GenLink - Infiltration: an intergenerational coop game about online safety

Sieb Scherpbier[1], Jasper Heijne[1], Philippe Henry[1], Paul Lindhorst[1], Omar Thabet[1], Tzu-Hsin Hsieh[1], Amir Zaidi[1], Iolanda Bernardino[2], and Rafael Bidarra[1]

[1] Delft University of Technology, Netherlands
R.Bidarra@tudelft.nl
[2] Universidade de Leiria e Oeste, Leiria, Portugal

Abstract. The knowledge and experience gap between children and seniors in the digital world is growing. Younger users may face challenges related to critical reflection, patience, and empathy in online interactions. Practicing these skills can feel cumbersome, discouraging both generations from improving. Instead, children and seniors can support each other, as they each excel in areas where the other faces challenges. To make cybersecurity practice more engaging, we developed *GenLink - Infiltration*, a serious game bringing a child and a senior together to learn from each other in a fun and interactive way. Players take on asymmetric roles in a shared mission to infiltrate a company. Each player operates in a different environment designed to match their strengths. Gameplay encourages communication and teamwork by providing role-exclusive information that players must combine to progress, thereby encouraging interaction. In addition to fostering collaboration, the game also reflects on cybersecurity and specifically online safety. Preliminary findings indicate that players had a positive experience, and expect the game to connect young and old players. We encourage future research with a larger, representative participant pool of *GenLink* to measure the increase in intergenerational collaboration and online safety knowledge.

Keywords: Serious Game · Inter-generational · Online Safety

1 Introduction

In the Netherlands, an estimated 2.4 million people aged 15 and over reported being cybercrime victims in 2024, corresponding to about 15.7% of the population in that age group, up from 14.8% in 2022 [11]. This illustrates the growing dangers of today's digital society, where cybersecurity literacy is no longer optional, but essential. While young people are more exposed to harassment and risky online interactions, elderly users are disproportionately targeted by fraud and scams. Younger generations, despite their digital fluency, often lack the patience or empathy to help their older relatives develop the skills needed to navigate these threats safely. At the same time, older adults bring life experience, critical

thinking, and resilience that can help younger users reflect on their own online behaviour. Bridging the divide could not only reduce cybercrime risks for seniors but also improve young people's online critical thinking and patience.

Serious games offer a promising approach to addressing this challenge. They transform the daunting prospect of learning digital skills into a positive experience, leading to less risk-taking and a reduction in anxiety over performance [14]. In a collaborative setting, interactions can provide a platform for seniors and younger players to engage in dialogue, which leads to strengthening mutual social bonds. Importantly, having players immersed in a controlled environment means their mistakes have no real-world consequences, stimulating risk-free learning.

We present *GenLink - Infiltration*, a serious inter-generational asymmetric coop game for two players: a child player, a youngster with less life experience, and a senior, an elder with lower digital literacy. By assigning complementary roles, the game fosters communication, shared problem-solving, and mutual dependence, while embedding online safety concepts into the gameplay.

To evaluate the effectiveness of *GenLink*, we focus on three key aspects that reflect its social and educational goals: interaction support between generations, increased awareness of online safety for seniors, and promoted patience and cooperation in younger players. We qualitatively evaluate these aspects with the following research questions:

- RQ1: Can *GenLink* foster intergenerational connections?
- RQ2: Does *GenLink* enhance seniors' awareness of online safety?
- RQ3: In what ways does *GenLink* encourage cooperative behaviour and intergenerational collaboration among younger players?

2 Related Work

Serious games have been used to enhance cybersecurity skills of seniors across multiple studies [1,3]. Bernardino et al. [1] investigated the potential of serious games as a tool to help seniors search the web more safely. Morrison et al. [4] identify reasons why seniors feel more at risk of cyber-attacks, and find that seniors experience increased anxiety and stress when managing cybersecurity.

Table 1 summarizes serious games related to digital literacy and cybersecurity. Some, like 'Interland' developed by Google [2], or 'Pro(f)Social' [5], are aimed at teaching children correct online behaviour by promoting pro-social behaviour and well-being among children. Other single-player games explain cybersecurity threats to adults in an engaging way, like 'More Than Meets the Eye' [8] or 'Phishing Academy' [9]. Multiplayer serious cybersecurity games are rare; an example is the competitive two-player anti-phishing game by Roepke et al. [7], which teaches players about phishing in a competitive manner. However, it fails to promote the collaborative aspect between players and teaches both players the same concepts. We adhere to the needs of two different demographics to teach both young and old players about online safety.

Commercial asymmetric cooperative games like 'Keep Talking and Nobody Explodes' [12] and 'We Were Here' [13] design puzzles so one player cannot guess

Table 1: Overview of related games

Game	**Target**	**Learning Goal**	**Multiplayer**
Interland [1]	Children	Online safety, pro-social behaviour	None
Pro(f)Social [10]	Children	Responsible digital behaviour	None
More Than Meets the Eye [14]	Adults	Cybersecurity awareness	None
Phishing Academy [15]	Adults	Recognize phishing threats	None
Anti-Phishing Game [13]	General	Phishing detection	Competitive
Keep Talking and Nobody Explodes [2]	General	Communication, teamwork	Coop. (asym.)
We Were Here [18]	General	Puzzle-solving, collaboration	Coop. (asym.)
GenLink – Infiltration	Seniors & children	Cyber awareness, patience, communication	Coop. (asym.)

their way to a solution: both players are fundamental to winning the game, which proves to be a good way to force communication and collaboration.

3 Game Design

GenLink is an asymmetric cooperative two-player puzzle game, connecting younger and older players through communication and teamwork in a cooperative experience while playfully teaching online literacy. It is played by one child ("**C**", aged 10-20) and one senior ("**S**", aged 60+), who take on the roles of a child and a grandparent infiltrating a company discriminating against seniors. Both players have unique information at their disposal and must communicate to exploit unsafe online behaviour by the company's employees, uncover hidden documents, and expose the company. The game takes about 20 minutes and is meant as a fun educational game.

3.1 Main Game Loop

Each level follows a loop (Figure 1). **S** sees an office map with information about the target to hack, and is responsible for guiding the young player. **C** explores the office environment, interacting with desks and non-playable characters (NPCs) to gather information. Both players use this information to decide which type of hack to perform out of a selection of options. Because neither player has sufficient information to solve the challenge independently, the mechanic creates a structural need for communication. Players must therefore share their findings and make joint decisions to progress.

3.2 Game Story and Style

The story is framed as a spy-themed infiltration of an evil corporation that is actively antagonising the senior generation. This creates purpose and excitement for both generations without making the game feel like a lesson or tutorial. The style is based on pixel art to show a simple and familiar style to both generations.

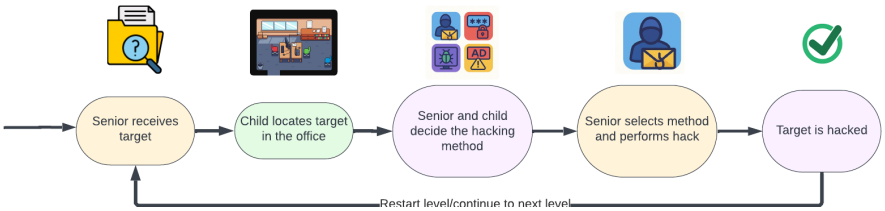

Fig. 1: Game Loop

3.3 Asymmetric Game Mechanics

GenLink uses asymmetric roles, to maximize engagement and intuition for both **C** and **S** and encourage their best qualities.

C explores the company's office with a narrow view, interacting with people and objects to gather information using on-screen buttons (Figure 2). **C** then receives information in speech balloons. As **C** is likely familiar with similar games, they should quickly understand their mechanics and find the large explorable area engaging. The asymmetry does not merely divide gameplay responsibilities; it creates conditions for reciprocal knowledge exchange. Each player holds information that the other needs, requiring them to communicate, explain their findings, and jointly interpret the available evidence.

S has access to a simplified map of the office, showing **C**'s location and clues for potential information, highlighted with exclamation marks (Figure 2). With the right information, the senior "hacks" by selecting the correct option related to common online threats: **phishing**, **weak passwords**, **scam advertisements**, and **social engineering**. We selected these four methods as seniors often fall victim to them [10,6]. By using them, seniors learn about the threats they pose and how to detect them. Additionally, **S** has a suspicion meter which shows how suspicious the players are, preventing them from interacting with everything and trying all hacking methods. Only **S** has access to this meter, to encourage **S** to monitor and guide **C**. Further, working within the limits of the suspicion meter teaches **C** patience and builds trust in their senior co-player.

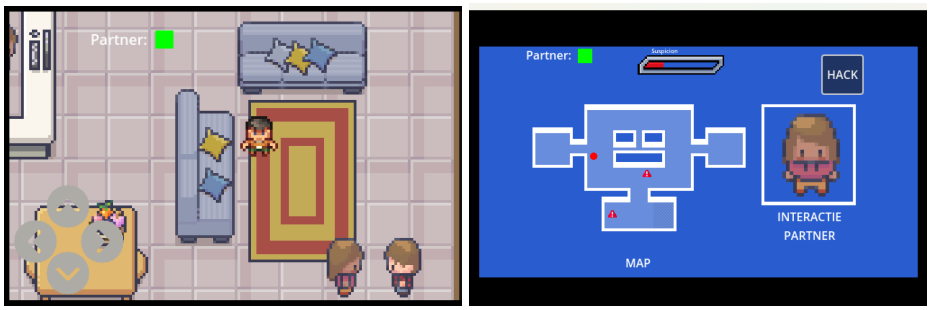

Fig. 2: User interface of **C** (left) and **S** (right).

Our UI for **S** is designed to be as intuitive as possible while remaining engaging. The hacking buttons are large and labelled with bold text to improve accessibility. They only become visible when pressing the "HACK" button. We do assume that **S** has minimal familiarity with user interfaces, as the target audience consists of seniors who use technology in their daily lives. This demographic is the intended group to learn about cybersecurity risks, as this is the demographic that might fall victim to these risks.

4 Evaluation proposal

Participants The proposed evaluation targets intergenerational pairs consisting of one younger participant and one older adult. Senior participants were recruited through a senior university, while younger participants were with them, so the participation was authorized by a legal guardian. Younger participants are expected to be aged between 10 and 20, while older participants should be aged 60 or over. Each pair will play the game together, providing the intended gameplay experience. An evaluator will facilitate the session and collect observational data.

Procedure The evaluation follows a pre-test/post-test design. Participants will first complete an initial questionnaire assessing their perceptions of cybersecurity, digital literacy and intergenerational learning. After a brief introduction, participants will play GenLink – Infiltration collaboratively, completing all the game levels. Afterwards, they complete a post-test questionnaire and participate in a short semi-structured discussion about their learning experience, how they collaborated, and their perceptions of the game.

Instruments Data collection combines quantitative and qualitative methods. The questionnaires were developed specifically for the exploratory evaluation of GenLink, based on the game's learning objectives and research questions. The pre- and post-test questionnaires include Likert-scale items and multiple-choice questions designed to assess intergenerational attitudes, cybersecurity awareness and collaborative behaviour. The game addresses the following cybersecurity learning outcomes: recognising phishing, being aware of social engineering, detecting deceptive advertisements, and understanding the importance of two-factor authentication. Additionally, observational notes and participant discussions are used to capture insights into communication patterns, cooperation and perceived learning during gameplay.

5 Preliminary findings

This section presents preliminary findings from the evaluation of $GenLink - Infiltration$, based on pre-game and post-game questionnaires, as well as a follow-up discussion with the participating junior/senior pair. Data were collected primarily through closed questions, utilizing a 5-point Likert scale (1 = strongly disagree to 5 = strongly agree) for attitude and self-estimation, and multiple-choice questions for objective knowledge assessment of online threats. These findings are based on 14 intergenerational pairs (N = 28 participants).

5.1 Fostering Intergenerational Connection and Engagement (RQ1)

Expectation of Bringing Generations Together Post-game evaluation assessed participants' agreement with the statement, "I believe this game can bring children and seniors together" (5 = completely agree).

Both demographics reported a high level of agreement that the game fulfills this purpose, where Junior players reported a high average agreement of **4.3** and Senior players reported an average of **3.8**.

These results suggest that participants perceived *GenLink* as having potential to support communication and collaboration between generations. This finding is consistent with the game's asymmetric design, which requires players to exchange role-specific information to progress.

Overall Game Positive Experience Participants were asked to provide an optional rating of the game on a scale of 1 (lowest) to 10 (highest). The distribution of the 28 reported scores demonstrated a **positive sentiment** toward the game.

The modal score was 8, and over **79%** of the participants rated the game 7 or higher (22 out of 28 responses). This suggests a high degree of player satisfaction, suggesting the game delivers a fun, accessible experience. These results indicate a generally positive reception of the game, although two senior participants reported low scores and identified unclear explanations as a concern.

5.2 Enhancing Online Safety Awareness (RQ2)

Prior to gameplay, the participants' existing knowledge was assessed through self-estimation and objective questions on specific online threats.

Self-Estimation of Knowledge (Scale 0–5): Participants were asked to estimate their own knowledge of online safety; Junior players reported an average self-estimation of **3.6**, and senior players reported a slightly lower average of **3.3**. These scores indicated that both groups already considered themselves to have a **solid understanding** of key online safety concepts before playing.

Objective Familiarity with Hacking Techniques: The game embeds four common online threats *(phishing, weak passwords (2FA), scam advertisements, and social engineering)* directly into the senior player's role. Initial multiple-choice questions measured objective familiarity with these concepts. The aggregated data across both age groups (combined junior and senior data) were very similar. Both seniors and juniors scored the same on average on the Phishing and Social engineering questions, 71% and 80%, respectively. On 2FA, Seniors scored better (93%) than Juniors (78%) and on Fake advertisements, Juniors scored better (79%) tan Seniors (64%)

The data show high pre-game familiarity, with awareness highest for **2FA** (85.5%) averaged. This high level of prior knowledge across the evaluation cohort is noted as a limiting factor, contributing to the observation that only "small

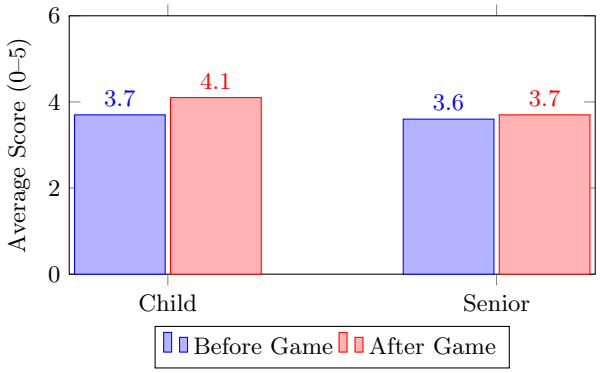

Fig. 3: Comparison Ability to Recognize Online Security Risks Before and After the Game.

improvements were recorded" in post-game assessments. This high baseline may be partly attributed to the specific demographic, as participants were noted to be slightly younger than typical seniors, suggesting they possessed more familiarity than the target group.

Pre- and Post-Game Recognition of Security Risks (Scale 0-5) The core evaluation of RQ2 involved comparing the ability to recognize security risks before and after playing the game, Fig. 3 highlights the before and after measurements for both demographics.

Both Senior and Junior players showed a small improvement in their ability to recognize online security risks. Senior players showed a small increase from 3.6 to **3.7**, while junior players increased from 3.7 to **4.1**.

Improvement in Online Safety (Scale 0-5) To further assess the depth of understanding achieved by participants regarding specific threats (RQ2), the post-game questionnaire required players to rate how clearly they improved in the four key online security aspects.

Participants reported positive perceived improvement across the four concepts (N=28). For Phishing, 17 participants rated their improvement as a high 4 or 5. Fake Ads and Two-Factor Authentication (2FA) demonstrated the highest improvement, with 18 and 19 participants, respectively, reporting ratings of 4 or 5. Even Social Engineering, which had the highest frequency of lower scores (ratings 1–3), still resulted in 14 participants reporting high improvement (4 or 5).

5.3 Encouraging Collaboration and Cooperation (RQ3)

Research Question 3 (RQ3) aimed to determine in what ways *GenLink* encourages **intergenerational collaboration and cooperative behaviour** among younger players. The asymmetric game design, where the senior is in charge and guides the child who operates under the limits of a suspicion meter, was intended to teach the child patience.

Increased Patience This element was evaluated post-game using a self-reported rating of agreement with the statement, "I have become more patient" (on a 0-to-5 scale).

Junior players reported an average rating of 2.2, suggesting a moderate self-reported increase in patience after gameplay. The senior players reported a slightly higher average increase of 3.0. The game's asymmetric design necessitated that the younger player have to depend on and coordinate with their senior partner to move forward. Comments from the post-game discussions showed that the senior's leadership helped the younger player become more patient and more focused.

Even so, the overall rise in patience was small. We found that using only a self-report questionnaire to measure patience did not give clear results. The change was described as a "mediocre increase," which was too vague to make a firm judgment about that learning goal.

5.4 Summary

In summary, the prelimenary results suggest that the game's strength in collaboration (RQ1), showing high positive experience and strong participant expectation that the game connects generations. While knowledge gains were modest due to the high baseline, a measurable improvement in security risk recognition was achieved specifically for the senior demographic (RQ2). The findings regarding patience (RQ3) were inconclusive, indicating a need for more concrete behavioral metrics in future research.

6 Conclusion

GenLink - Infiltration addresses the growing digital divide between younger and older generations. Seniors often struggle with online safety, while younger players can lack patience and empathy. The game's cooperative, asymmetric design aims to bridge this gap by encouraging communication and shared problem-solving.

We evaluated the level of the positive experience of the players, the increase in online safety knowledge, and the increase in patience from playing the game. Our results suggest that both age groups had a the positive experience while playing *GenLink* and that they expect it to create a stronger social connection between them, as it brings them together and creates an atmosphere where communication and collaboration are key. This encourages our demographic to play the game out of interest, without it feeling like a chore. While the game is engaging, the increase in online safety knowledge and patience seems modest, likely influenced by the small number of participants. The study participants already considered themselves knowledgeable about online safety risks prior to playing the game, which likely limited observable improvements in their knowledge. Future evaluations should include pre- and post-tests to objectively measure learning outcomes and involve a broader sample. Last, participants did self-report an increase in patience after playing the game, but more testing is needed to conclude meaningful improvement. As future work, we encourage a new evaluation with a larger participant pool of people inexperienced in online safety.

References

1. Bernardino, I., Vieira Baptista, R.J., de Almeida, J.M.E.B., São Mamede, J.H.P.: Serious games for seniors: Learning safe behaviors on the web : Position paper. In: 2021 16th Iberian Conference on Information Systems and Technologies (CISTI). pp. 1–4 (2021). https://doi.org/10.23919/CISTI52073.2021.9476310
2. Google: Interland (2026), `https://beinternetawesome.withgoogle.com/interland`
3. Kassner, L., Schönbohm, A.: A serious game to improve phishing awareness. In: Games and Learning Alliance: 11th International Conference, GALA 2022, Tampere, Finland, November 30 – December 2, 2022, Proceedings. p. 109–117. Springer-Verlag, Berlin, Heidelberg (2022). https://doi.org/10.1007/978-3-031-22124-8_11
4. Morrison, B., Coventry, L., Briggs, P.: How do older adults feel about engaging with cyber-security? Human Behavior and Emerging Technologies **3**(5), 1033–1049 (2021). https://doi.org/https://doi.org/10.1002/hbe2.291
5. Pereira, N., Ferreira, P., Francisco, S., Veiga Simão, A.M.: Pro(f)social: A serious game to counter cyberbullying. In: Games and Learning Alliance: 12th International Conference, GALA 2023, Dublin, Ireland, November 29 – December 1, 2023, Proceedings. p. 119–128. Springer-Verlag, Berlin, Heidelberg (2023). https://doi.org/10.1007/978-3-031-49065-1_12
6. Ray, H., Wolf, F., Kuber, R., Aviv, A.J.: Why older adults (don't) use password managers. In: 30th USENIX Security Symposium (USENIX Security 21). pp. 73–90. USENIX Association (2021)
7. Roepke, R., Ballmann, J.: Towards a competitive two-player anti-phishing learning game. In: Games and Learning Alliance: 12th International Conference, GALA 2023, Dublin, Ireland, November 29 – December 1, 2023, Proceedings. p. 56–66. Springer-Verlag, Berlin, Heidelberg (2023). https://doi.org/10.1007/978-3-031-49065-1_6
8. Roepke, R., Drury, V., Peess, P., Johnen, T., Meyer, U., Schroeder, U.: More than meets the eye - an anti-phishing learning game with focus on phishing emails. In: Games and Learning Alliance: 11th International Conference, GALA 2022, Tampere, Finland, November 30 – December 2, 2022, Proceedings. p. 118–126. Springer-Verlag, Berlin, Heidelberg (2022). https://doi.org/10.1007/978-3-031-22124-8_12
9. Schoebel, S., Roepke, R., Schroeder, U.: Phishing academy: Evaluation of a digital educational game on urls and phishing. In: Games and Learning Alliance: 10th International Conference, GALA 2021, La Spezia, Italy, December 1–2, 2021, Proceedings. p. 44–53. Springer-Verlag, Berlin, Heidelberg (2021). https://doi.org/10.1007/978-3-030-92182-8_5
10. Shang, Y., Wu, Z., Du, X., Jiang, Y., Ma, B., Chi, M.: The psychology of the internet fraud victimization of older adults: A systematic review. Frontiers in Psychology **Volume 13 - 2022** (2022). https://doi.org/10.3389/fpsyg.2022.912242
11. Statistics Netherlands (CBS): More victims of online crime in 2024 (Apr 2025), `https://www.cbs.nl/en-gb/news/2025/16/more-victims-of-online-crime-in-2024`
12. Steel Crate Games: Keep talking and nobody explodes (2015), `https://keeptalkinggame.com/`
13. TotalMayhemGames: We were here (Feb 2017), `https://totalmayhemgames.com/games/we-were-here`
14. Wouters, P., van Nimwegen, C., van Oostendorp, H., van der Spek, E.D.: A meta-analysis of the cognitive and motivational effects of serious games. Journal of Educational Psychology pp. 249–265 (2013). https://doi.org/10.1037/a0031311