Computer Games as a Pedagogical Tool for Creating Cyber Security Awareness

Per Godejord and Beata Godejord
Nord University Business School, Norway

per.a.godejord@nord.no
beata.j.godejord@nord.no

Abstract: Cyberattacks are increasing world-wide, both on corporate networks and public institutions network. During 2022 hackers were widening their aim to target business collaboration tools such as Slack, Teams, OneDrive, and Google Drive with phishing exploits, making for a rich harvest of sensitive data given that most organizations' employees continued to work remotely. In the later years we have also seen academic institutions becoming more frequent targets for both cybercriminals and state sponsored hackers. In 2022 the education/research sector was most attacked industry globally, seeing a 43% increase compared to 2021, with an average of 2,314 attacks per organisation every week. Schools and universities have the unique challenge of dealing with children or young adults, many of which use their own devices, work from shared locations, and often connect to public Wi-Fi without thinking of the security concerns. Additionally, Russia's war on Ukraine has led to an increase in spear-phishing activity targeting educational institutions in NATO countries. This situation calls attention to the need for awareness raising about personal cyber security. In Norway, Nord University is one of a few universities with specific focus on security and preparedness, including cyber security awareness. The university has two information security courses: one belonging to furthering education and one within the MBA-study program in Security and Preparedness Management. This paper examines the question whether serious games and online quizzes can create heighten cyber security awareness and motivate individual students to change their cyber security behaviour. The paper reports on the findings based on written reflection notes from students belonging to both courses. The technique of examination and interpretation applied to the data was qualitative thematic content analysis supported by computer-assisted qualitative data analysis software NVivo. Theoretical analysis was guided by social constructionist perspective on knowledge creation. While many advantages of the use of online quizzes and computer games were specified by students, challenges were identified as well. However, the findings show that the use of serious games and online quizzes can be an efficient approach to raising security awareness among participating students.

Key words: Information security, Cyber-attacks, Awareness raising, Serious games, online quizzes

1. Introduction

Core issues in the research on cognitive effects of video games were identified as early as in the mid-eighties when the early attempts were made to introduce theoretical rigor to understand the relation between playing video games and the development of thought. The result of this early investigation was the discovery that complex cognitive skills are required to play video games with success. Furthermore, a cognitive by-product of gaming was identified and defined as a new type of literacy for the technological age (Greenfield, 1984). Since then, it has been convincingly argued that games promote student motivation and engagement (Gee, 2007; Greenfield, 2010) as well as provide good arena to teach twenty-first century skills (Squire, 2006). In the big picture, digital games are environments for studying key processes involved in learning and gaining insight into how learning occurs (Gee, 2003; Gee, 2004; Gee 2005; Gee, 2007).

In the recent years computer games have also emerged as an increasingly powerful tool for pedagogy in cyber security education, providing better understanding and retention of cyber security concepts. Research has shown that computer games can enhance students' knowledge, skills, and attitudes towards cyber security by simulating real-world cyber-attacks and providing a safe environment to experiment with concepts without causing harm to actual systems (Alotaibi et al., 2016; Coenraad et al., 2020).

As cyberattacks are increasing world-wide, both on corporate networks and public institutions network, the importance of training students in information security has never been higher. This paper examines the question whether serious games and *online quizzes* may have an impact on creating a heighten cyber security awareness and motivate individual students to change their cyber security behaviour.

2. Background

2.1 The Cyber Security Courses at Nord University

At Nord University there are two cyber security courses: "ICT1013-Basic information security" belonging to a furthering education study program in ICT and Learning, and "ORG5005-Digital preparedness" belonging to the MBA-study program in Security and Preparedness Management.

The course "ICT1013-Basic Information Security" serves as an introductory course that covers fundamental terms and subject areas related to information security. The objective of this course is to enhance students' awareness regarding their responsibility for digital preparedness, both as private individuals and employees. The academic content of the course encompasses an elementary comprehension of computers, diverse cloud services, and the significance of digital preparedness. The course "ORG5005-Digital Preparedness" provides an in-depth understanding of current digital threats and vulnerabilities, along with relevant protective measures for daily preparedness and incidents within the upper crisis spectrum. The course aims to trigger reflective thinking in students to improve their emergency management skills and overall security consciousness as citizens of a predominantly digital society, rather than providing training to combat hackers, whether they are criminal or state actors. The intention is for students to comprehend that their own attitudes and digital preparedness play a crucial role in enhancing the overall preparedness of their employers and the nation. Additionally, students should be capable of conducting awareness-raising activities in their organizations and participating in preparedness exercises that encompass the loss of digital infrastructure.

Both courses use a set of computer games and online quizzes to enhance the students understanding of cyber security threats. The games were presented to the students in the form of an obligatory task where the students both had to play the games as well as analysing them based on relevant academic papers. The students were also asked to describe weather or not playing these games had any effect on their own cyber security awareness.

2.2 The Computer Games and Online Quizzes Used

“Can you spot when you’re being phished?” Is a quiz created by Google's Jigsaw team with the aim of educating individuals on how to identify phishing attempts. The quiz presents elaborate phishing messages visually and prompts users to ascertain if they are being phished. It enables users to enhance their skills by practicing the technique of hovering the mouse over links to display the actual web address. Furthermore, users can scrutinize email headers and attachments, as displayed in the screenshot below, to authenticate the credibility of the message.

The Norwegian National Communications Authority has developed a cyber security assessment tool titled "How Exposed Are You to Identity Theft?" This platform allows individuals to assess their adeptness in protecting personal data and evaluate their competence level in safeguarding against identity theft by undertaking a self-evaluation test.

"The Weakest Link: A User Security Game" was created in response to the findings of IS Decisions' research, which indicated that 48% of IT professionals consider training as a crucial factor in enhancing user security awareness. Furthermore, 38% of the professionals desired more innovative training materials and content. The game employs a question-and-answer format that is reminiscent of a "choose your own adventure" style. Its objective is to navigate through the first month of working for a fictitious employer without making too many security mistakes. Each working day presents a distinct scenario, and players are provided with response options. Points are awarded for selecting secure options and deducted for selecting non-secure options. The aim of the game is to complete the month without incurring a significant loss of points.

“The Cyber Awareness Challenge” was developed by the US Department of Defence (DoD) and aims to influence behaviour by emphasizing actions that authorized users can take to mitigate vulnerabilities and threats to DoD Information Systems. This training is both up-to-date and engaging, with a user-centric approach. The Cyber Awareness Challenge serves as the standard end-user awareness training for the DoD, providing awareness content that addresses emerging requirements from Congress, the Office of Management and Budget (OMB), the Office of the Secretary of Defence, and the DoD CIO chaired Cyber Workforce Advisory Group (CWAG). The course furnishes an overview of current cybersecurity threats and best practices to safeguard information and information systems, both at home and in the workplace. Furthermore, it reinforces best practices to protect classified information, controlled unclassified information (CUI), and personally identifiable information (PII).

3. Research design

The objective of the undertaken research was to explore students’ perceptions of their own cyber security awareness and whether playing the games/quizzes would lead them to change their cyber security behaviour. The assumption was that the undertaken investigation may provide some insight regarding possible advantages and disadvantages of using serious games and online quizzes as part of cyber security education.

3.1 Participants

Participants in the study were forty-three students in the online course "ICT1013-Basic information security" and forty-nine students in the online course "ORG5005-Digital preparedness" in the academic year 2022/23. Students in the course "ICT1013-Basic information security" are predominantly professionally trained and active teachers while students in the course "ORG5005-Digital preparedness" are professionally trained and active officers and non-commissioned officers of the Norwegian Armed Forces, police officers and managers from various public and private organizations with management responsibilities for national or local preparedness.

3.2 Data Collection

The data were collected from students' reflection documents. Writing reflection documents is a part of each assignment in both online courses. Reflection documents are metacognitive components in students work which require introspection and self-analysis and, in assumption, lead to self-regulated learning with a high level of students' agency. The presented analysis focused on the parts of documents where students were reflecting on the strengths and weaknesses of serious games and online quizzes as tools for creating cyber security awareness, and changes in their own cyber security behaviour.

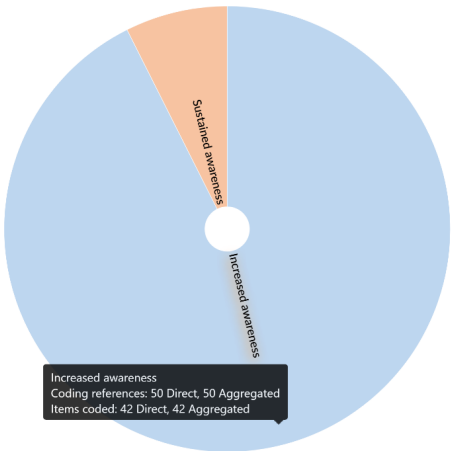
3.3 Data Analysis

The analytic method applied to the data was thematic analysis (TA). Thematic analysis is a qualitative research method aiming at exploring and identifying repeated patterns of meaning (themes) across a dataset. It is a theoretically flexible method used to address research questions related to people's experiences, views, and perceptions (Braun and Clarke, 2006). Conducted analysis was approached from the perspective of constructivist grounded theory and based on the assumption that "we know the empirical world through language and the actions we take toward it" (Charmaz, 2012).

Data analysis was conducted inductively, i.e., without using preconceived codes and categories. Assumptions were data driven. It was crucial to understand participants' views and their own perspectives and therefore follow grounded theory mandate. Data analysis was assisted by qualitative data analysis software (CAQDAS) NVivo.

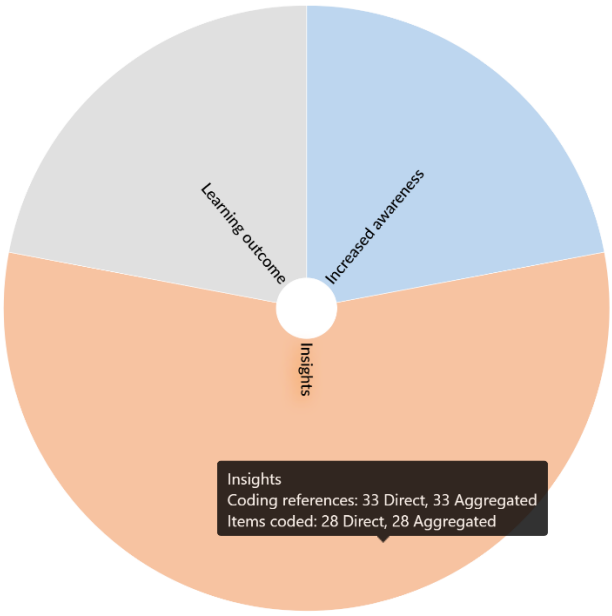
4. Results

The analysis of data revealed noticeable differences in the perceptions of the game and online quizzes related experience between the two groups of students. In the course "ICT1013-Basic information security", 98% of students (42 out of 43) explicitly pointed to increase in their cyber security awareness after playing the games and online quizzes required by the assignment (Fig. 1). Game experience, through the element of participation in the cyber security related situations, made them realize not only the gaps in their cyber security knowledge but also how important cyber security measures are and how broad the spectrum of cybercrime can be. The areas of cybercrime specifically reported by students as them being less vulnerable to after playing the games and online quizzes were fraud and theft identity.



Name	Files	References
Sustained awareness	4	4
Increased awareness	42	50

Figure 1: Themes that emerged in the reflections form students in the course "ict1013-basic information security". Source: CAQDAS



Name	Files	References
Learning outcome	11	13
Insights	28	33
Increased awareness	12	13

Figure 2: Themes that emerged in the reflections form students in the course "org5005-digital preparedness". Source: CAQDAS

Worth noticing is also the reflection that the game and online quizzes assignment helped students to develop better understanding and acceptance of cyber security rules at their workplaces. Before playing the games, they tended to prioritize focus on individual security over the focus on the cyber security at their organizations.

Conversely, in the course "ORG5005-Digital preparedness" only 24 % of students (12 out of 49) reported increased cyber security awareness after the game and online quizzes assignment. Interestingly, students' reflections in this group were more focused on games and online quizzes as educational settings, with 57% of students (28 out of 49) stating that games and online quizzes can be effective tools for raising cyber security awareness (Fig. 2). Worth noticing are the reflections pointing specifically to what type of games and online quizzes would best serve this purpose; they need to be realistic with themes and scenarios tailored to the individual organization, and preferably using Norwegian language. The participants highlighted the importance that the game and online quizzes scenarios focus on cyber threats and situations that feel relevant to the organizational needs. Perceptions concerning educational potential in computer games and online quizzes were labelled as "Insights" based on the words and phrases students used to express them: "I saw advantage …", "I realized games potential as learning arenas", "I acquired deeper understanding of how games, as a practical activity, can be supportive to learning theory". Furthermore, in the course "ORG5005-Digital preparedness" 22 % of students (11 out of 49) pointed to increase in their learning as an outcome of playing games and online quizzes. We may naturally assume that increase in learning also took place in case of 98 % of students in the course "ICT1013-Basic information security", which would be in an evident correlation with the increased awareness reported by students in this group. What is however interesting, students that are teachers by profession were more preoccupied with gaps in their knowledge, i.e., what they were not aware of than the knowledge acquired.

5. Discussion and Conclusions

In this paper we have explored the reflections of students participating in two cyber security courses at Nord University, Norway. While the students in the course "ICT1013 - Basic Information Security" specifically pointed to an increase in their cyber security awareness after playing the games, the students in the course "ORG5005 - Digital Preparedness" were focusing more on games and online quizzes as an educational platform for achieving goals such as raising digital security awareness. A possible explanation for this discrepancy is that

students in the course “ICT1013 – Basic Information Security” have a course “Digital Game Based Learning” in the same study program, and hence may already have a higher awareness of educational potential in computer games and online quizzes. For this reason, their attention was primarily directed to the content of the games and online quizzes and not the games as learning platforms. Also, students in the course “ORG5005 - Digital Preparedness” had evidently a higher cyber security awareness before they started working with the assignment compared with the students in the course “ICT1013 – Basic Information Security”. For this, when required to reflect on the impact of games and online quizzes on learning, their dominant observation was that games can actually be efficient learning environments. The important conclusion for us is that both groups of students find the use of computer games and online quizzes valuable in cyber security training, and their reflections give ample grounds for further work in this field. One of the focal points in our work will be to select computer games and online quizzes that are more tailored to the specific needs of two students' groups. For the students in “ORG5005” we may investigate games and online quizzes which focus more on technical security measures, while the students in “ICT1013” may benefit from games and online quizzes with a clearer focus on the importance of human factors in cyber security, such as risky user behaviours and lack of motivation to follow internal security rules. To gain deeper insights it will be also important to examine students’ reflections in several cycles of coding. This could inspire further ideas for improvements and following actions in the area of security, which remains a critical issue for both individuals and organizations.

Interpretative research, as the one presented in this paper, is prone to biases as the involved researchers can be, and usually are, a participating element of the research process and research results. There may be as many ways of ‘seeing’ the data as one can invent (Dei, 1993). This brings about the issue of the verifiability of qualitative data analysis. The results of the presented study are meaningful from the perspective of the purpose statement, however, not generalizable beyond the data sets.

6. References

Alotaibi, F., Furnell, S., Stengel, I. and Papadaki, M. (2016) “A Review of Using Gaming Technology for Cyber-Security Awareness”, *International Journal for Information Security Research*. Vol 6, Issue 2, pp. 660-666.

Braun, V. and Clarke, V. (2006) “Using thematic analysis in psychology”, *Qualitative Research in Psychology,* Vol. 3, Issue 2, pp. 77 – 101.

Charmaz, K. (2012) *Constructing Grounded Theory: A Practical Guide Through Qualitative Analysis,* Sage Publications, London.

Coenraad, M., Pellicone, A. Ketelhut, D.J., Cukier, M., Plane, J. and Weintrop, D. (2020) “Experiencing Cybersecurity One Game at a Time: A Systematic Review of Cybersecurity Digital Games”, *Simulation & Gaming*, Vol. 51, Issue 5, pp. 586–611.

Dey I. (1993) *Qualitative data analysis: A user-friendly guide for social scientists*. Routledge Kegan Paul, London.

Gee, J. P. (2003) “What video games have to teach us about learning and literacy”, Computers in Entertainment (CIE), 1(1), 20.

Gee, J.P. (2004) *Language, learning, and gaming: A critique of traditional schooling*. New York: Routledge.

Gee, J.P. (2005) *Why video games are good for your soul: Pleasure and learning*. Melbourne, Australia: Common Ground.

Gee, J. P. (2007) “Learning and games” in K. Salen (ed.), *The ecology of games: Connecting youth games, and learning* (K. Salen ed.), pp. 21-40, Cambridge/MA: MIT Press.

Greenfield, P.M. (1984) *Mind and media: Effects of television, video games, and computers*. Cambridge/MA.

Greenfield, P.M. (2010) “Video games revisited” in R. van Eck (ed.), *Gaming and cognition: Theories and practice from the learning sciences*, pp. 1-21, Hershey/PA: IGI Global, Hershey, PA.

Mitchell, A., & Savill-Smith, C. (2004) “The use of computer and video games for learning: A review of the literature”, *Learning and skills development agency,* UK.

Rochelle, L., & Brudvik, J. (2017) “The Impact of Game-Based Learning on Cybersecurity Knowledge and Attitudes”, *Journal of Cybersecurity Education, Research and Practice*, 2(1), 1-7.

Squire, K. (2006) “From Content to Context: Video Games as Designed Experience,” *Educational Researcher*, 35, Issue 8, pp. 19-29.