# Secret Hacker: A Learning-Based Cybersecurity Game for Group-Based Settings

**George Wolf-Jackson**
Oxford Brookes University, Oxford, UK

p0097074@brookes.ac.uk

**Abstract:** Existing cyber security training methods do not deliver sufficient behaviour change to address the growing threat landscape that comes with an ever-more interconnected world. Many people of all ages struggle to effectively recognise cyber threats, and despite increasing investment in cyber security, the incidence of damaging cyber security attacks has only increased. Game-based training methods have been used successfully in a variety of fields, and many gamified and game-based cyber security training methods have been developed. Game-based training methods, as they exist, do not provide a 'silver bullet' solution for cyber security training, as a lack of commercial options, a high upfront cost to develop, and similarity with traditional training means that new game-based training methods have not had the desired impact on the cyber security landscape. This paper discusses the potential of *Learning-Based Games* - game-like training methods that are developed based on games, rather than on the training materials that educators and trainers intend to deliver. By utilising existing popular games, and introducing cyber security learning content, Learning-Based Games begin their design cycle as proven fun and engaging games, potentially reducing the developmental burden and cost. A new educational card game: *Secret Hacker* (primarily aimed at school children) is proposed, developed, and provisionally tested with a pilot group of 8 participants. It is based on a popular existing card game, and this paper justifies the design elements that make it well-suited as a game for delivering behaviour change. In particular, Secret Hacker has a focus on fun and engagement, and built-in replayability - and the game structure itself can be adapted to be suitable for more advanced learners. Methods by which this game can be used to gather assessment data are also discussed, to help educators and trainers to understand the cyber security behaviour of the users. This paper will outline the design and investigative process which may subsequently lead to the development of further such educational games, the improvement of Secret Hacker itself, and insight into the effectiveness of Learning-Based Games compared to game-based learning and traditional training.

**Keywords:** Game-Based learning, Cyber security, Behaviour assessment, Awareness training, Cyber games

## 1. Introduction

People around the world use the internet and other online systems at a rate that continues to rapidly increase. These systems are utilised by people of all ages, with over half of all 8-year-old children reportedly having their own phone or tablet (Merod, 2025), and 90% of children over 8 already using the internet (The Educator Magazine, 2024). This usage does not wane with age, as organisations and adults in general continue to use the internet and internet-connected activities for everything from online games to online banking, and web forums to storing mission-critical resources. 96% of adults use the internet (Pew Research Centre, 2024), and this rises to 98% among 18-65-year-olds. The internet is popular because it offers many positive experiences and conveniences to all types of users.

However, these benefits come at a cost. Cyber attacks have been increasing in frequency and sophistication for almost as long as the internet has been available at large and continue to do so. 72% of children have reportedly experienced at least one cyber threat (The Educator Magazine, 2024), and organisations continue to lose hundreds of billions of dollars annually (Miliefsky, 2025), to say nothing of the financial and other losses individual adults may experience in their personal lives.

Despite a clear problem, progress on combating cyber security threats is insufficient to address it (Bada, Sasse & Nurse, 2015). One of the most significant influencers of cyber security threats is the online behaviour of individuals – or human error. While the exact number is not agreed upon, most sources agree that over half of cyber security incidents are caused primarily due to human error – anywhere from 64% (Kaspersky, 2023) to 95% (World Economic Forum, 2022).

One of the main ways to improve human behaviour in cyber security scenarios is through the use of cyber security interventions – usually cyber security awareness training (Alnajim et al., 2023). This training aims to improve cyber security awareness and understanding among some group: adults in a workplace, users of a website, children of a certain age. Unfortunately, many existing training methods have been criticised as not sufficiently engaging users (Bada, Sasse & Nurse, 2015).

Game-based methods are sometimes utilised to deliver learning materials in a more engaging manner and use the well-established fun of games to improve training. In this paper I will outline a game-based training method that I have developed, *Secret Hacker*, as well as the concept of Learning-Based Games. Learning-Based

Games go further than Game-Based Learning to develop training directly from existing games and game formulae, rather than starting from the learning materials aiming to be delivered. This offers an alternative to existing methods for developing game-based cyber security interventions. I have also undertaken a practical assessment of Secret Hacker with a small focus group and used the analysis to determine improvements to the game, best practices for future game-based learning methods, and next steps.

## 2. Existing Work

### 2.1 The Effectiveness of Traditional Cyber Security Training

Traditional methods of improving cyber security behaviour have been acknowledged as ineffective in a variety of studies. Most existing cyber security awareness training programs that are utilised share a common problem: They are considered boring, overly difficult, not relevant to real world problems, they fail to engage their users, and most importantly of all – they do not sufficiently change behaviour (Bada, Sasse & Nurse, 2015; Haney & Lutters, 2018). They generally attribute this to training methods simply not considering engagement during their development.

### 2.2 Existing Game-Based Cyber Security Training

Game-based cyber security training methods have been considered as an alternative to traditional training. Zhang-Kennedy & Chiasson (2022) review many of these methods, finding common themes. Overall, outcomes of game-based training show promising signs, with noticeable increases in performance over traditional methods of training. However, there is significant focus on phishing which, while not unjustified (as phishing is a very prevalent threat), does risk neglecting other important areas of cyber security. Hendrix, Al-Sherbaz & Bloom (2016) also review game-based cyber security training methods, with similar results, noting that a significant proportion of the reviewed games utilise some kind of simulation of real-world environments.

### 2.3 The use of Card Games in Cyber Security Training

Game-based training in cyber security is a relatively small field, with adoption in the workplace being minimal, and research often limited to small games for studies, such as Anti-Phishing Phil (Sheng *et al.*, 2007) which is a well-regarded example of cyber security gamification. A large proportion of these games have been developed with the workplace in mind, as opposed to being aimed at children and younger adults. However, educational cyber security card games in particular (such as those in this section) are disproportionately targeted at children. Intuitively, this makes sense, as physical resources are often used in classrooms and a card game would be simple to implement. While technological improvements are transitioning many environments away from physical resources, there is still value to be had in the collaborative elements of in-person educational materials. Several existing educational cyber security card games were reviewed using a Google Scholar search for cyber security card games. 7 appropriate games were found in total, however 2 were discarded due to missing information.

**Table 1: Card games for cyber security training**

| Author(s) | Game name | Gameplay | Evaluation |
|---|---|---|---|
| **Aladawy, Beckers & Pape (2018)** | PERSUADED | Players use special cards to carefully draw cyber attacks they can defend against and new defences | No clear evaluation of learning |
| **Anvik, Cote & Riehl (2019)** | Program Wars | Players accumulate points by attacking and defending with cards | No clear evaluation of learning |
| **Denning *et al*. (2013)** | Control-Alt-Hack | Players must carefully allocate resources to defeat cyber attacks | Users were asked to report on a number of items, including educational value, which most (11/14) found there to be. |
| **Shah & Agarwal (2023)** | Cyber Suraksha | Players match scenarios with defence mechanisms | No clear evaluation of learning |
| **Thomas *et al*. (2019)** | CySEC Crucible | Players manage hackers with differing abilities to hack other players | No clear evaluation of learning |

In general, it appears that these games tend to heavily prioritise either the fun element or the learning element. Program Wars (Anvik, Cote & Reihl, 2019), Control-Alt-Hack (Denning *et al.*, 2013) and CySEC Crucible (Thomas *et al.*, 2019) focus heavily on fun, with minimal learning content – players may successfully complete the game without demonstrating much or any (substantial) knowledge of cyber security. Cyber Suraksha (Shar & Agarwal, 2023), on the other hand, very clearly requires comprehensive knowledge of the learning objectives in order to successfully complete the game, however the primary mechanic involves simple expressions of knowledge, with no gameplay skill involved (as cards simply need to be matched to each other). PERSUADED (Aladawy, Beckers & Pape, 2018) performs reasonably well on both metrics, as there is a strategic game element for fun, but players are also required to understand cyber security content in order to correctly match scenarios and defences. Unfortunately, PERSUADED is not comprehensively studied for its impact on users' behaviour, but there is certainly potential in this concept.

### 2.4 Summary

Cyber security training remains in clear need of improvement, and game-based training is a promising method of accomplishing an improvement in cyber security outcomes. However, cyber security game-based training methods are mostly quite small-scale and generally fail to utilise fun as effectively as existing traditional games. Card games are a common method of engaging younger audiences, but most existing games seem to lean too heavily on either learning content or fun content.

## 3. Game Development

Secret Hacker was developed with collaborative learning and community engagement potential in mind. The full development process is ongoing, but the initial prototype was developed over 3 weeks using basic graphical tools, basic freely available graphics (Pixabay, 2025), and literature backed cyber security scenarios. By giving players an environment in which to discuss cyber security, and the motivation to do so, the aim of the game is to encourage critical evaluation of cyber security scenarios.

In the early stages of development, this game was intended to have randomly chosen groups of "Hackers" and "Defenders" who would have security-based tasks to complete. While investigating similar games, Secret Hitler (Goat, Wolf & Cabbage, 2016) was identified as a well-established game that followed a similar gameplay loop and was therefore selected as inspiration for the game. Secret Hitler revolves around two teams - effectively a "good" team and a "bad" team - where the "bad" team (fascists in Secret Hitler) would be required to engage in social deception in order to hide their status and trick the "good" team (liberals) into enacting fascist policies, after enough of which they would win.

In Secret Hacker, Liberals and Fascists and replaced with Defenders and Hackers, who aim to place down "good cyber security behaviours" and "bad cyber security behaviours" (respectively), replacing Liberal and Fascist policy tiles. Much like in Secret Hitler, hackers have an opportunity to identify themselves to each other at the start of the game, to allow additional avenues for strategy.

### 3.1 Justification for the use of Learning-Based Games

Secret Hacker is a game that was developed with the concept of Learning-Based games in mind. A Learning-Based Game (LBG) is similar to Game-Based Learning and Gamification - in the sense that game elements are combined with learning elements to make training/educational content that is fun to engage with, whilst also effectively delivering the learning content. Where Learning-Based Games differ, is that they consider the "fun" element of a game as the fundamental basis to build upon, rather than the learning element. Where most existing educational/training games start with training materials and gamify them - giving users points and badges when they answer questions correctly, or complete elements (e.g. Anti-Phishing Phil; Sheng *et al.*, 2007), Learning-Based Games start with an existing game, and replace or add some elements of the game to teach and/or test cyber security knowledge and behaviours. The advantage of this method is that it results in a very high likelihood that the game will be fun and engaging – as these are games existing players have chosen to play, sometimes for considerable lengths of time.

### 3.2 Secret Hacker Game Content

The Secret Hacker game is a card game, and therefore it consists of several physical components. As of publication, there are a total of 71 cards, a 4-page rulebook, and an A3-size game board. The rulebook contains the game rules, instructions on how to play the game, and a comprehensive list of all 51 behaviour cards with corresponding explanations. The game is intended for 5-10 players, though could be conducted with fewer.

The game board has 13 slots for cards: 5 for each team's good/bad behaviours, one for the draw pile, one for the discard pile, and one for the active pile (that players vote on). This board is shown in figure 1.

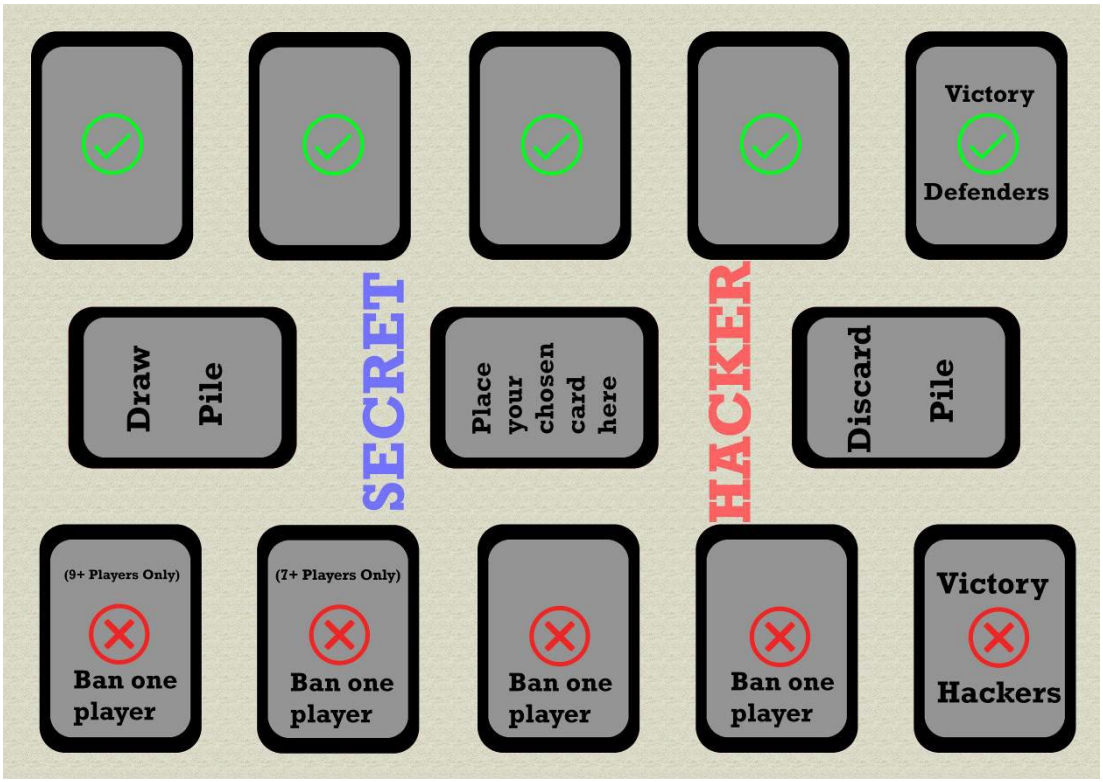


**Figure 1: Secret Hacker Game Board**

The 71 cards are of various types. There are 10 role cards – 6 defender and 4 hacker – to tell players which teams they are on. There are 10 yes/no double-sided voting cards – with a clear red-backed X on one side, and a green-backed tick on the other. The remaining 51 cards are all behaviour cards. In total, there are 3 sub-groups of 17 cards each, corresponding to password behaviours, phishing behaviours, and secure online behaviours, which is broadly in line with the cyber security content of existing cyber security training games. physical security, software behaviours, social media, and reporting behaviours were omitted at this stage but are intended to be added later with an additional 51 cards.

Each of these sub-groups has 7 good behaviours and 10 bad behaviours – as required for the game itself, so that an individual game on one of the cyber topic areas could be conducted, instead of the full game (in which cards come randomly from all three areas). As an example, if phishing has been identified as a particularly prevalent threat, the 17 phishing cards could be used in games, to focus on that area. These areas can then be mixed and matched as required.

A selection of these cards – each of the role cards, and a good/bad behaviour card from each of the three cyber areas is shown in figure 2. Note that the numbers in the bottom right correspond to entries in the rulebook, to ensure there is a way for players to ascertain whether the cards are good or bad behaviours.


**Figure 2: 5 sample cards from the Secret Hacker pack of 71**

### 3.3 Secret Hacker Rules

Throughout the standard gameplay loop, one player will be given three behaviours to choose from. They then have 15 seconds to choose two to pass to the player to their left, who similarly has 15 seconds to choose a card to place, face-up in the middle of the board. The entire table then has 15 seconds to either vote yes or no to this behaviour, based on their own personal strategy (generally, hackers will want bad behaviours, and defenders want good behaviours). If a majority vote no, then the card is permanently discarded. Otherwise, the card is placed on the row corresponding to whether it was a good or bad behaviour, moving towards a win for the defenders, if it was a good behaviour, or the hackers, if it was bad. After this, the players may discuss amongst themselves if they wish to question each other, and the explanation on why this behaviour was good or bad will also be read out. The rulebook contains a full list of all cards: whether they are a good or bad behaviour, and why.

The cards were designed to force players to think about whether they think that the actions being described are desirable, with the added condition of contributing towards the other team's win if they are incorrect. This is intended to motivate players to think about cyber security carefully, and to learn what makes behaviours good or bad. There are consequences for incorrectly identifying cards each way – if a card that helps the other team is voted for, their opponents progress towards victory. As there are a limited number of good and bad behaviour cards (7 good, 10 bad) and 5 are needed for a team to win, voting against cards that would help the players' team reduces their teams' chance of winning. The number of cards (7 good, 10 bad) were adjusted from traditional Secret Hitler (6 liberal, 11 fascist) to allow slightly more room for error, while discouraging reckless play in favour of carefully considering behaviours. If at any point the cards run out, the conclusion is up to the discretion of the officiator. If it is considered worthwhile the discarded cards may be reshuffled and put back into play, or the game may be called in favour of the hackers – as the defenders failed to facilitate good behaviours, and the hackers successfully disrupted service. After this, one of the teams will have won, and the group may discuss the gameplay.

As a final mechanic, after a number of bad behaviours (corresponding to the number of players) are played, the group has the option to *ban* one of their fellow players. If all of the hackers are banned, the Defenders win, and if over half of the defenders are banned, the hackers win (as they have successfully disrupted service – Availability of the CIA Triad). A full walkthrough of the rules and gameplay can be found at:

https://drive.google.com/file/d/1cv89_8Dfx9EResWaYlmzV61w5MYt3BmM/view?usp=sharing

### 3.4 Challenges with Learning-Based Games

While Learning-Based Games do not require the same level of challenging and often costly development for the games themselves, Learning-Based Games have their own set of challenges. One of the most significant difficulties is content generation. In total Secret Hacker has 51 distinct cyber security scenarios. A future expansion is planned which will add an additional 51 cards in 3 different cyber security areas, however each of these cyber security scenarios takes additional time on top of the basic development. Some scenarios can be developed from existing training materials; however, the fast-paced nature of many games necessitates more scenarios than traditional training. Consequently, this adds to the development burden. This may be an area where generative AI could be carefully used in the future, to develop such scenarios, but this approach is not considered in this research study.

Secret Hitler, and by extension Secret Hacker, is a social deception game. While popular, only a certain audience will enjoy the gameplay of Secret Hacker. This is the case with all games, and so in order to ensure a wide appeal, multiple different types of games would be required. While this would increase the development burden, the lack of appeal of some types of games to certain audiences is an issue that exists with standard game-based learning as well. Exploring methods of appealing to wider audiences with games is not typically explored with existing game-based learning methods and is beyond the scope of this study as well.

Among the most significant issues with Learning-Based games is the utilisation of Intellectual Property (IP). In the case of Secret Hacker, Secret Hitler is licenced under a creative commons licence, allowing non-commercialised re-distribution of modified content under certain conditions. Additionally, the principle of Fair Dealing and Fair Use may permit the use of copyrighted materials for limited research and educational purposes, but this involves legal complexities and significantly hinders commercial applications of Learning-Based Games. Successful large-scale use of Learning-Based Games would likely involve taking *inspiration* from existing games, rather than modifying existing games, unless in partnership with the original game developers.

## 4. Focus Group Evaluation

In order to understand the potential effectiveness of Secret Hacker as an educational game, and to improve it for more in-depth study, a small focus group study was conducted, with a total of 8 participants (2 in the first group and 6 in the second). As the first group was too small to fully play the game, the quantitative survey data has been omitted, though some of the comments and discussion from this group are still utilised.

### 4.1 Methodology

#### *4.1.1 Participant recruitment*

Participants were recruited primarily through convenience sampling. Posters were put out in the university building advertising the study, emails were sent around, and the study was advertised on an online forum. In the hours leading up to the study, potential participants were verbally invited. Participants were required to be 18+ but otherwise there were no restrictions on participation.

#### *4.1.2 Study procedure*

Participants in each group were asked to play the game once, for around 15-20 minutes. They were given an explanation of the rules, roughly in-line with the contents of the rulebook. They were given a sample round, in which a set of three cards were handed out as usual, but no time limit was applied and were given the opportunity to ask clarification questions throughout and after this practice round. Some guidance was given during the game segment, but this was limited, in order to not unduly influence the organic gameplay. Gameplay was terminated early, after only 4 "good" cyber security behaviours were placed down, as delays would have otherwise compromised the discussion section.

Throughout this study procedure, and the following discussion, an audio recording was taken, to capture relevant quotes and suggestions for future analysis. The participants were informed multiple times that this recording would be taken and agreed to it.

Only one playthrough (with practice round) was allowed in the study, however participants are able to access the game for future re-play if desired.

After the main gameplay, a short discussion segment was held, in which participants were asked to discuss:

- Which elements of the game they found enjoyable and not enjoyable.
- Whether they thought the game was fair and balanced, and they had broadly enough time in each segment.
- To what extent the cards could provide challenge and learning to them or others.
- What factors motivated them in the game.
- How the game could be improved, in enjoyment and learning.

After this discussion they were asked to complete a brief questionnaire that asked:

- Their cyber security knowledge from 1 to 10.
- How much they enjoyed Secret Hacker from 1 to 10.
- What they did/did not enjoy about the game.
- How much they felt they or others could've learned from Secret Hacker from 1 to 10.
- Which elements they feel did/didn't help the cyber security learning in Secret Hacker.

After these three steps were completed, participants were thanked for their time and left the study.

#### *4.1.3 Ethical considerations*

This study, of the game Secret Hacker, was granted full ethical approval by Oxford Brookes University UREC Registration No: L25372

No significant risks were identified in conducting this study, and the conditions of the approval were followed at all times.

### 4.2 Results

#### *4.2.1 Headline results*

Unfortunately, the first group only had 2 participants, and so the researcher needed to engage in the game in order for the study to go ahead. While the gameplay was not representative, some feedback was still gathered. The second group had 6 participants, and the game was able to progress in a much more realistic way. In total, 4 of the participants were members of staff, and 4 were university-level students. None of the participants were involved in the overall project at the time of the study, and all participants gave their consent to participate through physical consent forms before commencement of the study.

#### *4.2.2 Full results*

Due to the skewed experience of the first group (with 2 participants), only the 6 participant group is considered in these results.

**Table 2: Self-report questionnaire results from the second focus group**

| Participant number | Cyber security knowledge | Level of enjoyment of Secret Hacker | Learning potential of Secret Hacker |
|---|---|---|---|
| **1** | 6 | 8 | 7 |
| **2** | 8 | 10 | 5 |
| **3** | 9 | 8 | 8 |
| **4** | 8 | 9 | 9 |
| **5** | 8 | 8 | 8 |
| **6** | 9 | 10 | 5 |

Overall, on average, the participants rated themselves an 8 out of 10 in terms of cyber security knowledge – which is likely to be above the expected knowledge of a typical player of Secret Hacker (who would be expected to be an average school-aged child). In terms of "fun" content, on average participants reported 8.8 out of 10 "How much you enjoyed the game Secret Hacker". When asked how much they felt they did or could have learned from Secret Hacker, the result was 7 out of 10.

Two of the three participants that commented on the fun element of the game gave positive comments – "I genuinely had a lot of fun", "Engaging", "It's fun", but there was a significant body of constructive feedback as well. One comment asked for "room for more teamwork or us vs them elements".

### 4.3 Discussion

Broadly speaking, both groups found the game to be fun, and both groups felt that there was a reasonable possibility of learning from the game. In at least one instance, participants from each group incorrectly identified a card, and subsequently discussed why it was/wasn't a good behaviour, without prompting. There were some common issues – players found the game rules difficult to pick up initially, feeling that they needed more time to practice and adjust; that the strategy element may have overcomplicated matters; and that some of the cards felt more well-suited to the workplace than to school-aged children.

The level of fun participants experienced (8.8/10) is a very strong result, considering the preliminary nature of the game. These results likely stem from the *Secret Hitler* game that Secret Hacker is based on but does indicate that the "fun" of Secret Hitler was not significantly impacted by the addition of Learning Materials. The misidentification of at least one card, despite the relatively high (8/10) self-rated cyber security knowledge, indicates that there is a good amount of scope for learning content as this led to discussion in the group itself.

Participants were asked to consider the hypothetical learning, as well as their actual learning, and so it is possible the results of learning potential (7/10) were unduly skewed upwards.

The level of teamwork and competitiveness of the game may have been improved by the Hacker group being able to identify each other, as in Secret Hitler. In this instance it was not done, but in the future, it would be reasonable for the hackers to know who each other are.

While the game did run smoothly in the end, there were several comments on issues with understanding the rules – "it took a while to learn the meaning of the behaviours", "The beginning was a little confusing", "Took a

bit too long to get into it". The beginning was somewhat rushed, with participants arriving slightly late and a tight timeframe for the study, and there was only a single rulebook. The practice round did help, but it seemed to take 2-3 rounds for players to fully understand the game. One participant suggested that a "practice set of cards" could be used to not "[waste the] real cards". Additional copies of the rulebook and a more detailed explanation may help (though they would need to be modified to remove the answers), and a video explainer has also been developed. It was also suggested that the mention of strategy was confusing, and that players should simply be encouraged to vote according to their understanding of the cyber scenario and their role.

One participant said that "a discussion after each decision could be useful". This was already permitted under the rules, however this was evidently not made clear enough, and so will be clarified and encouraged in the future – as this discussion is a key aspect of the learning delivery.

The final major point that came up several times is with the suitability of the cards for the intended age group. A participant pointed out, to much agreement, that the cards are "all very work oriented". This prompted discussion around the types of threats that children face online, particularly ones that adults do not. This was reflected in the questionnaires with several comments suggesting to "add some cards [that] focus on cyber security attack[s] for children". The ability to swap out cards to address concerns for different population groups is one of the main strengths of the Secret Hacker concept, as the game structure does not rely on any particular scenario content.

### 4.4 Identified Game Improvements

The main points that were raised throughout this study, to improve the game experience for the target population can be summarised as follows:

- Encouraging teamwork and competitiveness by ensuring hackers identify each other at the start of the game (and where possible having odd-number groups, as the hackers struggled in an even-sized group).
- A better explanation of the rules, including more comprehensive practice rounds with special practice cards, and less focus on the strategic element of the game.
- Encouraging more discussion between rounds and explaining card results more fully (could be done by the players with their own modified rulebooks).
- Modification of some workplace-focused cards to be more appropriate to school-age children, as a separate version of the game.

## 5. Conclusions and Further Work

The aim of this study was to develop a game that can teach school-aged children cyber security concepts and reinforce positive cyber security behaviours. The results in this study, and of the paper more broadly, indicate a positive impact of Secret Hacker, though it is not definitely demonstrated that Secret Hacker achieves the stated purposes of this study – as this will need to be determined with further work. Participants enjoyed the game overall, maintaining the fun element of Secret Hitler, whilst providing a platform and motivation for players to engage with and discuss cyber security concepts, in such a way that helps to advance their understanding. Secret Hacker is an intact and enjoyable game, similar enough to a game that many individuals play for fun, while also delivering cyber security concepts. It is not necessarily a game that employees of a company, or students in a classroom would be required to complete once every 6, 12, or even 24 months, though it would also be possible to use it in such a way. With this in mind, it is certainly worthwhile to consider the dissemination of such games.

In a controlled environment, Secret Hacker was able to stimulate discussion of key cyber security concepts between experienced cyber security practitioners, whilst still being a fun and engaging game all around. The appeal of Secret Hacker was, if anything, more universal than expected, and certainly calls for further investigation of social-style games for cyber security education. With technology increasingly moving lifestyles online, interpersonal discussion and collaboration decreases, and games such as Secret Hacker help to reinvigorate this discussion, in a way that benefits understanding of cyber security.

Secret Hacker was, initially, intended as a game for school-age children – particularly teenagers – but the study was conducted with adults. A larger study will be required, in order to explore the impact of Secret Hacker on the cyber security behaviour of children, ideally in a classroom setting, with clear methods to measure any improvements in cyber security behaviour, and risk more widely. The results do, however, indicate that Secret Hacker could be effective among adults as well, and therefore the set of cards will need to be expanded to

include multiple versions – cards that address scenarios more typical to children, behaviours more typical to non-technical adults, and could be expanded to more technical fields as well. The Secret Hacker template appears to have been quite successful in initial testing, and with carefully chosen scenario cards could play a role in cyber security education for a wide variety of populations.

**Ethics Declaration**: Ethical approval was required and subsequently obtained for the study referenced in this paper, prior to the recruitment and commencement of this study, as detailed in section 4.1.3.

**AI Declaration**: AI was at no point used in the writing of this paper, the development or running of the study, or at any of the prior stages (e.g. ethical approval). AI was used in a limited capacity to transcribe two recordings from the study, to retrieve a small number of quotes from the text, in section 4.2.2. These quotes were, however, cross-referenced with other, non-AI sources.

## References


Aladawy, D., Beckers, K. and Pape, S. (2018) 'PERSUADED: Fighting Social Engineering Attacks with a Serious Game'. In *Proceedings of the 15th International Conference on Trust, Privacy and Security in Digital Business*. Regensburg (Germany), 5-6 September. pp. 103-118 Available at: https://doi.org/10.1007/978-3-319-98385-1_8

Alnajim, A. M. et al. (2023) 'Exploring Cybersecurity Education and Training Tech-niques: A Comprehensive Review of Traditional, Virtual Reality, and Augmented Reality Approaches', *Symmetry 2023*, 15(12), p. 2175.

Anvik, J., Cote, V. and Riehl, J. (2019) 'Program Wars: A Card Game for Learning Programming and Cybersecurity Concepts'. In *Proceedings of the 50th ACM Technical Symposium on Computer Science Education*. Minneapolis (Minnesota), 27 Febuary-2 March. pp. 393-399 Available at: https://doi.org/10.1145/3287324.3287496

Bada, M., Sasse, A.M. and Nurse, J.R.C. (2015) 'Cyber Security Awareness Campaigns: Why do they fail to change behaviour?'. *International Conference on Cyber Security for Sustainable Society (ICCSSS)*, Coventry (UK), 26 February. pp. 118-131. Available at: https://doi:10.48550/arXiv.1901.02672

Denning, T. *et al.* (2013) 'Control-Alt-Hack: the design and evaluation of a card game for computer security awareness and education'. In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*. Berlin (Germany), 4-8 November. pp. 915-928 Available at: https://doi.org/10.1145/2508859.2516753

Goat, Wolf, & Cabbage (2016) *Secret Hitler*, Available at: https://www.secrethitler.com/ (Accessed: 6th July 2025)

Haney, J and Lutters, W. (2018) '"It's scary...it's confusing...it's dull": how cybersecurity advocates overcome negative perceptions of security'. In *Proceedings of the Fourteenth USENIX Conference on Usable Privacy and Security (SOUPS '18).* Baltimore (Maryland), 12-14 August. pp. 411-425 Available at: https://doi.org/10.5555/3291228.3291261

Kaspersky. (2023) *Redefining the Human Factor in Cybersecurity*, Available at: https://www.kaspersky.com/blog/human-factor-360-report-2023/ (Accessed: 6th July 2025)

Merod, A. (2025) *Half of young children own a cell phone or tablet*, Available at: https://www.k12dive.com/news/half-of-young-children-own-a-cell-phone-or-tablet/741318/ (Accessed: 6th July 2025)

Miliefsky, G. (2025) *The True Cost of Cybercrime: Why Global Damages Could Reach $1.2 – $1.5 Trillion by End of Year 2025*, Available at: https://www.cyberdefensemagazine.com/the-true-cost-of-cybercrime-why-global-damages-could-reach-1-2-1-5-trillion-by-end-of-year-2025/ (Accessed: 6th July 2025)

Pew Research Centre (2024) *Internet, Broadband Fact Sheet*, Available at: https://www.pewresearch.org/internet/fact-sheet/internet-broadband/ (Accessed: 6th July 2025)

Pixabay (2025) Pixabay. Available at: https://pixabay.com/ (Accessed: 28 February 2025).

Shah, P. and Agarwal, A. (2023) 'Cyber Suraksha: a card game for smartphone security awareness', *Information and computer security* [Preprint]. Available at: https://doi.org/10.1108/ICS-05-2022-0087.

Sheng, S. *et al.* (2007) 'Anti-Phishing Phil: The design and evaluation of a game that teaches people not to fall for phish.' *3rd Symposium on Usable Privacy and Security (SOUPS'07).* Pittsburgh (Pennsylvania), 18-20 July. pp. 88-99. Available at: https://doi.org/10.1145/1280680.1280692.

The Educator Magazine. (2024) *Cybersecurity education from childhood is a vital tool: 72% of children worldwide have experienced at least one type of cyber threat*, Available at: https://the-educator.org/cybersecurity-education-from-childhood-is-a-vital-tool-72-of-children-worldwide-have-experienced-at-least-one-type-of-cyber-threat/ (Accessed: 6th July 2025)

Thomas, M.K. *et al.* (2019) 'Educational Design Research for the Development of a Collectible Card Game for Cybersecurity Learning', *Journal of Formative Design in Learning*, 3, pp. 27-38.

World Economic Forum (2022) *The Global Risks Report 2022*, Available at: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf (Accessed: 6th July 2025)