Cybersecurity Pedagogy & Practice Journal

Volume 4, No. 2
October 2025
ISSN: 2832-1006

In this issue:

4. **Strengthening Incident Response: Lessons from Cybersecurity Tabletop Exercises for Rural Critical Infrastructure**
Reda M. Haddouch, University of Montana
Shawn F. Clouse, University of Montana
Ryan T. Wright, University of Virginia
Theresa M. Floyd, University of Montana
Victor C. Valgenti, University of Montana
Patricia Akello, University of Montana
Thomas P. Gallagher, University of Montana

36. **PhishBusters: A Comprehensive Approach to Phishing Awareness Training in Organizational Settings**
Melissa Montes, University of Arizona
Shengjie Xu, University of Arizona

51. ***Teaching Case:***
Utilizing a Virtual Firewall Appliance for Introducing and Reinforcing the Concepts and Implementation of Devices to Improve Security in a Computing Environment
Stanley J. Mierzwa, Kean University
Christoper Eng, Kean University

iscap
Information Systems & Computing Academic Professionals

The **Cybersecurity Pedagogy and Practice Journal** (**CPPJ**) is a double-blind peer-reviewed academic journal published by **ISCAP** (Information Systems and Computing Academic Professionals). Publishing frequency is two times per year. The first year of publication was 2022.

CPPJ is published online (https://cppj.info). Our sister publication, the proceedings of the ISCAP Conference (https://proc.iscap.info) features all papers, panels, workshops, and presentations from the conference.

The journal acceptance review process involves a minimum of three double-blind peer reviews, where both the reviewer is not aware of the identities of the authors and the authors are not aware of the identities of the reviewers. The initial reviews happen before the ISCAP conference. At that point, papers are divided into award papers (top 15%), and other accepted proceedings papers. The other accepted proceedings papers are subjected to a second round of blind peer review to establish whether they will be accepted to the journal or not. Those papers that are deemed of sufficient quality are accepted for publication in the CPPJ journal.

While the primary path to journal publication is through the ISCAP conference, CPPJ does accept direct submissions at https://iscap.us/papers. Direct submissions are subjected to a double-blind peer review process, where reviewers do not know the names and affiliations of paper authors, and paper authors do not know the names and affiliations of reviewers. All submissions (articles, teaching tips, and teaching cases & notes) to the journal will be refereed by a rigorous evaluation process involving at least three blind reviews by qualified academic, industrial, or governmental computing professionals. Submissions will be judged not only on the suitability of the content but also on the readability and clarity of the prose.

Currently, the acceptance rate for the journal is under 35%.

Questions should be addressed to the editor at editorcppj@iscap.us or the publisher at publisher@iscap.us. Special thanks to members of ISCAP who perform the editorial and review processes for CPPJ.

Cybersecurity Pedagogy and Practice Journal

PhishBusters: A Comprehensive Approach to Phishing Awareness Training in Organizational Settings

Melissa Montes
melissamontes@arizona.edu

Shengjie Xu
sjxu@arizona.edu

University of Arizona
Tucson, AZ 85721

Abstract

This paper presents the design, implementation, and evaluation of PhishBusters, a comprehensive phishing awareness training program specifically developed for non-technical employees in organizational settings. The program employs a multi-faceted pedagogical approach that combines theoretical knowledge, hands-on exercises, and gamified learning to enhance participants' ability to identify and respond to phishing attempts. Through three structured training sessions, participants engage with realistic phishing simulations, interactive quizzes, and collaborative group discussions, fostering both individual skill development and peer learning. The effectiveness of the training program is demonstrated through comprehensive pre and post-assessment results, showing significant improvement in participants' ability to detect phishing attempts. The paper details the curriculum design process, implementation challenges, and participant feedback, providing practical insights into effective cybersecurity training methodologies. This case study contributes to the growing body of knowledge in cybersecurity education by demonstrating how well-designed training programs can successfully enhance organizational security awareness and reduce phishing susceptibility among non-technical staff.

Keywords:
Phishing awareness training, Cybersecurity education, Training program design, Employee security behavior, Interactive simulations, Organizational security training, Non-technical staff training

Recommended Citation: Montes, M., Xu, S., (2025). PhishBusters: A Comprehensive Approach to Phishing Awareness Training in Organizational Settings *Cybersecurity Pedagogy and Practice Journal;* v4(n2) pp 36-50. DOI# https://doi.org/10.62273/10.62273/JUZT9288

PhishBusters: A Comprehensive Approach to Phishing Awareness Training in Organizational Settings

Melissa Montes and Shengjie Xu

1. INTRODUCTION

In today's fast-paced digital landscape, the security of an organization heavily depends on the awareness and vigilance of its employees. Cyber threats are evolving daily, and one of the most common and dangerous methods used by attackers is phishing (Verizon, 2023). Phishing is an attempt to steal sensitive information, typically in the form of usernames, passwords, credit card numbers, bank account information, or other important data, to utilize or sell the stolen information. By masquerading as a reputable source with an enticing request, such as an email or text message, an attacker lures the victim into giving up the information (Butavicius et al., 2022). Phishing attacks exploit human behavior, aiming to deceive individuals into divulging sensitive information and granting unauthorized access to systems.

The PhishBusters program was designed to empower employees at an organization who possessed little to no background in cybersecurity, by equipping them with the essential knowledge and skills necessary to effectively identify, avoid, and report phishing attempts. This comprehensive program immersed employees in a range of learning experiences that demystified the tactics employed by cybercriminals. Participants gained a deep understanding of how these threats manifest, allowing them to recognize suspicious emails, deceptive links, and fraudulent websites with confidence.

Through a series of engaging modules and interactive scenarios, employees gained not only the ability to spot red flags associated with phishing attempts but also the confidence to adopt proactive safety practices that significantly bolstered the protection of both their personal information and the organization's sensitive information. The curriculum was thoughtfully designed to cover a wide array of real-world examples of phishing attacks, delving into the various techniques employed by cybercriminals. This included the exploration of social engineering tactics, spear-phishing methods that target specific individuals, and the use of malicious attachments that can compromise systems.

Participants engaged in hands-on activities that simulated phishing attempts, allowing them to practice their skills in a safe environment. They learned how to scrutinize emails for suspicious elements, identify dubious links, and recognize fraudulent websites. Through group discussions, participants were encouraged to share their experiences and insights, fostering a collaborative learning atmosphere that enhanced their understanding of the topic.

By the end of the program, participants felt empowered and informed, equipped with practical tools and strategies to navigate the digital landscape securely. This newfound knowledge not only enhanced their personal cybersecurity practices but also cultivated a culture of vigilance and security awareness throughout the organization. As employees became more aware of potential threats that existed in their daily communications, they were more likely to report suspicious activities, contributing to a proactive security environment.

Ultimately, PhishBusters aimed to create a resilient workforce that stood united against cyber threats. By instilling a collective sense of responsibility and vigilance, the program helped safeguard the integrity of the organization and its valuable information, ensuring that all employees played an active role in protecting against cyber risk. Through this initiative, the organization enhanced its security posture, reduced the likelihood of successful phishing attacks, and fostered a culture of continuous improvement in cybersecurity awareness and practices.

2. LITERATURE REVIEW

Why Phishing Works

Dhamija et al. (2006) aimed to address and test hypotheses on why users are most likely to fall for phishing attempts. Their study sought to understand the factors that contribute to users being deceived into falling for fraudulent websites. The goal of the Dhamija et al. study was to understand the reasons behind why phishing strategies work, in order to better learn from them and improve web browsers, websites, and other tools needed to protect users from phishing attacks.

The Dhamija et al. study highlights gaps in user knowledge that phishing attacks exploit, such as lack of system knowledge and lack of security awareness. In terms of lack of system knowledge, many users do not understand how operating systems, browsers, and domain names work. Without this understanding, users have a difficult time recognizing phishing sites or forged email headers. In terms of lack of security awareness, users will often misunderstand security indicators like SSL padlock icons, which can be mimicked in webpage content. Users lack the proper skills to verify SSL certificates properly, making them vulnerable to spoofed trust seals and other deceptive tactics.

The Dhamija et al. study presents a usability study assessing how participants identify legitimate and phishing websites. Using 22 participants, the study analyzed their decision-making while interacting with real spoofed sites from financial and e-commerce companies. Factors such as website content, domain names, and security indicators were used to judge the legitimacy of a website. The results of the study found significant variability in users' ability to detect fraudulent websites, with some participants relying on visual cues while others used more advanced security knowledge. The study highlighted the challenges that even informed users face in recognizing phishing attempts.

From this study, the key takeaway that we can use to further develop our curriculum for this lesson is to consider that there are key factors often overlooked by those who are not technically inclined in technology. One must consider that simple factors, such as paying attention to the URL bar, can make a difference in showing whether a website is legitimate or spoofed. A basic understanding of indicators can go a long way in ensuring online user safety. If we provide focus and have participants learn and understand the common indicators that are a determining factor, we can make a difference in ensuring that participants are less likely to fall for phishing attempts.

Does Phishing Training Work? Yes! Here’s Proof

Recent studies have shown that effective phishing training can significantly reduce employee susceptibility to phishing attacks (Goel et al., 2017). Phishing awareness training and phishing simulations are identified as the two main training approaches in this article (Moore and Clayton, 2007). The study aims to demonstrate how combining both training methods enhances the effectiveness of phishing training compared to using these methods separately.

Organizations that provide phishing awareness training report an 80% reduction in employee susceptibility after undergoing the training. This method aims to educate employees about the dangers of phishing threats, various attack types, and how to identify a phishing attempt in its tracks. Phishing simulations are tests that mimic real-world phishing scenarios, enabling employees to practice identifying potential threats. Research shows that simulation-based training can double learning retention, as employees have the ability to test their knowledge in real-life scenarios. By combining these two methods, organizations can see a 60% reduction in mistakes after a few sessions. The combination of both methods proves to be more effective than either method alone as it blends theory and practice, thus enhancing employees’ readiness for real-world phishing attacks.

The article highlighted the importance of not only providing employees with proper phishing training but also the importance of incorporating phishing simulations, as these methods, when combined, prove to be effective together. These methods can provide insight into areas for improvement within their organization, helping them better prepare employees for the possibility of falling victim to such attacks. Our key takeaway from this article is that it will be in the best interest of participants to be provided with both types of training methods. In our setting, we will provide a phishing simulation email to employees before they receive any training. This will be followed by phishing awareness training, and then another simulation email to demonstrate the improvement that has taken place from going from no training to receiving training. By doing so, we will provide participants with hands-on experience in spotting phishing attempts and better instruct them on the common flags they need to be fully aware of.

Phishing Detection: A Literature Survey

Phishing targets the human factor as it is the weakest link in the security chain (Khonji et al., 2013). There is no single solution that can be deployed to address the issue, as phishing is a layered problem that must be addressed at two different levels: the technical and human layers. Solutions to address both layers can be found already, but it is unclear exactly how well they are working and whether they are making a difference today. There are currently two forms of solutions employed: user education and software enhancement.

User education aims to increase awareness of phishing attacks and lower the risk of becoming a victim where software enhancements can be anything from apps to plugins to blacklist that provide support in stopping a phishing attack in its track.

The survey (Khonji et al., 2013) presents various phishing detection approaches, such as user education and awareness, Blacklists, Heuristic tests, and visual similarity, as well as machine learning-based classifiers, in which they test which approaches are best for dealing with phishing attempts. Their conclusions on the various approaches to combating phishing and enhancing end-user security are as follows:

- Education alone is insufficient because simply educating users about phishing risks is not enough. Even security experts can fall victim to phishing, suggesting that system complexities may exceed human cognitive limits. Hence, better system usability and user interfaces are crucial in addressing phishing risks. An example would be that active warnings (blocking content and visually signaling risks) are more effective than passive warnings.
- System behavior improvement can help mitigate phishing by automatically detecting and quarantining harmful messages through features like blacklists, heuristic rules, and machine learning techniques. These features are currently implemented in web browsers, email clients, and server-side filters.
- Blacklists are a list of previously detected phishing URLs, Internet Protocol addresses, and/or keywords, and are effective in reducing false positives. However, they struggle with mitigating zero-hour phishing attacks due to delays in detecting and updating the lists. Human-vetted blacklists, such as Phish Tank, have significant detection delays, leaving end-users vulnerable to new attacks during the early stage of a phishing campaign.
- Heuristic tests can detect zero-hour phishing attacks but tend to have higher false-positive rates than blacklights. The evolving nature of phishing tactics requires continuous updates to heuristic rules, making them expensive to maintain. Techniques that utilize visual similarity also incur computational overhead due to the rendering and analysis of web content, making them resource-intensive.
- Machine learning classifiers excel at addressing zero-hour phishing attacks and can automatically generate effective classification models from large datasets. They can achieve high accuracy, often with less than 1% false positives and over 99% true positives. ML classifiers can evolve over time, adapting to new phishing techniques without needing manual rule updates, making them more scalable and robust than heuristic-based approaches.

They concluded that while user education remains important, a more effective anti-phishing strategy involves a combination of systems usability improvements, blacklists, heuristics, and machine learning techniques to automate the detection and mitigation of phishing threats.

From their survey on different methods that can be used to prevent phishing attempts, our takeaway that we can use to further our program is to make it clear to employees that, in some cases, even with all the training in the world, not all phishing attacks can be prevented by being cautious. Some phishing attacks will be more sophisticated than others or be better hidden among legitimate emails. They will blend naturally and not raise any concern. In this case, ensuring that participants are well aware of risks that they may not be able to control and instead teach them to become aware and to communicate with the IT teams when it is deemed necessary. We can explore how advanced technologies such as machine learning, blacklists, and heuristic analysis contribute to mitigating phishing threats.

Who Falls for Phish? A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interventions

Sheng et al. (2010) evaluated different phishing educational materials to determine their effectiveness in training users. The materials tested included:

- Popular training materials include Microsoft Online Safety, OnGuardOnline phishing tips, and National Consumer League Fraud tips.
- Anti-Phishing Phil, which is an interactive game developed by Carnegie Mellon University (Sheng et al., 2007).
- Phish Guru Cartoon is a training system that uses cartoon images shown after users click on simulated phishing emails.
- Anti-Phish Phil with PhishGuru Cartoon, which is a combination of both training tools.

A total of 1001 participants were randomly assigned to different groups, including a control group (no training) and groups receiving one of the training materials. Participants were given role-playing scenarios both before and after the training, and their reactions were analyzed to assess the impact of each tool.

The study found that all training approaches improved the true positive (TP) rate, meaning users were more likely to correctly identify phishing emails. However, most training materials also reduced the true negative (TN) rate, causing some users to distrust legitimate emails due to fear from their training. On average, training materials reduced false negatives (missed phishing emails) by 39.79% but reduced true negatives by 7.69%. Anti-Phish Phil stood out as the only tool that did not lower the TN rate, indicating it was more balanced in its approach. The control group (untrained) also showed slight improvement, as they received no training on how to identify or detect phishing attacks.

The study highlights that while user training can reduce phishing risks, it may also cause users to be overly cautious about legitimate emails. The effectiveness of training depends on balancing awareness without overwhelming users. Sheng et al. (2010) also provide further perspectives, noting that expecting users to become tech-savvy while handling their primary job tasks may hit cognitive limits. Meaning we cannot expect users with little technology background to become experts in the matter, IT needs to employ as many safeguards as possible to minimize the risk of phishing emails getting through the filtering system.

Participants with little background in technology can feel overwhelmed by the amount of information they need to learn to stay safe. For someone who is not used to seeing or learning about phishing, it can seem like a lot to take in, let alone memorize. For our program, we plan on teaching them some of the resources and tools they have available to them. The program is meant to be more engaging than others in hopes that they can retain information longer than learning on their own. By learning in a group setting, participants can learn from each other too and ask questions on the spot on anything that may need clarification. In doing so, the goal is for participants to walk away with knowledge that will help them change their behavior, thus changing their online habits for the better.

Individual Processing of Phishing Emails: How Attention and Elaboration Protect Against Phishing

Harrison et al. (2016) explores the idea of the mechanisms that influence susceptibility to phishing. They focus on the characteristics of emails, users' knowledge and experience with phishing (Williams et al., 2018). They conduct an experiment with 194 subjects in which they expose participants to phishing attacks to measure the participants' actions towards it. The goal is to reach an understanding that explains why some attacks are successful and why some participants are better at detecting phishing attempts (Parsons et al., 2013).

The study was done mainly on college students, as the younger population is often the most targeted of phishing attacks because of their low levels of phishing knowledge and awareness. Specially crafted emails were sent out to the participants, in which they had a fear-based and a reward-based email. The following hypotheses were tested:

- A fear-based phishing attack is more likely to result in decreased attention and decreased elaboration of the message than a reward-based attack. (H1a)
- A fear-based phishing attack is more likely to result in victimization than a reward-based attack. (H1B)
- The presence of leakage cues will result in increased attention and increased elaboration of the phishing message. (H2a)
- The presence of leakage cues will result in a lower likelihood of phishing victimization. (H2B)
- Increased subjective knowledge of and experience with email will lead to increased attention and increased elaboration of the phishing message. (H3a)
- Increased objective knowledge of and experience with phishing-specific emails will lead to increased attention and elaboration of the phishing message. (H3b)

The results were that 47% of participants clicked on the experimental link and provided their private information. Only 5% of participants noticed that the email did not come from a school domain, whereas 37% stated it did. The study determined that neither fear versus reward messaging nor the presence of leakage cues influenced the extent of the message elaboration, providing no support for H1a and H2a hypotheses. However, the subjective email knowledge, experience, and objective phishing-specific knowledge significantly predicted elaboration, supporting H3a and H3b. The overall model was significant; neither subjective nor objective knowledge alone was a strong predictor of elaboration.

For attention, message factors again did not impact processing, but objective phishing knowledge significantly improved attention, supporting H3b. The analysis revealed that both attention and elaboration were protective against phishing, with attention to specific elements such as hyperlinks or sender address predicting higher elaboration. However, the misinterpretation of certain cues, like perceiving a refund, reduced elaboration. Therefore, successful phishing defense involves recognizing key message cues and engaging in deeper message analysis.

The key takeaways from this study that we can use to further help our program will be to understand that, depending on one's experience, it will determine how well they can pick up on cues of a phishing attempt. Teaching participants that fear and reward-based tactics are common among phishing attempts, and it is in their best interests that they look at all the cues found in an email before they proceed to think irrationally and act on impulse. If we learn to take our time and read and analyze correctly, the chances of becoming a victim of a phishing attempt are low.

3. PROJECT DESIGN AND STRUCTURE

Using live lectures that are held in person, the phishing awareness training is split into three sessions to avoid an overwhelming amount of information at one time. Each session has participants learning the tools and skills that they need to ensure their online safety from any potential phishing attacks.

Pre-Assessment

The goal of designing a pre-assessment is to test the participants' current knowledge about the topic of phishing. It helps establish a baseline in understanding their familiarity with phishing concepts, risks, and detection techniques. This initial insight allows for a more targeted training that addresses the specific gaps or misconceptions. The pre-assessment was a crucial step in further developing lesson plans because it allows for:

- Identification of knowledge gaps: Helps uncover areas where participants lack essential understanding, enabling focus on topics where knowledge is weaker. In this case, the pre-assessment revealed that participants lacked an understanding of recognizing phishing indicators.
- Customization of Training: With a clear sense of participants' starting knowledge, the training can be tailored to be more effective, ensuring it is neither too basic nor too advanced for participants.
- Measurement of Progress: The assessment provides a benchmark to compare against the post-assessment, which helps measure the effectiveness of the training by showing how much participants have learned.

A simple ten-question multiple-choice survey was developed that asked participants to assess their current knowledge with regards to phishing. Participants were asked to complete the survey within two days of receiving the link to ensure enough time was given afterwards to analyze results and adjust lessons as needed. Out of the forty-two participants who took part in the survey, only seven respondents received a perfect score. The overall average score was 4.05 out of ten. The results were promising as they allowed for the identification of where common mistakes were occurring.

Lecture Slides

Three different slide decks were created to coincide with each lesson plan for the specific workshop. The slide decks are an essential part of the curriculum because they provide a structured, visual approach to learning, making complex information about phishing accessible and engaging. To avoid overwhelming participants with an endless amount of information, each slide deck was carefully planned and created in a visually appealing way, where the information on the deck was short and straightforward.

The first slide deck for lesson number one included introductory topics on what phishing, spear-phishing, whaling, smishing, vishing, and social engineering are. The common reasons why cybercriminals carry out phishing attacks, along with the type of information that they aim to steal. This presentation also included the methods used by attackers to target individuals, the dangers of such attacks, and a quick visual to illustrate how a phishing email works.

The second slide deck for lesson number two contained information regarding common indicators, how to verify an email address, what a domain is in email, hovering over links, malicious attachments, and how to identify suspicious links. Compared to the first slide deck, the second slide deck was made to be more interactive. After going over the topics, the next part added examples of simulations in which participants would be asked to first identify if the email was legitimate or a phishing email. From there, each participant would receive a chance to identify the indicators that they saw that made them determine whether or not an email was legitimate.

The third and final slide deck contained a quick review of the first two sessions, along with topics that included:

- How to report phishing attempts to IT
- Steps to take if a malicious link is clicked
- Importance of multi-factor authentication
- Importance of strong passwords and password management

The purpose of this slide deck was to be more informative with information regarding how to mitigate and the tools at their disposal. The slide deck was not as interactive as the previous two, but it outlined important information to help change their online behaviors.

Phishing Email Simulations

Phishing simulations crafted in CanIPhish were a key part of the program to provide training to participants. These phishing simulations allowed for testing the participants' ability to identify and respond to phishing attacks without actual risk. A variety of emails were crafted to mimic the type of email an employee would be at risk of receiving daily. The phishing emails crafted displayed messages such as this person is trying to reach you via Teams, someone has shared a Dropbox file with you, reset password for Microsoft, the office Christmas party file has been shared with you, and the HR department is trying to share a file with you.

During the second session, participants used these emails crafted to identify the common red flags based on what they had just learned from the lecture slides. In doing so, participants had a better understanding of where exactly in an email would be signs of a phishing email, compared to just assuming. The simulations provided hands-on experience on the subject, which allowed for an interactive class in which they were taught and saw an example at the same time, which better served them to remember the indicators.

Before the first session of the program, along with the pre-assessment, participants were also sent a phishing simulation email to begin to test whether they would click on the link provided to them in the email in which it said they needed to update their password to a software application, however the link was malicious and instead collected their information and redirected them to a "ops, you've just been bait" message. After which the same email would be reviewed in session two and explained to participants, specifically those who clicked the email, on why it was a phishing email and what indicator was given in the email that was overlooked.

After the final session, participants would be sent another phishing email in hopes that all the information that they learned throughout the three sessions would benefit them in ensuring that they are able to identify the phishing email. The sole purpose of this final simulation email was to ensure that participants were able to properly identify common indicators, and in doing so it would allow for measuring the effectiveness of the program.

Phishing simulation emails are powerful tools for building resilience against phishing attacks. They give participants the practical, hands-on experience needed to recognize and avoid real-world phishing attempts, and ultimately help reduce the organization's vulnerability to these common attacks.

Game Quiz using Kahoot

Using Kahoot, an interactive quiz was made to be used during the live training to create an engaging learning environment while adding a bit of fun and competitiveness to empower employees to understand the topics. The game was designed to be used during the first session to review the topics and ensure participants understood what they had learned. It was created to test their new knowledge on the different types of phishing, the information they steal, and test their current knowledge of common red flag indicators, although this session would not touch on the subject.

Infographics

Using Canva, a quick and simple infographic was developed that participants could take with them and keep around their desk to refer to from time to time to refresh their memory on the subject, but also use when in doubt about an email. The infographic contains information about what cybercriminals are after, a quick definition of phishing, tips to help detect a phishing email, and what they can do to avoid falling victim to it.

Post-Assessment Survey

The last part in the structure of the program was to give out a post-assessment that would test participants on how well they remembered what they were taught. The post-assessment was sent out a week after the last session took place and was available to participants via Google Forms. The timeline for having results was the week of November 8, 2024, which gave time to compare results with the pre-assessment to determine whether the educational program was beneficial and find areas of improvement.

A final phishing simulation email was sent out as well that would truly test the knowledge retention of the participants to see if there had been improvement. The hope was to ensure that everyone who participated could differentiate legitimate emails versus fraudulent ones.

By the end of the course, participants understand common characteristics found in phishing attacks and the tools and skills to mitigate such a risk.

4. PILOT IMPLEMENTATION

The pilot of the program was given to the employees of a construction company. The program was given out in the span of two weeks, with almost every employee in attendance. Each live session was 45 minutes long in which included a period of lecture slides, examples, games, and questions/comments. Each of the live sessions included a group learning environment where participants were able to ask questions the moment they needed to and to encourage each other to do their best and learn the material. There were a total of 42 participants who took part in the PhishBusters training program, and the in-person training was held at an organization.

Pre-Assessment and First Simulation Email
The first part of the program included sending out the pre-assessment survey and the first phishing simulation email to help the trainer have a better understanding of where the gaps in knowledge lie, to better help this group of participants. Once the results were received, the lessons were adjusted if needed to focus more on the gaps determined by the pre-assessments. In this case, most of the gap was in just understanding the common indicators, so a big focus was placed on ensuring that this topic was touched on, along with practicing it.

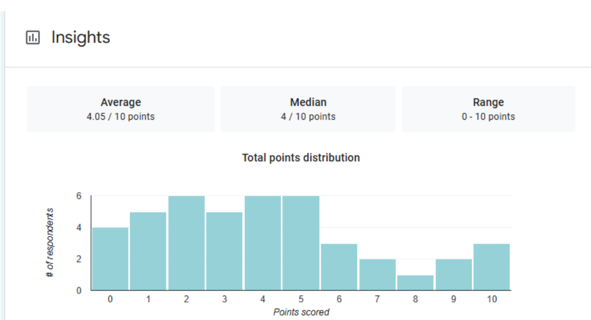

Figure 1: Pre-assessment results

The results of the pre-assessment in Fig. 1 showed that many of the participants understand what phishing is but fail to recognize common factors often used by cybercriminals. From the simulation email, over half of the participants actually inputted the credentials to change their passwords, hence falling victim to the simulated email. A quarter of the participants clicked on the link but never input their credentials, and the last bit of them discarded the email because some forgot, and the rest became suspicious of it. The results of the pre-assessment and the results of the simulation email helped pave the way for the pilot program to be implemented for a group of participants who showed a lack of understanding of the topic.

Session One
In session one of PhishBusters, participants were introduced to the fundamentals of phishing, covering essential topics to build a solid foundation. The session began by exploring the several types of phishing attacks, including email phishing, spear-phishing, smishing, vishing, and whaling. Each type of attack was explained with examples to better help participants recognize how these tactics differ in approach and target.

The session then went on to discuss the reasoning behind phishing attacks, highlighting the motivation of cybercriminals, such as financial gain, data theft, and unauthorized access to systems. Participants learned about the types of information these attacks aim to steal, which can include login credentials, personal data, and financial information.

The session also emphasized the dangers of phishing attacks, underscoring the potential for financial loss, reputational damage, identity theft, and compromised security within organizations. Real-world examples were reviewed to illustrate the serious consequences of falling victim to phishing and the broad impact it can have on individuals and businesses alike.

To reinforce learning in a memorable way, the session ended with an interactive Kahoot quiz. The game reviewed the day's material, allowing participants to test their knowledge in a fun, competitive environment. This not only solidified key concepts but also created a lively and engaging conclusion to the session, setting a positive tone for the training journey ahead.

Session Two
In session two of the PhishBusters, the focus was on building practical skills for recognizing phishing attempts, specifically in email form. The session began by discussing common indicators of phishing emails, such as suspicious sender

addresses, unexpected attachments, spelling and grammar errors, and urgent or threatening language designed to pressure the recipient into acting. The session covered how an attacker's main goal is to mess with their mind and act upon human behavior, in which one panics when receiving an alarming email instead of first stopping and thinking for a moment about where and why the email was coming.

Next, link-hovering techniques were introduced as a critical skill for phishing detection. Participants learned how to hover over links without clicking, revealing the actual URL and helping them verify the link's legitimacy. This led to exploring the concept of email domains with an emphasis on understanding how legitimate domains (like company URLs) differ from those commonly used in phishing attempts (such as a lookalike or slightly altered domains). The session then moved on to practicing identifying suspicious links, with participants examining examples to spot inconsistencies and subtle misspellings intended to trick users into trusting fake websites.

For hands-on practice, participants engaged with interactive slides where they reviewed simulated phishing emails to determine whether each one was legitimate or a phishing attempt. They were asked to highlight specific indicators that signaled a potential phishing email, helping them solidify their recognition skills in a controlled environment.

This session combined theoretical knowledge with practical exercises, empowering them to apply their training in real-world scenarios and boosting their confidence in identifying phishing emails accurately.

Session Three

In session three of PhishBusters, the session began by reviewing the key concepts covered in the first two sessions. The types of phishing attacks, common indicators, link-hovering techniques, and identifying suspicious domains were revisited, reinforcing participants' understanding and building confidence in their phishing detection skills.

After the review, participants were introduced to how to report phishing attempts within the organization, covering the steps for identifying and escalating suspicious emails. The session covered who the best person to contact is and the built-in reporting tools found in their email with a simple click. The importance of promptly reporting phishing attempts to reduce the organization risk and protect employees was emphasized.

The session discussed the proper steps to take if one does fall victim to clicking on a malicious link, including changing any compromised passwords, disconnecting from the network, and alerting the IT team so they can scan the system for any malware that may have been installed. It was an important topic to include in this session, as participants are left with an understanding of how to minimize potential damage if they were to fall victim to such an attack. Adding this topic to a phishing training program is important as not only do participants learn how to identify emails, but also what to do in case they mistakenly identify a fraudulent email as legitimate.

The session continued with a focus on multi-factor authentication (MFA) and password security. The importance of MFA as a defense mechanism that provides additional layers of security was covered, making it harder for attackers to gain unauthorized access even if credentials are compromised. Following that, strong password practices and password management tools were discussed, encouraging participants to create unique, complex passwords and use managers to securely store them.

The session concluded with a group discussion where participants shared their experiences, challenges, and thoughts on implementing these security practices in daily activities. This open forum allowed them to ask questions, exchange tips, and reinforce what they had learned in a collaborative environment, fostering a proactive approach to phishing prevention and cybersecurity awareness.

Post-Assessment and Final Simulation Email

In the post-assessment, participants completed a final evaluation to measure their knowledge retention and practical skills gained throughout the sessions. This assessment revisited key concepts covered in the program, including identifying phishing types, recognizing suspicious email indicators, and malicious links. The goal was to ensure that participants could confidently spot phishing attempts and respond correctly in real-world scenarios.

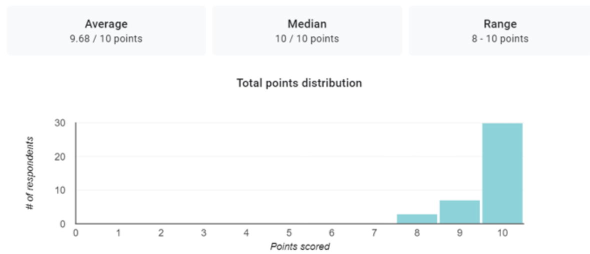

Figure 2: Post-assessment results

Fig. 2 shows the results of the post-assessment, where a significant jump in results from the pre-assessment can be seen. The results help give an insight into the success of the training, in which it can be seen that most participants increased their knowledge and understanding, and were able to accomplish significant improvement in identifying and understanding what phishing is.

Alongside the post-assessment, participants received a final phishing simulation email designed to test their ability to apply the training in a realistic situation. This simulation incorporated elements discussed in previous sessions, such as unusual sender addresses, subtle domain variations, and links to unverified websites. The hope was to ensure that the participants would use their newly acquired knowledge to ensure that they reported the email and did not act upon it. Successfully, all the participants were able to identify this email, and thirty-eight reported the email as phishing, and the rest deleted the email without clicking anything in it.

Feedback Collection Methodology

To systematically gather participant feedback, we employed a multi-faceted approach that combined structured and informal feedback collection methods. This comprehensive approach allowed us to capture both quantitative and qualitative insights about the training program's effectiveness and participant experience.

Structured Feedback Collection

We distributed a formal feedback survey to all 42 participants immediately following the completion of the third training session. The survey was administered through Google Forms and included both Likert-scale questions and open-ended response sections. The structured survey covered the following areas:

- Overall program satisfaction (1-5 scale)
- Clarity of content presentation (1-5 scale)
- Effectiveness of hands-on exercises (1-5 scale)
- Usefulness of phishing simulations (1-5 scale)
- Engagement level during group discussions (1-5 scale)
- Perceived improvement in phishing detection skills (1-5 scale)
- Open-ended questions about program strengths and areas for improvement

Informal Feedback Collection

In addition to the structured survey, we conducted informal feedback sessions during and after each training session. These included:

- Real-time verbal feedback during group discussions
- Post-session informal conversations with participants
- Observations of participant engagement and interaction during activities
- Follow-up discussions with participants who had clicked on the initial phishing simulation

Feedback Analysis

The feedback from the phishing program was overwhelmingly positive, with participants expressing high satisfaction across multiple areas that contributed to an enjoyable and effective learning experience. Everyone expressed their gratitude in terms that they felt the program was clear, effective, and easy to understand the concepts.

One of the main highlights was the clarity of the concepts presented. Participants consistently noted that the training content was broken down into easy-to-understand, digestible parts, making even complex aspects of phishing accessible to all skill levels. The straightforward explanations and clear examples helped demystify phishing tactics, enabling participants to grasp essential concepts quickly without feeling overwhelmed.

The hands-on practical exercises and realistic phishing simulations were another standout feature of the program. These exercises allowed participants to apply what they had learned immediately, giving them a chance to practice identifying phishing attempts in a controlled, real-world-like environment. Many participants commented that these simulations helped build confidence in recognizing phishing attempts and improved their skills in assessing suspicious emails and messages. This immersive approach not only reinforced theoretical knowledge but also equipped them with practical skills they felt ready to use in their daily routines.

Some of the participants also highlighted the value of learning in a group environment. They found that collaborating with colleagues and discussing examples added an engaging, social dimension to the training. Working alongside others allowed for shared insights, encouraged discussions, and provided additional perspectives, making the learning process more dynamic and interactive. This environment also fostered a sense of teamwork and mutual support, further enhancing the experience.

Another popular element was the Kahoot quiz game that was incorporated after some of the lessons. This interactive quiz added a fun and competitive edge to the training, which helped lighten the learning atmosphere and made key takeaways memorable. By testing their knowledge in a playful format, participants could immediately see what they had retained, reinforcing core concepts while boosting their enthusiasm and engagement. The game also highlighted any remaining areas for improvement in a positive, low-pressure setting, which contributed to a lasting understanding of the material.

Overall, the training left participants feeling more confident and informed about phishing. They expressed appreciation for a well-rounded program that combined clarity, practical experience, interactive group work, and gamified learning to create a thorough and engaging educational experience.

5. REFLECTION

Reflecting on the PhishBusters program, the impact and positive feedback received from participants were extremely pleasing. Going into the training, the aim was to create a program that was accessible, engaging, and directly applicable to participants' everyday experiences with phishing. Seeing that participants found the material easy to understand confirmed that the right balance was struck in breaking down complex concepts into clear, straightforward explanations. Their comments on the clarity and accessibility of the content affirm that the efforts to demystify phishing terminology and methods were successful.

The hands-on practical exercises and simulations seemed to be a standout feature of the training, which was particularly rewarding to hear. These simulations were designed to bridge the gap between theory and real-world application, and participants' feedback suggests that they felt more confident in recognizing phishing attempts as a result. Watching them actively engage with these exercises reinforced the belief that practical experience is invaluable in cybersecurity training.

The group learning environment also played an impressive role. It was observed that it encouraged open discussions and knowledge sharing among participants. It was great to see how this setting fostered collaboration and allowed participants to learn from one another, making the training not only informative but also socially interactive. This added a level of engagement that contributed to the program's success, as participants felt supported and motivated by their peers.

The incorporation of the Kahoot game was a deliberate choice to make the training experience enjoyable and memorable. Based on feedback, the game's competitive yet lighthearted atmosphere achieved its purpose. It reinforced key concepts in a way that was both fun and effective, making the program feel less like a lecture and more like an interactive experience. Seeing participants eager to test their knowledge in this format confirmed the value of incorporating gamified learning into future sessions.

Participants' responses indicate that the program not only improved their phishing detection skills but also left them feeling more confident and empowered. This training reflection has reinforced the importance of balancing clarity, practicality, interactivity, and fun in cybersecurity education. Moving forward, these elements will continue to be refined to enhance engagement and effectiveness, knowing they resonate well and leave participants with a solid foundation to recognize and handle phishing threats confidently.

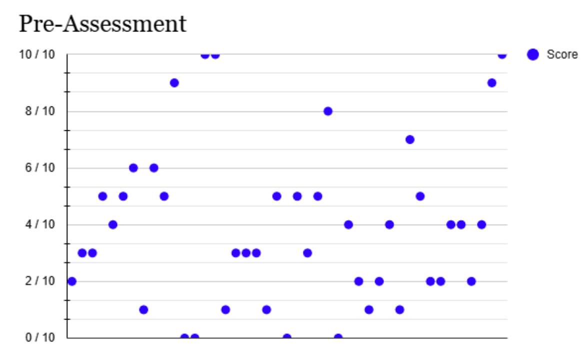

Figure 3: Pre-Assessment Confidence Levels

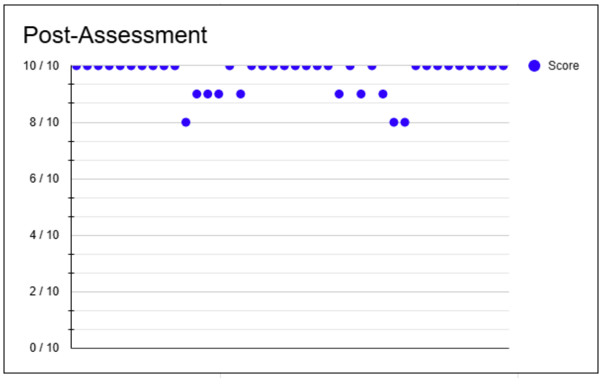

Figure 4: Post-Assessment Confidence Levels

The success of the program can be seen in comparing Fig. 3 and Fig. 4, which show the results of the pre-assessment scores and the post-assessment. An improvement can be seen where almost all participants scored significantly improved as compared to their first test scores. Analyzing the scores side by side allows for the conclusion that a vast majority of participants walked away with new understanding about phishing and have a better understanding of what it is and what they can do to protect sensitive information.

6. CHALLENGES

Developing a phishing training curriculum for employees with no prior knowledge of phishing presented several challenges that needed to be overcome to create a successful training program that would benefit everyone who participated in it.

Simplifying Technical Concepts
Phishing involves various technical elements such as domains, spoofing, and social engineering tactics that are difficult for non-technical participants to grasp. Having to simplify these concepts without oversimplifying or overwhelming participants is a challenge of its own, as one must figure out what information is key or a building block to ensure that participants will successfully understand the concepts at the end.

Overcoming Initial Skepticism or Disinterest
Participants unfamiliar with cybersecurity may not fully understand the relevance or importance of phishing prevention, which leads to disengagement. This makes it a crucial step to show them how phishing impacts them personally and professionally by showing them real-world examples or testimonies of victims who have lost so much by not being informed. This is a stepping stone in getting participants to want to participate and learn more about the topic.

Building Confidence with New Skills
For those participants with limited tech experience, actions like hovering over links or identifying email domain inconsistencies can feel intimidating. Ensuring they gain confidence and feel capable of using these skills requires a gradual, supportive approach with plenty of practice. Showing them and having them practice these skills while they are there ensures they can ask questions during the learning process, so when they are alone, they know exactly what to do and not to do.

Avoiding Overload while Covering Essentials
Participants new to phishing may begin to feel overwhelmed if there is too much information being presented at once. It is essential to prioritize key concepts and provide information incrementally, making it digestible and allowing time for practice. This was the main reason for splitting the training into three different sessions, in which each session covered different core concepts that serve as the foundation for understanding the topic.

Creating Engaging and Relatable Examples
Many phishing examples are built around IT-specific contexts. Finding examples that resonate with non-technical employees and relate to their everyday work and personal experiences is critical for engagement and retention. By creating examples that align with their work environment, an environment is created in which they see examples of what they may encounter in their everyday lives.

7. NEXT STEPS

After carefully analyzing the results of this training and considering the feedback received, several next steps and ideas have been identified to further refine the phishing training program.

Enhance Realism in Simulations
The introduction of more nuanced phishing simulations that mimic evolving tactics, including spear-phishing and whaling attacks, will help participants advance from basic to more sophisticated scenarios, building resilience against varied phishing techniques. Adding simulations that include smishing and social media-based phishing attempts will help broaden awareness beyond email-based phishing and reinforce cross-platform vigilance.

Expand Hands-On Practical Components

Beyond incorporating phishing exercises during the training, providing "surprise" phishing emails throughout the training can help test participants' skills at random points and see how vigilant they are. A module could also be added where participants simulate reporting a phishing attack, documenting it, and following an incident response plan. This step could help reinforce proper response protocols and ensure participants know what to do when they spot a potential threat.

Increase Personalized Feedback and Follow-up
Personalized feedback can be provided after each phishing simulation, focusing on what participants did well and areas where they can improve. This will encourage continuous learning and allow individuals to refine their skills in real time. The introduction of quarterly phishing simulations as ongoing training, with reports that track improvements and highlight recurring issues, would create a continuous learning loop and help reinforce the knowledge gained in the initial training.

Introduce Gamification and Interactive Learning Modules
In addition to Kahoot, other quiz formats or gamified challenges (like scenario-based role-playing games) could be considered, where participants decide how to respond to a potential phishing email in different contexts. A leaderboard through the program could be implemented that recognizes top performers in phishing simulations or quizzes. This could foster friendly competition and motivate participants to stay engaged and alert.

Leverage Peer Learning and Group Exercises
Opportunities could be created for participants to analyze real phishing cases in small groups, encouraging discussion on what tactics were used and how they could be detected. This could also be used as an ongoing activity that keeps teams informed of new phishing techniques. Another option could be to pair participants with a "security buddy" to encourage collaboration, allowing them to check in with each other on suspicious emails or share insights, fostering a culture of teamwork and continuous learning.

Expand the Scope of Training with Specialized Modules
PhishBusters could develop specialized modules tailored to specific roles, such as finance or HR, which often face unique phishing risks. Customizing content to match participants' job functions will improve the relevance and applicability of the training. Optional modules on advanced phishing tactics (like email spoofing and social engineering) could be provided for those participants who may require a deeper understanding of these issues.

Gather Long-Term Feedback and Track Progress
Follow-up surveys and periodic knowledge assessments could be implemented to track how well participants retain the material over time, allowing adjustments based on the latest trends or areas of improvement. The data collected could be used to identify trends such as common mistakes or departments with higher click rates, to tailor future training and reinforce high-risk areas.

By building on these next steps, the phishing training can become an even more comprehensive, practical, and engaging program, promoting continuous improvement in phishing awareness and response across the organization. In the future, the possibility of implementing a program like this one at the high school level when teenagers are using technology a lot more could be explored to ensure phishing education begins early on in their lives.

8. CONCLUSION

In conclusion, the PhishBusters training program has proven to be a valuable and well-received initiative, effectively enhancing participants' phishing awareness and response skills. Feedback has highlighted the program's clarity, hands-on exercises, and engaging group environment, as well as the success of interactive elements like the Kahoot game, which made learning enjoyable and memorable. Reflecting on the training experience, it is clear that combining straightforward explanations, practical simulations, and gamified learning can significantly enhance confidence and knowledge in phishing detection, particularly for individuals with diverse skill levels.

Looking ahead, there are many promising opportunities to further refine the program. By increasing simulation complexity, expanding role-specific training, and incorporating ongoing assessments and feedback, it can be ensured that PhishBusters training remains relevant, practical, and effective. Adding quarterly simulations, leaderboards, and real-life case discussions will keep participants engaged and vigilant, fostering a culture of continuous learning. Altogether, these steps will not only improve phishing recognition skills but also support a proactive and security-minded organization well-pared to handle evolving phishing threats.

By creating PhishBusters, employees were empowered with the knowledge and skills to recognize and respond to phishing threats. A proactive security culture was fostered that reduces the likelihood of successful phishing attacks and mitigates potential organizational risks. By educating employees on phishing tactics, prevention strategies, and response protocols, their confidence and vigilance were enhanced, making them the first line of defense against cyber threats. Additionally, by incorporating engaging and practical elements like simulations and group activities, the training was made impactful and memorable, leading to long-term behavioral change and a more resilient organization overall.

9. REFERENCES

Marcus Butavicius, Ronald Taib, and Sigi J. Han. Why people keep falling for phishing scams: The effects of time pressure and deception cues on the detection of phishing emails. *Computers & Security*, 123: 102937, 2022. doi: 10.1016/j.cose.2022.102937. URL https://doi.org/10.1016/j.cose.2022.102937.

Rachna Dhamija, J. Doug Tygar, and Marti Hearst. Why phishing works. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 581–590, New York, NY, 2006. Association for Computing Machinery. doi: 10.1145/1124772.1124861. URL https://doi.org/10.1145/1124772.1124861.

Sanjay Goel, Kevin Williams, and Ersin Dincelli. Got phished? Internet security and human vulnerability. *Journal of the Association for Information Systems*, 18(1):2, 2017. doi:10.17705/1jais.00447. URL https://doi.org/10.17705/1jais.00447.

Brian Harrison, Elena Svetieva, and Arun Vishwanath. Individual processing of phishing emails: How attention and elaboration protect against phishing. *Online Information Review*, 40(2):265–281, 2016. doi: 10.1108/OIR-04-2015-0116. URL https://doi.org/10.1108/OIR-04-2015-0116.

Mahmoud Khonji, Youssef Iraqi, and Andrew Jones. Phishing detection: a literature survey. *IEEE Communications Surveys & Tutorials*, 15(4):2091–2121, 2013. doi: 10.1109/SURV.2013.032213.00009. URL https://doi.org/10.1109/SURV.2013.032213.00009.

Tyler Moore and Richard Clayton. Examining the impact of website take-down on phishing. In *Proceedings of the Anti-Phishing Working Groups 2nd Annual eCrime Researchers Summit*, pages 1–13, New York, NY, 2007. Association for Computing Machinery. doi: 10.1145/1298955.1298956. URL https://doi.org/10.1145/1298955.1298956.

Kathryn Parsons, Agata McCormac, Marcus Pattinson, Marcus Butavicius, and Cate Jerram. Phishing for the truth: A scenario-based experiment of users' behavioural response to emails. In *Security and Privacy Protection in Information Processing Systems: 28th IFIP TC 11 International Conference, SEC 2013*, pages 366–378, Berlin, Heidelberg, 2013. Springer. doi: 10.1007/978-3-642-39345-7_39. URL https://doi.org/10.1007/978-3-642-39345-7_39.

Steve Sheng, Bryant Magnien, Ponnurangam Kumaraguru, Alessandro Acquisti, Lorrie Faith Cranor, Jason Hong, and Elizabeth Nunge. Anti-phishing phil: the design and evaluation of a game that teaches people not to fall for phish. In *Proceedings of the 3rd Symposium on Usable Privacy and Security*, pages 88–99, New York, NY, 2007. Association for Computing Machinery. doi: 10.1145/1280680.1280692. URL https://doi.org/10.1145/1280680.1280692.

Steve Sheng, Mandy Holbrook, Ponnurangam Kumaraguru, Lorrie Faith Cranor, and Julie Downs. Who falls for phish? a demographic analysis of phishing susceptibility and effectiveness of interventions. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 373–382, New York, NY, 2010. Association for Computing Machinery. doi: 10.1145/1753326.1753383. URL https://doi.org/10.1145/1753326.1753383.

Verizon. 2023 data breach investigations report. Verizon Business, 2023. URL https://www.verizon.com/business/resources/reports/dbir/. Retrieved from https://www.verizon.com/business/resources/reports/dbir/.

Emma J. Williams, Joanne Hinds, and Adam N.

Joinson. Exploring susceptibility to phishing in the workplace. *International Journal of Human-Computer Studies*, 120:1–13, 2018. doi: 10.1016/j.ijhcs.2018.07.003. URL https://doi.org/10.1016/j.ijhcs.2018.07.003.