Virtual Reality (2025) 29:150
https://doi.org/10.1007/s10055-025-01228-8

ORIGINAL ARTICLE

Exploring a novel approach to cybersecurity: the role of ecological simulations on cybersecurity risk behaviors

Tiago Abril[1] · Pedro Gamito[1] · Carolina da Motta[1] · Jorge Oliveira[1] · Fábio Dias[1] · Filipe Pinto[1] · Miguel Oliveira[2]

Received: 20 June 2024 / Accepted: 16 August 2025

Abstract
In response to the growing cybersecurity problem, this study presents an innovative approach using virtual reality to train individuals in reducing the risk of cyberattacks. The research involved adult participants with or enrolled in higher education studies, who participated in a virtual reality task that simulates a typical workday in a corporate setting. Participants were divided into three groups: a control group engaged in tasks without cybersecurity threats, and two experimental groups exposed to cybersecurity threats, but one with feedback on performance and the other without feedback. By comparing the control group with the experimental groups, the findings suggest that virtual reality is a promising tool for delivering immersive and ecologically valid cybersecurity training. The presence of performance feedback within these simulations was crucial for participants to better comprehend the complexities of cyber threats. Additionally, within the experimental groups, risky behaviors displayed during the virtual tasks, along with participants' age, emerged as predictors of their attitudes toward cybersecurity and cybercrime in organizational settings. In conclusion, by taking advantage of this cutting-edge virtual reality approach, individuals, businesses, and governments can foster more secure cybersecurity practices, contributing to a safer digital landscape for everyone.

Keywords Cybersecurity · Virtual reality · Social engineering · Phishing · Simulation

1 Introduction

In today's fast advancing technological landscape, one of the most pressing challenges is the rise of the internet of things or cyber-physical systems (Arpaci and Sevinc 2022). The demand for strong cybersecurity has reached a critical juncture as devices link up, new pathways for cyber threats emerge, heightening the importance of safeguarding sensitive data and vital infrastructure through robust cybersecurity measures (Arpaci and Sevinc 2022; AlDaajeh et al. 2022; Zwilling et al. 2022).

During the COVID-19 pandemic, cybersecurity threats rose due to increased hacker activity owing to the expansion of remote work (Choudhary et al. 2022; Corallo et al. 2022). Endpoints shifted from devices to people, amplifying vulnerability for both individuals and organizations (Choudhary et al. 2022; Corallo et al. 2022; Zwilling et al. 2022). The consequences of inadequate cybersecurity are far-reaching, impacting the global economy (Cremer et al. 2022; Malik et al. 2020).

Recent studies highlight a crucial focus: the human dimension in cybersecurity (AlDaajeh et al. 2022; Cains et al. 2022; Corallo et al. 2022; Fatokun et al. 2019; Veneruso et al. 2020). This approach redefines the traditional machine-centric view, acknowledging humans' multifaceted roles as users, defenders, and attackers (Cains et al. 2022).

The human factor, both its behavioral aspects and the individual characteristics, poses the greatest risk in cybersecurity, potentially opening critical systems to unauthorized access (Alqahtani 2022).

From a behavioral prism, users misbehave resulting from risky practices, lack of online knowledge, or resistance to

✉ Tiago Abril
tiago.abril@ulusofona.pt

[1] HEI-Lab: Digital Human-Environment Interaction Labs, Escola de Psicologia e Ciências da Vida, Universidade Lusófona (UL), Campo Grande, 376, 1749-024 Lisbon, Portugal

[2] Faculty of Medicine of the University of Porto, Porto, Portugal

Published online: 08 September 2025

comply with security procedures can cause serious problems (Ansari 2022). Cybercriminals leverage these vulnerabilities through action like phishing (Fatokun et al. 2019; Veneruso et al. 2020), vishing (Alsharif et al. 2021; Ansari et al. 2022; Patel et al. 2023), and by exploiting unattended computers (Branley-Bell et al. 2022; Kautwima et al. 2021).

Phishing is a type of social engineering attack in which criminals send fake emails (Alsharif et al. 2021; Patel et al. 2023), where simple actions like opening suspicious email attachments or falling for phishing links can pave the way for cyber breaches (Fatokun et al. 2019). Cybercriminals can collect specific data about their targets, enhancing the appeal and persuasiveness of their messages (Xu et al. 2023).

Vishing is a variation of phishing attacks, in which phone calls are used to deceive victims (Alsharif et al. 2021; Ansari et al. 2022; Patel et al. 2023). These tactics further diversify cybercriminals' approaches to compromising sensitive data (Alsharif et al. 2021; Ansari et al. 2022; Patel et al. 2023).

The end-user behaviors like leaving computers unattended were identified as other typical occurrences (Branley-Bell et al. 2022; Kautwima et al. 2021). It is common that unattended computers are left with active sessions, making them vulnerable to insider threats, and potentially leading to unauthorized access and data breaches (Kautwima et al. 2021).

Identifying misbehaviors as vulnerable aspects and promoting protective behaviors is a cornerstone to safeguard individuals and organizations from cyber threats (Alqahtani 2022; Nunes et al. 2021). Cybersecurity awareness training seems to be vital for educating users about risks and consequences of engaging in unsafe cybersecurity behavior (Nunes et al. 2021; Zwilling et al. 2022), empowering them to make informed decisions and defend themselves against cyber threats (Ansari et al. 2022).

Within this context, some groups of researchers have proposed innovative gamification methods for cybersecurity training and behavioral change (Khan et al. 2022; Matovu et al. 2022; Veneruso et al. 2020). However, the prevailing emphasis is on nonecological gamification methodologies, as observed in the study by Adinolf et al. (2019). These authors tested an interaction with a virtual agent where metaphors were translated into cybersecurity concepts. This approach, while providing valuable learning experiences, does not entirely replicate real-life cyber threats (Seo et al. 2019).

This suggests the need for new cybersecurity strategies and education approaches with an ecological valence (AlDaajeh et al. 2022; Corallo et al. 2022). To address this gap, Seo et al. (2019) developed a Virtual Reality (VR)-based ecological training of security skills for students and professionals in the field of cybersecurity. The authors attempted to augment the cyber infrastructure, yet they neglected the behavioral aspects of interactions. Also, their research primarily concentrated on a specific professional group, namely cybersecurity professionals.

Besides behavioral aspects, human factors such as age seem to play an important role on cybersecurity perceptions, attitudes and behaviors (Alsharida et al. 2023; Fatokun et al. 2019; Lee and Chua 2023). Older users demonstrate greater awareness and familiarity with cyber-threats, yet exhibit lower likelihood to keep their devices safe when compared to younger users (Branley-Bell et al. 2022; Fatokun et al. 2019). Yet, some authors have not found any significant effect of age (Ugwu et al. 2022; Zaoui and Sadqi 2023).

Furthermore, as cybersecurity threats grow in complexity, the integration of advanced technologies such as Artificial Intelligence (AI), Blockchain, and Cloud Computing has significantly reshaped the threat landscape, especially in emerging digital ecosystems like the Metaverse (Radanliev 2024a, b). These technologies not only offer innovative defenses, such as AI-driven predictive models and quantum-resistant blockchain infrastructures, but also introduce new vulnerabilities and regulatory challenges that demand proactive and human-centered responses (Radanliev 2024a). Within this shifting paradigm, immersive simulation-based training can serve to educating users about real-world threats rooted in advanced infrastructures and reinforcing secure behavioral patterns. In particular, the Metaverse highlights the urgent need for ecologically valid training approaches that anticipate cross-platform, cross-border risks involving cloud infrastructure, decentralized networks, and user data privacy (Radanliev 2024a). Recent work by Radanliev (2024b) underscores the need for cybersecurity strategies that are adaptive, sector-specific, and psychologically informed. As digital security culture shifts from reactive to proactive models, incorporating real-time threat detection, zero-trust principles, and behavioral change techniques, training interventions must evolve accordingly. Psychological ownership of data, the feeling of control and responsibility over one's digital footprint, is emerging as a critical factor in motivating secure behavior (Radanliev 2024b). VR-based simulations, by immersing users in realistic and personally relevant security scenarios, may cultivate this sense of ownership while closing the gap between security intentions and actual practices.

The first objective of this study is to push the boundaries of gamification by taking hold of VR to create a more immersive and engaging simulator experience on cybersecurity threats where risky behaviors could be tested within an ecological setting that aims at replicating a real-life context (Clarke 2021; Personeni and Savescu 2023; Yunchao et al. 2023), fostering a deeper understanding of cybersecurity

risks, ultimately leading to a reduction in risky behaviors (Seo et al. 2019).

Additionally, as demonstrated by previous research (Švábenský et al. 2022), the delivery of personalized, targeted instruction and feedback plays a crucial role in boosting the effectiveness of cybersecurity training programs. As such, the second objective is to test a simulator that effectively raise awareness and promote the reduction of risky behaviors by adding feedback to the experience. This feedback mechanism may help participants comprehending the relevance of the VR application in relation to cybersecurity.

Following this avenue, the third objective of this study is to show that the risky conduct displayed by lay individuals, who are not cybersecurity professionals, within the VR ecological-based application, along with the age of participants, can act as predictors for attitudes toward cybersecurity and cybercrime.

2 Method

2.1 Sample

For the first and second objectives, an a priori power analysis was conducted using G*Power version 3.1.9.7 (Faul et al. 2007) to determine the minimum sample size required for a *F*-test Multivariate Multiple Linear Regression (MMLR), with two predictors and assuming a medium effect with a statistical power of 0.80, at a significance criterion of $\alpha = 0.05$, was 68. For the third objective the same procedure was conducted for a *t*-test Ordinary Least Squares (OLS) Regression with three predictors, and the sample size required was 43.

The sample for this study comprised 70 undergraduates or higher education adults. The mean age was 22.81 years (± 7.04). 57.1% participants were female.

To carry out the present study, three conditions were established. In the first condition (C1), a group of participants engaged in a virtual reality task (see Design and Procedures section) without cybersecurity threats present ($n = 24$). In the second condition (C2), a group of participants performed a similar task, but with cybersecurity threats in place ($n = 23$). Lastly, in the third condition (C3), the participants completed the same task as in the second condition, but also received feedback on their cybersecurity performance ($n = 23$).

2.2 Measures

Questionnaire of socio demographic data (sex, age, civil status, education, professional status, level of experience with computers, how often video games are played, and how often virtual reality is experienced).

Number of risky behaviors (NIR) committed within the VR task, ranging from 0 to 5. These threats included three phishing emails, a vishing phone call and leaving the work computer active and accessible to others when leaving the desk for few moments.

Experience questionnaire (EQ) was created for the present study, and was based on Zwilling et al. 2022 study, with six items and a Likert-type scale from 0 "Nothing" to 10 "A lot". The EQ evaluates cybersecurity awareness, knowledge, and protection behaviors acquisition perception towards the application in virtual reality. The EQ shows good internal consistency within the present dataset ($\alpha = 0.96$) as a one-dimensional scale.

An adapted version of risky cybersecurity behaviors scale (RScB), Portuguese version by Nunes et al. (2021). This adapted version included the instruction "After the experience in virtual reality you still consider:", followed by 20 items depicting several cybersecurity behaviors rated in a Likert-type scale from 0 "Never" to 4 "Always". The internal consistency was good $\alpha = 0.82$ in the current sample.

Attitudes towards cybersecurity and cybercrime in business (ATC-IB), Portuguese version by Nunes et al. (2021). The ATC-IB consists of a 25 items scale aimed at the assessment of engagement and awareness regarding cybersecurity, rated in a Likert-type scale from 1 "Totally Agree" to 4 "Totally Disagree". The internal consistency found in the current sample was also good ($\alpha = 0.76$).

2.3 Design and procedures

This study (Fig. 1) was approved by the ethics committee of the School of Psychology and Life Sciences of Lusófona University (CEDIC-2023-1-10) and was carried out in the Experimental Psychology Laboratory of HEI-Lab at the Lusófona University, in a 3 × 3 m room. Sampling took place between May 2023 and July 2023.

Sample recruitment was conducted at the Lusófona University campus, and potential participants willing to enroll in the study were invited to schedule a session. Inclusion criteria included participants over 18 years old and native Portuguese speakers. Pregnant participants or participants that previously experienced cybersickness were excluded from the study.

Participants were randomly assigned to a control group (C1), an experimental group without feedback (C2), and an experimental group with feedback (C3). All participants were given an informed consent form, describing the inclusion and exclusion criteria. Participation was voluntary and data anonymity and confidentiality was warranted. Participants were informed that the main objective was to replicate

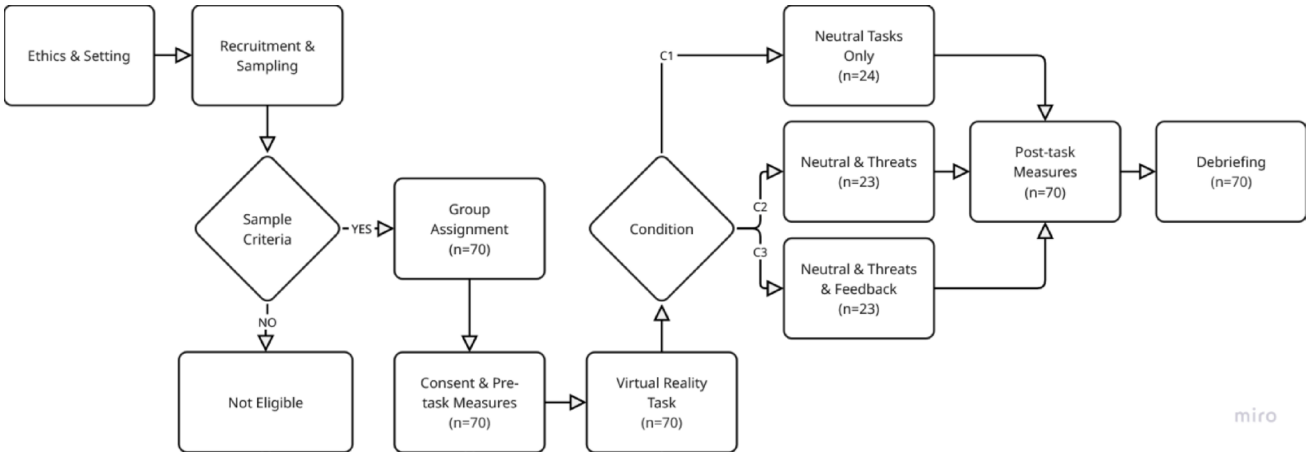

Fig. 1 Procedure flow of the present virtual reality cybersecurity study

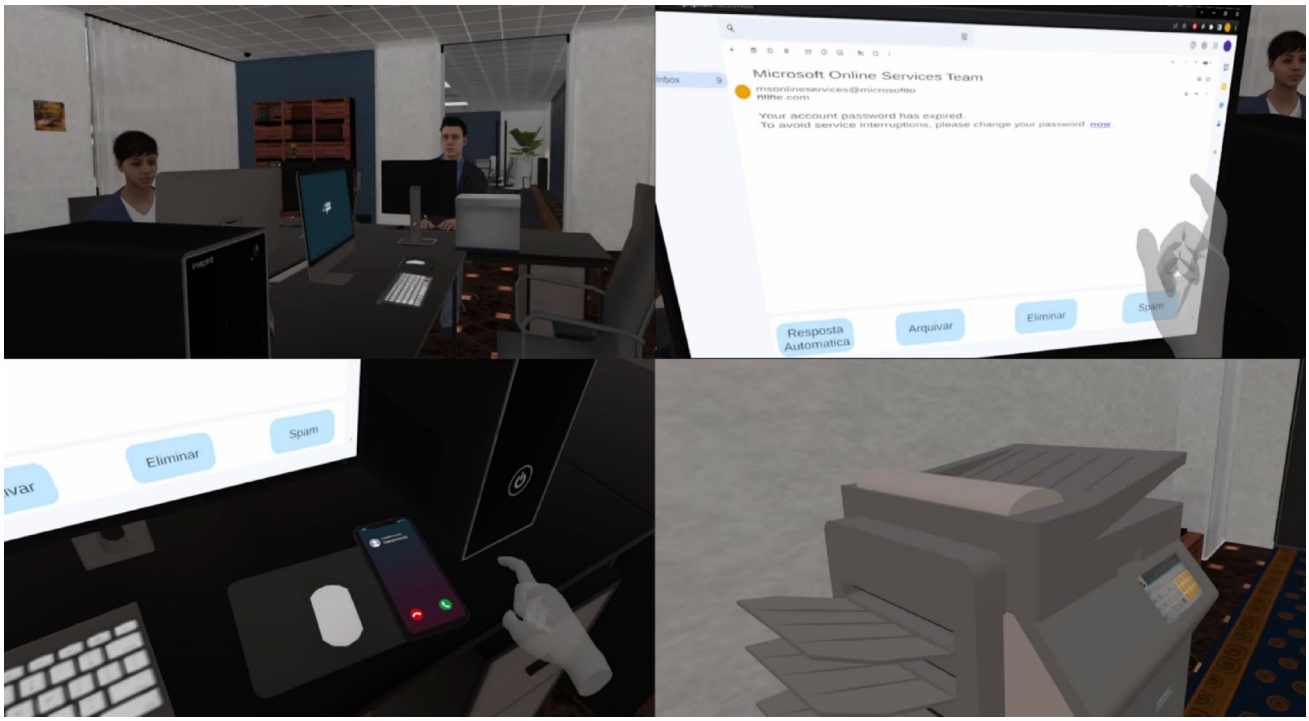

Fig. 2 Sample of the virtual reality business environment (**a**: shared workspace with male and female colleagues in a business environment; **b**: replying to emails, including phishing attempts; **c** handling phone calls, including vishing phone calls; **d**: leaving the computer unattended and accessible by others while performing other tasks)

in virtual reality a typical workday in an office setting to access their opinion on that experience, and filled a questionnaire regarding demographic data on Qualtrics.

After that, and under the supervision of a qualified technician, each participant engaged in a 10-min virtual reality task, with hand tracking, using the VR Quest 2. The task simulates a typical workday in an office setting, starting with a tutorial to familiarize participants with the virtual environment. After completing the tutorial, participants were transferred to a business environment, sharing a room with a female and a male colleague (Fig. 2a). Participants completed various tasks in an office environment, such as replying to emails (Fig. 2b), answering phone calls (Fig. 2c), and leaving their work desk while carrying out other tasks (Fig. 2d).

The control group (C1) engaged on neutral tasks, whereas the experimental groups (C2 and C3) engaged in the same neutral tasks, with additional cybersecurity threat interactions. Participants in the experimental group with feedback (C3) received feedback, upon experience's conclusion, on what they did wrong, explaining why that was considered incorrect and what was the right thing to do.

Upon completion, all participants returned to the Qualtrics platform and filled in the EQ, RScB, and ATC-IB questionnaires. Lastly, participants received a debriefing highlighting the real objective of the study. The entire procedure took approximately 30 min to complete.

2.4 Statistical analysis

Regarding the statistical analysis, we began by conducting a preliminary analysis to identify potential confounding variables. Subsequently, we performed a MMLR to examine the effects of the independent variables on two criterion variables (RScB and EQ). This method was chosen to assess how the predictors jointly impact several criterion variables, while also considering the relationships among those outcomes. An analogic stepwise backward selection procedure was employed to address potential confounding variables, with the goal of including the most relevant predictors while simplifying the overall model.

Finally, we conducted an OLS Regression using only participants from the experimental groups (C2 and C3), again applying the same stepwise backward selection procedure to account for confounding variables. This analysis was used to assess the effects of the independent variables on ATC-IB.

All analyses were conducted in IBM SPSS, with a significance level set at $\alpha = 0.05$.

3 Results

Prior to analysis to confounding variables, was confirmed no statistically significant differences were found between the three conditions regarding sex ($\chi^2(2) = 1.12$, $p = 0.572$), age ($F(2, 69) = 0.46$, $p = 0.635$), civil status ($\chi^2(6) = 6.16$, $p = 0.405$), education ($\chi^2(6) = 3.27$, $p = 0.775$), professional status ($\chi^2(6) = 7.78$, $p = 0.255$), level of experience with computers ($F(2, 69) = 0.12$, $p = 0.891$), how often play video games ($F(2, 69) = 1.01$, $p = 0.368$), and how often experience virtual reality ($F(2, 69) = 0.61$, $p = 0.545$).

Regarding the first objective, a MMLR was carried out with the three conditions under investigation (C1, C2, and C3, with C3 as the reference category) as predictors, and RScB as the criterion variable. The model explained 12.8% of the total variance of the RScB (Adjusted $R^2 = 0.13$ ($F(2, 67) = 6.05$, $p = 0.004$). The experimental condition with feedback (C3) towards the control condition with only neutral tasks (C1) ($\beta = 0.43$, $p = 0.001$) yielded significant predictive results. condition However, no significant predictive results were observed when compared with the condition without feedback (C2) ($\beta = 0.11$, $p = 0.412$).

Regarding the second objective, the same MMLR was carried out with the three conditions under investigation (C1, C2, and C3, with C3 as the reference category) as predictors, and EQ as the criterion variable. The model explained 12.8% of the total variance of the EQ (Adjusted $R^2 = 0.13$ ($F(2, 67) = 6.06$, $p = 0.004$). The experimental condition with feedback (C3) towards the control condition with only neutral tasks (C1) ($\beta = -0.43$, $p = 0.002$), and towards the condition without feedback (C2) ($\beta = -0.35$, $p = 0.008$) yielded significant predictive results.

Regarding the third objective an OLS Regression was carried out with both experimental conditions (C2 and C3), NIR, the confounding variable age and the experimental condition as a dichotomous variable without feedback (C2) and with feedback (C3) as predictors, and ATC-IB as the criterion variable. The model explained 21.2% of the total variance of the ATC-IB (Adjusted $R^2 = 0.21$ ($F(3, 42) = 5.04$, $p = 0.005$). NIR ($\beta = -0.41$, $t(42) = -3.03$, $p = 0.004$), and age ($\beta = 0.37$, $t(42) = 2.77$, $p = 0.008$) yielded significant predictive results towards ATC-IB. The experimental conditions without feedback (C2) and with feedback (C3) ($\beta = 0.06$, $t(42) = 0.44$, $p = 0.661$) yielded no significant predictive results.

4 Discussion

The findings of this study seem to shed some light on several critical aspects of cybersecurity awareness and training.

The first objective of the study was to explore the potential of using VR to create an immersive and engaging simulating experience. The results demonstrate that incorporating VR into cybersecurity training, as Seo et al. (2019) did, but for individuals that are not cybersecurity professionals, may enhance bring into play the ecological factor (Clarke 2021; Personeni and Savescu 2023; Yunchao et al. 2023). This immersive approach is central as it replicates specific real-world scenarios, allowing participants to experience cybersecurity challenges firsthand, which could significantly improve their ability to recognize and respond to real cyber threats effectively. This outcome may underscore the critical role of organizational culture and awareness in fostering secure cybersecurity practices among employees. It highlights the viability of adopting an ecological simulation training approach, which may effectively demonstrate the real-world impact of risky behaviors and their consequences at both personal and organizational levels. Further investigation is needed to assess the extent to which integrating VR into cybersecurity training could act as a complement or as a surrogate for traditional cybersecurity training.

Our second objective was to emphasize the importance of feedback in the efficacy of cybersecurity training programs.

The results suggest that providing personalized, targeted instruction, and feedback may significantly improve the participants' overall experience of training regrading cybersecurity awareness and risk-reduction behaviors. Feedback is a powerful tool that helps participants comprehend the relevance and implications of their actions within the VR environment. This understanding may translate into better cybersecurity practices and a more cautious approach towards potential threats, congruous with Švábenský et al. (2022). These findings underscore the significance of feedback as an effective tool, fostering participants' comprehension of the relevance and implications of their actions in a VR environment. However, further longitudinal data is needed in order to fully understand the pivotal role it plays in the effectiveness of cybersecurity training programs.

The third objective of this study emphasizes how risky conduct and age predicts the attitudes, of individuals that are not cybersecurity professionals, toward cybersecurity and cybercrime. Our research indicates that engaging in risky behaviors diminishes positive attitudes toward cybersecurity and cybercrime. Moreover, concerning age, being older seems to positively shape these attitudes. These age-related results align with previous research (Branley-Bell et al. 2022; Fatokun et al. 2019), highlighting the importance of age as a factor when promoting secure practices among younger employees. The findings accentuate the relevance of exposing individuals to day-to-day scenarios, where they can learn from their mistakes, fostering changes in decision-making and attitudes regarding cybersecurity. In addition, since no differences were found between feedback strategies in predicting attitudes toward cybersecurity and cybercrime, these results suggest that the VR simulation experience could be useful not only as a training tool but also as an assessment tool. It could potentially be used to predict attitudes toward cybersecurity and cybercrime during the interview and recruitment process. However, further studies involving non-cybersecurity professionals working within the same company are needed.

Nevertheless, the current study is not free from methodological limitations that require further studies. Its cross-sectional design and the absence of a baseline assessment of the attitudes and risk cybersecurity behaviors hinders the establishment of causality. Furthermore, the convenience sampling method used to recruit participants and the non-representativity of the samples included in this study requires that the generalization of findings be made with caution. On the other hand, the present VR simulation approach, focusing on the human element, serves as a promising strategy to address the growing need for effective cybersecurity training. By providing participants with hands-on experiences in dealing with cyber threats, the study contributes to closing the gap between theoretical knowledge and practical application, but also, by accessing and giving feedback on real behavior. Bridging this gap is essential, as the main challenge in cybersecurity awareness lies not in lacking essential knowledge but in applying that knowledge effectively in real-world situations.

The findings resonate with Radanliev's (2024b) broader call for holistic, sector-aware, and psychologically grounded approaches to digital security. As the study of psychological ownership, behavioral intention gaps, and proactive security culture gains prominence, VR training offers a powerful platform for integrating these insights into practice. Furthermore, gaining added relevance in light of recent advancements in cybersecurity involving AI, blockchain, and cloud-based systems, especially as they relate to emerging digital infrastructures like the Metaverse. The dynamic nature of these technologies introduces not only new defensive capabilities, such as AI-enhanced threat prediction and blockchain's quantum-resistant frameworks, but also new behavioral and regulatory challenges. As cloud adoption accelerates and single-provider dependencies become widespread, a human-centric and ecologically grounded training approach becomes critical to mitigating emerging risks.

By fostering realistic, embodied experiences of threat detection and response, such simulations align with the trend toward dynamic, continuous, and trust-centered cybersecurity strategies. Moreover, VR-based approaches may help bridge the persistent gap between awareness and action, a gap that remains a key vulnerability across businesses, allowing lay individuals to rehearse and internalize secure behaviors within realistic digital environments, potentially extending their value beyond traditional corporate training to future-facing digital platforms and infrastructures.

This approach may not only raise awareness but also fosters a deeper understanding of the importance of adhering to cybersecurity protocols and best practices. Ultimately, a comprehensive training can help create a stronger cybersecurity culture within companies and improve overall cybersecurity posture, reducing the likelihood of successful cyberattacks and safeguarding sensitive information.

Acknowledgements This work was funded by Fundação para a Ciência e Tecnologia (FCT), under HEI-Lab R&D Unit (UIDB/05380/2020, https://doi.org/10.54499/UIDB/05380/2020).

Author contributions A.T. and G.P. wrote the main manuscript. A.T. prepared Fig. 1, Data 1 and Video 1. D.F. and P.F. developed the VR task. All authors reviewed the manuscript.

Funding Open access funding provided by FCT|FCCN (b-on).

Data availability Data is provided within the manuscript and within supplementary information files.

Declarations

Conflict of interest The authors declare no competing interests.

References

Adinolf S, Wyeth P, Brown R et al (2019) Towards designing agent based virtual reality applications for cybersecurity training. OzCHI. https://doi.org/10.1145/3369457.3369515

AlDaajeh S, Saleous H, Alrabaee S et al (2022) The role of national cybersecurity strategies on the improvement of cybersecurity education. Comput Secur 119:102754. https://doi.org/10.1016/j.cose.2022.102754

Alqahtani MA (2022) Factors affecting cybersecurity awareness among university students. Appl Sci 12(5):2589. https://doi.org/10.3390/app12052589

Alsharida RA, Al-rimy BAS, Al-Emran M et al (2023) A systematic review of multi perspectives on human cybersecurity behavior. Tech Soc 73:102258. https://doi.org/10.1016/j.techsoc.2023.102258

Alsharif M, Mishra S, AlShehri M (2021) Impact of human vulnerabilities on cybersecurity. Comput Syst Sci Eng 40(3):1153–1166. https://doi.org/10.32604/csse.2022.019938

Ansari MF (2022) A quantitative study of risk scores and the effectiveness of AI-based cybersecurity awareness training programs. IJSSAN 3(3):1–8. https://doi.org/10.47893/IJSSAN.2022.1212

Ansari MF, Sharma PK, Dash B (2022) Prevention of phishing attacks using AI-based cybersecurity awareness training. IJSSAN 3(3):61–72. https://doi.org/10.47893/IJSSAN.2022.1221

Arpaci I, Sevinc K (2022) Development of the cybersecurity scale (CS-S): evidence of validity and reliability. Inf Dev 38(2):218–226. https://doi.org/10.1177/0266666921997512

Branley-Bell D, Coventry L, Dixon M et al (2022) Exploring age and gender differences in ICT cybersecurity behaviour. Hum Behav Emerg Technol. https://doi.org/10.1155/2022/2693080

Cains MG, Flora L, Taber D (2022) Defining cyber security and cyber security risk within a multidisciplinary context using expert elicitation. Risk Anal 42(8):1643–1669. https://doi.org/10.1111/risa.13687

Choudhary A, Choudhary G, Pareek K et al (2022) Emerging cyber security challenges after COVID pandemic: a survey. JISIS 12(2):21–50. https://doi.org/10.22667/JISIS.2022.05.31.021

Clarke E (2021) Virtual reality simulation—the future of orthopaedic training? A systematic review and narrative analysis. Adv Simul 6:2. https://doi.org/10.1186/s41077-020-00153-x

Corallo A, Lazoi M, Lezzi M et al (2022) Cybersecurity awareness in the context of the industrial internet of things: a systematic literature review. Comput Ind 137:103614. https://doi.org/10.1016/j.compind.2022.103614

Cremer F, Sheehan B, Fortmann M et al (2022) Cyber risk and cybersecurity: a systematic review of data availability. Geneva Pap Risk Insur Issues Pract 47:698–736. https://doi.org/10.1057/s41288-022-00266-6

Fatokun FB, Hamid S, Norman A et al (2019) The impact of age, gender, and educational level on the cybersecurity behaviors of tertiary institution students: an empirical investigation on Malaysian universities. ICCSE. https://doi.org/10.1088/1742-6596/1339/1/012098

Faul F, Erdfelder E, Lang AG et al (2007) G*power 3: a flexible statistical power analysis program for the social, behavioral, and biomedical sciences. Behav Res Methods 39:175–191. https://doi.org/10.3758/BF03193146

Kautwima P, Haiduwa T, Sai K et al (2021) System end-user actions as a threat to information system security. IJNSA 13(6):71–83. https://doi.org/10.5121/ijnsa.2021.13606

Khan MA, Merabet A, Shamma Alkaabi S et al (2022) Game-based learning platform to enhance cybersecurity education. Educ Inf Technol 27:5153–5177. https://doi.org/10.1007/s10639-021-10807-6

Lee CS, Chua YT (2023) The role of cybersecurity knowledge and awareness in cybersecurity intention and behavior in the United States. Crim Delinq. https://doi.org/10.1177/00111287231180093

Malik J, Akhunzada A, Bibi I et al (2020) Hybrid deep learning: an efficient reconnaissance and surveillance detection mechanism in SDN. IEEE Access 8:134695–134706. https://doi.org/10.1109/ACCESS.2020.3009849

Matovu R, Nwokeji JC, Holmes T et al (2022) Teaching and learning cybersecurity awareness with gamification in smaller universities and colleges. FIE. https://doi.org/10.1109/FIE56618.2022.9962519

Nunes P, Antunes M, Silva C (2021) Evaluating cybersecurity attitudes and behaviors in Portuguese cybersecurity attitudes and behaviors. Procedia Comput Sci 181:173–181. https://doi.org/10.1016/j.procs.2021.01.118

Patel AU, Williams CL, Hart SN et al (2023) Cybersecurity and information assurance for the clinical laboratory. JALM 8(1):145–161. https://doi.org/10.1093/jalm/jfac119

Personeni G, Savescu A (2023) Ecological validity of virtual reality simulations in workstation health and safety assessment. Front Virtual Real 4:1058790. https://doi.org/10.3389/frvir.2023.1058790

Radanliev P (2024a) Integrated cybersecurity for metaverse systems operating with artificial intelligence, blockchains, and cloud computing. Front Blockchain 7:1359130. https://doi.org/10.3389/fbloc.2024.1359130

Radanliev P (2024b) Digital security by design. Secur J 37:1640–1679. https://doi.org/10.1057/s41284-024-00435-3

Seo JH, Bruner M, Payne A et al (2019) Using virtual reality to enforce principles of cybersecurity. J Comput Scince Educ 10(1):81–87. https://doi.org/10.22369/issn.2153-4136/10/1/13

Švábenský V, Vykopal J, Čeleda P et al (2022) Applications of educational data mining and learning analytics on data from cybersecurity training. Educ Inf Technol 27:12179–12212. https://doi.org/10.1007/s10639-022-11093-6

Ugwu C, Ani C, Ezema M et al (2022) Towards determining the effect of age and educational level on cyber-hygiene. NIGERCON. https://doi.org/10.1109/NIGERCON54645.2022.9803154

Veneruso SV, Ferro LS, Marrella A et al (2020) CyberVR: an interactive learning experience in virtual reality for cybersecurity related issues. AVI. https://doi.org/10.1145/3399715.3399860

Xu T, Singh K, Rajivan P (2023) Personalized persuasion: quantifying susceptibility to information exploitation in spear-phishing attacks. Appl Ergon 108:103908. https://doi.org/10.1016/j.apergo.2022.103908

Yunchao M, Mengyao R, Xingman L (2023) Application of virtual simulation technology in sports decision training: a systematic review. Front Psychol 14:1164117. https://doi.org/10.3389/fpsyg.2023.1164117

Zaoui M, Sadqi Y (2023) Toward understanding the impact of demographic factors on cybersecurity awareness in the moroccan context. In: Idrissi N, Hair A, Lazaar M et al (eds) Artificial intelligence and green computing. ICAIGC 2023. Lecture notes in networks and systems, vol 806. Springer, Cham, pp 207–214. https://doi.org/10.1007/978-3-031-46584-0_16

Zwilling M, Klien G, Lesjak D et al (2022) Cyber security awareness, knowledge and behavior: a comparative study. J Comput Inf Syst 62(1):82–97. https://doi.org/10.1080/08874417.2020.1712269