Cybersecurity on the Move: Investigating the Efficacy of a Movable Escape Room as an Educational Tool for Healthcare Employees

Luka Koning and Jan-Willem Bullee
Industrial Engineering and Business Information Systems - Faculty of Behavioural, Management and Social Sciences (BMS), University of Twente, Enschede, The Netherlands

l.koning@utwente.nl
j.h.bullee@utwente.nl

Abstract: *Introduction*: This research investigates the effectiveness of a cybersecurity escape room as an educational intervention to increase awareness of cybersecurity risks towards a safer work environment. The escape room aims to educate participants and cybersecurity and to make them more resilient against various cyberthreats. *Method*: To validate the effectiveness, a pre-test-post-test design with 96 participants was conducted, 42 also completing a delayed post-test and 29 participants served as a control group. All participants were healthcare professionals. Using the HAIS-Q, six themes were investigated (namely email usage, passwords, ransomware, social engineering, incident reporting, and software updates) using the three constructs from the Knowledge, Attitude and Behaviour model. *Results*: The escape room had an overall immediate positive effect on participants ($t(95) = -6.259$, $p < 0.001$), and this effect persisted after 1 month ($t(25) = -2.946$, $p = .006$). Zooming in on individual themes, the immediate scores improved for email usage, passwords, social engineering and software updates, whereas the delayed scores improved specifically for email usage and passwords. *Conclusion*: The results show that the cybersecurity escape room may be a promising way to enable employees to resist cybersecurity threats. Nonetheless, the results need to be interpreted with caution. The research design experienced some dropout, meaning that results could differ with increased participation. Furthermore, it is not entirely evident which aspects of the escape room caused the observed effect; this is subject to future research.

Keywords: Cybersecurity, Educational Intervention, Escape Room, HAIS-Q, Healthcare.

1. Introduction

The implementation of Electronic Health Records (EHR), widespread use of wireless devices and the uptake of the Internet of Things (IoT) has changed patient care and hospitals in a rapid pace. The use of interconnected devices is now a standard practice of almost every patient (Cartwright, 2023). This, however, also results in an increased and diverse attack surface, threatening the operational continuity of both patient data and hospital processes.

To illustrate, EHRs are crucial in patient care. Its operational unavailability disrupts hospital functions and endangers patient safety (Larsen, 2019). When confronted with EHR failures, some hospitals shut down departments (Guardian, 2017). Between 2018 and mid-2022, 14 Dutch hospitals experienced IT failures leading to the unavailability of EHRs, closure of Emergency Rooms, delays for outbound patients, and postponed surgeries (IGJ 2022). The most common causes for the unavailability of EHRs arise from cyberthreats, both in the digital (e.g., hacking or data exfiltration) and in the social domain (e.g., password sharing or shadow IT). A recurring theme for cybercrime is human error, which manifests in sending information to the wrong recipient, reusing passwords, connecting to unsafe public hotspots, or being manipulated via social engineering tactics.

1.1 Countermeasures

To counter cyberattacks, both technical and non-technical countermeasures can be implemented (Khonji et al., 2013). Technical countermeasures, such as automated email classification using content, meta data or destination URL inspection are increasingly effective to counter email phishing (Khonji et al., 2013). However, despite major advancements, technological approaches may not be able to detect all threats as they are based on historic data and attackers constantly innovate (Hoheisel et al., 2023).

Mitigating these cybersecurity risks extends beyond technological solutions; the human element, which is often overlooked, plays a pivotal role in securing the organization (Safa, Von Solms & Futcher, 2016). This requires employees to learn behaviour and skills which contribute to a cybersecure organization. Unfortunately, learning new skills and behaviour is challenging (Lewis et al., 2013). Through deliberate practice one can improve their skills (Issenberg et al., 2005). There are four principles involved in successful practice: i) repetition of the skill, ii) continuous assessment of the performance and improvements, iii) with detailed feedback, this will result in iv) improving skills in a controlled setting. Deliberate practice is commonly implemented in medical practice for skill development (Lehtinen, 2023). In the context of cybersecurity training, with a focus on social engineering (i.e. a

cyberthreat that aims to manipulate the end user), a meta-analysis containing 19 studies, 37 effect sizes and 23 146 research subjects, found a medium effect size of educational interventions (Bullee & Junger, 2020). Moreover, the effect size differs for different interventions. Some are highly effective, whereas others have a negative or no effect (approximately 1 in 3). Interventions where participation is highly intensive (e.g., playing a game) were associated with a higher effect size compared to those with a low intensity (e.g., reading a static text) (Bullee & Junger, 2020). Finally, the researchers found a slight but significant decay in the effects of interventions over time.

An alternative to improve cybersecurity awareness could be an escape room. An escape room offers an interactive adventure, engaging groups of usually 2-8 individuals in collaborative puzzle-solving to exit the room (Cohen et al., 2020). These themed environments create immersive challenges, demanding effective teamwork for success. The cognitive and social abilities of each team member and their collective synergy significantly influence the team's performance. To thrive in an escape room, participants must synergize, emphasizing interdependence among teammates striving for a common objective.

The potential success of the educational escape rooms lies in the interplay between the story line which provides the scenario, problem-based puzzles that require teamwork to get solved, and a post-game reflection (Fotaris & Theodoros, 2022). Benefits of escape rooms include improvements of various of skill types in interpersonal, intrapersonal, and academic skill development. Thereby, escape rooms have been shown to be effective in improving both knowledge and skills in different subject areas (Morrell & Eukel, 2020, von Kotzebue, Zumbach & Brandlmayr, 2022).

The potential success of learning in an escape room may be explained as the product of multiple learning theories coming together (Fotaris & Theodoros, 2022). Relevant are the following theories of learning:

- Social Constructivism, a learning theory that emphasizes active participation and collaboration, finds practical application in escape rooms. In an escape room, participants engage in real-time experiences, collaborating with peers to overcome challenges, fostering critical thinking skills (McKinley, 2015).
- Bloom's Taxonomy, a framework for designing learning objectives and assessing understanding, plays a crucial role in the design of escape room puzzles. These puzzles cater to different levels of thinking, such as classifying information for understanding, thereby promoting higher-order thinking skills and deeper understanding (Bloom, 1956).
- Kolb's Experiential Learning Cycle, which outlines a four-stage process: concrete experience, reflective observation, abstract conceptualization, and active experimentation, emphasizing hands-on learning and reflection for a deeper understanding and application of knowledge (Kolb, 1984). According to this theory, learning occurs through experiencing, reflecting, thinking, and doing. In an escape room, participants actively engage with puzzles (Concrete Experience), reflect on their experiences and challenges (Reflective Observation), form concepts and theories (Abstract Conceptualization), and apply their knowledge in new situations (Active Experimentation). This holistic approach to learning allows participants to integrate their experiences into a cohesive whole.

Summarized, puzzles within an educational escape room (EER) are problem-based and require communication and team-working skills, which are considered intrinsic parts of the way in which adults learn, while a robust storyline helps to set the stage, and post-game reflection helps to solidify the learning goals. This creates a dynamic educational environment which may improve the retention rates compared to traditional learning (Abdulmajed, 2015).

Despite potential benefits, little work has been done on using escape rooms for organizational cybersecurity. Some initiatives are available, such as the briefcase-based escape room for high school juniors and seniors (Mello-Stark et al., 2020). In teams of three, the participants need to complete seven puzzles to solve the mystery. All games relate to codes and encryption, including Caesar cypher, Steganography, strong passwords and soft skills. The latter is to prevent a single person from completing the entire game alone (Mello-Stark et al., 2020). The games allow for discussion on security practices. For example, the game starts by figuring out how to open the case. The code is the birthday that can be found on the card; this is an opportunity to discuss whether using your birthday is a good password. Regarding evaluations, these are suggestions by the authors for future research.

DeCusatis et al. present a security awareness virtual escape room based, which is themed as a science fiction environment where the participants play a robot that learns about cybersecurity (2022). The game is diverse and handles nine topics: USB devices, passwords, cryptography, multi-factor authentication, phishing, social

engineering, defence in depth, firewalls and malware. Focus on (pre-) college students. In total, 120 participants tested the game, resulting in 5 out of 8 Octalysis metrics scoring at least 7.9 out of 10. The before-and-after security awareness assessment showed improvements, but the exact extent was not detailed in the manuscript (DeCusatis et al., 2022).

A third initiative from Löffler et al. used the principles of an escape room to build a virtual equivalent for teaching staff about cybersecurity awareness (2021). In teams, the participants go through 8 different topics, including physical security, passwords, phishing, social engineering, and online banking. The learning goals in that study relate to raising cybersecurity awareness and knowledge sharing, peer learning, and problem-solving. The overall mystery in the escape room is to reveal the rogue employees who are committing financial fraud, thereby aiming to teach employees about cybersecurity awareness (Löffler et al., 2021). The outcome of the player evaluation was that 65 out of 81 rated the game as positive, 4 were negative and 12 did not answer.

Although there is limited work on cybersecurity escape rooms, it is good to see initiatives for different audiences emerging. However, a general shortcoming is the limited systematic evaluation of the achievement of the intended learning outcome.

1.2 Research Question

In this study we aim to determine if an escape room can be used to improve cybersecurity knowledge, attitudes, and behaviour of healthcare employees. Therefore, the research question of this study is: "*How does participation in a cybersecurity-themed escape room affect participants' cybersecurity knowledge, attitudes, and behaviour over time?*"

Two hypotheses were formulated:

> **H1**) The null hypothesis is that there is no significant difference in participants' overall scores on the HAIS-Q survey immediately after completing the cybersecurity-themed escape room, as compared to their pre-test scores.
>
> **H2**) The null hypothesis is that there is no significant difference in participants' overall scores on the HAIS-Q survey approximately one month after completing the cybersecurity-themed escape room, as compared to their pre-test scores.

2. Methodology

2.1 Subjects

Employees from 26 healthcare organisations in the eastern part of the Netherlands were invited via email to participate in a cyber themed escape room. This was part of a larger cybersecurity effort for all healthcare personnel in the eastern part of the Netherlands.

2.2 Power Analysis

An a priori power analysis was performed using G*Power (Faul et al., 2007) to establish the minimum sample size needed to test this study's hypotheses. Results indicated the required sample size to achieve 90% power for detecting a medium effect (i.e., $d = 0.5$), at a significance criterion of $\alpha = .05$, was $N = 44$ for a two-tailed paired t-test. Therefore, the obtained sample size of $N = 96$ is considered adequate for testing the study's primary hypothesis.

2.3 Materials

Two types of materials were used in this study: 1) a survey for measuring information security awareness and 2) the cybersecurity truck escape room. The survey consisted of the Human Aspects in Information Security Questionnaire (HAIS-Q) (Parsons et al. 2014). This instrument is built on top of KAB (Knowledge, Attitude, and Behaviour) model that assumes that if knowledge increases, attitudes can be improved which could lead to an improvement in behaviour. The scale consists of 7 areas, each divided into 3 sub-areas, with each 1 question for each of the KAB constructs, resulting in a total of 63 items. To measure the items, a 5-point Likert scale was used, whereby each statement is answered using answer options ranging between 'Strongly disagree' and 'Strongly agree'. For example, the focus area 'Password Management' has the sub-areas: 1) 'Using the same password', 2) 'Sharing passwords' and 3) 'Using a strong password'. Examples of questions from the password focus area

are: “It is a bad idea to share my work passwords, even if a colleague asks for it” (Attitude), “I use a different password for my social media and work accounts” (Behaviour) and “A mixture of letters, numbers and symbols is necessary for work passwords” (Knowledge). The reliability of the HAIS-Q was originally calculated based on the responses of 500 employees and showed a Cronbach's alpha of .88 (Knowledge), .88 (Attitude) and .91 (Behaviour) (Parsons et al. 2014). In our study, only the 12 relevant sub-areas to the cybersecurity truck were included.

The employed cybersecurity truck escape room is a mobile escape room fitted inside a 40 ft container[1] and can be considered a ‘pop-up escape room’ (Fotaris & Theodoros, 2022). The experience was split into 3 parts: a) pre-briefing, b) game, and c) de-briefing. During the pre-briefing, participants are explained the safety procedures and the scenario of the escape room. In the main part, the game, participants had to solve cybersecurity related puzzles and handle correctly given the scenarios they encountered. As such, the escape room followed the Three Act Structure in narrative creation (Davison, 2006). Summarized, the procedure for the escape room was as follows:

- The pre-briefing consisted of 3 elements: *i*) the participants received a safety briefing (since they will be in a 40 ft cargo container standing on a trailer); *ii*) directly after, the participants are confronted with the first cyberthreat, the social engineer, where they are persuaded to share Personally Identifiable Information (PII) as if this was required to start the game (i.e. name, date of birth and phone number); *iii*) introduction to the game scenario, where the goal is to obtain a code to disarm arm a bomb before the timer runs out. Then, the participants climb into the truck and the escape can begin.
- During the game, participants solved puzzles to get codes for locks and safes; secure behaviour earned additional time, while insecure actions lost time. Solving all puzzles in time disarmed the bomb and completed the game. Games and situations in the escape room included:
    - Social engineering: At the beginning of the game, directly after the briefing, the game leader tries to make the participants share Personally Identifiable Information (PII). Although none of the retrieved data was stored during the debriefing, it is explained that by sharing PII, the offender can tailor the attack to you.
    - Data classification: In this puzzle, the participants had to place the given data items (e.g., information flyer, invoice, health record) in the correct category (public, confidential, restricted). A code appeared once all items were in the correct position (and turned around).
    - Maze + Periscope: In this two-person game, player 1 controls an arrow on a screen, where the left and right are swapped, as well as forwards and backwards. Player 2 looks through a periscope and looks out for a code that could open a lock.
    - Items: In the escape room, various items found in an office environment are lying around. Some items contained PII, so returning them to the 'security box' could earn additional time. One of these items is a USB storage device that fits in the USB port of the PC. Returning this item would also earn additional time; however, plugging it into the PC triggers a ransomware attack and reduces the time left on the timer.
    - Phishing: One of the codes can be unlocked by correctly identifying the suspicious elements of a potential phishing email in the PC's inbox.
- In the third and final stage, the participants were debriefed by doing a walkthrough of the threats they encountered during the experience. The debriefing was led by a policy officer of the healthcare organization, who discussed a series of question with the escape room participants. These questions focused on what the participants observed during the escape room, what actions they took and why, how they reflect on their cooperation during the escape room, and on how the themes presented in the escape room relate to organizational policy and how participants would act if a real cyberthreat occurred in the organization.

2.4 Procedure

A pre-test post-test control group design was used as an experimental design. The target population for this study were employees employed in the healthcare sector and can included: Information Security Officers, Data and Privacy Officers, Department Managers, Nurses or Physicians. These employees were invited through a mailing via a network partner who facilitates cooperation in both the area of daily routine care and the field of

[1] https://escaperoommobiel.nl/cybersecurity-truck/

medical assistance in the case of a disaster or crisis. One of their activities is organizing training sessions for their network in the region. The healthcare employees, who stem from different organisations, had to register a timeslot in teams of 3-8 persons in advance (the majority registered a team of 8). In the dataset, teams of 2-9 (median = 5) were observed. There were 3 days of data collection during which participants took part in the escape room. One month after the data collection, participants were invited via e-mail to complete the delayed post measure. Additionally, after the 3 days of data collection, employees who were invited but did not participate in the escape room study were invited via email to complete the survey so that they could function as a control group. For an overview of the data collection timeline, please refer to Table 1.

Table 1: Time schedule of the data collection

	Pre-test	Cybersecurity truck	Post-test	Delayed post-test
Experimental	3/4/5 October 2023			2 November 2023
Control	6-30 October 2023	-	-	-

2.5 Study codes

To anonymously track an individual participant through multiple surveys, Self-Generated Identification Codes (SGICs) were used (Audette 2019). Such a code is created by combining the answers to a set of 5 personally salient questions in a pre-determined order. Examples of such questions are: “First initial of your first middle name?”, “First initial of your mother’s first name?”, or “Number of older siblings”. Answers could be “Katherine”, “Mary” and "2"; these answers would translate into the code: ‘KM2'.

2.6 Variables

The variables in the analysis were: pre, post, delayed.

‘Pre’ measured the score on the HAIS-Q scale before participating in the cybersecurity truck. ‘*Post’* measured the HAIS-Q score directly after, whereas ‘*delayed*’ measured the score after one month. All HAIS-Q answers were coded to range from –2 up to +2. For all variables, the score was calculated by the sum of all 36 items and therefore ranged from –72 up to +72.

2.7 Analysis

A t-tests were used to test the hypotheses. For the analysis, we adopted an "intervalist" perspective, aligning with the concept of Likert scale construction and usage. This meant that we treat the averaged scale as an approximation of continuous data (Harpe, 2015, Schrum et al, 2020). The following three data assumptions must be met for the paired t-test: 1) independence, 2) paired and 3) normality (Pallant, 2020). **Independence** of observations refers to research subjects being independent. This criterium is met since each research participant completed their own form. **Paired** means that the pre and post measure occur from the same individual; this is the case, since we were able to track each respondent anonymously using study codes. **Normality** is the requirement of the difference between the pre, and post measure are normally distributed; a visual inspection of the Q-Q plots was performed, and this did not indicate problematic non-normality.

Comparing the control group (M = 27.2, SD = 5.9) and the pre-test (M = 26.3, SD =7.1), no significant difference was observed (t(47.56) = -0.714, p = 0.479) for the overall scores. Zooming in on the thematic scores, no significant differences appeared, refer to Table 2. Thus, participants in the escape room did not appear to significantly differ from non-participants.

Table 2: Overview of scores for the different conditions, with their p-values per theme and for the total HAIS-Q score.

	Pre-test vs control group (N = 133 vs 29)		
Theme	Pre	Control	p value
Email	6.9 (3.0)	7.7 (3.0)	0.193
Passwords	8.5 (2.0)	8.7 (1.5)	0.497
Ransomware	1.1 (1.4)	0.8 (1.3)	0.359
Social engineering	-0.5 (2.4)	-1.2 (3.0)	0.196
Incident reporting	6.8 (2.4)	7.6 (1.7)	0.075
Software updates	3.5 (2.4)	3.7 (1.7)	0.648
Total	**26.3 (7.1)**	**27.2 (5.9)**	**0.479**

* p<0.05; ** p<0.01; *** p<0.001;

3. Results

3.1 Hypothesis 1

The results from the pre-test (M = 16.3, SD = 7.3) and post-test (M = 30.8, SD = 6.1) indicate that the cyber truck escape room made an improvement in the HAIS-Q scores, t(95) = -6.259, p = .001 (two-sided). This translates to a Cohen's d of 2.16 and can be classified as a large effect (Cohen, 2013). Hypothesis 1 is therefore rejected in favour of its alternative H1a: participants will achieve significantly higher overall scores on the HAIS-Q survey immediately after completing the cybersecurity-themed escape room compared to their pre-test scores. Zooming in on the scores for the individual themes, an improvement in the scores for email, password, social engineering, and software updates was observed, whereas no improvement was found for the remaining themes: ransomware and incident reporting. Please refer to Table 3 for an overview of scores for both the pre-test and post-test by theme.

3.2 Hypothesis 2

There was a significant increase in the HAIS-Q score measured one month after the cyber truck (M = 31.0, SD = 4.4) compared to the score directly before the cyber truck (M = 26.5, SD = 7.4), t(25) = -2.946, p = -.006. This translates to a Cohen's d of 0.74 and can be classified as a medium effect (Cohen, 2013). Hypothesis 2 is therefore rejected in favour of its alternative H2a: participants will maintain significantly higher overall scores on the HAIS-Q survey one month after completing the cybersecurity-themed escape room compared to their immediate post-test scores. An improvement was observed for the themes social engineering and software updates. No difference was observed for the remaining themes: email, passwords, ransomware, and incident reporting. Please refer to Table 3 for an overview of scores for both the pre-test and post-test by theme.

Table 3: Overview of scores for the different conditions, with their significance levels per theme and for the total HAIS-Q score.

	Pre-test vs post-test (N = 96)		Pre-test vs delayed post-test (N = 26)†	
Theme	Pre	Post	Pre	Delayed post
Email	**6.8 (3.1)**	**7.9 (2.9)** ***	6.9 (3.5)	7.1 (2.6)
Passwords	**8.3 (2.0)**	**8.8 (2.0)** *	8.3 (1.9)	9.1 (1.8)
Ransomware	1.1 (1.4)	1.3 (1.1)	1.2 (1.4)	1.4 (1.2)
Social engineering	**-0.4 (2.4)**	**1.6 (1.4)** ***	**-1.0 (2.7)**	**1.4 (1.7)** ***
Incident reporting	7.0 (2.5)	7.3 (1.9)	7.3 (2.6)	7.7 (1.3)
Software updates	**3.5 (2.4)**	**4.0 (2.1)** ***	**3.8 (2.1)**	**4.4 (1.8)** *
Total	**16.3 (7.3)**	**30.8 (6.1)** ***	**26.5 (7.4)**	**31.0 (4.4)** ***

* p<0.05; ** p<0.01; *** p<0.001; pre-test was conducted directly before, post-test was conducted directly after, and delayed post-test was conducted approximately one month after the escape room.
† 42 respondents completed the delayed post-test, only 26 could be matched with their pre-test results.

4. Discussion and Conclusion

The present study took a novel approach to cybersecurity training in the form of an educational escape room. Results showed a positive effect on the knowledge, attitude, and behavioural intention of participants on a mixture of cybersecurity themes; positive effects were observed directly after the participation and persisted for at least one month.

These results are particularly promising because traditional cybersecurity suffers from problems. Even though traditional training often has a positive effect (Bullee & Junger, 2020), motivation for and participation in traditional training tends to be lower (Aldawood & Skinner, 2019), potentially even problematically so (Tally et al., 2023). An educational escape room may not suffer from the same problems. Furthermore, an educational escape room, being a more intensive training form, due to the active participation and collaboration with peers (in line with the Social Constructivism learning theory) and application of knowledge in new situations together with the reflection on outcomes and experiences (Experiential Learning theory), has the potential to achieve stronger, longer-lasting effects in participants. Our study indeed found that the cybersecurity educational escape room had large effects; on the total HAIS-Q score, comparing the pre-test to the direct post-test and the delayed post-test scores, the achieved effect sizes were respectively 2.16 and 0.74 (Cohen's d). In comparison, traditional training methods achieve a lower average effect size of 0.54 (Bullee & Junger, 2020). Bullee and Junger (2020),

also found that interventions with a high intensity (e.g. a game) had a significantly higher effect compared to those that were less intense. From experience the second author can say that this intervention was intense, even for those with a background in cybersecurity. Moreover, it was also found that interventions that focus on a specific topic were more effective compared to those with a broader focus. Although the entire escape room focuses on many topics, it had a large effect size. Alternatively, one could explain the escape room experience as a *collection o*f small specific interventions, bundled together in a shell. Looking at the individual themes, 4 out of 6 had a significant improvement when comparing the pre and post-test measures.

In line with Bullee & Junger (2020) and the decay effect in general (Ebbinghaus, 1913), the effect of the escape room reduced over time. For some themes, the effect completely decayed over time, whereas others did not decay that much, refer to Table 3. The improvement for the theme of social engineering remained significant over time. To reduce the effect of social engineering via the telephone, previous research reported a significant reduction of victimisation after the distribution of an information flyer and a card holder. This effect was observed 1 week after the distribution of materials. However, the second week after distribution, the effect disappeared (Bullee et al., 2016). Although there was a difference in modality (Face-to-Face vs Telephone), the intervention part in the escape room experience that tackled social engineering made a lasting impression. A suggestion for future research would be to test of this finding remains stable if the sample size improved, given that this was based on only 26 observations.

5. Limitations

However, some caution is warranted when interpreting the results of our study. The research design suffered from several dropouts; partially due to errors in the study code system and partially due to some participants simply not completing all surveys. This could have affected the results. Furthermore, due to the voluntary characteristic of the intervention, resulting in a range of different team sizes from 2 to 9 participants (rather than 8), with a median of 5 participants. Since the escape room experience can differ depending on the number of participants, this could have influenced the results of our study.

Furthermore, even though the HAIS-Q measurement instrument has been validated (Parsons et al. 2014), it should be noted that intention does not always translate into actual behaviour (Fishbein et al., 2023). Additionally, our latest measurement was approximately one month after the intervention. Future research needs to investigate for how long the effect would last exactly and when a new intervention is required. In the case of repeating this intervention, is it also not yet known if this would have similar effects. Finally, the applied cybersecurity escape room intervention consisted of many elements: the escape room task with various parts, as well as a final debriefing reflecting on the experience and its themes. It is not yet clear which elements exactly caused the effect that we found.

Nonetheless, this study showed promising results about an escape room as a novel cybersecurity training intervention in the healthcare sector.

Acknowledgements

The authors would like to thank Charlotte Scholten and Robin Schär from AcuteZorg Euregio for making this research possible. Moreover, the authors would like to thank the students that were involved in the data collection: Abdur-Rehman Malik, Ahmed Saadawy, Beril Cosar, Daniël Blik, Luuk Spelbos, and Zuhayr Mirza.

References

Abdulmajed, H., Park, Y. S., & Tekian, A. (2015). Assessment of educational games for health professions: A systematic review of trends and outcomes. In Medical Teacher (Vol. 37, Issue sup1, pp. S27–S32). Informa UK Limited. DOI:10.3109/0142159x.2015.1006609

Aldawood, H., & Skinner, G. (2019). Reviewing CyberSecurity Social Engineering Training and Awareness Programs—Pitfalls and Ongoing Issues. In Future Internet (Vol. 11, Issue 3, p. 73). MDPI AG. DOI:10.3390/fi11030073

Audette, L. M., Hammond, M. S., & Rochester, N. K. (2019). Methodological Issues With Coding Participants in Anonymous Psychological Longitudinal Studies. In Educational and Psychological Measurement (Vol. 80, Issue 1, pp. 163–185). SAGE Publications. DOI:10.1177/0013164419843576

Bloom, B. S. (1956). Taxonomy of educational objectives: The classification of educational goals (1st ed.). Longman Group.

van Boven, L. S., Kusters, R. W. J., Tin, D., van Osch, F. H. M., De Cauwer, H., Ketelings, L., Rao, M., Dameff, C., & Barten, D. G. (2024). Hacking Acute Care: A Qualitative Study on the HealthCare Impacts of Ransomware Attacks Against

Hospitals. In Annals of Emergency Medicine (Vol. 83, Issue 1, pp. 46–56). Elsevier BV. DOI:10.1016/j.annemergmed.2023.04.025

Bullee, J.H., and Junger, M. (2020). How effective are social engineering interventions? A meta-analysis. Information and Computer Security, 28(5), 801-830. DOI:10.1108/ICS-07-2019-0078

Bullee, J.H., Montoya, L., Junger, M., & Hartel, P. H. (2016). Telephone-based social engineering attacks: An experiment testing the success and time decay of an intervention. In A. Mathur, & A. Roychoudhury (Eds.), Proceedings of the inaugural Singapore CyberSecurity R&D Conference (SG-CRC 2016) (pp. 107-114). (Cryptology and Information Security Series; Vol. 14). IOS. DOI:10.3233/978-1-61499-617-0-107

Cartwright, A. J. (2023). The elephant in the room: cybersecurity in healthcare. In Journal of Clinical Monitoring and Computing (Vol. 37, Issue 5, pp. 1123–1132). Springer Science and Business Media LLC. DOI:10.1007/s10877-023-01013-5

Cohen, T. N., Griggs, A. C., Keebler, J. R., Lazzara, E. H., Doherty, S. M., Kanji, F. F., & Gewertz, B. L. (2020). Using Escape Rooms for Conducting Team Research: Understanding Development, Considerations, and Challenges. In Simulation & Gaming (Vol. 51, Issue 4, pp. 443–460). SAGE Publications. DOI:10.1177/1046878120907943

Davison, B. W. (2006). The Narrative of Flippy Johnson: The Three Act Structure - Criticisms and Alternatives Script and Script Analysis (Thesis, Master of Arts (MA)). The University of Waikato, Hamilton, New Zealand. Retrieved from https://hdl.handle.net/10289/2454

DeCusatis, C., Gormanly, B., Alvarico, E., Dirahoui, O., McDonough, J., Sprague, B., Maloney, M., Avitable, D., & Mah, B. (2022). A Cybersecurity Awareness Escape Room using Gamification Design Principles. In 2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC). 2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC). IEEE. DOI:10.1109/ccwc54503.2022.9720748

Ebbinghaus, Hermann (1913). Memory: A Contribution to Experimental Psychology. Translated by Ruger, Henry; Bussenius, Clara. New York city, Teachers college, Columbia university.

Faul, F., Erdfelder, E., Lang, A.-G., & Buchner, A. (2007). G*Power 3: A flexible statistical power analysis program for the social, behavioral, and biomedical sciences. In Behavior Research Methods (Vol. 39, Issue 2, pp. 175–191). Springer Science and Business Media LLC. DOI:10.3758/bf03193146

Fishbein, M., Hennessy, M., Yzer, M., & Douglas, J. (2003). Can we explain why some people do and some people do not act on their intentions? In Psychology, Health & Medicine (Vol. 8, Issue 1, pp. 3–18). Informa UK Limited. DOI:10.1080/1354850021000059223

Fotaris, P., and Mastoras, T. (2019). Escape Rooms for Learning: A Systematic Review. In Proceedings of the 12th European Conference on Game Based Learning. 2th European Conference on Game Based Learning. ACPI. DOI:10.34190/gbl.19.179

Fotaris, P., and Theodoros M. (2022). "Room2Educ8: A Framework for Creating Educational Escape Rooms Based on Design Thinking Principles" Education Sciences 12, no. 11: 768. DOI:10.3390/educsci12110768

Guardian News and Media. (2017, May 13). NHS seeks to recover from global cyber-attack as security concerns resurface. The Guardian. https://www.theguardian.com/society/2017/may/12/hospitals-across-england-hit-by-large-scale-cyber-attack

Harpe, S.E., 2015. How to analyze Likert and other rating scale data. Currents in pharmacy teaching and learning, 7(6), pp.836-850.

Hoheisel, R., van Capelleveen, G., Sarmah, D. K., & Junger, M. (2023). The development of phishing during the COVID-19 pandemic: An analysis of over 1100 targeted domains. In Computers & Security (Vol. 128, p. 103158). Elsevier BV. DOI:10.1016/j.cose.2023.103158

Inspectie Gezondheid.en Jeugd (2022). ICT-storingen in ziekenhuizen: lessen voor bestuurders en ICT-managers. Retrieved from Ministerie van Volksgezondheid, Welzijn en Sport website: https://www.igj.nl/publicaties/publicaties/2022/09/27/ict-storingen-in-ziekenhuizen-lessen-voor-bestuurders-en-ict-managers

Issenberg, B. S., Mcgaghie, W. C., Petrusa, E. R., Lee Gordon, D., & Scalese, R. J. (2005). Features and uses of high-fidelity medical simulations that lead to effective learning: a BEME systematic review. In Medical Teacher (Vol. 27, Issue 1, pp. 10–28). Informa UK Limited. DOI:10.1080/01421590500046924

Kolb, D. A. (1984). Experiential learning: Experience as the source of learning and development. Englewood Cliffs, N.J: Prentice-Hall.

von Kotzebue, L., Zumbach, J., & Brandlmayr, A. (2022). Digital Escape Rooms as Game-Based Learning Environments: A Study in Sex Education. In Multimodal Technologies and Interaction (Vol. 6, Issue 2, p. 8). MDPI AG. DOI:10.3390/mti6020008

Khonji, M., Iraqi, Y., & Jones, A. (2013). Phishing Detection: A Literature Survey. In IEEE Communications Surveys & Tutorials (Vol. 15, Issue 4, pp. 2091–2121). Institute of Electrical and Electronics Engineers (IEEE). DOI:10.1109/surv.2013.032213.00009

Larsen, E., Hoffman, D., Rivera, C., Kleiner, B. M., Wernz, C., & Ratwani, R. M. (2019). Continuing Patient Care during Electronic Health Record Downtime. In Applied Clinical Informatics (Vol. 10, Issue 03, pp. 495–504). Georg Thieme Verlag KG. DOI:10.1055/s-0039-1692678

Lehtinen, E. (2023). Can simulations help higher education in training professional skills? In Learning and Instruction (Vol. 86, p. 101772). Elsevier BV. DOI:10.1016/j.learninstruc.2023.101772

Lewis, D., O'Boyle-Duggan, M., Chapman, J., Dee, P., Sellner, K., & Gorman, S. (2013). 'Putting Words into Action' project: using role play in skills training. In British Journal of Nursing (Vol. 22, Issue 11, pp. 638–644). Mark Allen Group. DOI:10.12968/bjon.2013.22.11.638

Löffler, E., Schneider, B., Zanwar, T., & Asprion, P. M. (2021). CySecEscape 2.0—A Virtual Escape Room To Raise Cybersecurity Awareness. In International Journal of Serious Games (Vol. 8, Issue 1, pp. 59–70). Serious Games Society. DOI:10.17083/ijsg.v8i1.413

Marchal, S., Armano, G., Grondahl, T., Saari, K., Singh, N., & Asokan, N. (2017). Off-the-Hook: An Efficient and Usable Client-Side Phishing Prevention Application. In IEEE Transactions on Computers (Vol. 66, Issue 10, pp. 1717–1733). Institute of Electrical and Electronics Engineers (IEEE). DOI:10.1109/tc.2017.2703808

McGlave, Claire and Neprash, Hannah and Nikpay, Sayeh, Hacked to Pieces? The Effects of Ransomware Attacks on Hospitals and Patients (October 4, 2023). Available at SSRN: http://dx.doi.org/10.2139/ssrn.4579292

McKinley, J. (2015). Critical Argument and Writer Identity: Social Constructivism as a Theoretical Framework for EFL Academic Writing. In Critical Inquiry in Language Studies (Vol. 12, Issue 3, pp. 184–207). Informa UK Limited. DOI:10.1080/15427587.2015.1060558

Mello-Stark, S., VanValkenburg, M. A., & Hao, E. (2020). Thinking Outside the Box: Using Escape Room Games to Increase Interest in CyberSecurity. In Innovations in Cybersecurity Education (pp. 39–53). Springer International Publishing. DOI:10.1007/978-3-030-50244-7_3

Morrell, B., & Eukel, H. N. (2020). Shocking Escape: A Cardiac Escape Room for Undergraduate Nursing Students. In Simulation & Gaming (Vol. 52, Issue 1, pp. 72–78). SAGE Publications. DOI:10.1177/1046878120958734

Pallant, J. (2020). SPSS Survival Manual. Routledge. DOI:10.4324/9781003117452

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). In Computers & Security (Vol. 42, pp. 165–176). Elsevier BV. DOI:10.1016/j.cose.2013.12.003

Reason, J. (1990). The contribution of latent human failures to the breakdown of complex systems. Philosophical Transactions of the Royal Society of London B: Biological Sciences, 327(1241), 475–484.

Schrum, M.L., Johnson, M., Ghuy, M. and Gombolay, M.C., 2020, Four years in review: Statistical practices of likert scales in human-robot interaction studies. In Companion of the 2020 ACM/IEEE International Conference on Human-Robot Interaction (pp. 43-52).

Tally, A. C., Abbott, J., Bochner, A. M., Das, S., & Nippert-Eng, C. (2023). Tips, Tricks, and Training: Supporting Anti-Phishing Awareness among Mid-Career Office Workers Based on Employees' Current Practices. In Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems. CHI '23: CHI Conference on Human Factors in Computing Systems. ACM. DOI:10.1145/3544548.3580650