Gamification of Cyber Security Training - EnsureSecure

Callum Brady
Department of Computing
Bournemouth University
Poole, Uk
callum_brady@yahoo.com

Andrew M'manga
Department of Computing
Bournemouth University
Poole, Uk
ammanga@bournemouth.ac.uk

Abstract— There is an ever-growing fear of cyber-attacks in the modern workplace and these attacks are increasingly being linked to the human element. Securing this weak point is essential and this can be done through investment into workplace training. The current basic training methods have many issues that discourage the retention of the information learnt during the training. An example of one such issue is the level of engagement that the basic cyber security training provides the non-experienced participants. Low engagement means inefficient knowledge transfer and retention. This paper presents the results of a study aimed at improving cyber security knowledge retention of participants through the use of a conceptual physical card game that could be developed into an e-learning resource. This paper will document the preliminary research, design process and evaluation of the game.

Keywords—Cyber Security Education, Knowledge Retention, Game Design

I. INTRODUCTION

Information security is an ever-evolving sector and with this comes new challenges and a need for modern research. Modern cyber-attacks have steered away from exploiting traditional vulnerabilities and have instead opted for the exploitation of human elements as they are seen to be the weakest link in an organisation [1]. Interest in security from both the public and private sectors has invited a lot of investment into effective protection from security threats [2] and an important part of this protection is successful training for employees.

Traditional information security training is not effective at promoting good security practises and usually does not engage participants. One example of this type of ineffective training is an unenthusiastic drawn-out training video that employees are required to watch alone. This form of training can lead to participants forgetting the information they were provided with, which can then lead to security vulnerabilities in the business. This problem can apply to any individual or organisation that has significant assets that could be put at risk due to the insecure human element of their system.

A survey conducted in 2020 by TalentLMS along with Kenna Security highlighted a serious lapse in security awareness and knowledge amongst 1,200 employees [3]. 61% of participants failed a basic cyber security quiz and 69% of the participants had taken part in cyber security training from their employers [3]. This evident problem has inspired the research question:

What design requirements should be taken into consideration for a security-based serious game that can improve security awareness and improve the retention of knowledge?

To address the research question, current security and non-security-based games were analysed to identify aspects that allow for successful retention of information and positive engagement from participants. Upon solving this research question, a prototype for a cyber security game is created.

II. RELATED WORK

A. Traditional and Security Training Challenges

Traditional training has many challenges that need to be addressed when designing training programmes for desired outcomes to be met. A 2018 paper by Aldawood and Skinner [1] discussed some of the issues with training programmes. Some of these challenges are as follows:

- **Environmental**

Due to hybrid working patterns, training needs to be delivered both in office and remotely from various geographical locations .

- **Economic**

A lack of investment can lead to a lack of innovative solutions to training challenges. Outdated and cheap training can lead to activities being boring and the formal setting of workplace training can lead to a lack of knowledge retention.

- **Time**

A lack of time to complete the training. This could mean that there isn't enough time to cover all necessary topics and some topics could be rushed and therefore not remembered.

- **Personal**

Bada et al [4] also showcased that security and traditional training relies on an individual's ability to understand and apply the knowledge learnt in the training session. An individual's personality and past experiences could make them unable to perceive and understand risks with security training. These personal aspects could be influenced by external factors such as mental or physical workloads [5].

B. Delivery Methods

A 2012 paper written by Abawajy [6] presented different methods of delivering training programmes. These methods include:

- Conventional
- Instructor Led
- Online
- Game
- Video-based
- Simulation

The Game delivery method was chosen for this research over the others as, if done correctly, it creates a fun environment where participants will be engaged in the training, and it can also introduce a competitive aspect that can encourage participants to pay attention as they aim to win. Other methods such as the simulation method could possibly be more engaging than the game method however the cost of a simulation-based training program is far higher than the potential cost of a game-based training program [6]. The game solution aims to transfer security knowledge of an appropriate complexity level to players and will allow for discussions on the topics. The solution does not aim to replace current security training programmes, but rather complement them and propose an alternative way of learning.

C. Current games and Online Campaigns

Games have previously been created to try and address the cyber security training problem and although successful in many parts, the games have been less successful in essential aspects. An example of one of these games is 'Control-Alt-Hack'. The game attempted to use innovative game mechanics to create a fun and engaging game where unexperienced participants could learn about security. The game received mixed feedback from some students who played the game. The game was deemed to be engaging and the students learnt new security concepts [7], however it was too complicated and took too long to learn, therefore making it not suitable for a training session set in a time-sensitive setting and where the aim is to deliver the correct information in the most efficient manner [5].

Some online campaigns have also been created to provide cyber security guidance to business. An example of one of these campaigns is the National Cyber Security Centre's Cyber Aware campaign [8]. This campaign provided 6 simple steps to improve cyber security however this advice can be seen as too general and not specific to individual organisations. This lack of specific guidance can lead to the information not being applied correctly in the business environment and therefore not reducing the risk of cyber-attacks.

D. Knowledge Retention

Knowledge retention is defined as having information stored in long-term memory, in a format that can be easily accessed, and applied to a real-life scenario [9]. One famous experiment resulted in a diagram known as Ebbinghaus' forgetting curve [10][11]. Fig. 1 shows the curve and displays how a person's retention of information fades overtime. The green lines in Fig. 1 show how information retention improves after reviewing the information again. The aim of any form of training, including traditional or security, will be to make the gradient as shallow as possible which would mean that the information is retained at a good level for a longer period of time. A poor training method could result in a steep gradient and therefore the information is forgotten quickly. The effectiveness of training can be visualised on a forgetting curve graph.

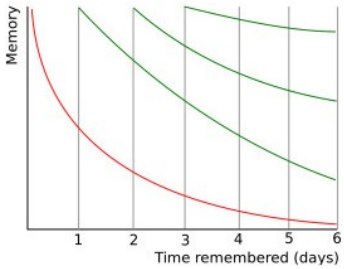

Fig. 1. **The Forgetting Curve [10][11]**

III. APPROACH

The second part of addressing the research question involved eliciting requirements for game design with groups of participants. The requirements were used to design a prototype of the game which was then used to evaluate game effectiveness. Details of the participant and questionnaires used for data collected are presented below.

A. Participants

Data collection for the research begun by identifying participants that could take part in the research. The study only required that the participants were of legal age to provide consent and that they had any level of experience working. Participants were found by advertising the research on social media platforms, those that responded were fully informed of the expectations and ethical considerations. A total of 23 participants were recruited, the participants came from a range of backgrounds that included a twenty something full-time student working part-time, to professionals in their early sixties approaching the end of their careers. The diversity of participants from various backgrounds made it possible to create a game that is suited for a wide range of players.

B. Questionnaires

Primary data collection came in the form of three questionnaires at different points in the research that were created using Jisc online surveys. The table below shows the three questionnaires that were created and the rationale behind them.

TABLE 1: QUESTIONNAIRE RATIONALE

Questionnaire	Rationale
1 – Predesign Attitude to training and current security knowledge	This allowed participants to say what they like and dislike about training in general and then their current security knowledge was understood. Their likes and dislikes were used to create game requirements along with additional research on current security games and training methods. Their

	security knowledge score was used in the comparison with questionnaire 3.
2 – Post design Game mechanics feedback	This questionnaire allowed the participants to provide feedback on how the game itself functioned. For example, was the game easy to learn? Their feedback was then analysed and improvements to the game could then be identified.
3 – Post design Knowledge retention feedback	This questionnaire tested participants on the topics they learnt during the physical play testing of the artefact. The results of this questionnaire were then compared to questionnaire 1 and successful knowledge retention could either be proved or disproved.

Questionnaire 1 was completed by 23 participants before the game was created as mentioned in Table 1, it was to understand their security knowledge and attitude to training. Examples of questions used in the questionnaire included:

- Have you previously taken part in information security or any training with a current or former employer?
- Please rate the security training in terms of engagement.
- What would you say made the security training engaging or not?
- What does the 's' at the end of "https://" mean at the beginning of a URL?
- Which of the following is a DoS/DDoS attack?

Questionnaire 2 was completed post-design, immediately after the participants had played the game. Some of the questions include:

- Please rate the level of enjoyment you felt while completing the activity (1 being not enjoying the game at all, and 5 being enjoying the game a lot)
- Please rate the level of engagement you felt while completing the activity (1 being not engaged at all, and 5 being very engaged)
- What, if anything, worked well with the activity?
- Would you recommend the use of this game as a part of a security training program?

Questionnaire 3 was completed by participants post-design, at least five days after they had completed the play testing session. This was done to test how well the participants would remember the training after a few days had elapsed. Some questions in questionnaire 3 included:

- What does the T in S.T.R.I.D.E stand for?
- Select the definition below that most closely matches the term 'Malware':
- What is a D.O.S attack?
- What is the name given to a virus that threatens to disclose victim's data unless payment is received?

IV. Data Analaysis

Both a qualitative and quantitative approach was used to analyse the data collected from the participants through the questionnaires. The first part of the analysis was on the first questionnaire, and this allowed requirements for the game to be specified. These requirements were ranked by priority using the MoSCoW requirements prioritization. Prioritization was driven by how critical the requirements were for the successful design of the game. Further analysis of the second and third questionnaire took place after the play testing sessions and allowed for an evaluation of the game.

A. Qualitative

The first part of qualitative analysis involved focusing on the anonymised feedback from the first part of Questionnaire 1. This qualitative analysis was beneficial to the study as through the use of open-ended questions, it allowed participants to fully explain their feelings towards training in the workplace. The findings from this analysis are shown below along with some examples of participant responses:

- Participants felt that engagement is a critical aspect of a training session as training can often be seen as boring.
  "Boring and somewhat easy to guess"
  "Interactive style makes it more engaging"

- Participants said that training is important to them – reinforcing the importance of effective workplace training.
  "It is important to develop the knowledge and skills of staff"
  Training is important "to safeguard myself, colleagues, the company and customers"

- Participants felt that security training is sometimes at the forefront of their minds when using IT equipment.
  Your Security Training is at the forefront of your mind at all times when working with IT equipment:
  Strongly Disagree – 1
  Disagree – 8
  Neutral – 5
  Agree – 6
  Strongly Agree – 3

B. Quantitative

The second part of analysis was quantitative which is from the second part of Questionnaire 1. This part was testing the participant's current security knowledge on a variety of topics. From the responses, the percentage of correct answers were identified and therefore topics were identified that had a low knowledge score. A few examples of topics that participants struggled with are Social Engineering (21.7% correct), Denial

of Service (17.4% correct), and Strong Passwords (8.7% correct).

The average score from this part of Questionnaire 1 was 64.6% which showed that there were gaps in the participant's security knowledge. This score was then compared with the score from Questionnaire 3 to see if there was an improvement in the participant's security knowledge and their retention of the knowledge.

V. Design

A. MoSCoW

Some of the requirements for the game could be deemed must haves, and others could be added in due course. Because of this, the requirements were outlined in a MoSCoW format as mentioned previously (Must, Should, Could, Will Not) [12]. The 'Must' requirements are as follows:

- Include each aspect of STRIDE
- Be a physical game
- Be easy to learn
- Engage participants

B. Card Design

Based on research and responses to the qualitative part of Questionnaire 1, it was determined that the cards for this game needed to be straightforward and simple to understand in order to have a low entrance barrier and therefore allow for positive engagement in the game. Fig. 2 displays a pair of sample cards along with the indicator card. An explanation card and a word card make up each pair of cards.

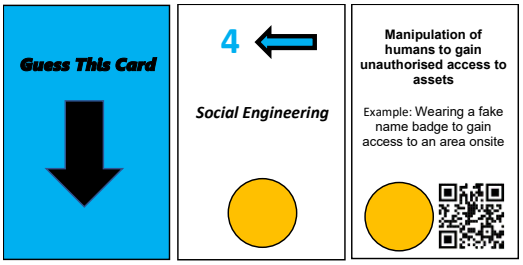

Fig. 2. **Indicator Card, Term Card, Description Card**

As shown in Fig. 2, the term card consists of a simple, bold term for participants to remember and the paired description card provides a simple explanation of the term along with an example. The terms and descriptions chosen were simple enough that participants could understand them, but also covers essential foundations of cyber security training.

The complexity level of the game must be suitable for the participants who will be playing it. If this complexity level is not suitable, the effectiveness of knowledge transfer will not be optimal, and the game will not meet its intended goal of improving participant security retention. Through research, multiple sources of appropriate IT knowledge were found that could be used as content for the artefact. For example, STRIDE was initially proposed by Microsoft, and it is used to assist when threat modelling a system by allowing for clear classification of 6 cyber security threat types [13][14]. The understanding of these 6 terms can allow for participants to be more aware of the threats posed to them while using IT systems and what the consequences of these threats could be [15].

C. Gameplay

The requirements allowed for the creation of a prototype. The game takes inspiration from two current games, 'Shopping List' [16], and 'Sherlock' [17]. Engaging participants in multiple different ways is essential to the outcome of the created game. This engagement must not only stem from the participant interactions but also from the game mechanics and game design. Although aimed at a younger age demographic, the game mechanics from both these games were adapted and applied in this research. These games were chosen as a source of inspiration over other potential games as they combined memory and simplicity in order to engage players.

Shopping List is a simple card matching game. This aspect was adapted for use in one of the ways of playing our game (EnsureSecure). The simple images and text used for Shopping List highlighted the importance of simple card design to allow players to remember not only what was on a card, but also where it is in the grid.

Sherlock focuses more on the memory side of learning with players attempting to memorize images in a circle and recall them when indicated to do so. Sherlock demonstrates how a simple game can be played in different ways depending on the complexity level desired. Sherlock also can be played with different ways of winning, for example first to a number of cards, or first to finish a deck of cards. This adaptive way of playing and different ways of winning was utilized in the design of EnsureSecure.

Humans will eventually forget information, as shown by the green lines on the forgetting curve in Fig. 1, however this concern can be avoided by reviewing training material frequently. Based on this, two distinct ways of playing EnsureSecure were developed to allow users to acquire the same material in different ways, reinforcing the content learned,in an effort to improve knowledge and memorability. Process flows for each form of game play were created and used as guides to ensure that the game complied with requirements.

The process flows for the Sherlock and Shopping List inspired gameplay type is shown below in Fig. 3 and 4.

One appealing aspect of this game is that both gameplay types can be played in different ways depending on the skill level of the players. This ability to adapt the game allows for people with different capabilities to successfully take part and the game complexity level can be increased gradually to prevent the game becoming too easy and boring after each round. To ensure that participants were not discouraged from the game, the simplest setup was chosen for each gameplay type during the test sessions. Another strength to this game is its simplicity in comparison to other cyber security-based games such as Control-Alt-Hack [7] as EnsureSecure can be learnt easily and adapted to the skill level of the players taking part.

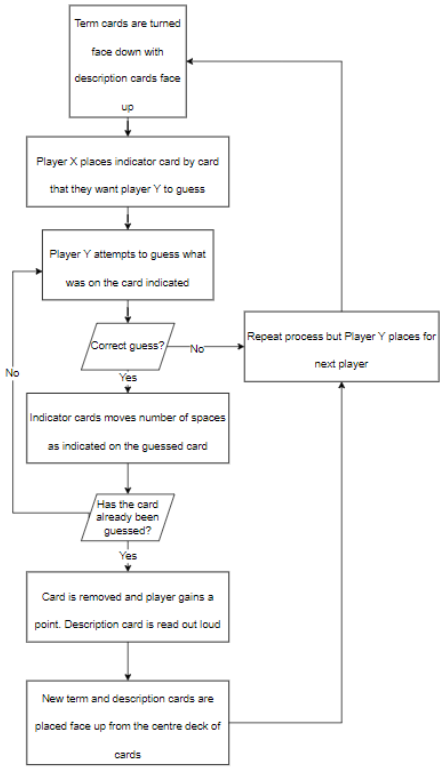

Fig. 3. **Gameplay Type 1 Process Flow**

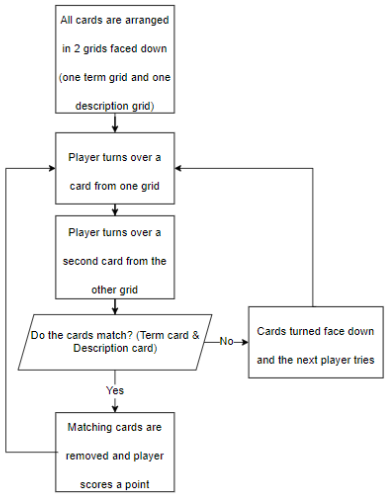

Fig. 4. **Gameplay Type 2 Process Flow**

VI. Findings

A. Play Testing Sessions

Players were divided into different play testing sessions based on their availability, with eight sessions scheduled with varying numbers of participants in each. Due to the concerns linked with the Covid-19 pandemic, it was decided that measures needed to be taken and a maximum of 4 individuals, excluding the researcher, could play at once. In a perfect world, the participants would have already learned some of the terms in a previous training session, to counter this, the researcher was present during the sessions to define each term, discuss good and bad security practices, and respond to any queries the participants might have. Participants played both gameplay styles during the hour-long sessions, and if they were picking up the concept rapidly, the difficulty level was gradually increased.

B. Feedback

After completing the play testing sessions, the participants then completed Questionnaire 2 to provide feedback on the mechanics of the game. Feedback from participants indicated that they had a positive experience and gave a positive review of the game design. Participants also proposed some modifications that may be made to the game to allow for even more learning opportunities:

"Adding the validation of winning the pair of cards increases confidence. Could maybe race against the clock in the second round."

"Add harder cards in gradually when replaying the game for a second time as we were more confident"

"Playing multiple rounds of the game adapting it to different methods such as switching around which cards are seen first"

Participants also commented that the information on the cards was appropriate, but the text may be easier to read if the cards were larger. The game initially seemed confusing to the participants, but after they got going, they found it to be quite simple to understand. The process flows from Figs. 3 and 4 may have been presented on an information sheet with rules to help avoid this initial confusion.

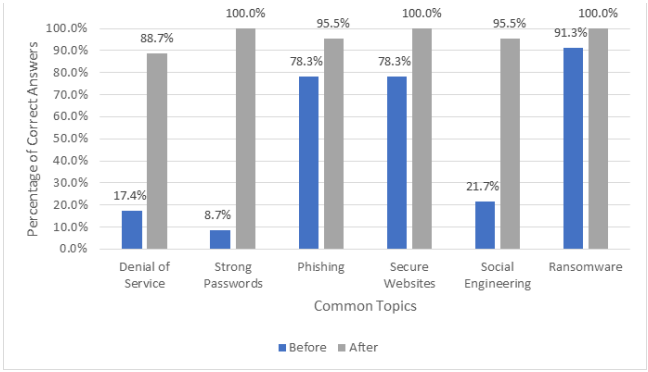

Fig. 5. **Comparison of Topics**

Participants were then evaluated on the subjects they had learned while playing the game in Questionnaire 3 which was distributed to them at least five days after their play testing session. This test has an average score of 92.8%. Comparing this to Questionnaire 1, the average score has increased by 43.7%. The artefact can be deemed to have had a considerable beneficial impact on the participants' recall of cyber security information because this is close to a 50% improvement in average score. There were some common subjects that were explored between questionnaires 1 and 3. The average score for each of the topics both before and after the game is displayed in Fig. 5 above. The topic about strong passwords saw the largest increase, going from 8.7% to 100%. This rise in correctly answered questions for the topics under test shows that the artefact was effective in

helping participants understand and remember the game's material.

C. Limitations

One limitation is the sample size as only 23 participants took part in the research. Although the number allowed reasonable feedback, a larger sample size would provide more reliable results, increase the validity of the research, and have a lower percentage of potential outliers.

Another limitation is on the retention test. The retention test was given to participants and completed five days after the play testing sessions. This does provide time for participants to potentially forget newly learned information, as shown in the Forgetting Curve [10][11], however, completing multiple retention tests over a period of months could lead to a more in-depth understanding of what topics were retained in the long term.

VII. Conclusion and Future Work

This study described the development of a prototype game focused on cybersecurity. The proposed game contains two play methods to provide for a variety in learning processes, and it can be modified based on the players' knowledge. The work is a step towards solving the human as the weakest link in cybersecurity [18] and that the existing cyber security training is not sufficient as it does not promote successful knowledge retention.

A. Future Work

This study is the preliminary work required for a larger scale future study. The game was designed based on the use of physical cards as specified by study participants, however, an online version of the game could be designed to allow for remote play, as some players may not be able to meet in person. By adding this, more people will be able to play the game thus turning it into an e-learning tool. In this iteration, QR codes were included to the card design but were not fully developed. The addition of an external online source via the QR codes for extra reading is a future development consideration. Players could increase their expertise at their own pace in this way.

Augmented reality is another topic worth considering. Studies on the connection between augmented reality and workplace training, for instance, Herbert and colleges' paper "Cognitive load considerations for Augmented Reality in network security training" [20], examined how augmented reality could help beginners by up to 25% in improving knowledge retention. The QR codes on the card design might be replaced by augmented reality, enabling a more engaging game by adding more visual aids to learning through the augmented reality technology and therefore presenting visual scenarios to players which could more accurately replicate a real world situation.

References

[1] Aldawood, H., and Skinner, G., 2018. Educating and Raising Awareness on Cyber Security Social Engineering: A Literature Review [online]. In: IEEE International Conference on Teaching, Assessment and Learning for Engineering (TALE), Wollongong 4-7 December 2018. ieeexplore.ieee.org: IEEE. 62-68. Available from: https://ieeexplore.ieee.org/xpl/conhome/8600698/proceeding

[2] Hendrix, M., Al-Sherbaz, A., and Bloom, V., 2016. Game Based Cyber Security Training: are Serious Games suitable for cyber security training? International Journal of Serious Games [online], 3 (1), 53-61.

[3] Marousis, A., 2021. Cybersecurity training lags, while hackers capitalize on COVID-19 [online]. Available from: https://www.talentlms.com/blog/cybersecurity-statistics-survey/#How_much_do_employees_actually_know_about_cybersecurity [Accessed 2 February 2022].

[4] Bada, M., Sasse, A., and Nurse, J. R. C., 2015. Cyber Security Awareness Campaigns: Why do they fail to change behaviour? [online]. Available from: reearchgate.net

[5] Ki-Aries, D., and Faily, S., 2017. Persona-centred information security awareness. Computers & Security [online], 70, 663-674.

[6] Abawajy, J., 2012. User preference of cyber security awareness delivery methods. *Behaviour & Information Technology* [online], 33 (3), 237-248.

[7] Denning, T., Lerner, A., Shostack, A., and Kohno, T., 2013. Control-Alt-Hack: the design and evaluation of a card game for computer security awareness and education [online]. In: CCS '13: Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security, Berlin 4-8 November 2013. dl.acm.org: Association for Computing Machinery. 915-928. Available from: https://dl.acm.org/doi/proceedings/10.1145/2508859

[8] NCSC, 2020. *Cyber Aware*. Available from: https://www.ncsc.gov.uk/cyberaware/home [Accessed 27 February 2022].

[9] Bennett, A. G., and Rebello, N. S., 2012. Encyclopedia of the Sciences of Learning [online]. 2012 edition. Boston: Springer.

[10] Murre, J. M. J., and Dros, J., 2015. Replication and Analysis of Ebbinghaus' Forgetting Curve. PLoS ONE [online], 10 (7).

[11] Ebbinghaus, H., 1885. Memory: A Contribution to Experimental Psychology [online]. Available from: https://psychologie.lw.uni-leipzig.de/wundt/opera/ebbing/memory/GdaechtI.htm

[12] ProductPlan, ca 2022. MoSCoW Prioritization [online]. Available from: https://www.productplan.com/glossary/moscow-prioritization/ [Accessed 4 March 2022].

[13] AAT, 2019. STRIDE: Acronym of Threat Modeling System [online]. Available from: https://allabouttesting.org/stride-acronym-of-threat-modeling-system/ [Accessed 27 April 2022].

[14] Khan, R., McLaughlin, K., Laverty, D., and Sezer, S., 2017. STRIDE-based Threat Modeling for Cyber-Physical Systems [online]. In: IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT Europe), Turin 26-29 September 2017. ieeexplore.ieee.org: IEE. 1-6. Available from: https://ieeexplore.ieee.org/xpl/conhome/8246021/proceeding

[15] Donovan, F., 2021. What is STRIDE and How Does It Anticipate Cyberattacks? [online]. Available from: https://securityintelligence.com/articles/what-is-stride-threat-modeling-anticipate-cyberattacks/ [Accessed 3 March 2022].

[16] RainbowFun, ca 2022. Orchard Toys - Shopping List Game [online]. Available from: https://www.rainbowfun.com.au/orchard-toys-shopping-list-game [Accessed 25 March 2022].

[17] Whitcoulls, ca 2022. Sherlock Memory Card Game [online]. Available from: https://www.whitcoulls.co.nz/product/sherlock-memory-card-game-6597607 [Accessed 25 March 2022].

[18] Chouhan, Y. A., Liu, L., Li, T., and Fatima, R., 2019. Improving software security awareness using a serious game. IET Software Special Issue: Gamification and Persuasive Games for Software [online], 13 (2), 159-169.

[19] Adams, J., 1999. Risky Business: The Management of Risk and Uncertainty [online]. London: Admin Smith Institute. Available from: adamsmith.org

[20] Herbert, B., Wigley, G., Ens, B., and Billinghurst, M., 2022. Cognitive load considerations for Augmented Reality in network security training. Computers & Graphics [online], 102 (February 2022), 566-591.