips to Safely Browse the Web,” (Abdul,) providing practical advice on maintaining security and privacy while browsing. The second resource is a Cloudflare page explaining the importance of HTTPS for secure communication (Cloudflare,). The third link leads to PhishTank (phi,), where participants can see real-time reports of phishing attempts. Lastly, a section on AdBlockers like uBlock Origin details how they enhance user safety by blocking malicious ads, reducing tracking, improving browser performance, and preventing scams.

In the Practical Application folder, participants will engage in hands-on exercises to reinforce secure browsing techniques. They will perform a Google search and analyze the sponsored results to identify potential threats. Next, they will visit dawn.com to understand the risks of allowing website notifications. Participants will also learn to update their web browsers to ensure they have the latest security updates. Finally, they will visit a non-secure webpage hosted on an AWS EC2 instance, demonstrating the importance of HTTPS and recognizing browser security warnings.

3.2.4 Virus Simulation

The Virus Simulation module educates participants on recognizing and responding to virus and malware threats through a combination of theoretical resources and practical exercises. Participants learn best practices for preventing and removing malware and engage in simulations to identify and respond to fake virus warnings and real threats effectively.

In the Concepts & Theory folder for the Virus Simulation module, participants will find two essential resources. The first link directs participants to a Microsoft support page (mic, a) that provides comprehensive guidelines on how to prevent and remove viruses and other malware. This resource covers best practices for maintaining a secure system, including tips for avoiding malware and steps for virus removal. The second link leads to an AVG (avg,) article that helps participants identify fake virus warnings; a common tactic used by cybercriminals to deceive users into installing malware.

In the Practical Application folder, participants will engage in hands-on exercises to reinforce their understanding of virus and malware threats. They will interact with a series of simulated virus alerts within the virtual environment, designed to look and feel like real security threats. Participants will learn understand the behavior of various types of malware, and practice performing virus scans using Windows Defender. These exercises aim to enhance awareness and recognition of potential security incidents, helping employees to identify and respond appropriately to different types of virus alerts.

3.3 User Interaction

How users interact with the platform and complete training tasks. The two main components of this project that participants will interact with throughout the training are the Blackboard course and the Virtual Training Environment. Users will begin their training by navigating to the course page on Blackboard. On this platform, they will find detailed instructions on how to connect to and interact with the virtual environment. The Blackboard course provides a structured pathway, guiding participants through each module with clear, step-by-step instructions. Once connected to the Virtual Training Environment, users will engage with various simulated scenarios and practical exercises designed to reinforce the theoretical concepts presented in the course. This dual-platform approach ensures that participants can seamlessly transition between learning materials and hands-on practice, enhancing their overall training experience.

3.4 Data Collection

Methods used to collect feedback and measure user performance. To collect feedback and measure user performance, two primary methods are employed: Qualtrics surveys and Blackboard assignments. The Blackboard assignments are designed to gauge participants' understanding of the practical application sections of each learning module. These assignments provide a direct measure of how well users can apply what they have learned in real-world scenarios. In parallel, Qualtrics surveys are used to assess overall comprehension and knowledge retention. These surveys include pre- and post-training assessments to evaluate changes in participants' understanding and identify areas where further clarification may be needed. By combining these two data collection methods, we obtain a comprehensive view of user performance and the effectiveness of the training program. This approach not only helps in fine-tuning the current training but also provides valuable insights for future improvements.

During the initial testing phase for the CyberWise virtual environment, we encountered several issues. Initially, we planned to use a Docker container to develop and easily deploy the virtual environment. After extensive trial and error and hours of documentation, we were close to setting up a basic Docker container.

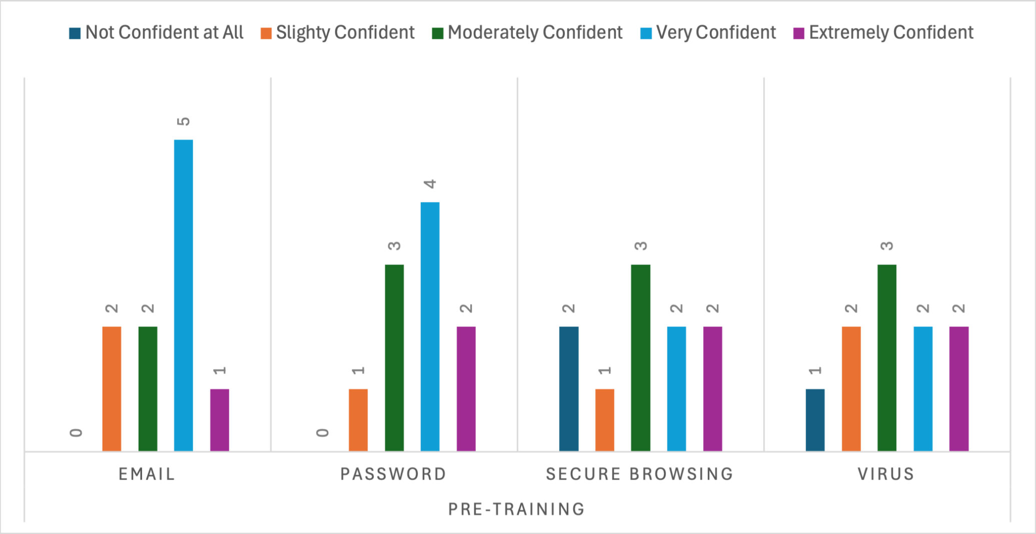

Figure 2: Number of participants with their confidence levels in subject matters pre-training.

However, multiple attempts led to a critical error on our testing device, rendering it unusable. After over a week of troubleshooting, we decided to find an alternative to Docker.

In the CyberWise virtual training environment, we used an EICAR test file to allow participants to detect a ”virus” after running a scan with Windows Defender. However, after each scan, the file would be removed from the environment. This required manually re-adding the file for future participants. To resolve this, we modified the training to focus on running a Quick Scan with Windows Defender, avoiding the need to manually add the test file. This change was necessary to prevent skewing the results gathered from our surveys, as participants had already started testing the environment.

The Institutional Review Board (IRB) is responsible for ensuring the privacy and safety of participants and their personally identifiable information. Submitting an IRB request for approval took about two and a half weeks, with an additional week for approval. The main challenge was that more information was required than initially expected, delaying the IRB submission until the requested information could be provided. As the project progressed, the IRB approval became less relevant because Blackboard was used to manage the virtual lab environment, identifying CyberWise participants in the Blackboard roster.

In the virtual lab environment, each Python script had a shortcut with a specific icon to make it easier for participants to run the correct file. However, we encountered an issue where the icons would become blank every few days. Due to more pressing time constraints, we could not fully resolve this technical issue. Our workaround was to reselect the shortcut images whenever this occurred.

Lastly, one of our most significant challenges was finding participants interested in completing the modules and surveys. Initially, we contacted approximately 50 staff and faculty members to gauge interest. Out of these, 15 individuals expressed interest and filled out the CyberWise Qualtrics survey. We sent three reminders to encourage participation before releasing CyberWise to participants, allowing them seven days to complete the modules. Although we anticipated this would be sufficient time, only 10 participants completed all the modules and surveys after a four-day extension. While the data collected is still relevant and valuable, having more participants would have provided more statistically significant data points.

4 EVALUATION

4.1 Feedback Analysis

The pre-training survey revealed that security awareness training was generally not engaging for many participants based on their past experiences. Most participants expected navigating the virtual training environment to be neither easy nor difficult. Secure Browsing Techniques and Email Security were anticipated to be the most useful modules, with four participants expecting Secure Browsing Techniques to be the most useful and three participants expecting Email Security to be the most useful. On average, previous security training was some-what likely to be applied to daily work by most participants.

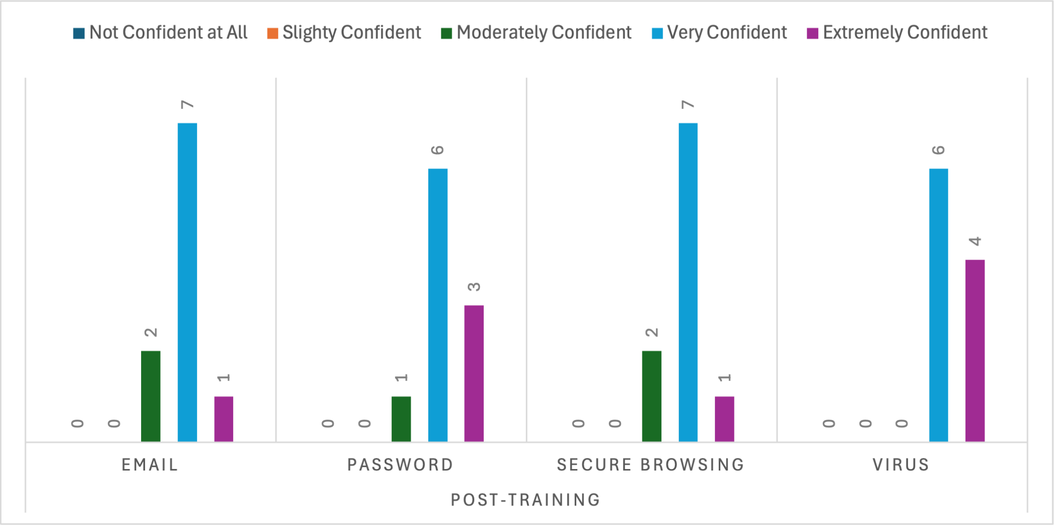

Figure 3: Number of participants with their confidence levels in subject matters post-training.

5 CHALLENGES

The post-training survey showed improvements in participants' confidence. Confidence in identifying phishing emails increased, with 80% of participants reporting feeling very or extremely confident, with some users having moved over from feeling moderately confident to very confident. Confidence in creating and identifying strong passwords increased, with 90% feeling very or extremely confident, with some participants moving from moderately confident to very confident, and one participant feeling extremely confident. Confidence in secure browsing practices improved, with 80% feeling very or extremely confident. Notably, 30% of participants went from feeling not confident at all or slightly confident to feeling moderately, very, or extremely confident in this area. The ability to deal with virus-related popups saw significant improvement, with 100% feeling very or extremely confident, a stark contrast to the initial survey where 60% of participants felt moderately confident, slightly confident, or not confident at all. The training was found to be very or extremely engaging by 70% of participants. Most participants found navigating the virtual training environment practical, with 90% finding it somewhat easy or extremely easy. Secure Browsing Techniques and Virus Simulation were considered the most useful modules. The likelihood of applying the completed security training to daily work increased, with 90% feeling very or extremely likely to apply the training.

5.1 Performance Metrics

The phishing email detection rate showed improvement, with the percentage of participants who felt very confident or extremely confident increasing from 60% pre-training to 80% post-training. In secure browsing practices, the percentage of participants who felt very confident or extremely confident increased from 40% pre-training to 80% post-training. For password management, the percentage of participants who felt very confident or extremely confident in creating and identifying strong passwords increased from 60% pre-training to 90% post-training. The ability to respond to virus-related popups improved significantly, with the percentage of participants who felt very confident or extremely confident increasing from 40% pre-training to 100% post-training.

5.2 Comments Analysis

Participants provided valuable feedback at the end of the post-training survey, which offers insights into the effectiveness and areas for improvement in the security awareness training program. One participant highlighted the realism and relevance of the browser hijacker simulation, suggesting that additional examples like fake email popups linked to phishing sites could enhance the training. This comment underscores the importance of practical, real-world scenarios in engaging participants and improving their skills. Another participant expressed appreciation for the training, noting that it was beneficial and brought back memories of previous virus incidents. This pos-

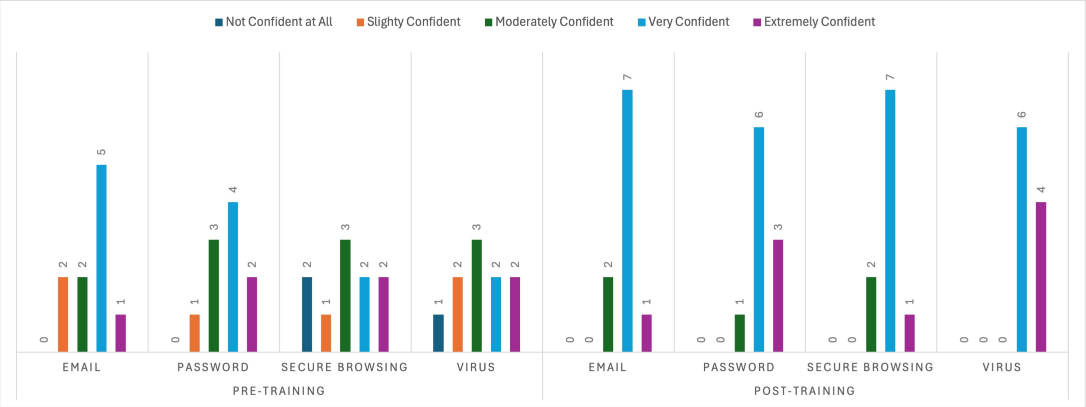

Figure 4: Number of participants with their confidence levels in subject matters pre- and post- training.

itive feedback reflects the training's impact on reinforcing cybersecurity awareness and preparedness.

One detailed comment mentioned the overall high quality of the training, appreciating the hands-on approach and the variety of simulated attacks. The participant suggested that while the training was highly informative, there could be more integration with actual production environments to enhance realism further. They also mentioned the value of continuous learning and suggested that the training be part of an ongoing security education program rather than a one-time event. A participant mentioned a specific issue where the virus alerts did not appear as expected on the desktop, indicating a potential technical glitch that should be addressed in future iterations of the training. This feedback highlights the need for thorough testing of the training environment to ensure all simulations run smoothly.

Lastly, a participant emphasized the importance of ongoing security training and expressed a desire for continuous and consistent security education. This comment aligns with best practices in cybersecurity training, which advocate for regular updates and refresher courses to keep skills sharp and up-to-date. Overall, the feedback comments were overwhelmingly positive, with participants appreciating the interactive and practical nature of the training. Suggestions for improvement included adding more varied and realistic scenarios, ensuring technical issues are resolved, and incorporating continuous training programs.

6 RESULTS AND DISCUSSION

The pre-training results reveal varying levels of confidence across the four modules, with noticeable gaps in higher confidence levels, as demonstrated by Figure 2. For example, in the Email Security module, 5 participants reported being Very Confident, while no one selected Not Confident at All. However, lower confidence categories like Slightly Confident and Moderately Confident still accounted for 2 participants each, and only 1 participant reported feeling Extremely Confident. In other modules like Password Best Practices and Virus Awareness, confidence levels were more evenly distributed. For instance, in Password Best Practices, 4 participants reported being Very Confident, while 3 were Moderately Confident and 2 felt Extremely Confident. Similarly, in Virus Awareness, confidence was modest, with the majority (3 participants) reporting Moderately Confident and only 2 participants each selecting Very Confident or Extremely Confident. These results highlight that, while participants had some familiarity with cybersecurity concepts, deeper understanding and confidence were needed prior to the training.

The post-training results demonstrate significant improvements in confidence across all modules, validating the effectiveness of the CyberWise platform (Figure 3). In the Email Security module, confidence consolidated into higher categories, with 7 participants reporting being Very Confident and 1 participant feeling Extremely Confident. No one selected lower confidence levels, such as Not Confident at All or Slightly Confident. Similar improvements occurred in Password Best Practices, where 6 participants reported being Very Confident and 3 participants moved up to Extremely Confident. The most dramatic shift appeared in the Virus Awareness module, where confidence surged: 6 participants reported being Very Confident and 4 participants reached Extremely Confident, with no participants reporting lower confidence. Overall, the post-training results reflect a clear upward shift in participant confidence, demonstrating that the CyberWise training successfully addressed knowledge gaps and reinforced critical cybersecurity principles.

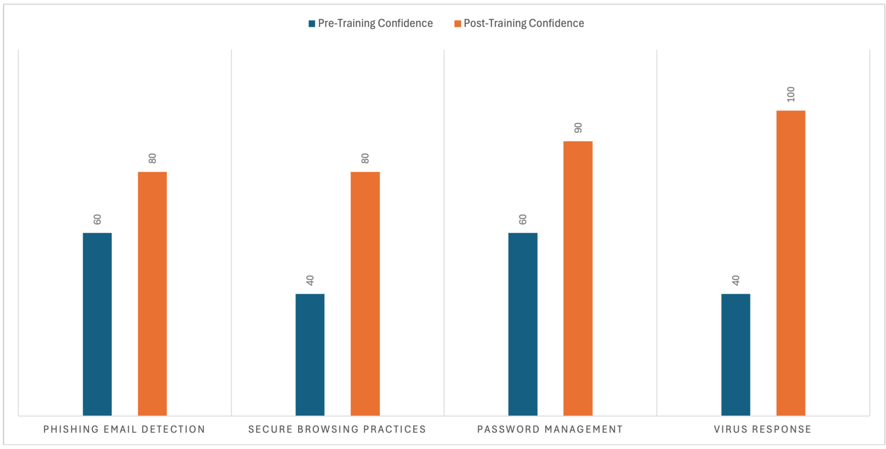

Figure 5: Percentage of participants who responded feeling very confident or extremely confident in these subject matters pre-training vs. post training.

There was a marked increase in participants' confidence in identifying phishing emails, creating strong passwords, secure browsing, and dealing with virus-related popups after the training. Participants found the training to be significantly more engaging compared to their previous experiences. Most participants found the virtual training environment practical and easy to navigate.

The training program successfully increased participants' confidence and skills in key areas of cybersecurity. The practical, hands-on approach likely contributed to the improved engagement and effectiveness. The focus on realistic simulations and interactive exercises helped solidify the concepts taught. Traditional security awareness training is often perceived as unengaging. The interactive and simulation-based approach used in this training was found to be significantly more engaging. Participants felt more confident in applying what they learned to their daily work, which is a critical measure of the training's effectiveness.

7 CONCLUSION AND FUTURE WORK

CyberWise project aimed to enhance security awareness among staff and faculty members at the university through a comprehensive, hands-on training platform. The pre- and post-training surveys revealed improvements in participants' confidence and skills in key areas of cybersecurity. Specifically, the percentage of participants who felt very confident or extremely confident in identifying phishing emails increased from 60% to 80%, confidence in secure browsing practices rose from 40% to 80%, confidence in creating and identifying strong passwords increased from 60% to 90%, and confidence in dealing with virus-related popups improved from 40% to 100%. Additionally, 70% of participants found the training very or extremely engaging, and 90% found navigating the virtual training environment to be somewhat easy or extremely easy. These results underscore the effectiveness of the CyberWise platform in improving cybersecurity awareness and preparedness.

While CyberWise platform has proven effective, there are several areas for future improvement and further research. First, expanding the sample size to include a broader range of participants beyond the IT department would provide more generalizable results. Second, incorporating long-term follow-up surveys would help assess the retention and ongoing application of the skills learned. Third, addressing any technical issues, such as ensuring all simulations run smoothly, will enhance the overall training experience. Finally, integrating additional realistic scenarios, such as fake email popups linked to phishing sites, could further enhance the training's realism and effectiveness.

The CyberWise project has made a contribution to the field of cybersecurity by demonstrating the value of immersive, hands-on training in enhancing security awareness. The interactive and simulation-based approach not only engaged participants more effectively than traditional methods but also ensured better retention and application of security best practices. By providing a practical and familiar training environment, CyberWise has equipped staff and faculty members with the knowledge and skills necessary to protect themselves and their organization from cyber threats. Overall, this project highlights the importance of innovative training solutions in fostering a robust security culture within educational institutions.

The relatively small sample size may limit the generalizability of the results. The data is based on self-reported confidence levels, which may not always accurately reflect actual skill levels. The surveys were conducted immediately after the training, so long-term retention and application of the skills were not measured. CyberWise can be further enhanced to ensure long-term effectiveness and expand its impact. One key area for potential improvement is incorporating real-time threat simulations that reflect the evolving cybersecurity landscape. By pulling in live feeds of new phishing techniques, malware strains, and social engineering tactics actively being used to compromise organizations, the platform could deliver even more realistic training scenarios. Highlighting how individuals and businesses are falling victim to emerging attacks, such as deepfake phishing, AI-driven malware, and sophisticated ransomware campaigns, would give participants a deeper understanding of modern threat methods and help them proactively recognize and respond to these risks.

Another opportunity for enhancement is introducing AI-driven phishing simulations and personalized learning paths based on pre-training assessments. Tailoring modules to individual knowledge gaps would ensure a more targeted and effective training experience. Additionally, implementing gamification elements, like leaderboards, badges, and timed challenges, could boost engagement and motivation, creating a more interactive learning environment. Finally, expanding survey metrics to include long-term follow-up assessments would provide valuable insight into how well participants retain and apply their knowledge over time. These improvements would position CyberWise as a dynamic and adaptive platform, keeping pace with emerging cybersecurity challenges while maximizing user learning and engagement.

REFERENCES

Fake Virus Warnings: How to Spot and Avoid Them — avg.com. https://www.avg.com/en/signal/spot-fake-virus-warning. [Accessed 15-12-2024].

How to prevent and remove viruses and other malware - Microsoft Support — support.microsoft.com. https://support.microsoft.com/en-gb/topic/how-to-prevent-and-remove-viruses-and-other-malware-53dc9904-0baf-5150-6e9a-e6a8d6fa0cb5. [Accessed 15-12-2024].

PhishTank — Join the fight against phishing — phishtank.com. https://www.phishtank.com/. [Accessed 15-12-2024].

Protect yourself from phishing - Microsoft Support — support.microsoft.com. https://support.microsoft.com/en-us/windows/protect-yourself-from-phishing-0c7ea947-ba98-3bd9-7184-430e1f860a44. [Accessed 15-12-2024].

Use Strong Passwords — CISA — cisa.gov. https://www.cisa.gov/secure-our-world/use-strong-passwords. [Accessed 15-12-2024].

What Is Email Security? — Microsoft Security — microsoft.com. https://www.microsoft.com/en-us/security/business/security-101/what-is-email-security. [Accessed 15-12-2024].

Why Multi-Factor Authentication (MFA) Is Important — Okta — okta.com. https://www.okta.com/identity-101/why-mfa-is-everywhere/. [Accessed 15-12-2024].

Abdul, S. 9 Tips to Safely Browse the Web — howtogeek.com. https://www.howtogeek.com/9-tips-to-safely-browse-the-web/. [Accessed 15-12-2024].

Alkhazi, B., Alshaikh, M., Alkhezi, S., and Labbaci, H. (2022). Assessment of the impact of information security awareness training methods on knowledge, attitude, and behavior. *IEEE access*, 10:132132–132143.

Cloudflare. What is https? https://www.cloudflare.com/learning/ssl/what-is-https/. [Accessed 15-12-2024].

Emkei. Emkei's Fake Mailer — emkei.cz. https://emkei.cz/. [Accessed 15-12-2024].

Haney, J. and Lutters, W. (2020). Security awareness training for the workforce: moving beyond "check-the-box" compliance. *Computer*, 53(10).

Labuschagne, W. A. and Eloff, M. (2012). Towards an automated security awareness system in a virtualized environment. In *11th European Conference on Information Warfare and Security 2012, ECIW 2012*, pages 163–171.

Lee, D., Kim, D., Lee, C., Ahn, M. K., and Lee, W. (2022). Icstasy: an integrated cybersecurity training system for military personnel. *IEEE Access*, 10:62232–62246.

Mikova, I., Komarkova, L., Pudil, P., and Pribyl, V. (2021). Hr management and perceived effectiveness of further education and training methods of millennial employees in the czech republic. *Journal of East European Management Studies*, 26(3):415–439.

Vykopal, J., Seda, P., Švábenskỳ, V., and Čeleda, P. (2022). Smart environment for adaptive learning of cybersecurity skills. *IEEE Transactions on Learning Technologies*, 16(3):443–456.