The case for intergenerational serious games on cybersecurity awareness – a conceptual framework

Iolanda Bernardino[1][a], José Bidarra[2][b] and Rafael Bidarra[3][c]
[1]*Instituto Politécnico de Leiria, Leiria, Portugal*
[2]*Universidade Aberta, Lisbon, Portugal*
[3]*Delft University of Technology, Delft, The Netherlands*
iolanda.bernardino@ipleiria.pt, jose.bidarra@uab.pt, r.bidarra@tudelft.nl

Keywords: Serious games, Intergenerational learning, Cybersecurity, Digital skills, Safe online practices.

Abstract: Today's society is becoming increasingly digitized, and many unprepared citizens fall prey to cybersecurity threats. For different reasons, developing safe online behaviors is a particular challenge for both older and younger generations. In this paper, we build on previous research to argue that intergenerational serious games can offer a promising educational approach to addressing this problem. We pose that, if carefully designed, a serious game that brings older and younger generations together can both enable older adults to improve their cybersecurity skills while sharing their life experience, and allow younger people to grow as they share their digital expertise. We discuss how playful collaboration between these two demographics may support the development of safe online practices. As a result, we propose a conceptual framework for the development of intergenerational digital safety learning through serious games, aimed and guiding the design and testing of such experiences. Finally, we recommend exploring and developing supportive learning environments as a means to foster a digitally secure and socially connected society.

1 INTRODUCTION

Although the internet plays an important role in everyday life, seniors and young people find themselves navigating a digital landscape with very different levels of familiarity and expertise. On the one hand, seniors can struggle with digital illiteracy and cybersecurity threats, but they also have a long and invaluable life experience. Their experience makes them more cautious in certain situations or better at identifying social engineering tactics based on real-world interactions (e.g., being more skeptical of unsolicited offers). On the other hand, young people typically possess greater technological fluency, but may be more vulnerable to deceptive online practices due to limited experience and developing critical judgement. This paper argues that intergenerational serious games represent a promising educational approach, that by combining their strengths through serious games, both groups could learn safe web practices together, overcoming generational barriers, and fostering mutual support: seniors may remain mentally engaged through gameplay, while younger generations may acquire new soft skills.

We know from previous research that older adults, while eager to participate in the digital world, often face significant barriers due to lack of experience and exposure to technology (Bernardino et al., 2021). This research has shown that many seniors have a keen desire to navigate the internet safely, particularly as they move towards greater digital independence. However, they often face challenges such as digital illiteracy, difficulties in understanding navigation, and fears related to cybersecurity threats (Smith, 2014). This scenario (i) underscores the critical need for tailored educational interventions that enhance their digital skills while promoting safe online behaviors (Morrison et al., 2021), and (ii) highlights the specific benefits of intergenerational learning and serious games, such as younger generations providing support and reducing fear of mistakes in a game environment.

Research on serious games for digital safety and cybersecurity awareness further suggests that such approaches are particularly effective when learning objectives focus on socially mediated risks—such as

[a] https://orcid.org/0000-0002-3956-4554
[b] https://orcid.org/0000-0002-2082-5996
[c] https://orcid.org/0000-0003-4281-6019

phishing, scams, data sharing, and online manipulation—rather than on technical skills alone (Hart et al., 2020; Moumouh et al., 2023; Kassner and Schönbohm, 2022; Zyda, 2005). When designed for educational purposes, serious games can support engagement, motivation, and dialogue, especially when combined with discussion and reflection activities (Cardona et al., 2024; Gutiérrez-Pérez et al., 2023). Importantly, the educational value of games in these contexts lies not only in their content, but in their ability to structure interaction and communication among participants.

In the context of cybersecurity education, serious games can effectively address vulnerabilities that seniors face online, such as susceptibility to phishing attacks and misinformation (Kassner and Schönbohm, 2022; Gwenhure and Rahayu, 2024). These games can simulate real-world online interactions, allowing seniors to practice and reinforce safe browsing habits in a controlled, risk-free environment (e.g., think of a game mechanic that mimics identifying a phishing email). Bernardino *et al.* (Bernardino et al., 2021) outline how such games can be instrumental in understanding seniors' cybersecurity issues, thus empowering them to become more resilient and informed internet users.

In addition, the pandemic period has significantly accelerated the shift towards digital communication and interactions, making it essential for seniors to adapt to online environments not only to engage but also to maintain family and social connections, thus promoting intergenerational exchange (Flynn, 2022). This necessity has galvanized efforts to implement intergenerational educational programs using serious games that convey cybersecurity concepts, bridging the generational divide while also equipping seniors with vital skills for the digital age (Hart et al., 2020). So far, there have been a few research prototypes aimed specifically at the cybersecurity domain (Gupta et al., 2020; Yamin et al., 2021).

In summary, intergenerational learning, facilitated through serious games, holds promise in improving cybersecurity education. This dual approach may foster digital literacy and encourage more inclusive forms of lifelong learning, ensuring that older adults and young people can navigate the complexities of the online world. The younger generation can learn from the wisdom of older people and gain new perspectives on life. And seniors may remain cognitively engaged and experience positive well-being outcomes.

2 SERIOUS GAMES'S ROLE IN INTERGENERATIONAL LEARNING

In this paper, serious games are understood primarily as digital games designed for purposes beyond entertainment, where learning objectives are intentionally embedded in gameplay (Zyda, 2005). This definition emphasizes computer-based environments and mental challenges, distinguishing the scope of this work from broader interpretations that may include non-digital or purely analogue games (Abt, 1987). While other perspectives highlight the reuse of game resources for non-entertainment purposes (Sawyer, 2009), this paper focuses on digitally mediated, scenario-based games that support collaborative reflection on digital safety and cybersecurity awareness.

Serious games for educational purposes are a powerful medium for facilitating intergenerational learning (Khalili-Mahani et al., 2020). They combine the engaging elements of gaming with structured opportunities for knowledge sharing, collaboration, and skill acquisition. Serious games can support structured and low-risk learning contexts where seniors can engage with younger individuals, fostering mutual understanding and skill development while overcoming common barriers associated with traditional educational methods (Marzo, 2024). Proper serious game design is instrumental in their effectiveness for intergenerational learning. For example, a player-friendly game interface and relevant real-life scenarios help reduce cognitive overload and facilitate smoother navigation for older adults. Additionally, features such as immediate feedback and iterative challenges can foster engagement and provide a sense of accomplishment, encouraging players to return to the game for further practice and learning.

One of the primary benefits of serious games is their ability to promote engagement and motivation among players (Cardona et al., 2024): because the prospect of learning new digital skills can be daunting, the interactive and immersive nature of serious games transforms the learning experience into an enjoyable activity. Unlike conventional educational methods that may feel monotonous or intimidating, games allow older adults to explore and experiment in a playful environment, encouraging risk-taking and reducing anxiety over performance. A gamified approach can significantly increase their willingness to participate in learning activities, especially when supported by younger generations who can help navigate technology.

Many serious games promote collaborative interactions, and some are even directly aimed at training

or assessing such skills (Alaka et al., 2019; Kochar et al., 2023). This is another key component for intergenerational learning: when seniors and younger players participate in team-based gaming experiences, they engage in dialogue, share insights, and help each other solve problems. This collaborative learning environment can create numerous opportunities for younger players to communicate essential digital skills and cybersecurity knowledge, while seniors can contribute valuable life experiences, contextual understanding and decision making (Flynn, 2024). Such synergy not only facilitates the transfer of knowledge but also builds social bonds and reduces stereotypes, fostering a collaborative learning environment where perspectives from both age groups enrich the overall experience. For instance, while playing a serious game focused on cybersecurity, seniors might share their critical thinking strategies (e.g. recognizing social engineering tactics based on real-world scams), while younger players might impart technical skills necessary for navigating digital threats. Moreover, explaining technical concepts to someone less familiar can also deepen the young player's understanding.

By design, many serious games immerse players in scenarios relevant to their real lives, encouraging context-based learning. This may foster discussions between older and younger players about digital practices, such as online security and privacy, a crucial aspect in today's digital environments. For example, as seniors navigate through a gameplay scenario that mimics phishing attempts or risky browsing practices, younger players can share tips that make the process easier and more intuitive. This reciprocal exchange of knowledge enriches the learning experience for both groups and emphasizes the value of collaboration between generations.

Prior research suggests that serious games may support aspects of emotional engagement, confidence, and social interaction among older adults, particularly when designed with accessibility and collaborative reflection in mind. By creating a shared experience that fosters interaction and enjoyment, serious games can combat feelings of isolation that often affect older adults. Engaging in games with younger individuals, seniors are more likely to develop a growth mindset, and boost their confidence in digital interactions. Even more, such playful interactions provide opportunities for socialization and connection, which are vital for mental health and overall well-being. These positive emotional outcomes further reinforce the learning process, as participants are more likely to engage in learning opportunities when they feel socially connected.

Another important aspect of serious games is their potential to create a safe and supportive learning environment for players. Mistakes made in game contexts do not carry the same consequences as in real life; therefore, players can experiment with different strategies without fear of personal repercussions. This safety net encourages exploration and learning from failures, a critical element in developing digital skills and cybersecurity knowledge, where trial and error often lead to deeper understanding and competency. Evidence from pilot programs, such as the 'Cyber Seniors' initiative [1], has shown that older adults gain significant confidence and skills through structured sessions with younger facilitators. Furthermore, intergenerational learning through games offers a multitude of benefits, bridging gaps between different age groups while fostering mutual understanding, collaboration, and skill development (Hewett, 2014). The integration of gaming as a learning platform provides innovative pathways for engagement and knowledge sharing between generations.

Many collaborative gaming experiences rely on effective communication to ensure successful collaboration. This encourages players of different generations to articulate their thoughts, discuss strategies and reflect together. This interaction helps to break down barriers, enhancing verbal and non-verbal communication skills. Seniors can learn to express technical concepts more clearly, while younger players develop patience and adaptability when explaining processes to their older peers. This exchange nurtures an inclusive dialogue around technology and learning.

Engaging in shared gaming experiences has been associated with opportunities for dialogue, mutual understanding, and perspective-taking in intergenerational learning contexts. On the one hand, seniors can exercise and enhance their cognitive abilities, which are crucial for maintaining mental agility as they age.

On the other hand, younger players can refine their critical thinking and analytical skills as they navigate challenges and learn from the accumulated experience of their older counterparts. The cooperative problem-solving tasks present in games encourage engagement that is mentally stimulating for both generations. In addition, it can help break down ageist stereotypes and foster a greater appreciation for older adults.

At its core, gaming is about enjoyment. The fun elements of gaming create a relaxed atmosphere conducive to learning, where fear of failure is minimized. When both generations engage in enjoyable activities, they naturally become more inclined to participate and invest in the learning process. This shared enjoyment strengthens bonds and cultivates a positive view of intergenerational interactions.

[1] https://cyberseniors.org/

This paper does not advocate comprehensive cybersecurity simulations or professional training environments, such as large-scale technical exercises designed for cybersecurity specialists. Instead, it focuses on serious games aimed at raising awareness among non-expert users and supporting reflection, discussion and a shared understanding of everyday digital risks.

These games may involve collaborative, parallel or facilitator-guided play, and do not necessarily require synchronous communication between players. This acknowledges that effective awareness-raising games may incorporate single-player experiences, guided reflection activities or turn-based interactions, as demonstrated by existing educational games centred on phishing or online safety. These approaches are united not by the presence of direct communication, but by the intentional design of scenarios that prompt learners to reason about decisions, consequences, and safe online practices.

In intergenerational settings, such games are particularly valuable when they facilitate reciprocal contributions, enabling older adults to share their life experience and contextual judgment, and allowing younger participants to contribute their operational familiarity with digital platforms. Therefore, the educational value lies more in the structured learning interactions that games facilitate.

3 DIGITAL LITERACY SKILLS BUILT THROUGH SERIOUS GAMES

According to Eurostat (Pereira, 2025), the population of the European Union (EU) at the beginning of 2024 was estimated at 449.3 million people, a fifth of whom were over the age of 65 years. This percentage increased by 0.3% in 26 EU countries compared to 2023, with only Malta showing a decrease. This fraction will tend to grow due to an increase in average life expectancy and low birth rates.

According to a Pew Research Center 2024 survey (Research, 2024) and an AARP's Tech Trends 2025 report (Kakulla, 2024), 90% of seniors are online with their own smartphones, spending increasingly more time browsing the web, communicating with others, shopping online, and navigating to where they need to go. Other researchers found that seniors spend more than an hour a day on social media sites such as YouTube and Facebook (Ruhle, 2025). Another interesting finding of this research was that 50% of seniors use their smartphones to play games and 70% of seniors prefer to search for information online. Technology is perceived positively and as an enrichment in the lives of seniors, helping with daily tasks and making aging more bearable.

As they age, seniors face a decline in visual acuity, which makes it harder to see small objects and instructions/captions or to locate information. They also face a reduction in their motor skills, which impairs their ability to maintain continuous and steady movements that are difficult to control with the mouse. Moreover, with the decline of cognitive processes, elderly people have less attention, working memory, problem solving and reasoning skills, which can be stringent in remembering information or processing the load of information (Ijsselsteijn et al., 2007; Bernardino et al., 2023). These limitations can be overcome through the appropriate design principles of effective serious games, such as user-friendly design, clear information, and incremental challenges (Moumouh et al., 2023).

In recent times, there has been a surge in educational institutions, such as senior universities, adult education, and ICT classes, which help seniors develop the right skills, providing a tutor or teacher who helps them become familiar with digital technologies (Coelho, 2019). (Bernardino et al., 2023) showed that a serious game for seniors should follow some critical guidelines: (1) the learning process must be accessible by focusing on the game and the learning purpose; (2) the game design and presentation must be user-friendly to avoid cognitive overload; (3) the game must support players' daily tasks by helping them remember small things that are done in their usual routine; (4) the information must be clear and easy to understand and read; and (5) the game must progress in small challenges to increase motivation and competition among classmates.

(Bernardino et al., 2023) designed their serious game around three topics: personal data, fake news and online shopping. During game play, seniors who were more comfortable with computers progressed quickly, while those who were less comfortable finished the game with the help of tutors. This research found that online shopping was the most anxiety-inducing topic, although the one with the highest interest for seniors. Despite the great challenge and the initial discomfort and anxiety, older adults' knowledge of web safety, and safe behavior skills improved with game play.

Today's elderly people have a larger social network that includes their grandchildren and friends, which encourages them to learn to use the internet not only to connect with others, but also to use technology to engage in meaningful activities (Lee and

Kim, 2019). Digital learning is still a challenge for elderly people due to the mix of anxiety and lack of confidence in using technology, but research has also found that they enjoy the opportunity for intergenerational interaction with youth (Tomczyk et al., 2023).

Conversely, younger generations are spending increasingly more time in the digital world, and even without realizing it, smart toys, video games, chatbots and artificial intelligence are shaping their digital interactions and influencing their choices regarding what they watch, read and listen to. This can expose younger generations to manipulative and misleading information, which threatens their right to protection (UNICEF, 2025).

Depending on their age, younger generations understand and interpret the principles of good web practice differently, particularly with regard to password creation. As younger generations are increasingly connected to the digital world, educators, parents, and even grandparents should promote and teach these good practices from an early age. By applying these practices, younger generations develop healthier web browsing habits, approach strangers on their digital profiles more carefully, and access their online accounts more securely (Gerster et al., 2023). Without being told that certain behaviors will affect their digital lives, they may develop fragile or insecure routines (Prior and Renaud, 2020).

Younger generations are more likely to internalize and apply what they have learned if they are given clear guidelines (Hartikainen et al., 2019). These good practices should be explained dynamically, for example through serious games. In recent years, game-based learning strategies have attracted increased attention. As a new digital lifestyle becomes established, this approach feels natural to today's younger generations, who have grown up with new technologies such as the internet. Serious games capitalize on young people's openness towards new media and can convey knowledge in a natural and non-intrusive way (Hetzner et al., 2009).

In their study, (Damenu et al., 2025) found that games can have a positive impact on learning outcomes by helping young people to gain knowledge of and awareness about cybersecurity. However, the scope of many games and studies is very limited — they focus on a specific topic, such as phishing, passwords or privacy, rather than offering a comprehensive approach to cybersecurity. This reduces the depth and coherence of young people's digital literacy. The age and developmental diversity of young generations also makes it difficult to generalize results, as games usually fail to consider the cognitive differences between various age groups. Furthermore, little attention is paid to ethics, privacy and cultural contextualization, as many studies do not discuss implications related to design ethics, nor do they adapt content to the local or cultural context (Damenu et al., 2025; Ebrahimi et al., 2025).

Learning improves when games are combined with practical exercises. The greatest impact was seen with the following sequence: game, practical lab and explanation. Simply playing is not enough to facilitate deep learning in young people. Practical experience builds confidence and turns knowledge into competence in handling (even simplified) real-world scenarios. This solidifies what the game introduced and develops a better understanding of cybersecurity concepts. Students therefore had a better grasp of digital risks, basic attacks and safe practices (Jin et al., 2018).

Several researchers adopt a hybrid design and evaluation strategy, combining a bottom-up approach involving young people, parents, and educators in the design process with a top-down approach involving theoretical guidelines and clear educational objectives. They argue that this enables you to cover broader and more integrated themes, promoting digital literacy in areas such as privacy, ethics, digital citizenship, data security and safe online behavior, rather than focusing solely on phishing or passwords (Damenu et al., 2025; Jin et al., 2018).

Research by (de la Hera et al., 2017) showed that intergenerational digital games strengthen family bonds by reinforcing relationships, introducing new topics of conversation, avoiding social friction, improving communication, and creating opportunities for younger and older adults to share their learning. Furthermore, games also improve mutual understanding by discovering their family members' skills and knowledge, and they reduce social anxiety, especially for older adults who face situations of social isolation.

In their survey, (Huang et al., 2025) point out that game-based approaches to cybersecurity and privacy in academic papers were targeted at students from elementary school to college level, as well as players aged 5–25 and professionals. However, none of these approaches were specifically developed for seniors. Also, the topics of interest for the non-technical audience include network security, technology-specific topics, threats and corresponding defensive strategies, and privacy and data protection.

Game-based educational approaches are important to build digital literacy and cybersecurity knowledge among students in various age groups. Adapting and customizing content based on age, knowledge level and educational background ensures it remains relevant and engaging for all learners (Quayyum and Jaccheri, 2025; Cerezo et al., 2023).

(Quayyum et al., 2021) pointed out that reducing cybersecurity risks for young people requires strengthening cybersecurity awareness and ensuring safe internet use. Moreover, the various cybersecurity threats they identify for youth aged 9–18 mostly also hold for seniors as well, including:

1. *online privacy*;
2. *online harassment*, including cyberbullying and cyberstalking, which can have psychological and social impacts, and unwanted communication via technological channels;
3. *stranger danger*, including risks associated with interactions with strangers, such as catfishing and identity theft, and oversharing personal information, which can lead to
4. *social engineering* attacks and phishing, where older people are vulnerable to fraudulent sites;
5. *content-related risks*, including inappropriate (Violent, pornographic or illegal) content; invasive advertising; and spam;
6. *sexual solicitation*, e.g. sexting and receiving sexually explicit requests from strangers;
7. *technology-based threats*, including malware, viruses and device hacking;
8. *economic risks*: excessive online spending due to access to payment methods can lead to online gambling and financial fraud;
9. *internet addiction* contributes to risky behaviors and has a negative offline impact. It is also associated with poor cyber-wellness;
10. *password practices and management*: a lack of password security literacy makes seniors and children vulnerable (Quayyum et al., 2021).

While cybersecurity encompasses a wide range of technical threats such as malware, vulnerabilities, and network attacks, everyday digital risks faced by non-expert users are predominantly socially mediated. These include phishing, scams, identity theft, and deceptive online practices, which rely on human behavior rather than technical exploitation (European Union Agency for Cybersecurity, 2024). For this reason, this paper focuses on awareness-oriented learning rather than technical skill acquisition.

4 CONCEPTUAL FRAMEWORK FOR INTERGENERATIONAL DIGITAL SAFETY LEARNING

Building on prior research on serious games, intergenerational learning, and digital safety education discussed in previous sections, we propose a conceptual framework for intergenerational digital safety learning supported by serious games. This framework synthesizes insights from the literature, structuring key design and educational considerations into six interrelated dimensions:

1. Learning objectives - Focus on awareness, critical reflection, confidence, and safe online decision-making rather than technical mastery.
2. Intergenerational roles - Recognition of complementary contributions, with older adults providing experiential and contextual insight, and younger participants contributing operational digital knowledge.
3. Game mechanics - Use of scenario-based challenges, decision points, feedback, and prompts for reflection that support joint discussion.
4. Accessibility and inclusion - Design considerations addressing cognitive load, pacing, readability, and simplicity of interaction, to accommodate diverse abilities and experiences.
5. Ethical and safety considerations - Attention to informed consent, data protection, power dynamics, and safeguarding within an intergenerational learning context.
6. Evaluation and outcomes - Alignment between learning objectives and assessment strategies.

In order to assess the proposed conceptual framework, we recommend its application within, at least, the following two educational scenarios:

- Family-based scenario - A short workshop in which an older adult and a younger family member play a serious game about phishing and online scams. This is followed by a guided discussion, facilitated by prompts embedded in the game.
- Community-based scenario - An intergenerational learning session at a community center or as part of an educational program, pairing participants of disparate ages and combining gameplay with facilitated reflection activities.

The focus of this position paper is on the sound development of the proposed conceptual framework, not on particular field studies. However, we do envision several evaluation approaches that could be suitable for such future projects:

- Knowledge and awareness - Pre- and post-intervention questionnaires on digital safety.
- Confidence and self-efficacy - A Likert-scale measures of perceived ability to recognize and respond to online risks.

- Interaction quality - Observational rubrics capturing turn-taking, explanations, and joint decisions.
- Behavioral intention - Self-reported likelihood of adopting safer online practices.

These metrics should provide a solid basis for systematic evaluation while remaining appropriate for intergenerational, non-expert educational settings.

5 CONCLUSION

This paper argues that intergenerational learning facilitated by serious games represents a promising and potentially impactful educational strategy for promoting digital safety and literacy across generations. Integrating young people into the serious gaming experience aimed at enhancing seniors' cybersecurity awareness can lead to mutual benefits, bridging the digital divide, and cultivating safe online behaviors in both groups.

We argue that such an intergenerational strategy promotes reciprocal learning, strengthens social relationships and creates a collaborative community that values both digital literacy and shared experiences. The main challenge is the integration of a bottom-up approach that involves young people, parents, and educators in the design process, following a top-down approach based on theoretical guidelines and clear educational objectives. To facilitate this, we presented a conceptual framework for intergenerational digital safety learning, and recommended several educational scenarios and evaluation approaches for its assessment in future projects.

Future research should explicitly investigate the optimal design features of serious games dealing with cybersecurity in an intergenerational context. This could include detailing elements such as user-friendly design, clear information, and incremental challenges, which are known to overcome limitations faced by seniors, such as declining visual acuity, motor skills, and cognitive load. Moreover, it is needed to investigate novel and effective strategies to facilitate intergenerational interactions, possibly exploring the use of generative AI within the game environment. Future work should focus on systematically assessing the extent to which such games support improvements in knowledge, confidence, and attitudes toward cybersecurity across age groups.

REFERENCES

Abt, C. C. (1987). *Serious Games*. University Press of America, Lanham, MD.

Alaka, S., Lopes Cunha, M., Vermeer, J., Salamon, N. Z., Balint, J. T., and Bidarra, R. (2019). Stimulating ideation in new teams with the mobile game Grapplenauts. *International Journal of Serious Games*, 6:87–101.

Bernardino, I., Bidarra, J., Baptista, R., and Mamede, H. (2021). Serious games for seniors: Learning safe behaviors on the web. In *Iberian Conference on Information Systems and Technologies*, pages 23–26, Portugal. IEEE.

Bernardino, I., Bidarra, J., Baptista, R., and Mamede, H. (2023). Desenvolvimento do jogo sério Web Segura. *Rotura–Revista de Comunicação, Cultura e Artes*, 3(1):74–101.

Cardona, J. S., Lopez, J. A., Vela, F. L. G., and Moreira, F. (2024). Meaningful learning: motivations of older adults in serious games. *Universal Access in the Information Society*, 23:1689–1704.

Cerezo, E., Coma-Roselló, T., Aguelo, A., Blasco-Serrano, A. C., and Garrido, M. Á. (2023). Exploring intergenerational interactions through an online storytelling experience. *IEEE Transactions on Learning Technologies*, 17:157–171.

Coelho, A. R. R. (2019). *Seniores 2.0: inclusão digital na sociedade em rede*. PhD thesis, ISCTE - University Institute of Lisbon.

Damenu, T. K., G"okbay, I. Z., Covaci, A., and Li, S. (2025). Cyber security educational games for children: A systematic literature review.

de la Hera, T., Loos, E., Simons, M., and Blom, J. (2017). Benefits and factors influencing the design of intergenerational digital games: A systematic literature review. *Societies (Basel)*, 7(3):18.

Ebrahimi, E., Paré, E., Stoker, L., and White, J. (2025). Cybersecurity early education: A review of current cybersecurity education for young children. In *Proceedings of the 17th International Conference on Computer Supported Education (CSEDU 2025)*, pages 1–12, Porto. SCITEPRESS.

European Union Agency for Cybersecurity (2024). Enisa threat landscape 2024: July 2023 to june 2024. Technical report, Publications Office of the European Union, Luxembourg.

Flynn, S. (2022). Bridging the age-based digital divide: An intergenerational exchange during the first COVID-19 pandemic lockdown period in Ireland. *J. Intergener. Relatsh.*, 20(2):135–149.

Flynn, S. (2024). Intergenerational and informal learning in communities. *Networked Learning Conference*, 14:1–4.

Gerster, R., Swinkels, B., Streefkerk, T., Sjerps, T., van Melis, K., and Bidarra, R. (2023). Little big data - a secondary school game raising awareness on data collection and analysis. In *In Proceedings of CoG*, pages 1–6, New York. IEEE Press.

Gupta, S., Gupta, M. P., Chaturvedi, M., Vilkhu, M. S., Kulshrestha, S., Gaurav, D., and Mittal, A. (2020). Guess who? - a serious game for cybersecurity professionals. In *Games and Learning Alliance*, volume LNCS

15348, pages 421–427, Laval, France. Springer International Publishing.

Gutiérrez-Pérez, B.-M., Martín-García, A.-V., Murciano-Hueso, A., and de Oliveira Cardoso, A.-P. (2023). Use of serious games with older adults: systematic literature review. *Humanities and Social Sciences Communications*, 10(1):1–17.

Gwenhure, A. K. and Rahayu, F. S. (2024). Gamification of cybersecurity awareness for non-IT professionals: A systematic literature review. *International Journal of Serious Games*, 11(1):83–99.

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

Hartikainen, H., Iivari, N., and Kinnula, M. (2019). Children's design recommendations for online safety education. *International Journal of Child-Computer Interaction*, 22:100146.

Hetzner, S., Pannese, L., Hallmeier, R., and Confalnorieri, L. (2009). Storytelling and serious games for creative learning in an intergenerational setting. In *Proceedings of 3rd European Conference on Games Based Learning*, pages 303–311, Graz. Academic Conferences.

Hewett, M. (2014). Developing a board game to facilitate the relationship between older people and young adults. Master's thesis, Northwest University.

Huang, Y., Grobler, M., Ferro, L. S., Psaroulis, G., Das, S., Wei, J., and Janicke, H. (2025). Systemization of knowledge (SoK): Goals, coverage, and evaluation in cybersecurity and privacy games. In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems*, pages 1–27, Yokohama Japan. ACM.

Ijsselsteijn, W., Nap, H. H., de Kort, Y., and Poels, K. (2007). Digital game design for elderly users. In *Conference on Future Play*, page 17–22, Toronto, Canada. ACM.

Jin, G., Tu, M., Kim, T.-H., Heffron, J., and White, J. (2018). Evaluation of game-based learning in cybersecurity education for high school students. *Journal of Education and Learning*, 12:150–158.

Kakulla, B. (2024). 2025 tech trends and adults 50-plus. Technical report, AARP, Washington, DC.

Kassner, L. and Schönbohm, A. (2022). A serious game to improve phishing awareness. In *Games and Learning Alliance*, volume LNCS 13647, pages 109–117, Tampere, Finland. Springer International Publishing.

Khalili-Mahani, N., De Schutter, B., Mirgholami, M., Holowka, E. M., Goodine, R., DeJong, S., McGaw, R., Meyer, S., and Sawchuk, K. (2020). For whom the games toll: A qualitative and intergenerational evaluation of what is serious in games for older adults. *Comput. Games J.*, 9(2):221–244.

Kochar, R., Karklins, A., van den Hurk, T., Akutsu, T., Paardekooper, G., Kooij, R., and Bidarra, R. (2023). Mirrors in Smog City - a serious game to assess collaboration potential. In *54th ISAGA Conference*, volume 04209935, pages 106–117, La Rochelle. ISAGA.

Lee, O. E.-K. and Kim, D.-H. (2019). Bridging the digital divide for older adults via intergenerational mentor-up. *Research on Social Work Practice*, 29(7):786–795.

Marzo, R. R. (2024). Bridging the gap: Understanding and fostering intergenerational communication in the digital age. In Klimczuk, A., editor, *Intergenerational Relations*. IntechOpen, London.

Morrison, B., Coventry, L., and Briggs, P. (2021). How do older adults feel about engaging with cybersecurity? *Human Behavior and Emerging Technologies*, 3(5):1033–1049.

Moumouh, C., Chkouri, M. Y., and Fernández-Alemán, J. L. (2023). Cybersecurity awareness through serious games: A systematic literature review. In *Lecture Notes on Data Engineering and Communications Technologies*, volume 147, pages 190–199. Springer International Publishing, Cham.

Pereira, I. T. (2025). Mais de 65 anos e a aumentar: estará a UE a enfrentar uma crise demográfica? https://pt.euronews.com/embed/2758258. Accessed: 2025-5-2.

Prior, S. and Renaud, K. (2020). Age-appropriate password "best practice" ontologies for early educators and parents. *International Journal of Child-Computer Interaction*, 23:100169.

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

Quayyum, F. and Jaccheri, L. (2025). CyberFamily: A collaborative family game to increase children's cybersecurity awareness. *Entertainment Computing*, 52:100826.

Research, P. (2024). Internet, broadband fact sheet. Technical report, Pew Research Center.

Ruhle, J. (2025). What do seniors do online? 2025 data for marketers. https://creatingresults.com/blog/2025/03/13/what-do-seniors-do-online-2025-data-for-marketers/. Accessed: 2025-5-2.

Sawyer, B. (2009). Foreword: From virtual U to serious game to something bigger. In Ritterfeld, U., Cody, M., and Vorderer, P., editors, *Serious Games: Mechanisms and Effects*, pages xi–xvi. Routledge, New York, NY.

Smith, A. (2014). Older adults and technology use. Technical report, Pew Research Center.

Tomczyk, L., d'Haenens, L., Gierszewski, D., and Sepielak, D. (2023). Digital inclusion from an intergenerational perspective: promoting the development of digital and media literacy among older people from a young adult perspective. *Pixel-Bit-Revista de Medios y Educacion*, 68:115–154.

UNICEF (2025). Keeping children safe online. https://www.unicef.org/protection/keeping-children-safe-online. Acedido: 21 novembro 2025.

Yamin, M. M., Katt, B., and Nowostawski, M. (2021). Serious games as a tool to model attack and defense scenarios for cyber-security exercises. *Computers & Security*, 110:102450.

Zyda, M. (2005). From visual simulation to virtual reality to games. *Computer (Long Beach Calif.)*, 38(9):25–32.