information

Article

Design and Evaluation of an Augmented Reality Game for Cybersecurity Awareness (CybAR)

Hamed Alqahtani * and Manolya Kavakli-Thorne

Department of Computing, Macquarie University, Sydney 2113, Australia; manolya.kavakli@mq.edu.au
* Correspondence: hsqahtani@kku.edu.sa

Received: 12 January 2020; Accepted: 19 February 2020; Published: 21 February 2020

Abstract: The number of damaging cyberattacks is increasing exponentially due in part to lack of user awareness of risky online practices, such as visiting unsafe websites, ignoring warning messages, and communicating with unauthenticated entities. Although research has established the role that game-based learning can play in cognitive development and conceptual learning, relatively few serious mobile games have been developed to educate users about different forms of cyberattack and ways of avoiding them. This paper reports the development of an effective augmented reality (AR) game designed to increase cybersecurity awareness and knowledge in an active and entertaining way. The Cybersecurity Awareness using Augmented Reality (CybAR) game is an AR mobile application that teaches not only cybersecurity concepts, but also demonstrates the consequences of actual cybersecurity attacks through feedback. The design and evaluation of the application are described in detail. A survey was conducted to verify the effectiveness of the game received positive responses from 91 participants. The results indicate that CybAR is useful for players to develop an understanding of cybersecurity attacks and vulnerabilities.

Keywords: augmented reality; cybersecurity awareness; game-based learning; gamification

1. Introduction

The past decade has witnessed phenomenal growth in cybercrime, including phishing, financial fraud, identity theft and denial of service. In November 2018, the personal data of up to 500 million people were stolen due to a hack on Marriott International [1]. Two months earlier, press accounts reported that British Airways had experienced a data breach involving the personal and financial details of almost 400,000 customers, while in the previous month hackers swiped the data of 2 million subscribers from T-Mobile [1].

Many security breaches are due to users' lack of knowledge about unsafe behaviour, such as sharing passwords, opening attachments from unknown emails, and running untrustworthy software or applications. It is therefore vital that individuals become knowledgeable about cybersecurity through appropriate training in how to protect themselves in cyberspace.

Although numerous organisations have installed technology-oriented safeguards such as firewalls and intrusion detection systems, less attention has been paid to the human factors in cybersecurity [2]. Most users of computers and mobile devices lack awareness of cybersecurity due to inadequate education and training [3]. Yet, according to many researchers, the human factor is the key to cybersecurity [4,5]. Al-Janabi and Al-Shourbaji in [6] analysed cybersecurity awareness among academic staff, researchers, undergraduate students and employees in the education sector in the Middle East. The results revealed that the participants did not have the required knowledge and understanding of the importance of cybersecurity principles and their practical application in daily life. Such findings highlight the importance of educating individuals in how to protect themselves when using online services.

The information systems literature shows that awareness techniques are effective in improving users' cybersecurity-related knowledge and promoting cybersecurity-conscious decision-making [7], therefore protecting them against cybersecurity attacks. Many organisations provide their employees with information on how to defend against cybersecurity attacks in the form of email bulletins or information security websites [8]. However, these types of materials only work if people pay attention to them, and some researchers have recommended that cybersecurity awareness may be more effectively created through specially developed mobile games applications [9].

Mobile games are played by millions of adolescents and adults around the world [10]. They are highly diverse in relation to their purposes, interactivity and technology. Quality mobile games have been shown to improve concentration [11], enhance retention of information [12] and bring about behavioural change [13]. Over recent decades, mobile games—both serious games and gamification—have been designed for serious purposes: to educate, motivate and persuade users in health, educational and other settings [14]. Serious games use gaming as the primary medium [15], whereas gamification involves the addition of game elements to non-game contexts. The potential for employing serious games and gamification to educate users about cybersecurity has been under-researched.

A small number of games to promote cyberattack awareness have been developed to better engage learners and change user behaviour. It has been claimed that well-designed games for user education can effectively mitigate cyberthreats [16]. Examples of such games include CyberCIEGE and antiphishing gaming tools. Most of these games, however, are technically oriented and, more importantly, are limited to web-based games. Although evaluations of these games have demonstrated an improvement in players' ability to identify phishing websites, their designs are not particularly effective at teaching players how to detect other forms of cybersecurity threat such as identity theft, ransomware and phishing through social media networks.

Accordingly, we developed a game that incorporates all potential cyberattack techniques and provides a more engaging experience for the acquisition of practical and conceptual knowledge. CybAR is a Mobile Augmented Reality (MAR) that increases awareness of safe cybersecurity practices in an enjoyable, competitive environment. Although MAR applications are currently used in various domains [17–19], their potential for educating people about cybersecurity threats and promoting safe cybersecurity behaviour has been relatively less explored.

CybAR is a MAR-based serious game consistent with the situated learning theory [20], which advocates that learning is more effective through collaborative authentic problem solving, in the natural environment where the constructed knowledge is used [21]. CybAR game supports the mixture of modern pedagogical approaches (e.g., constructivist, game-based, inquiry learning) for the creation of authentic learning experiences, which enables participants to form their own learning paths, to engage, and to interact meaningfully via digital narrative and virtual (role) identities [22]. For this purpose, CybAR employs quizzes and was developed using the Vuforia engine in Unity on the android platform.

The main characteristics of the proposed AR game are to provide interactivity and display the disastrous consequences of careless cybersecurity habits. The user is trained through an engaging series of gamified tasks designed to educate them about important cybersecurity related concepts through an interactive user interface. Each task requires players to make the correct choice to avoid cyberthreats. The tasks are based on real cybersecurity case studies collected at Texas A & M University. Unlike computer games such as CyberCIEGE [23] and What.Hack [16], CybAR is a competitive game focusing on high-level user behaviours, rather than on detailed technical knowledge of system software, with the aim of providing both conceptual and procedural knowledge about cyberthreats. CybAR challenges each user to collect points while engaging in cybersecurity practices and avoiding cybersecurity missteps. CybAR teaches several cybersecurity concepts to train users to stay safe online. It tests the ability of users to recognise spoofed emails, SMS phishing, scam phone calls, identity theft, ransomware and phishing through social media networks. It teaches users to avoid clicking on unsafe links, and to authenticate software downloads, perform integrity checks of system software, keep antivirus protection up-to-date and choose strong passwords. In CybAR, we applied learning principles, such as quizzes, to optimise the learning effect. Gamification elements, including clear goals, points, achievements, feedback and leaderboards, were also incorporated to increase motivation. We followed a user-centred design, including an initial survey to ascertain users' preferences with regard to an educational app. Key elements of the CybAR game interface were selected based on Technology Threat Avoidance Theory (TTAT) [24,25] to enhance user interaction used in [26].

To test the effectiveness of the CybAR game for cybersecurity education, an experimental study was conducted among students at Macquarie university. The results showed that 91 participants indicated that the game was engaging and increased awareness of cybersecurity practices. It can be concluded that this innovative pedagogical method makes cybersecurity concepts more accessible to students.

2. Literature Review

There is no widely accepted definition of cybersecurity [27]. Kassicieh et al. [28] define cybersecurity as a set of approaches that protect data, systems and networks from cyberattacks. The United States Army defines cybersecurity as a combination of the underlying hardware, communication nodes and a social layer of human and cognitive elements. According to Dhamija et al. [2], the general public's lack of awareness of cybersecurity means that hackers can efficiently and effectively target users. Therefore, user education is vital to protect against cyberattacks. Cybersecurity awareness involves assessing users' vulnerabilities while providing knowledge about how to detect and avoid cyberattacks. Materials widely used for cybersecurity training include notes, videos and email bulletins. However, these materials are often not very engaging and separate the learning material from the context in which users routinely apply the information [9]. Automated tools have largely failed to mitigate cybersecurity attacks: even the best antiphishing tools have been found to miss more than 20% of phishing attempts [29]. This situation is exacerbated by the fact that most systems depend on humans to make sensitive trust decisions during their online activities [30]. Accordingly, there has been a shift in thinking about the best ways of combating cybercrime to emphasise creating awareness and encouraging individuals to adopt better cybersecurity practices [31], including gamified approaches to educate users and improve their threat avoidance behaviour. Gamification shows promise as a technique to enhance the effectiveness of cybersecurity awareness programs, and several cybersecurity games have been developed to engage users better and change their behaviour to avoid cyberattacks [32].

Gamification emerged as a concept of interest in the field around 2010 [33,34]. Several researchers have demonstrated multiple benefits from cybersecurity games such as Control-Alt-Hack, Protection Poker, CyberCIEGE, Anti-Phishing Phil and What.Hack [16]. A few games have been designed to teach cybersecurity concepts. For example, Control-Alt-Hack [35] is a board game that teaches players about high-level security concepts such as phishing and social engineering. Although this does help to increase awareness and understanding of cybersecurity issues as a whole, it is not sufficiently specific to imitate the low-level decisions required for antiphishing strategies in practical contexts. Protection Poker is a software security game designed to help software development teams estimate risks and prevent most damaging attacks [36]. CyberCIEGE presents a virtual world interface that mimics the role of a network manager in safeguarding the network with a limited budget [23]. Capture-The-Flag (CTF) is a game-based computer security competition for students to practise the skills necessary to defend against hackers [37]. In general, board games in information security do not teach hands-on security skills, such as how to define cybersecurity attacks, which are the main purpose of our game.

Recently, new designs for antiphishing games [26,29] have drawn inspiration from the popular framework for antiphishing training to teach users how to prevent computer system and network settings from being compromised. Anti-Phishing Phil and What.Hack online games were developed to challenge players to recognise real-life phishing URLs and emails in an entertaining way. These games have two main limitations: First, they only focus on phishing attacks and neglect other forms of cybersecurity risk, leaving players vulnerable to content-based attacks such as social engineering, identity fraud and social media scams. Therefore, one of the main aims of CybAR was to provide more comprehensive education about cybersecurity attacks and to do so in a way that closely matches how they occur in the real world. Second, their design fails to incorporate design elements from well-known information system theories.

Augmented Reality (AR) has also recently emerged as a technology that can enhance users' experience by overlaying computational information onto their reality. Azuma [38] defines augmented reality as "An interactive experience of a real-world environment where the objects that reside in the real world are enhanced by computer-generated perceptual information, sometimes across multiple sensory modalities, including visual, auditory, haptic, somatosensory and olfactory." Despite the popularity of AR applications in various fields, such as education, marketing, medicine and tourism [19], no previous AR-based application has been developed to educate users about cybersecurity attacks and raise their cybersecurity awareness.

Serious games are also effective training tools for educating the users. Serious games are goal-oriented games rather than purely for entertainment and have been effectively deployed to achieve behavioural change in school education; healthcare; advertising; and, recently, in cybersecurity [39]. The game-based approach motivates players to move towards the goal using the appropriate actions and allows them to observe the consequences of failure to do so without incurring real-life costs. Compared to traditional training methods, game-based approaches are more engaging, relatively cost-effective, easily transferrable to a large number of trainees and customised to each player [40].

The effectiveness of these games suggests that a mobile-based application focused on raising cybersecurity awareness would be a useful tool. Thus, we develop an effective augmented reality (AR)-based serious game called CybAR, which is designed to increase cybersecurity awareness and knowledge in an active and entertaining way. The Cybersecurity Awareness using Augmented Reality (CybAR) game is an AR mobile application that teaches not only cybersecurity concepts but also demonstrates the consequences of actual cybersecurity attacks through feedback. CybAR's design considers safeguard effectiveness, perceived susceptibility and other elements derived from Technology Threat Avoidance Theory (TTAT) [24], as shown in Figure 1. The goal of CybAR is to educate a less technically sophisticated audience to increase their awareness of the potential for cybersecurity attacks in their day-to-day online behaviour based on these elements from TTAT, rather than to teach specific technical or management skills.

3. CybAR Game Development

3.1. Game Design Framework

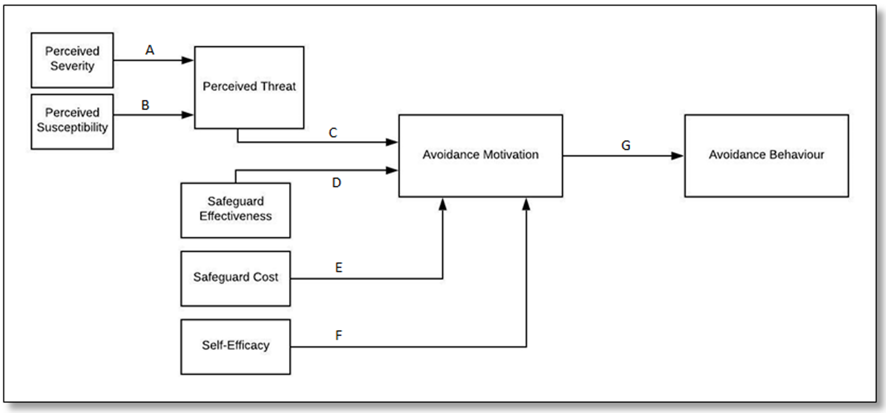
The aim of the work reported in this paper was to develop a game design that improves users' avoidance behaviour by motivating them to protect against cybersecurity attacks. A theoretical model derived from Technology Threat Avoidance Theory (TTAT) was used to develop the game design framework, which is shown in Figure 1 [25].

TTAT describes individual users' behaviour to avoid the threat of cybersecurity attacks. Consistent with TTAT, the user's threat avoidance behaviour is identified by avoidance motivation. Important determinants of avoidance motivation include Perceived threat, Safeguard effectiveness, Safeguard cost and Self-efficacy. Perceived threat is affected by perceived severity and susceptibility.

Although the proposed framework identifies the issues that the game design needs to address, it also suggests how information (content) should be structured and presented in a game context. Therefore, a mobile game design based on this theoretical framework should meet the requirements shown in Table 1, which contains a set of guidelines for designing an educational mobile game. The aim is to develop threat perceptions, making individuals more motivated to avoid cybersecurity attacks and use safeguarding measures.

Table 1. Requirements for game design.

Elements of the Game Design Framework	Game Design Sketch
Perceived Susceptibility: An individual's subjective probability that a cyber attack will negatively affect him or her [24,25].	Each task displayed in the game is associated with a potential cybersecurity threat which appears as a case study in the game. The game player's job is to perform the tasks correctly; each task performance is followed by immediate positive or negative feedback. This element of the game design addresses the user's awareness of susceptibility to the cybersecurity threat.
Perceived Severity: The extent to which an individual perceives that negative consequences caused by a cyberattack will be severe [24].	If the game player makes the incorrect decision, each wrong attempt loses one point out of a total of 20 points needed to complete the game. This develops awareness of the severity of the cybersecurity threat.
Perceived Threat: The extent to which an individual perceives the cybersecurity threat as dangerous or harmful [24,25].	The main goal of the game player is to avoid potential cybersecurity threats in real life, therefore he or she should be aware of the various ways in which hackers can operate. This represents the development of threat perception in the game design, and negative feedback shows the damaging consequences of hacking.
Perceived Safeguard Effectiveness: The individual's assessment of the potential effectiveness of a safeguarding measure against a cybersecurity threat [24,30].	If a player finds it difficult to identify if something is suspicious or not, the player can complete the task, learn the expected consequences and replay later. The feedback provides tips on how to identify cyberattacks. This element addresses safeguard effectiveness in the game design.
Perceived Safeguard Cost: This refers to the physical and cognitive costs, such as time, money, inconvenience and mental effort, required to use the safeguard measure [24,41].	When the game player scores less than 65%, he or she is asked to replay the game. This feature of the game design addresses the costs involved in the safeguard.
Self-Efficacy: Individuals' confidence in adopting the safeguard measure [24–26].	The game is designed to educate users in safe online behaviour. The player is with a series of tasks, each of which is associated with a different form of cybersecurity attack. As the player moves from task to task through the game, he or she gains conceptual knowledge of how to identify cyberthreats, thus helping to develop self-efficacy.



A - Perceived severity has a positive interaction with Perceived threat
B - Perceived susceptibility directly affects Perceived threat
C- Perceived threat motivates the users to avoid them
D & E - Effectiveness of safeguard and cost of safeguard are important elements for motivating users for adopting avoidance mechanism
F - Self-confidence for taking threat measures motivate users for adopting avoidance mechanism
G - Users' avoidance motivation leads to their avoidance behavior, which is taking safeguarding measures to reduce the threat.

Figure 1. Game design framework.

3.2. Game Concept

The design of the CybAR app includes a core set of game tasks that could easily be adapted and extended to other cybersecurity concepts. The game offers flexibility to create teachable moments that maximise the educational impact. The main characteristics that distinguish our game from some other cybersecurity awareness games are interactivity and the presentation of the damaging consequences of careless cyber habits. These features will effectively increase awareness and contribute to the development of a safer cybersecurity culture. This game focuses on the most common cyber vulnerabilities of individuals, such as lack of awareness about social engineering, use of weak or default passwords, URL manipulation, malicious attachment, two-factor authentication, identity fraud, sharing location services, ransomware, social networking scams/spam and use of outdated apps and public Wi-Fi.

The design of CybAR relies on components derived from a theoretical model that are embedded in a task that simplifies the conceptual and procedural knowledge presented to the user by employing persuasive design principles through an interactive interface. It familiarises players with important cybersecurity attack phenomena through challenges (tasks) presented to them during the game.

To make the CybAR game more persuasive, we based its design on the knowledge model proposed by Conde-pumpido [42], which was adopted in [32]. This onion model, shown in Figure 2, has three spiral layers. The inner layer relates to visual, linguistic, haptic and sound signs. The middle layer includes scripts and scenes that enhance the persuasiveness of the game. The outer layer refers to the persuasiveness of the setting or context of the CybAR game. We utilised visual persuasion to satisfy the first layer. As it is an AR game, other types signs, such as sound and linguistic signs, were included, which was not possible in [32]. We employed narrative and procedural persuasion for the second layer and tactical and affective persuasion for the third layer.

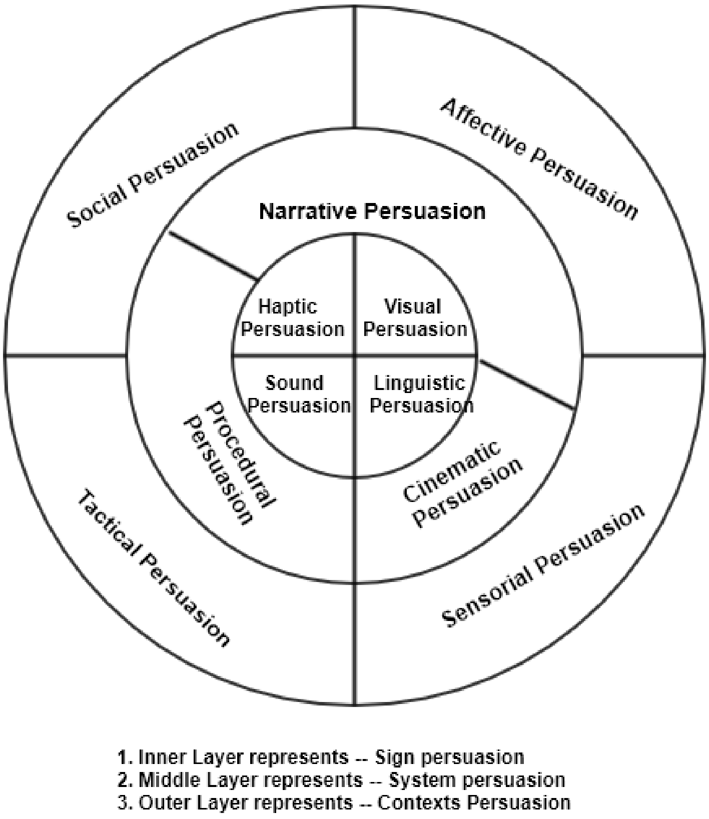


Figure 2. Knowledge model for CybAR game.

In the CybAR game, conceptual and procedural knowledge interact in mutually supportive ways via an iterative process [43]. Each task is associated with three options (decisions) and can be performed either correctly or incorrectly. As the player moves through the game, the diversity of the tasks is apparent. This helps to develop procedural knowledge of different tasks. Each task is in question and answer format. When the player moves through the game, options assigned to each task are checked. In this process, the player learns the different patterns of cybersecurity attacks. This helps to develop conceptual knowledge of different tasks. The game design also includes specific procedural tips that appear after each task, such as "Don't share your password with anyone. Use strong, unique passwords on your accounts (see Figure 3a)." This aspect of game design addresses conceptual-procedural knowledge of cybersecurity threats.

4. Game Description

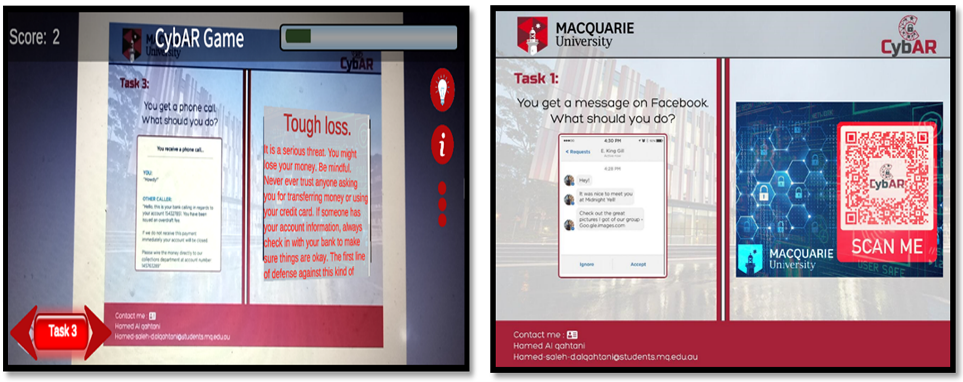
4.1. Use Case

Layla is a 22-year-old graduate student in psychology and is not very computer savvy. She is extensively engaged in social networking activities such as posting, commenting on friends' posts, liking and so on. She is always online and has downloaded many apps on her mobile phone, which she uses and enjoys. Layla considers herself a lazy computer user as she never updates the apps on her computer or mobile device. She frequently forgets the passwords she creates so she has decided to use two simple passwords that she can remember. She is also constantly online chatting, sharing stories or discussing issues. Layla's days are very busy, and she does not have much time to do things like improving her computer skills. She recently dealt with a phishing attack where she clicked on an email that ultimately infected her computer. She lost a lot of data and was forced to reformat her computer. Despite this incident, she still struggles to back up her computer, protect her account, update her applications or even check her bank account statements. Recently, one of her friends was the victim of a ransomware attack, which proved very costly. Layla knows she should protect her data and computer access after these serious incidents, but she does not know exactly what she needs to do. She started reading about cybersecurity attacks, and she is now aware of the importance of cybersecurity awareness, as promoted by different sources of media and cybersecurity awareness campaigns. However, she still does not practise safe cybersecurity behaviour. Walking around the Macquarie University campus one day, she sees a poster about an AR game called CybAR. She decides to download the mobile app because she is interested in playing mobile games. She then starts scanning the poster using the CybAR app and the AR content appears on the poster showing important materials related to cybersecurity. She is amazed because this is her first experience of interactive AR content. The game shows her different forms of cyberattack. She starts playing the game and receives a different score at each attempt. She continues to play to achieve the highest score to win the game. She finds that her best score is not in the top ten, so she tries again to beat the other gamers. Eventually she succeeds. By that time, she has been exposed to the AR cybersecurity content and her game playing has positively changed her intention toward cybersecurity attacks. In this way, the CybAR app helps her to develop and practise safe cybersecurity habits.

4.2. Tasks

The CybAR game contains 20 tasks. Each task is designed to provide players with a challenge in relation to one form of potential cybersecurity threat and engage them in the activity by providing interactive answers and feedback. We cover several common cybersecurity threats including cybersecurity fundamentals such as phishing, ransomware and WiFi security, password creation, use of data protection such as virtual private networks (VPNs) and file backups and best practice in relation to activities such as social media sharing.

We chose the specific cybersecurity threats by first examining respected cybersecurity awareness websites such as Accellis Technology Group and Texas A & M University to identify the most common cyberthreats. The feedback content was chosen based on reports from cybersecurity awareness programs conducted at SANS Institute. Following consultations on our findings with professionals in the Cyber Hub at Macquarie University, we identified 20 threats that represent today's pervasive threats. An example of the tasks is shown in Figure 3b.



You get a phone call. What should you do?

You receive a phone call..

YOU: "Howdy"

OTHER CALLER: "Hello, this is your bank calling in regards to your account 154327851. You have been issued an overdraft fee.

If we do not receive this payment immediately your account will be closed.

Please wire the money directly to our collections department at account number 145763289"

Tough loss.

It is a serious threat. You might lose your money. Be mindful. Never ever trust anyone asking you for transferring money or using your credit card. If someone has your account information, always check in with your bank to make sure things are okay. The first line of defense against this kind of

Contact me:
Hamed Al qahtani
Hamed-saleh-d.alqahtani@students.mq.edu.au

You get a message on Facebook What should you do?

4:30 PM
< Requests E. King Gill
4:28 PM
Hey!
It was nice to meet you at Midnight Yell!
Check out the great pictures I got of our group - Goo.gle.images.com

Contact me:
Hamed Al qahtani
Hamed-saleh-d.alqahtani@students.mq.edu.au

(**a**) (**b**)

Figure 3. (**a**) Feedback after making a wrong decision. (**b**) Example of CybAR Task.

4.3. Mobile Game Design

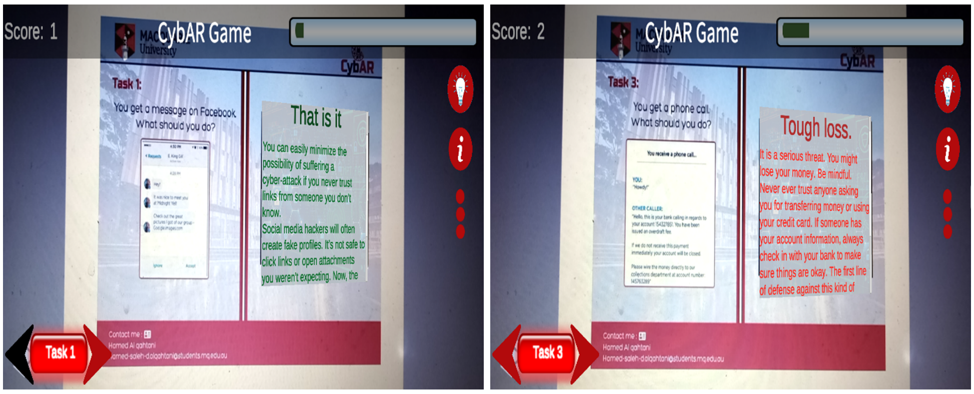
Because our aim was to create a user-centred and interactive interface for CybAR, we conducted a focus group to identify key components that needed to be addressed in the design. This was done to ensure that users' preferences were included during the design process to maximise user interaction. After all, users will only learn about cybersecurity concepts if they enjoy playing the game, and interaction is essential to enhancing awareness. We invited 10 individuals from Macquarie University aged 22 to 37 to share their opinions about how the game should be designed. All the participants had been using smartphones for at least 6 years. They were provided with a description of the CybAR game before the discussion, during which they were encouraged to describe how they visualised the design and flow of the game. The moderator asked specific questions about the look and feel of the CybAR game to elicit ideas for representing its features and the training elements. Analysis of the data from the focus group identified the following components that needed to be incorporated into the game design:

- **Rules:** Rules organise the game. Each task was based on rules derived from the game design framework (TTAT). The participants were unanimous in their opinion that the game, while being educational and aiming to spread awareness of cybersecurity attacks, should have an evolving format that would keep the player engaged.
- **Goals and objectives:** Goals and objectives are what the player works to achieve. The goal is to perform all tasks correctly. This is reflected in the game design by providing three options (one correct, two false) for each task.

  An important aspect of cybersecurity training is teaching learners to appreciate the risks of a bad decision. Existing training materials often describe these as high-level risks, but do not really show the learner what will happen if something goes wrong. Therefore, CybAR simulates how the player's decisions lead to various outcomes, both positive and negative. If the player makes a wrong decision, a violation feedback will appear, as shown in Figure 2. Similarly, if the player thinks an unsafe email is a phishing email, the immediate feedback will be that that this decision is correct. This approach helps players reflect on unfamiliar cyberattacks, which helps retain knowledge.
- **Outcome and feedback:** Outcome and feedback measure progress against goals. The user obtains feedback on the current status in the game. The feedback provides timely opportunities to explain

consequences and deliver information. This ability to provide players with immediate and specific feedback based on their decisions optimises learning by explaining how their errors occurred and how their expectations failed [44]. Players also receive positive feedback when they make sound cybersecurity choices.

In each task, we apply protection motivation theory [45] in immediate feedback when players accomplish the task. Two PMT-inspired guidelines are designed to trigger more secure behaviour after the task has been completed: If the task is performed correctly, a coping message appears telling the user it is easy to minimise the chances of cyberattacks by making the right decision for the task. For example: "GOOD JOB! It was easy to neglect such tweets because you are aware of cyberattacks. Fake social media profiles are easily created by scammers." If the task is performed incorrectly, a message warns users that their action could leave them vulnerable to cyberattacks. For example, "Oops. That was not a legit pop up and your account has been hacked" (see Figure 4).



Task 1:

You get a message on Facebook. What should you do?

Hey!

It was nice to meet you at Midnight Yell

Check out the great pictures I got of our group - Googleimages.com

Ignore Accept

That is it

You can easily minimize the possibility of suffering a cyber-attack if you never trust links from someone you don't know.
Social media hackers will often create fake profiles. It's not safe to click links or open attachments you weren't expecting. Now, the

Contact me :
Hamed Al qahtani
Hamed-saleh-d.alqahtani@students.mq.edu.au

Task 3:

You get a phone call. What should you do?

You receive a phone call...

YOU:
"Howdy!"

OTHER CALLER:
"Hello, this is your bank calling in regards to your account 15432785. You have been issued an overdraft fee.

If we do not receive this payment immediately your account will be closed.

Please wire the money directly to our collections department at account number 145763289"

Tough loss.

It is a serious threat. You might lose your money. Be mindful. Never ever trust anyone asking you for transferring money or using your credit card. If someone has your account information, always check in with your bank to make sure things are okay. The first line of defense against this kind of

Contact me :
Hamed Al qahtani
Hamed-saleh-d.alqahtani@students.mq.edu.au

(**a**) (**b**)

Figure 4. (**a**) Correct answer feedback. (**b**) Wrong answer feedback.

- **Rewards:** These are addressed in the mobile game design as the opportunity to gain points. The game should incorporate a rewards mechanism to incentivise players and keep their engagement levels high by rewarding them for their performance in the game. In CybAR, rewards are available by completing each task correctly and learning about cybersecurity-related concepts. If the user identifies all decisions correctly while avoiding all incorrect decisions, the player is awarded 20 points (for each attempt it is possible to score 1 point). If the user makes the wrong decisions, each attempt loses one point out of the total points remaining to complete the game. Participants can play the game as many times as they wish until they achieve a winning score. They can continue to play until their score is in the top ten on the leaderboard. If a player's score is less than 65% (13 points out of 20), he or she is encouraged to replay the game to learn how to be safe online.
- **Interaction:** Interaction is the social aspect in the game design. This is accomplished by providing immediate feedback, a progress bar and scores. Players are able to view their progress. According to the focus group participants, the player's progress should be contextualised in relation to the remaining game threats to convince them that successfully completing the game is an achievable target. They also recommended that players should not feel they were navigating away from the game when feedback was provided.

5. Implementation and Development Cycles

We implemented CybAR with two main sets of components—front-end and back-end. The back-end is the server software running the game, whereas the front-end is a client's mobile phone running the CybAR game.

Back-end component. CybAR is hosted on a dedicated server. The server runs a LAMP stack (Linux, Apache, MySQL and PHP). The back-end component is hosted on a Linux virtual machine. It consists of HTTP handlers, which deal with all requests from the front-end components; CybAR MySQL DB, which contain user profiles, tasks and play data; CybAR Admin Portal, through which the administrator of the CybAR app can update some of the content and see a range of information about the app; and the File Resources Directory, which stores all the photos and videos used by the app.

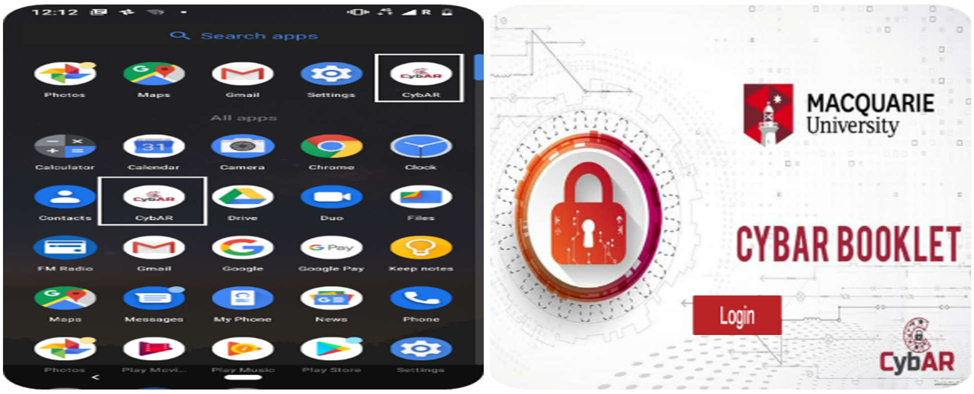
Front-end component. The CybAR application was developed for Android devices. Android is an open source mobile operating system (OS) developed by Google. The CybAR application was built using the game engine Unity3d which supports cross-platform development; therefore, different platforms can be targeted in future studies. Vuforia SDK was used to build the AR functionality. The CybAR game can be downloaded via Google Play Store.

5.1. Development Cycles

We paid particular attention to evaluation throughout the creation and development of CybAR. Each step of the game development cycle was iterative, alternating focus on appearance and interface with new game features. For example, the first version was tested by 10 participants during the design stage at Macquarie University. Student feedback included requests for a greater variety of cybersecurity concepts, increased speed, and better graphics. The second development cycle focused on the visual appearance of the game, including images for all tasks. We also added short video materials to increase users' knowledge of cybersecurity. The final version was more formally evaluated using usability testing.

5.2. User Interfaces

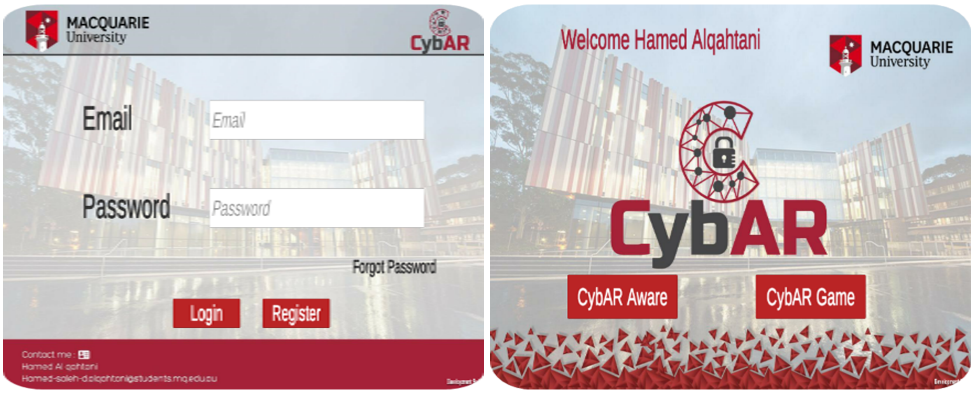
This section illustrates interface for the CybAR app. A successful installation of CybAR app will result to access the app interface presented Figure 5 with login interface depicted in Figure 6a.



(**a**) (**b**)

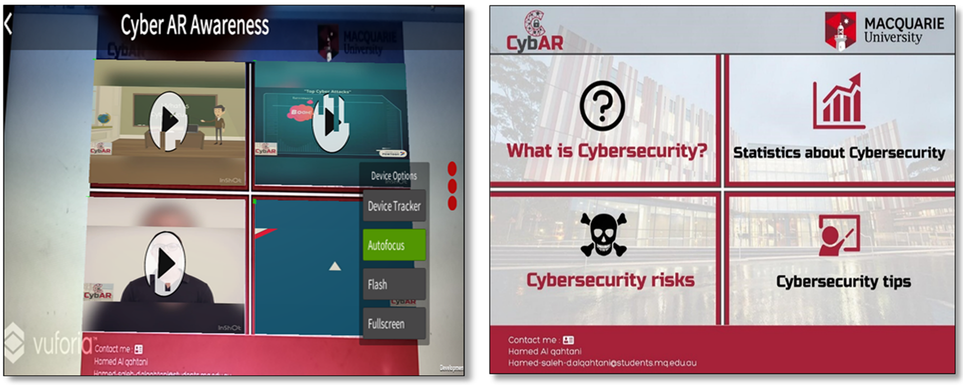
Figure 5. (**a**) CybAR app. (**b**) CybAR home UI.

New users are required registration for login into CybAR app. After logging into CybAR app, users are allowed to access cybersecurity awareness materials (Figure 6) as cybersecurity videos. The awareness materials can also be accessed by using mobile camera view to recognise the study marker as depicted in Figure 7.



(**a**) (**b**)

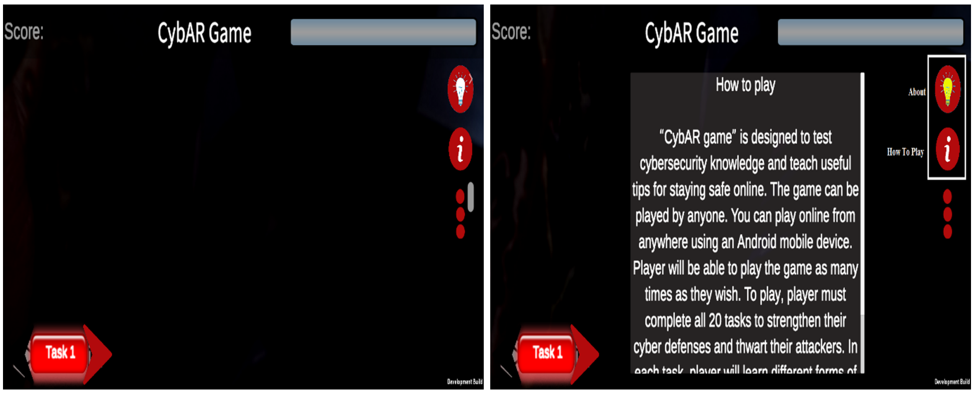
Figure 6. (**a**) CybAR app. (**b**) CybAR login UI.



(**a**) (**b**)

Figure 7. (**a**) CybAR awareness materials. (**b**) CybAR awareness materials marker.

Users can access the CybAR game by clicking the CybAR game button (Figure 6b). Then, they are taken to the AR game UI (Figure 8a). The AR game UI contains two main options on the right of the screen: How to play and About buttons. When users click on the About and How to play buttons, some static information about the application is displayed (Figure 8b).



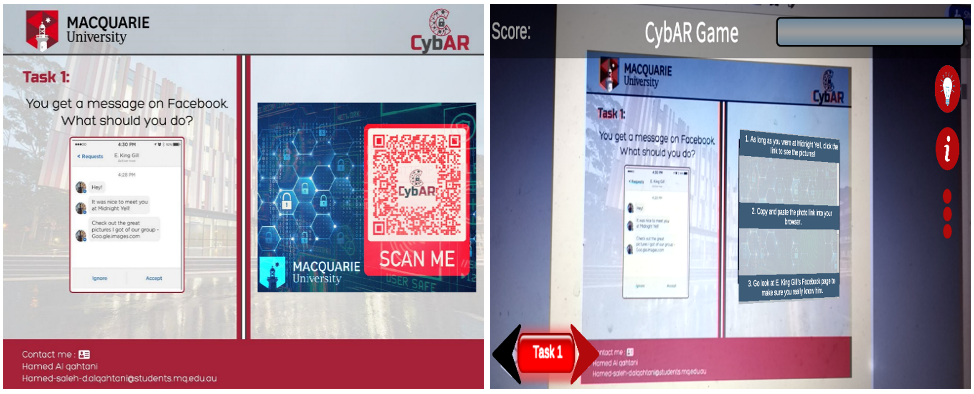
How to play

"CybAR game" is designed to test cybersecurity knowledge and teach useful tips for staying safe online. The game can be played by anyone. You can play online from anywhere using an Android mobile device. Player will be able to play the game as many times as they wish. To play, player must complete all 20 tasks to strengthen their cyber defenses and thwart their attackers. In each task, player will learn different forms of

(**a**) (**b**)

Figure 8. (**a**) CybAR Game UI. (**b**) CybAR Game About and How to play buttons.

Before players begin a CybAR game, they can access an electronic booklet that contains all 20 tasks. They can see the AR contents for each task by moving the camera on the target image inside the booklet. As shown in Figure 9a, users perform the first task by targeting the phone's camera on the SCAN ME QR code to view the answers and select the best option, as shown in Figure 9b. The user can move to the next task by pressing on the arrow in the bottom left corner (Figure 8a) after reading the task's instruction in the CybAR booklet. The user cannot move to the next task before the previous task has been completed.



Task 1:

You get a message on Facebook
What should you do?

Hey!

It was nice to meet you at Midnight Yell!

Check out the great pictures I got of our group - Goo.gle.images.com

Contact me :
Hamed Al qahtani
Hamed-saleh-d.alqahtani@students.mq.edu.au

1. As long as you were at Midnight Yell, click the link to see the pictures!

2. Copy and paste the photo link into your browser.

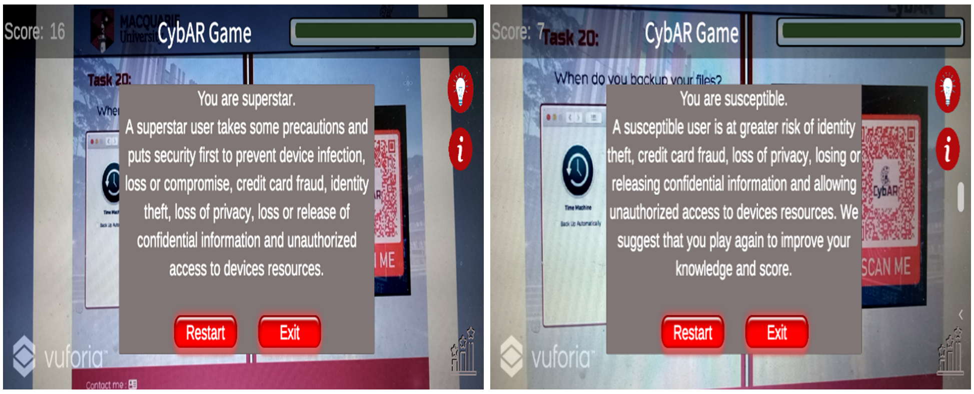
3. Go look at E. King Gill's Facebook page to make sure you really know him.

(**a**) (**b**)

Figure 9. (**a**) Example of CybAR task 1. (**b**) Example of CybAR task 2.

The score increases after the right decision for each task has been chosen, and the progress bar shows the game's progression (Figure 4a). The score will not increase if an incorrect choice is made (Figure 4b). The messages for correct and incorrect answers are displayed in green and red, respectively, accompanied by different sounds to increase engagement.

On completion of the game, one of two messages is displayed: an encouraging message if the player scores more than 13 points (Figure 10a), or a fear message that encourages the user to play the game again to avoid cyberattacks (Figure 10b). Both messages have two button options: Restart (which restarts the game) and Exit which takes the user to the main CybAR game interface (Figure 6b).



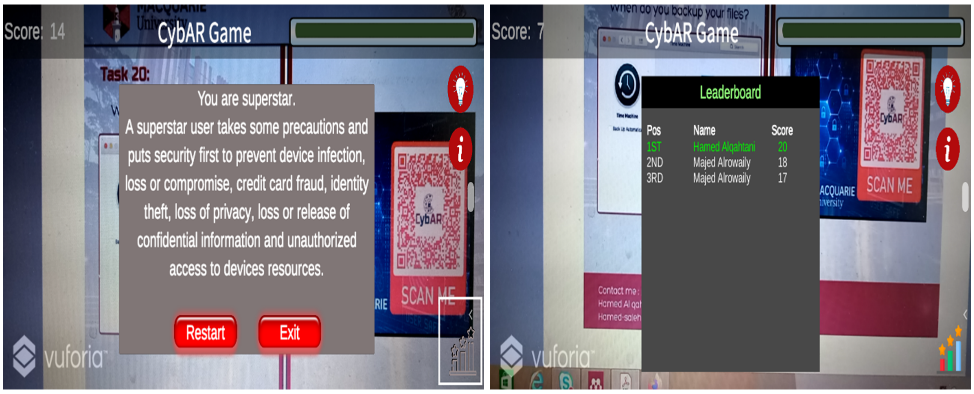
You are superstar.
A superstar user takes some precautions and puts security first to prevent device infection, loss or compromise, credit card fraud, identity theft, loss of privacy, loss or release of confidential information and unauthorized access to devices resources.

You are susceptible.
A susceptible user is at greater risk of identity theft, credit card fraud, loss of privacy, losing or releasing confidential information and allowing unauthorized access to devices resources. We suggest that you play again to improve your knowledge and score.

(**a**) (**b**)

Figure 10. (**a**) Final Message (Score > 13). (**b**) Final Message (Score < 13).

The Leaderboard button, which shows the top scores, is in the bottom right corner (Figure 11a). When the user presses this button, it shows the top ten users' highest scores (Figure 11b). Participants can play the game as many times as they wish until they achieve their best score or until their score is in the top ten in the leaderboard.



You are superstar.
A superstar user takes some precautions and puts security first to prevent device infection, loss or compromise, credit card fraud, identity theft, loss of privacy, loss or release of confidential information and unauthorized access to devices resources.

Leaderboard

Pos	Name	Score
1ST	Hamed Alqahtani	20
2ND	Majed Alrowaily	18
3RD	Majed Alrowaily	17

(**a**) (**b**)

Figure 11. (**a**) Leaderboard button. (**b**) Leaderboard (top scores).

6. Research Methodology

CybAR Evaluation

The primary aim of the CybAR game is to increase interest in cybersecurity and raise general awareness of cybersecurity attacks; therefore, CybAR helps users to understand appropriate and safe online behaviour. To evaluate the effectiveness of the developed cybersecurity education game, an invitation to participate in a study was disseminated via email and social media (FaceBook and Twitter) among students at Macquarie University. The eligibility criteria were that participants should be aged between 18 and 65 years and participation was voluntary. Those who accepted the invitation were asked to complete an online survey after using the CybAR game. The survey questions were adapted from a previously validated instrument in [32] and were carefully reviewed by academic experts at Macquarie University. Some amendments were made to the original questions to make the items more clearly related to our study. One item ("The game trains us working in team") was excluded because CybAR is a single-player game. The final 11-item questionnaire (Table 2) contained four demographic questions and seven questions requiring responses on a five-point Likert scale with anchors for strongly agree and strongly disagree. The survey aimed to assess features of the CybAR game such as clarity, content and enjoyment, to measure the effectiveness of CybAR in improving players' understanding of cybersecurity concepts and to estimate the extent to which it increased players' motivation. During the evaluation phase, participants were provided with an educational video explaining how to use the CybAR game.

Demographic information included gender, level of education, self-rating of cybersecurity knowledge (expert, good or poor) and awareness of cybersecurity attacks such as social engineering, phishing, ransomware, malware and identity fraud (very aware, neither aware nor unaware or very unaware).

Table 2. Survey Questions.

Item	Questions
Q1	CybAR game is an effective method of learning cybersecurity related concepts.
Q2	CybAR game helps me to learn more about cybersecurity attacks from mistakes.
Q3	CybAR game is a fun method of learning cybersecurity.
Q4	CybAR game has motivated me to learn more about cybersecurity.
Q5	CybAR game is easy to understand and play.
Q6	CybAR game mimics a real-life cybersecurity scenario in a presentable way.
Q7	I am motivated to play CybAR game in future.

7. Results and Analysis

The questionnaire was completed by 91 participants who were students at Macquarie University. The invitation letter included an explanation of the CybAR game to ensure that participants would be ready to engage with it as soon as the developer released the game in Google Play.

As shown in Figure 12, 59% of participants were male and 41% were female. The majority (45%) were studying for a bachelor degree, whereas 37% and 18% were Masters and PhD students, respectively (see Figure 12).

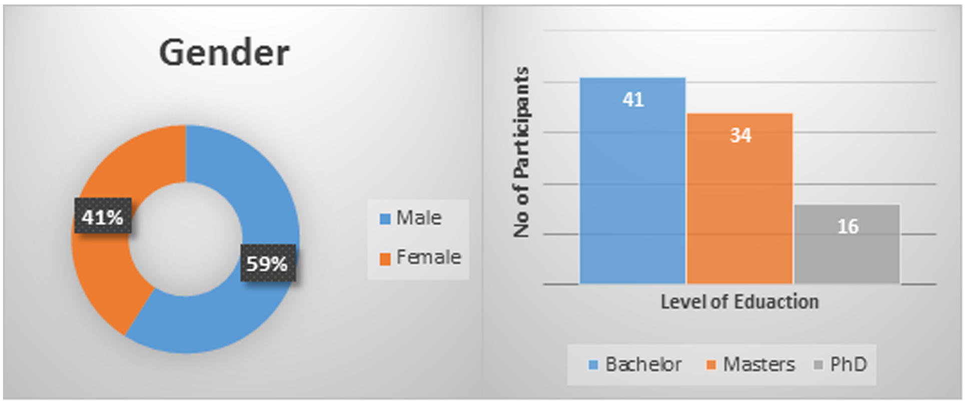


Figure 12. Gender and Level of Education Charts.

In relation to the item on cybersecurity knowledge, only 14 participants rated themselves as expert, whereas 37 and 40 participants chose good and poor, respectively, as shown in Figure 13. In other words, 44% of participants had poor prior knowledge of cybersecurity, 41% had good knowledge and only 15% rated themselves as expert (Figure 13). This finding that the majority of respondents did not consider themselves to have a good understanding of cybersecurity concepts is consistent with the results from previous research [46].

In relation to the item on awareness of cybersecurity attacks, 56% (51) of respondents were very unaware of cybersecurity attacks, and 30% (27) and 14% (13) were very aware or neutral, respectively (Figure 13) . As suggested in [33], this indicates an urgent need for a creative curriculum and pedagogical methods in cybersecurity education.

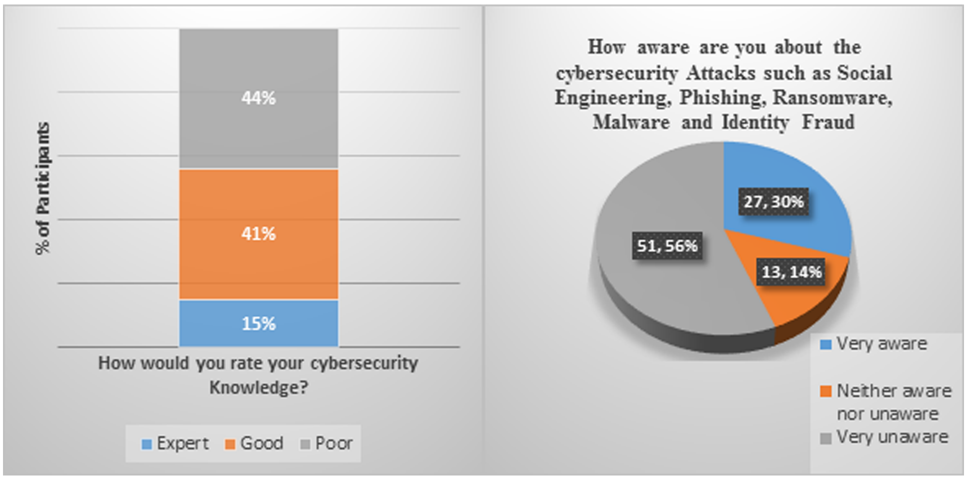


Figure 13. Cybersecurity Knowledge and Awareness Survey Charts.

In relation to the items in Table 2, the majority of respondents (more than 90%) agreed, which was a promising result, indicating that the CybAR game and the concept of gamification were well received by participants (Figure 14).

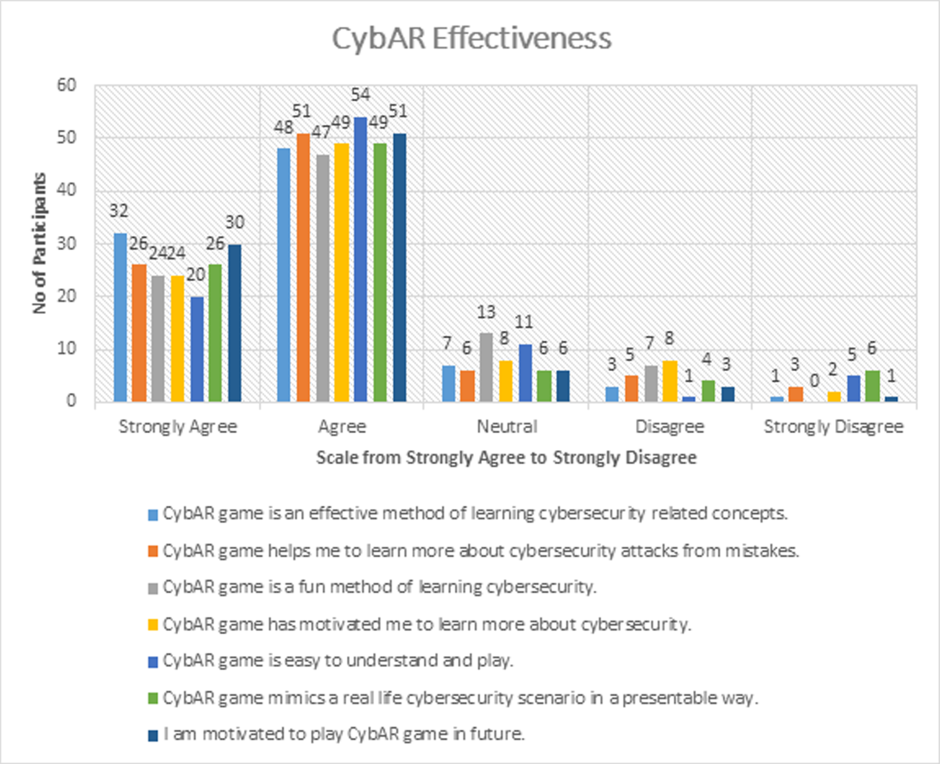


Figure 14. Survey responses on CybAR game.

In response to the statement CybAR game is an effective method of learning cybersecurity related concepts, the majority agreed or strongly agreed (mode = 4, mean = 4.18) (Figure 14). More importantly, 88% of participants stated that they understood cybersecurity better after playing the CybAR game and that the challenges were very interesting. The results in relation to the perceived effectiveness of gamification were in line with previous research [16,33].

In relation to cybersecurity awareness, the majority of respondents agreed that the CybAR game helped participants learn more about cybersecurity attacks from mistakes, as shown in Figure 14 and Table 3 (mode = 4, mean = 4.01). The participants agreed that the feedback displayed in the CybAR app is informative and helpful. Previous studies have shown that students learn only 20% of what they hear and read, but can learn 90% of what they have practised [47]. In this study, CybAR users stated that the game was more helpful in avoiding risky cybersecurity online behaviour than just reading paper-based information about cybersecurity awareness.

Table 3. Survey items mean.

No	Questions	Mean
1	CybAR game is an effective method of learning cybersecurity related oncepts.	4.18
2	CybAR game helps me to learn more about cybersecurity attacks from mistakes.	4.01
3	CybAR game is a fun method of learning cybersecurity.	3.97
4	CybAR game has motivated me to learn more about cybersecurity.	3.93
5	CybAR game is easy to understand and play.	3.91
6	CybAR game mimics a real life cybersecurity scenario in a presentable way.	3.93
7	I am motivated to play CybAR game in future.	4.16

The majority of participants strongly agreed that CybAR game is a fun method of learning cybersecurity and the mode indicated agreement (mean = 3.97) (Figure 14). The participants felt they benefited from the use of gamification techniques in cybersecurity learning. This is consistent with research by Giannakas et al. [48], who developed a mobile game-based app that helped users learn about potential phishing attacks in a fun and interactive way. However, 19% of our respondents selected neutral or disagree. This result indicates that the presentation of the game needs to be improved to make it more enjoyable. In relation to learning material about the game, the majority of participants preferred that it be included in the game itself rather than in the CybAR booklet. This result strengthened our view about the importance of minimising the volume of information provided.

In response to the item "CybAR game has motivated me to learn more about cybersecurity", 84% of participants strongly agreed (mean = 3.93). Consistent with these results, previous studies [16,47,48] showed that games designed to promote cybersecurity education and awareness helped users learn more about the most common cybersecurity attacks. In our study, eight participants disagreed, possibly because they had only played the game once and did not concentrate on the feedback displayed on the screen. This suggests that more needs to be done to make the game more enjoyable and increase player motivation to learn.

In response to the item "CybAR game is easy to understand and play", only 15 participants selected the neutral or strongly disagree options. This indicates that some aspect of the game (mechanisms, rules or explanations) may be overly complex and need to be improved. However, the majority of participants did not encounter any problems while playing the game, as shown in Table 3 (mean = 3.91).

In response to the item "CybAR game mimics a real life cybersecurity scenario in a presentable way", 82% of participants agreed (mean = 3.93), which is consistent with a previous study by Jin et al. [33]. In our study, however, six players selected neutral, four selected disagree and four selected strongly disagree. A possible explanation for this is that these players did not read the CybAR booklet first. The booklet could be improved by describing and representing real life examples rather than only photos of cybersecurity attacks.

In relation to the final item, I am motivated to play CybAR game in future, the mode indicated that the majority of participants agreed (mean = 4.16) (Figure 14)

In summary, the results of the survey indicate three main benefits the game: it is very easy to play, it helps players improve their cybersecurity awareness and it increases their understanding of cybersecurity problems and solutions.

8. Conclusions and Future Work

A consistent, continuous and timely education to individuals can enable them to improve their awareness and transform their behaviour. This paper has described a design, implementation and evaluation of MAR-based serious game called CybAR, an innovative gamified approach to educate users about cybersecurity attacks and enhance their avoidance behaviour, which integrates elements derived from a theoretical model, TTAT. It has an interactive user interface designed around key components that have been identified through empirical investigation.

The game was played and evaluated by 91 university students. The results indicated that CybAR can be an effective and fun way of learning cybersecurity related concepts. CybAR mimics a real life cybersecurity problem setting in an enjoyable and understandable way. CybAR also motivates players to learn more about cybersecurity related concepts in future. Additionally, participants reported that gamification elements were an important means of raising cybersecurity awareness. The reporting results of CybAR app for raising their awareness about cybersecurity and adopting them to avoidance mechanism for a small group of 91 university students justify the effectiveness of Cybar app for impact for a variety of age group peoples. Thus, our future work will seek to extend the CybAR game into a comprehensive cybersecurity awareness application, covering a range of technical and non-technical topics for different age groups. In addition, Risky Cybersecurity Behaviours (RCsB) survey can also be incorporated into CybAR app to examine knowledge flow that impacts users' self-efficacy and ultimately improves their cybersecurity threat avoidance behaviour. This work is validated using a small sample size of 91 participants only. The research, however, can be expanded in a number of ways in future. First, it was an experimental study, with small sample size. In future, we will plan to evaluate its effectiveness using a large sample size from geographical distributed locations. Second, we will include a long-term evaluation regarding the retention of knowledge about cybersecurity attacks. Third, the game will be improved to make it more enjoyable since it is not good at making much enjoyment for players by including more gamification elements. To overcome this limitation, in our future work, we will embed the quiz within an overarching storyline to make the experience more immersive and also add more actions and elements derived from game refinement theory or other frameworks to enhance enjoyment. Finally, we will conduct longitudinal research to explore the memorability of the cybersecurity-related concepts delivered through CybAR in future.

Author Contributions: Investigation, H.A.; Supervision, M.K.-T. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Moallem, A. *Cybersecurity Awareness Among Students and Faculty*; CRC Press: Boca Raton, FL, USA, 2019.
2. Dhamija, R.; Tygar, J.D.; Hearst, M. Why phishing works. In *Proceedings of the SIGCHI conference on Human Factors in Computing Systems*; ACM: New York, NY, USA, 2006; pp. 581–590.
3. Hui, C.P. How to study home users. In *TKK T-110.5190, Seminar on Internetworking*; Citeseer: Princeton, NJ, USA, 2007.
4. Ciampa, M. *Security Awareness: Applying Practical Security in Your World*; Cengage Learning: Boston, MA, USA, 2013.
5. Howard, D.; Prince, K. *Security 2020: Reduce Security Risks This Decade*; Wiley Publishing: Hoboken, NJ, USA, 2010.
6. Al-Janabi, S.; Al-Shourbaji, I. A study of cyber security awareness in educational environment in the middle east. *J. Inf. Knowl. Manag.* **2016**, *15*, 1650007. [CrossRef]
7. Alotaibi, F.; Furnell, S.; Stengel, I.; Papadaki, M. A review of using gaming technology for cyber-security awareness. *Int. J. Inf. Secur. Res. (IJISR)* **2016**, *6*, 660–666. [CrossRef]
8. Conway, D.; Taib, R.; Harris, M.; Yu, K.; Berkovsky, S.; Chen, F. A qualitative investigation of bank employee experiences of information security and phishing. In Proceedings of the Thirteenth Symposium on Usable Privacy and Security ({SOUPS} 2017), Santa Clara, CA, 12–14 July 2017; pp. 115–129.
9. Kumaraguru, P.; Sheng, S.; Acquisti, A.; Cranor, L.F.; Hong, J. Teaching Johnny not to fall for phish. *ACM Trans. Internet Technol. (TOIT)* **2010**, *10*, 7. [CrossRef]
10. Brooks, F.M.; Chester, K.L.; Smeeton, N.C.; Spencer, N.H. Video gaming in adolescence: factors associated with leisure time use. *J. Youth Stud.* **2016**, *19*, 36–54. [CrossRef]
11. Connolly, T.M.; Boyle, E.A.; MacArthur, E.; Hainey, T.; Boyle, J.M. A systematic literature review of empirical evidence on computer games and serious games. *Comput. Educ.* **2012**, *59*, 661–686. [CrossRef]
12. Shumaker, R. *Virtual and Mixed Reality-Systems and Applications: International Conference, Virtual and Mixed Reality 2011, Held as Part of HCI International 2011, Orlando, FL, USA, 9–14 July 2011, Proceedings*; Springer: Berlin, Germany, 2011; Volume 6774.
13. Read, J.L.; Shortell, S.M. Interactive games to promote behavior change in prevention and treatment. *JAMA* **2011**, *305*, 1704–1705. [CrossRef]
14. Burke, J.W.; McNeill, M.; Charles, D.K.; Morrow, P.J.; Crosbie, J.H.; McDonough, S.M. Optimising engagement for stroke rehabilitation using serious games. *Vis. Comput.* **2009**, *25*, 1085. [CrossRef]
15. Deterding, S.; Dixon, D.; Khaled, R.; Nacke, L. From game design elements to gamefulness: Defining gamification. In *Proceedings of the 15th International Academic MindTrek Conference: Envisioning Future Media Environments*; ACM: New York, NY, USA, 2011; pp. 9–15.
16. Wen, Z.A.; Lin, Z.; Chen, R.; Andersen, E. What. Hack: Engaging Anti-Phishing Training through a Role-playing Phishing Simulation Game. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*; ACM: New York, NY, USA, 2019; p. 108.

17. Alqahtani, H.; Kavakli, M. iMAP-CampUS (an Intelligent Mobile Augmented Reality Program on Campus as a Ubiquitous System): A Theoretical Framework to Measure User's Behavioural Intention. In *Proceedings of the 9th International Conference on Computer and Automation Engineering*; ACM: New York, NY, USA, 2017; pp. 36–43.
18. Alqahtani, H.; Kavakli, M. iMAP-CampUS: Developing an Intelligent Mobile Augmented Reality Program on Campus as a Ubiquitous System. In *Proceedings of the 9th International Conference on Computer and Automation Engineering*; ACM: New York, NY, USA, 2017; pp. 1–5.
19. Alqahtani, H.; Kavakli, M.; Sheikh, N.U. Analysis of the Technology Acceptance Theoretical Model in Examining Users Behavioural Intention to Use an Augmented Reality App (IMAP-Campus). *Int. J. Eng. Manag. Res. (IJEMR)* **2018**, *8*, 37–49. [CrossRef]
20. Lave, J.; Wenger, E. *Situated Learning: Legitimate Peripheral Participation*; Cambridge University Press: Cambridge, UK, 1991.
21. Markouzis, D.; Fessakis, G. Interactive Storytelling and Mobile Augmented Reality Applications for Learning and Entertainment A rapid prototyping perspective. In Proceedings of the 9th International Conference on Interactive Mobile Communication, Technologies and Learning (IMCL2015), Thessaloniki, Greece, 19–20 November 2015.
22. Bower, M.; Howe, C.; McCredie, N.; Robinson, A.; Grover, D. Augmented Reality in education–cases, places and potentials. *Educ. Media Int.* **2014**, *51*, 1–15. [CrossRef]
23. Thompson, M.F.; Irvine, C.E. CyberCIEGE scenario design and implementation. In Proceedings of the 2014 {USENIX} Summit on Gaming, Games, and Gamification in Security Education (3GSE 14), San Diego, CA, USA, 18 August 2014.
24. Liang, H.; Xue, Y. Avoidance of information technology threats: A theoretical perspective. *MIS Q.* **2009**, 71–90. Available online: https://www.jstor.org/stable/20650279 (accessed on 20 February 2020). [CrossRef]
25. Liang, H.; Xue, Y. Understanding security behaviors in personal computer usage: A threat avoidance perspective. *J. Assoc. Inf. Syst.* **2010**, *11*, 394–413. [CrossRef]
26. Misra, G.; Arachchilage, N.A.G.; Berkovsky, S. Phish Phinder: A Game Design Approach to Enhance User Confidence in Mitigating Phishing Attacks. *arXiv* **2017**, arXiv:1710.06064.
27. Stevens, T. Global Cybersecurity: New Directions in Theory and Methods. *Politics Gov.* **2018**, *6*, 1–4. [CrossRef]
28. Kassicieh, S.; Lipinski, V.; Seazzu, A.F. Human centric cyber security: what are the new trends in data protection? In Proceedings of the IEEE 2015 Portland International Conference on Management of Engineering and Technology (PICMET), Portland, OR, USA, 2–6 August 2015; pp. 1321–1338.
29. Sheng, S.; Magnien, B.; Kumaraguru, P.; Acquisti, A.; Cranor, L.F.; Hong, J.; Nunge, E. Anti-phishing phil: the design and evaluation of a game that teaches people not to fall for phish. In *Proceedings of the 3rd Symposium on Usable Privacy and Security*; ACM: New York, NY, USA, 2007; pp. 88–99.
30. Arachchilage, N.A.G.; Love, S.; Beznosov, K. Phishing threat avoidance behaviour: An empirical investigation. *Comput. Hum. Behav.* **2016**, *60*, 185–197. [CrossRef]
31. Kirlappos, I.; Sasse, M.A. Security education against phishing: A modest proposal for a major rethink. *IEEE Secur. Priv.* **2011**, *10*, 24–32. [CrossRef]
32. Yasin, A.; Liu, L.; Li, T.; Wang, J.; Zowghi, D. Design and preliminary evaluation of a cyber Security Requirements Education Game (SREG). *Inf. Softw. Technol.* **2018**, *95*, 179–200. [CrossRef]
33. Jin, G.; Tu, M.; Kim, T.H.; Heffron, J.; White, J. Game based cybersecurity training for high school students. In *Proceedings of the 49th ACM Technical Symposium on Computer Science Education*; ACM: New York, NY, USA, 2018; pp. 68–73.
34. Gondree, M.; Peterson, Z.N. Valuing security by getting [d0x3d!]: Experiences with a network security board game. Presented at Part of the 6th Workshop on Cyber Security Experimentation and Test, Washington, DC, USA, 12 August 2013.
35. Denning, T.; Lerner, A.; Shostack, A.; Kohno, T. 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*; ACM: New York, NY, USA, 2013; pp. 915–928.
36. Williams, L.; Meneely, A.; Shipley, G. Protection poker: The new software security "game". *IEEE Secur. Priv.* **2010**, *8*, 14–20. [CrossRef]

37. Mirkovic, J.; Peterson, P.A. Class capture-the-flag exercises. In Proceedings of the 2014 {USENIX} Summit on Gaming, Games, and Gamification in Security Education (3GSE 14), San Diego, CA, USA, 18 August 2014.
38. Azuma, R.T. A survey of augmented reality. *Presence Teleoperators Virtual Environ.* **1997**, *6*, 355–385. [CrossRef]
39. Hendrix, M.; Al-Sherbaz, A.; Bloom, V. Game based cyber security training: Are serious games suitable for cyber security training? *Int. J. Serious Games* **2016**, *3*. [CrossRef]
40. Kurkovsky, S. Engaging students through mobile game development. In *ACM SIGCSE Bulletin*; ACM: New York, NY, USA, 2009; Volume 41, pp. 44–48.
41. Wong, J.K.; Sheth, J.N. Explaining intention-behavior discrepancy—A paradigm. *ACR N. Am. Adv.* **1985**. Available online: www.acrwebsite.org/volumes/6419/volumes/v12/NA-12 (accessed on 20 February 2020).
42. de la Hera Conde-Pumpido, T. A Conceptual Model for the Study of Persuasive Games. **2013**. Available online: https://repub.eur.nl/pub/110458/ (accessed on 20 February 2020).
43. Rittle-Johnson, B.; Koedinger, K.R. Comparing Instructional Strategies for Integrating Conceptual and Procedural Knowledge. In Proceedings of the 24th annual meeting of the North American Chapters of the International Group for the Psychology of Mathematics Education, Athens, GA, USA, 26–29 October 2002.
44. Gee, J.P. Deep learning properties of good digital games: How far can they go? In *Serious Games*; Routledge: Abingdon, UK, 2009; pp. 89–104.
45. Rogers, R.W. A protection motivation theory of fear appeals and attitude change1. *J. Psychol.* **1975**, *91*, 93–114. [CrossRef] [PubMed]
46. Scholefield, S.; Shepherd, L.A. Gamification Techniques for Raising Cyber Security Awareness. *arXiv* **2019**, arXiv:1903.08454.
47. Findley, M.R. The relationship between student learning styles and motivation during educational video game play. *Int. J. Online Pedagog. Course Des. (IJOPCD)* **2011**, *1*, 63–73. [CrossRef]
48. Giannakas, F.; Kambourakis, G.; Gritzalis, S. CyberAware: A mobile game-based app for cybersecurity education and awareness. In Proceedings of the IEEE 2015 International Conference on Interactive Mobile Communication Technologies and Learning (IMCL), Thessaloniki, Greece, 19–20 November 2015; pp. 54–58.