Hidden in Onboarding: Cyber Hygiene Training and Assessment

Alex Katsarakes[1], Thomas Morris[2], and Jeremiah D. Still[2]

[1] Old Dominion University, Norfolk, VA, 23529, USA
[2] Eastern Kentucky University, Richmond, KY 40475, USA
{ekats002 | jstill}@odu.edu

Abstract. End-users are our first line of defense against cyber-attacks. The U.S. government has endorsed training videos that teach cyber hygiene best practices, aiming to harden our defenses. In this pilot study, we explored the effectiveness of those security training videos under the cover of an employee onboarding scenario and general computer competency questions. Masking the cybersecurity focus of this study was critical to prevent unnatural heightened vigilance. For example, increased awareness of cybersecurity threats can artificially increase sensitivity to phishing emails or identify malicious links. Participants' cyber hygiene knowledge was assessed by pre- and post-tests after receiving the training. In addition, we measured behavioral onboarding task performance based on the training learning objectives. Our findings showed a lack of improvement in quiz knowledge and onboarding security activities after exposure to the training. We echo others in the literature by claiming the need for a paradigm shift in how traditional cybersecurity training is taught and how success is measured.

Keywords: Cybersecurity, Human Factors, Training.

1 Introduction

1.1 Current State of Cyber

The prevention of cyberattacks has become a critical concern for organizations worldwide [1]. Cybersecurity attacks have only continued to rise in recent years, with organizations, individuals, and critical infrastructure remaining vulnerable to various threats [2]. The consequences of successful breaches, including loss of productivity, financial destruction, and damage to institutional credibility, underscore the potential severity of the issue [3].

Many cyber incidents are attributed to vulnerabilities associated with human actors, exemplifying the importance of end-user competency in preventing attacks [4, 5]. Users tend to overestimate their cybersecurity expertise and abilities [4], leading to an underestimation of risk. Prior cyber hygiene research has shown that users' self-perception of their expertise in home network cybersecurity is higher than their practical task performance scores [6]. As the Home Computing (HC) environment blends with organizational resources [7], assets become both personal and institutional. Within this new technological ecosystem, lack of cyber hygiene abilities can cost an individual as well

as their employer. It is not merely a matter of personal security; it translates into a substantial risk factor for businesses and, by extension, the broader economy. For example, hackers demanded a $4.4 million ransom during the 2021 Colonial Pipeline Co. attack [8]. The effects of this attack rippled throughout the US economy, by causing a fuel shortage. Hackers entered Colonial Pipeline Co.'s networks through a compromised Virtual Private Network (VPN) account, which was created to allow employees to access the company's computer network remotely from their home network. A single employee's poor cyber hygiene practices caused significant damage to the company and the U.S. economy. This recent crisis also demonstrates the progression beyond the Bring-Your-Own-Device (BYOD) strategy to a hybrid Bring-Your-Own-Network (BYON) model. The current merge of the HC ecosystem with organizational computing will generate a unique set of human-centered cybersecurity challenges [7].

To address these challenges, cyber defenders are teaching end-users to follow best practices in cyber hygiene [9]. This focus is driven, in part, by the realization that many contemporary cybersecurity threats cannot be entirely mitigated via technological avenues [10-11]. With most incidents being caused by user error, those interested in avoiding breaches must focus on the human elements of cyber hygiene and information security [4, 11].

The traditional approach taken by cybersecurity training programs is generally referred to as *awareness* [12-13]. Particularly prevalent in government-led initiatives, these security campaigns target improving cyber hygiene behaviors through comprehensive education and heightened awareness of potential threats [13]. These programs operate assuming that end users who are aware of cybersecurity risks and provided with information on how to subvert them will change their behavior accordingly [13]. While these campaigns play an important role in cybersecurity training, their effectiveness has been scrutinized. The assumption that providing information alone will induce change has limitations, with many of these programs failing to generate a desirable impact [14, 11]. As Ghazvini and Shukur [15] put it quite concisely, "Even though the number of information security awareness training programs are growing progressively, there is inadequate evidence to verify their effectiveness and impact on daily activities in a work environment" (p. 1). While it is important to ensure that end-users are aware of potential cyber threats, being informed is only an initial step to generating real modifications in behavior [14, 16] Actual change requires more than providing information about risks and prevention; individuals must be able to comprehend the information and be motivated to actively apply the advised practices [17]. Current approaches fall short in multiple aspects, often producing minimal practical outcomes for trainees and organizations [18]. Training users in cyber hygiene competency is essential to preventing cyber-attacks on organizations and institutions, but the field has been unable to determine the optimal approach [9].

1.2 Training Types

In the dynamic landscape of cybersecurity training, an array of methods are employed to reinforce cyber hygiene behaviors and bolster awareness. Some of the most common techniques include game-based, presentation-based, simulation-based, video-based,

text-based, and discussion-based [9]. Game-based training involves the gamification of learning, creating interactive scenarios that engage participants in immersive experiences to enhance comprehension [2]. Conventional presentation-based training relies on conveying crucial cybersecurity information through presentations such as slideshows, lectures, or other multimedia formats to deliver key concepts and demonstrate best practices [2]. Simulation-based training replicates real-world cyber threats and scenarios, allowing participants to actively engage with simulated incidents and develop practical skills in response and mitigation [16]. Video-based training employs visual content, such as educational videos or documentaries, to communicate cybersecurity concepts [2]. Text-based training conveys cybersecurity information through written materials, such as documents and manuals designed to educate end-users on security practices and potential threats [9]. Discussion-based training fosters interaction and dialogue among participants, utilizing group discussions, case studies, and collaborative problem-solving sessions to facilitate the exchange of insights [9]. The continual exploration of these diverse training methods and the generation of new ones reflects ongoing efforts to discover effective approaches for developing robust cyber hygiene practices among end-users.

1.3 Assessing Effectiveness

While analyzing training programs' efficiency, there was a notable lack of consistency in how the outcomes of cyber hygiene and security training are measured [16]. According to Prümmer et al.'s [9] literature review, the measurements often deviate from direct assessments of cyber security behaviors and instead focus on attitudinal changes, user perceptions, or simple behavioral intentions instead of real behavioral change. Although these factors can be considered predictors of behavioral change, they fail to assess the application of the training on end-user competency. Their review concludes by encouraging the implementation of objective behavioral measurements to determine training effectiveness.

Beyond the commonly used perceptual and attitudinal aspects, a wide range of performance measures are currently utilized to assess cyber security trainee performance. In their review of cybersecurity training evaluation metrics, Koutsouris et al. [12] named 20 such measures, ranging from the number of successful attacks to the efficiency of reporting cyber incidents. While the sheer number of metrics speaks to the researcher's attempts to uncover the impact of training on practical outcomes, the evident inability to consistently measure training success sabotages the field's capacity to compare various training types. Across the board, there is a notable lack of agreement on methods for evaluating training solutions, which makes it strikingly difficult to assess the efficacy of solutions [2].

1.4 Our Study

We utilized an employee onboarding scenario to test the transference of cyber hygiene knowledge and skills into day-to-day work activities. One of the primary aspirations of awareness training programs is to push employees to actively engage in cyber security

behaviors for their everyday employment activities [15]. Given the increasing overlap between organizational and personal security, ensuring that users within a home computing environment are able to apply knowledge is crucial to safeguarding information and resources [7].

As Ghazvini and Shukur [15] pointed out, many training programs fail to measure user behavior before and after implementing an intervention, which prevents an accurate evaluation of practical outcomes. We attempted to remedy this issue within our research by utilizing a pre/post-test methodology for both the knowledge acquisition and user behavior measures. The knowledge tests include two components: 1) answering questions from the training videos and 2) completing the Cyber Hygiene Inventory (CHI). According to Vishwanath et al. [19], CHI is a valid and consistent measure of five distinct dimensions of cyber hygiene. The measure is meant to be predictive of behavior. We plan to use CHI to capture our participants' general cyber hygiene knowledge and examine its ability to predict behavioral onboarding performance.

Notably, this study camouflages its cybersecurity research focus. This was done by masking the cyber security assessment within general computer competence questions, placing demographic questions at the end of the study procedure, and disguising cyber hygiene tasks within an employee onboarding scenario. The primary justification for this approach lies in the well-documented phenomenon known as demand characteristics, which are aspects of a study that convey what behaviors are expected or desirable, which artificially change behavior [20]. This is particularly pertinent in cybersecurity research, where participants' awareness of being assessed on cyber hygiene might lead them to behave more cautiously than they would in a non-evaluative environment.

Masking the cybersecurity intent in this study was critical to prevent heightened vigilance in tasks such as responding to phishing emails or identifying malicious links. Being aware that the research assessed cyber security could inflate their performance on these tasks, skewing the results and undermining the study's ability to accurately evaluate their adherence to best practices [21]. Using an employee onboarding scenario also increased the ecological validity of the study, making the results more indicative of how individuals may act in everyday cyber scenarios within organizations [15, 22]

2 Methods

2.1 Participants

This pilot study had ten undergraduate students from a large public university in the southeastern region of the United States of America. They were recruited through the Psychology department's SONA system. Each participant was compensated with two research credits for their involvement in the study. The average age of the participants was 19.6 years (SD = 1.32). The sample had a balanced gender distribution, with an equal split of the biological sexes.

Other relevant demographics were collected, including average technology use time in a day, college major, and prior cybersecurity experience. In terms of digital technology usage, participants reported an average of 11.1 hours per day (SD = 5.39) spent engaging with various forms of technology, including academic work, social media

usage, entertainment, and other personal use. Two participants were majoring in technical fields, which encompassed disciplines related to engineering, computer science, or information technology. Finally, 2 participants had prior training in cybersecurity. This prior exposure to technical and cybersecurity-related content is notable, as it may influence the participants' interaction with and understanding of the technological aspects of the study. Their performance will be considered separately within the results section.

2.2 Materials

The onboarding tasks and cybersecurity training were conducted using a standard desktop computer. The computer had an Intel Core i5 processor with a Windows 10 operating system. The monitor was a 24-inch LED display with a resolution of 1920 x 1080 pixels. This setup provided a consistent and controlled environment for all participants to engage with the training material. The video training consisted of interactive government-sponsored instructional videos designed to enhance participants' knowledge and awareness of cybersecurity principles [23]. These videos training, totaling approximately 30 minutes, covered various topics, including password security, phishing, malware prevention, and safe information practices. To assess participants' baseline cyber hygiene knowledge, participants completed a custom cyber hygiene quiz to evaluate the effectiveness of the training. The quiz was integrated into a broader set of computer competency questions and hosted on the Qualtrics survey platform. The quiz consisted of multiple-choice questions designed to assess key learning outcomes from the videos and onboarding tasks. Topics covered in the quiz included identifying phishing attempts, best practices for password creation, and utilizing VPN software. In addition, participants' baseline cyber hygiene knowledge was tested via the Cyber Hygiene Inventory [19]. This inventory is a validated assessment tool comprising items that measure various dimensions of cyber hygiene, including personal cybersecurity practices, awareness of common cyber threats, and knowledge of safe online behaviors. The inventory is structured as a self-report questionnaire with 5 point Likert-scale responses ranging from 'strongly disagree' to 'strongly agree'.

2.3 Procedure

Participants' cyber hygiene skills were assessed through a multi-step process, seamlessly integrated into an employee onboarding experience (Fig. 1). After providing informed consent, each participant completed an initial cyber hygiene quiz, masked within general computer competency questions. This was a deliberate effort to obscure the primary focus of the quiz and prevent participants' awareness of the study's intent from corrupting their answers. We aimed to elicit genuine responses reflecting participants' real-world knowledge levels by embedding the cyber hygiene components within a broader assessment. This quiz, therefore, provided a baseline measure of participants' cybersecurity knowledge and abilities.

Once the survey was complete, participants were immersed in the scenario via a verbal script read out by the researcher. They were instructed to assume a character

completing an onboarding process for their new job at POD Corp. The researcher asked each participant to complete tasks utilizing the character's information and adhere to all company policies. Much like the quiz, the onboarding simulation was presented in a manner that did not explicitly reveal its true purpose. This technique was employed to mitigate the risk of participants altering their natural behavior or decision-making processes due to preconceived notions about the study's objectives.

Participants received an onboarding sheet containing three explicit tasks and a list of company policies, which contained instructions for cyber hygiene behaviors. The three primary tasks were (1) Generate a corporate email account and password (2) Keep an eye out for any relevant emails and (3) Fill out and securely store company files. Attached to the task document was the list of company policies, which instructed all employees to perform behaviors such as "Make sure to encrypt files containing sensitive information", "Always enable two-factor/multi-factor authentication on any company-related accounts", and "Keep all software on your system up to date". The three primary tasks, and the implicit steps derived from the company policies, constituted the full onboarding process. Researchers observed, took notes, and marked completed tasks off on a behavioral checklist.

After the initial onboarding, participants were asked if they felt they had thoroughly completed everything the company required. If they did not, they were given more time to complete the tasks. If they responded affirmatively, they were notified that they would be completing an interactive cybersecurity training. This video-based DOD training aimed to enhance participants' understanding of cybersecurity practices and underscored the importance of adhering to policies on cyber behavior. Participants completed the training at their own pace and then moved into the next portion of the study.

Following the training, participants were prompted to revisit, redo, or revise their initial onboarding process based on knowledge gained from the cybersecurity training videos. Each was asked to consider the question: "Is there any part of the onboarding process that you would do differently, based on the information you just learned?" After being encouraged to redo or alter any initial onboarding tasks, participants were given the time to make any necessary changes. Researchers took detailed notes and marked off completed tasks on the behavioral checklist. This checklist served as a systematic record of participants' cybersecurity behaviors. Once participants felt they had completed all the tasks, they indicated to the researcher that they intended to make no further changes. They were then asked to complete a post-hoc Qualtrics survey on computer competency, which was an exact replica of the pre-test with the addition of a few demographic questions. Upon completing the survey, participants were dismissed from the study and received SONA research credit.

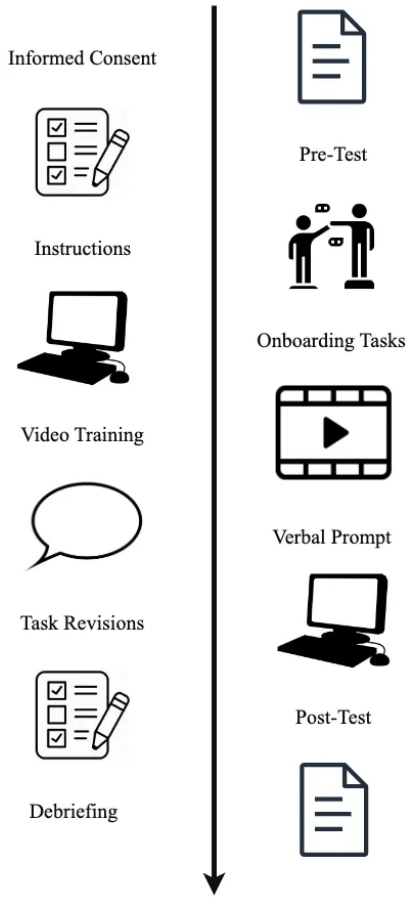

Fig. 1. The figure shows the experimental procedure of the study. The figure is meant to be read from left to right and top to bottom. The center arrow shows the progression of time with the labels and icons on either side of the arrow.

3 Results

3.1 Primary Analyses

The results were assessed for outliers and missing values. Of particular interest were two individuals who self-identified as cybersecurity experts. In terms of potential prior knowledge and skills, they were treated as outliers. We conducted the analyses with and without those participants' data and found that they only performed differently on the behavioral checklist. Therefore, their data were treated separately for the behavioral

checklist measure comparisons. No data had to be excluded for any of the other statistical tests. All the measures were converted to percentages for easier interpretation.

A paired samples t-test was conducted to determine the effect of the video training on post-test quiz scores. The findings indicate no significant difference between video training and quiz scores pre (M = 72%, SD = 18%) versus post (M = 79%, SD = 8%), $t(9) = -1.41$, $p = .193$, $d = -.44$. Therefore, we did not observe an effect of training on quiz performance.

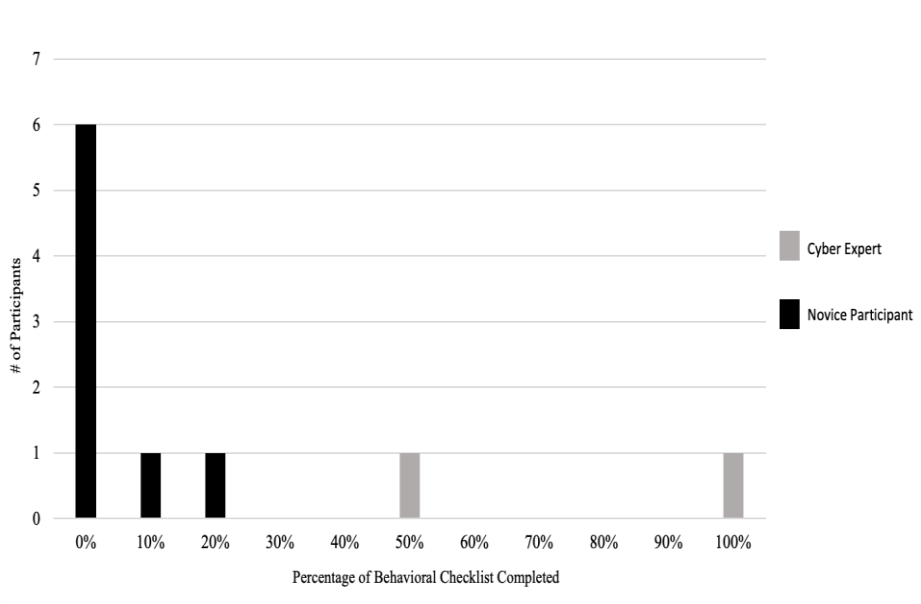

Fig. 2. The figure provides a bar graph showing the distribution of participants by the percentage of onboarding security checklist successfully completed. Cyber experts are represented by grey bars, while the black bars represent those not self-identifying as cyber experts.

Upon analyzing the results of the behavioral checklist, it was evident that participants fell short in their ability to execute cybersecurity behaviors. The checklist was designed to encapsulate both explicitly instructed and implicitly implied cyber hygiene practices as delineated in the company policy document. Initial scores assessment revealed a considerable shortfall in executing practical cyber hygiene behaviors among participants. The pre-intervention data (see Fig. 2), underscores widespread non-compliance with the suggested cybersecurity actions. This initial finding aligns with existing literature that emphasizes the gap between knowledge of cybersecurity best practices and applied behavior [17]. Following the intervention, only two participants demonstrated a tangible improvement in their cyber hygiene practices by completing additional tasks that aligned with the intervention's objectives, one of which was a self-identified cyber security expert. Conversely, a significant portion of the cohort exhibited no change, with completion rates stagnating at 0%. The checklist is also the only

measure where the self-identified cyber security experts showed different performance than the novice participants. A stark disparity in checklist completion rates becomes apparent when the two experts are excluded from the analysis. No novice participant scored over 20% on the behavioral checklist, demonstrating a substantial gap in cyber hygiene practices between individuals with specialized knowledge and those without.

Our final analysis compared scores on the Cyber Hygiene Inventory (M = 61%, SD = 12%) with behavioral checklist performance to assess if knowledge translated into the behavioral checklist. Coming into the laboratory, participants performed about average on the Cyber Hygiene Inventory. The CHI and the performance on the behavioral checklist scores were highly correlated, $r(9) = .69$, $p = .03$. However, only when including the self-identified experts. This indicates that for individuals with prior expertise in cyber hygiene, CHI may be predictive of their practical application skills as measured by the behavioral checklist. However, a different picture emerges when we consider the data excluding the experts. Among the non-expert participants, the CHI did not demonstrate predictive validity for performance on the behavioral checklist. The correlation coefficient was only $r(6) = -.22$, $p = .604$; this might be due to the restricted range from our small sample size. This suggests that for individuals without pre-existing expertise, knowledge does not necessarily translate into practical application proficiency.

In summary, the results do not show an improvement in scores from the pretest to the posttest, suggesting that the intervention was ineffective in enhancing the participants' behavior or knowledge.

4 Discussion

This study evaluated the effectiveness of government-endorsed cybersecurity training videos. We considered the impact the training had on enhancing cyber hygiene knowledge and behavioral outcomes during onboarding tasks. Across experts and novices, there was an evident failure to improve post-intervention, which questions the effectiveness of the training videos. This lack of improvement is striking, particularly given the increasing emphasis on the role of end-users in cybersecurity and the resources devoted to training initiatives. However, we do have to recognize this pilot study's limitations. The sample only contained ten participants, and two self-identified as having expertise in cyber security. It seemed participants lacked motivation towards the activities, which may have been due to participants not feeling actual ownership of data or the potential costs associated with not behaving securely. Future research ought to consider ways to address motivation and engagement.

A notable observation was the gap between scores on the CHI and behavioral checklist scores. Despite the expectation that enhanced knowledge would translate into adherence to cyber hygiene best practices, this congruence was not observed in novice users. On the other hand, self-identified cyber security experts showed a distinct proficiency in translating their knowledge into practical application, as observed by their substantially better behavioral checklist scores. This highlights that for those with a higher level of expertise, general cyber hygiene knowledge may be able to predict

performance in real-world scenarios. The distinction between experts and novices in their ability to apply information is critical in understanding the efficacy of cyber hygiene training programs and tailoring these programs to different levels of prior knowledge. Future research will have to look closer at the types of knowledge (e.g., declarative, procedural) in training programs to work towards improved real-world outcomes.

Similar to Bada et al. [14] and Van Steen et al. [13], our findings suggest that traditional methods might not be as effective as desired, especially for promoting behavioral change. The contrast may be attributed to differences in intervention design, participant demographics, or evaluation methods.

A key aspect of traditional cybersecurity training that is often overlooked is it application to real-world scenarios [15]. Uniquely, we embedded the cyber hygiene assessments within an employee onboarding scenario. Adding the situational information afforded us a realistic work setting to assess behavioral outcomes. This also enabled us to mitigate potential biases and ensure a more authentic assessment of participants' knowledge and behavior by hiding our research focus on cybersecurity.

Our approach aligns with the call for more objective behavioral measurements in assessing training effectiveness, as well as the need to develop more practical metrics [9]. And, it resonates with the writings of Bada et al. [14] and McCarthy [11], who question the efficacy of information-provision strategies in changing user behavior. Successfully training end-users in cyber hygiene best practices will require updated instructional practices along with more ubiquitous measures of success.

5 Conclusion

Our pilot study explored the effectiveness of government-endorsed training videos under the cover of an employee onboarding scenario. Masking the cybersecurity focus of the study was important to prevent heightened vigilance. The lack of improvement in both knowledge and application among participants after exposure to the training videos signals a need for a paradigm shift in how cybersecurity training is taught, and success is benchmarked. But, our findings must be considered with caution. Future work should address our study's limitations of a small sample size and participant motivation. Our data and real-world technical reports [24] show the current training is ineffective. Hackers are capturing significant amounts of data and society's limited resources. Cybersecurity as a discipline needs a heavier emphasis on human-centered design to address this significant societal issue [25].

Disclosure of Interests. The authors have no competing interests to declare that are relevant to the content of this article.

References

1. Ulsch, N.M. ed: Cyber Threat! Wiley (2014). https://doi.org/10.1002/9781118915028.
2. Chowdhury, N., Gkioulos, V.: Cyber security training for critical infrastructure protection: A literature review. Computer Science Review. 40, 100361 (2021). https://doi.org/10.1016/j.cosrev.2021.100361.
3. Abawajy, J.: User preference of cyber security awareness delivery methods. Behaviour & Information Technology. 33, 237–248 (2014). https://doi.org/10.1080/0144929X.2012.708787.
4. Cain, A.A., Edwards, M.E., Still, J.D.: An exploratory study of cyber hygiene behaviors and knowledge. Journal of Information Security and Applications. 42, 36–45 (2018). https://doi.org/10.1016/j.jisa.2018.08.002.
5. Chowdhury, N., Katsikas, S., Gkioulos, V.: Modeling effective cybersecurity training frameworks: A delphi method-based study. Computers & Security. 113, 102551 (2022). https://doi.org/10.1016/j.cose.2021.102551.
6. Vishwanath, A.: Stop telling people to take those cyber hygiene multivitamins. In: Prepared for Evolving Threats. pp. 225–240. WORLD SCIENTIFIC (2020). https://doi.org/10.1142/9789811219740_0014.
7. Morris, T.W., & Still, J.D.: Cybersecurity hygiene: Blending home and work computing. In W. Patterson (Ed.), New Perspectives in Behavioral Cybersecurity. Boca Raton, FL: CRC Press (2023).
8. Bogage, J.: Colonial Pipeline CEO says paying $4.4 million ransom was ‘the right thing to do for the country. (2021).
9. Prümmer, J., Van Steen, T., Van Den Berg, B.: A systematic review of current cybersecurity training methods. Computers & Security. 136, 103585 (2024). https://doi.org/10.1016/j.cose.2023.103585.
10. Craigen, D., Diakun-Thibault, N., Purse, R.: Defining Cybersecurity. Technology Innovation Management Review. 4, 13–21 (2014). https://doi.org/10.22215/timreview/835.
11. McCarthy, K.: Cybersecurity Awareness Training Methods and User Behavior. ProQuest Dissertations and Theses. (2021).
12. Koutsouris, N., Vassilakis, C., Kolokotronis, N.: Cyber-Security Training Evaluation Metrics. In: 2021 IEEE International Conference on Cyber Security and Resilience (CSR). pp. 192–197. IEEE, Rhodes, Greece (2021). https://doi.org/10.1109/CSR51186.2021.9527946.
13. Van Steen, T., Norris, E., Atha, K., Joinson, A.: What (if any) behaviour change techniques do government-led cybersecurity awareness campaigns use? Journal of Cybersecurity. 6, tyaa019 (2020). https://doi.org/10.1093/cybsec/tyaa019.
14. Bada, M., Sasse, A.M., Nurse, J.R.C.: Cyber Security Awareness Campaigns: Why do they fail to change behaviour? (2019). https://doi.org/10.48550/ARXIV.1901.02672.
15. Ghazvini, A., Shukur, Z.: Awareness Training Transfer and Information Security Content Development for Healthcare Industry. ijacsa. 7, (2016). https://doi.org/10.14569/IJACSA.2016.070549.
16. Kävrestad, J., Nohlberg, M.: Evaluation Strategies for Cybersecurity Training Methods: A Literature Review. In: Furnell, S. and Clarke, N. (eds.) Human Aspects of Information Security and Assurance. pp. 102–112. Springer International Publishing, Cham (2021). https://doi.org/10.1007/978-3-030-81111-2_9.
17. Deakin University Melbourne, Australia, Alruwaili, A.: A REVIEW OF THE IMPACT OF TRAINING ON CYBERSECURITY AWARENESS. ijarcs. 10, 1–3 (2019). https://doi.org/10.26483/ijarcs.v10i5.6476.

18. Proctor, W. R.: Investigating the efficacy of cybersecurity awareness training programs. ProQuest Dissertations & Theses Global; SciTech Premium Collection. (2016).
19. Vishwanath, A., Neo, L.S., Goh, P., Lee, S., Khader, M., Ong, G., Chin, J.: Cyber hygiene: The concept, its measure, and its initial tests. Decision Support Systems. 128, 113160 (2020). https://doi.org/10.1016/j.dss.2019.113160.
20. Nichols, A.L., Maner, J.K.: The Good-Subject Effect: Investigating Participant Demand Characteristics. The Journal of General Psychology. 135, 151–166 (2008). https://doi.org/10.3200/GENP.135.2.151-166.
21. Sharma, K., Zhan, X., Nah, F.F.-H., Siau, K., Cheng, M.X.: Impact of digital nudging on information security behavior: an experimental study on framing and priming in cybersecurity. OCJ. 1, 69–91 (2021). https://doi.org/10.1108/OCJ-03-2021-0009.
22. Fahl, S., Harbach, M., Acar, Y., Smith, M.: On the ecological validity of a password study. In: Proceedings of the Ninth Symposium on Usable Privacy and Security. pp. 1–13. ACM, Newcastle United Kingdom (2013). https://doi.org/10.1145/2501604.2501617.
23. Cybersecurity Awareness. Security Awareness Hub: Select eLearning Awareness Courses for DOD and Industry (2014).
24. Basset, G., Hylender, C., Langlois, P., Pinto, A., Widup, S.: Data breach 2020 investigations report - Verizon business. Retrieved April 10, 2022, from https://www.verizon.com/business/en-gb/resources/reports/2020-data-breach-investigations-report.pdf (2020).
25. Still, J. D.: Cybersecurity needs you! ACM Interactions (May + June: Feature), 23, 54-58 (2016).