Design of a Disinformation Awareness Digital Game

Clara Maathuis[1], Frederick Janssens[2] and Ebrahim Rahimi[1]
[1]Open University of the Netherlands, Heerlen, The Netherlands
[2]Independent Researcher, Belgium

clara.maathuis@ou.nl
frederick.janssens.BSc@gmail.com
ebrahim.rahimi@ou.nl

Abstract: Social media is the digital canvas where users' thoughts, ideas, and voices converge, and are being brought to the world. It is the environment where individuals and groups are connected and empowered in ways that were previously unimaginable. Nonetheless, the users are exposed and engage without knowledge or willingly to various social media manipulation mechanisms like disinformation and misinformation which have the potential to influence their believes, behaviour, and attitudes. Although social media represents a valuable arena for connectivity and expressivity to the younger generation, it also poses risks like access to sensitive information and exposure to altered or false narrative and misleading content which can shape young minds in ways that are detrimental to critical thinking and overall well-being. To combat these, it is crucial for families and teachers as well as the educational system to promote security awareness, digital literacy, and critical thinking to high school students. Since research and practitioner initiatives and programs are in an incipient phase to tackle such threats, this research aims to design a digital game for security awareness regarding broken authentication and social bots to high school students. To achieve this objective, a transdisciplinary approach is considered by merging methods from cyber security awareness, social media manipulation, software engineering, game-based learning, and computer science education domains using the Design Science Research methodology. This research strives to contribute to building responsible efforts that bring and/or strengthen awareness and resilience to social media security threats of adolescents to assure a safe digital domain.

Keywords: Disinformation, Misinformation, Cyber security awareness, Social media, Game-Based learning

1. Introduction

"We can only see a short distance ahead, but we can see plenty there that needs to be done." (Alan Turing)

The proliferation of cyber security incidents became a global pressing societal concern, especially within the social media realm. Primer cyber threats in this realm are targeting data and human behaviour and believes through information access and information manipulation operations (ENISA, 2023a). An increasing trend in this direction that escalates the complexity of the security landscape is represented by the persuasion of targeting authentication mechanisms that serve as the first line of defence against unauthorized access through broken authentication exploits and the deployment of social bots that represent automated software agents designed to mimic human interactions for producing/amplifying dis/misinformation among users (UNICEF, 2021; Fard & Maathuis, 2021; Kaur & Ramkumar, 2022; Pastor-Galindo, Marmol & Pérez, 2022). As these threats continue to evolve in sophistication and scale, there is an urgent need for building and adopting intelligent, adaptive, and robust cyber security programs and solutions that counter and further prevent them. Nevertheless, effectively countering and preventing such multifaceted challenges implies firstly awareness and education of users (Zwilling, 2022) concerning their action and impact (Caramancion et al., 2022) through public awareness campaigns, professional training courses, and tailored educational programs (ITU, 2018). Given their reliance on digital platforms for activities like education, communication, and entertainment as well as their implicit vulnerability, cyber security awareness is vital for adolescents since they are in a forming stage of development, and they lack the necessary experience, emotional and cognitive maturity to deal with social media threats (Lazer et al., 2018; Smith & Ali, 2019) like unauthorized access to sensitive information, and content manipulation. While dedicated efforts for building and implementing cyber security awareness solutions that facilitate digital safety and media literacy (IRIS Plus, 2022) are proposed by various academic, governmental, and private stakeholders, they are limited in relation to dedicated tailored solutions to adolescents/high school students. This represents the knowledge gap that this research tackles adopting a multidisciplinary approach by means of designing a digital game for raising cyber security awareness of high school students focusing on disinformation social bots and broken authentication threats.

To achieve the aim of this research, the Design Science Research methodology is used to build the design architecture of a cyber security awareness digital game (Hevner et al., 2004; Peffers et al., 2007; Ibrahim & Jaafar, 2009). Accordingly, this research aims to bring a contribution to ongoing academic and professional efforts for building cyber security awareness tailored to children, and in particular high school students, to

increase their resilience, responsibility, and media literacy skills in relation to evolving cyber threats that the social media domain embeds using gaming technologies as this approach previously showed valuable results and is considered enjoyable by high school students.

The outline of this article is structured as follows. Section 2 sets the background of this research and discusses relevant related studies. Section 3 discusses the methodological approach considered in this research. Section 4 presents the design of the game architecture that this research proposes. At the end, Section 4 provides concluding remarks and future research perspectives.

2. Background and Related Research

In its future vision on cyber threats, ENISA (2023b) stresses that both state and non-state actors are increasing their technological capabilities and that by 2023, they continue to expand their disinformation efforts using bots and deepfakes as part of influence operations and campaigns. Accordingly, ENISA (2021) calls for collaboration, cooperation, and coordination of governmental, professional, and scientific cyber security efforts on building tailored awareness strategies, programs, and solutions. In the Netherlands, cyber security awareness campaigns are carried out at national level through efforts that the Ministry of Security and Justice direct in respect to producing and enhancing awareness of civilians and municipalities by cooperating with police and private sector players like Google, Facebook, Microsoft, and telecommunication companies, while the Ministry of Economic is raising security awareness among companies and entrepreneurs. This reflects the importance of media literacy that social media users need to have to critically evaluate and use information before transforming it into knowledge. Hence, users, and in particular children and young people need to be aware of aspects like the source of information, the ways how the information received represents the world, and further what kind of implications these could have (Glas et al., 2023). Quayyum, Cruzes & Jaccheri (2021) conduct a systematic literature review on the importance of cyber security awareness among children in relation to existing risks and provide a series of awareness mechanisms that could be developed to allow them to avoid and/or mitigate them. The authors identify the following core risks: online privacy, online harassment, stranger danger, social engineering, content related, sexual solicitation, technology-based threats, economic, Internet addiction, and password practice and management. In the systematic literature review conducted by Zhang-Kennedy & Chiasson (2021) on cyber security awareness and education tools, the authors stress the need to develop gaming and media solutions for building and supporting awareness and education of people in a structured manner following clear design and evaluation principles. The study proposes the following research agenda: focus on impactful and current educational topics, consider interdisciplinarity, integrate a rigorous evaluation methodology without jeopardizing users' security and privacy (i.e., ecological validity), consider users' motivation and engagement, establish a consistent reporting template, and embed various cultural perspectives.

Shamsi (2019) investigates the effectiveness of cyber security awareness programs for students aged 8 to 10 years old based on interviews conducted with teachers and students. The results position the online safety, authentication, privacy, online strangers, and cyber bullying among the core issues that children deal with online. At the same time, while the results of the two parts are similar, the children emphasize cyber bullying more based on their own experiences. Nevertheless, as Bada, Sasse & Nurse (2019) stresses, cyber security awareness campaigns can fail due to (i) personal factors such as tiredness, perceived control, and self-regulation, and (ii) cultural and environmental factors like perception of risk, social disruption, and positive/negative perception of the outcomes.

Hart et al., (2020) propose Riskio, a tabletop serious game for increasing cyber security awareness of people without technical background working as employees in various organizations and students. In this game, the users play scenarios that cover a broad range of cyber attacks for whom they need to define proper countermeasures based on existing standards and learn in a fun and enjoyable environment that promotes players' active learning (i.e., constructivism learning theory). Yasin et al., (2018) develop a serious game for security requirements education of university students and young professionals focusing on understanding security concepts, analysing them in real life situations, and motivating players for further learning and remaining updated on future developments of security issues. This is done by presenting the cyber-attack mechanism which starts from identifying the target, searching, and finding a vulnerability to be exploited, and preparing the attack surface using a scenario-based learning approach. Literat, Chang & Hsu (2020) design for primary school students two serious games named Fakeopoly and Lying Geese based on the Monopoly and Buffalo games, respectively. While the first game focuses on production and sharing fake news, the second game focuses on the story of the fake news including the writer and reader roles and deciding the trustfulness

of the news story. Along these lines, Giannakas, Kambourakis & Gritzalis, (2015) develop a cyber security education and awareness game for K-6 (Kindergarten to sixth grade – elementary school) students aiming at providing understanding of general security concepts and attacks. Given the young age of the target audience, the study considers attention, relevance, confidence, and satisfaction are core design elements. With a broader target audience, Jin et al. (2018) build a cyber security training named GenCyber for K-12 (Kindergarten from 5-6 years old to twelfth grade – up to 17-18 years old) students for raising cyber security awareness and providing understanding to what safe online behaviour means and implies aiming at increasing diversity in the US cyber security workforce by focusing on social engineering, online behaviour security, and defence strategy.

Micallef et al. (2021) developed Fakey, an online fake news awareness game directed to a general online audience. The game is online available since November 2019, adopts a human-centred computing approach by including users' needs, goals, and expectations since the design phase. In the assessment process, the study included semi-structured interviews to evaluate the interaction and the achievement of learning objectives. A human-centred approach is also taken by Mikka-Muntuumo & Peters (2021) who propose an online game for engaging both high school students and their teachers, parents, and caregivers for producing and sustaining online safety awareness focusing on core threats like identity theft and cyber bullying. Considering a different implementation perspective, Paraschivoiu et al. (2021) propose an escape room AR game for fake news education of high school students and young adults that contains quizzes with multiple-choice questions, matching games, and minigames, a chatbot for narrative storytelling, and an exploration mode. The game focuses on the following four pillars for assuring a balance between challenge and skill: (i) learning that captures knowledge, skills, and attitude elements, (ii) storytelling which provides engagement with the narrative, (iii) gameplay which refers to the activities taken in the game (mechanics), (ii) dynamics, and (iii) and emotional responses (affection). Using web technologies, Olano et al. (2014) built a web-based game named Security Empire for high school students for building cyber security awareness skills in a setting of building a green energy company. The skills imply issues regarding unsafe links, encryption auction bids, authentication and software downloads, integrity checks of system software, antivirus protection up-to-date, and selection of strong passwords. Addressing university students, Wu et al. (2021) propose an information awareness security online game that focuses on general security awareness aspects like social media use, information handling, and password management. The study assesses the attitude and intention to comply with the game security principles and measures if gender differences can be seen in this process. Based on the results obtained, the authors did not see an increase in interest of students towards further engaging and approaching information security topics and did not see a difference in gender among engaging with the content among the participants.

In relation to social media trolls, Lees et al. (2023) built an online game named Spot the Troll Quiz addressed to a general audience tailored to generating and sustaining awareness to social media trolls. As a response to the infodemic phenomenon born and further developed in the Covid-19 pandemic, Cernicova-Buca & Ciurel (2022) proposed a paper-based game for university students for disinformation awareness during crisis such as the Covid-19 pandemic aiming at increasing fake news awareness skills and promoting media literacy. As a professional effort, Common Sense (2018) developed the Digital Passport which is a web-based educational game for digital awareness to primary school students in relation to issues like password protection and online sharing using a series of mini games. Focused on disinformation awareness, Urban, Hewitt & Moore (2018) developed a web-based game named Fake it to make it that helps identifying and simulating common fake news techniques, analysing potential disinformation, understanding how fake news are created and spread, and provide players ways to distinguish fake news from real news. A similar tool called Bad News is proposed by Barabas (2023) where the users can engage in building and spreading disinformation for reflecting on the implications of their actions, and further gaining insights in these mechanisms.

The studies above discussed are summarized in Table 1 for capturing their goals, direct target audience as well as educational, gaming, implementation, and evaluation methods. Based on this extensive literature review, one can see that limited attention is provided to building cyber security awareness gaming solutions to K-6 and K-12 students or primary and secondary school students in relation to social media threats like social bots and broken authentication. This represents the knowledge gap that this article aims to tackle through a gaming approach given its effectivity in previous awareness settings and appreciation by high school students.

Table 1: Core elements and methods of the related studies

Article no	Aim	Target audience	Educational method	Gaming method	Implementation method	Evaluation method	Reference
1	Cyber security awareness on attack and defence mechanisms	Non-technical employees of organizations (primary) and university students (secondary)	Constructivism learning theory (e.g., motivation, experimentation, responsibility, feedback)	Game design (e.g., planning, collaboration, game turns, tokens, scoring)	Multiplayer card game	Three experiments with 14, 15, and 12 players, respectively	(Hart et al., 2020)
2	Security requirements education	University students and professionals	Scenario based learning (planning, communication, problem solving) using the Bloom taxonomy	Game design (e.g., planning, rules, characters, scoring)	Multiplayer card game in English and Chinese languages	One experiment with 16 players	(Yasin et al., 2018)
3	Fake news awareness	Primary school students between 10-14 years old	Learning by participatory game design (reflection, discussion, and participation)	Participatory game design	Multiplayer board game	Two experiments both with three players on two different games	(Chang & Hsu, 2020)
4	Cyber security training	K-12 students	Scenario based learning	Participatory game design	Single-player game developed in Unity 3D	One experiment with 181 high school students	(Jin et al., 2018)
5	Fake news awareness	General audience	Scenario based learning	Game design	Single player game developed in Python, Javascript, and Django	Ongoing as it is online available since November 26, 2019	(Micallef et al., 2021))
6	Fake news	High school and young adults	Scenario based learning	Game design (learning, storytelling, gameplay, and user experience)	Single-player escape-room AR game developed in Unity 3D	An experiment with 49 high school and young adults	(Paraschivoiu et al., 2021)
7	Online safety awareness	High school students	Scenario based learning	Game design	Single-player online game	Two experiments: first where 29 high school students and teachers ranging between 7 to 35 years old, second with 18 teachers, parents, and caregivers.	(Mikka-Muntuumo & Peters, 2021)
8	Information security awareness	University students	Experimental learning	Gamification for learning (e.g. points, levels, and leaderboards)	Single-player online game	One experiment with 110 university students ranging between 18 to 21 years old	(Wu et al., 2021)

9	Cyber security education and awareness	K-6 students	Game-based learning and Instruction Design Model	Game design (e.g., challenge, points, mini games)	Single-player mobile game built using the Android Development Kit and libGDX game engine	One experiment with 43 elementary school students aged between 9 to 11 years old	(Giannakas, Kambourakis & Gritzalis, 2015)
10	Cyber security education	High school students	Game-based learning	Game design	Multi-player online game	One experiment with high school students	(Olano et al., 2014)
11	Troll detection awareness	General audience	Experimental learning	Game design	Single-player online game	Multiple experiments with 2847 players of various age	(Lees et al., 2023)
12	Disinformation awareness	University students	Game-based learning	Game design	Single-player paper and online game	One experiment with 50 university students	(Cernicova-Buca & Ciurel)
13	Digital security awareness	Primary school students	Game-based learning	Game design	Single-player online game	Ongoing web-based functional game	(Common Sense, 2018)
14	Disinformation, troll detection awareness	General audience	Game-based learning	Game design	Single-player online game	Ongoing web-based functional game	(Urban, Hewitt & Moore, 2018)
15	Disinformation, troll detection awareness	General audience	Game-based learning	Game design	Single-player online game	Ongoing web-based functional game	(Barabas, 2023)

3. Research Methodology

The fast-paced advancements of cyber attackers and their corresponding threats overscore the awareness and readiness of existing scientific and professional efforts on building cyber security awareness, education, and training of the younger generation of students, as already discussed in the previous section of this article. This represents the knowledge gap that this research aims to address by designing a cyber security awareness digital game for high school students/adolescents focusing on social bots and broken authentication threats. To this end, the following research questions are formulated:

- RQ1: Which cyber security awareness games that focus on disinformation social bots and broken authentication exist for high school students?
- RQ2: How to design a disinformation social bots and broken authentication cyber security awareness game for high school students?

Given the scope of creating innovative artefacts that address real-world problems through an iterative design, the Design Science Research methodology is applied in this research considering the perspective illustrated in Figure 1, as follows (Hevner et al., 2004; Peffers et al., 2007; Ibrahim & Jaafar, 2009):

- Problem identification and motivation: extensive literature review was carried out in the fields of cyber security, software engineering, gaming, and computer science education domains to identify relevant studies, methods, design requirements, and metrics. Accordingly, scientific literature and practitioner and governmental publications were considered based on combinations of keywords like disinformation, social bot, broken authentication, security awareness, and game. In this process, the IEEE Digital Library, ACM Digital Library, Scopus, Wiley, and Google Scholar scientific databases were queried, and only English documents were included.
- Game design: based on the results obtained in the previous research phase, the core concepts, methods, and techniques are established to build the architecture of the game which is proposed in this article.
- Evaluation: in this research, the evaluation will be carried out when the game is developed with high school students in a setting established by the Dutch-Belgium research partners respecting the ethical assessment that was conducted and approved by the ethical committee of the university.
- Dissemination: the initial results of this research are presented focusing on the architecture of the game as described in this article.

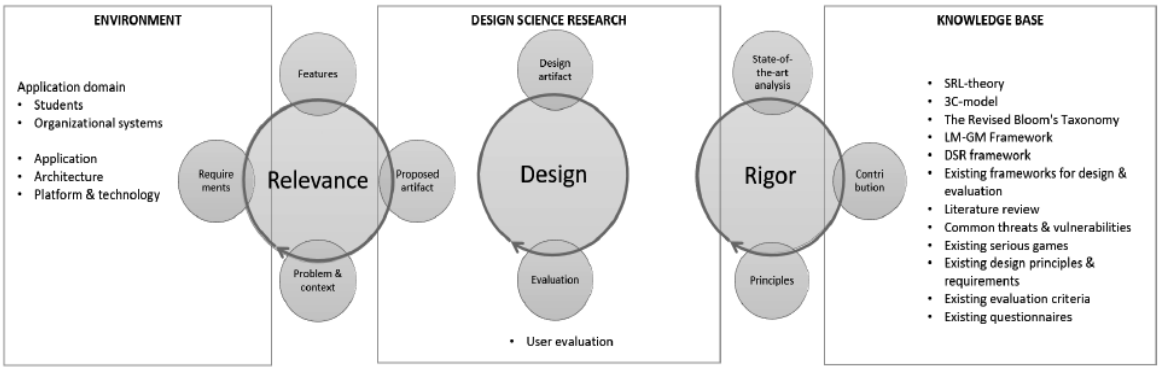

Figure 1: Research methodology application based on Hevner et al. (2004)

4. Digital Game Design

The design of a cyber security awareness game is a thoughtful process as it plays a pivotal role in developing it as it directly influences users' engagement and knowledge retention. This implies clearly establishing its target audience, learning goals, scenarios and content development, implementation choices, user interface, and the overall aesthetic aspects. Accordingly, the design requirements are established based on a set of corresponding technical and educational requirements and principles. Based on the extensive literature review conducted in this research and addressed in the previous section of this article, the following design requirements and principles are captured in Table 2, are tailored to the target audience of this research, and are considered for the game proposed. Next to these, taking into consideration the technical core of the game proposed, the ISO/IEC 25010: 2011 Systems and software engineering standard (ISO, 2011) is considered for assuring a proper quality and evaluation mechanism of the game. Furthermore, the instances considered in Table 1 are further elaborated in respect to the design of the game proposed in this research:

Educational and gaming methods: scenario-based learning and gamification design using the 3C-model are considered in this research (challenge, choices, and consequences of these choices) (Kuhlmann, 2019). This approach aims to challenge students to reflect on their choices for triggering their understanding about the learning materials, and further encouraging self-reflection and raising awareness in various settings.

Implementation and evaluation methods: the game will be implemented in Java and use MySQL as a relational database management system. Moreover, a series of scenarios are built inside the game considering effectiveness, game enjoyment, and usability as core evaluation criteria (Zhang-Kennedy & Chiasson, 2021).

Learning goals: the primary goal is to propose a game that increases the cyber security awareness of adolescents in relation to social bots and broken authentication cyber threats. Accordingly, the following core learning objectives are defined:

- Differentiate between credible and misleading information spread through disinformation campaigns.
- Explain and assess common patterns, functionalities, and tactics employed by social bots.
- Understand and apply corresponding mechanisms for controlling and/or avoiding engagement and the action of social bots.
- Understand and assess common vulnerabilities of authentication mechanisms in social media.
- Explain and assess the implications of broken authentication threats in social media.
- Understand and apply relevant mechanisms for assuring safe authentication in social media.

Table 2: Overview of requirements/principles

Design Requirement/Principle Categories	Design Requirement/Principle Description	Article No
1	Consider realistic scenarios that enhance learning and facilitate critical thinking	(Yasin et al., 2018; Maathuis et al., 2023)
2	Use the Bloom taxonomy	(Yasin et al., 2018)
3	Provide real-time feedback	(Wolfenden, 2019)
4	Consistency (the information presented is consistent), integrity (learning-by-doing), explicit or inferred aspects, and stand-alone assessments. Consistency in tracking and reporting progress.	(Zhang-Kennedy & Chiasson, 2021; Khader, Karam & Fares, 2021)
5	Guide and provide explanations to the user.	(De Troyer & Janssens, 2014)
6	Distinguish between mandatory and optional components of the game.	(De Troyer & Janssens, 2014)
7	Provide alternatives, visualize them, change them, and relate them to the impact of their choices.	(De Troyer & Janssens, 2014)
8	Easy to use graphical interface and provide feedback to users.	(De Troyer & Janssens, 2014)
9	Assess the effectiveness of the game by measuring the (i) usability and satisfaction, (ii) learning/knowledge acquisition, and (iii) impact on future online behaviour. Assess the effectiveness of the game by measuring (i) its adaptability to current situations, (ii) usability reducing the cognitive load and time spent, (iii) usability through easy to learn, efficient to use, and re-playability/re-usability, and (iv) learning considering an active and collaborative learning approach and measure the performance.	(Quayyum, Cruzes & Jaccheri, 2021) (Shamsi. 2019)

Game narratives and rules: the game uses and will be assessed in respect to its quality and effectiveness in relation to three use case scenarios: register, login, and game play. The narratives of the use cases capture real-world situations allowing the developers to foster understanding and the players to experience the consequences of their choices and actions in a simulated user-friendly controlled environment. The architecture of the game narratives is captured in Figure 2 below. Specifically, the game use cases contain the following elements:

- *Preconditions:* the student is already logged in.
- *Postconditions*: the student played one or more challenges.
- *Scenario logic:* the student selects the level of a topic -> the student starts a challenge -> the system presents the current challenge with its choices -> the student submits a choice -> the system verifies the choice -> the system presents consequences and feedback -> the system updates achievements and progress -> the system shows additional learning material -> if desired, the student selects additional learning material -> repeat until the current level of a topic is finished.
- *Additional rules:* in all the following cases the system records all states at events: (i) at any moment, the student can abort the game, (ii) in case of system failure, (iii) at any moment, the student can make a note, (iv) at any moment, the student can select informational help, and (v) the student can skip the additional learning material provided.

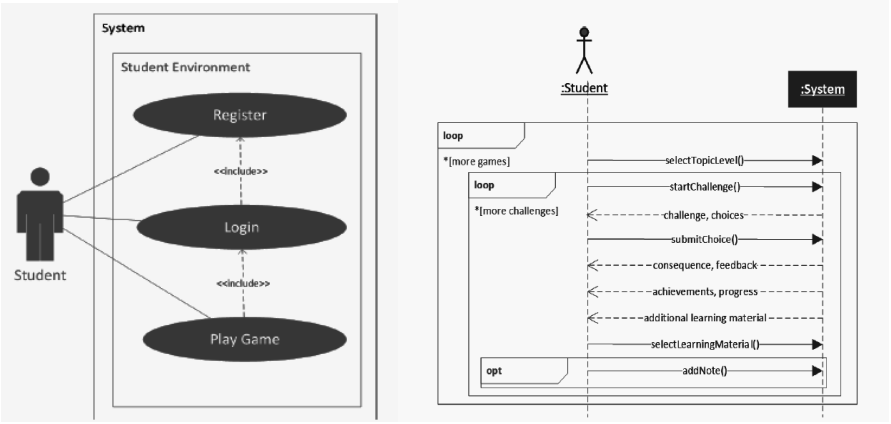

Figure 2: Use case diagram

Game architecture: this serves as the foundational framework that describes the overall user experience, feedback mechanism, educational effectiveness, and information flow between its core components. The architecture of the game proposed is illustrated in Figure 3 and has a modular structure allowing modular updates and extensions that enable the game to remain current with emerging cyber threats developments. Hence, the game architecture encompasses the following three layers:

- *Presentation layer:* represents the interface through which players interact with the game, containing graphics, user interface, and interactive elements. The implementation of this layer is done in JavaFX and FXML. JavaFX is a Java framework for developing cross-platform client applications with immersive media and graphical content, and FXML (Effects Extended Markup Language) is an XML-based language for defining the structure of the JavaFX interfaces.
- *Domain layer:* represents the backbone of the game as it contains the core logic and rules that govern the game while managing players' progression and feedback, in other words, it assures the alignment between the game mechanics and learning objectives of the game. The implementation of this layer is done in Java programming language.
- *Data layer:* represents the place where the game data is stored, retrieved from, and operated on for actions like creating players' profile, tracking players' performance, and scenario outcomes. Herein, MySQL is the relational databased management system used for managing and querying the data.

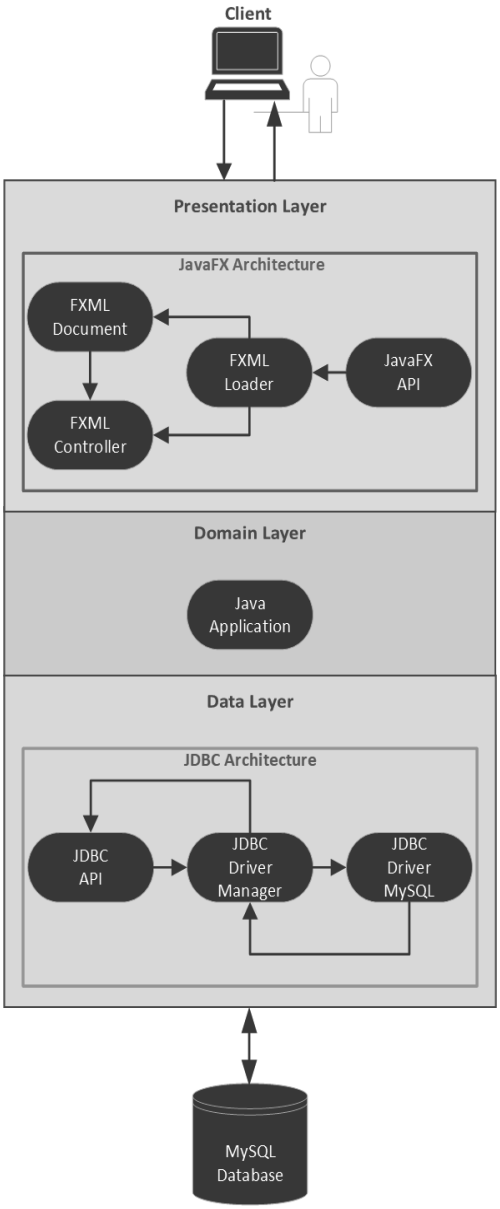

Figure 3: Game Design Architecture

5. Conclusions

While the advent of new technologies ushered unprecedent opportunities for connectivity and innovation across various societal domains, concomitant with these advancements are the uprising and escalating risks that reveal the importance and urgency of cyber security awareness. Although cyber security strategies and programs exist at regional, national, and local/organizational levels, they primarily focus on core assets like the infrastructure and corresponding systems and tools used, and only secondarily, on people (Tatum, 2023). Given the dynamism, complexity, and uncertainty that surround cyberspace (i.e., the digital domain), preventing, detecting, and responding in an effective manner to advanced, intelligent, and sophisticated threats is difficult as the threat landscape is continuously evolving and its effects cross the digital borders into the physical/human realm. Hence, cultivating cyber security awareness supports behaviour change and media literacy by building knowledge, skills, and resilience against cyber threats. Nevertheless, given the fact that children are digital natives being naturally drawn to social media platforms and content, they are also the most vulnerable and exposed ones to various cyber threats like authentication and disinformation as they lack cognitive maturity and discernment skills to navigate the digital sphere in a safe and responsible way (Maathuis & Chockalingam, 2022).

Based on the extensive literature review conducted in this research, efforts for building and enhancing cyber security awareness to primary and secondary schools through tools tailored to their cognitive abilities and age are in an incipient phase considering academic, governmental, or professional approaches and settings. It is then the aim of this research to tackle this knowledge gap and societal need by designing a cyber security awareness digital game for building and enhancing cyber security awareness among high school students in relation to cyber threats like social bots and broken authentication, which represent top cyber threats in the social media realm at global level. To achieve this aim, the architecture design of a cyber security awareness digital game is proposed in this research as the fundament for implementing the game using the Design Science Research methodology. This research continues with the implementation and evaluation of the game with high school students in real settings. Through this effort, this research strives to contribute to bringing cyber security awareness into the educational curricula and supporting the development of digital literacy programs tailored to children as the foundation of building a secure, privacy preserving, and responsible digital citizenship from an early age.

References

Bada, M., Sasse, A. M., & Nurse, J. R. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? *arXiv preprint arXiv:1901.02672*.

Barabas, R. (2023). What's the News About Bad News? A Review of Bad News Games as a Tool to Teach Media Literacy. *Libri*, *73*(4), 283-292.

Caramancion, K. M., Li, Y., Dubois, E., & Jung, E. S. (2022). The missing case of disinformation from the cybersecurity risk continuum: A comparative assessment of disinformation with other cyber threats. *Data*, *7*(4), 49.

Cernicova-Buca, M., & Ciurel, D. (2022). Developing Resilience to Disinformation: A Game-Based Method for Future Communicators. *Sustainability*, *14*(9), 5438.

Common Sense (2018). Digital Passport Educator Guide. https://www.commonsense.org/

De Troyer, O., & Janssens, E. (2014). Supporting the requirement analysis phase for the development of serious games for children. *International Journal of Child-Computer Interaction*, *2*(2), 76-84.

ENISA (2021). National cyber security strategies: with a vision on raising citizens' awareness. https://www.enisa.europa.eu/news/enisa-news/national-cybersecurity-strategies-with-a-vision-on-raising-citizens2019-awareness

ENISA (2023a). ENISA Threat Landscape 2023. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

ENISA (2023b). Identifying emerging cyber security threats and challenges for 2030. https://www.enisa.europa.eu/news/cybersecurity-threats-fast-forward-2030

Fard, A. E., & Maathuis, C. (2021). Toward Capturing the Underlying Offensive Mechanisms of Social Manipulation: A Data Model Approach.

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

Glas, R., van Vught, J., Fluitsma, T., De La Hera, T., & Gómez-García, S. (2023). Literacy at play: an analysis of media literacy games used to foster media literacy competencies. *Frontiers in Communication*, *8*, 1155840.

Hart, S., Margheri, A., Paci, F., & Sassone, V. (2020). Riskio: A serious game for cyber security awareness and education. *Computers & Security*, *95*, 101827.

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2008). Design science in information systems research. *Management Information Systems Quarterly*, *28*(1), 6.

Ibrahim, R., & Jaafar, A. (2009, August). Educational games (EG) design framework: Combination of game design, pedagogy and content modeling. In *2009 international conference on electrical engineering and informatics* (Vol. 1, pp. 293-298). IEEE.

IRIS Plus (2022). User empowerment against disinformation online. European Audiovisual Observatory.

ISO (2011). ISO/IEC 25010:2011 – System and software engineering standard. https://www.iso.org/standard/35733.html

ITU (2018). ITU Regional Workshop for Europe and CIS on Cybersecurity and Child Online Protection.

Jin, G., Tu, M., Kim, T. H., Heffron, J., & White, J. (2018). Game based cybersecurity training for high school students. In *Proceedings of the 49th ACM Technical Symposium on Computer Science Education* (pp. 68-73).

Kaur, J., & Ramkumar, K. R. (2022). The recent trends in cyber security: A review. *Journal of King Saud University-Computer and Information Sciences*, *34*(8), 5766-5781.

Khader, M., Karam, M., & Fares, H. (2021). Cybersecurity awareness framework for academia. *Information*, *12*(10), 417.

Kulhmann (2009). Build branched e-learning scenarios in three simple steps. https://blogs.articulate.com/rapid-elearning/build-branched-e-learning-scenarios-in-three-simple-steps/

Lees, J., Banas, J. A., Linvill, D., Meirick, P. C., & Warren, P. (2023). The Spot the Troll Quiz game increases accuracy in discerning between real and inauthentic social media accounts. *PNAS nexus*, *2*(4), pgad094.

Lazer, D. M., Baum, M. A., Benkler, Y., Berinsky, A. J., Greenhill, K. M., Menczer, F., ... & Zittrain, J. L. (2018). The science of fake news. *Science*, *359*(6380), 1094-1096.

Literat, I., Chang, Y. K., & Hsu, S. Y. (2020). Gamifying fake news: Engaging youth in the participatory design of news literacy games. *Convergence*, *26*(3), 503-516.

Maathuis, C., & Chockalingam, S. (2022). Responsible digital security behaviour: Definition and assessment model. In *European Conference on Cyber Warfare and Security* (Vol. 21, No. 1).

Maathuis, C., Kerkhof, I., Godschalk, R., & Passier, H. (2023). Design Lessons from Building Deep Learning Disinformation Generation and Detection Solutions. In *European Conference on Cyber Warfare and Security* (Vol. 22, No. 1, pp. 285-293).

Micallef, N., Avram, M., Menczer, F., & Patil, S. (2021). Fakey: A game intervention to improve news literacy on social media. *Proceedings of the ACM on Human-Computer Interaction*, *5*(CSCW1), 1-27.

Mikka-Muntuumo, J., & Peters, A. N. (2021). Designing an Interactive Game for Preventing Online Abuse in Namibia. In *2021 3rd International Multidisciplinary Information Technology and Engineering Conference (IMITEC)* (pp. 1-6). IEEE.

Olano, M., Sherman, A., Oliva, L., Cox, R., Firestone, D., Kubik, O., ... & Thomas, D. (2014). {SecurityEmpire}: Development and evaluation of a digital game to promote cybersecurity education. In *2014 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 14)*.

Paraschivoiu, I., Buchner, J., Praxmarer, R., & Layer-Wagner, T. (2021). Escape the Fake: Development and evaluation of an augmented reality escape room game for fighting fake news. In *Extended Abstracts of the 2021 Annual Symposium on Computer-Human Interaction in Play* (pp. 320-325).

Pastor-Galindo, J., Marmol, F. G., & Pérez, G. M. (2022). Profiling users and bots in Twitter through social media analysis. *Information Sciences*, *613*, 161-183.

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of management information systems*, *24*(3), 45-77.

Quayyum, F., Cruzes, D. S., & Jaccheri, L. (2021). Cybersecurity awareness for children: A systematic literature review. *International Journal of Child-Computer Interaction*, *30*, 100343.

Al Shamsi, A. A. (2019). Effectiveness of cyber security awareness program for young children: A case study in UAE. *Int. J. Inf. Technol. Lang. Stud*, *3*(2), 8-29.

Smith, D. T., & Ali, A. I. (2019). YOU'VE BEEN HACKED: A TECHNIQUE FOR RAISING CYBER SECURITY AWARENESS. *Issues in Information Systems*, *20*(1).

Tatum, D. (2023). *Gamification of security awareness training programs: a literature* (Doctoral dissertation, Georgia State University).

UNICEF (2021). Digital misinformation/disinformation and children. https://www.unicef.org/globalinsight/stories/digital-misinformation-disinformation-and-children

Urban, A., Hewitt, C., & Moore, J. (2018). Fake It to Make It: Game-based Learning and Persuasive Design in a Disinformation Simulator. In *Conference: Association for Educational Communications and Technology*.

Wolfenden, B. (2019). Gamification as a winning cyber security strategy. *Computer Fraud & Security*, *2019*(5), 9-12.

Wu, T., Tien, K. Y., Hsu, W. C., & Wen, F. H. (2021). Assessing the effects of gamification on enhancing information security awareness knowledge. *Applied Sciences*, *11*(19), 9266.

Yasin, A., Liu, L., Li, T., Wang, J., & Zowghi, D. (2018). Design and preliminary evaluation of a cyber security Requirements Education Game (SREG). *Information and Software Technology*, *95*, 179-200.

Zhang-Kennedy, L., & Chiasson, S. (2021). A systematic review of multimedia tools for cybersecurity awareness and education. *ACM Computing Surveys (CSUR)*, *54*(1), 1-39.

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber security awareness, knowledge, and behavior: A comparative study. *Journal of Computer Information Systems*, *62*(1), 82-97.