Journal of Cybersecurity Education, Research and Practice

Volume 2024 | Number 1 Article 11

11-29-2023

Preparing UK students for the workplace: The Acceptability of a Gamified Cybersecurity Training

Oliver J. Mason
University of Surrey, o.mason@surrey.ac.uk

Siobhan Collman
University of Surrey, siobhancollman@gmail.com

Stella Kazamia
University of Surrey, s.kazamia@surrey.ac.uk

Ioana Boureanu
University of Surrey, i.boureanu@surrey.ac.uk

Recommended Citation

Mason, Oliver J.; Collman, Siobhan; Kazamia, Stella; and Boureanu, Ioana (2023) "Preparing UK students for the workplace: The Acceptability of a Gamified Cybersecurity Training," *Journal of Cybersecurity Education, Research and Practice*: Vol. 2024: No. 1, Article 11.
DOI: 10.32727/8.2023.35
Available at: https://digitalcommons.kennesaw.edu/jcerp/vol2024/iss1/11

Preparing UK students for the workplace: The Acceptability of a Gamified Cybersecurity Training

Abstract

This pilot study aims to assess the acceptability of Open University's training platform called Gamified Intelligent Cyber Aptitude and Skills Training course (GICAST), as a means of improving cybersecurity knowledge, attitudes, and behaviours in undergraduate students using both quantitative and qualitative methods. A mixed-methods, pre-post experimental design was employed. 43 self-selected participants were recruited via an online register and posters at the university (excluding IT related courses). Participants completed the Human Aspects of Information Security Questionnaire (HAIS-Q) and Fear of Missing Out (FoMO) Scale. They then completed all games and quizzes in the GICAST course before repeating the HAIS-Q and FoMO scales as well as several open-ended questions. Pre-training HAIS-Q Knowledge, Attitude and Behaviour all improved from 'reasonable' pre-training levels to become 'very high' following training with large effect sizes estimated. FoMO improved to a lesser degree but also predicted the degree of HAIS-Q improvement suggesting it is relevant to the impact of this training course. Qualitatively, five key themes were generated: enjoyment, engagement, usability of GICAST, content relevance, and perceived educational efficacy. Overall, sentiment towards training was very positive as an enjoyable engaging and usable course. GICAST was found to be a feasible course for a wide range of students at a UK university: overall the training improved cyber-security awareness on a well validated measure with outcomes comparable to information-security-trained employees of a secure workplace. Despite a diversity of views about content, the course appears to be well suited to the non-IT undergraduate sector and may suit wide uptake to enhance students' employability in a wide range of cybersecurity relevant contexts.

Keywords

gamified, training, undergraduate

Cover Page Footnote

ACKNOWLEDGMENTS We would like to thank Dr. Chitra Balakrishna and her colleagues at the Open University for their assistance in respect of GICAST. CONFLICT OF INTEREST STATEMENT The authors declare no conflicts of interest. FUNDING This work was supported by the National Cyber Security Centre, as part of the programmes for Academic Centres of Excellence in Cyber Security Education.

Preparing UK students for the workplace: The Acceptability of a Gamified Cybersecurity Training

Oliver J. Mason
School of Psychology
University of Surrey
Guildford
GU2 7XH
England
o.mason@surrey.ac.uk
https://orcid.org/0000-0001-8376-0694

Siobhan Collman
School of Psychology
University of Surrey
Guildford
GU2 7XH
England

Stella Kazamia
Department of Computer Science
University of Surrey
Guildford
GU2 7XH
England

Ioana Boureanu
Department of Computer Science
University of Surrey
Guildford
GU2 7XH
England

This pilot study aims to assess the acceptability of Open University's training platform called Gamified Intelligent Cyber Aptitude and Skills Training course (GICAST), as a means of improving cybersecurity knowledge, attitudes, and behaviours in undergraduate students using both quantitative and qualitative methods. A mixed-methods, pre-post experimental design was employed. 43 self-selected participants were recruited via an online register and posters at the university (excluding IT related courses). Participants completed the Human Aspects of Information Security Questionnaire (HAIS-Q) and Fear of Missing Out (FoMO) Scale. They then completed all games and quizzes in the GICAST course before repeating the HAIS-Q and FoMO scales as well as several open-ended questions. Pre-training HAIS-Q Knowledge, Attitude and Behaviour all improved from 'reasonable' pre-training levels to become 'very high' following training with large effect sizes estimated. FoMO improved to a lesser degree but also predicted the degree of HAIS-Q improvement suggesting it is relevant to the impact of this training course. Qualitatively, five key themes were generated: enjoyment, engagement, usability of GICAST, content relevance, and perceived educational efficacy. Overall, sentiment towards training was very positive as an enjoyable engaging and usable course. GICAST was found to be a feasible course for a wide range of students at a UK university: overall the training improved cyber-security awareness on a well validated measure with outcomes comparable to information-security-trained employees of a secure workplace. Despite a diversity of views about content, the course appears to be well suited to the non-IT undergraduate sector and may suit wide uptake to enhance students' employability in a wide range of cybersecurity relevant contexts.

Keywords—cybersecurity, training, undergraduate

I. INTRODUCTION

The exponential growth of cyberspace is affecting how we communicate and conduct our personal and professional lives, and the digital world has become central to national prosperity and security in the UK as elsewhere [1, 2]. These developments have also brought new forms of risk. Cybersecurity breaches are a major threat to economies, corporations, and individuals, and this threat continues to grow and diversify as cybercriminals and even state-sponsored actors adopt increasingly sophisticated methods of attack [3; 4]. Indeed, the magnitude of risk is high enough that the National Cyber Security Centre (NCSC) was launched in 2016, with a focus on nurturing cybersecurity capability, reducing risk, and safeguarding the UK's £10.1 billion cybersecurity sector [5].

Alongside technical solutions, it is essential that members of the general public, including those accessing IT as part of their occupation, also possess a degree of cyber security awareness. Around 95% of all cyberattacks involve human error, including using easily guessable passwords, opening unsafe attachments, and disclosing regulated information [6]. Furthermore, only 11% of UK businesses have provided non-cyber employees with cybersecurity training, with major skills gaps existing around firewall set-up, personal data storage, and detecting malware [7]. Consequently, there is a clear need to address this skills shortage and improve the workforce's preparedness to respond to cyber-threats [8; 2]. The NCSC provided a short assessment of the threats to universities [9] highlighting that they remain a target due to high-value intellectual property, their open, outward-facing nature as a sector, and the high turnover of staff and students. This burgeoning field of cyber-security education in university students has recently been reviewed systematically by Švábenský, Vykopal and Čeleda [10] who described a wide variety of approaches including awareness campaigns, instructor-led sessions, and e-learning. They concluded that, out of 71 evaluations the median sample size was 40 and only 16 used pre-post designs with formal measures. Details of both data and training were also largely lacking.

In addition, many standard training approaches lack effectiveness due to the rapid, passive delivery of high volumes of information, leaving participants feeling overwhelmed, unengaged, and disconnected (11; 8; 12). More effective training hinges on delivery of complex content in a simple, interactive manner, wherein students have opportunities to fail and try again [8; 13]. Gamified training

This work was supported by the National Cyber Security Centre, as part of the programmes for Academic Centres of Excellence in Cyber Security Education

shows great promise here, with the topic of cybersecurity seeming particularly well-suited to this medium [14]. Indeed, using game characteristics (e.g., points systems, storylines, avatars) in learning environments can foster emotional engagement and prolonged interest in the content [15; 8], tackling some of the major downfalls of traditional learning. Furthermore, gamified content exemplifies several good learning principles, including providing information in context [16; 17], challenging the limits of learners' knowledge [16; 15], and promoting the development of new skills through active learning [16; 2]. Consequently, gamified training has the potential to be much more effective than standard awareness and e-learning approaches [18].

II. Background

A. Gamification and Cybersecurity

Gamified applications used in undergraduate cybersecurity education have been extensively described by Weitl-Harms and colleagues [19] including several that have received evaluation. These are extremely varied in nature and content and the reader is pointed to this source for further details. The majority in their review are specifically for computer science students taking courses in cybersecurity; several have cybersecurity elements embedded in wider generalized education gamification frameworks; and some focus on specific areas such as phishing, or how to defend against hacking attacks. The same group has usefully provided a classification scheme of genres for cybersecurity education on computer science course [20]. Even though the current study is not in the computer science education context we would note that their classification of 'Visualization of abstract ideas' as a broad category is an apt one that applies in the present context of a gamified course for non-specialist undergraduate education.

The badged open course Gamified Intelligent Cyber Aptitude and Skills Training (GICAST) [21] is introductory and suitable for broader education of the non-technical population [2]. GICAST was developed by The Open University and NCSC, and teaches foundational cybersecurity concepts such as firewalls, viruses, and passwords across eight units. Each week contains a short analogy-driven or real-life-inspired game, which begins with an overview of key concepts (e.g., the authentication unit characterises a strong password) before learners' cybersecurity behaviour is assessed through in-game tasks (e.g., write a strong password to protect property). Written content aims to provide deeper learning. At the end of each unit, learning is assessed through a quiz and has been shown to improve retention of knowledge in relatively low skilled workers [2].

Meta-analyses indicate gamified educational content like GICAST provides various benefits to learners and performs better than traditional means of education [22; 23]. Sitzmann's [23] meta-analysis of 65 studies using pre-test post-test designs found digital game-based content to be a more effective means of instruction when compared to control groups receiving either no training or non-game-based education. Subsequently, a meta-analysis and systematic review of 69 studies [22] found digital games significantly enhanced learner performance against a range of outcomes when compared to non-game learning conditions. Positive learner experience, rather than visual realism, seems to be the key to this benefit.

Despite these promising findings around benefits to learning and attitudes, there is a relative dearth of studies investigating the impact of gamified training on cybersecurity behaviours and associated psychological factors involved. A rare experimental study found serious cybersecurity games resulted in higher perceived behavioural control; intention to act in a cybersecure manner; and actual cybersecure behaviours versus controls [18]. While this is a positive early indication that gamified cybersecurity training can effect both attitude and behaviour change, it remains difficult to reach firm conclusions [14]. The wider literature on cybersecurity also posits several factors pertinent to the impact on training that have yet to be widely explored. Fear of Missing Out (FoMO) is probably the most pertinent and is defined as apprehension that one is not included in fun or rewarding experiences that others may be having [24], and has been identified as a significant predictor of risky online behaviour. Popovac and Hadlington [25] describe how high-FoMO individuals may overshare via digital platforms due to fear of ostracism, increasing susceptibility to cyberthreats and victimisation. FoMO significantly predicts online risk taking (e.g., sharing passwords and opening email attachments from strangers) [25], is associated with problematic internet use [26], and is the most potent single negative predictor of information security awareness, outperforming Big Five personality traits, age, and gender [27]. Such findings include FoMO as an essential component to consider when evaluating cybersecurity behaviours and the influence of gamified training.

B. Aims and Hypotheses

The current pilot study aims to assess the acceptability of gamified training as a means of increasing cybersecurity awareness and knowledge among individuals without a technical background. This will be achieved by examining and documenting the rate of training completion in those who express an interest as well as their feedback on the training provided. Quantitatively, though not formally a strongly powered outcome study able to accurately estimate training effect size, the aim was to recruit a sufficiently large sample size to examine the potential positive changes in cybersecurity knowledge, attitudes, and behaviours. We hypothesised significant improvements in these areas, as measured by the Human Aspects of Information Security Questionnaire (HAIS-Q) [28]. Additionally, we also hypothesised that the Fear of Missing Out (FoMO) construct would be related to poorer cybersecurity knowledge, attitudes, and behaviours, and we intended to further investigate its potential role in predicting training effect size.

We also aimed to use qualitative outputs to lend depth and dimension to quantitative results around the acceptability of gamified training. We anticipated that qualitative feedback would offer rudimentary insight into factors which may contribute towards, or inhibit, training acceptability. To address this, open-ended questions were designed with a several key objectives in mind. Firstly, we aimed to understand the attractive, successful features of gamified training (i.e., "What did you enjoy and not enjoy about doing the Gamified Intelligent Cyber Aptitude and Skills Training (GICAST) training?", and "Did you see benefits to it, and if so, what?). Secondly, we aimed to establish where friction points and potential challenges or obstacles exist within gamified training (i.e., "What did you enjoy and not enjoy

about doing the Gamified Intelligent Cyber Aptitude and Skills Training (GICAST) training?", and "What would you change about the training for the future?"). And lastly, we aimed to gauge the relevance of gamified training for participants without a technical background (i.e., "Would you recommend it to other students?").

III. Methods

A. GICAST Course

GICAST is an innovative training program collaboratively developed by the Open University and the UK Government's National Cyber Security Programme. Its primary objective is to provide individuals with a comprehensive knowledge and understanding of essential cyber security concepts to safeguard their digital presence, such as malware, identity theft, network security, and risk management [20]. GICAST combines the principles of gamification and intelligence-based techniques to create a dynamic learning environment. Specifically, learners actively engage with short, Minecraft-style games that serve as instructional tools to teach cybersecurity principles and assess their online behaviours through a mix of analogy-based, real-world-inspired, and concept-driven storylines. Learning is allocated into eight weekly units (e.g., week 1 covers 'Threat Landscapes' and week 2 covers 'Authentication') and gives learners the flexibility to progress through the material at their own pace. Each week contains a unique game, written content, and a quiz to test comprehension. Successful completion of all weekly quizzes unlocks an industry-recognised digital badge and a certificate of achievement.

The development of GICAST was influenced by the valuable input of Balakrishna and Charlton [2], who contributed their expertise in course development and game mechanics, respectively. Their insights and contributions played a crucial role in shaping the program's design, ensuring its alignment with best practices in both instructional design and gamification principles.

B. Participants, Sampling and Recruitment

Participants were mostly volunteers, with some clustered targeting of courses and faculties in the latter stages of recruitment to improve representativeness. Participants were recruited through an online research register and poster advertisements at the university. Exclusion criteria were not being a University of Surrey student, being a postgraduate student, and being a student on an information technology-related course (such as Computer and Internet Engineering, Computer Science, or Electronic Engineering with Computer Systems).

The pre-training survey had 71 replies in total. 20 people were denied advancement due to meeting one or more of our exclusion criteria. 51 progressed to the training. 8 dropped out during the training period, while 43 completed the training and post-training survey giving a completion rate of 84%. Of those who completed the study, most were male (69.8%), Caucasian (44.2%), and majored in social science or arts subject (e.g., psychology, criminology, business) (67.4%). Participants ranged in age from 18 to 26 years old, with a mean age of 21.40 years (SD = 1.94). The demographic characteristics are summarized in Table 1.

TABLE I. Demographics (N=43)

		n	%
Ethnicity	Asian	4	9.3%
	Black	5	11.7%
	Mixed	14	32.5%
	Other	1	2.3%
	White	19	44.3%
Gender	Male	12	27.9%
	Female	30	69.8%
	Non-binary	1	2.3%
Age	18-20	16	37.2%
	21-22	16	37.2%
	23-26	11	25.6%
Course	Hard science	14	32.6%
	Arts/Social science	29	67.4%

Participants provided informed consent upon reading the Participant Information Sheet. Following completion, each participant was contacted by a member of the research team, who verified their enrolment in a non -information technology course at the University of Surrey and detailed the procedures necessary to complete the study. Eligible participants then proceeded to independently create their own Open University OpenLearn account, which provides students with free access to a range of online courses as well as records of their learning achievements. They subsequently enrolled in the course to complete GICAST (www.open.edu/openlearn/science-maths-technology/gamified-intelligent-cyber-aptitude-and-skills-training-gicast).

Participants were required to complete the game and quiz from each of GICAST's eight units, then email their certificate to a member of the research team. Participants were allowed to take as long as needed to complete the training, enabling them to fit it around their full-time studies. Successful completion enabled participants to proceed to the online post-training survey and feedback form, consisting of the questionnaires as well as four qualitative questions with free-text answer boxes. Once feedback was provided, a member of the research team emailed the participant an Amazon voucher and thanked them for their participation and time.

C. Design and Procedure

A pre-post experimental design was employed. For quantitative outputs, we conducted an *a-priori* power analysis for a conventionally medium effect size ($d = 0.5$, $\alpha = 0.05$, $1-\beta = 0.80$) which suggested a minimum of 34 participants to test our hypothesis. Based on the obtained sample size, the data set is suitable to detect an effect of $d = 0.44$.

For qualitative outputs, we employed a conventional, conceptual content analysis approach, wherein text is examined closely to determine the presence and frequency of themes. In this approach, researchers are immersed in the data and allow insights and code names to emerge organically, rather than relying on predetermined classifications [29]. Conceptual content analysis is a qualitative research method that aims to interpret textual data by identifying and categorising recurring themes or concepts. In the context of assessing the effectiveness of GICAST, this approach was

applied to the open-ended questions (e.g., 'What would you change about the training for the future?') in the survey, which aimed to elicit participants' experiences and perception of the training session. In contrast to word-based content analysis wherein word frequency is counted, conceptual approaches necessitate a more holistic understanding of the data. In this analysis, the themes of interest included the usability of the training session, content relevance, perceived educational efficacy, engagement, and enjoyment. Each code represented a specific concept or idea within the data. The codes were subsequently refined and grouped into broader themes, consolidating related concepts to form coherent categories that captured the underlying content and sentiment expressed in the responses [30]. Manual coding was conducted initially, followed by further analysis in NVivo [31], a qualitative analysis software tool. Using NVivo, a more systematic coding approach was conducted of the responses by assigning descriptive codes to segments of text related to the identified themes. Additionally, NVivo facilitated the creation of frequency tables to quantify the occurrence of specific themes, providing a complementary quantitative perspective to the qualitative analysis. Moreover, sentiment analysis was conducted using NVivo to evaluate the overall sentiment conveyed in the responses.

An ethical review was provided by University of Surrey Ethics and Governance Committee (FHMS 21-22 270 EGA) prior to the commencement of the experiments in this study. Participation was incentivized by offering Amazon vouchers for completion of the study.

D. Measures

Human Aspects of Information Security Questionnaire: Information security awareness was assessed using the Human Aspects of Information Security Questionnaire (HAIS-Q). The HAIS-Q [28] consists of 63 items that are answered on a five-point Likert scale (ranging from strongly agree to strongly disagree) and assesses seven broad areas of information security awareness: password use, email use, internet use, social networking site use, mobile computing, information handling, and incident handling. Each of these seven broad areas is divided into three more specific areas of focus (for example, 'password use' is broken down into 'locking workstations,' 'password sharing,' and 'choosing a good password'), resulting in 21 sub-areas. Each sub-area is assessed in terms of knowledge (e.g., 'It's acceptable to use my social media passwords on my work accounts'), attitudes (e.g., 'It's safe to use the same password for my social media and work accounts'), and behaviour (e.g., 'I use a different password for my social media and work accounts'). The HAIS-Q has been validated as internally consistent and a reliable measure of information security awareness, with Cronbach's alpha scores ranging from .75 to .82 [32; 28].

Fear of Missing Out Scale: Fear of missing out (FOMO) was measured using the FoMOs [24]. The FoMOs is a unidimensional, 10-item scale answered using a five-point Likert scale (ranging from 'not at all true of me' to 'extremely true of me'), with participants being requested to answer according to their true feelings, rather than what they believe their feelings should be. Items reflect the anxieties and fears that individuals may experience in relation to their social life and friendships (e.g., 'I get worried when I find out my friends are having fun without me' and 'Sometimes, I wonder if I spend too much time keeping up with what is going on'). Evidence suggest the FoMOs is a reliable measure of FOMO, with sensitivity across the spectrum of intensity (I.e., from low-level to high-level FOMO presentations) and shows high consistency (a = 0.87 [24]).

IV. Results

A. Quantitative Analysis

All pre-training HAIS-Q scores were in the range judged 'reasonable' by Parsons et al. [28] and were in line with those of a general non-technical workforce. FoMO scores were reasonably typical of a young population and were in line with those seen elsewhere in young people [24]. After training, all HAIS-Q mean scores moved to what Parsons et al. [28] describe as in the 'very high' range: indeed, post-training scores were more comparable to information-security-trained employees of a highly secure workplace [33]. All skewness and kurtosis z-scores were within acceptable limits for parametric analysis for a small (n <50) sample [34] and are given in Table 2. Table 3 shows the results of dependent t-tests for all measures. To account for multiple comparisons, Bonferroni correction was performed so as to use a stricter criterion for significance (p = 0.05/5 = 0.01). For all comparisons, post-training scores were significantly higher than pre-training scores, with large effect sizes for all HAIS-Q measures.

TABLE II. Measures before and after training (n=43)

			Skewness		Kurtosis	
	Mean	SD	Skewness	SE	Kurtosis	SE
Pre-training Knowledge	74.93	13.98	0.44	0.36	-1.17	0.71
Post-training Knowledge	92.91	9.78	-0.56	0.36	-1.05	0.71
Pre-training Attitude	75.30	15.61	0.49	0.36	-1.28	0.71
Post-training Attitude	91.70	11.11	-0.71	0.36	-0.59	0.71
Pre-training Behaviour	74.05	9.45	0.49	0.36	-0.47	0.71
Post-training Behaviour	86.33	11.86	-0.33	0.36	-0.79	0.71
Pre-training HAIS-Q	224.28	36.71	0.53	0.36	-1.12	0.71
Post-training HAIS-Q	270.93	29.24	-0.54	0.36	-0.64	0.71
Pre-training FoMO	3.03	0.68	-1.05	0.36	0.57	0.71
Post-training FoMO	2.76	0.74	-0.50	0.36	-0.11	0.71

TABLE III. Differences after training

	Difference Score	*t*(42)	Cohen's d
Knowledge	17.98	9.85**	1.50
Attitude	16.40	8.08**	1.23
Behaviour	12.28	6.59**	1.00
HAIS-Q Total	46.65	9.40**	1.43
FOMO	0.27	3.17**	0.48

** p<.001

In line with the hypothesized relationship, there was a strong negative correlation between baseline FoMO scores and pre-training total HAIS-Q scores ($r(41) = -.52$, $p < .001$) such that those with greater fear of missing out had poorer cyber security awareness. At the end of training, FoMO scores had reduced significantly with a medium effect size (see table 3). Interestingly baseline FoMO scores were not significantly correlated with post-training total HAIS-Q scores ($r(41) = -$

.21, $p = .183$) suggesting that the pre-training relationship had perhaps been at least partially mitigated by the training. FoMO scores after training had a moderate negative correlation with post-training HAIS-Q scores suggesting a complex pattern of change to and influence of FoMO. Finally, baseline FoMO scores were positively related to change in total HAIS-Q scores in the course of training ($r(41) = .40$, $p = .008$).

B. Content Analysis

The qualitative responses to the post-training survey were subjected to conceptual content analysis. Through this analysis, twenty codes were generated and subsequently categorised into five distinct themes. The comprehensive compilation of these codes and themes can be found in Table 4. Codes and themes span a range of dimensions of the cybersecurity training experience, including practical aspects (e.g., usability and user experience), educational aspects (including the efficacy, relevance, and content accuracy of GICAST), and emotional aspects (for example how enjoyable, novel, and rewarding the training felt). NVivo [31] software was employed, to gauge the frequency of quotes conveying a strong sentiment across all survey questions, as well as to determine whether the sentiment expressed was positive or negative. Notably, 74.5% of the quotes analysed, expressed a positive sentiment. The most prominently discussed positive theme revolved around the perceived educational efficacy of GICAST, which was referenced in 49.7% quotes, with 91.4% of those expressing favourable sentiments. Further positive sentiment was also contributed in quotes highlighting the participants' enjoyment of the tool. Conversely, 25.5% of the quotes expressed a negative sentiment, which was largely derived from quotes pertaining to engagement which accounted for 14.1% quotes, of which 61.9% were negative. Additional negative sentiment was contributed by quotes related to the usability of GICAST. Further details of the sentiment analysis outcomes can be found in Table 5.

TABLE V. Quotes in relation to Themes and their Sentiment

	Negative Sentiment Quotes		Positive Sentiment Quotes	
Theme	*n*	%	*n*	%
Usability of GICAST	12	70.6	5	29.4
Content Relevance	5	100	0	0
Perceived educational efficacy	7	8.6	74	91.4
Engagement	13	61.9	8	38.1
Enjoyment	1	4.0	24	96.0
Total	38	25.5	111	74.5

Note – only strong sentiments are included

TABLE IV. Codes & Themes

Theme	**Codes**	**Example Quote**
Usability of GICAST	Strong visuals or UX	*I did like the presentation of their work*
	Finicky marking	*...one of the questions in a quiz was asking for "junk mails" and I put "junk emails" and it didn't count*
	Slow and frustrating UX	*I found the games a little slow and difficult to move through*
Content relevance	Cybersecurity-irrelevant content	*The interactive elements often did not directly relate to the content (e.g. just clicking on a blender etc)*
	Extraneous for non-tech population	*A lot of the content isn't really useful for the average person*
	Incorrect content	*The quizzes sometimes weren't user friendly and a couple of them were wrong*
Perceived educational efficacy	Effective way of learning	*I enjoyed some of the quizzes and found them to be an effective learning tool*
	Simple and clear	*…everything was clear and well explained*
	Detailed and informative	*I enjoyed that it contained detailed information about social media cyber attacks*
	Improved knowledge	*It did help improve my awareness of how likely certain risks were to occur...*
	Hard to understand	*It contained a lot of technical terms, some which were difficult to understand*
Engagement	Engaging content	*I can see how it's meant to keep you engaged vs just watching a video*
	Rewarding	*I like that you get a badge at the end of the course*
	Interactive	*I really enjoyed the games in the training as it has a visual and interactive way to learn the information*
	Tedious and longwinded	*I don't know if many students would take the course without incentive, as it is a bit long and slow*
Enjoyment	Variety	*I enjoyed... the variety (with some being multiple choice, drag and drop, etc.)*
	Novelty	*..the games were novel as well*
	Enjoyable	*I enjoyed playing the games*
	Better than traditional learning	*It didn't just involve reading lots of text*

The findings obtained from the survey conducted among the participants strongly support the effectiveness of the proposed gamified training session as a valuable technique for learning. The majority of the participants expressed a high level of satisfaction with the training session, highlighting its significant benefits in terms of knowledge enhancement. Despite encountering certain technical difficulties, such as delayed tool interactions, the participants described their experience as enjoyable and engaging.

V. Discussion

The main study finding suggested that the GICAST training is widely acceptable to an undergraduate student population, and indeed produces strong gains in cybersecurity awareness. This is in keeping with earlier results using this training [2] and align with previous research on gamification in cyber education, lending further support to the positive impact of incorporating gamified elements into training sessions [22,23]. Overall, across the sample, the post-training levels of knowledge, attitudes and behaviour may be seen to be broadly equivalent to levels seen in information-security trained employees in the workplace. In the context of ensuring the preparedness and employability of future graduates, training of this nature could play a central role in respect of cybersecurity awareness. The sample size is admittedly too small to generalize from, and future work at scale should ensure that a wide variety of academic disciplines and diversity of students in respect of gender, socio-demographics, neurodiversity, and ability should be studied in more detail. Nevertheless, the present study recruited students from a wide variety of arts, social science and hard science backgrounds and did not find evidence of strong negatives for any.

The findings in respect of Fear of Missing Out are necessarily preliminary but suggest that greater FoMO characterizes those with lower awareness prior to training (as seen previously [27]), as well as characterising those that benefit correspondingly more from training. A by-product of training may be that it reduces FoMO itself as a reduction was seen in this variable. However, a much larger sample size is required to explore relationships and change over time in this area. Future research should explore FoMO and other online variables such as internet ‘addiction’ in relation to the effects of training.

The qualitative feedback received was highly encouraging with a strong majority of positive sentiments across a wide range of aspects of training. Echoing the positive sentiments of the current study, Armstrong and Landers [35] documented the engagement, motivation, and information retention among learners that gamification can engender. Furthermore, Thompson et al. [36] argue that traditional methods for teaching cyber security concepts often fall short in terms of effectiveness, highlighting the potential of gamification as a more engaging and impactful pedagogical approach. Negative sentiments largely related to perceptions about the relevance of content as not all participants saw all the content as relevant to them. The course could be slightly modified to allow some customisation of content without, however, reducing its depth and breadth too significantly for students. It should be noted that keyword frequency does not necessarily indicate genuine participant opinion, and as such is a limited indicator. Further research should use more in-depth qualitative methodologies to investigate the perceptions and impact of gamified training.

VI. Conclusions

Overall, the overwhelmingly positive sentiment towards the proposed gamified training session highlights its potential as a valuable learning tool that can be employed more broadly. The alignment of our findings with existing literature further supports the notion that incorporating gamified elements into educational interventions can yield substantial benefits for learners in the field of cyber education.

Acknowledgment

We would like to thank Dr. Chitra Balakrishna and her colleagues at the Open University for their assistance in respect of GICAST.

References

[1] Cabinet Office. National Cyber Strategy 2022. London: HM Government, Web, <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1053023/national-cyber-strategy-amend.pdf>, Version April 2023

[2] Balakrishna, Chitra, and Patricia Charlton. "Using Game-Based Learning Methods to Demystify Cyber Security Concepts for Adult Learners", In Proceedings of the 16th European Conference on Games Based Learning (Costa, Conceição ed.), 16(1), pp 73–80, 2022

[3] Li, Yuchong, and Qinghui Liu. "A Comprehensive Review Study of Cyber-Attacks and Cyber Security; Emerging Trends and Recent Developments." Energy Reports 7 (2021), pp 8176-8186, 2021.

[4] Aslan, Ömer. "A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions." MDPI Journal of Electronics 12.6 (2023): 1333, 2023

[5] National Cyber Security Centre. "About the NCSC: What we do."2023. Web, <https://www.ncsc.gov.uk/section/about-ncsc/what-we-do>, Version April 2023

[6] IBM. IBM Security Services 2014: Cyber Security Intelligence Index. Somers, NY: IBM Corporation, 2014. Web. Apr 5, 2023.

[7] Zatterin, Gabriele. “Cyber Security Skills in the UK Labour Market”, Ipsos Public Affairs, 2022. Web, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1072767/Cyber_security_skills_in_the_UK_labour_market_2022_-_findings_report.pdf, Version 2022

[8] Adams, Mackenzie, and Maged Makramalla. "Cybersecurity Skills Training: An Attacker-Centric Gamified Approach." Technology Innovation Management Review 5.1 (2022): 5-14, 2022.

[9] National Cyber Security Centre. The Cyber Threat to Universities., 2019. Web < https://www.ncsc.gov.uk/report/the-cyber-threat-to-universities >., Accessed 2023

[10] Švábenský, Valdemar, Jan Vykopal, and Pavel Čeleda. "What are Cybersecurity Education Papers about?". A Systematic Literature Review of SIGCSE and ITiCSE Conferences. In Proceedings of the 51st ACM Technical Symposium on Computer Science Education (SIGCSE '20). Association for Computing Machinery, New York, NY, USA, pp 2–8, 2020.

[11] Githens, Rod P. "Understanding Interpersonal Interaction in an Online Professional Development Course." Human Resource Development Quarterly 18.2 (2007), pp 253-74, 2007.

[12] Abu-Amara, Fadi. "A Novel SETA-Based Gamification Framework to Raise Cybersecurity Awareness." International Journal of Information Technology 13 (2021): 1-10, 2023.

[13] Thompson, Michael, and Cynthia Irvine. "Active Learning with the CyberCIEGE Video Game." (2011) In Proceedings of the 4th conference on Cyber security experimentation and test (CSET'11), USENIX Association, USA, pp. 10, 2011

[14] Hendrix, Maurice, Ali Al-Sherbaz, and Victoria Bloom. "Game Based Cyber Security Training: Are Serious Games Suitable for Cyber Security Training?" International Journal of Serious Games 3.1 (2016), 2016

[15] Johnson, David W., Roger T. Johnson, and Karl A. Smith. "Cooperative Learning: Improving University Instruction by Basing Practice on Validated Theory." Journal on excellence in college teaching 25.3-4 (2014): 85. ERIC.

[16] Gee, James Paul. "What Video Games have to Teach Us about Learning and Literacy." Computers in Entertainment 1.1 (2003), 2023

[17] Coenraad, Merijke. "Experiencing Cybersecurity One Game at a Time: A Systematic Review of Cybersecurity Digital Games." Simulation & gaming 51.5 (2020): 586-611, 2020

[18] van Steen, Tommy, and Julia R. A. Deeleman. "Successful Gamification of Cybersecurity Training." Cyberpsychology, behavior and social networking 24.9 (2021): 593-8, 2021.

[19] Naval Postgraduate School. "CyberCIEGE." nps.edu. March 2017. Web. <https://nps.edu/web/c3o/cyberciege>, Version Apr 5, 2023

[20] The Open University. "Gamified Intelligent Cyber Aptitude and Skills Training (GICAST)." www.open.edu/openlearn. October 2020. Version Apr 5, 2023.

[21] Vail, J. "Gamification of an Information Security Management Course".Montreal, Quebec, Canada: Association for the Advancement of Computing in Education (AACE) , 2015. 1720-1731, 2015.

[22] Clark, Douglas B., Emily E. Tanner-Smith, and Stephen S. Killingsworth. "Digital Games, Design, and Learning: A Systematic Review and Meta-Analysis." Review of educational research 86.1 (2016): 79-122. ERIC, 2011

[23] Sitzmann, Traci. "A Meta-Analytic Examination of the Instructional Effectiveness of Computer-Based Simulation Games." Personnel psychology 64.2 (2011): 489-528, 2011

[24] Przybylski, Andrew K. "Motivational, Emotional, and Behavioral Correlates of Fear of Missing Out." Computers in Human Behavior 29.4 (2013): 1841-8, 2012

[25] Popovac, Maša, and Lee Hadlington. "Exploring the Role of Egocentrism and Fear of Missing Out on Online Risk Behaviours among Adolescents in South Africa." International Journal of Adolescence and Youth 25.1 (2020): 276-91, 2020

[26] Alt, Dorit, and Meyran Boniel-Nissim. "Parent–Adolescent Communication and Problematic Internet use: The Mediating Role of Fear of Missing Out (FoMO)." Journal of family issues 39.13 (2018): 3391-409, 2018

[27] Hadlington, Lee, Jens Binder, and Natalia Stanulewicz. "Fear of Missing Out Predicts Employee Information Security Awareness Above Personality Traits, Age, and Gender." Cyberpsychology, behavior and social networking 23.7 (2020): 459-64. PubMed, 2020.

[28] Parsons, Kathryn. "A Study of Information Security Awareness in Australian Government Organisations." Information management & computer security 22.4 (2014): 334-45, 2014.

[29] Hsieh, Hsiu-Fang, and Sarah E. Shannon. "Three Approaches to Qualitative Content Analysis." Qualitative health research 15.9 (2005): 1277-88. MEDLINE, 2005.

[30] Kulatunga, Udayangani, Dilanthi Amaratunga, and Richard Haigh. "Structuring the Unstructured Data: The use of Content Analysis", Mar 2007, 2007.

[31] Lumivero (2018) NVivo (Version 12), www.lumivero.com

[32] Parsons, Kathryn. “The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies.” Computer Security 66 (2017): 40-51, 2017.

[33] Pattinson, Malcolm Robert. “The Information Security Awareness of Bank Employees.” International Symposium on Human Aspects of Information Security and Assurance (2016), 2016.

[34] Kim, Hae-Young. "Statistical Notes for Clinical Researchers: Assessing Normal Distribution (2) using Skewness and Kurtosis." Restorative Dentistry & Endodontics 38.1 (2013): 52-4. PubMed, 2013.

[35] Armstrong, Michael and Landers, Richard (2018), “An evaluation of gamified training: using narrative to improve reactions and learning”, Simulation & Gaming, 48-4: 513–38, 2018

[36] Thompson, Lilly, Nicholas Melendez, Justin Hempson-Jones, and Francesca Salvi (2022) "Gamification in cybersecurity education: The rad-sim framework for effective learning", *European Conference on Games Based Learning*, vol. 16, no. 1, pp. 562-569., 2022