First Steps to Improve Cybersecurity Behaviour: A Virtual Reality Experience

Lara Klooster[1], Robby van Delden[1] and Jan-Willem Bullée[2]

[1]Human Media Interaction - Faculty of Electrical Engineering, Mathematics and Computer Science (EEMCS), University of Twente, Enschede, The Netherlands

[2]Industrial Engineering and Business Information Systems - Faculty of Behavioural, Management and Social sciences (BMS), University of Twente, Enschede, The Netherlands

lara2001@gmail.com
r.w.vandelden@utwente.nl
j.h.bullee@utwente.nl

Abstract: Internet is completely integrated and absorbed in our life. Facilitating transfer of files across the world or wiring money from the couch, we could not imagine a world without it anymore. With these benefits, as with any new technology, there is also the introduction of risks and threats, for internet primarily in the form of cybercrime and online fraud. To reduce victimisation of this cybercrime, interventions are used to teach people to not perform risky behaviour. To overcome criticisms of current training materials, such as being tedious and boring, we created an Immersive Virtual Reality experience. By using a 4-step design process (i.e. ideation, specification, realisation, and evaluation), we designed a playful VR environment with simplistic non player characters to train the user to perform basic cybersecurity tasks in the right way. In the simulation, the participants are exposed to the challenge of creating a new password and a potential ransomware attack using USB storage device. The program allows for monitoring the user's cybersecurity knowledge and behaviour and provides feedback. An evaluation of the VR environment among 16 respondents using a pretest-posttest evaluation with the Human Aspect Information Security Questionnaire (HAIS-Q) showed a statistically significant increase in scores after exposure to the VR environment. The system showed an above average SUS score. These initial findings indicate that a VR environment can be an alternative to consider for future development of cybersecurity interventions. Future research could expand our social VR environment with additional cybersecurity challenges, real-time actors, and running simulations among a broader audience to also investigate the retention of knowledge and skills.

Keywords: Cybersecurity, Design, Immersive virtual reality, Intervention, Prototyping, USB drop

1. Introduction

The internet has become an indispensable part of our lives, offering the ability to connect with people from all corners of the globe, and conduct financial transactions from the comfort of our couches. However, it also comes with risks in the form of cybercrime and online fraud. From phone calls from fake bank representatives to scam text messages, it is important to remain vigilant to protect ourselves online.

To reduce vulnerability to cyber threats, typically two types of defences are deployed: technical and non-technical (Pollini et al, 2021). Technical defences involve the use of automated techniques, such as machine learning algorithms, to identify and prevent cyber threats. For example, automated detection of malicious software, unauthorized access attempts, and other suspicious activities on computer networks (Marchal et al., 2017). Although techniques can detect advanced attacks in certain conditions, they are limited by their reliance on past data. Therefore, additional measures may be necessary to detect potential attacks.

Non-technical defences, involve training users to become proficient in recognizing and responding to cyber threats. This can include educating users on how to secure their devices and networks, recognizing and reporting phishing attempts, and staying up to date on the latest security risks and best practices. Typical ways of delivering such user training are in text-like format, which users must read, classroom lecturing, or e-learning (Dahabiyeh, 2021). While these methods might be cost efficient, the user experience is sometimes tedious or boring (Aldawood & Skinner, 2019).

To offer more engaging experiences, there are serious games that teach about various forms of cyberthreats, for instance, around document inspection of phishing emails akin to the game *'Papers Please'* (Wen et al. 2019). An alternative approach that could be even more engaging and can be at least as effective is the implementation of a cyber security training in an Immersive Virtual Reality (IVR) (Veneruso et al, 2020). The goal of our current work is to explore the potential use of IVR for training to reduce vulnerability against cyber threats. Specifically, our contribution lays in our investigation of opportunities to train for both online (e.g. password choice) as well as real-world behaviours (e.g. the use of a USB thumb stick, physical access, and/or social interactions).

In this paper we will first discuss related work. We then point out the chosen design process for creative technology which fits novel integrations of existing technologies (Mader & Eggink, 2014, Mader & Dertien, 2014) it adds intermediate structuring points to methods such as the spiral model for reflective transformative design (Hummels & Frens, 2009). In our process we highlight expert interviews as an important grounding step for designing our intervention. Afterwards, we show the resulting design including the underlying design rational. Following this, we present our evaluation, first the method, and second the results of how evaluated the environment on effectiveness of training and usability using a convenience sample (N=16). We finish the paper with a brief discussion including possible future steps.

2. Related Work

A thorough investigation about games for cybersecurity is outside the scope of this paper, so we use examples only to provide an overview of general directions. In the field of game-based learning of cybersecure behaviour there are mobile app games such as *CyberAware* (Giannakas et al, 2015), online games such as *What.Hack* (Wen et al. 20019), PC games such *CyberCIEGE* which combined this with an online scenario database (Irvine et al 2005), and our direction of immersive VR intervention for which we only encountered *CyberVR* (Veneruso et al 2020). Besides the form an important distinction can be seen in the type of training that is offered.

Samy et al. (2010) took a broad approach to identifying threats to cybersecurity, identifying 22 elements in a healthcare setting. Huang et al (2010) adopted a similar broad strategy and established 12 categories of cybersecurity threats. Badie and Lashkari (2012) defined nine less generalised factors. The categories included technical hardware/software failures, forces of nature, or deliberate acts of espionage and trespass. In these overviews several descriptions are used for the human error, which is the focus of our work: acts of human error or failure, staff shortage, and operational issues (Samy et al, 2010), "acts of human error or failure" (Huang et al, 2010), and error and omission, phishing, and social engineering (Badie and Lashkari, 2012).

In various estimates human error is recognised as the biggest source of security breaches (Nobles,2018). Huang et al. (2010) also recognize this importance, delineating the human factor as the weakest point in information security. In the past this human aspect has regularly been disregarded (Nobles,2018, Pollini et al, 2021). Metalidou et al. (2014) even assert that technology is regularly recognized as the only fix of these problems.

Even the field of human error within security breaches is very broad and to build an intervention within the scope of our project we need a better view on aspects of human error. When looking at literature there is consensus on at least two human factors, lack of knowledge (Desolda et al, 2022, Huang et al 2010, Pollini et al 2021, Metalidou et al, 2014, Zimmerman & Renaud, 2019) and a related lack of awareness (Desolda et al, 2022)) Zimmerman and Renaud (2019) and Pollini et al (2021) both expand this with lack of skills, and the latter also add violations, the lack of adherence to rules, and malicious violations. Similarly, Zimmerman and Renaud (2019) include the possibility of malicious users, this vulnerability encompasses those who make the "mistakes" without the intent of doing the right thing. Metalidou et al. (2014) appoint risky belief, risky behaviour, and inadequate technology use as additional vulnerable human factors. Desolda et al. (2022) describe the vulnerability of norms and complacency. Unsafe norms are practices users become accustomed to over time (e.g., not locking the office/computer when leaving the workplace). Complacency is users' self-overestimation of cybersecurity skills, which can in term be related to a lack of knowledge and awareness. Another human vulnerability is a lack of policies and compliance, which are predetermined written guidelines which an employee should adhere to (Zimmerman & Renaud, 2019).

Gillam and Foster (2020) use another approach towards defining human error, culminating in the use of Human Aspect Information Security Questionnaire (HAIS-Q) by Parsons et al (2017), to identify vulnerable areas rather than underlying reasons. Using the HAIS-Q is a holistic method of measuring human factors in cybersecurity (Parsons et al, 2017). It differentiates between seven topics: 1) password management, 2) e-mail use, 3) internet use, 4) social media use, 5) mobile devices, 6) information handling and 7) incident reporting. These topics are more specialised and application oriented; moreover, they constitute known security risks related to the human factor. Consequently, these topics should be part of a cyber security training.

3. Design Process Based on Interviews

We follow a design process fitting for creative technology (Mader & Dertien, 2014) consisting of 4 steps: ideation, specification, realisation, and evaluation (Mader & Eggink, 2014). This approach employs a balance between divergent and convergent steps, and spiral models such as the Eindhoven Reflective Transformative Design Process (Hummels & Frens, 2009) while adding more structured intermediate steps. An important step in our ideation and subsequent specification was a semi-structured interview with two experts handling cybersecurity at our university, for which we obtained a positive advice from our Ethics Committee Computer & Information Science under RP 2022-27.

Although, the related work already provided a picture on relevant topics, with a semi-structured six question interview we wanted to get a better grip on the most dangerous and/or often occurring errors. We started with an introduction of the interviewer and the aim of the project. The first three questions were themed 'current ways of monitoring, testing, and educating cybersecurity'. Sample questions include: "*Which audience performs the worst in your cybersecurity testing and who performs the best? Do you have any idea why this is the case?*" and "*How do you test employees on their cybersecurity knowledge? Has it proven to be effective?*". The next three questions where themed 'mistakes and important topics'. Sample questions include: "*What are the most often made mistakes in cybersecurity that you encounter?*" and "*What are the topics that in your opinion should most definitely be treated in a cyber/ information security awareness training?*".

Regarding the question about which mistakes are made most often, sample responses included: "*Phishing and maltreatment of privacy sensitive cases. The most dangerous ones are those that include getting a virus on the computer. This can be through opening an email attachment or plugging a found USB with software in the computer.*" (interviewee 1) and "*Most dangerous mistakes are those where human weakness is exploited.*" (interviewee 2).

The interviewees discussed recent cybersecurity assessments and training programs at our university. In a baseline program in 2021 47% of employees and students participated. This program assessed awareness on 7 different topics. The results can be grouped into three classes based on average performance. Participants performed worst on protecting mobile devices and information. The second worst topic was related to phishing, social media and secure data protection and disposal. The third topic regarded protection against scams, physical risks, and safe use of the internet.

According to the first interviewee the most common human mistakes in cybersecurity are related to phishing and maltreatment of privacy sensitive cases. The most dangerous ones are those that include getting a virus on the computer. This can be through opening an email attachment or plugging a found USB with software in the computer. The second interviewee generalises this answer by saying that the most dangerous mistakes are those in which human weakness is exploited. Given examples included hack attempts, phishing and social engineering. It also includes the use of personal information from social media (e.g., to answer password reminders or find usernames). Hence, according to this, the topics that should be treated are password management: strong passwords, no reuse, and multi-factor authentication. Secondly, a topic to be treated in the training is the importance of thinking before handling, taking a break when things do not seem right. Somewhat related to the latter, the training should also help to recognize social engineering techniques.

4. VRCyberEducation

Based on the interviews combined with the related work, we highlight two very concrete elements to train in the domain of human error in cybersecurity, spanning the physical and digital realm: *password management* and *removable media use*. Using strong passwords is key for cybersecurity; in 2020 approximately 20% of initial attack vectors against companies are compromised credentials (Juozapavičius, 2022). Removable media and USB storage devices should be handled with care and can cause malware or ransomware attacks. Exemplary is the infected USB storage device that was used to sabotage an Iranian nuclear power plant (Chen, 2011).

The result of our iterative design process and especially the specification and devised steps is the immersive VR world *VRCyberEducation* accessible within a Social VR platform. We designed VRCyberEducation to address poor information security awareness among staff members of an organization. We chose for Social VR (networked VR environments where users are represented with virtual avatars) to provide a variety of possible follow-up studies (e.g., have multiplayer scenarios).

To be able to program interactions within a Social VR world and building on personal experiences regarding ease of use with available platforms, we chose for the freely accessible NeosVR. This platform had several benefits. NeosVR already includes user input from handheld controllers and/or VR headset for navigation and object interaction (including grabbing) within the virtual environment. It supports most types of VR hardware (i.e., relying on SteamVR) including the Oculus Quest 2 we had available. It is capable of integrating physical and cyber aspects of cybersecurity within the program through programming a variety of interaction-responses. The program also eased distribution, in NeosVR users can open and share worlds between accounts, whereas Unity does not take care of the distribution. Finally, fitting this context we could quickly emulate a realistic, lifelike virtual environment through importing various freely accessible assets.

These assets included an office building we constructed through combining a blueprint and 3D models from Turbosquid and Sketchfab. We added doors to let users travel between rooms. Additionally, inspired by existing tutorials and pictures online we modelled a monitor, USB storage device, desk, and box for cyber unsafe objects, see Figure 1. These objects all had an in-game function. The screen stands on the desk and plays a central role in the password task. The USB storage device, the desk and the cyber unsafe objects box play a role in the USB task.

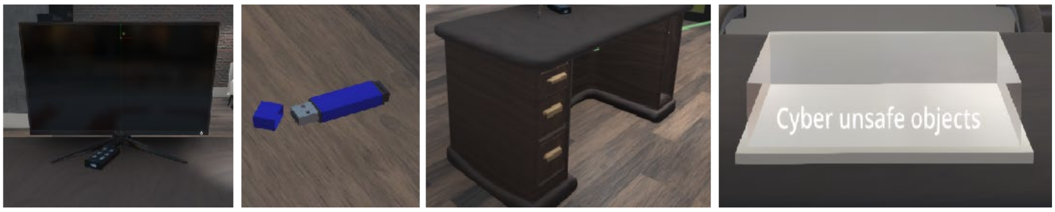

Figure 1: Office objects; From left to right: Screen, USB storage device, desk, box for cyber unsafe objects

Besides objects we had four characters, one for the player and three non-player characters. The first avatar is the players', partially visible in the VR environment (e.g. hands) and completely when they would look into a mirror. We choose to use a single avatar over the participant choosing one out of multiple, since the time needed to understand that interaction (and accompanying experience of switching bodies) to us felt too distracting. The second set of avatars included two security officers in an IT-department room, both a male and female, sitting at their desk and looking at their screen and then looking around, typing, blinking with their eyes, see Figure 2. Upon entering with the USB device, the female character was triggered to point at the cyber unsafe objects box, see Figure 1. The third avatar was a character which walked in, representing a friendly colleague, who plays a role at the beginning of the USB task. The character informed that he found a USB storage device in the hallway and put it in the top drawer of the desk. The animations of the characters were made using Blender.

To steer the user through the environment, we guided the user with a floating virtual canvas in the office. This screen is displaying the current task for the participant. An example is to meet Susan in the IT-department or to move the plant from one location to another. This helped the participants that were new to VR to get used to the controls. Moreover, to overcome that users would get stuck in a task, a timer was implemented. When the time was up, the participant is informed and had to move on to the next task.

Having a VR environment without any sound can distract the participant since they can hear the surroundings from the physical realm. To overcome this, background traffic sounds were included. For the IT-department office, instead we included office background chatter.

To show content on the computer screen, which we needed for the password task we used a canvas layover attached to the screen that can show text on images. Based on the status of a button in the game, a certain flow is triggered and can display various screens (e.g., a change password screen).

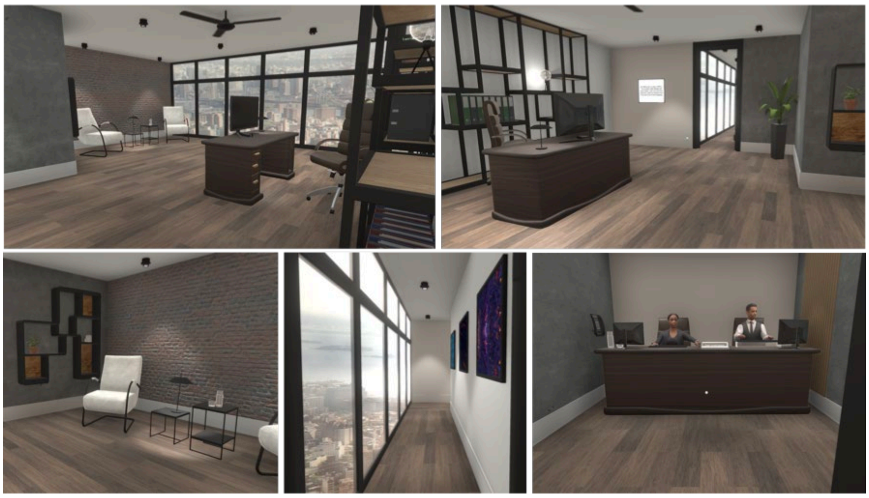

Figure 2: Fully decorated office

The learning objective of the password task is to get to know what good passwords are and the importance of enabling multi factor authentication. Therefore, the user performs tasks which test their knowledge on passwords. It starts with the user turning on the computers. Secondly, the user should change the password. When this task would let users insert their own password there is the potential danger that they fill in one of their current passwords, this would be ethically irresponsible. In order to simulate this action, but remove the included danger, it was we implemented a multiple-choice option. The multiple-choice options include both strong and weak passwords. The third step focuses on multi factor authentication, the computer will let the user choose to enable this multi factor authentication. The timing of information for the training can either be as instructions or in the form of feedback on choices. As we were afraid pausing the task of the user to provide feedback would interrupt them too much and only had a short overall interaction, we provided the feedback on both the password and USB tasks simultaneously at the end of the whole interaction. For the password this included the text *"Password management is an important aspect in cybersecurity. A strong password consists of over eight characters, including both alphanumerical and special characters. Furthermore, one should never reuse passwords from other accounts. A possible way to create such a strong password is the use of a passphrase.".* And for the USB task it read as follows: *"Removable media such as a usb can contain malware that can be installed on your computer when you plug it in. Therefore, you should always safely dispose of unknown removable media. For example, by handling it in an at the IT department.*

5. Method

The evaluation of the environment was tested using a pretest-posttest design. The Human Aspects of Information Security Questionnaire (HAIS-Q) was used to assess participants' knowledge, attitude, and self-reported behaviour (Parsons et al., 2014). The System Usability Scale (SUS) was used to measure usability (Brooke, 1995).

5.1 Participants

The pool of subjects in this research were university staff members, students and acquaintances of the authors. All were recruited via direct contact or in the case of staff members via a colleague. Those that are prone to motion sickness are advised not to participate in this study. In total 16 people participated in this study. Half of the participants indicated to be female, and the age ranged between the 18 and 65 yo. There were 10 (62.5%) participants in the age group 18-35, the remaining participants were older. Finally, there were 8 (50%) participants who completed a university bachelor or master.

5.2 Materials

The VR environment as described in Section 4 and loaded onto an Oculus Quest 2 Business Edition headset, running software version 37.0. The supporting laptop ran Windows 10 with an NVIDIA GeForce RTX 3050 graphics card. For validation, the Human Aspect Information Security Questionnaire (HAIS-Q) was used to measure information security awareness (Parsons et al. 2017). The underlying KAB model uses Knowledge, Attitude and Behaviour to measure awareness. Thereby assuming: if knowledge increases, attitude can be improved and eventually an improvement of behaviour. The scale consists of 63 items (based on 7 focus areas, each with 3 sub-areas, having 3 items (one for Knowledge, Attitude and Behaviour)) to be measured using a 5-point Likert scale, with answer options ranging from 'Strongly disagree' to 'Strongly agree'. Sample questions include: "It is a bad idea to share my work passwords, even if a colleague asks for it" and "I use a different password for my social media and work accounts". A study among 500 Australian employees showed an internal consistency of .88, .88 and .91 for Knowledge, Attitude and Behaviour, respectively (Parsons et al. 2014). These alpha values are in the range 0.8 - 0.9 and are considered 'good'. Within our study we only used a subset of the HAIS-Q, limiting to the relevant focus areas. For the password management focus area of the HAIS-Q there were 9 questions ($\alpha = .75$), the dropped USB focus area consisted of 3 questions ($\alpha = .81$) and the overall scale of 12 questions ($\alpha = .71$) which is considered as 'acceptable'.

To measure the environments' usability, the System Usability Scale (SUS) was used (Brooke, 1995). The SUS is often referred to as the 'quick and dirty' tool for measuring usability. While the scale is easy to administer, scores consistent and reliable for small sample sizes. A downside is the complexity of interpreting the score, where people tend to perceive a score between 0 and 100 as percentage (Brooke, 2013). The scale consists of 10 items to be answered using a 5-point Likert scale, with answer options ranging from 'Strongly disagree' to 'Strongly agree'. Sample questions include: "I found the system unnecessarily complex" and "I would imagine that most people would learn to use this system very quickly". Regarding the reliability of the SUS, an aggregate result of N = 2324 SUS survey responses from K = 206 studies shows a Cronbach's Alpha value of .911 (Bangor et al. 2008).

5.3 Procedure

Our research received another positive advice by our faculty's ethical committee. The evaluation used a pretest-posttest design; first, the participants completed 1 round of the HAIS-Q. Since the VR environment only included two cyber challenges (i.e., dropped USB and change passwords), the corresponding focus areas from HAIS-Q (i.e., Information handling and password management) were included in the questionnaire. Second, the participants played in the VR environment and completed two tasks (i.e., cyber challenges). Finally, once more participants completed the HAIS-Q, and a SUS questionnaire.

5.4 Analysis

The increase in knowledge because of participating in the VR environment was tested using a paired-samples t-test. The following 4 assumptions must be met for this t-test: (1) Continuous data; (2) Independent observations; (3) Normal distribution of score differences; (4) no outliers (JMP, 2023). A Likert scale was used to collect data, for analysis we follow our "intervalist" view fitting the idea behind how Likert scales are created and used, and where we assume the averaged *scale* to approximate continuous data (cf Harpe, 2015, Schrum et al, 2020). Although this is hard to test, it is reasonable to assume that the participating employees are independent of one another. A Shapiro-Wilk test showed no evidence of non-normality (W = 0.936, p = .318). Finally, a boxplot was used to detect outliers, see Figure 3, hence we conclude there are no outliers. All 4 assumptions are met and therefore we use a paired-samples t-test.

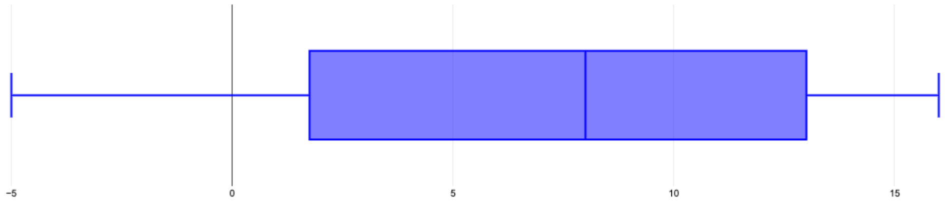

Figure 3: Boxplot for outlier detection on HAIS-Q score difference

6. Results

There was a significant increase in the Knowledge score of the HAIS-Q after the VR experience (M = 54.75, SD = 3.42) compared to the scores before (M = 47.5, SD = 6.31), t(15) = 4.7, p < .001. This translates to a Cohen's d of 1.46 and can be classified as a large effect (Cohen, 2013). For an illustration of the before and after HAIS-Q score distribution, refer to Figure 4. Furthermore, the SUS score (M = 72.5, SD = 8.4) is higher than the threshold of 68 and can be translated to the percentile score of 65% or 'acceptable' in terms of acceptance.

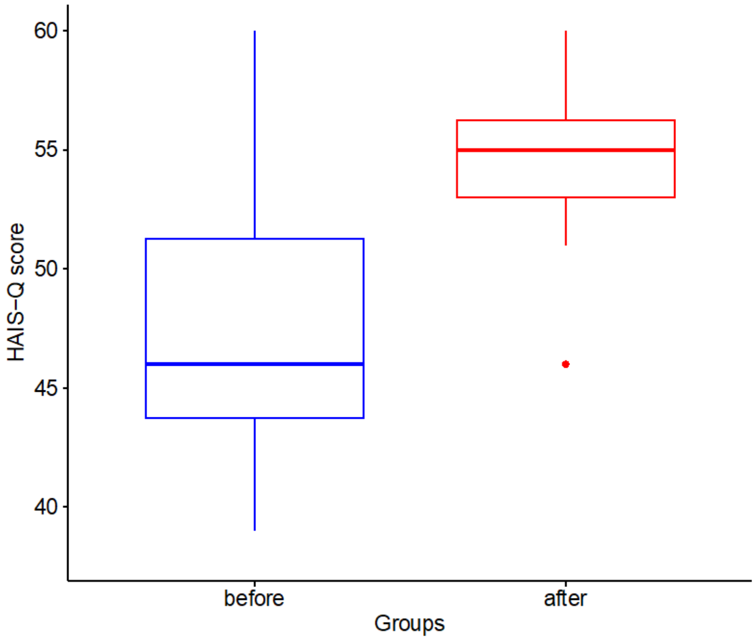

Figure 4: Boxplot for the HAIS-Q scores of the before and after measures

7. Discussion and Conclusion

In this study, we explored the use of IVR for cybersecurity training. Resulting in VRCyberEducation an interactive Social VR world which aims to reduce victimisation of cybercrime among users. We evaluated interaction with this environment on both usability and effectiveness. The study demonstrated a statistically significant improvement in knowledge scores related to information handling and password management among participants who engaged in the VR environment. These results show that using a VR environment can be a promising modality for providing cybersecurity training. Note that the post-test was performed immediately after the VR experience with the feedback close to the end. Previous research shows that these training effects decay over time in similar populations (Bullee & Junger, 2020).

The participants indicated that the usability of the environment, as measured with SUS, was acceptable but also leaves room for further improvement. The limited sample size and convenience sample severely limits the generalisability to a broader audience. Nonetheless, VRCyberEducation can already inspire future research, training for instance the limited sharing of personal information via social media and mobile devices, or the appropriate behaviour of locking doors and computers.

We end this paper with two important suggestions for future research to overcome current limitations: 1) In the current study, a convenience sample of 16 participants was used. First the number of participants can be increased with a homogeneous sample and later with a representative sample of an organisational workforce. 2) The current set-up consists of two cyber challenges. For future research, we plan on extending the environment so that other challenges can be included and to investigate the form and timing of feedback. Furthermore, to make full use of the power of SocialVR the environment can easily be extended to a multi-user environment so that multiple users can participate in real-time simultaneously in a single session. This would allow users to interact with each other and have a discussion.

References

Aldawood H, Skinner G. Reviewing Cyber Security Social Engineering Training and Awareness Programs—Pitfalls and Ongoing Issues. *Future Internet*. 2019; 11(3):73. doi:10.3390/fi11030073

Badie, N. and Lashkari, A.H., 2012. A new evaluation criteria for effective security awareness in computer risk management based on AHP. *Journal of Basic and Applied Scientific Research*, *2*(9), pp.9331-9347.

Bangor, A., Kortum, P. T., & Miller, J. T. (2008). An Empirical Evaluation of the System Usability Scale. In *International Journal of Human-Computer Interaction* (Vol. 24, Issue 6, pp. 574–594). Informa UK Limited. doi:10.1080/10447310802205776

Brooke, J. (1995). SUS: A quick and dirty usability scale. *Usability Evaluations in Industry* (Vol. 189).

Brooke, J. (2013). SUS: A retrospective. *Journal of Usability Studies* (Vol. 8, Issue 2, PP 29--40).

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

Chen, T. M. and Abu-Nimeh, S. (2011). Lessons from Stuxnet. *Computer* (Vol. 44, Issue 4, pp. 91-93). doi: 10.1109/MC.2011.115.

Cohen, J. (2013). Statistical power analysis for the behavioral sciences (2nd ed.). London, England: Routledge.

Dahabiyeh, L. (2021). Factors affecting organizational adoption and acceptance of computer-based security awareness training tools. *Information & Computer Security, 29*(5), 836-849.

Desolda, G., Ferro, L.S., Marrella, A., Catarci, T. and Costabile, M.F., 2021. Human factors in phishing attacks: a systematic literature review. *ACM Computing Surveys (CSUR)*, *54*(8), pp.1-35.

Giannakas, F., Kambourakis, G. and Gritzalis, S., 2015, November. CyberAware: A mobile game-based app for cybersecurity education and awareness. In *2015 International conference on interactive mobile communication technologies and learning (IMCL)* (pp. 54-58). IEEE.

Gillam, A.R. and Foster, W.T., 2020. Factors affecting risky cybersecurity behaviors by US workers: An exploratory study. *Computers in Human Behavior*, *108*, p.1-12.

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

Huang, D.L., Rau, P.L.P. and Salvendy, G., 2010. Perception of information security. *Behaviour & Information Technology, 29*(3), pp.221-232.

Hummels, C. and Frens, J., 2009. The reflective transformative design process. In *CHI'09 Extended Abstracts on Human Factors in Computing Systems*, pp. 2655-2658.

Irvine, C.E., Thompson, M.F. and Allen, K., 2005. CyberCIEGE: gaming for information assurance. *IEEE Security & Privacy*, *3*(3), pp.61-64.

Juozapavičius A, Brilingaitė A, Bukauskas L, Lugo RG. Age and Gender Impact on Password Hygiene. *Applied Sciences*. 2022; 12(2):894. https://doi.org/10.3390/app12020894

JMP (2023). Paired T-test. JMP. https://www.jmp.com/en_nl/statistics-knowledge-portal/t-test/paired-t-test.html

Mader, A. H., & Eggink, W. (2014). A Design Process for Creative Technology. In E. Bohemia, A. Eger, W. Eggink, A. Kovacevic, B. Parkinson, & W. Wits (Eds.), Proceedings of the 16th International conference on Engineering and Product Design, E&PDE 2014. (E&PDE). The Design Society, pp. 568-573 https://www.designsociety.org/publication/35942/a_design_process_for_creative_technology

Mader, A. and Dertien, E., (2014). How to educate for creativity in creative technology?. In E. Bohemia, A. Eger, W. Eggink, A. Kovacevic, B. Parkinson, & W. Wits (Eds.), Proceedings of the 16th International conference on Engineering and Product Design, E&PDE 2014. (E&PDE). The Design Society, pp. 562-567 https://www.designsociety.org/publication/35941/how_to_educate_for_creativity_in_creative_technolog

Marchal, S., Armano, G., Gröndahl, T., Saari, K., Singh, N., & Asokan, N. (2017). Off-the-hook: An efficient and usable client-side phishing prevention application. *IEEE Transactions on Computers, 66*(10), 1717-1733.

Metalidou, E., Marinagi, C., Trivellas, P., Eberhagen, N., Giannakopoulos, G. and Skourlas, C., 2014. Human factor and information security in higher education. *Journal of Systems and Information Technology*, *16*(3), pp.210-221

Nobles, C., 2018. Botching human factors in cybersecurity in business organizations. *HOLISTICA–Journal of Business and Public Administration*, *9*(3), pp.71-88.

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). doi:10.1016/j.cose.2013.12.003

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. *Computers & Security* (Vol. 66, pp. 40–51). doi:10.1016/j.cose.2017.01.004

Pollini, A., Callari, T.C., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F. and Guerri, D., 2022. Leveraging human factors in cybersecurity: an integrated methodological approach. *Cognition, Technology & Work*, *24*(2), pp.371-390.

Samy, N., Ahmad, R., and Ismail, Z. “Security threats categories in healthcare information systems.,” Health Informatics J., vol. 16, no. 3, pp. 201–209, Sep. 2010, doi: 10.1177/1460458210377468.

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).

Veneruso, S. V., Ferro, L. S., Marrella, A., Mecella, M., & Catarci, T. (2020). CyberVR. In *Proceedings of the International Conference on Advanced Visual Interfaces. AVI ’20: International Conference on Advanced Visual Interfaces. ACM.*

Wen, Z.A., Lin, Z., Chen, R. and Andersen, E., 2019, May. What. hack: engaging anti-phishing training through a role-playing phishing simulation game. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (pp. 1-12).

Zimmermann, V. and Renaud, K., 2019. Moving from a ‘human-as-problem” to a ‘human-as-solution” cybersecurity mindset. *International Journal of Human-Computer Studies*, *131*, pp.169-187.