Gamification of Cyber Security Awareness – A Systematic Review of Games

Cyber Security
Master's Degree Programme in Information and Communication Technology
Department of Computing, Faculty of Technology
Master of Science in Technology Thesis

Author:

Barack Onduto

Supervisors:

Post Doctoral Researcher Ali Farooq
Adjunct Professor Jouni Smed

December 2021

Master of Science in Technology Thesis

Department of Computing, Faculty of Technology

University of Turku

Subject: Cyber Security

Programme: Master's Degree Programme in Information and Communication Technology

Author: Barack Onduto

Title: Gamification of Cyber Security Awareness – A Systematic Literature Review

Number of pages: 95 pages, 44 appendix pages

Date: December 2021

Abstract.

The frequency and severity of cyber-attacks have increased over the years with damaging consequences such as financial loss, reputational damage, and loss of sensitive data. Most of these attacks can be attributed to user error. To minimize these errors, cyber security awareness training is conducted to improve user awareness. Cyber security awareness training that is engaging, fun, and motivating is required to ensure that the awareness message gets through to users. Gamification is one such method by which cyber security awareness training can be made fun, engaging, and motivating. This thesis presents the state of the art of games used in cyber security awareness. In this regard, a systematic review of games following PRISMA guidelines was conducted on the relevant papers published between 2010 to 2021. The games were analyzed based on their purpose, cyber security topics taught, target audience, deployment methods, game genres implemented and learning mechanics applied. Analysis of these games revealed that cyber security awareness games are mostly deployed as computer games, targeted at the general public to create awareness in a wide range of cyber security topics. Most of the games implement the role-playing genre and apply demonstration learning mechanics to deliver their cyber security awareness message effectively.

Keywords: gamification, cyber security awareness, serious games, systematic literature review.

Contents

Table of tables

Table of figures

1 Introduction

We live in an increasingly interconnected world thanks to cyberspace. Cyberspace has brought immense benefits to users and organizations because it has enabled connectivity, faster communication, information sharing, cost-saving, better service delivery, entertainment, and collaboration. Unfortunately, cyberspace has also brought new threats and risks to users and organizations. Malware, password theft, network traffic interception, phishing attacks, distributed denial of service (DDoS), zero-day exploits, social engineering, ransomware, water hole attack, and Trojan virus are common problems faced by users and organizations (Mathoosoothenen et al., 2017). Due to these ever-present threats and risks, there is an urgent need for cyber security.

Cyber security is the activities designed to safeguard the confidentiality, integrity, availability, and non-repudiation of information within a computer system against unauthorized access and attacks (Boyce et al., 2011). Cyber security is a broad socio-technical topic that requires the input of people, processes, and technology to succeed (Veneruso et al., 2020). Cyber security is critical to national infrastructure, military, industry, business, personal privacy, national and local governments (Jin et al., 2018). It is especially important for organizations because its systems are used by different users i.e. employees, customers, visitors, 3rd party vendors. These users connect to different services e.g. social media, web applications, and websites. Furthermore, they access these systems using different devices e.g. tablets, laptops, PCs, and mobile phones. All these factors combined increases the cyber security risks and threats within an organization (Nagarajan et al., 2012).

Users have varied knowledge and skill levels that range from novice to expert. Naturally, these differences amongst users result in varied cyber security awareness requirements (Nagarajan et al., 2012; Reeves et al., 2021). Users play a pivotal role in a cyber security socio-technical system. They are also considered the weakest link in this system (Filipczuk et al., 2019). Beckers & Pape (2016) state that it is easier to manipulate a user than to manipulate technology. User weakness stems from the fact that the level of sophistication of cyber-attacks has increased over the years. Few people outside the ‘hacker world’ are familiar with these levels of sophistication. Users are also often ignorant of the value of information in their possession and the potential of a hacker using this information against them (Underhay et al., 2016). Despite being

the weakest link in a cyber security socio-technical system, users have received little attention (Farooq 2019a; Tioh et al., 2017). Mitigating user error and vulnerability can greatly contribute towards increased cyber security (Quayyum 2020). Omiya & Kadobayashi (2019) add that to ensure cyber security users require cyber security knowledge and skills.

Cyber security has become a buzzword because of recent cyber-attacks such as those carried out on Microsoft Exchange Server, Colonial Pipeline, SolarWinds, and Finnish parliament (Euronews 2020; Osborne 2021; Turton & Mehrotra 2021; Oladimeji & Kerner 2021). As a result of increased cyber-attacks and data breaches, the subject of cyber security awareness has gained significance (Mathoosoothenen et al., 2017). Cyber security awareness is the attentiveness of users to cyber security, enabling users to recognize concerns and respond effectively (Rieff 2018). By raising cyber security awareness, users' assessment of risks and awareness of threats increases. Cyber security awareness training equips users with the tools and knowledge to mitigate cyber security threats and risks with the ultimate goal of changing user cyber security behaviour and posture (Quayyum 2020). It can be concluded that cyber security awareness is the synchronization of the capabilities of people, processes, and technology. Synchronization is done to secure and control information systems (Rieff 2018).

1.1 Problem statement

Organizations typically have cyber security policies that govern user cyber security behaviour. Holdsworth & Apeh (2017) defines cyber security policy as set standards for user behaviour that regulate activities such as email encryption and restrict social media usage. These policies assist users in understanding how to secure an organization's data and systems. Cyber security awareness training in conjunction with cyber security policy develops a cyber security culture within the organization (Ashenden 2008). Ashenden (2008) defines organizational culture as patterns of assumptions that users within an organization use as guidance when responding to unfamiliar situations. From this, we see that cyber security awareness training is an important component in ensuring cyber security within an organization. Having this in mind, organizations aim to provide cyber security awareness training that engages, motivates, and changes users' cyber security behaviour and attitude. Unfortunately, current cyber security awareness training methods do not guarantee the achievement

of the aforementioned objectives (Holdsworth & Apeh 2017; Farooq 2019a). Moreover, users find the current cyber security awareness training as boring, ridiculous, overwhelming, low-quality productions, not relevant to their roles, and do not capture real-world workplace variables (Reeves et al., 2021).

1.2 Purpose and objective

As mentioned earlier current cyber security awareness training methods have proved inadequate. Gamification is the new mode of education in the modern era. Humans naturally like to play games and gamification takes advantage of this to integrate game structures into education. The application of gamification in education ensures positive learning outcomes such as changes in user behaviour are achieved. Gamification implements game mechanics that make the learning process fun and entertaining (Kocakoyun & Ozdamli 2018). Games can also be applied in cyber security awareness training to achieve positive learning outcomes in a fun, engaging, entertaining, and motivational manner (Quayyum 2020; Jin et al., 2018; Mathoosoothenen et al., 2017). As Confucius famously said, “Tell me and I will forget, show me and I may remember, involve me and I will understand.” Gamification actively involves users during cyber security awareness training, to ensure users understand the awareness message.

This thesis answers the following research question.

RQ1: “What is the state of art on games used in cyber security awareness?”

The objectives within this research question are to:

1. Identify the purpose and topics taught by cyber security awareness games
2. To understand the deployment methods used by the cyber security awareness games
3. To identify the target audience of cyber security awareness games
4. To explore the different game genres implemented by the cyber security awareness games
5. To examine the learning mechanics applied by cyber security awareness games

By achieving these objectives knowledge that will help game designers develop a comprehensive cyber security awareness game will be collated, practitioners will have the knowledge base of cyber security awareness games that will assist them to select a suitable game, and end-users can opt for the best gaming solution for their needs.

This thesis also provides a critical view of the benefits and challenges of gamification of cyber security awareness.

1.3 Methodology

To address this research question, a review of cyber security games following the PRISMA guidelines was conducted on the relevant papers published between 2010 to 2021. I searched and retrieved 506 papers on the gamification of cyber security awareness from scientific digital databases published between 2010 to 2021. Thereafter, a systematic review of the games described in these papers was conducted.

1.4 Thesis structure

The rest of the thesis is structured as follows. Chapter 2 covers background information which includes the human element in cyber security, security education training and awareness (SETA), current security awareness delivery mechanisms, and gamification. Chapter 3 looks at the research methodology where the research process is explained. Chapter 4 contains the literature review results and chapter 5 contains a discussion of the results. Lastly, chapter 6 has the conclusion.

2 Background

2.1 The human element in cyber security

The leading cause of security breaches in organizations is human error. It is a widely held belief that humans are the weakest link in cyber security (Nguyen & Pham 2020; Farooq et al., 2015a). Zoto et al., (2018) define the human element in cyber security as the cyber security and privacy risks that arise from human activity. Cyber security depends on socio-technical systems that recognize the interaction between people and technology (Zimmermann & Renaud 2019; Ashenden 2008). Socio-technical systems involve the complex interactions between social, psychological, technical, and environmental components. These components need to work together cohesively for the system to efficiently function (Mittal 2015). The technical component comprises machines and methods subcomponents. The socio component comprises structure and culture subcomponents. Additionally, the structure subcomponent describes the position of a user within the organization. The user can either be management or support staff. The cultural subcomponent describes the values and traditions of a user (Zoto et al., 2018).

The human element in cyber security is affected by differences in people's characteristics, personalities, and behaviours. These differences are a result of people having different cyber security attitudes, beliefs, values, traditions, and threat perceptions (Ashenden 2008; Farooq et al., 2019b). Demography, personality traits, risk-taking, and decision-making also affect the human element in cyber security. Demography attribute includes factors such as the age, gender, and citizenship of the user (Farooq et al., 2015a; Farooq et al., 2015b). Personality trait attribute include factors such as agreeableness, conscientiousness, neuroticism, openness, and extraversion of the user. Risk-taking and decision-making attributes include factors that affect a user's decision-making processes such as rationality, avoidance, dependance, intuitivity, and spontaneity. All these attributes collectively affect people's cyberspace interactions (Alqahtani & Thorne 2020).

The human element cannot be substituted in a cyber security socio-technical system since they play a central role. Humans are responsible for implementing the cyber security processes and operating the cyber security technology. Activities such as authentication, account management, and incidence response cannot be fully

automated and thus require human involvement. Therefore effective cyber security can only be achieved by correctly applying the human element in the mitigation against cyber security threats and risks (Ashenden 2008; Boyce et al., 2011; Zimmermann & Renaud 2019).

While humans play an important role in a cyber security socio-technical system, the fact that they constitute the weakest link in the system cannot be overlooked (Boyce et al., 2011; Zimmermann & Renaud 2019; Farooq 2019a). Humans are the weakest link because they lack cyber security awareness, engage in poor cyber security practices, lack shared cyber security responsibility, lack the motivation to implement cyber security practices, and are required to implement cyber security practices that are not user friendly (Boyce et al., 2011; Metalidou et al., 2014; Farooq 2019a; Reeves et al., 2021). These factors make the human element prone to errors of omission and commission. As a result of human error, cyber security threats such as elevation of privilege, social engineering, unauthorized access, denial of service, identity theft, phishing attacks, and ransomware are likely to occur (Metalidou et al., 2014).

The more predictable and rational a system is the more secure the system. Due to the complicated nature of human decisions making, human behaviour is often unpredictable and sometimes irrational. This unpredictability and irrationality in humans often compromise cyber security (Benson et al., 2018). It is sometimes difficult to accurately pinpoint human error during a cyber security incident. This is because cyber security socio-technical systems are complex, and many different factors collectively contribute towards a cyber security incident. Therefore the notion that humans are the weakest link in cyber security can be disputed. The role of humans in creating or mitigating cyber security risks needs to be properly understood (Boyce et al., 2011). The human element in a cyber security socio-technical system should not necessarily be thought of as a problem but as a solution in ensuring cyber security (Zimmermann & Renaud 2019).

The success or failure of cyber security within an organization depends on the users (Metalidou et al., 2014). Therefore the management of humans in a cyber security socio-technical system should be prioritized. User management is achieved through cyber security awareness which I will simply refer to as security awareness for the rest of this thesis. Security awareness help minimize human error by enlightening users to

the value of information and alerting them to information risks (Ashenden 2008; Boyce et al., 2011). Security awareness can be targeted at a few users or all the users within an organization. Changes in the cyber security behaviour of a few users within an organization can result in an overall change of cyber security behaviour within the organization. This is because users tend to change their attitudes and behaviour to match their peers (Benson et al., 2018). When an organization fully understands its users' knowledge gaps and cyber security requirements and provides them with the proper technical support in the form of security awareness. The human element stops being a problem in cyber security and instead becomes a solution (Zimmermann & Renaud 2019; Amankwa et al., 2014).

2.2 Security Education, Training and Awareness (SETA)

Users increasingly have access to important organizational information through ubiquitous and organization-wide systems. While these systems increase efficiency and effectiveness within the organization, they also increase the organization's risk exposure. Organizations are increasingly vulnerable to user action therefore management of user behaviour becomes important (Burns et al., 2015). To manage user behaviour organizations have used cyber security policies, procedures, and security awareness training. A cyber security policy is a set of standards, rules, and practices that regulate user activity within an organization. Activities regulated by cyber security policy include email usage, social media, passwords, remote access, and information encryption. Users are usually required to comply with cyber security policies (Ashenden 2008). Cyber security policies prevent bad cyber security behaviour by telling users what not to do. The policies don't focus on telling users what should be done (Burns et al., 2015). Security awareness is conducted through security education, training, and awareness (SETA) programs. SETA programs are essential in protecting important information within the organization i.e. the organization's crown jewels (Alshaikh et al., 2018).

SETA is defined as educational programs within the organization that seeks to reduce cyber security breaches by increasing security awareness amongst users (Caballero 2017; Amankwa et al., 2014; Hight 2015). SETA programs are targeted at all the users within the organization. They direct user attention towards the organization's cyber security policy and define cyber security standards according to their roles within the organization (Caballero 2017). SETA programs do not just review the organization's

cyber security policies, they also explain the security policy and the reason behind these policies to users. For a SETA program to be effective it should be tailored to meet the user's and organization's unique cyber security requirements (Hight 2015). A successful SETA program alerts users to cyber security threats and risks. Which in turn increases a user's cyber security consciousness which results in better cyber security behaviour from the user (Amankwa et al., 2014).

2.2.1 Cyber security education

Amankwa et al., (2014) define cyber security education as the process of providing cyber security professionals with comprehensive expertise. Cyber security education provides professionals with the skills and knowledge to perform complex cyber security activities in line with the evolving cyber threat landscape. The focus of cyber security education is to provide insights into cyber security practices. Its purpose is to provide cyber security professionals with an understanding of how to maintain confidentiality, integrity, and availability of information. Cyber security education is conducted using theoretical instructions methods such as seminars and lectures (Alshaikh et al., 2018); Von Solms & Von Solms 2009). Von Solms & Von Solms (2009) state that cyber security education aims to have a long-term impact on cyber security professionals.

2.2.2 Cyber security training

Amankwa et al., (2014) define cyber security training as the practice of improving users' knowledge, skills, and attitude on cyber security issues. The knowledge and skills acquired during training enable users to securely perform their roles within the organization. Cyber security training demonstrates to users that the organization takes cyber security seriously. With this demonstration, it is hoped that users also change their cyber security attitudes. A successful cyber security training exercise results in users practising good cyber security behaviour while performing their roles. It focuses on what users need to know to perform their role as opposed to what they should know regarding cyber security (Amankwa et al., 2014). The focus of cyber security training is to ensure users have the competencies to securely perform their roles within the organization (Alshaikh et al., 2018). Its purpose is to provide users with the necessary skills and knowledge to ensure confidentiality, integrity, and availability of information. Cyber security training is conducted using practical instruction methods such as seminars, workshops, and hands-on experience (Alshaikh et al., 2018; Von Solms &

Von Solms 2009). Von Solms & Von Solms (2009) state that cyber security training has a medium-term impact on users.

2.2.3 Cyber security awareness

Amankwa et al., (2014) define cyber security awareness as the practice of encouraging a user to recognize cyber security problems and act accordingly. One way of doing this is by alerting users to the organization's cyber security policy and encouraging compliance with these policies. Cyber security education and training should be conducted before cyber security awareness. This is because cyber security education and training introduce users to cyber security terms contained in the policy (Amankwa et al., 2014). The focus of cyber security awareness is to alert users to the organization's cyber security policy. Its purpose is to inform users of their role in information protection. Cyber security awareness is conducted through print and electronic media such as videos, newsletters, posters (Alshaikh et al., 2018; Von Solms & Von Solms 2009). Von Solms & Von Solms (2009) state that cyber security awareness has a short-term impact on users.

2.2.4 Successful SETA program attributes

Both users and organizations have somewhat similar expectations from SETA programs. They expect business prosperity, work gratification, competency growth, and clear objects from SETA programs (Gjertsen et al., 2017). Figure 1 below lists the attributes of a successful SETA program, which include:

1. *Focus* is an important attribute to have in a SETA program. A SETA program's focus should be to enhance the cyber security knowledge of users within the organization and ultimately improve the cyber security culture within the organization (Amankwa et al., 2014; Amankwa et al., 2015). SETA should sensitize users to cyber security issues according to their various roles within the organization. It should also encourage compliance with the organization's cyber security policy and clearly state the penalties for noncompliance (Reeves et al., 2021). SETA programs should be compulsory for users handling sensitive information (Amankwa et al., 2014).
2. SETA programs should have a *purpose*. The purpose of a SETA program should be to serve users with different personalities, interests, and educational backgrounds (Amankwa et al., 2014; Amankwa et al., 2015; Reeves et al., 2021).

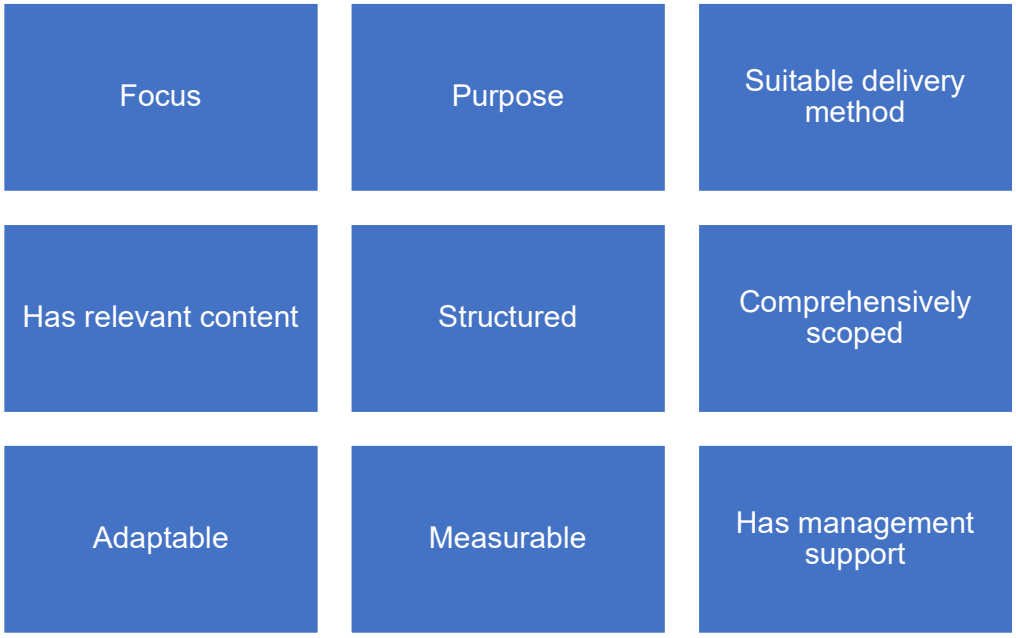


Figure 1: Attributes of a successful SETA program

SETA programs should identify different user cyber security needs and address these needs. The programs should also identify and address the organization's cyber security needs and gaps (Amankwa et al., 2014; Amankwa et al., 2015).

3. SETA programs should use *suitable content delivery methods*. The delivery method affects the impact of a SETA program. Cyber security awareness is delivered via posters and flyers. Cyber security education and training are delivered via lectures, workshops, and seminars (Amankwa et al., 2014; Amankwa et al., 2015; Von Solms & Von Solms 2009). Different delivery methods can be used in combination to achieve the best results (Amankwa et al., 2014).
4. SETA programs should *contain relevant content* for users and the organization. The program content is determined by the user or the organization and is sourced from the organization's cyber security policy, individual user cyber security needs, and cyber security best practices. Relevance of the content ensures that users are not overburdened with irrelevant and unnecessary information during training (Reeves et al., 2021).
5. SETA programs should be *structured*. The structure of a SETA program can either be functional or skill-based. Functional training focuses on a user's role and responsibility within an organization. Skilled-based training focuses on a user's skill

level. Different SETA programs should be organized for novices, intermediate and advanced users (Caballero 2017).

6. SETA programs should be *comprehensive in scope*. During the development of a SETA program, the information gathered from cyber security policy, users, and best practices should be broad enough to satisfy different user and organizational requirements. A well-scoped SETA program provides the organization with end to end coverage. End to end coverage means that all the organization's cyber security aspects are covered by the SETA program. The comprehensiveness of a SETA program also means it provides up-to-date information regarding the cyber security threats landscape (Amankwa et al., 2014; Amankwa et al., 2015).
7. SETA programs should be *adaptable*. Adaptability means the SETA program can be applied to different users within the organization with minimal modification. Since SETA programs borrow from cyber security best practices and the organization's cyber security policy. Different departments within the organization should be able to use the same SETA program (Amankwa et al., 2014; Amankwa et al., 2015).
8. SETA programs should be *measurable*. The evaluation criteria of a SETA program should be aligned with the focus and purpose of the SETA program. The evaluation criteria should be simple, measurable, articulate, reasonable, time-bound, and illustrate whether the program's goals have been achieved (Amankwa et al., 2014; Amankwa et al., 2015).
9. Successful SETA program also requires *top management support*, provides incentives to reward the best learners, engage the users, and regularly reinforce the awareness message through refresher training to ensure users remember the information (Holdsworth & Apeh 2017).

2.2.5 Formal and ad hoc SETA programs

SETA programs within an organization can be implemented using a formal or ad hoc approach. A formal SETA program approach that is implemented as outlined by ENISA and has 4 steps as shown in figure 2 below (Mäses et al., 2018).

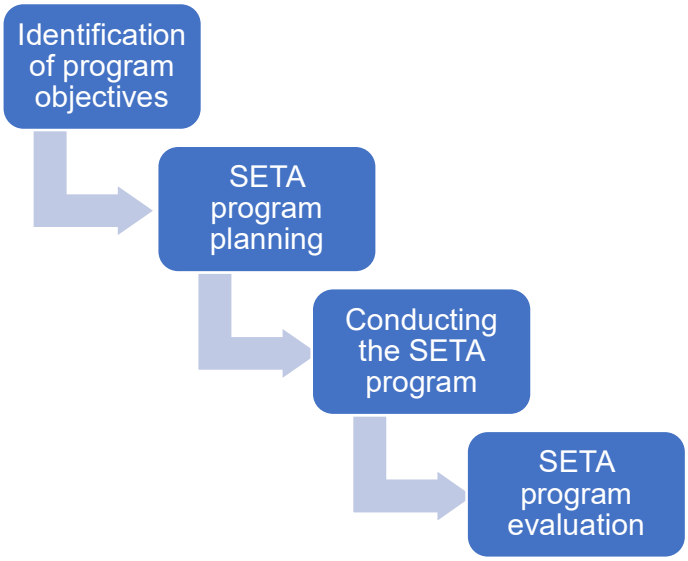


Figure 2: ENISA Formal SETA implementation steps (Mäses et al., 2018)

Step 1 involves the identification of the SETA program's objectives, scenarios, types of exercises to be conducted, key participants, and the program scope. Step 2 involves the planning of the SETA program. Step 3 involves conducting the actual SETA program. Step 4 involves evaluating the effectiveness of the SETA program (Mäses et al., 2018). Alshaikh et al., (2018) propose a formal SETA implementation model that includes development, implementation, and evaluation phases as shown in figure 3 below.

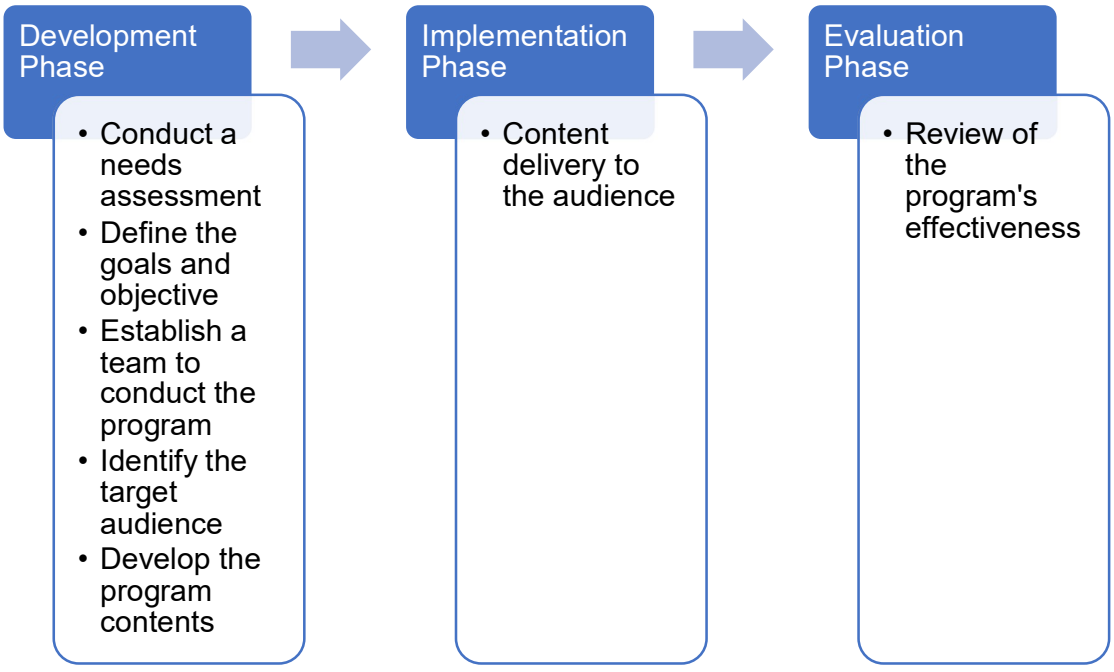


Figure 3: Formal SETA implementation phases (Alshaikh et al., 2018)

SETA programs implemented using the ad hoc approach do not have the planning elements found in the formal approach. Ad hoc SETA programs are created and conducted as deemed necessary by organizations. The focus and purpose of an ad hoc SETA program are to satisfy the organization's cyber security requirements as defined by its cyber security policy. The organization's CISO is responsible for developing and conducting an ad hoc SETA program. Its content is sourced from a previously used SETA program or another organization's SETA program. Ad hoc SETA programs are delivered using scheduled computer-based training sessions to the audience. Statistical information collected from the computer-based training sessions is used to evaluate the program (Alshaikh et al., 2018).

2.2.6 SETA program benefits

Organizations that successfully implement SETA programs enjoy the following benefits:

1. SETA programs increase user cyber security knowledge and skills, therefore increasing the threshold for cyber-attacks to occur within the organization. Informed users make it difficult for attackers to infiltrate or breach the organization's systems (Caballero 2017).
2. SETA programs create a human firewall within the organization. A human firewall is defined as the number of users actively participating in protecting the organization's systems. Having users aware of cyber security within an organization is similar to having an expanded information security department (Hight 2015).
3. Implementing a successful SETA program can be considered as risk management by an organization. An organization's risks are reduced as a result of increased user security awareness (Hight 2015). Cyber security risk premiums paid to insurance companies are also reduced as a result of the successful implementation of the SETA program (Caballero 2017).
4. Successful implementation of SETA programs helps organizations satisfy regulatory requirements and acquire standards certification e.g. ISO/IEC 27001. This help organization while they bid for contracts.
5. The goal of SETA programs is to positively affect users' cyber security behaviour and knowledge. When a large number of user behaviour and knowledge is positively affected, the overall cyber security culture within the organization is

positively affected (Reeves et al., 2021). The outcome is an organization with a good cyber security posture and culture (Caballero 2017).

2.2.7 SETA program challenges

Figure 4 below describes the challenges faced by SETA programs during implementation.

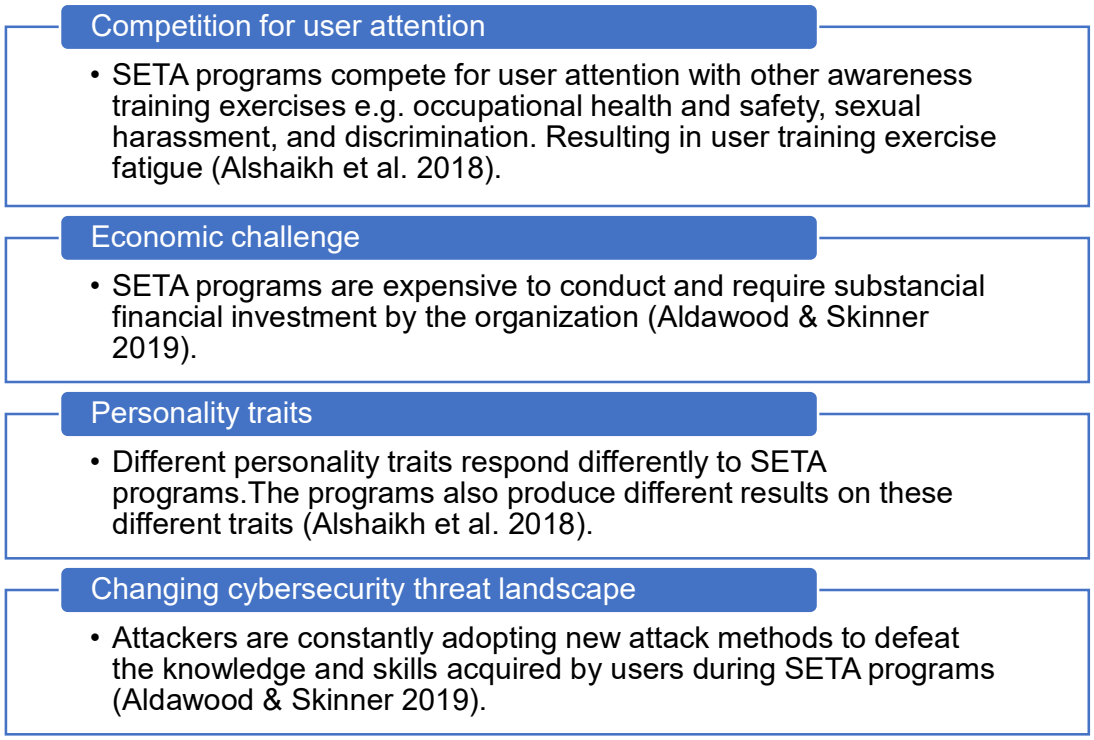


Figure 4: Challenges faced by SETA programs

2.3 Current security awareness delivery methods

The success of security awareness depends on the delivery techniques used to deliver the message to audiences i.e. users during training sessions. The delivery techniques are important because they directly affect the effectiveness of security awareness and have a correlation to audience engagement. The success of security awareness depends on the delivery method (Nguyen & Pham 2020). There currently exist various delivery methods through which security awareness can be delivered to the audience (Abawajy 2014).

Once a security awareness delivery method is selected an organization can target the security awareness message to individuals, a segment of the audience, a subset of the audience, or all the audience within an organization as shown in figure 5 below.

One-on-one security awareness sessions are highly effective and are applied to high-level audiences e.g. administrators and managers. Security awareness training can be targeted at a segment of the audience in a classroom or group meeting setting.

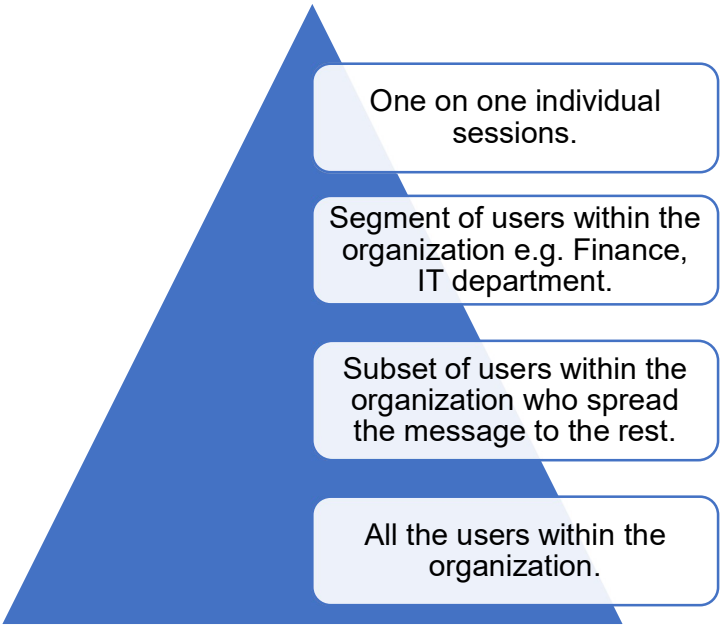


Figure 5: Security awareness training target audience (Caballero 2017)

Security awareness targeted at different segments should be customized to meet each segment's security awareness requirements. Security awareness can also be targeted at a subset of the audience within the organization. This subset of the audience then delivers the security awareness message to the rest of the audience within the organization in a peer-to-peer fashion. Peer-to-peer learning is effective in developing cyber security social norms within the organization. Security awareness can be targeted at all the users within an organization. Organization-wide security awareness addresses general cyber security topics relevant to the entire organization (Caballero 2017).

The cyber security topics to be delivered to the audience include password generation, password management, access control, Internet usage, telephone fraud, email usage and security, information privacy, virus detection and protection, backups, software licensing, social engineering, identity theft, and home office security (Al-Hamdani 2006).

An organization can choose to use security awareness delivery methods developed by cyber security companies. An organization can also develop and customize its delivery methods according to its security awareness requirements. Branding is very important during security awareness as it provides the audience with consistency and recognition. Therefore security awareness delivery methods should be branded and have similar themes and logos during security awareness training (McCoy & Fowler 2004).

The goal of security awareness delivery methods is to deliver cyber security knowledge, skills, and capabilities to the audience. The role of knowledge in behaviour change can be explained by the knowledge, attitude, and behaviour (KAB) model. KAB model states that knowledge leads to a change in attitude which culminates in the change of behaviour (Chmura 2017). There is a correlation between an audience's attitude and their knowledge, belief, behaviour intention, behaviour, and emotional response to a given situation. The audience's knowledge and belief encompass their understanding of how they should behave in a certain circumstance. The audience's emotional response is their reaction to a certain circumstance. Behaviour intention is defined as the intention of an audience to behave in a particular way given a certain circumstance. Behaviour is defined as the audience's actual conduct in a certain circumstance. Behaviour does not always match the behaviour intention (Thomson & von Solms 1998).

It is important to understand how people learn and the various learning principles that encourage compliance. Security awareness delivery methods should persuade the audience towards good cyber security behaviour. This is because persuasion has a long-term effect on behaviour change. For persuasion to work the audience needs to be exposed and attentive to the security awareness content. The audience needs to understand and accept the content (Puhakainen & Siponen 2010). The audience also needs to retain the content for security awareness to have a long-term impact. Retention is achieved by repetition and activation of the audience's imagination. Therefore security awareness delivery methods should regularly reinforce content and strive to activate the audience's imagination. Lastly, the delivery method should communicate the consequences of non-compliance and market cyber security to the audience (Thomson & von Solms 1998). Figure 6 below lists the current security awareness delivery methods.

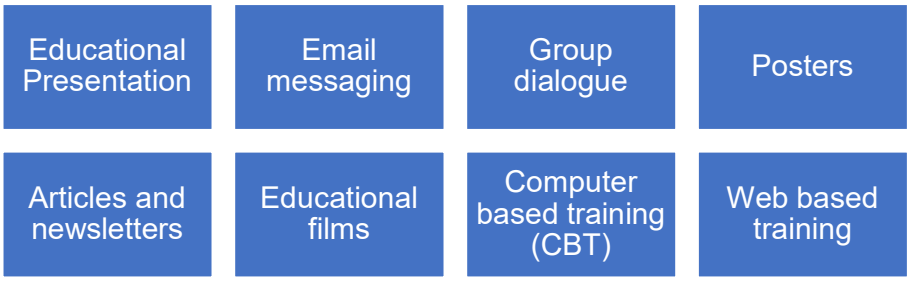


Figure 6: Current security awareness delivery methods

2.3.1 Educational presentation

Education is the process of an instructor giving instructions and the audience receiving the instructions. During educational presentations, information regarding cyber security is transferred from the instructor to the audience thus increasing the audiences' knowledge (Khan et al., 2011; Al-Daeef et al., 2017). According to the KAP model knowledge has a positive impact on attitude and behaviour (Chmura 2017). Education presentations can be conducted during one on one sessions or group sessions involving large audiences (McCoy & Fowler 2004). Educational presentations can be categorized as behaviourist and constructivist. Behaviourist education presentation is defined as one-way interaction in which the instructor gives information, and the audience receives information. Constructivist education presentation is defined as a two-way interaction between the instructor and the audience. This interaction activates the audience's thinking ensuring that the audience reflects on the information provided (Puhakainen & Siponen 2010).

Educational presentation has the advantage of being an informative security awareness delivery method that is cheap and manageable. Since it involves face-to-face interaction between the instructor and the audience, the instructor is available to answer questions. This also enables the instructor to observe nonverbal cues from the audience and adjust the content accordingly. In an educational presentation, the instructor is also able to monitor the knowledge progression of the audience (Khan et al., 2011; Alotaibi & Alfehaid 2018; Mathoosoothenen et al., 2017).

The disadvantages of educational presentation are that sessions can be boring and therefore demotivating to the audience. They lack social norms which are essential in changing audience behaviour. Social norms are behavioural cues the audience gets from their peers. It is important to note that educational presentations are only as

informative as the instructor's experience (Khan et al., 2011; Alotaibi & Alfehaid 2018; Puhakainen & Siponen 2010).

2.3.2 Email messaging

Mass emails sent to a large audiences' inbox disseminate cyber security information. The information disseminated in the email could include social engineering, ransomware, and cyber security incidences. The audience gets to increase their knowledge and awareness of cyber security issues by reading the emails. Emails however may not capture the audiences' attention because it is a one-way mode of communication. Some audiences may dismiss these emails as spam. It is important to note that reading an email does not guarantee that the audience has understood and internalized the information contained within the email. Therefore emails are an ineffective method of delivering security awareness if the goal is changing the audiences' behaviour (McCoy & Fowler 2004; Khan et at. 2011; Al-Daeef et al., 2017).

Emails have the advantage of being an inexpensive delivery method, that is effective at providing periodic security awareness information to a large audience situated in wide geographical areas. Well-read and understood emails increase the audience's security awareness knowledge. They also provide the audience with readily and always available security awareness information. The audience can access the emails and learn at their own pace because they are always available in their inbox (Khan et al., 2011; Alotaibi & Alfehaid 2018; Mathoosoothenen et al., 2017).

2.3.3 Group dialogue

Group dialogue is defined as an informal meeting of 15-20 participants in which free-flowing security awareness discussions are held. The group can discuss the organization's cyber security policy or freely pick cyber security topics. During these discussions, participants contribute their viewpoints and share their cyber security knowledge and experiences. Experiences include the cyber security incidences the participants have encountered and their consequences. By sharing, participants get to learn about other participants' cyber security attitudes. Shared learning promotes social norms which are effective in changing behaviour. The discussions also capture the participant's attention thus increasing their cyber security knowledge (Khan et at. 2011).

2.3.4 Posters

A poster is a large, printed picture, photograph, or notice used to capture the audience's attention and deliver a security awareness message. Posters are especially effective in announcing security awareness messages if they have an attractive design and a caughty phrase (Khan et al., 2011; Al-Daeef et al., 2017). Posters are also used to reinforce security awareness messages (Chmura 2017). The location of a poster plays a big role in capturing the audience's attention. Therefore posters should be placed in highly visible areas e.g. the cafeteria or office building entrance (Abawajy 2014). Posters are a cheap delivery method although there is a limit to the amount of information that can be placed on a poster. Posters lack social norms which are important in changing attitudes and behaviour (Khan et al., 2011).

2.3.5 Articles and newsletters

A newsletter is a monthly or quarterly cyber security report distributed to audiences within an organization. Newsletters can be in print or electronic format and are usually 1-4 pages long. They discuss emerging cyber security threats e.g. a newly discovered malware and inform about the occurrence of a cyber security incident (Chmura 2017; Al-Daeef et al., 2017). Newsletters can also be used to deliver knowledge on a selected cyber security topic apart from being a cyber security report (McCoy & Fowler 2004). Newsletters are informative and good at knowledge transfer thus resulting in behaviour change (Khan et at. 2011). They pass more than one security awareness message at a time compared to posters and are effective in delivering periodic information (Alotaibi & Alfehaid 2018). However, just like emails, newsletters can be mistaken for spam. They also do not guarantee that the audience has understood and internalized the information they contain. Newsletters lack social norms which are important in changing attitudes and behaviour (Khan et at. 2011).

2.3.6 Computer-Based Training (CBT)

CBT delivers security awareness content through stand-alone or networked computers. The content is available to the audiences at all times without the pressure of having to attend lectures, seminars, and workshops. The audience can learn at their own pace as a result (Khan et at. 2011). CBT caters to audiences within the organization unable to attend security awareness conducted through other methods (McCoy & Fowler 2004). Security awareness content delivered through CBT is mostly generic and not customized to meet an organization’s security awareness

requirements. Therefore financial investment is required to customize CBT security awareness content. CBT also lacks the human interaction found in education presentation and may therefore not be effective in changing cyber security behaviour and attitudes (Khan et al., 2011).

2.3.7 Educational films

Educational films are movies, animations, and multimedia content whose primary purpose is education. Educational films ensure that security awareness content is available to the audience at all times. Therefore the audience can commence and end training at any time. Educational films keep the audience motivated because they are entertaining. However, the production cost of an educational film can be expensive. They also lack the interactivity found in educational presentations between the instructor and audience (Chmura 2017).

2.3.8 Web-based training

Web-based training utilizes the online environment to deliver, administer and analyze security awareness training. The audience access security awareness websites that provide and test their security awareness knowledge (McCoy & Fowler 2004). Security awareness knowledge increases after taking an online security awareness test (Al-Daeef et al., 2017). The websites have helpful discussion forums where the audience can discuss cyber security issues amongst themselves and with cyber security experts (Mathoosoothenen et al., 2017). Web-based training is user-friendly and provides the audience with flexibility because the content is delivered via the web. Therefore the security awareness content is always available. Unfortunately, web-based training may not challenge the audience enough. The delivery method is one way thus lacks interactivity and can be monotonous. Since the audience is free to learn at their own pace, the audience may allocate little time for security awareness training (Alotaibi & Alfehaid 2018).

2.3.9 Factors affecting the choice of a delivery method

The factors that affect the choice of delivery methods during security awareness training are (Mathoosoothenen et al., 2017):

1. Effectiveness of the delivery method - in promoting the audience's active learning process.

2. Time flexibility of the delivery method - in providing the audience ample time to learn during the security awareness training.
3. The Scalability of the delivery method - determines the ability of the delivery method to reach a wide audience during the security awareness training. Some delivery methods have a wide reach while others have limited reach.
4. The cost-effectiveness of the delivery method - determines whether the security awareness training can be implemented within budgetary constraints. Some delivery methods are expensive to implement while others are cheap.
5. The scope of the delivery method - determines the number of cyber security topics the delivery method can deliver to an audience during security awareness training. Some delivery methods have a wide scope and can be used to deliver a wide variety of cyber security topics while others have limited scope.
6. The accessibility of the delivery method - determines how often the audience can access the security awareness content during training. In some delivery methods, the security awareness content is accessible to the audience at all times while in others access to the content is limited to specific times.
7. The ability of the delivery method to be customized - some delivery methods can be customized to meet individual and organizational security requirements.
8. Ease of update of the delivery method - to keep up with the fast-changing cyber security threat landscape. Some delivery methods are rigid and do not allow for content to be easily and quickly updated.
9. The level of engagement of the delivery method - ensures that the audience's attention is captivated in a fun and entertaining manner.
10. The responsiveness of a delivery method - allows the audience to give feedback during security awareness training.
11. The measurability of the delivery method - enables metrics to be used to evaluate the effectiveness of the delivery method during security awareness training.
12. The ability of the delivery method to be supervised - giving management oversight during security awareness training.

2.3.10 Security awareness delivery methods challenges

The challenges security awareness delivery methods face during implementation include:

1. New technology - the audience is sometimes required to learn new technology to enjoy the benefits of some delivery method e.g. learn to use a new application during computer-based training. Learning new technology alongside security awareness training could be mentally exhausting and result in a poor understanding of security awareness content (Alotaibi & Alfehaid 2018).
2. Out of date delivery methods - some of the delivery methods are old-fashioned and were designed to provide security awareness to the older generation. These methods are not designed to provide security awareness to the digitally native younger generation (Wolfenden 2019; Ariffin et al., 2016).
3. Updatability - cyber security is a rapidly evolving field with new threats and evolving mitigation mechanisms. Some delivery methods cannot be easily and regularly updated and may therefore lack up-to-date information (Alotaibi & Alfehaid 2018).
4. One size fits all – most delivery methods are designed to deliver a security awareness message to a generalized audience. Therefore the delivery methods do not consider different preferences and requirements amongst the audience. Few delivery methods can be customized to meet individual preferences and requirements (Alotaibi & Alfehaid 2018).
5. Information overload – some delivery methods provide users with unnecessary information which tends to overshadow the important security awareness information. The audience is demotivated and retains less information as a result of information overload (Alotaibi & Alfehaid 2018).
6. Inconsistent - for the audience is to follow and understand security awareness training there has to be consistency. Security awareness training should be conducted and reinforced regularly. Some delivery methods are not designed to provide continuous security awareness training (Alotaibi & Alfehaid 2018; Nagarajan et al., 2012).
7. Poor communication - the delivery methods fail to communicate the importance of cyber security. If the audience does not understand the importance of cyber security, whatever delivery method is used is unlikely to change their attitude and behaviour. Few delivery methods fully engage the audience during security awareness training (Alotaibi & Alfehaid 2018). Delivery methods that are dependent on an instructor succeed or fail on the communication abilities of the instructor (Nagarajan et al., 2012).

8. Lack of management support - management support plays an important role in the success of security awareness training. Some delivery methods require a large financial investment by the organization and therefore management support is important (Alotaibi & Alfehaid 2018).
9. Realist – the delivery methods may be unable to realistically simulate cyber security scenarios, incidences, and their consequences. As a result, the audience is unable to transfer the knowledge acquired during security awareness training to their everyday life experiences (Nagarajan et al., 2012; Reeves et al., 2021).

Figure 7 below lists the good qualities of a security awareness delivery method.

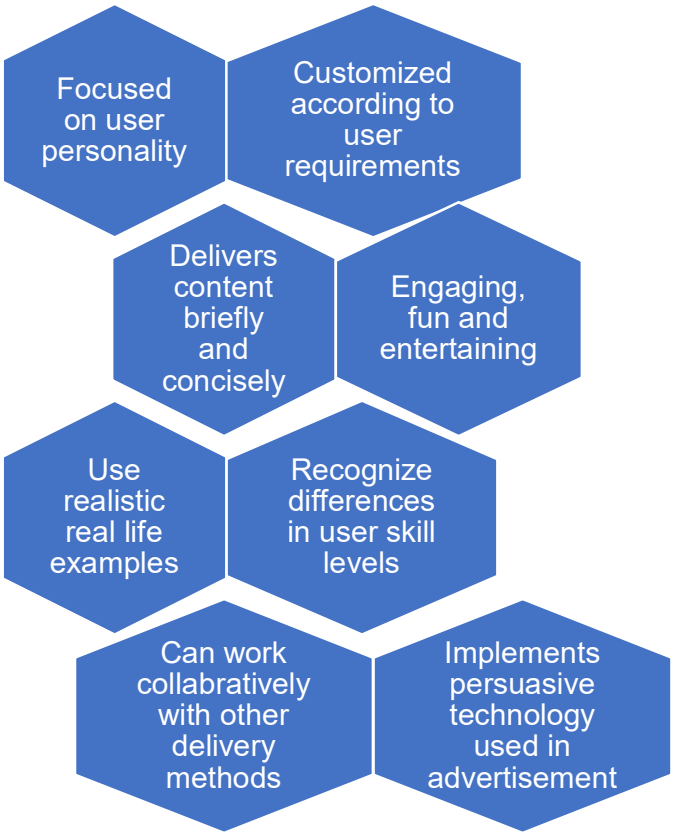


Figure 7: Qualities of a good security awareness delivery method (Alotaibi & Alfehaid 2018)

2.4 Gamification

Gamification is increasingly being used in education to improve learning outcomes in a fun and entertaining manner. Gamification has revolutionized education with player engagement being a high priority (Kocakoyun & Ozdamli 2018). Gamification can be

applied in security awareness training to improve cyber security knowledge and skills in a fun and engaging manner. By seamlessly blending entertainment, competition and learning gamification can increase enthusiasm during security awareness training (Rieff 2018; Armstrong & Landers 2018). It takes advantage of the addictive nature of the human brain to create enthusiasm and motivation lacking in current security awareness training (Holdsworth & Apeh 2017).

Silic & Lowry (2020) define gamification as utilizing game mechanics and concepts in day-to-day life in an engaging, entertaining, and robust manner to improve the player experience. Rieff (2018) defines gamification as using game concepts such as rewards, feedback, progress report, collaboration, problem-solving, stories, and competition in non-gaming situations. Gamification of security awareness is the use of game concepts during security awareness training to increase player motivation and engagement (Gjertsen et al., 2017). The process of gamification is shown in figure 8 below. There is a difference between gamifying content and the gamification method. Gamifying content converts security awareness content into a story or animation. This conversion makes the content more descriptive, explanatory, and also introduces an entertaining element. However, there is a risk that in the process of gamifying content the converted content becomes unrecognizable to the player. As a result, the security awareness training objectives are missed. In gamification the security awareness content remains the same, the difference being the introduction of game elements to the content (Armstrong & Landers 2018).

Mostafa & Faragallah (2019) define a game as an artificial system in which players follow provided rules to achieve set objectives or overcome obstacles. Games provide players with a virtual environment that is similar to their real-world environment. They use these virtual environments to practice, get hands-on experience and explore the consequences of their actions. The best way to learn and understand is through trial and error (Alotaibi et al., 2016; Wolfenden 2019). By practising in a virtual environment players can learn, improve, and reinforce good cyber security behaviour (Rieff 2018). Games also satisfy other requirements such as skill-building, mastery, socializing, and prestige. There are a lot of benefits to be gained from gamification if it is applied to the right players and in the correct context (Gjertsen et al., 2017).

The use of games in learning is referred to as game-based learning. Game-based learning has been used in education, health, advertising, and behavioural science (Alotaibi et al., 2016). Le Compte et al., (2015) define serious games as games that have a purpose besides entertainment. Serious games are used to promote learning and behavioural change.

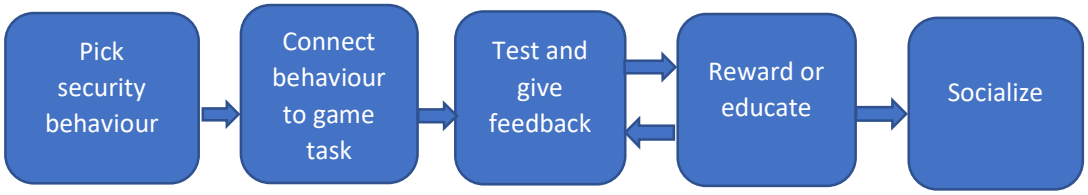


Figure 8: The process of gamification of security awareness (Holdsworth & Apeh 2017)

Armstrong & Landers (2018) propose the following steps when implementing gamification in security awareness. Firstly the security awareness training goals need to be set within the organization. This is done by identifying the knowledge, skills, and performance gaps that exist in the current security awareness training. Secondly, an initial security awareness game is developed. This involves the selection of appropriate game design elements which are discussed later in this section. Game elements incorporate theoretic knowledge in education and psychology during game development. They also incorporate instructional best practices during game development. Thirdly, the organization conducts security awareness training using the developed game. After the initial security awareness training, data is collected to evaluate the game's effectiveness and appropriateness of the game elements used. Lastly, redesign and refinement of the game and its game elements are undertaken. These adjustments are done according to the feedback collected. These steps are performed iteratively until the desired cyber security knowledge and behavioural outcomes are achieved from the security awareness game.

Security awareness games should be customization to meet individual player and organizational requirements (Underhay et al., 2016). Customizing the games makes their content more relatable, relevant, and understandable to the player (Rieff 2018). The focus of gamification in security awareness training is to increase player motivation. Games accomplish this because they involve more than just gaining cyber security knowledge, they require the practical application of this knowledge. Games also can focus players' attention and alert them of their progress through continuous

feedback and these are accomplished by implementing game elements (Gjertsen et al., 2017; Rieff 2018).

2.4.1 Types of games

Gamification of security awareness manifests itself differently in the form of different types of games. Security awareness games can be deployed as (Mostafa & Faragallah 2019; Shostack 2021; Wolfenden 2019).

1. Board games – board games are tabletop games involving two or more players in the competition. The players move or places pieces or pre marked playing surfaces. A board game may feature dice, cards, virtual money, and token pieces representing the different players.
2. Card games – card games are tabletop games played using a deck or pack of cards that are identical in shape and size. Cards have two sides the face and the back. The back of a card is indistinguishable, and the face of a card is unique and contains some information.
3. Computer games – computer games are electronic games in which the player interacts using an input device e.g. controller, joystick, keyboard, and motion-sensing device. Players receive audio and visual feedback from visual display units and speakers.
4. Escape room – escape room is a game where a player or a team is locked in a room with the goal of escaping the room. They are required to solve a series of puzzles within a set amount of time. Solving the puzzles results in finding the key to unlock the room.
5. Virtual reality (VR) - VR games immerse players into a 3D virtual environment. It provides players with interactivity through audio, visual, and haptic feedback. VR technology has become more affordable and accessible hence it is widely used by games (Veneruso et al., 2020). Augmented reality (AR) is an enhanced version of the real-world achieved using visual, sound, and sensory digital technology (Alqahtani & Thorne 2020).

2.4.2 Game elements

Scholefield & Shepherd (2019) define game elements as the components that make up a game. It is also referred to as game attributes. Game elements make security awareness games enjoyable while maintaining their learning aspects (Gjertsen et al.,

2017). The target audience and the game's intervention purpose determine the game elements used (Armstrong & Landers 2018).

The game elements essential in security awareness games are (Armstrong & Landers 2018; Antonaci et al., 2017; Scholefield & Shepherd 2019; Gjertsen et al., 2017; G-Cube 2016; Kapp 2014).

1. Conflict – conflict presents players with tasks to conquer which capture their attention. These tasks could be an obstacle to overcome, combat with another player, or a puzzle to solve. Conflict could also take the form of a collective challenge that requires collaboration to overcome. A game could incorporate cyber security conflict from which players learn to deal with such situations. Players are thus equipped with the necessary cyber security knowledge and skills to overcome similar real-life conflicts.
2. Strategy and chance – strategy games empower players with control, therefore decisions made by the player affect the course of the game and the odds of achieving their goals. In a game of chance, players react to random outcomes from the game. This results in uncertainty for the player which creates excitement. Security awareness games should incorporate both strategy and chance. Such that during gameplay the problems a player encounters are based on chance and the solution are based on strategy.
3. Aesthetics – the game should have an appealing look to be able to attract players. The game's visuals have the power to capture a player's attention and immerse them into the game. Aesthetics are not so important in security awareness games, but they should not be overlooked either.
4. Theme and story – themes contain the game's subject matter and create a connection between the game and the players. They provide the game's background story and are usually included in the rules. Stories provide a narrative throughout the game. Players find it easy to remember facts that are part of a story as opposed to facts that are out of context.
5. Rewards – are things a player earns as a result of achieving or accomplishing a set task in a game. Armstrong & Landers (2018) define rewards as digital tokens that represent achievement. Rewards such as points, and badges boost players' status. In a security awareness game, rewards should be awarded to players on

completion of a task according to set proficiency standards. Players should understand how to accrue rewards because they are a powerful feedback tool.

6. Mystery – a game should have a gap between the known and the unknown. Players should be aware of this gap and should search for information to fill this gap. Mystery provokes a player's curiosity to learn and motivates the player to find the missing information. In a security awareness game knowing where to find the organization's cyber security policy could be akin to finding the hidden key to unlock a door.
7. Challenge – games should challenge players at every opportunity. Security awareness games learning modules should start with a challenge, which activates players into critical thinking and problem-solving.
8. Penalty – is the opposite of reward. Players in the game should be required to start afresh or lose points as a result of wrong decisions. When the stakes are high in a game players pay close attention to the game and the learning within the game. Penalty in security awareness games prepares players for the consequences of cyber security mistakes in the real world.
9. The opportunity of mastery – a game should provide players with an opportunity to have mastery of the subject matter. The game should have visible signs to show a player's mastery. When a player conquers a level or solves a puzzle the game should promote the player to the next level. Game levels should get progressively more advanced and difficult as the player learns more and progresses further in the game.
10. Visibility of progress – games should give players feedback on their performance. Security awareness games should inform players of their progress through the learning modules. The progress report should be constantly updated and not only provided at the end of the game. It could be implemented as a progress bar in the game.
11. Emotional content – games should bring out the human emotions in players such as frustration, excitement, anger, happiness, sadness, and joy. This is in contrast to the educational presentation which has no emotional content. Security awareness games should encourage and embrace these emotions, thereby eliciting a strong emotional reaction from players. Players remember content better when they have a strong emotional attachment.

2.4.3 Game genres

Game genres consist of games grouped because they are of a particular type or share a similar style (Mostafa & Faragallah 2019; Nagarajan et al., 2012). Game genres provide game designers and the player with an idea of the nature of the game and the skills required to play the game. Security awareness games usually implement multiple genres (Nagarajan et al., 2012). Listed below are some game genres and their applicability is security awareness games:

1. Action genre – these games provide players with an adrenaline rush that keeps them involved at all times. The games require hand-eye coordination and quick reflexes. The player is also required to make quick decisions with little time for deliberation (Nagarajan et al., 2012; Mostafa & Faragallah 2019). Games that require players to protect themselves against cyber-attacks e.g. tower defence games implement action genre (Nagarajan et al., 2012).
2. Role-playing genre – these games require players to assume character roles in a fictional setting. Players act out the fictional character role according to the game's rules or story. They make decisions and strategize based on their character's role**.** Role-playing genre games have well-developed storylines and are played over a longer period. Role-playing games (RPG) focus on a player's character growth, as the game progresses players obtain more experience and capabilities. This is accompanied by the increased complexity of the game's challenges (Nagarajan et al., 2012; Mostafa & Faragallah 2019). Games that require players to take various roles e.g. system administrator charged with the responsibility of protecting a server or hacker required to break into a system to obtain information needed to save a hostage implement role-playing (Nagarajan et al., 2012).
3. Simulation genre – these games build replicas of real-world activities in the form of scenarios for training (Nagarajan et al., 2012; Mostafa & Faragallah 2019). Simulation games use models which are a physical, mathematical, or logical representation of a system or process. These models are mapped to real-world cyber events from which scenarios emerge. Models create a normalized view of the cyber security situations and simulations building of scenarios that imitate attacks on infrastructure with specific security controls (Zoto et al., 2018). The simulation genre is used to model a network environment with realistic traffic and

network activities. Players are therefore required to defend or attack this network model (Nagarajan et al., 2012).

4. Adventure genre – these games have a storyline full of exploration and puzzles. Players are required to solve puzzles to enable them to open up additional areas of exploration. Players piece together the storyline by solving puzzles (Nagarajan et al., 2012; Mostafa & Faragallah 2019). The adventure genre is used to train disaster recovery operations after a security breach (Nagarajan et al., 2012).
5. Sports genre – these games require team formation and assignment of roles to each member. Team members perform their roles that contribute to the team's overall success. They normally work together towards a common goal (Nagarajan et al., 2012; Mostafa & Faragallah 2019). The sports genre can be implemented in security awareness games to train players on their roles during a cyber-attack or network defence (Nagarajan et al., 2012).
6. Casual genre – these games are easy to learn and master and are mostly video game versions of a board or card games. Each play session starts a new game, games do not continue from a previous session (Nagarajan et al., 2012; Mostafa & Faragallah 2019). In security awareness games casual genre can be used to familiarize and train players on basic cyber security terminology and techniques (Nagarajan et al., 2012).
7. Capture the flag (CTF) genre – these games set opposing players against each other in a test of their cyber security skills. Players work alone or as part of a team to solve a series of challenges with increasing difficulty. Once a challenge is solved the player or team receives a flag which is a measure of success. CTF games are timed, once the time expires the flags received are tabulated (Prinetto et al., 2020). Capture the flag game can either be attack-defend CTF or jeopardy CTF. In attack-defend CTF players attack the opponents to capture the flag while defending their flag. Flags are files in the opponents' server. In jeopardy CTF, players have to solve puzzles to capture the flag (Wen et al., 2019).

2.4.4 Game dynamics

Game dynamics describe the pattern of how the game and player evolve giving the player a reason to keep playing. Players have different preferences, some are competitive while others are collaborative. Game dynamics customize the game mechanics to address the individual player motivation for playing (Nagarajan et al.,

2012). Below are some game dynamics and their application in security awareness games (Nagarajan et al., 2012):

1. Territorial acquisition dynamic revolves around limited resources. The player's focus is to acquire as much of this limited resource as possible with the goal of strategically controlling it. The limited resource could be network bandwidth, computer memory, or servers in a security awareness game.
2. Prediction dynamic prompts players to guess the future and rewards players for correct guesses. Players could be rewarded for correctly guessing the source of the next cyber-attack in a security awareness game.
3. Spatial reasoning dynamics involve puzzles. Players could be required to use puzzles to develop a defence in depth cyber security strategy in a security awareness game.
4. Survival dynamic taps into the human instinct of self-preservation with the game focusing on life and death struggles. Players could be required to protect a dying server from cyber-attacks in a security awareness game.
5. Destruction dynamic has the goal of destroying everything in sight. Players could be required to destroy all viruses or intruders residing within a network in a security awareness game.
6. Building dynamic focuses on developing a better player or environment. Players could be required to build a secure network or protect themselves in an online environment in a security awareness game.
7. Chasing and evading dynamic has the goal of either capturing prey or evading a predator. Players could take the role of a hacker required to attack a network while evading detection. Alternatively, the player could take the role of a system administrator hunting for network threats in a security awareness game.
8. Trading dynamics is prevalent in tabletop games and involves negotiation and collaboration i.e. players exchanging resources. Players may be required to purchase cyber security resources and make tradeoff decisions based on the available resources in a security awareness game.
9. Race to the end dynamics involves competition to arrive at a destination first. Players could compete to be the first to fully secure a network or get a software update in a security awareness game.

Figure 9 below lists the attributes essential in a security awareness game.

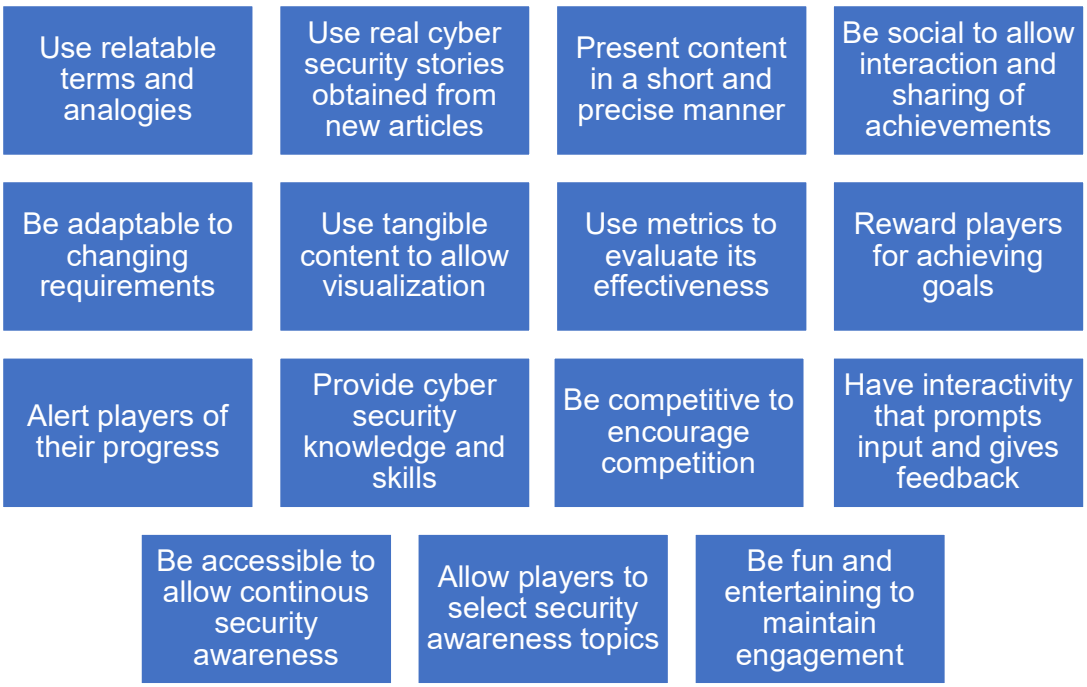


Figure 9: Good attributes essential to a security awareness game (Gjertsen et al., 2017)

3 Methodology

Kitchenham et al., (2009) defines systematic literature review as a form of secondary study on a research question where all relevant information regarding a research question is collected, analyzed, and synthesized. Through a systematic literature review, papers that provide a better understanding of previous studies conducted on a research topic can be found. Thus strengthening knowledge and identifying research gaps on the research topic. The identification of research gaps is useful in providing future research direction on the topic (Paul & Criado 2020). Kitchenham et al., (2009) states that a systematic literature review has the following steps:

1. Definition of a research question.
2. Literature search process.
3. Inclusion and exclusion criteria applied to the literature.
4. Assessment of the quality of the literature.
5. Extraction of data from the literature.
6. Data analysis.
7. Interpretation of the literature results.

The 1st step is defining the purpose of the literature review. The purpose of this review is to assess games used in cyber security awareness training. This systematic literature review aims to answer the research question:

RQ1: "What is the state of the art of cyber security awareness games?"

The objectives within this research question are to:

1. Identify the purpose and topics taught by cyber security awareness games
2. To understand the deployment methods used by the cyber security awareness games
3. To identify the target audience of cyber security awareness games
4. To explore the different game genres implemented by the cyber security awareness games
5. To examine the learning mechanics applied by cyber security awareness games

The 2nd step is a literature search which was conducted on scientific digital databases between 12th and 14th May 2021. The search resulted in academic papers published in journals, workshops, and conferences. It was conducted in English therefore the

search results were limited to English papers. There were no geographic limitations specified during the search therefore it yield academic papers from around the globe.

3.1 Search terms

The search terms cyber security, games, and awareness were used during the search. These terms were chosen because they best answer the research question i.e. gamification of cyber security awareness. Search terms help determine the scope of the thesis and provide the best literature coverage across the digital libraries (Connolly et al., 2012; Petri & von Wangenheim 2017). Cyber security is a broad term and has many variants which have evolved. Therefore the terms information security, information assurance, computer security, communication security, data security, and network security can be used instead of cyber security (Olijnyk 2015). Table 1 below shows the search terms and the synonyms used during the digital database search.

Terms	Synonyms	Sources
Cyber Security	"information security" OR "information assurance" OR "computer security" OR "communication security" OR "network security" OR "social engineering" OR "phishing" OR "passwords" OR "ransomware" OR "malware" OR "privacy" OR "digital citizenship" OR "NotPetya" OR "internet security"	Zhang-Kennedy & Chiasson (2020); Hendrix et al., (2016); Olijnyk (2015); Roepke & Schroeder (2019)
Games	"gamification" OR "game-based learning" OR "gamified" OR "simulation" OR "game elements" OR "capture the flag" OR "augmented reality"	Zhang-Kennedy & Chiasson (2020); Connolly et al., (2012); Battistella & Wangenheim (2016); Sardi et al., (2017); Roepke & Schroeder (2019); Petri & von Wangenheim (2017)
Awareness	"perception" OR "understanding" OR "realization" OR "training" OR "learning" OR "education" OR "compliance" OR "impact" OR "change" OR "literacy" OR "decision making" OR "human-centred"	Zhang-Kennedy & Chiasson (2020); Connolly et al., (2012); Battistella & Wangenheim (2016); Petri & von Wangenheim (2017)

Table 1: The search terms, synonyms, and sources

3.2 Databases searched & the search strategy

From the wide variety of digital databases, 2 that collect high impact academic papers and are often used by researchers was selected. For this systematic literature review

Elsevier's database i.e. Scopus and, Clarivate Analytics' database i.e. Web of Science was used. Scopus is a highly interdisciplinary database that has global geographical coverage of academic literature. Scopus outperforms Google scholar in terms of accuracy, consistency, and coverage of academic papers (Hendrix et al., 2016). Web of Science is the oldest bibliographic database, which allows researchers to search, filter, and analyze papers on a given topic (Mongeon & Paul-Hus 2016). Peer reviewed papers published in conferences, workshops, and journals were searched with a focus on papers that theoretically or empirically discussed games used in cyber security awareness.

The Boolean "OR" was used to combine the search term and synonyms. The search terms were combined by the Boolean "AND". The search string was applied to the digital database's metadata i.e. article title, abstract, and keywords. The search string was calibrated to suit different libraries because they have different string structures. After each query, the search string was recalibrated and adapted to get the best query results (Petri & von Wangenheim 2017; Sardi et al., 2017). Table 2 below shows the scientific digital databases searched and the number of hits on each digital library.

Library	Delimitation criteria	Hits
Scopus	Language: English Document type: Conference, Workshops, and Journal literature. Publication year: 2010 to 2021	275
Web of Science	Language: English Document type: Conference, Workshops, and Journal literature. Publication year: 2010 to 2021	231

Table 2: The digital online libraries searched and the search results

Some of the papers found from the digital libraries were used to find additional papers of interest. This was done by looking at the reference section of interesting papers to find papers they referenced in a backward snowball effect of the paper collection. The popular search engine Google Scholar was used to search for snowball papers using their titles. Google scholar is a good source of academic papers on serious games. It is also a good source of academic papers published outside the computing domain (Petri & von Wangenheim 2017; Hendrix et al., 2016).

3.3 Data Extraction and synthesis

The query on the two online libraries returned a total of 506 academic papers which were exported to a Microsoft Excel file. The search results from Google scholar were downloaded and the paper's information was manually input into the Excel file. The information extracted, catalogued, and input into the Excel file from the papers were:

1. The title of the paper.
2. A list of contributing authors.
3. Year of publication of the paper.
4. The paper volume, issue, and the number of pages.
5. An URL link to the paper.
6. The paper source and document type.
7. The paper target population.
8. The context in which the paper is written.
9. The language used to write the paper.
10. The abstract of the paper.
11. Keywords used in the paper.

In the Excel file, the papers were classified according to (PICO) population, intervention, context, and outcome (Soomro et al., 2016). I used Juypter notebook pandas to organize and remove duplicate papers from the search results since the two digital libraries complement each other. This process resulted in a total of 214 unique papers. The papers were screened using preferred reporting items for systematic reviews and meta analyses (PRISMA) methodology. During prescreening, the paper's title was read and papers whose title did not answer the research question or contained content not applicable to the research topic were removed. After prescreening, a total of 198 papers remained. The inclusion and exclusion criteria were applied to these remaining papers. This was done by reading the paper's metadata i.e. title, keywords, and abstract and applying the inclusion and exclusion criteria mentioned below. After this process, a total of 78 relevant papers remained.

3.4 Inclusion and exclusion criteria

The 3rd step is the application of inclusion and exclusion criteria to remove literature beyond the scope of the systematic literature review. By reviewing the paper's

metadata and setting inclusion and exclusion criteria relevant papers to the research question remained. The inclusion criteria were:

- Papers that focused on cyber security awareness of children, youth, and adults.
- Papers that used games and gamification as a method of cyber security awareness training.
- Papers that had empirical evidence on the impact of gamification in knowledge, behavioural and attitudinal change during cyber security awareness training.
- Papers that focused on the use of games in cyber security awareness training in a school, university, organization, and general public context.

The exclusion criteria were:

- Papers not written in English even though the abstract is in English.
- Papers published before 2010, this was to avoid using antiquated data.
- Papers on gamification of education on topics not related to cyber security awareness.
- Papers not available or accessible via the university online access.
- Papers focused on gamification of cyber security awareness for experts.
- Papers from books, white papers, short papers, and reports issued by companies.

3.5 Screening using PRISMA

To assess the paper quality papers were screened using PRISMA guidelines. Preferred Reporting Items for Systematic Reviews and Meta-Analysis (PRISMA) brings transparency and accountability in a systematic literature review. The guidelines consist of a checklist and a flow diagram shown in figure 10 below. The checklist determines which data should be included in the SLR and the flow diagram ensures transparency of the papers used in the systematic literature review (Moher D et al., 2009). The 78 relevant paper's metadata i.e. title, keywords, and abstract were read to identify papers featuring the intervention of games during cyber security awareness training. In situations where this was not clear from reading the paper's metadata, the paper's full text was read. Papers that answered the research question were selected for review. Papers whose metadata or full text did not answer the research question were excluded. Screening is also done to ensure the papers used in the systematic literature review were manageable (Khando et al., 2021).

3.6 Analysis and synthesis of results

After the literature search, a total of 40 papers describing 31 security awareness games were analyzed in detail. Some early developed and popular games e.g. CyberCIEGE and Anti-Phishing Phil were described by 2 or more papers. I categorized the papers describing the games into two broad categories. One category had papers describing games that introduced players to a single cyber security topic. The other had papers describing games that introduced players to multiple topics. Primary information regarding these games was obtained from the papers. The papers were expected to have information on the games regarding the topics taught, the game genres implemented, and the target audience. Secondary information regarding the game was obtained from the actual website containing the games whenever this was possible.

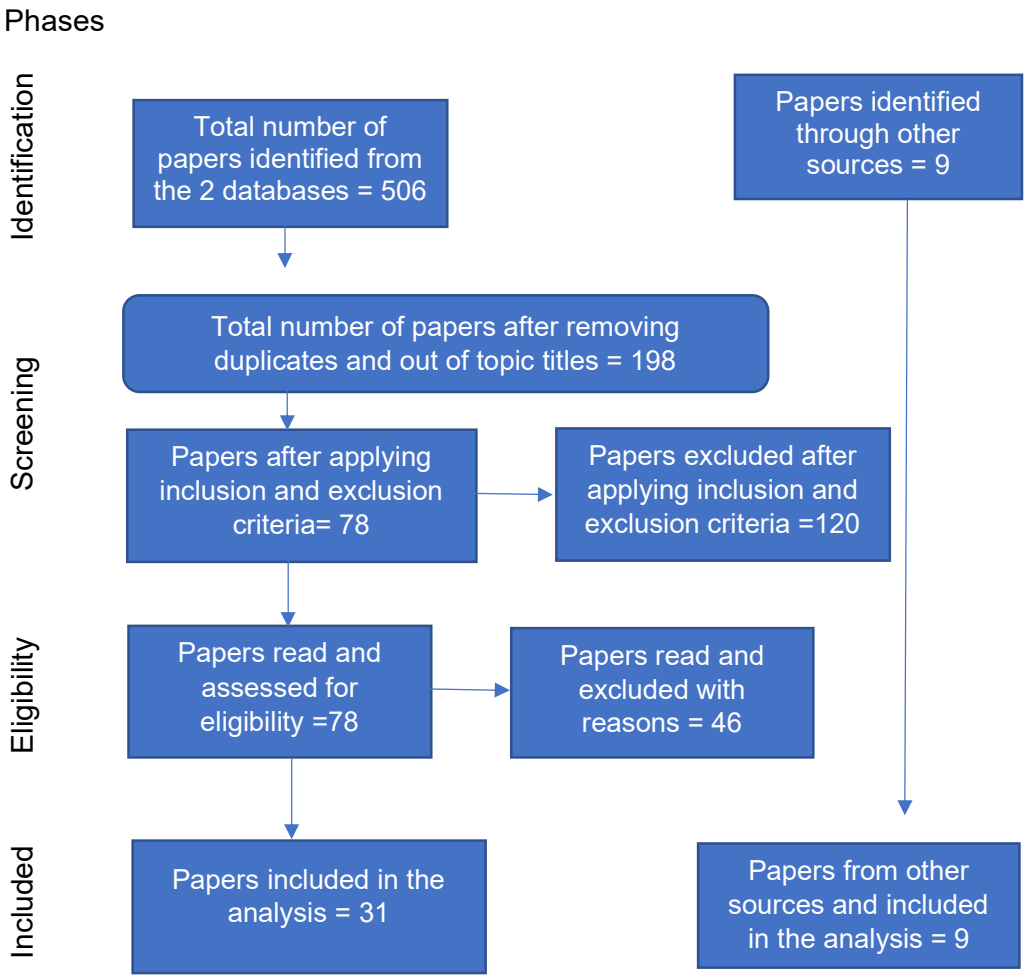


Figure 10: Literature screening using PRISMA flow diagram

4 Results

4.1 Identify the focus of security awareness games

Addressing the first objective I report the general focus of security awareness games. I categorize the papers as those describing specific purpose security awareness games and those describing multipurpose security awareness games. Specific purpose security awareness games have a narrow scope and focus on a singular cyber security topic. Multipurpose security awareness games have a wide scope and focus on multiple cyber security topics.

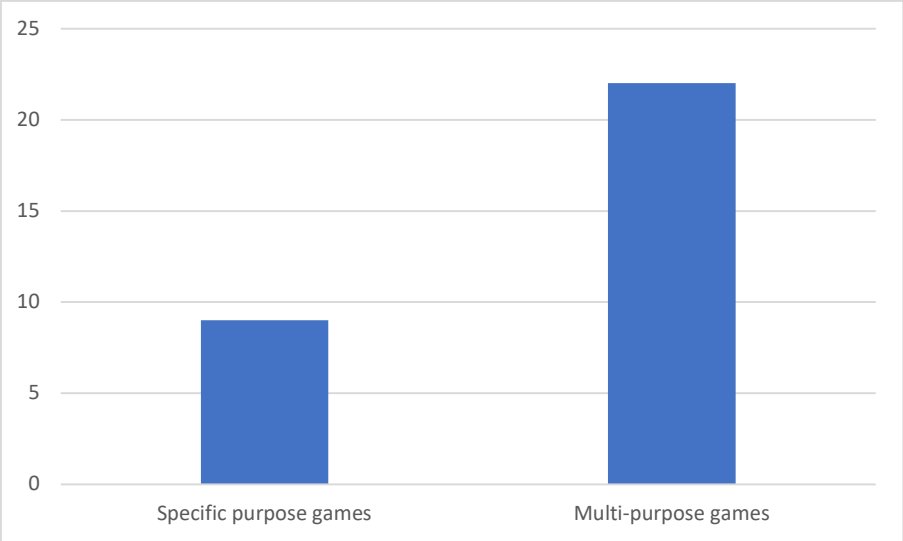


Figure 11: Security awareness games focus

Figure 11 shows that of the reviewed papers, 9 specific purpose security awareness games are described. The 9 games described by these papers introduced players to a single topic such as social engineering, password management, or software threat modelling as shown in table 3 below. The remaining papers described 22 multipurpose security awareness games as shown in table 4 below. The games introduced players to multiple topics with varying levels of detail.

4.2 Identify the topics taught by security awareness games

Addressing the second objective I report the various topics taught by the security awareness games. Since specific purpose security awareness games focus on one cyber security topic. I categorize the games according to the subtopics taught within the broader topical area of their focus. Social engineering is a broad topical area with many subtopics such as URL, social media, phishing emails, tailgating, shoulder

surfing, voice of authority, impersonation, spear phishing, and dumpster diving (Röpke et al., 2020). Specific purpose games focused on social engineering tend to introduce the player to one or more of the aforementioned subtopics.

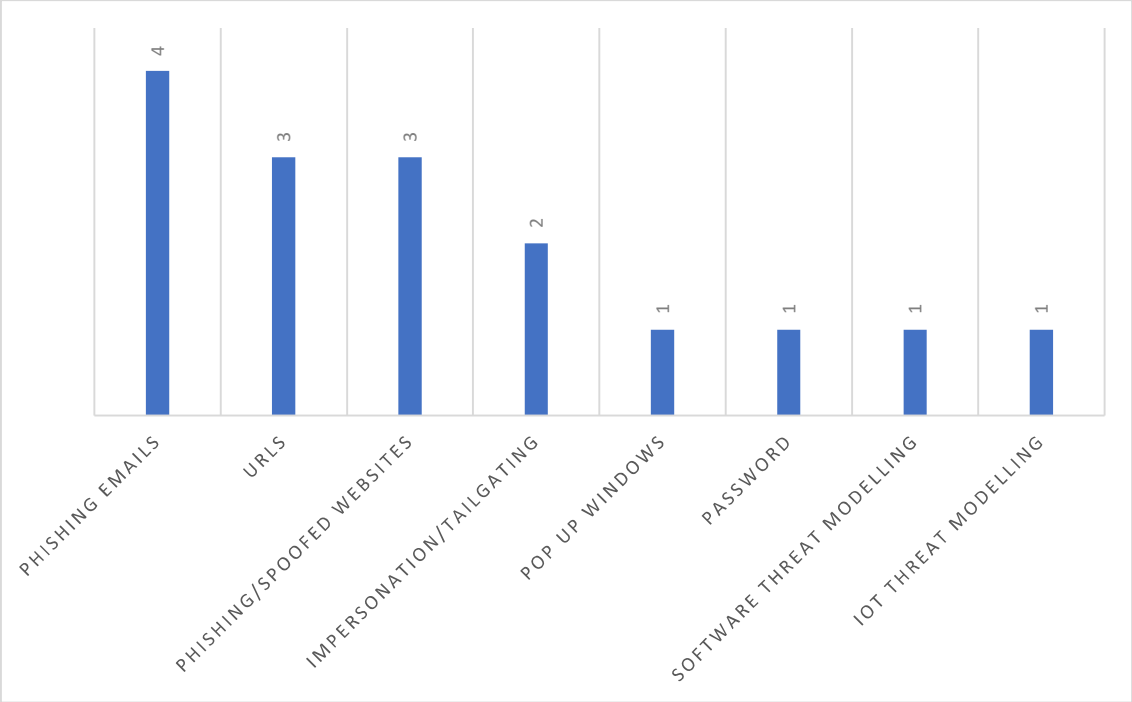


Figure 12: Topics of specific purpose security awareness games

Figure 12 shows that of the 9 specific purpose games, 4 focused on phishing email subtopic. URLs and phishing websites subtopic was the focus of 3 games each. Impersonation/tailgating was the focus of 2 games. 1 game each focused on the broad topics of passwords, software threat modelling, and IoT threat modelling. It is important to note that some specific purpose games introduced players to two or more subtopics within one topical area e.g., some games focused on the topic of social engineering introduced players to both phishing emails and phishing websites subtopics.

Appropriate use of hardware, software management, access control, password management, and social engineering are important topics that security awareness games should cover (Le Compte et al., 2015). Figure 13 below shows that the topic of password management was featured in a majority of the multipurpose security awareness games. 15 of the 22 multipurpose games introduced players to this topic in one form or another. Software management and social engineering are the 2nd and

3rd most popular topics featured in multipurpose games. 13 multipurpose games introduced players to software management while 12 games introduced players to aspects of social engineering. Appropriate use of hardware and access control are the least popular topics featured in multipurpose games. 9 games each introduced players to the appropriate use of hardware and access control. As stated earlier all the multipurpose security awareness games featured two or more cyber security topics to be introduced to players.

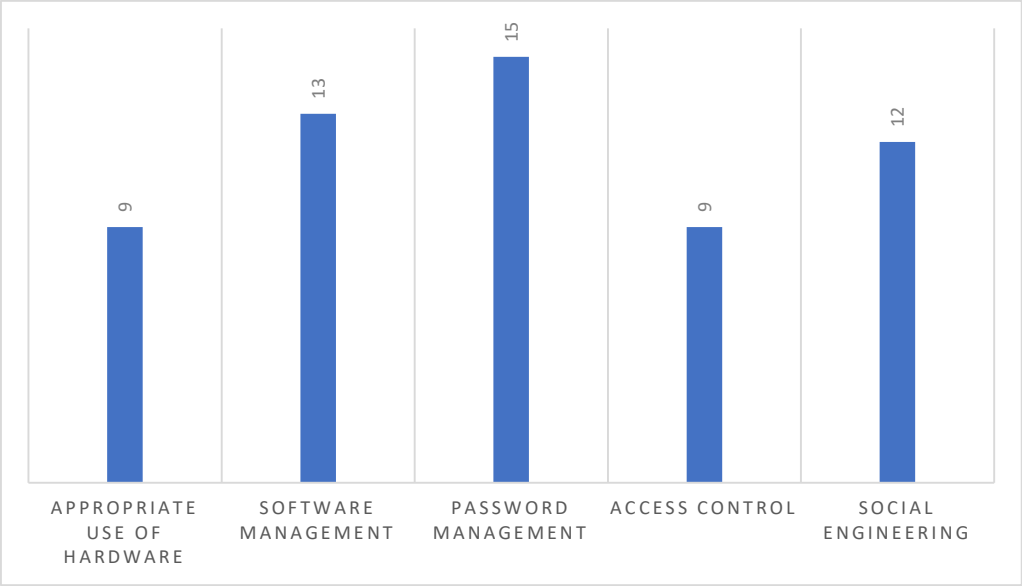


Figure 13: Topics of multipurpose security awareness games

Game name	Cyber security topics	Game genre	Target audience	Deployment method	Reference
Anti-Phishing Phil	• URLs	• Interactive narrative • Role-playing	• General public	• Computer game	Sheng et al., (2007)
Phishy	• URLs	• Adventure • Interactive narrative • Role-playing	• General public	• Computer game	CJ et al., (2018)
What.Hack	• Phishing emails	• Role-playing	• Employees	• Computer game	Wen et al., (2019)
Persuaded	• Baiting • Tailgating • Phishing • Mail attachment • Impersonation • Voice of authority • Pop-up windows	• Turn-based strategy	• General public	• Card game	Aladawy et al., (2018)
Social Engineering Awareness Game (SEAG)	• Basic social engineering concepts	• Quiz	• General public	• Card game • Computer game	Olanrewaju & Zakaria (2015)
CyberPhishing	• Email • Social media • Web browsers	• Simulation • Role-playing	• General public	• Computer game	Hale et al., (2015)
Role-playing quiz application	• Password generation • Password to avoid • Password hygiene	• Role-playing • Quiz • Survival	• General public	• Computer game	Scholefield & Shepherd (2019)

Elevation of Privileges (EoP)	• Spoofing • Tampering • Repudiation • Information disclosure • Denial of service • Elevation of privileges	• Turn-based strategy	• Employees	• Card game	Tøndel et al., (2018); Shostack (2014)
IoT-Poly	• risk identification • risk analysis • risk evaluation	• Turn-based strategy	• Employees • Students	• Card game	Omiya et al., (2019)

Table 3: Names, topics, genre, target audience, deployment methods and sources of specific purpose security awareness games

Game name	Cyber security topic	Game genre	Target audience	Deployment method	Reference
Control-Alt-Hack	• Botnets • Censorship • Unpatched software • Insider threat • Reverse engineering • Social engineering • Tracking	• Role-playing	• Students	• Card game	Aladawy et al., (2018); Le Compte et al., (2015); Denning et al., (2013)
Project config. play	• Authentication requirements • Network configuration • Race conditions • Common vulnerabilities and exposure (CVE)	• Turn-based strategy	• General public	• Boardgame • Card game	Enriquez & Kadobayashi (2018)
Cyber CIEGE	• Cyber security definitions • Information value • Access control • Social engineering • Malware • Data protection • Physical security	• Role-playing	• Employees	• Computer game	Aladawy et al., (2018); Le Compte et al., (2015); Cone et al., (2006)
Network nightmares	• Viruses • Network monitoring • Port vulnerabilities	• Shooter	• General Public	• Computer game	Ryan et al., (2013)
M-learning	• Passwords • Phishing	• Quiz • Survival	• Employees	• Android mobile	Filipczuk et al., (2019)

	• Social engineering • Malware • Data protection			application game	
Integrated ethical hacking toolkit/cyber security awareness game/ educational platform	• Screen and keyboard capture • Web camera and microphone access • Secure file transfer • Command-line injection • Ransomware	• Simulation • Quiz	• General public	• Computer game	Mathoosoothenen et al., (2017)
Hacked time	• Data breach • Cyber security threats identification • Cyber security threats mitigation	• Puzzle • Role-playing • Interactive narrative • Tower defence	• General public	• Computer game	Chen et al., (2020); Chen et al., (2019)
Cyber smart	• Firewall • Safe web surfing • Security software • Secure wireless connection • Passwords • Physical security • Software patching • Network monitoring • Cryptography • Back up • Social media	• Role-playing	• Students	• Computer game	Underhay et al., (2016)

Cyber security requirements awareness game	• Network security • Physical security • Social engineering	• Narrative • Role-playing • Puzzle	• Employee • Students	• A board game that uses a floor map • Cards	Yasin et al., (2018)
Secu-one	• Cyber security threat analysis • Cyber security incident handling • Cyber security countermeasures assessment	• Turn-based strategy	• Students • Employees	• Card game	Omiya & Kadobayashi (2019)
Cyber Agents' Interactive Modelling and Simulation (CyberAIMs)	• Factors that affect cyber security motivation and incentives • Factors that affect cyber security resources e.g. device, security methods, and money allocation • Factors that affect cyber security skills e.g. awareness and literacy levels	• Simulation	• Students	• Computer game	Zoto et al., (2018)
Internet Hero	• Emails • Malware • Social networks • Internet connection	• Fiction • Interactive narrative	• Children	• Computer games	Bauer et al., (2013)

Educational games for cyber security	• Laptop security • Social networks • Malware • Smart Internet usage	• Quiz • Shooter • Endless runner	• Students • Children	• Card matching game • Computer game	Sookhanaphibarn & Choensawat (2020)
Escape room	• A clean desk and screen policy • Secure storage and use of access equipment • Passwords • Secure mobile usage • Social networks • Shredding	• Simulation • Role-playing	• Employees	• Escape room	Oroszi (2019)
Security Empire	• Social engineering • Cryptography • Software authentication • Software patching • Passwords • Anti-virus	• Role-playing	• General public	• Computer game	Olano et al., (2014)
Cyber VR	• Data privacy • Malicious code injection • Software patching • Software analysis • Access privileges • Cryptography	• Role-playing • Fiction • Interactive narrative	• General public	• Virtual reality game • Computer game	Veneruso et al., (2020)
CybAR	• Demographic factors, risk-taking factors, decision-making	• Role-playing • Quiz	• General public	• Augmented reality	Alqahtani & Thorne (2020)

	factors, and personality traits affecting cyber security • Bad cyber security behaviour to avoid			• Android mobile application game	
3D Virtual reality (VR) game	• Social engineering e.g. piggybacking, mantrap, and tailgating • Secure online behaviour • Information protection • Viruses • Ransomware • Distributed denial of service • Trojan	• Role-playing • Simulation • Strategy • Tower defence	• Students	• Cards • Virtual reality game • Computer game	Jin et al., (2018)
CyberNEXS	• Cyber defence • Penetration testing • Cyber forensic	• Simulation	• Students	• Computer game	Nagarajan et al., (2012)
Capture the Flag (CTF)	• Cyber security terminology • Cyber defence • Vulnerability exploitation • Network configuration • Network vulnerabilities • Passwords • Privilege escalation	• CTF scavenger hunt • CTF king of the castle • Quiz • Turn-based Strategy •	• Students	• Computer game	Leune & Petrilli (2017)

	• Phishing • Network snooping				
Class Capture the Flag (CCTF)	• Cryptography • Intrusion • Denial of Service • Domain name system (DNS) security	• Role-playing • Capture the Flag • Turn-based Strategy	• Students	• Computer game	Mirkovic et al., (2015)
Hardware CTF	• Hardware Trojans • Unprotected test infrastructure • Undocumented functions and features • Design bugs and flaws • Side-channel attacks • Weak hardware-based security implementation	• Quiz • Capture the Flag • Turn-based Strategy	• General public	• Digital hardware design representation • Physical hardware devices • Electronic device automation tool	Prinetto et al., (2020)

Table 4: Names, topics, genre, target audience, deployment methods and sources of multipurpose security awareness games

4.3 Understand the deployment methods of security awareness games

Addressing the third objective I report the various methods used to deploy security awareness games during training. I categorized the security awareness games deployment methods as card games, board games, virtual reality games, escape room games, mobile application games, computer network games, and computer games. The above-mentioned deployment methods are explained in the gamification section of this thesis.

Figure 14 shows that majority of security awareness games are deployed as computer games during security awareness training. 19 games are deployed as computer-based games. Card games are the second most popular deployment method used by security awareness games. 9 games are deployed as card-based games. 3 games each are deployed as virtual reality and computer network-based games. Surprising only 2 games are deployed as mobile phone applications. Board-based games are deployed by 2 games and 1 game is deployed as an escape room. It is important to note that there is some crossover in the method of deployment used by security awareness games. All board games include some elements of cards therefore they are classified as both board and card games. Some card games are played on the computer as computer games therefore they are classified as both computer games and card games. All computer network-based games and virtual reality-based games are also computer games therefore they are classified in both categories. Some virtual reality games are implemented as mobile phone applications therefore they are also classified as both virtual reality and mobile application games.

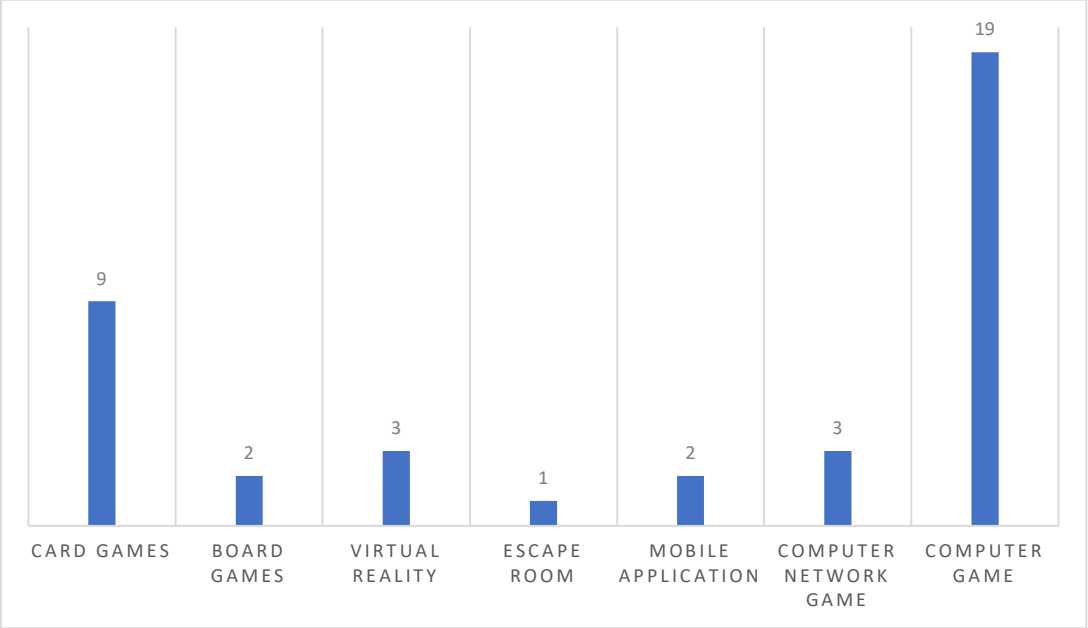


Figure 14: Deployment method used by security awareness games

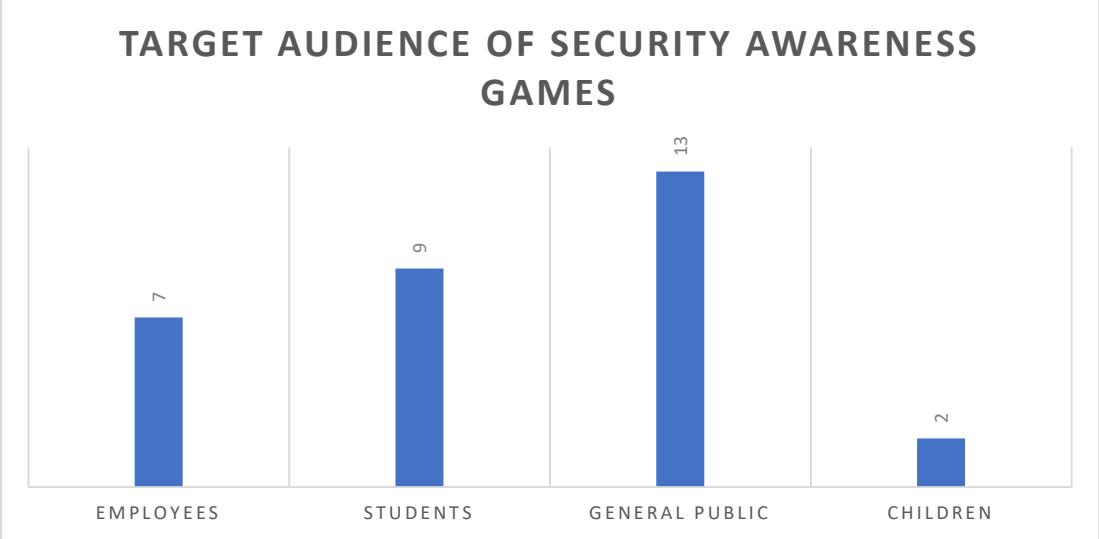


Figure 15: Target audiance of security awareness games

4.4 Identify the target audience of security awareness games

Addressing this fourth objective I report the various audiences targeted by the security awareness games. I categorize the target audience as the general public, students, children, and employees. Games targeted at the general public mean they are targeted at all people regardless of their age, gender, and profession. Games targeted at students mean they are targeted at university and high school level learners. Games

targeted at children mean they are targeted at young learners of elementary school age. Games targeted at employees mean they are targeted at personnel working within an organization.

Figure 15 shows that majority of security awareness games are targeted at the general public. 13 games are targeted at the general public. Students constitute the second most targeted audience by security awareness games. 9 games are targeted at students. 7 games are targeted at employees. Children constitute the least targeted audience, only 2 games are targeted at children. It is important to note that some games target more than one audience group e.g. some games are targeted at both students and employees.

4.5 Explore the game genres implemented by security awareness games

Addressing the fifth objective I report the different game genres implemented by security awareness games. I categorize the game genres as role-playing, interactive narrative, simulation, turn-based strategy, quiz, survival, puzzle, CTF, tower defence, and fiction. The aforementioned genres are discussed in the gamification section of this thesis. Figure 16 shows that role-playing is the genre most commonly implemented in security awareness games. 16 games implement the role-playing genre. Turn-based strategy and quizzes are the 2nd and 3rd most commonly implemented genres. 9 games implement turn-based strategy and 8 games implement quiz genre. The simulation genre is implemented by 6 games while 5 games implement interactive narrative genre. 4 games implement fiction genre and 3 games each implement survival, capture the flag, and tower defence genre respectively. The least implemented game genre is a puzzle, only 2 games implement this genre.

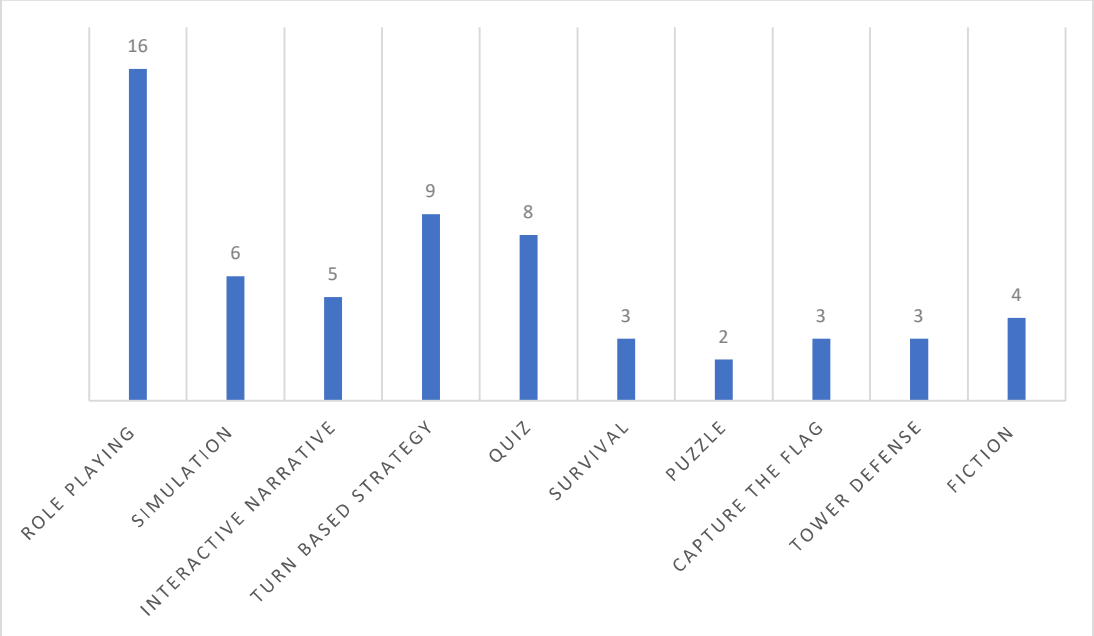


Figure 16: Game genres implemented in security awareness games

4.6 Examine the learning mechanics applied by security awareness games

Addressing the sixth objective I report the different learning mechanics implemented by the security awareness games. I categorize the learning mechanics as instructional learning mechanics, demonstration learning mechanics, exploration learning mechanics, simulation learning mechanics, motivation learning mechanics, and tutorial learning mechanics. The learning mechanics are explained further in the discussion chapter of this thesis.

Figure 17 shows that all the games apply demonstrational learning mechanics. The second most applied learning mechanic is exploration. 17 games apply exploration learning mechanics. 11 games apply instructional learning mechanics, 10 apply motivational learning mechanics and 7 apply simulation learning mechanics. The least applied learning mechanics is tutorials, only 6 games apply this learning mechanic.

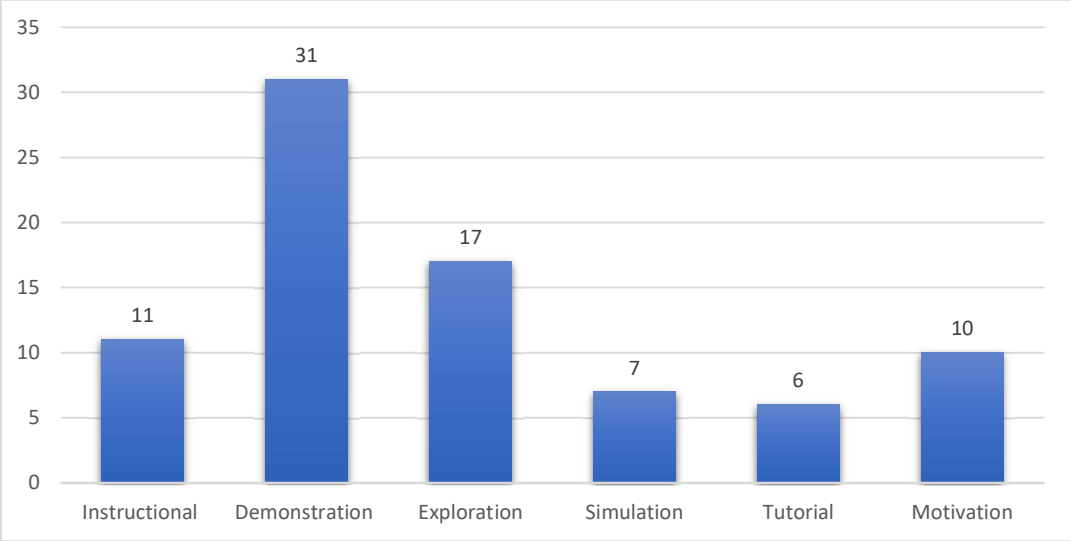


Figure 17: Learning mechanics used in security awareness games

5 Discussion

After describing the results of the systematic literature results, their interpretation according to the objectives is done in this chapter. Detailed descriptions of all the security awareness games mentioned in this section including their gameplay can be found in the appendix section of this thesis.

5.1 The focus of security awareness games

The first objective was to identify the focus or scope of security awareness games. As shown in figure 11 majority of the games are multipurpose, these games are listed in table 4. The evolving nature of the cyber security threat landscape makes multipurpose games popular. Cyber-attacks are launched using different attack vectors e.g. social engineering, outdated software, and password cracking. Keeping players up to date on the different attack vectors and their mitigation strategies is vital. Since multipurpose introduce players to 2 or more cyber security topics, players develop well-rounded cyber security awareness. They can therefore better protect themselves against cyber security threats. The level of detail to which the games introduce players to these topics is not very clear from the papers describing these games.

CyberCIEGE and Cyber smart are examples of multipurpose games. CyberCIEGE game develops player security awareness in 8 cybersecurity-related topics. These topics include cyber security definitions, information value, access control mechanisms, social engineering, password management, malware, safe computing, and physical security mechanisms (Cone et al., 2006; Aladawy et al., 2018; Le Compte et al., 2015). Cyber smart game introduces players to firewalls, security software, safe web surfing, secure wireless connection, passwords, software patching, physical security, network monitoring, cryptography, and backup (Underhay et al., 2016).

Specific purpose security awareness games focus on one topic which could either be social engineering, passwords, or software threat modelling. Table 3 lists the specific purpose security awareness games many of which focus on social engineering. Since the games have a singular focus, they can develop user awareness on the topic to greater detail. Anti-Phishing Phil, Phishy, Social engineering awareness game SEAG, What.Hack, Persuaded, and CyberPhishing games are examples of specific purpose games.

The role-playing quiz application is a specific purpose game exclusively focused on passwords and develops players' awareness on this topic. The game provides players with knowledge on how to generate strong passwords, commonly used passwords to avoid, and good password hygiene practices (Scholefield & Shepherd 2019). Elevation of Privileges (EoP) is a specific purpose game focused on software threat modelling. Tøndel et al., (2018) state that threat modelling identifies security defects in software during the software development life cycle (SDLC). Software development implemented using threat modelling is referred to as a secure software development lifecycle (SSDL). Threat modelling ensures that the software developed keeps performing under attack.

Elevation of Privileges is a specific purpose game that develops player security awareness during software design. The architecture of the software under design forms the basis of the game. The game helps players identify potential vulnerabilities in the software design (Omiya et al., 2019; Tøndel et al., 2018; Shostack 2014). IoT Poly is a specific purpose game that develops player security awareness during IoT device development. The game helps players develop practical skills in IoT device risk assessment which entails risk identification, analysis, and revaluation. The game assists players to identify potential threats to IoT devices and the processes that occur after the identification of these threats (Omiya et al., 2019).

5.2 Topics in security awareness games

The second objective was to identify the different cyber security topics taught by security awareness games. As mentioned earlier specific purpose security awareness games focus on one topic. However, some topics are broad and contain different subtopics. Social engineering is an example of such a topic that contains many subtopics such as URL, social media, phishing emails, tailgating, shoulder surfing, voice of authority, impersonation, spear phishing, and dumpster diving (Röpke et al., 2020). Specific purpose games focusing on social engineering introduce players to granular details within this topic. As shown in figure 12 phishing email is the most common social engineering subtopic featured in specific purpose games. Presented are a few specific purpose games from the results set that focus on phishing emails, URLs, and phishing website subtopics.

What.Hack and CyberPhishing games introduce players to phishing emails. What.Hack game simulates actual phishing attacks through which players get to learn about phishing concepts and experiences phishing email attacks as they would in the real world. The phishing emails used in the simulation are obtained from templates of actual real-world phishing emails (Wen et al., 2019). CyberPhishing game is implemented on a client-server web simulation platform. The platform provides players with a realistic web environment that is controlled, therefore limiting players' exposure during security awareness training. The platform provides players with phishing emails, phishing websites, and social media simulations. From these players learn and experience social engineering attacks as they would in the real world. The platform also has data tracking capabilities (Hale et al., 2015).

Anti-Phishing Phil and Phishy games introduce players to phishing URLs. Anti-Phishing Phil game helps players identify phishing URLs. The game narrative is based on a fish called Phil that eat worms to grow. The worms that Phil eats to grow represent URLs. Players in the game represent Phil, they are required to eat worms associated with safe URLs and reject phishing URLs worms. Phil's father is a game character that represents an experienced fish that gives Phil advice on worms to reject as shown in figure 18 below (Sheng et al., 2007; Wen et al., 2019). Phishy game introduces players to short URLs, URL inspection methods, and online brand name search as shown in figure 19 below.

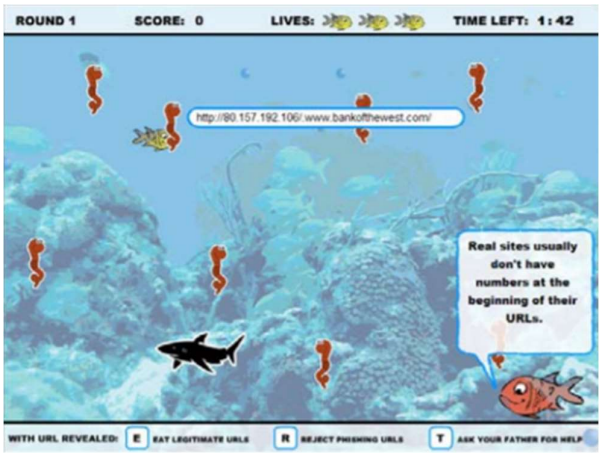


Figure 18: Game screen of Phil inspecting an URL before eating (Sheng et al., 2007)

Social engineering awareness game (SEAG), and Persuaded games introduce players to phishing websites. Persuaded game, develops players' resistance to social

engineering attacks by inoculating players against such attacks. Inoculation occurs as a result of players continuously being exposed to realistic social engineering attack scenarios. This makes players develop appropriate responses to social engineering attacks. These developed responses become common practice players apply while dealing with real-life social engineering attacks (Aladawy et al., 2018). SEAG introduces players to basic social engineering concepts which include phishing websites and emails (Olanrewaju & Zakaria 2015).

Figure 19: Phishy game screen showing (A) Story how Sam got lost at sea (B) Sam failing to hook a fish to feed the tiger and hooking a fish to feed the tiger (CJ et al., 2018)

Figure 13 shows that password management is the most common topic featured in multipurpose games. 15 of the 22 games introduced players to various password topics such as secure online payment, password generation, trusted networks, and securing personal information. Password management is rightfully the focus of many multipurpose games because passwords are the primary mechanism for accessing Internet services. Passwords provide the first line of cyber defence and are used to protect computers, data, and online accounts. Generating and maintaining several strong passwords is often a difficult task. Applications may also require the passwords

to be frequently changed resulting in players using weak and easy to remember passwords. Players could also write down the passwords to assist in remembering them (Nagarajan et al 2012; Scholefield & Shepherd 2019).

Players are introduced to passwords from the common vulnerability and exposure (CVE) perspective by the game project config.play (Enriquez et al., 2018). CyberCIEGE game introduces players to the importance of keeping passwords secret from outside entities (Cone et al., 2006). M-learning game introduces players to passwords by requiring them to answer quiz questions regarding good password practices (Filipczuk et al., 2019). Educational games for cyber security, Hacked time, Cyber smart, Internet Hero, Secu-one, Escape room, Security empire, Cyber VR, CybAR, 3D VR game, Capture the Flag, and Class Capture the Flag games also develop players security awareness on passwords in one form or another.

The second most common topic featured in multipurpose games is software management. 13 multipurpose games introduced players to software management topics such as patch management, antivirus software, and secure remote access. Additional software code is often released to address problems in earlier released software versions. Software updates are done to fix security flaws or increase software functionality. If a software flaw is not patched, it can be exploited by an attacker. Timely software updates are vital in maintaining confidentiality, integrity, and availability of software. Unfortunately keeping track of software updates can be a difficult task, therefore equipping players with software management skills and knowledge is important during security awareness training (Nagarajan et al 2012).

Network nightmares game introduces players to antivirus software concepts via a shooting game. Players are required to aim and hit network nodes with viruses in a similar fashion to the angry birds game (Ryan et al., 2013). CyberCIEGE game requires players to make investment and tradeoff decisions on the purchase of anti-virus software thus introducing them to anti-virus software (Cone et al., 2006). Control-Alt-Hack, Cyber CIEGE, M-learning, Hacked time, Internet Hero, Educational games for cyber security, Cyber smart, Security Empire, Cyber VR, 3D VR game, Capture the Flag, and Class Capture the Flag games also develop players security awareness on software management and anti-virus software in one form or another.

12 multipurpose games introduced players to social engineering, which is increasingly being used to launch cyber-attacks. Attackers are using social engineering to gain access to information or insert malware into computer systems. Social engineering aims to influence a person to perform actions they would otherwise not perform using non-technical means. It does not require the use of advanced technical tools, is cheap to execute, and can be performed by anyone (Aladawy et al 2018; Beckers & Pape 2016; Wen et al 2019).

Cyber security requirements awareness game requires players to deploy social engineering attacks against their opponents thus introducing them to social engineering (Yasin et al., 2018). 3D VR game requires players to select appropriate responses to different social engineering scenarios presented by the game. This introduces players to possible social engineering attacks (Jin et al., 2018). Control-Alt-Hack, Cyber CIEGE, M-learning, Hacked time, Cyber security requirements awareness game, Secu-one, Educational game for cyber security, Security empire, CybAR, Capture the Flag, and Class Capture the Flag games also develop players security awareness knowledge on social engineering in one form or another.

The least popular topics in the multipurpose security awareness games are access control and appropriate use of hardware. The 9 games that feature access control introduced players to rules on system usage and protecting access to critical assets. Cyber VR game requires players to scan system users with root privileges and determine whether their root privilege is legitimate or not thus introducing players to access control (Veneruso et al., 2020). Project config.play game introduces players to access control by requiring them to attack their opponent authentication requirements based on CVE (Enriquez et al., 2018). Cyber CIEGE, Cyber smart, Cyber security requirements awareness game, Escape room, CyberNEXS, Capture the Flag, and Class Capture the Flag games also develop players security awareness on access control. The 9 games that feature appropriate use of hardware introduced players to topics such as proper handling and disposal of hardware devices. Escape room game requires players to securely store equipment such as workplace badges, keys, and proximity cards to prevent attackers from accessing their computer. Thus introducing players to the appropriate use of hardware. Project config. play, Cyber CIEGE, Cyber smart, cyber security requirements awareness game, educational games for cyber

security, Escape room, Secu-one, Cyber VR, and Hardware CTF games also develop players security awareness on the appropriate use of hardware in one form or another.

It is important to note that each of the multipurpose games featured 3 or more of the aforementioned topics. The papers mentioned that the topics featured in the games, but details of exactly how these topics are covered by these games were not very clear. The papers that gave details of how these topics were covered indicated that the games only addressed basic concepts and mitigation strategies within these topics. Since the scope of multipurpose games is wide, topics within these games are mostly addressed at a superficial high level.

5.3 Deployment method used by security awareness games during training

The third objective was to identify the different deployment methods used by security awareness games during training. Figure 14 shows that 19 games are deployed as computer-based games during security awareness training. Computer-based games have design and usability aspects that make them the preferred choice of security awareness games. This is because computer games have historically been based on solid game design and usability principles that have taken years to research. Security awareness games find it easy to build upon these existing principles (Fry 2021). Secondly, most cyber security tools and practices are implemented on a computer. Therefore computer-based games provide a good platform for players to practice the implementation of these tools and practices.

9 games are deployed as card games during security awareness training. Card games are deployed because they minimize communication barriers that may be present between players. This is because they require each player to contribute and encourage discussion. The review sessions after a card game promote peer-to-peer learning (Yasin et al., 2018). Persuaded game is a single-player card game that develops players social engineering awareness. The cards consist of attack cards, defence cards, skip turn cards and see the future cards as shown in figure 20 below. Skip turn and see the future cards are used to support game mechanics (Aladawy et al., 2018). Control-Alt-Hack game is a 3 – 6 player card game that develops player security awareness on high level cyber security concepts and challenges. The game has 156 cards game divided into 4 card decks i.e. hacker cards, mission cards, entropy cards, and attendance cards as shown in figure 21 and 22 below. Entropy and

attendance cards are used to support game mechanics (Denning et al., 2013). Social engineering awareness game, Project config.play, Cyber security

Figure 20: Persuaded cards (1) Attack card (2) Defence card (3) Skip turn card (4) See the future card (Aladawy et al., 2018)

Figure 21: Control-Alt-Hack cards backside (1) Hacker card (2) Mission card (3) Entropy card (4) Attendance card (Denning et al., 2013)

Figure 22: Control-Alt-Hack cards front side (1) Hacker information (2) Mission statement (3) Entropy bag of tricks card (4) Entropy lightning strikes card (Denning et al., 2013)

requirements awareness game, Secu-one, 3D virtual reality game, Elevation of Privileges, and IoT Poly games are also deployed as card games.

3 games each are deployed as virtual reality and computer network-based games. VR games increase intuitivity, immersivity and usability which are essential during security awareness training (Kasurinen 2017). Cyber VR game immerse players in a virtual world whereby they use their hand gestures to interact with the object in the virtual world during security awareness training (Veneruso et al., 2020). CybAR and 3D VR games are also deployed as virtual reality-based games. Computer network games or online games are computer games played over a computer network. Capture the Flag (CTF) game is an example of such a game that provides players with access to a virtual network containing virtual servers as shown in figure 23 below. This virtual network enables players to apply their skills in exploiting vulnerabilities and defending networks (Leune & Petrilli 2017). Class Capture the Flag (CCTF) and An Integrated Real-Time Simulated Ethical Hacking Toolkit with Interactive Gamification Capabilities and Cyber Security Educational Platform games are also deployed as computer network-based games.

2 games each are deployed as board games and mobile application games. Board games have the benefit of being cheap, easy to set up, modifiable and they encourage social interaction (Shostack 2021). Project config.play game is an 8*16 grid board game. The game also incorporates the use of cards as shown in figure 24 below. The red part represents the opponent's territory, and the green part represents a player's local territory. The two territories are separated by a middle line. Players are required to attack each other vulnerabilities based on the Common Vulnerabilities and Exposure concept (Enriquez et al., 2018). Cyber security requirements awareness game uses a board based on an organization's floor map plan during security awareness training. Players are required to use different cyber-attack methods e.g. social engineering to access different rooms on the floor map. Thereafter players are required to exploit and compromise devices within these rooms (Yasin et al., 2018).

M-learning and CybAR games are deployed as mobile application games. Access to mobile phones is widespread and therefore games deployed as mobile applications can reach a wide audience. Mobile application games also provide players with the flexibility to learn at their own pace during their free time. M-learning game has the

additional benefit of being downloadable. As a result, the game can be run locally on the phone without the need for Internet access (Filipczuk et al., 2019). CybAR game is an augmented reality game also deployed as a mobile application.

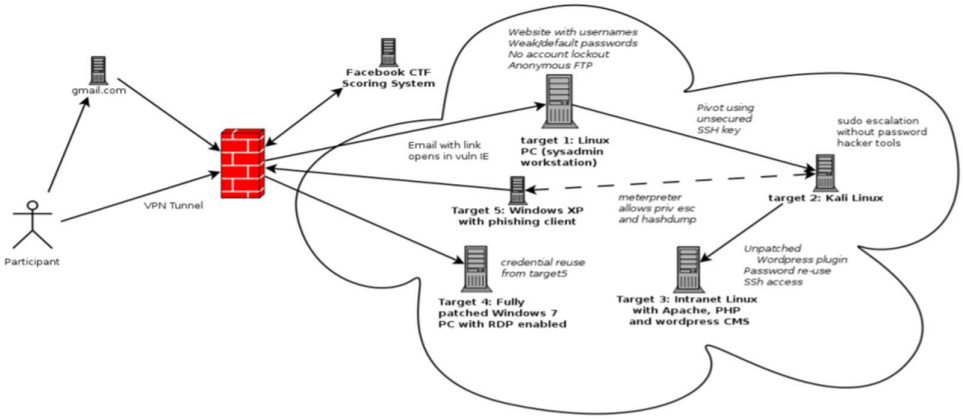


Figure 23: Virtual network showing servers and PC that contain flags (Leune & Petrilli 2017)

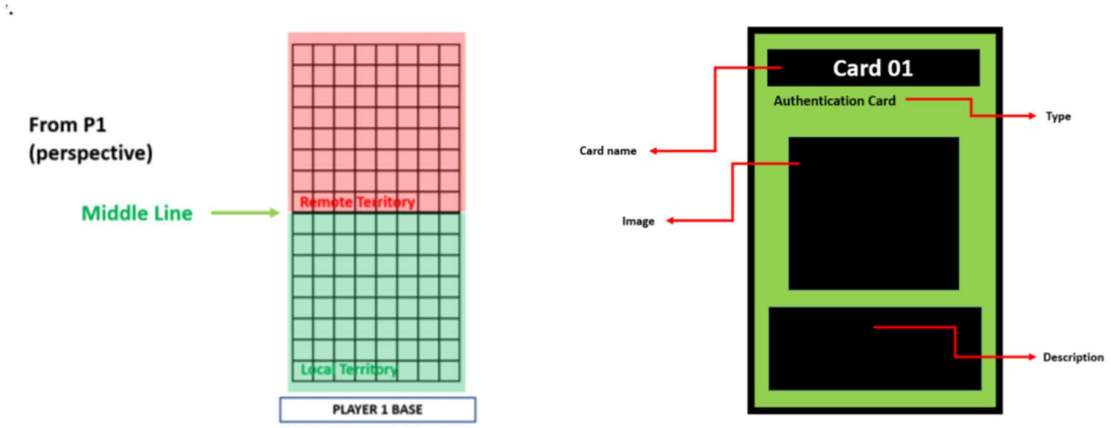


Figure 24: Project config. Play (A) The game board is divided into territories (B) config.Play action card (Enriquez et al., 2018)

The escape room game is deployed as an escape room-based game. The game is played by 3-5 people and uses a realistic imitation of a player's office environment and cyber security policies. The game determines players' security awareness knowledge and deficiencies. Players are required to access a computer file in a room that mimics

their office space. Escape room games actively require player involvement thus promoting active learning (Oroszi 2019).

5.4 The target audience of cyber security awareness games.

The fourth objective was to identify the target audience of the security awareness games. Figure 15 shows that the majority of games are targeted at the general public. Internet connectivity and use are widespread amongst the general public as a result, they provide a large pool of audiences with security awareness requirements. Unfortunately, they are often neglected when it comes to cyber security awareness (Farooq 2019a). For commercial purpose security awareness games, the general public provides a large source of potential customers. The security awareness requirements of the general public tend to be generic and are therefore met by most of the games. The generic nature of their requirements also means that the games do not require a lot of customization compared to games targeted at organizations. All these factors contribute towards making the general public a popular target for security awareness games. Anti-Phishing Phil, Phishy, Persuaded, Social engineering awareness game, CyberPhishing, Network nightmares, An Integrated Real-Time Simulated Ethical Hacking Toolkit with Interactive Gamification Capabilities and Cyber Security Educational Platform, Hacked time, Security Empire, Cyber VR, CybAR, Hardware CTF, and role-playing quiz application are some security awareness games targeted at the general public.

9 games are targeted at students, they constitute the second-largest audience group targeted by security awareness games. There is a need for new security awareness training methods that serves the younger digitally native generation accustomed to using diverse tools and devices to access the Internet. They are also accustomed to different learning styles and have different security awareness requirements (Ariffin et al., 2016). The younger generation prefers socialized learning that recognizes learning as a cognitive process that occurs in a social context where new behaviour is acquired by observing and imitating others. The younger generation like to share their achievements on social media to get validation from their peers, require immediate feedback and are interested in experiential learning. Experiential learning is a learning process where people learn by doing and reflect on their experiences thereafter. The younger generation also likes to visualize connections between what is learned and

its application in real-life situations (Ariffin et al., 2016; Wolfenden 2019). These factors contribute towards a lot of security awareness games targeting the student audience.

Security awareness games are mostly designed as courses for use in schools and universities (Le Compte et al., 2015). Since they are designed for use in schools and universities, students are naturally the target of such games. Students also constitute the digitally native age group likely to embrace and be receptive to the gamification of security awareness training (Ariffin et al., 2016). Control-Alt-Hack, Cyber smart, Secu-one, CyberNEXS, Capture the Flag, Class Capture the Flag, 3D VR game, CyberAIMs, and Educational game for cyber security are some security awareness games targeted at students.

7 games are targeted at employees within an organization. Organizations are faced with increasing cyber security challenges and therefore effective security awareness training is important. Employees also find current security awareness training as boring, ridiculous, overwhelming, low-quality productions, not relevant to their roles and do not capture real-world workplace variables (Reeves et al., 2021). Since security awareness training is often mandatory within organizations, employees find them boring but compulsory exercise that disrupts normal work activities (Baxter et al., 2015). New innovative security awareness training methods are required by organizations, therefore many security awareness games are rightfully targeted at employees within an organization.

Security awareness games are designed for on-the-job training to be used in workplace environments (Le Compte et al., 2015). CyberCIEGE game is targeted at employees and introduces them to security awareness through resources management. Players are required to make decisions regarding cyber security resource allocation and purchases during the construction of a network (Cone et al., 2006). M-learning game also provides management with an assessment of employees' security awareness knowledge apart from providing security awareness knowledge to the employee (Filipczuk et al., 2019). What.Hack, IoT Poly, Elevation of Privileges, M-learning, Escape room, and Secu-one are security awareness games targeted at employees.

Few security awareness games are targeted at children. Children are increasingly accessing the Internet, which has its benefits and risks. Preparing children to safely

navigate the Internet is important and therefore they constitute a legitimate target of security awareness games (Quayyum 2020). Internet hero is a video game targeted at children to assist them safely navigate the Internet. Players are transported into a fictional Internet world with 4 characters ping, dot net, dot com, and dot evl. Dot evl is a villain character intent on taking over the Internet. Players are heroes tasked with the responsibility of helping ping solve 4 mini-games challenges related to Internet usage (Bauer et al., 2013). Educational games for cyber security introduce children to safe laptop usage, social networks, malware, and smart Internet usage. The game consists of 5 mini-games that deploy trivia, matching, shooting, and runner game (Sookhanaphibarn & Choensawat 2020). It is important to note that some games are targeted at more than one audience group. IoT Poly and Secu-one are examples of security awareness games, targeted at both students and employees.

5.5 Game genres implemented by security awareness games

The fifth objective was to identify the different game genres implemented by the security awareness games. The different game genres are discussed in the gamification section of this thesis. Figure 16 shows that more than half of security awareness games implement the role-playing genre. The role-playing genre is popular because it helps build a player's character. The genre also builds behavioural momentum which ensures that a player's cyber security behaviour persists after the game (Le Compte et al., 2015). Control-Alt-Hack game requires players to take the role of a white hat hacker (Denning et al., 2013). In the Cyber CIEGE game players take the role of a decision-maker within an organization (Cone et al., 2006). In Hacked time game players take the role of a detective assisting a student friend to resolve a data breach incident. The role of assisting a friend personalizes the game and makes it relatable to the player (Chen et al., 2020). In Cyber smart game the player takes the role of a system administrator responsible for maintaining a network (Underhay et al., 2016). In What.Hack game the players take the role of a bank employee responsible for sorting phishing and non-phishing emails (Wen et al., 2019). In Cyber security requirements awareness game players working as a team take the role of ethical hackers required to access locations and devices on a floor plan (Yasin et al., 2018). Escape room, Security Empire, Cyber VR, CybAR, 3D virtual reality game, CyberPhishing, Anti-Phishing-Phil, Phishy, and Class Capture the Flag security

awareness games also implement role-playing genre to achieve behavioural momentum and build player character.

9 games implement turn-based strategy genre. The turn-based strategy genre is synonymous with board and card games. In the turn-based strategy genre, players take time during gameplay to make decisions. These decisions require planning or resources management by players (Le Compte et al., 2015). In the IoT Poly game, players draw a card describing a threat they consider faces an IoT device under consideration. They also draw a card describing a countermeasure they consider effective against the aforementioned threat (Omiya et al., 2019). Project.config.play game players plan and strategize which opponent's vulnerabilities to exploit (Enriquez et al., 2018). Capture the Flag, Class Capture the Flag, and Hardware CTF games require players working as teams to strategize how to attack or defend networks. Cyber security requirements awareness game, Secu one, Persuaded, and Elevation of Privileges security awareness games, also implement turn-based strategy genre.

8 games implement quiz genre. The quiz genre is effective in assessing the level of knowledge of players. Quizzes test players' comprehension of course material and provide insights into their progress and knowledge gaps. M-learning game provides players with multiple-choice questions. Players are required to select one correct answer and are awarded rewards for the correct choice (Filipczuk et al., 2019). Role-playing quiz application game also provides players with multiple choice questions which must be answered within some set time limit (Scholefield & Shepherd 2019). Social engineering awareness game (SEAG), An Integrated Real-Time Simulated Ethical Hacking Toolkit with Interactive Gamification Capabilities and Cyber Security Educational Platform, Educational games for cyber security, CybAR, Capture the Flag (CTF), and Hardware CTF security awareness games also implement quiz genre.

6 games implement simulation genre. Simulation genre can immerse players into the game and provide an authentic learning experience by replicating their real-world environment during security awareness training. This has led to the wrong assumption that simulation genre is the best for security awareness games, although other genres are equally effective (Le Compte et al., 2015). Escape room game implement simulation genre and requires the replication of a player's work environment which include the furniture and office equipment. Access to the escape room and equipment

also follows the cyber security policies that govern the player (Oroszi 2019). 3D VR game develops player security awareness by simulating their bedroom or school computer lab environment (Jin et al., 2018). CyberNEXS, CyberAIMs, An Integrated Real-Time Simulated Ethical Hacking Toolkit with Interactive Gamification Capabilities and Cyber Security Educational Platform, Educational games for cyber security, and CyberPhishing security awareness games all implement simulation genre.

5 games implement the interactive narrative genre, and 4 games implement the fiction genre. The interactive narrative genre uses storytelling to structure learning. Interactive narrative makes players believe their choices are central to the unfolding story, therefore, immersing them into the game. The genre invokes emotions and provides a framework through which security awareness games can be structured (Thompson 2017). Interactive narrative is a powerful story-based learning tool since it is easier to remember details that are part of a story. Phishy game tells a story of how Sam got stuck in a boat at Sea with a hungry tiger as a result of social engineering. Subsequently, Sam needs to feed the tiger with fish as he navigates his way back to shore. The tiger is fed as a result of Sam selecting the correct answer to URL-related questions (CJ et al., 2018). Hacked time game tells a story of a student who is a data breach victim and a detective friend who helps the student recover from this breach (Chen et al., 2020). Internet Hero tells a story of Ping and the problems he encounters navigating the Internet. In this storyline, Ping can overcome these challenges with the help of a friend i.e. the player (Bauer et al., 2013). Anti-Phishing Phil and Cyber VR games also implement interactive narrative genre during security awareness training. The fiction genre is created from imagination and is not presented as facts although it may be based on actual situations. Cyber VR game is based on a fictional post-apocalyptic world in which players are required to secure a network (Veneruso et al., 2020). Phishy, Anti-Phishing Phil, Internet Hero, and Cyber VR security awareness games also implement the fiction genre.

Survival, capture the flag, and tower defence genres are implemented by 3 games each. The survival genre uses a constant life and death struggle to tap into the human instinct to survive through challenges (Filipczuk et al., 2019; CJ et al., (2018). M-learning, Phishy, and role-playing quiz application security awareness games implement survival genre. In M-learning game players struggle to save their job and avoid being fired by answering quiz questions correctly (Filipczuk et al., 2019). In the

Phishy game, players struggle to get to shore before being eaten by a hungry tiger. They can achieve this by answering URL-related questions which enable them to feed the tiger (CJ et al., 2018). In the role-playing quiz application game, players struggle to maintain their health by answering password-related quiz questions correctly (Scholefield & Shepherd 2019). Capture the Flag genre encourages teamwork and practice, resulting in players gaining practical experience and skills (Wen et al., 2019). Capture the Flag, Class Capture the Flag, and Hardware CTF security awareness games implement capture the flag genre. The tower defence genre is a sub-strategy genre. In the tower defence genre, players are allocated resources to build a tower and prevent enemies from attacking this tower. Hacked time, Internet Hero, and 3D VR games implement tower defence genre**.** The least implemented genre is puzzles. Hacked time and Cyber security requirements awareness security awareness games implement puzzles genre. In the Cyber Security Requirements Awareness game, players are required to solve a puzzle before accessing a room on the floor map. This is similar to guessing a password before accessing an account (Yasin et al., 2018).

5.6 Learning mechanics implemented in security awareness games

The sixth objective was to identify the different learning mechanics applied by the security awareness games. The games need to be more than just fun and engaging but should have meaningful learning. The learning mechanics essential in a security awareness game are instructional, exploration, demonstration, simulation, tutorial, and motivation (Le Compte et al., 2015).

Figure 17 shows that all the games implement demonstration learning mechanics. Demonstration learning mechanic requires players to actively participate in tasks by taking up different roles, answering questions, giving advice, selecting an appropriate response to a scenario, or aiming and shooting at an object. Active participation ensures players receive and internalize the security awareness message (Le Compte et al., 2015). In no game was the player required to be passive during security awareness training.

Exploration is the second most applied learning mechanic. 17 games applied exploration as a learning mechanic. Exploration requires players to identify and discover knowledge and skills during security awareness training. Discovery ensures that players retain the security awareness message (Le Compte et al., 2015). Project

config.play game requires players to discover and exploit an opponent's vulnerabilities according to CVE (Enriquez et al., 2018). Hacked time game requires players to discover clues of the cause of a data breach in a room as they try to help a friend resolve the data breach (Chen et al., 2020). Network nightmares game requires players to discover weak network spots that can be used to launch viruses (Ryan et al., 2013). Ethical hacking toolkit with interactive gamification capabilities and cyber security educational platform, Cyber smart, Cyber security requirements awareness game, CyberAIMs, Internet Hero, Educational game for cyber security, Escape room, Security Empire, Cyber VR, 3D VR game, CyberNEXS, Capture the Flag, Class Capture the Flag, and Hardware Capture the Flag security awareness games also implement exploratory learning mechanics in one form or another.

Instructional learning mechanics is applied by 11 games. Instruction learning mechanic guides players during security awareness training. Instructions ease players learning process and ensure they receive knowledge during security awareness training (Le Compte et al., 2015). Cyber CIEGE game has balloon speeches from virtual users that give players feedback and instruction during gameplay (Cone et al., 2006). Escape room game provides players with instructions on how to play the game, the game story, and its goal before introducing them to the game (Oroszi 2019). M-learning, Ethical hacking toolkit with interactive gamification capabilities and cyber security educational platform, Hacked time, Cyber security requirements awareness game, Internet Hero, Cyber VR, CybAR, Class Capture the Flag, and Hardware Capture the Flag security awareness games also implement instructional learning mechanics in one form or another.

Motivation learning mechanics is applied by 10 games. Motivation learning mechanic gives players a sense of ownership, responsibility, and incentives during security awareness training thus encouraging accountability (Le Compte et al., 2015). In Hacked time game players have the responsibility of helping a friend in trouble i.e. student who is a data breach victim (Chen et al., 2020). In the Security empire game, players have the responsibility of managing the network systems of a company (Olano et al., 2014). In CyberNEXS players have the responsibility of looking for and exploiting network vulnerabilities. Once a network is exploited players are responsible for defending the same network (Nagarajan et al., 2012). Cyber smart, Cyber security requirements awareness game, Cyber VR, 3D VR game, Capture the Flag, Class

Capture the Flag, and Hardware Capture the Flag security awareness games also implement motivational learning mechanics.

Simulation learning mechanic is applied by 7 games. Simulation learning mechanic models a player's everyday environment similar to the simulation genre (Le Compte et al., 2015). Games such as Ethical hacking toolkit with interactive gamification capabilities and cyber security educational platform, CyberAIMs, Escape room, 3D VR game, and CyberNEXS security awareness games implement simulation learning mechanics.

The least applied learning mechanic is the tutorial mechanics applied by 6 games. Tutorial learning mechanics assess players' knowledge progression during security awareness training. This is done through game levels that vary in degree of difficulty as the game progresses (Le Compte et al., 2015). What.Hack game has a rule book that players use to screen and distinguish phishing emails from legitimate emails. This rule book becomes more specific as the game progresses and emails to screen become more complicated (Wen et al., 2019). Ethical hacking toolkit with interactive gamification capabilities and cyber security educational platform game has an informative website where players learn about cyber security threats and their countermeasures. The website also has a discussion forum where players can discuss cyber security issues amongst themselves and with professionals (Mathoosoothenen et al., 2017). Cyber Security requirements awareness game, Escape room, Cyber VR, and Class Capture the Flag security awareness games apply tutorial learning mechanics in one form or another.

5.7 Benefits of security awareness games

The existing literature highlights the following benefits of games in security awareness:

1. Games increase players visual and audio stimuli which increase players' interest in security awareness training and cyber security in general (Baxter et al., 2015).
2. Games make security awareness training interactive, engaging, and entertaining. This results in a better understanding of the security awareness content because player imagination and attention are captured (Baxter et al., 2015; Alotaibi et al., 2016; Tioh et al., 2017).

3. Games are adaptable and flexible therefore they can provide better coverage of different cyber security topics during security awareness training (Alotaibi et al., 2016).
4. Games reduce the teaching time and instructor load during security awareness training (Alotaibi et al., 2016).
5. Games are a low-cost security awareness training method. Although they may require a high initial investment once they are set up and running, games are cheap to maintain (Alotaibi et al., 2016).
6. Games scale well and provide an easy avenue through which security awareness training can be delivered to a large audience (Rieff 2018).
7. Games can be played repetitively resulting in better retention of security awareness content. Repetitive playing ensures that players are constantly exposed to security awareness which helps them internalize the content (Rieff 2018).
8. Games provide players with realistic virtual environments. These environments are difficult to replicate using other security awareness training methods. Players can safely make mistakes and observe the consequences of their mistakes in these virtual environments offered by games (Baxter et al., 2015; Tioh et al., 2017).
9. Games encourage learning by exploration which enables players to gain practical experience and learn by making mistakes (Tioh et al., 2017).
10. Games give players the feeling of rapid progression through their short feedback cycles and rewards. Rapid progression motivates players to continue learning during security awareness training (Tioh et al., 2017).

5.8 Challenges facing security awareness games

Below are some of the challenges security awareness games face during their implementation, as found in the literature:

1. Security awareness games are mostly designed for use in school, university, and workplace environments. Therefore players may be unable to play these games in other environments, at their pace, and during their time. Thus limiting continuous security awareness training due to lack of availability of the game (Le Compte et al., 2015).
2. Security awareness games are most proprietary games and are not available through the normal distribution channels e.g. online stores and video games shops. The games are only available from the developer's official website or on request

from the game developer. They are also rarely mentioned in video game chat forums. All these factors contribute towards security awareness games having limited reach and unexplored potential (Le Compte et al., 2015; Hendrix et al., 2016).

3. Security awareness games are formal games. Formal games are played under supervision, within some time limits, and framed within an educational context. The development and implementation of formal games have added complexity compared to informal games (Le Compte et al., 2015).
4. Security awareness games have privacy and trust issues. During gameplay, players fill in passwords, open phishing emails, and choose appropriate security behaviour according to their opinion. Data collected by the game risks exposing private player information (Blythe & Coventry 2012).
5. Security awareness games have limited scope on the number of cyber security topics covered. Games that cover many topics are unable to cover these topics in great detail, therefore games tend to focus on a few topics. In real life, players encounter multiple cyber security challenges that deploy different attack vectors and require different mitigation strategies. Therefore games limited in scope do not adequately prepare players for real-life cyber security situations (Blythe & Coventry 2012).
6. Security awareness games maintain game logs that contain sensitive information. The games log players' gameplay details and a summary of their progress during security awareness training. Access to these logs can be used for malicious purposes e.g. management using the logs to dismiss employees performing poorly (Blythe & Coventry 2012).
7. Security awareness serious games are themselves vulnerable to social engineering attacks. Players could be tricked into believing they are playing a security awareness game while the malicious game is collecting players' information for malicious purposes (Blythe & Coventry 2012).
8. Security awareness games could be challenging to beginners with little or no gaming experience. This could harm players' motivation during security awareness training. Others may feel intimated and underprepared to participate in the competition. Game tutorials are recommended for such players (Thomas et al., 2019).

9. Individual differences in demography, risk-taking, decision making, and personality affect cyber security behaviour. These differences also affect security awareness requirements, customizing games to meet individual requirements is difficult. Security awareness games are usually designed for a broad audience and customized according to the security awareness requirements of an organization (Alqahtani & Thorne 2020).
10. Security awareness games need to be constantly updated with new content because of the ever-changing cyber security threat landscape. Attackers are constantly innovating and changing attack strategies. The games need to keep up with this to remain relevant which is not an easy task (Zimmermann & Renaud 2019).
11. Some players might view games as recreational activities for children and teenagers. Others might view game elements such as competition and reward as manipulative Such players are likely to have a negative attitude in general towards security awareness games (Baxter et al., 2015; Armstrong & Landers 2018).
12. Security awareness games can either give a detailed or vague player experience. A detailed player experience occurs when a game's simulation includes all possible scenarios and requires players to check all potential options until they arrive at a secure decision. A vague player experience occurs when a game introduces topics to players briefly and in high-level detail (Alqahtani & Thorne 2020).

6 Conclusion

Cyber security is a wide topical area that includes people, processes, and technology. Research shows that security awareness training is effective in improving the human element in cyber security. The training improves cyber security knowledge and provides incentives to change cyber security behaviour (Islam et al., 2019). Unfortunately, the current security awareness training methods have not been effective. New innovative and effective security awareness training methods are required (Ariffin et al., 2016).

This thesis investigated the state of the art of games used in cyber security awareness. Gamification of education is effective in improving learning outcomes (Kocakoyun & Ozdamli 2018). Gamification of cyber security awareness is effective in increasing user knowledge and improving cyber security behaviour. Users find security awareness games to be, educational, motivational and entertaining (Yasin et al., 2018). However, the use of games in security awareness training is a relatively new and developing research topic (Hendrix et al., 2016).

This thesis reviewed some games developed to raise security awareness. Most of these games have been developed for academic and workplace research, as opposed to being developed for large-scale commercial purposes (Hendrix et al., 2016). The games are mostly exploratory meaning they are developed to examine the idea of using games in security awareness training. Interestingly these games are not easily accessible through the normal distribution channels i.e. google or apple online stores. The games mostly exist as academic articles, some are available on the developer's official website and others are available on request from the developer. A conclusion can be drawn that security awareness games are not commercially viable. Another surprise in the results is the few games designed for deployment as a mobile phone application. Especially since mobile phones use and availability is widespread, ensuring that games deployed via this platform can reach a large audience (Alqahtani & Thorne 2020).

Various evaluations have been conducted to measure the effectiveness of some of the security awareness games. Results show that gamification of security awareness is effective in increasing knowledge and changing cyber security behaviour. In games that have conducted an evaluation, the results are based on small sample size. This

is surprising since games can scale well to a large audience who can be used for evaluation purposes. Robust research with bigger sample sizes is needed to better evaluate the effectiveness of games in cyber security awareness.

Most security awareness games target the general public and students. The review found only 7 games targeted specifically at employee security awareness training. Cyber security and security awareness are big issues facing organizations that need to be urgently addressed (Reeves et al., 2021). There is a demand for games with high engagement that can revolutionize employee security awareness training. Games targeted at employees need to be streamlined with the organization's security awareness requirements. The review showed that games are mostly focused on providing players with knowledge on multiple cyber security topics. The games however fail to explain why these topics are important and elaborate on cyber security risks. There is a need for games that explain the importance of cyber security topics and elaborate on risks associated with cyber security to be developed.

It was noted that most security awareness games were developed for short-term purposes. The games are developed and presented to players for quick feedback cycles. Hence the evaluation results are based on short-term players' feedback responses. A follow-up evaluation on the long-term effectiveness of security awareness games is lacking. Long-term evaluation is useful in determining player retention of security awareness content. Therefore research on the long-term effectiveness of security awareness games is needed. It is my conclusion that gamification of cyber security awareness has untapped potential.

7 References

Abawajy, J. (2014). User preference of cyber security awareness delivery methods. *Behaviour & Information Technology*, *33*(3), 237-248.

Al-Daeef, M. M., Basir, N., & Saudi, M. M. (2017). Security awareness training: A review. *Lecture Notes in Engineering and Computer Science*.

Al-Hamdani, W. A. (2006, September). Assessment of need and method of delivery for information security awareness program. In *Proceedings of the 3rd annual conference on Information security curriculum development* (pp. 102-108).

Aladawy, D., Beckers, K., & Pape, S. (2018, September). PERSUADED: fighting social engineering attacks with a serious game. In *International Conference on Trust and Privacy in Digital Business* (pp. 103-118). Springer, Cham.

Aldawood, H., & Skinner, G. (2019, May). Challenges of implementing training and awareness programs targeting cyber security social engineering. In *2019 Cybersecurity and Cyberforensics Conference (CCC)* (pp. 111-117). IEEE.

Alotaibi, F., Furnell, S., Stengel, I., & Papadaki, M. (2016). A review of using gaming technology for cyber-security awareness. *Int. J. Inf. Secur. Res.(IJISR)*, *6*(2), 660-666.

Alotaibi, M., & Alfehaid, W. (2018). Information security awareness: A review of methods, challenges and solutions. *Proceedings of the ICITST-WorldCIS-WCST-WCICSS-2018, Cambridge, UK*, 10-13.

Alqahtani, H., & Kavakli-Thorne, M. (2020, February). Exploring Factors Affecting User's Cybersecurity Behaviour by Using Mobile Augmented Reality App

(CybAR). In *Proceedings of the 2020 12th International Conference on Computer and Automation Engineering* (pp. 129-135).

Alshaikh, M., Maynard, S. B., Ahmad, A., & Chang, S. (2018). An exploratory study of current information security training and awareness practices in organizations.

Amankwa, E., Loock, M., & Kritzinger, E. (2014, December). A conceptual analysis of information security education, information security training and information security awareness definitions. In *The 9th International Conference for Internet Technology and Secured Transactions (ICITST-2014)* (pp. 248-252). IEEE.

Amankwa, E., Loock, M., & Kritzinger, E. (2015, November). Enhancing information security education and awareness: Proposed characteristics for a model. In *2015 Second International Conference on Information Security and Cyber Forensics (InfoSec)* (pp. 72-77). IEEE.

Ariffin, M. M., Ahmad, W. F. W., & Sulaiman, S. (2016, August). Investigating the educational effectiveness of gamebased learning for IT education. In *2016 3rd International Conference on Computer and Information Sciences (ICCOINS)* (pp. 570-573). IEEE.

Armstrong, M. B., & Landers, R. N. (2018). Gamification of employee training and development. *International Journal of Training and Development*, *22*(2), 162-169.

Ashenden, D. (2008). Information Security management: A human challenge?. *Information security technical report*, *13*(4), 195-201.

Battistella, P., & von Wangenheim, C. G. (2016). Games for teaching computing in higher education–a systematic review. *IEEE Technology and Engineering Education*, *9*(1), 8-30.

Bauer, G., Martinek, D., Kriglstein, S., Wallner, G., & Wölfle, R. (2017). Digital game-based learning with" Internet Hero": a game about the internet for children aged 9–12 years. In *Context Matters!: Exploring and Reframing Games in Context. Proceedings of the 7th Vienna Games Conference FROG 2013* (pp. 148-161). New Academic Press.

Baxter, R. J., Holderness Jr, D. K., & Wood, D. A. (2016). Applying basic gamification techniques to IT compliance training: Evidence from the lab and field. *Journal of information systems*, *30*(3), 119-133.

Beckers, K., & Pape, S. (2016, September). A serious game for eliciting social engineering security requirements. In *2016 IEEE 24th International Requirements Engineering Conference (RE)* (pp. 16-25). IEEE.

Blythe, J. M., & Coventry, L. (2012, September). Cyber security games: a new line of risk. In *International Conference on Entertainment Computing* (pp. 600-603). Springer, Berlin, Heidelberg.

Boyce, M. W., Duma, K. M., Hettinger, L. J., Malone, T. B., Wilson, D. P., & Lockett-Reynolds, J. (2011, September). Human performance in cybersecurity: a research agenda. In *Proceedings of the Human Factors and Ergonomics Society annual meeting* (Vol. 55, No. 1, pp. 1115-1119). Sage CA: Los Angeles, CA: SAGE Publications.

Burns, A. J., Roberts, T. L., Posey, C., Bennett, R. J., & Courtney, J. F. (2015, January). Assessing the role of security education, training, and awareness on insiders' security-related behavior: An expectancy theory approach. In *2015 48th Hawaii International Conference on System Sciences* (pp. 3930-3940). IEEE.

Caballero, A. (2017). Security education, training, and awareness. In *Computer and information security handbook* (pp. 497-505). Morgan Kaufmann.

Chen, T., Hammer, J., & Dabbish, L. (2019, May). Self-efficacy-based game design to encourage security behavior online. In *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems* (pp. 1-6).

Chen, T., Stewart, M., Bai, Z., Chen, E., Dabbish, L., & Hammer, J. (2020, July). Hacked Time: Design and Evaluation of a Self-Efficacy Based Cybersecurity Game. In *Proceedings of the 2020 ACM Designing Interactive Systems Conference* (pp. 1737-1749).

Chmura, J. (2017). Forming the awareness of employees in the field of information security. *Journal of Positive Management*, *8*(1), 78-85.

CJ, G., Pandit, S., Vaddepalli, S., Tupsamudre, H., Banahatti, V., & Lodha, S. (2018, October). Phishy-a serious game to train enterprise users on phishing awareness. In *Proceedings of the 2018 annual symposium on computer-human interaction in play companion extended abstracts* (pp. 169-181).

Cone, B. D., Thompson, M. F., Irvine, C. E., & Nguyen, T. D. (2006, May). Cyber security training and awareness through game play. In *IFIP International Information Security Conference* (pp. 431-436). Springer, Boston, MA.

Connolly, T. M., Boyle, E. A., MacArthur, E., Hainey, T., & Boyle, J. M. (2012). A systematic literature review of empirical evidence on computer games and serious games. *Computers & education*, *59*(2), 661-686.

Denning, T., Kohno, T., & Shostack, A. (2013, March). Control-Alt-Hack™: a card game for computer security outreach and education. In *Proceeding of the 44th ACM technical symposium on Computer science education* (pp. 729-729).

Enriquez, H., Kadobayashi, Y., & Fall, D. (2018, October). Project config. play a turn-based strategy security board game. In *Proceedings of the 12th European conference on games based learning (ECGBL 2018)* (pp. 72-81).

Euronews. (2020). Cyber-attack in Finland hits email accounts of MPs and parliament. Accessed from https://www.euronews.com/2020/12/28/cyber-attack-in-finland-hits-email-accounts-of-mps-and-parliament

Farooq, A. (2019a). *In Quest of information security in higher education institutions: Security awareness, concerns and behaviour of students* (Doctoral dissertation, Ph. D dissertation, University of Turku, Turku, 2019. Accessed on December 25, 2019. [Online]. Available: https://www. utupub. fi/handle/10024/148447).

Farooq, A., Ndiege, J. R. A., & Isoaho, J. (2019b). Factors Affecting Security Behavior of Kenyan Students: An Integration of Protection Motivation Theory and Theory of Planned Behavior. In *2019 IEEE AFRICON* (pp. 1-8). IEEE.

Farooq, A., Isoaho, J., Virtanen, S., & Isoaho, J. (2015a). Information security awareness in educational institution: An analysis of students' individual factors. In *2015 IEEE Trustcom/BigDataSE/ISPA* (Vol. 1, pp. 352-359). IEEE.

Farooq, A., Isoaho, J., Virtanen, S., & Isoaho, J. (2015b). Observations on genderwise differences among university students in information security awareness. *International Journal of Information Security and Privacy (IJISP)*, *9*(2), 60-74.

Ferragut, E. M., Brady, A. C., Brady, E. J., Ferragut, J. M., Ferragut, N. M., & Wildgruber, M. C. (2016, April). HackAttack: game-theoretic analysis of realistic

cyber conflicts. In *Proceedings of the 11th Annual Cyber and Information Security Research Conference* (pp. 1-8).

Filipczuk, D., Mason, C., & Snow, S. (2019, May). Using a game to explore notions of responsibility for cyber security in organisations. In *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems* (pp. 1-6).

Fry, R. (2021). What Cyber Security Can Learn From Video Games. Retrieved from https://www.securityweek.com/what-cybersecurity-can-learn-video-games

G-Cube LMS Enterprise. (2016). 5 game elements that create effective learning games. Retrieved from https://elearningindustry.com/5-game-elements-create-effective-learning-games

Gjertsen, E. G. B., Gjære, E. A., Bartnes, M., & Flores, W. R. (2017, February). Gamification of Information Security Awareness and Training. In *ICISSP* (pp. 59-70).

Hale, M. L., Gamble, R. F., & Gamble, P. (2015, January). CyberPhishing: A game-based platform for phishing awareness testing. In *2015 48th Hawaii International Conference on System Sciences* (pp. 5260-5269). IEEE.

Hendrix, M., Al-Sherbaz, A., & Victoria, B. (2016). Game based cyber security training: are serious games suitable for cyber security training?. *International Journal of Serious Games*, *3*(1).

Holdsworth, J., & Apeh, E. (2017, September). An effective immersive cyber security awareness learning platform for businesses in the hospitality sector. In *2017 IEEE 25th International Requirements Engineering Conference Workshops (REW)* (pp. 111-117). IEEE.

Islam, T., Becker, I., Posner, R., Ekblom, P., McGuire, M., Borrion, H., & Li, S. (2019, November). A socio-technical and co-evolutionary framework for reducing human-related risks in cyber security and cybercrime ecosystems. In *International Conference on Dependability in Sensor, Cloud, and Big Data Systems and Applications* (pp. 277-293). Springer, Singapore.

Jin, G., Tu, M., Kim, T. H., Heffron, J., & White, J. (2018, February). Game based cybersecurity training for high school students. In *Proceedings of the 49th ACM Technical Symposium on Computer Science Education* (pp. 68-73).

Kapp, K.M. (2014). 8 Game Elements to Make Learning More Intriguing. Retrieved from https://www.td.org/insights/eight-game-elements-to-make-learning-more-intriguing

Kasurinen, J. (2017). Usability issues of virtual reality learning simulator in healthcare and cybersecurity. *Procedia computer science*, *119*, 341-349.

Khan, B., Alghathbar, K. S., Nabi, S. I., & Khan, M. K. (2011). Effectiveness of information security awareness methods based on psychological theories. *African journal of business management*, *5*(26), 10862-10868.

Khando, K., Gao, S., Islam, S. M., & Salman, A. (2021). nEnhancing Employees Information Security Awareness in Private and Public Organisations: A Systematic Literature Review. *Computers & Security*, 102267.

Kitchenham, B., Brereton, O. P., Budgen, D., Turner, M., Bailey, J., & Linkman, S. (2009). Systematic literature reviews in software engineering–a systematic literature review. *Information and software technology*, *51*(1), 7-15.

Antonaci, A., Klemke, R., Stracke, C. M., Specht, M., Spatafora, M., & Stefanova, K. (2017, June). Gamification to empower information security education. In *International GamiFIN Conference 2017* (pp. 32-38).

Kocakoyun, S., & Ozdamli, F. (2018). A review of research on gamification approach in education. *Socialization-A Multidimensional Perspective*.

Le Compte, A., Elizondo, D., & Watson, T. (2015, May). A renewed approach to serious games for cyber security. In *2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace* (pp. 203-216). IEEE.

Leune, K., & Petrilli Jr, S. J. (2017, September). Using capture-the-flag to enhance the effectiveness of cybersecurity education. In *Proceedings of the 18th Annual Conference on Information Technology Education* (pp. 47-52).

Mathoosoothenen, V. N., Sundaram, J. S., Palanichamy, R. A., & Brohi, S. N. (2017, December). An Integrated Real-Time Simulated Ethical Hacking Toolkit with Interactive Gamification Capabilities and Cyber Security Educational Platform. In *Proceedings of the 2017 International Conference on Computer Science and Artificial Intelligence* (pp. 199-202).

McCoy, C., & Fowler, R. T. (2004, October). " You are the key to security" establishing a successful security awareness program. In *Proceedings of the 32nd annual ACM SIGUCCS conference on User services* (pp. 346-349).

Metalidou, E., Marinagi, C., Trivellas, P., Eberhagen, N., Skourlas, C., & Giannakopoulos, G. (2014). The human factor of information security: Unintentional damage perspective. *Procedia-Social and Behavioral Sciences*, *147*, 424-428.

Mirkovic, J., Tabor, A., Woo, S., & Pusey, P. (2015). Engaging Novices in Cybersecurity Competitions: A Vision and Lessons Learned at {ACM} Tapia 2015. In *2015 {USENIX} Summit on Gaming, Games, and Gamification in Security Education (3GSE 15)*.

Mittal, S. (2015). Understanding the human dimension of cyber security. *Indian Journal of Criminology & Criminalistics (ISSN 0970–4345)*, *34*(1), 141-152.

Moher, D., Liberati, A., Tetzlaff, J., & Altman, D. G. (2010). Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement. *Int J Surg*, *8*(5), 336-341.

Mongeon, P., & Paul-Hus, A. (2016). The journal coverage of Web of Science and Scopus: a comparative analysis. *Scientometrics*, *106*(1), 213-228.

Mostafa, M., & Faragallah, O. S. (2019). Development of serious games for teaching information security courses. *IEEE Access*, *7*, 169293-169305.

Nagarajan, A., Allbeck, J. M., Sood, A., & Janssen, T. L. (2012, May). Exploring game design for cybersecurity training. In *2012 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems (CYBER)* (pp. 256-262). IEEE.

Nguyen, T. A., & Pham, H. (2020, October). A Design Theory-Based Gamification Approach for Information Security Training. In *2020 RIVF International Conference on Computing and Communication Technologies (RIVF)* (pp. 1-4). IEEE.

Oladimeji, S., & Kerner, S.M. (2021). SolarWinds hack explained: Everything you need to know. Accessed from https://whatis.techtarget.com/feature/SolarWinds-hack-explained-Everything-you-need-to-know

Olano, M., Sherman, A., Oliva, L., Cox, R., Firestone, D., Kubik, O., ... & Thomas, D. (2014). SecurityEmpire: Development and evaluation of a digital game to promote cybersecurity education. In *2014 {USENIX} Summit on Gaming, Games, and Gamification in Security Education (3GSE 14)*.

Olanrewaju, A. S. T., & Zakaria, N. H. (2015). Social engineering awareness game (SEAG): an empirical evaluation of using game towards improving information security awareness.

Olijnyk, N. V. (2015). A quantitative examination of the intellectual profile and evolution of information security from 1965 to 2015. *Scientometrics*, *105*(2), 883-904.

Omiya, T., & Kadobayashi, Y. (2019). Secu-One: A Proposal of Cyber Security Exercise Tool for Improving Security Management Skill. In *Proceedings of the 2019 7th International Conference on Information and Education Technology* (pp. 259-268).

Omiya, T., Fall, D., & Kadobayashi, Y. (2019, November). IoT-Poly: An IoT Security Game Practice Tool for Learners Motivation and Skills Acquisition. In *Proceedings of the 19th Koli Calling International Conference on Computing Education Research* (pp. 1-10).

Oroszi, E. D. (2019, June). Security awareness escape room-a possible new method in improving security awareness of users. In *2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)* (pp. 1-4). IEEE.

Osborne, C. (2021). Everything you need to know about the Microsoft Exchange Server hack. Accessed from https://www.zdnet.com/article/everything-you-need-to-know-about-microsoft-exchange-server-hack/

Patriciu, V. V., & Furtuna, A. C. (2009, December). Guide for designing cyber security exercises. In *Proceedings of the 8th WSEAS International Conference on E-Activities and information security and privacy* (pp. 172-177). World Scientific and Engineering Academy and Society (WSEAS).

Paul, J., & Criado, A. R. (2020). The art of writing literature review: What do we know and what do we need to know?. *International Business Review*, *29*(4), 101717.

Petri, G., & von Wangenheim, C. G. (2017). How games for computing education are evaluated? A systematic literature review. *Computers & education*, *107*, 68-90.

Prinetto, P., Roascio, G., & Varriale, A. (2020, September). Hardware-based Capture-The-Flag Challenges. In *2020 IEEE East-West Design & Test Symposium (EWDTS)* (pp. 1-8). IEEE.

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: an action research study. *MIS quarterly*, 757-778.

Quayyum, F. (2020, June). Cyber security education for children through gamification: Challenges and research perspectives. In *International Conference in Methodologies and intelligent Systems for Techhnology Enhanced Learning* (pp. 258-263). Springer, Cham.

Reeves, A., Calic, D., & Delfabbro, P. (2021). “Get a red-hot poker and open up my eyes, it's so boring” 1: Employee perceptions of cybersecurity training. *Computers & Security*, *106*, 102281.

Rieff, I. (2018). Systematically Applying Gamification to Cyber Security Awareness Trainings: A framework and case study approach.

Roepke, R., & Schroeder, U. (2019). The Problem with Teaching Defence against the Dark Arts: A Review of Game-based Learning Applications and Serious Games for Cyber Security Education. In *CSEDU (2)* (pp. 58-66).

Röpke, R., Schroeder, U., Drury, V., & Meyer, U. (2020, July). Towards Personalized Game-Based Learning in Anti-Phishing Education. In *2020 IEEE 20th*

International Conference on Advanced Learning Technologies (ICALT) (pp. 65-66). IEEE.

Ryan, W., Stewart, J., Verleger, D., & Crofts, J. (2013). Network Nightmares: Using games to teach networks and security. In *FDG* (pp. 413-416).

Sardi, L., Idri, A., & Fernández-Alemán, J. L. (2017). A systematic review of gamification in e-Health. *Journal of biomedical informatics*, *71*, 31-48.

Scholefield, S., & Shepherd, L. A. (2019, July). Gamification techniques for raising cyber security awareness. In *International Conference on Human-Computer Interaction* (pp. 191-203). Springer, Cham.

Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L. F., Hong, J., & Nunge, E. (2007, July). 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* (pp. 88-99).

Shostack, A. (2014). Elevation of privilege: Drawing developers into threat modeling. In *2014 {USENIX} Summit on Gaming, Games, and Gamification in Security Education (3GSE 14)*.

Silic, M., & Lowry, P. B. (2020). Using design-science based gamification to improve organizational security training and compliance. *Journal of management information systems*, *37*(1), 129-161.

Sookhanaphibarn, K., & Choensawat, W. (2020, October). Educational Games for Cybersecurity Awareness. In *2020 IEEE 9th Global Conference on Consumer Electronics (GCCE)* (pp. 424-428). IEEE.

Soomro, A. B., Salleh, N., Mendes, E., Grundy, J., Burch, G., & Nordin, A. (2016). The effect of software engineers' personality traits on team climate and

performance: A Systematic Literature Review. *Information and Software Technology*, *73*, 52-65.

Thomas, L. J., Balders, M., Countney, Z., Zhong, C., Yao, J., & Xu, C. (2019, July). Cybersecurity Education: From beginners to advanced players in cybersecurity competitions. In *2019 IEEE International Conference on Intelligence and Security Informatics (ISI)* (pp. 149-151). IEEE.

Thompson, M. (2017). 6 reasons why interactive narrative learning is an effective eLearning strategy. Retrieved from https://elearningindustry.com/interactive-narrative-learning-effective-elearning-strategy-6-reasons

Thomson, M. E., & von Solms, R. (1998). Information security awareness: educating your users effectively. *Information management & computer security*.

Tioh, J. N., Mina, M., & Jacobson, D. W. (2017, October). Cyber security training a survey of serious games in cyber security. In *2017 IEEE Frontiers in Education Conference (FIE)* (pp. 1-5). IEEE.

Tøndel, I. A., Oyetoyan, T. D., Jaatun, M. G., & Cruzes, D. (2018, April). Understanding challenges to adoption of the Microsoft Elevation of Privilege game. In *Proceedings of the 5th Annual Symposium and Bootcamp on Hot Topics in the Science of Security* (pp. 1-10).

Turton, W., & Mehrotra, K. (2021). Hackers breach colonial pipeline using compromised passwords. accessed from https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password

Underhay, L., Pretorius, A., & Ojo, S. (2016, May). Game-based enabled e-learning model for e-Safety education. In *2016 IST-Africa Week Conference* (pp. 1-7). IEEE.

Veneruso, S. V., Ferro, L. S., Marrella, A., Mecella, M., & Catarci, T. (2020, September). CyberVR: An Interactive Learning Experience in Virtual Reality for Cybersecurity Related Issues. In *Proceedings of the International Conference on Advanced Visual Interfaces* (pp. 1-8).

Von Solms, S. H., & Von Solms, R. (2009). Information security education, training and awareness. In *Information security governance* (pp. 1-14). Springer, Boston, MA.

Wen, Z. A., Lin, Z., Chen, R., & Andersen, E. (2019, May). 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* (pp. 1-12).

Yasin, A., Liu, L., Li, T., Fatima, R., & Jianmin, W. (2019). Improving software security awareness using a serious game. *IET Software*, *13*(2), 159-169.

Zhang-Kennedy, L., & Chiasson, S. (2021). A systematic review of multimedia tools for cybersecurity awareness and education. *ACM Computing Surveys (CSUR)*, *54*(1), 1-39.

Zimmermann, V., & Renaud, K. (2019). Moving from a 'human-as-problem" to a 'human-as-solution" cybersecurity mindset. *International Journal of Human-Computer Studies*, *131*, 169-187.

Zoto, E., Kowalski, S. J., Lopez Rojas, E. A., & Kianpour, M. (2018). Using a socio-technical systems approach to design and support systems thinking in cyber security education. CEUR Workshop Proceedings.

8 Appendix

8.1 Anti-Phishing Phil

Anti-Phishing Phil is an animation game that helps players identify phishing URLs. The game's narrative is based on a fish called Phil that eat worms which represent URLs to grow. Players representing Phil are required to eat worms associated with safe URLs and reject worms associated with phishing URLs. Phil's father is a game character that represents an experienced fish that gives Phil advice on worms to reject (Sheng et al., 2007; Wen et al., 2019).

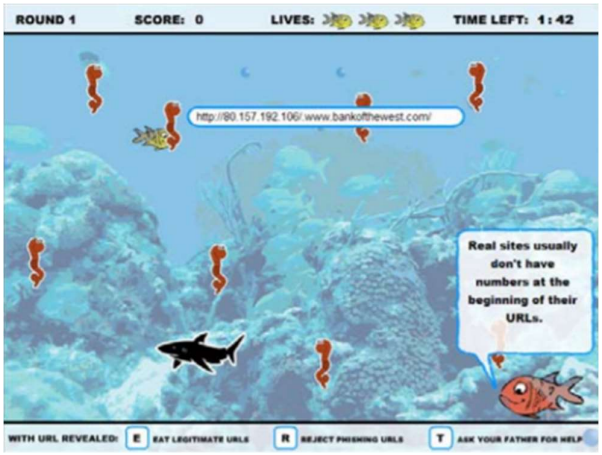


Figure 1: Game screen of Phil inspecting an URL before eating (Sheng et al., 2007)

Gameplay consists of four rounds and each round is two minutes long. During a round, players select which worms to eat and which worms to reject from a selection of eight worms. Players are shown the complete URL when they move the mouse over the worm as shown in figure 1 above. Players are awarded points and get positive feedback messages for each correct worm-eaten and are slightly penalized for each good worm rejected. This indicates a false positive determination of a phishing URL. Players are severely penalized and get negative feedback messages for each bad worm-eaten. This indicates the player has fallen victim to a phishing URL. Players have to make six correct worm determinations during each round before proceeding to the next round. Each subsequent round is more difficult than the previous round and includes predators that players must avoid. After each round players review the URLs and have a brief tutorial before proceeding to the next round (Sheng et al., 2007).

Anti-Phishing Phil is out of context and does not accurately reflect a player's realistic experience of malicious URLs. The game focuses on malicious syntax in URLs and ignores its semantics (Wen et al., 2019). An evaluation of the game indicates increased phishing awareness amongst players. Players also found the game to be fun and educational (Sheng et al., 2007).

8.2 What.Hack

What.Hack as a phishing game that attempts to mitigate context failures found in Anti-Phishing Phil. It is a role-playing game that simulates actual phishing attacks. Players learn about phishing concepts and experiences phishing attacks as they would in a real-world environment. The phishing emails used in the game are obtained from templates of real-world phishing emails. The game combines different phishing techniques as deployed by attackers further reinforcing the game's realism and similarity to the real world (Wen et al., 2019).

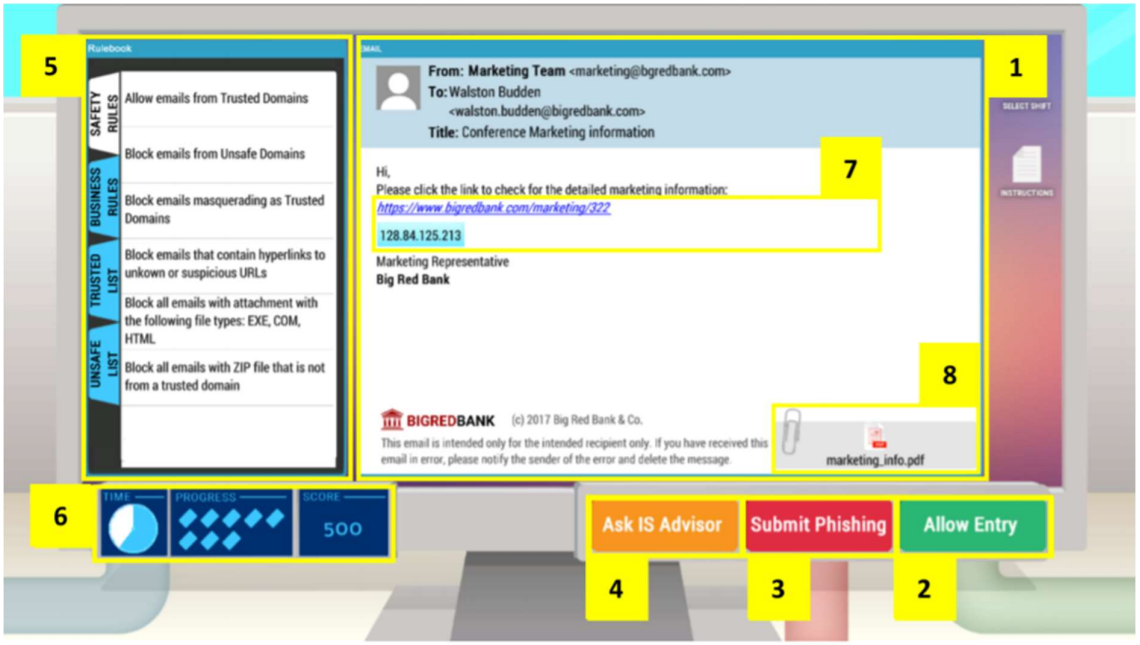


Figure 2: Game screen of What.Hack showing (1) player receives an email (2) allow entry button for legitimate emails (3) submit email as phishing (4) ask IS advisor when unsure of email legitimacy (5) rulebook that helps players decide email legitimacy (6) number of emails processed within a given time (Wen et al., 2019)

Gameplay consists of a series of quizzes that introduce players to phishing concepts. As shown in figure 2 the game has a tutorial that introduces players to the rules used

to screen emails to determine their legitimacy or illegitimacy. As the game progresses the screening rules become more specific culminating in a rule set the player can apply in evaluating real-world emails. Players assume the role of a bank employee tasked with the responsibility of processing their business emails while avoiding phishing emails. Players are required to learn and apply the screening rules to process business emails and discard phishing emails as shown in figure 3 (B) below. If a player is unsure of an email, they can ask the IS advisor as shown in figure 3 (A) below. The IS advisor assists players in determining the legitimacy or illegitimacy of emails. To win the game players must correctly process as many business-related emails as possible and discard all phishing emails (Wen et al., 2019).

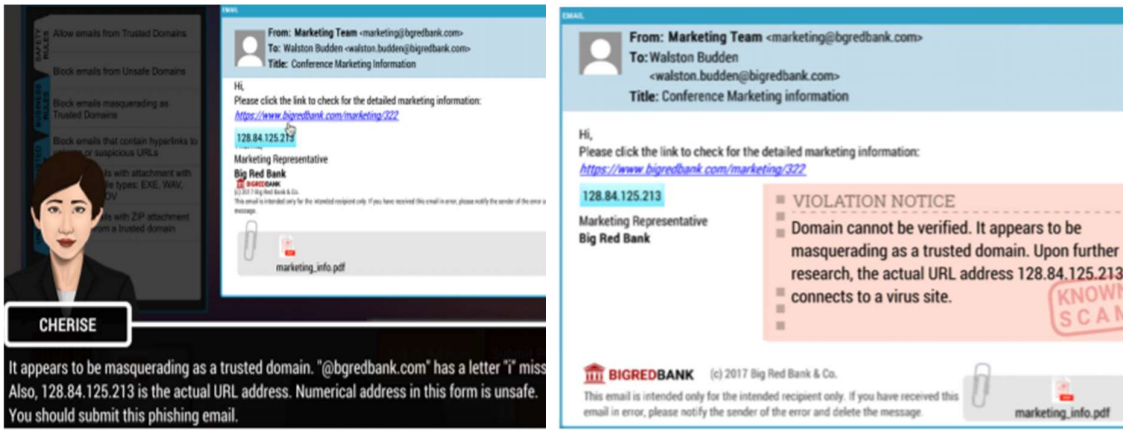


Figure 3: Game screen showing (A) IS advisor's advice (B) The game's feedback when a player decides on the email's legitimacy (Wen et al., 2019)

What.Hack correctly mimics the email processing tradeoffs experienced by players in their daily life. The game includes time pressure which reflects the time constraints players experience when screening emails. The game includes IT help desk interaction which correlates to players' work reality of having to report suspected phishing emails to the IT help desk. An evaluation of the game shows improved phishing email detection amongst players. Players learn phishing concepts and anti-phishing skills engagingly from the game. The game also increases phishing efficacy i.e. the confidence of a player in their judgment on phishing emails (Wen et al., 2019).

8.3 Phishy

Phishy is a phishing awareness game that introduces players to the following:

- Familiarization of short URLs.
- URL inspection methods to identify phishing.
- An online search of brand names to discover legitimate URLs.

Phishy is a story-based single-player animation game based on a character called Sam who gets lost at sea in a boat with a hungry tiger as a result of a phishing scam as shown in figure 4 (A) below. Sam has a mission of returning to shore by navigating the boat while feeding the hungry tiger with fish. The hungry tiger moves one step closer to Sam each time Sam fails to feed it and threatens Sam's chance of navigating back to shore. Sam is required to hook a fish and feed the tiger by selecting the correct answer to URL-related questions that pops up in the game. Feeding the tiger prevents it from moving one step closer to Sam. Selecting the wrong answer results in the fish unhooking and the tiger moving one step closer to Sam as shown in figure 4 (B) below. The game provides players with URL tips that assist them in answering the questions (CJ et al., 2018).

Figure 4: Game screen showing (A) Story how Sam got lost at sea (B) Sam failing to hook a fish to feed the tiger and hooking a fish to feed the tiger (CJ et al., 2018)

The game has 3 levels, level 1 introduces players to IP addresses and asks basic questions like ‘is the link a phishing URL?’. The questions require a yes or no answer indicating a true positive for a phishing URL and a true negative for a legitimate URL. At the beginning of each level, players are provided with tips on how to determine the validity of URLs in the real world. Level 2 introduces players to short URLs, at the beginning of the level players are provided with tips on how to expand short URLs and determine their legitimacy. Level 3 introduces players to brand URLs with syntax changes to the domain name. Combosquatting is a popular phishing attack method in which attackers register variations to popular domain names. Each level features different fish to be caught and feed to the tiger. On successful completion of level 3, Sam arrives back at the shore (CJ et al., 2018).

The story at the beginning of the game explaining how Sam got stranded at sea with the tiger encourages story-based learning by the player. Phishy game deploys survival game element which requires Sam to overcome challenges to get back to shore. This brings out the player’s self-preservation instinct to survive the game odds which is also a motivating factor. The adventure game element in Phishy is useful for player retention of the lessons learned during the game. An evaluation of the game shows increased knowledge and skills in phishing URL detection amongst players. Player’s confidence in their abilities to detect URL phishing also increased after playing the game. Players found the game to be entertaining, fun, and educational (CJ et al., 2018).

8.4 Persuaded

Persuaded is a single-player social engineering awareness card game that develops players' resistance to social engineering attacks by inoculating them. Inoculation occurs by continuously exposing players to realistic social engineering attack scenarios which helps them develop appropriate responses to social engineering attacks. These developed responses to social engineering attacks become common practice players apply in real life (Aladawy et al., 2018).

The game consists of attack cards, defence cards, see the future cards and skip turn cards as shown in figure 5 below. Attack cards have descriptions of social engineering attack scenarios in textual format. Defence cards have descriptions of appropriate responses to social engineering attacks, for each attack card scenario, there is a

defence card. See the future cards are action cards that allow players to have a sneak peek into the upper three cards in the card deck. Skip turn cards are action cards that allow players to place the card currently at the top of the deck to the bottom of the deck. The game introduces players to baiting, phishing, tailgating, mail attachment, impersonation, voice of authority, and popup windows social engineering content (Aladawy et al., 2018).

The gameplay consists of a player drawing a card from hand or the card deck as shown in figure 6 below. If a player does not draw an attack card from the deck, the drawn card is added to the player's cards in hand. If a player draws an attack card, they must play a defence card for the drawn attack card. The correct defence card, gains players points likewise the wrong defence card loses them points. Matching attack and defence cards are discarded thereafter. If a player does not have a defence card at hand for a drawn attack card, they lose a life. When a player loses three lives the game is over. See the future card help a player view the next 3 cards on the deck. A player can then postpone an attack card if they do not have a matching defence card using a skip turn card. Action cards i.e. see the future cards and skip turn cards can only be played before drawing a card from the card deck. The game is won when the deck is empty (Aladawy et al., 2018).

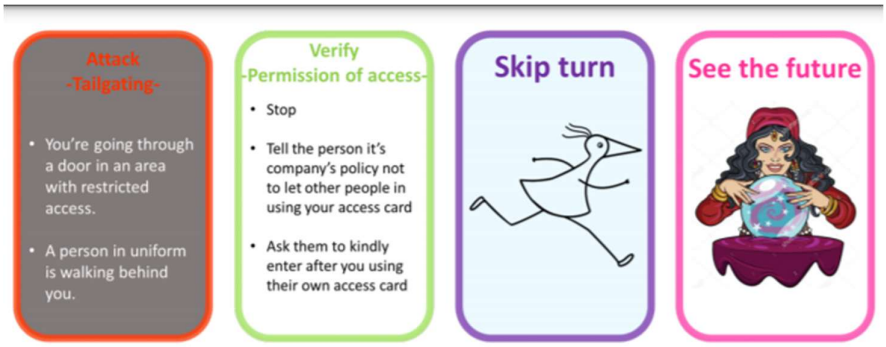


Figure 5: Persuaded cards (1) Attack card (2) Defence card (3) Skip turn card (4) See the future card (Aladawy et al., 2018)

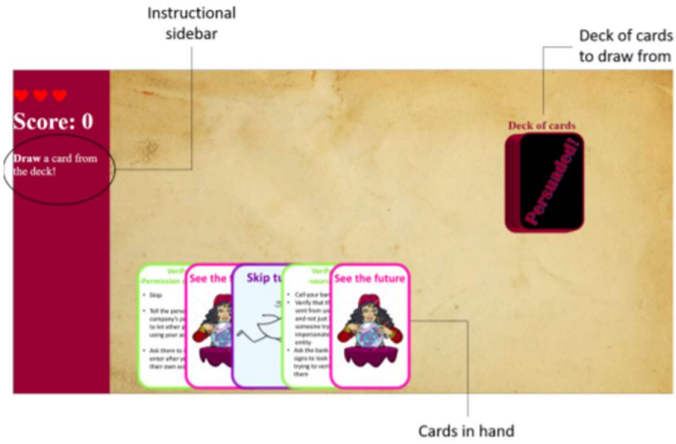


Figure 6: Gameplay using Persuaded cards (Aladawy et al., 2018)

An empirical evaluation of the game indicates improved tailgating awareness amongst players. Phishing links and mail attachment awareness showed little improvement and the game resulted in worse baiting awareness amongst players. Players were interested in replaying the game since they found it engaging (Aladawy et al., 2018).

8.5 Social Engineering Awareness Game (SEAG)

SEAG uses cards and quizzes to introduce players to basic social engineering concepts. The card game consists of 24 cards with 12 cards having social engineering terms textually written and 12 cards having corresponding pictorial representation of the terms. To maintain player engagement and monitor their progress the game is organized in levels one through three (Olanrewaju & Zakaria 2015).

Gameplay consists of level 1 where quizzes are used to increase player knowledge. Players answer basic social engineering questions meant to introduce them to basic social engineering concepts. Level 2 is a card matching game, where players match social engineering terms with their corresponding pictorial illustration. Players select two cards simultaneously, one from the terms deck and the other from the picture deck. If the terms and pictures match the cards are removed from the deck. Otherwise, the cards are returned to their respective decks and the player has to make another set of card selections. The Player's ability to link pictures with definitions is tested which help them visualize social engineering attack. Level 3 requires players to apply the knowledge obtained from the previous 2 levels. Players are required to analyze real-life social engineering attack scenarios and answer questions (Olanrewaju & Zakaria 2015).

An empirical evaluation of the game shows improved player knowledge and ability to detect social engineering attacks. However, players did not view the game to be user-friendly and user-centric (Olanrewaju & Zakaria 2015).

8.6 CyberPhishing

CyberPhishing is a client-server web simulation platform that provides players with a realistic web environment. The web environment is controlled thus limiting players' exposure during security awareness training. The platform provides players with phishing simulation and data tracking capabilities across three mediums mainly emails, web browsers, and social media. The platform can capture and analyze player data and use this analysis to customize future phishing awareness games (Hale et al., 2015).

According to Hale et al., (2015), player interaction with emails, web browsers, and social media are conducted as part of a game scenario. CyberPhishing game platform architecture consists of the following modules:

- The economy engine reacts to user actions and drives the game scenarios. Simulation.
- Simulation modules that mediate emails, web browsers, and social media as part of a game scenario.
- Administration module which allows phishing content to be dynamically built.

Gameplay consists of phishing, web browsing, and social media simulation. Players assume roles within the platform scenarios, and their tasks are explained to them by video and text. Email simulation provides players with HTML-enabled emails that included links and pictures. The emails are presented in an inbox format as shown in figure 7 (A) below. Web browser simulation provides players with browsers that have the lock icon associated with HTTPS, website certificates, and website URLs as shown in figure 7 (B) below. Social media simulation imitates twitter's interface and functionality with features like friends, followers, and username as shown in figure 7 (C) below. Players are presented with nine content items from each medium and are required to select whether to trust or not to trust the content. Further modification to the platform could include a trustworthiness index to understand finer trust granularity. Scores, badges, and titles are awarded to players based on how well the player detects phishing (Hale et al., 2015).

8.7 Personalization of social engineering games

Existing phishing awareness games have shortcomings that limit the learning potential of players. These shortcomings are a result of games lacking relevant phishing content which may be out of context. Phishing attacks have become more sophisticated with attackers using compromised accounts to send phishing emails from known senders. Attackers are also using information from data breach information for targeted phishing. Therefore personalization of phishing awareness games would mitigate these shortcomings (Röpke et al., 2020).

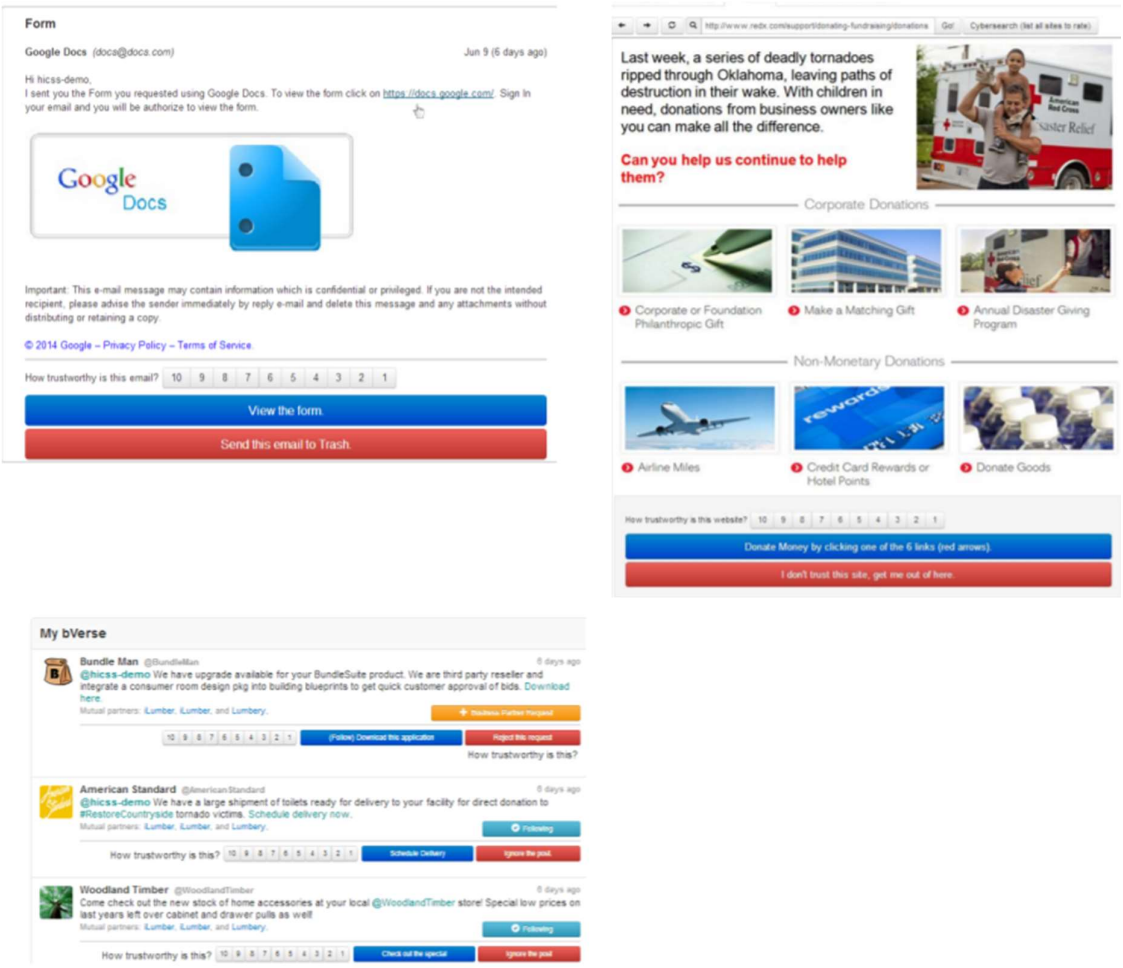


Figure 7: Game screen showing (A) CyberPhishing social engineering (B) CyberPhishing web browsing (C) CyberPhishing social media (Hale et al., 2015)

Players may be unfamiliar with some service e.g. social media and therefore cannot conclusively determine whether the service presents a threat or not. As a result,

phishing games are not an authentic representation of players' environments. Players therefore cannot transfer the phishing knowledge obtained from games to their day-to-day activities. A personalization pipeline is recommended to personalize social engineering games. This is achieved through data collection, content generation, and content delivery (Röpke et al., 2020).

1. Data collection is done to understand player requirements to build a customized player model. Player data can be collected manually, automatically, and through hybrid methods that use both manual and automatic collection. Data can be collected from players who provide data regarding their past online activity from memory. Data collected from players is subjective. Data can be collected from a player's browser history, bookmarks, login credentials, and cookies. Data collected from player data is objective. Data collected through the hybrid method is more accurate and trustworthy because it combines both objective and subjective player data (Röpke et al., 2020).
2. After synthesis of the player requirements from the data collected personalized content generation can proceed. For a personalized phishing game information regarding applications frequently visited by a player can be used to generate phishing URLs, websites, and emails (Röpke et al., 2020).
3. The generated content needs to be integrated using suitable interfaces into the game during content delivery. The personalized game content can be embedded into the game using JSON format (Röpke et al., 2020).

8.8 Role-playing quiz application

Role-playing quiz application develops players' security awareness on passwords. The game provides players with knowledge on how to generate strong passwords, commonly used passwords to avoid, and good password hygiene practices. The game implements role-playing, immediate feedback, time pressure, consequences, and competition game elements (Scholefield & Shepherd 2019).

The gameplay involves 2 characters a golden knight and a dark knight. The golden knight represents the player while the dark knight represents an opponent. Players answer multiple-choice questions related to passwords as shown in figure 8 below within some set time limit. For every correct answer, the dark knight loses health. Incorrect answers result in the golden knight losing health. This process is repeated

until one of the two characters loses all their health. The players' points are recorded on a leaderboard (Scholefield & Shepherd 2019).

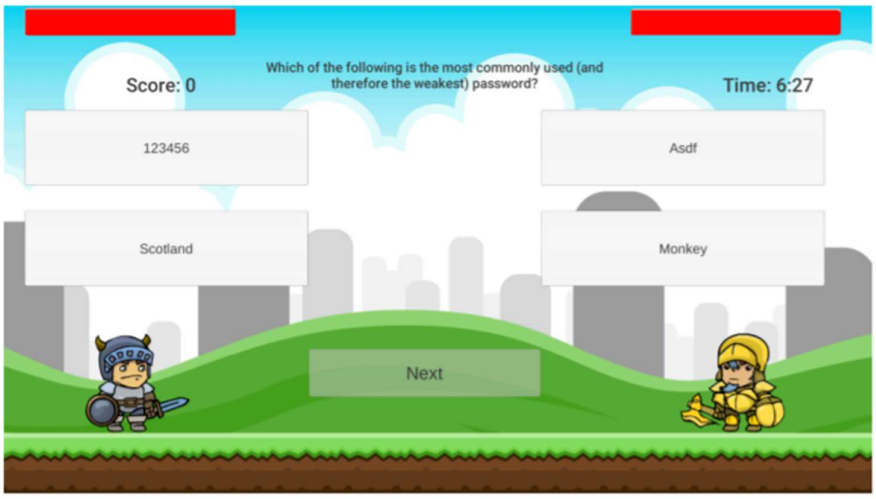


Figure 8: Game screen showing the game's sample questions and multiple choice answers (Scholefield & Shepherd 2019)

An evaluation of the game shows increased player knowledge on password security. Players also found the game to be fun and engaging (Scholefield & Shepherd 2019).

8.9 Elevation of Privileges (EoP)

Threat modelling identifies security defects in software during the software development life cycle (SDLC). Software development implemented using threat modelling is referred to as secure software development lifecycle (SSDL) and ensures that the software developed keeps performing under attack (Tøndel et al., 2018).

Elevation of Privileges (EoP) is a 3-6 player card game that develops player security awareness during software development. The architecture of software under design forms the basis of playing this game. The game helps players identify potential vulnerabilities in the software design. EoP card game consists of 84 cards, divided into 6 suits based on STRIDE i.e. Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privileges. Each suit has cards that are numbered from 2-10 an Ace, Jack, Queen, and King similar to normal playing cards. Each card lists the suit it belongs to, a number, and the threat the suit is based on as shown in figure 9 below. The Ace card represents an open threat in a suit. Players use

it to identify threats in a software design not listed by other cards on that suit (Omiya et al., 2019; Tøndel et al., 2018; Shostack 2014).

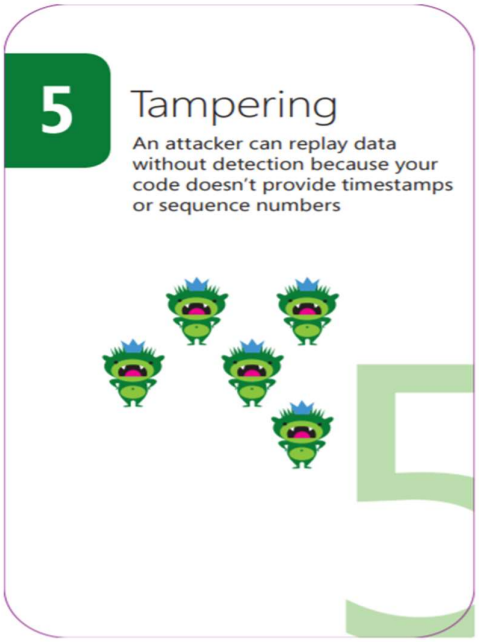


Figure 9: Elevation of Privileges card showing '5 of Tampering' (Shostack 2014)

Gameplay involves cards being dealt to players in a clockwise manner. Players read their cards out loud and the threat on the card is discussed. During discussions, players are required to determine whether the threat applies to the software design under consideration. Players should also determine whether the software design already has countermeasures to mitigate against this threat. If a player can't link the threat to the software design or the software design already has a countermeasure against the threat, play proceeds. If a player can link the threat to software design, a point is awarded to the player. When all the cards have been played the player with the most point is the winner (Shostack 2014).

The goal of the game is not to score points but to identify bugs and security vulnerabilities in software design. The game is designed to assist cyber security experts to identify flaws in software design. The game is good for learning about software security and aiding software security discussion amongst experts. However, the game only assists players in the identification of threats in software design but does not identify the threat's countermeasures. EoP game is not meant for novices who might find it hard to associate threats with system design. An evaluation of the

game shows that players find the game engaging. However players complained that the game took a long time to play, and the cards were not suitable for many software designs (Omiya et al., 2019; Tøndel et al., 2018).

8.10 IoT-Poly

IoT-Poly is an IoT security awareness card game targeted at cyber security personnel. The game helps players develop practical skills in IoT systems risk assessment. Cards assist players identify IoT system threats and the processes that occur after the identification of a threat. Players use a worksheet to record discussion during gameplay (Omiya et al., 2019). IoT system risk assessment involves:

- Risk identification - identifies and describes the risk to IoT systems. Risk identified are converted to a value that can be reduced to acceptable levels by deploying countermeasures in risk analysis (Omiya et al., 2019).
- Risk analysis - involves discussion of the IoT system characteristics and impact of the risk on the IoT system (Omiya et al., 2019).
- Risk evaluation – involves discussion on risks, their countermeasures, risk management, and risk acceptance approaches. Players also acquire communication skills during risk evaluation (Omiya et al., 2019).

IoT-poly cards consist of:

- IoT cards – which represent the IoT system and describe the system using a configuration diagram as shown in figure 10 (A) below. IoT system has different characteristics and players practice risk assessment on these characteristics. Players prioritize and rank the IoT system characteristics (Omiya et al., 2019).
- Attack surface cards – represent the attack surfaces present in an IoT system. The attack surfaces on the cards are as prescribed by the OWASP IoT project shown in figure 10 (B) below. OWASP link attack surfaces with their corresponding vulnerabilities from the OWASP top 10 vulnerabilities. Players make connections between IoT systems and attack surfaces thus determining the attack surface vulnerability (Omiya et al., 2019).
- Threat cards – use the common attack pattern enumeration and classification (CAPEC) attack library as shown in figure 10 (C) below. The library list common attack methods using different abstract levels. Threat cards summarize these attack methods (Omiya et al., 2019).

- Countermeasure cards – summarize best IoT security practices guidelines as prescribed by ENISA. The cards illustrate countermeasures developed for IoT systems as shown in figure 10 (D) below. The best practices are divided into policy, q, and technology (Omiya et al., 2019).

Figure 10: IoT-Poly (A) IoT Card (B) Attack Surface Card (C) Thread Card (D) Countermeasure Card (Omiya et al., 2019)

Gameplay involves the distribution of 10 threat and countermeasures cards amongst the players. A player draws an IoT card, and the rest of the players rank the card's characteristics according to the card's system configuration diagram. A player draws a random attack surface card and presents it. Each player presents one threat card they consider serious from the threat cards at hand. Players discuss and rank the threats in order of severity. Players use the worksheet to describe the risk scenario based on the most severe threat discussed. Each player then presents one countermeasure they consider to be effective against the risk scenario on the worksheet. The players discuss and rank the countermeasures in order of effectiveness. Players also discuss outstanding risks associated with the top-ranked countermeasure and determine whether the risk is acceptable. These discussions are entered on the worksheet. The game is repeated with different attack surfaces and IoT cards (Omiya et al., 2019).

An evaluation of IoT-Poly shows that players learned IoT security awareness as a result of playing the game. Players also found the game to be engaging and fun to play (Omiya et al., 2019).

8.11 Control-Alt-Hack

Control-Alt-Hack is a 3 – 6 player card game that increases players' knowledge of high level cyber security concepts and challenges. Granular concepts like anti-phishing techniques are not the focus of this game. The game's target audience is players without considerable computer science education, training, and awareness. The game introduces players to topics such as botnets, censorship, exploiting unpatched software, exploiting weak passwords, insider threats, reverse engineering, social engineering, and tracking (Denning et al., 2013; Wen et al., 2019).

Control-Alt-Hack has 156 cards game divided into 4 card decks i.e. hacker cards, mission cards, entropy cards, and attendance cards as shown in figures 11 and 12 below. Entropy and attendance cards support game mechanics. Players play the role of white hat hackers working in a company. Players complete a mission to get hacker credentials and lose hacker credentials for failing on a mission. The goal is to accumulate enough hacker credentials to become the company's CEO (Denning et al., 2013).

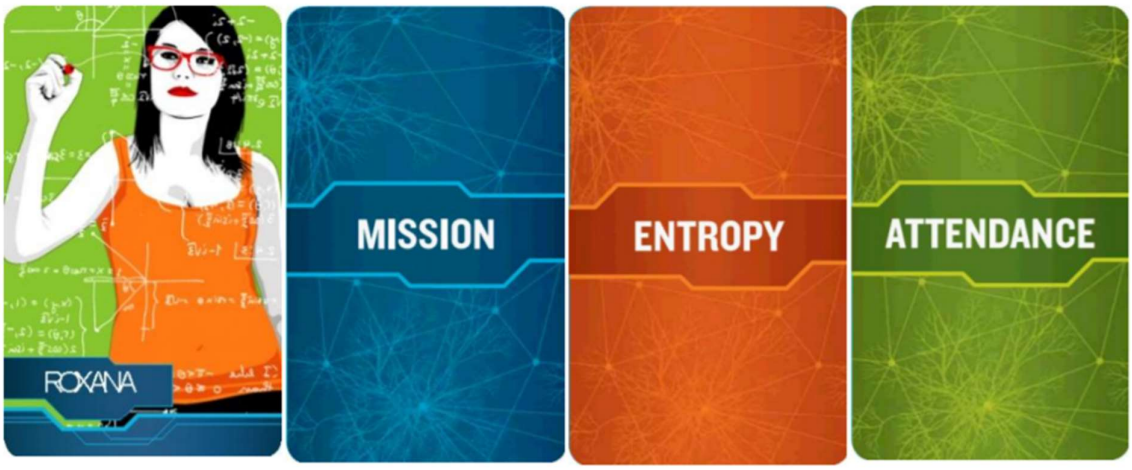


Figure 11: Control-Alt-Hack cards backside (1) Hacker card (2) Mission card (3) Entropy card (4) Attendance card (Denning et al., 2013)

Gameplay consists of players getting hacker cards with skills such as hardware hacking, software wizardry, social engineering, network ninja, cryptanalysis, and

forensic skills. Players also get entropy cards, attendance cards, money, and hacker credentials. Players draw a mission card that contains a task to be accomplished by the player. The dice roll and hacker skills level on the hacker card determines the success or failure of a mission. Players may use bag of trick cards which are entropy cards to buy skills they lack and require for the mission. Players may also use lightning strike cards which are also entropy cards to sabotage their opponent. On successful completion of a mission, players are awarded hacker credentials. Failure to complete a mission results in loss of hacker credentials (Denning et al., 2013).

Figure 12: Control-Alt-Hack cards front side (1) Hacker information (2) Mission statement (3) Entropy bag of tricks card (4) Entropy lightning strikes card (Denning et al., 2013)

8.12 Project config. Play

Project config.play is a 2 person strategy board game in which players take turns to attack the opponent's vulnerabilities while protecting their territory. The game includes a board and action cards of different colours as shown in figure 13 (A) and (B) below. The game also includes colour and number dice. The game simulates authentication requirements, configuration conditions, race conditions and introduces players to common vulnerabilities and exposure (CVE). CVE is a list of all known and publicly disclosed computer security flaws. A common vulnerability scoring system (CVSS) is used to build the game's scenarios. CVSS assigns numerical scores to vulnerabilities allowing responders to prioritize responses and resources according to the threat's numerical score (Enriquez et al., 2018).

According to Enriquez & Kadobayashi (2018), some game scenarios are built using CVSS features that do not change over time such as:

- Access vector – indicates how the vulnerability is exploited either locally or remotely.
- Access complexity – indicates the level of complexity required to exploit the vulnerability once an attacker has access to the target system.
- Authentication – measures the number of times an attacker must authenticate to a target to exploit the vulnerability.
- Confidentiality impact – measures the impact on confidentiality of a successfully exploited vulnerability. It could be none, partial, or complete.
- Integrity impact – measures the impact on system integrity if a vulnerability is successfully exploited. It could be none, partial or complete.
- Availability impact – measure the impact of system availability if a vulnerability is successfully exploited. It could be none, partial or complete.

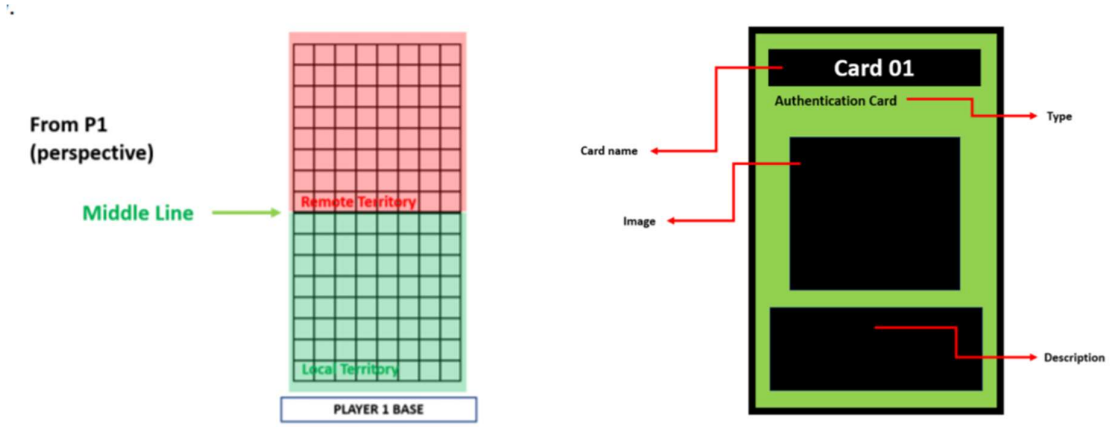


Figure 13: Project config.play (A) The game board is divided into 2 territories (B) Project config.play action card (Enriquez et al., 2018)

According to Enriquez & Kadobayashi (2018), the game also includes CVSS features that change over time such as:

- Exploitability – measures the current state of an exploit technique. It could be unproven, proof of concept, functional, and high.
- Remediation level – measures the availability of a solution to a vulnerability. It could be an official fix, temporal fix, workaround, or unavailable.

- Report confidence – measures the degree of confidence in the existence of the vulnerability and the credibility of the technical details. It could be unconfirmed, un collaborated, or confirmed.

Gameplay involves a player configuring vulnerabilities and placing blockades and treasure chests on the board to block access to the vulnerabilities. Players roll both the numbers and colours dice during their turn. The number's dice indicates the number of spaces a player can move on the board. The colour's dice indicate the colour of the action card players must draw. Players are required to attack their opponent's vulnerabilities and deplete their health gauge. The health gauge points are confidentiality, integrity, and availability. Players who manage to deplete all their opponent's 3 points win the game (Enriquez et al., 2018).

8.13 CyberCIEGE

CyberCIEGE is a role-playing simulation video game that develops security awareness in 8 cyber security topics. Players assume the role of a decision-maker within an organization tasked with the responsibility of constructing and configuring a network. They are required to use the available resources to construct this network and make security decisions e.g. user background checks, procedural security, user training, computer OS, computer configuration, type of network, physical access, alarms, and locks. Players are required to maintain a balance between productivity and security while making these decisions. Their decision should minimize risks while ensuring network goals are achieved. They also get to experience the consequences of their decisions (Aladawy et al., 2018; Le Compte et al., 2015; Cone et al., 2006).

The CyberCIEGE game introduces players to the following security awareness topics (Cone et al., 2006):

- Introduction to security awareness – where players are introduced to security awareness definitions. The game also describes to players important cyber security elements and their interactions.
- Information value – where players are required to protect high-value information within their virtual organization. They are also required to answer questions regarding information communication.
- Access control mechanism – where players are introduced to optional and compulsory network access control mechanisms.

- Social engineering – the game presents players with scenarios that result in social engineering attacks if the player does not deploy the necessary countermeasures.
- Password management – where players are required to prevent a game character from revealing their password to an unknown outside entity.
- Malware and safe computing – where players are required to invest their resources in buying software that will prevent malware from infecting and spreading within the network.
- Safeguarding data – where players are required to mitigate a scenario where a malicious insider tries to leave the organizational premises with sensitive data.
- Physical security mechanisms – where players are required to implement physical security mechanisms that prevent outsiders from gaining unauthorized access.

CyberCIEGE architecture consists of a simulation engine, domain-specific scenario definition language, scenario development, and video-enhanced encyclopedia. The scenario definition language communicates different scenarios using risk management tradeoffs. The simulation engine displays different simulations based on the scenario definition language. The scenario definition language defines gameplay and gameplay consequences. All the topics feature in the game's scenarios and the objective of players is to raise the organization's security posture. The game engine trigger attacks when a player fails to complete set objectives within a given time. After completion of an objective, the game provides players with a security awareness message that explains the real-life consequences of their actions. A player wins by completing their objective without experiencing major penalties (Cone et al., 2006).

The game is not based on a player's actual environment therefore the security lessons learned are not easily transferable to the player's real-world environment. The scenarios generated by the game's simulation engine are limited and lack diversity (Le Compte et al., 2015).

8.14 Network nightmares

Network nightmares is a video game in which players are computer crackers looking for vulnerabilities in a network to exploit. The network setup and security issues are represented by graphical images as shown in figure 14 below. The network setup includes network nodes represented by a ring, connections represented by lines joining the ring, hubs represented by rings connected to multiple rings, ports

represented by separate network connected by a lock, a virus is represented by a hazardous material symbol, infection represented by red instead of blue lines and a network administrator in charge of the network. Players attempt to launch viruses into the network by shooting at targeted nodes (Ryan et al., 2013).

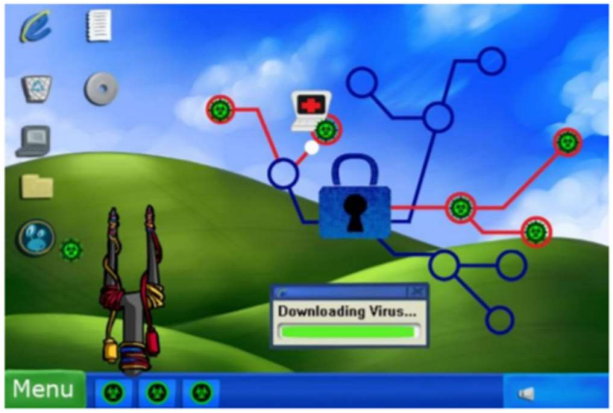


Figure 14: Game screen showing virus being aimed and launched towards the network (Ryan et al., 2013)

Gameplay requires players to aim and hit nodes with viruses as shown in figure 14 above. Players have 3 viruses that can be launched into the network, their virus arsenal is replenished each time they hit and infect a node within the network. The network administrator tries to heal the infected nodes. If a player manages to infect all nodes, they win. The goal is to inflict maximum damage to the network therefore players aim to infect network hubs, ports, and nodes farthest away from the network administrator (Ryan et al., 2013).

By aiming viruses at network hubs players learn that viruses leverage network structures to maximize damage. Hubs are connected to many other nodes in the network and attackers usually target nodes with the maximum number of connections to maximize the spread of viruses. By aiming viruses at ports players learn about port vulnerability in the spread of viruses. Ports represent channels of communication in a network and attackers usually target network ports with viruses. By aiming at nodes farthest away from the network administrator players learn about network monitoring complexities. Hidden and infrequently scanned network locations are more vulnerable to viruses (Ryan et al., 2013).

8.15 M-learning game

M-learning is a mobile application security awareness game that uses quizzes to develop player security awareness. The mobile platform allows players to learn without Internet access once the game is downloaded it is run locally. The platform also provides a flexible content delivery environment. The game uses quizzes with short interaction time to gauge players' cyber security knowledge and provides management with this assessment. The topics introduced by the game include passwords, phishing, social engineering, malware, and data protection as shown in figure 15 (A) below. Players have the responsibility of maintaining the organization's cyber security. The game's genre is survival therefore players have to avoid getting fired because of bad cyber security decisions (Filipczuk et al., 2019).

Gameplay involves scenarios being presented to players who then answer multiple-choice questions as shown in figure 15 (B) below. Each topic has multiple scenarios and questions. After answering a question the game provides players with a dialogue box that contains additional information regarding the question. The game requires players to answer all the questions on each topic. Players fail a topic if they get more than 3 answers wrong. The game displays the final score on each topic to players who can compare scores on the leaderboard. If a player fails a topic the game redirects the player to learning material relevant to the topic where they can read more about the topic. Once players have read the material, they can retake the quiz. The game logs the time taken to answer the questions, the player's score, and the learning material read by players (Filipczuk et al., 2019).

An evaluation done on the m-learning game showed the game to be (Filipczuk et al., 2019):

- User friendly – players found the game to be easy to use and navigate.
- Engaging – the game's survival genre which required the players to fight to keep their job increased players' engagement in the game.
- Increased security awareness – the game increased the security awareness knowledge of players.
- Game content and completion – the game's content was relevant to players' requirements.

8.16 An Integrated Real-Time Simulated Ethical Hacking Toolkit with Interactive Gamification Capabilities and Cyber Security Educational Platform

The game uses simulations, quizzes, and an informative website to develop security awareness amongst players. The ethical hacking toolkit provides players with an integrated real-time simulation of current real-world cyber-attacks. Players experience simulations of cyber-attacks such as screen capture, keyboard stroke capture, web camera access, microphone access, command-line injection, file transfer, and ransomware.

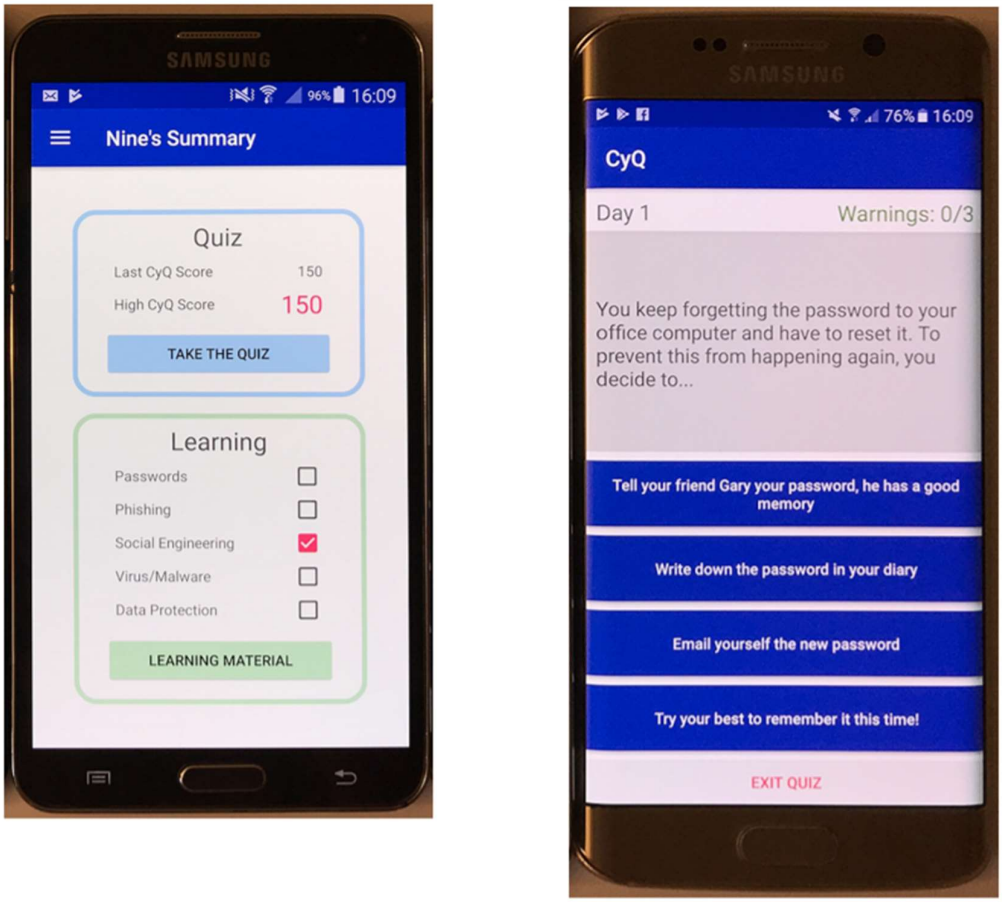


Figure 15: M-learning game screen showing (A) The game's security awareness topics (B) Sample quiz questions and multiple choice answers (Filipczuk et al., 2019)

Players also experience the effects of these attacks. Ethical hacking toolkit simulation is implemented through hacker side program, server-side program, and victim side program as shown in figure 16 below. The server-side program is a web server

program that has a public IP address. The victim side program is a malicious program that uses user datagram protocol (UDP). The hacker side program carries out attacks by sending commands to a malicious program in the victim's device (Mathoosoothenen et al., 2017).

The game uses quizzes to evaluate players' understanding of cyber security issues. The quiz presents players with several scenarios on different cyber security topics. Players are required to analyze the questions and identify the best practices to implement to prevent attacks. The quizzes are based on real-life scenarios players may experience while using the Internet. Scores are based on how well a player answers the questions. To pass the security awareness test a player is required to score 75% and above. Players can reattempt the quiz questions. Using the ethical hacking toolkit simulations players assist a fictional character in the game to identify cyber security threats and their countermeasures (Mathoosoothenen et al., 2017).

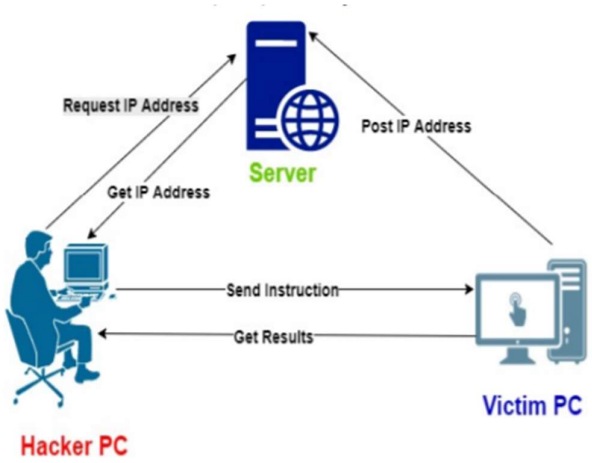


Figure 16: The game's ethical hacking toolkit architecture Mathoosoothenen et al., (2017)

The educational platform is an informative website where players learn about current cyber security threats and their countermeasures. Players conduct discussions on cyber security issues amongst themselves through the website's online forums. This promotes social norms and peer-based learning. Through the forums, players can also consult cyber security experts to clarify areas they have doubts about (Mathoosoothenen et al., 2017).

8.17 Hacked time

Hacked time is a desktop game that uses puzzles, role-playing, interactive narrative, and tower defence to elicit behavioural change in players. The elements that constitute security awareness are skill development, risk awareness, and guided practice. Security awareness games tend to focus on one of these elements. The link between theory, game design practices, and the player behavioural outcome is also not clear in most games. Therefore the games are unable to provide players with meaningful and complete security awareness that can impact their behaviour (Chen et al., 2020).

Hacked time games seek to increase play self-efficacy. Self-efficacy is a player's belief to execute behaviour necessary to produce specific goals which is the first step towards behaviour change. The 4 self-efficacy principles mapped into Hacked time game's design are (Chen et al., 2020; Chen et al., 2019):

- Communicate risk information – this principle increases players' knowledge of cyber security risks. Hacked time design includes game characters that elicit a player's empathy to effectively communicate the risk. The game's design also includes player interaction with a friend to make risks more relatable and observable to the player.
- Skill development – this principle translates players' concerns into preventative action and helps players develop skills to mitigate risks. The game's design includes hidden objects that allow a player to interact with the environment and diagnose threats. A smartwatch consultant in the game design provides players with information to mitigate threats. The time energy in the game's design allows a player to reflect on the lessons learned and how these lessons can be implemented.
- Skill enhancement and application – players are guided to practice cyber security skills in the real world with this principle. The game's design includes mock tools which players implement to gain implementation experience and practice their skills.
- Social support – this principle enlists social support for the player to encourage cyber security behavioural change.

Gameplay involves players taking the role of a time-travelling detective who helps their student friend to deal with a security breach. The game is relatable since a player is

helping a friend. At the beginning of the game, the student informs the player of a security breach they experienced and the consequence of this breach. This information is given to players in the form of a story. The story provides players with risk information and the consequences of risky behaviour. Assisting the friend after a data breach includes searching the friend's visual environment for clues of cyber security risks as shown in figure 17 (A). These clues help players solve the genesis of the data breach puzzle. Players click on clues in the visual environment to gain useful information regarding the breach. After discovering a security risk the smartwatch informs the friend on how to mitigate this risk (Chen et al., 2020; Chen et al., 2019).

To advance in the game player selects different dialogue options to give the friend advice as shown in figure 17 (B). The smartwatch provides feedback on the appropriateness of the players' advice to the friend. The game's story branches according to the player selected dialogue option. By providing useful advice to the friend players acquire time energy. The more useful the advice the more time energy players receive. This exercise develops players' risk identification and mitigation skills. On acquiring enough time energy players can travel back in time to before the data breach. After the time travel players can choose security precautions for the friend to implement to prevent the data breach as shown in figure 17 (C). Players then travel to the present day to see the effects of their security precautions. Time travel allows players to apply the lessons learned throughout the game (Chen et al., 2020; Chen et al., 2019).

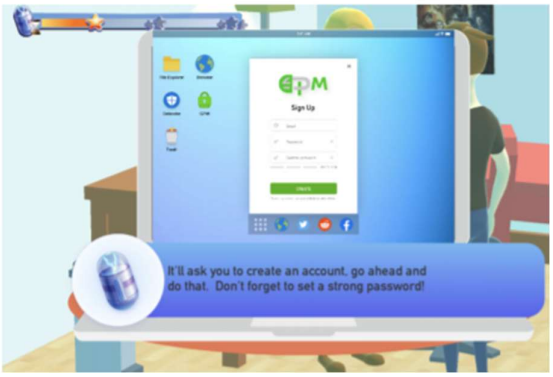


Figure 17: Game screen showing (A) Player searching environment for clues (B) Player advising the student about security (C) Player giving guided security practice after time travel (Chen et al., 2020)

A quantitative evaluation carried out on the game show it is effective in increasing players' self-efficacy, response efficacy, and security awareness (Chen et al., 2020).

8.18 Cyber smart e-safety game

Cyber smart is a single-player, role-playing game in which players are responsible for securing and protecting systems. The game introduces players to various cyber security topics. Using a system administrator's computer in a lab setting players get hands-on experience in the implementation of cyber security. They use a mouse and keyboard as input devices and receive output from the game through the screen and speakers. Cyber smart deploys survival dynamics game genre where players are required to survive in their role as a system administrator (Underhay et al., 2016).

Gameplay involves players taking the role of a system administrator responsible for network security. The game provides players with information to analyze and act upon while playing this role. Players are required to use this information to perform actions geared towards securing the network and network devices. They are also required to implement best practices within the network to protect the network. Players' actions to the information given affect the state of the game. If a player's actions fail to protect the network the game is lost (Underhay et al., 2016).

8.19 Cyber Security-Requirements Awareness Game (CSRAG)

Cyber Security Requirements Awareness Game (CSRAG) is a board game that includes role-playing, solving puzzles, and cards. Players are divided into teams of 3-

4 people that compete against each other. The game elements implemented in the game include badges, fantasy, challenges, clear goals, and limited resources. The game board is based on an organization's floor plan which has different assets to be protected. The board tiles have rooms and security personnel as shown in figure 18 below. Inside the rooms are assets such as spies, undercover agents, and devices represented by cards. Spies represent insider threats within the organization, undercover agents represent the organization's security personnel, and the devices represent organizational equipment vulnerable to attacks. CSRAG introduces players to social engineering, network, and physical security cyber security topics. The game's story at the beginning introduces the organization, its network systems, and players to their roles. Included in the story are threats faced by the organization (Yasin et al., 2018).

Gameplay involves players taking the role of ethical hackers. Players are divided into teams with each player having different roles within the team e.g. network attacker, social engineering attacker, and physical attacker. They plan which room to attack and the path along the board to get to this room. Players move on the board by the roll of a dice, if they land on board tile with security personnel, they lose a life. To access a room players have to solve a puzzle that mimics real-life situations where attackers have to guess a password. Inside the room, players need to randomly select an asset they suspect of being a spy. If the random selection is a spy players are directed to the device they need to infect otherwise players lose a life (Yasin et al., 2018).

Players are required to devise attack strategies to infect the device using the device description card. The card describes the device's position within the organization and its vulnerabilities. Players write hypothetical attack scenarios once they have devised an attack strategy on a device. Teams discuss and exchange ideas on their various attack strategies. After these discussions teams refine their attack strategies based on the consensus. An empirical evaluation of the game shows increased engagement and participation amongst players. The game also increases player security

awareness (Yasin et al., 2018).

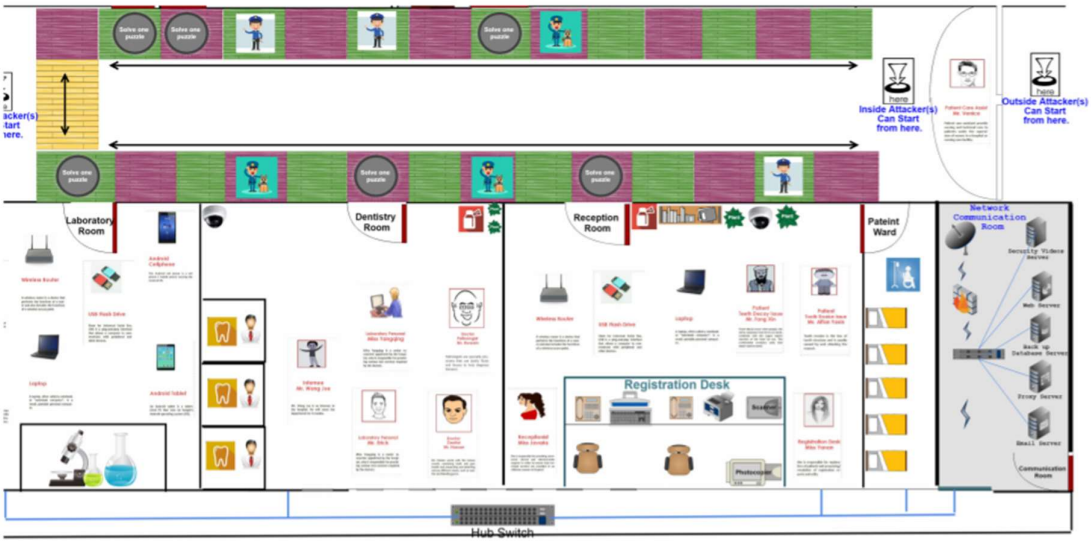


Figure 18: Cyber Security Requirements Awareness Game floor plan map (Yasin et al., 2018)

8.20 Secu-one

Games such as capture the flag are focused on enhancing a player's security awareness technical capacity. Other games tend to focus on building incident response and system development security awareness amongst players. Secu-one a 3 – 6 player security awareness card game aimed at equipping players with knowledge and skills in system operation management. The game is turn-based and has 1 game master. The game develops players' knowledge and skills in asset, operational, system development, vulnerability, incident, human, and physical security management. It seeks to increase player knowledge on cyber security terms, their characteristics, and their countermeasures. The game also develops players' skills in risk analysis, incident handling, and assessment of the validity of countermeasures. The game models cyber security activities within an organization e.g. log monitoring, vulnerability assessment, security awareness, incident response, and security settings. The game's attack cards list the latest cyber-attack methods. The game's defence cards list cyber-attacks countermeasures. These cyber-attack methods and countermeasures are obtained from attack libraries (Omiya & Kadobayashi 2019).

Gameplay involves the use of one deck of attack cards and another deck of defence cards. A player draws a random attack card and other players are supposed to draw

from their handheld card defence cards they consider appropriate for the attack card as shown in figure 19 below. The first player with an idea of the appropriate defence card draws the card. Players are required to justify why their drawn defence card is appropriate and earn points if the other players agree with their explanation. If players cannot agree on the appropriateness of a defence card the game master gives the final verdict. Failure to submit a defence card results in a player losing points as indicated on the attack card. Failure by a player to explain the appropriateness of a defence card results in the player missing the next turn. Each player records their points during each turn and the winner is the player with the most points. The attack cards set used vary in difficulty depending on players' knowledge and skills levels (Omiya & Kadobayashi 2019).

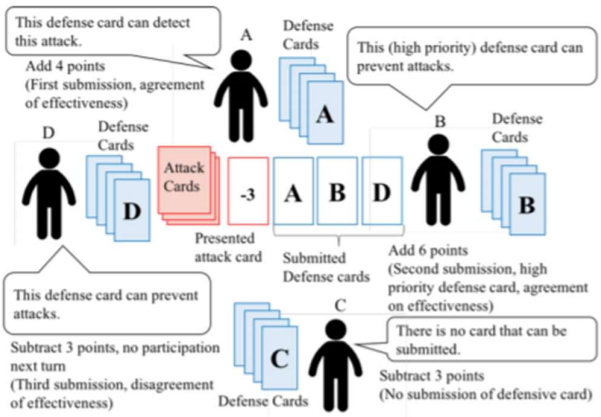


Figure 19: Secu-One game play round (Omiya & Kadobayashi 2019)

An evaluation of Secu-one shows the game to be effective in increasing players' cyber security knowledge. Players also found the game to be fun and increased their motivation during security awareness (Omiya & Kadobayashi 2019).

8.21 Cyber Agents' Interactive modelling and simulation (CyberAIMs)

CyberAIMs is a cyber warfare game that uses adversarial thinking to develop player security awareness. Adversarial thinking encourages players to think like attackers resulting in players always considering potential attackers' actions. The game focuses on the socio-technical attributes of cyber security. The game uses a simulation modelling program to simulate different socio-technical attributes of cyber security. The simulator gives weights to different socio-technical attributes such as resources, skills, and motivation. The resource attribute is classified as a technical component

and includes cyber security methods, money allocated, and devices deployed. The motivation attribute is classified as a socio component and includes skills, cyber security awareness level, incentives, and literacy (Zoto et al., 2018).

Gameplay involves players defining the number of agents on the attack and defence sides. Agents represent users on each side of the warfare game. Players also define the initial attribute values for each agent on the attack and defence sides. The simulator uses the player-defined agent attribute values to predict the attack side and defence side behaviour. If an attack is successful, defence side agents lose resources attribute, and agents on the attack side gain the lost resources attribute. A successful attack also results in both the attack and defence side agents gaining skill attributes. Skills attributes are gained by both sides because they both learn from an attack experience. However, the defence side agents gain more skill attribute compared to the attack side. A successful attack also results in the attack side agents gaining motivation attributes. An unsuccessful attack results in loss of motivation attribute on the attack side agents and motivation attribute gains on the defence side agents. Successive successful attacks result in the complete draining of the defence side's agents' resource attribute resulting in the agent going offline and being unable to communicate with other agents (Zoto et al., 2018).

8.22 Internet Hero

Internet hero is a video game targeted at children to assist them safely navigate the Internet. The game deploys the fiction game genre and aims to increase players' digital literacy. Players are transported into a fictional Internet world with 4 characters ping, dot net, dot com, and dot evl. Dot evl is a villain character intent on taking over the Internet. Players are heroes tasked with the responsibility of helping ping solve 4 mini-games challenges related to Internet usage. The game introduces players to emails, malicious programs, social networks, and Internet connections (Bauer et al., 2013).

The gameplay presents players with different scenarios. In the first scenario players meets ping who works in a mail server room. Players are required to assist ping to distinguish between legitimate and spam mail. Legitimate mail is forwarded, and spam mail is discarded as shown in figure 20 (A) and (B) below. A player reads incoming mail and categorizes them as either spam or legitimate. Correct categorization of two or more emails results in bonus rewards for players. During the categorization of

emails, players are required to be attentive to emails from unfamiliar senders, emails with winning notifications, emails with suspicious links, and attachments. In the second scenario, players accompany ping to the hospital because ping is sick from virus infection. The USB doctor explains different types of viruses and methods of preventing the virus from weakening ping. Thereafter players are required to build a defence tower to protect ping from further virus infection as shown in figure 20 (C) below. The defence tower includes walls illustrating firewalls to stop viruses, shooters illustrating anti-virus to shoot down viruses, and scanners illustrating intrusion detection to identify trojan viruses. Players experience ten attack waves and each time players kill a virus they gain currency which they use to upgrade their defence tower. If an attack is success ping's health decreases. Consecutive successful attacks result in ping's death. Players learn the importance of anti-virus, firewall, scanners in virus detection and prevention.

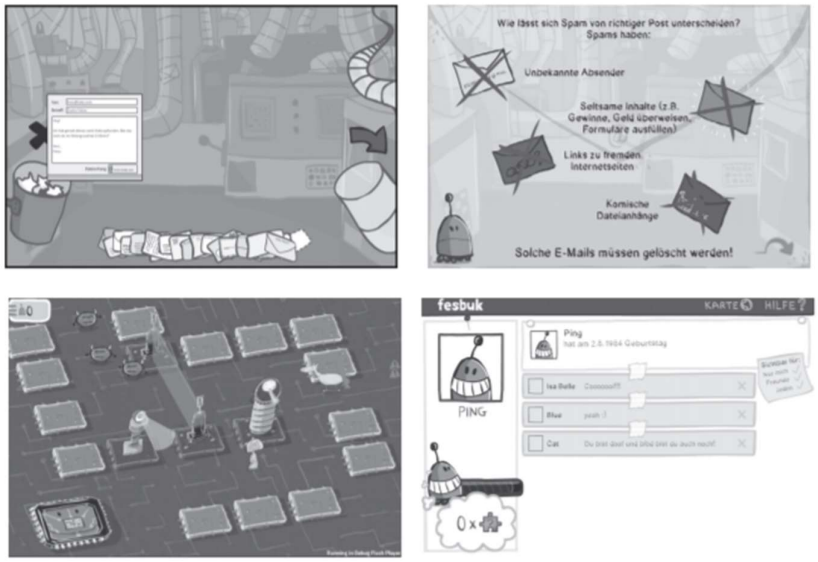


Figure 20: Game screen showing (A) E-mail mini-game (B) Explaining the difference between legitimate and illegitimate email (C) Tower defence game (D) Social network security settings (Bauer et al., 2013)

The third scenario continues with ping at home using social networks as he recovers from the virus. Messages, pictures, and status updates can be posted on this social network as shown in figure 20 (D) above. Ping's social network has cyberbullying, and players are required to manage ping's social network security by selecting the appropriate security settings. For each correct security setting, players get a puzzle

which when solved identifies the bully and results in the disappearance of the bully's post. Players learn the importance of restricting access to social networks. In the final scenario the player and ping want to inform dot net and dot com about dot evl, but dot evl is intent on intercepting this message. The player's task is to win a race to safely deliver ping through the various Internet connection i.e. wired and wireless to dot net and dot com without being intercepted by dot evl. During the delivery of ping, players encounter packet collisions which slow them down. They also encounter speed boosts which speed them up. Players win if they successfully deliver ping to dot net and dot com. From this players learn about the different Internet connections (Bauer et al., 2013).

An evaluation of the game shows that players found the game to be fun and increased security awareness (Bauer et al., 2013).

8.23 Educational games for cyber security

Educational games for cyber security comprise 5 mini-games that deploy trivia, matching, shooting, and runner game genres to develop security awareness. The games introduce players to safe usage of laptops, social networks, malware, and smart Internet usage (Sookhanaphibarn & Choensawat 2020).

- The laptop security game is a story about a spy with a mission to keep a notebook stolen from a villain safe, as the spy tries to decode the secret data it contains. Players take the role of the spy as shown in figure 21 (A) below. Gameplay involves questions, items search, and a chase. Players are required to answer questions that determine how the game proceeds. Item search requires players to explore the game environment for items which when found result in the game proceeding. The chase involves players evading capture by the villain (Sookhanaphibarn & Choensawat 2020).
- The social network game simulates a social network site with features such as like, comment, add, and follow friend as shown in figure 21 (B) below. The simulator generates friends for the player. Gameplay involves players making decisions on friends to add and posts to like. These decisions determine the player's score. The game also has an animation video to educate players on the best social network practices (Sookhanaphibarn & Choensawat 2020).

- Cyber defender game introduces players to virus and malware security using a shooting game. The game story is based on a malicious alien army intent on destroying the earth with their spaceship. Players are required to shoot down the attacking spaceship. Game sessions are limited to 3 minutes, during which the spaceship attacks are endless. Gameplay involves players loading bullets and shooting at the approaching spaceship. The bullets have text which describes a certain type of malware. The incoming spaceship has text with the name of malware as shown in figure 21 (C) below. To shoot down the spaceship players are required to match the malware description in the bullet with the malware name in the spaceship. Each successful shot is recorded in the player's score, failure to shoot down the spaceship results in the earth being destroyed (Sookhanaphibarn & Choensawat 2020).
- Quiz tank game introduces players to smart computer usage. The game story is based on an alien attack and a tank responsible for protecting Earth as shown in figure 21 (D) below. Gameplay involves players controlling the tank to protect the earth by shooting at aliens and answering questions thereafter. The questions have multiple correct answers with varying degrees of harmfulness or usefulness. Players are required to answer these questions and receive scores based on their answers. The varying degree of harmfulness or usefulness of an answer is reflected in the player's score (Sookhanaphibarn & Choensawat 2020).
- Cyber runner introduces players to smart use of the Internet to avoid cybercrime. The game story is based on a robot that spends time running on a platform in a computer city. The gameplay involves the robot running through computer city collecting items while avoiding obstacles as shown in figure 21 (E) below. When the robot collects four items the game asks players questions. Players have energy levels that decrease when the robot hits an obstacle or runs without collecting items. The game ends when the robot runs out of energy or falls from the platform (Sookhanaphibarn & Choensawat 2020).

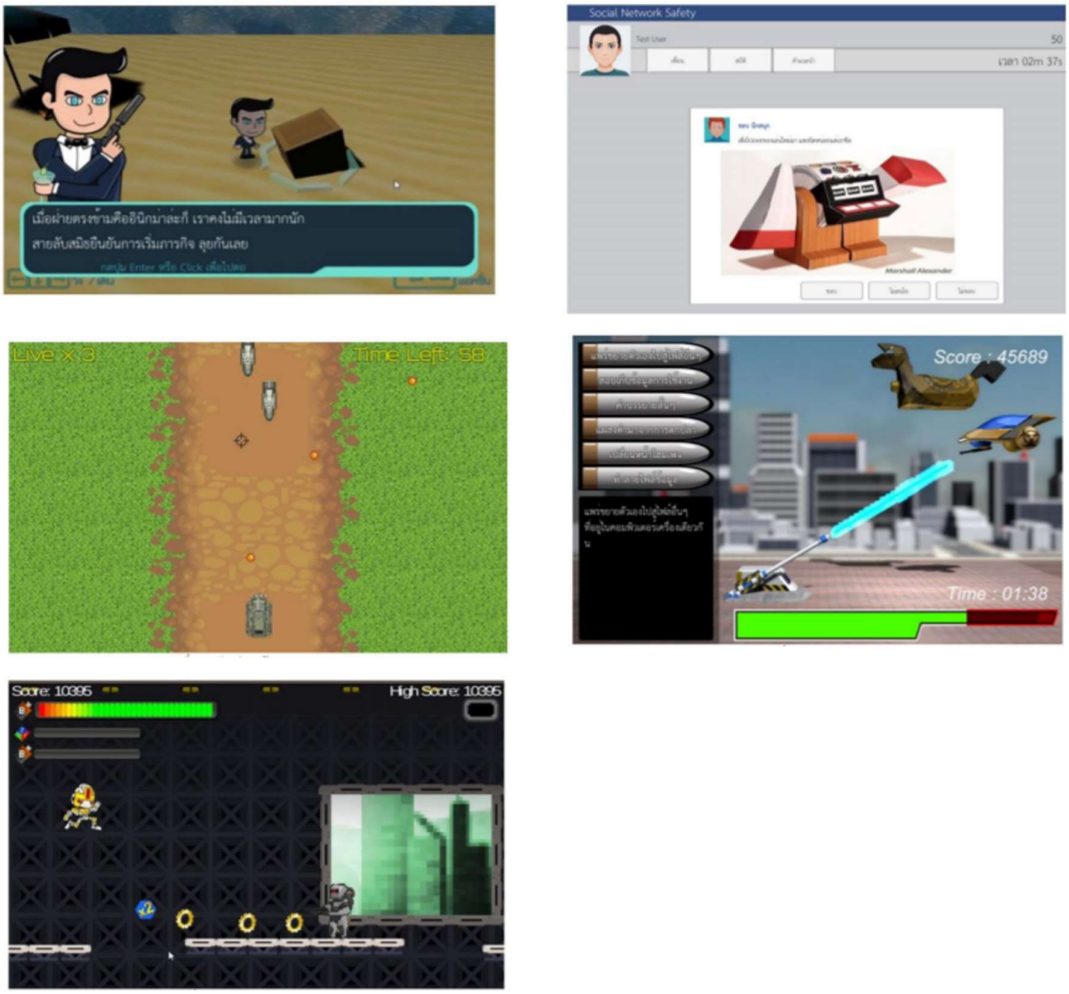


Figure 21: Game screen showing (A) Spy laptop game (B) Social network game (C) Quiz tank game (D) Cyber defender game (E) Cyber runner (Sookhanaphibarn & Choensawat 2020)

An evaluation of the game shows increased knowledge amongst players. Players also found the game easy to use and useful in security awareness (Sookhanaphibarn & Choensawat 2020).

8.24 Escape room game

The escape room game is played by 3-5 people and develops security awareness by using a realistic imitation of a player's workplace environment. A game session lasts between 15-30 minutes. Players' knowledge and deficiencies are tested by the game. To develop a realistic escape room game for players, their security awareness requirements need to be collected. Devices used by the player and the policy the player operates under need to be identified. The player's physical work environment

is recreated together with escape room characters and scenarios. The escape room also requires the player's office equipment, internet connection, a computer with target files, a webcam, and a supervisor (Oroszi 2019).

The game introduces players to the following security awareness topics (Oroszi 2019):

- A clean desk and screen policy that ensures all sensitive or confidential material is removed from a player's workspace and locked when not in use.
- Secure use and storage of workplace badges, keys, proximity cards, and office equipment that enhance physical security.
- Use of strong and secure passwords and PIN codes.
- Secure usage of mobile devices.
- Appropriate security settings for application and secure use of applications.
- Encryption of communication and devices.
- Secure use of social networks and appropriate information sharing within social networks.
- Shredding of documents to discourage dumpster diving.

Before the game, players are required to register. Players are also introduced to the game's story and goals. A supervisor observes the game and keeps time. Photos and videos are taken during the game and used during the game's postmortem analysis. Gameplay involves players taking the role of an attacker with access to a computer. Players are required to log onto the computer and access specific files. An evaluation of the game shows the game is effective in increasing security awareness amongst players. The game is also entertaining and fun (Oroszi 2019).

8.25 Security Empire

Security Empire is a multi-player game that develops fundamental cyber security concepts amongst players. Players are introduced to social engineering, cryptography, software authentication, software upgrade, anti-virus software, and password protection. Security empire's game story is goal-driven in which players are required to build a green empire by collecting 6 components required to build an energy system. Players interact with other players in the game's marketplace to auction and trade-in components required to build an energy system (Olano et al., 2014).

Gameplay involves players taking the role of a green technology company owner responsible for managing the company's systems. In this role, players are required to manage the company's budget including its cyber security budget. From the game's security centre players can purchase security solutions for their company. The centre also provides players with useful cyber security threats information, good cyber security practices, available security solutions, and their characteristics. These solutions have different prices according to their characteristics. Players utilize different security solutions as they build their green empire and are required to wisely spend their budget. From this exercise, players gain knowledge about cyber security threats, their countermeasures, and the tradeoffs made while buying security solutions (Olano et al., 2014).

The security solutions assist players in buying and selling components needed to build the green empire. Buying and selling of components are done in competition with other players. When a player buys 6 components, they can build an energy system. Trading of components is fast-paced, and players are required to be on the lookout for fraudulent marketplace offers akin to social engineering. Players are required to encrypt their bids for components during auctions, to avoid eavesdropping from competitors. Unencrypted bidding by a player can result in competitors outbidding the player for components akin to encryption of communication to avoid eavesdropping. Players are also required to maintain and upgrade their software systems to maintain a competitive advantage over their competitors. A player's software could break down due to lack of maintenance resulting in costly repairs and delays. From this players gain knowledge about security incidences and their consequences (Olano et al., 2014).

An evaluation of the game shows that players found the game engaging (Olano et al., 2014).

8.26 Cyber VR

Cyber VR is a first-person virtual reality video game that introduces players to data privacy, malicious code injection, software patch management, software analysis, access privileges, and cryptography. Players use a headset to see objects in a 3D virtual environment and hand gestures which are tracked to directly interact with objects in the virtual environment as shown in figure 22 (A) below. The game story is

based on a post-apocalyptic world where players take the role of an IT technician. Players are tasked with the responsibility of securing the IT systems of a building shown in figure 22 (B) below. They get help in securing the systems from an invisible administrator. A tutorial at the beginning of the game helps players learn how to use hand gestures to move and interact with objects (Veneruso et al., 2020).

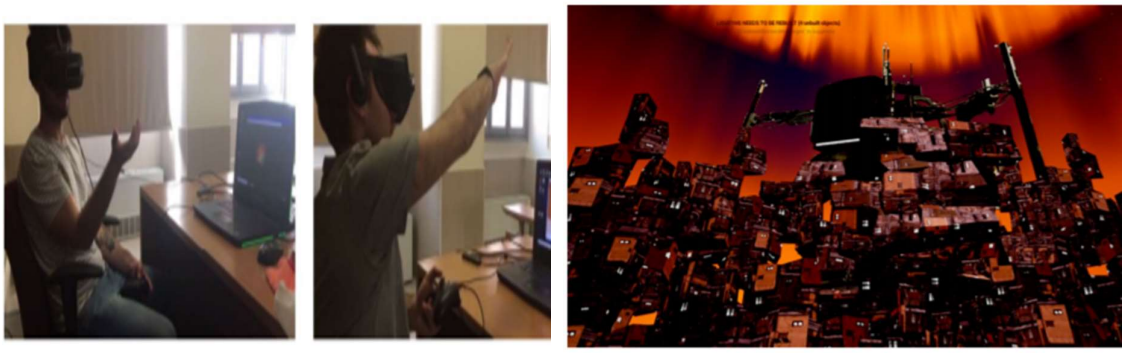


Figure 22: (A) A player using virtual reality equipment to play the game (B) Game screen of the building with IT system the player is required to protect (Veneruso et al., 2020)

Gameplay consists of 6 mini-games that can be played in any order. Each mini-game develops security awareness on one topic (Veneruso et al., 2020):

- In the information flow, mini-game players scan packets represented by cubes and classify them as sensitive or public as shown in figure 23 (A) below. This classification is done according to the data contained within these packets. Once players have identified the type of packet, they redirect the packet to the correct stream i.e. either sensitive or public. Each correct classification of packets earns players a score.
- The code injection mini-game uses a board to represent source code. Players a required to search the board for malicious pieces as shown in figure 23 (B) below. Once a player identifies a malicious piece of the board, they are required to destroy this piece.
- The patch management mini-game represents a piece of software as a cube shown in figure 23 (C) below. Players are required to scan each layer of the cube and apply the correct patch on them.
- The dynamic software analysis mini-game observes software behaviour during runtime. Players are required to run some code in this mini-game and notice

security issues in the code represented by protruding orange poles as shown in figure 23 (D) below. Each pole is labelled with an issue name. Players are required to decide whether to address or reject the named software issue.

- The privilege escalation mini-game requires players to scan the IT system for users with root privileges. Players are required to decide whether a user's root privilege is legitimate or not. After making the decision players are required to remove illegitimate root privileges users as shown in figure 23 (E) below.
- The public key cryptography mini-game has two characters Alice and Bob that want to exchange secure messages. Players are required to implement public-key cryptography to ensure secure message transfer between Alice and Bob as shown in figure 23 (F) below.

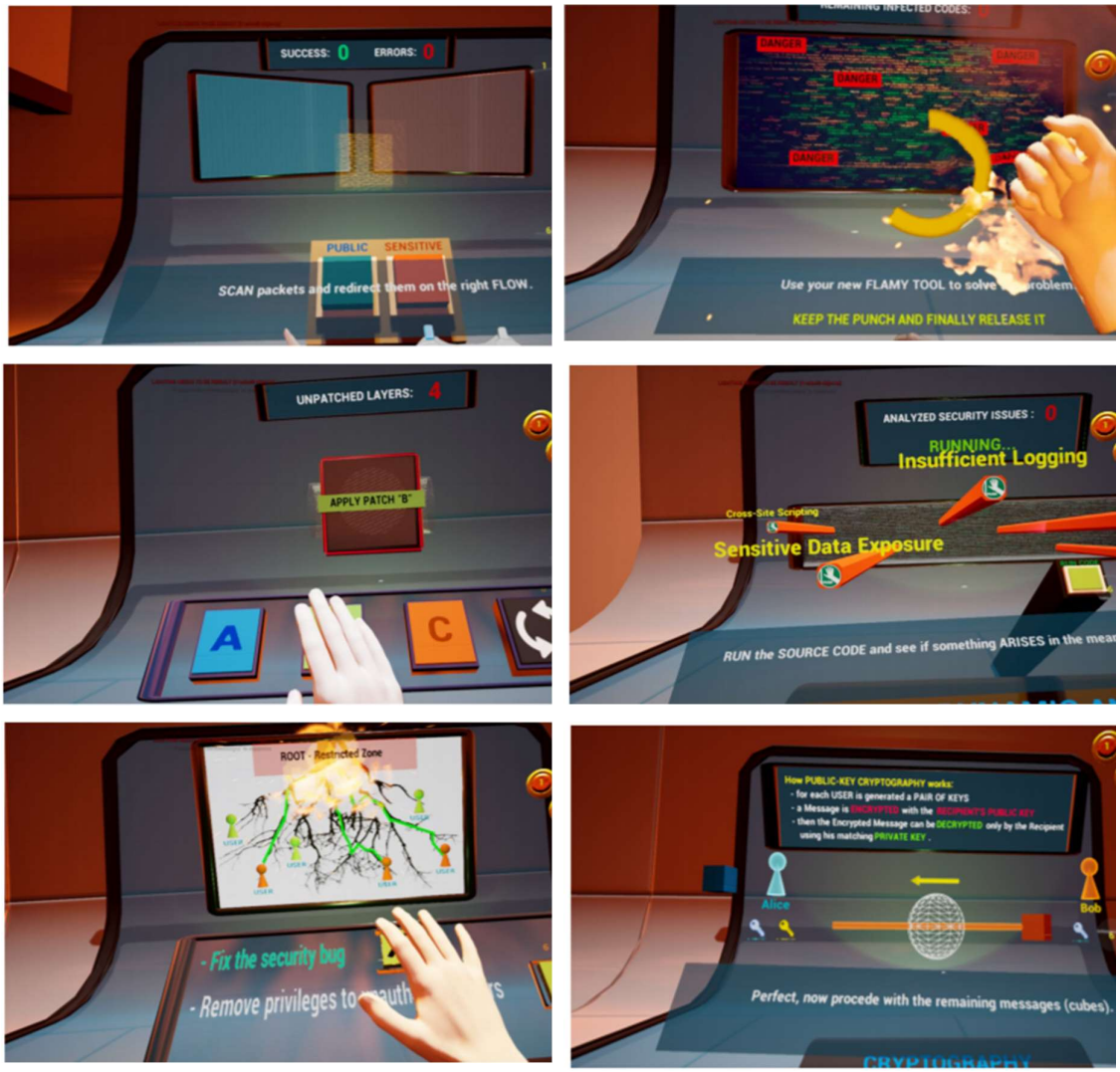


Figure 23: Game screen showing (A) Information flow mini-game (B) Code injection mini-game (C) Patch management mini-game (D) Dynamic software analysis mini-game (E) Privilege escalation mini-game (F) Public-key cryptography mini-game (Veneruso et al., 2020)

On completion of one mini-game players earn a coin once a player achieves 6 coins, they can unlock the database of threats. Players can then update the threats database with the knowledge obtained from each mini-game. A study conducted on the game shows that players found the game engaging and effective in security awareness (Veneruso et al., 2020).

8.27 CybAR

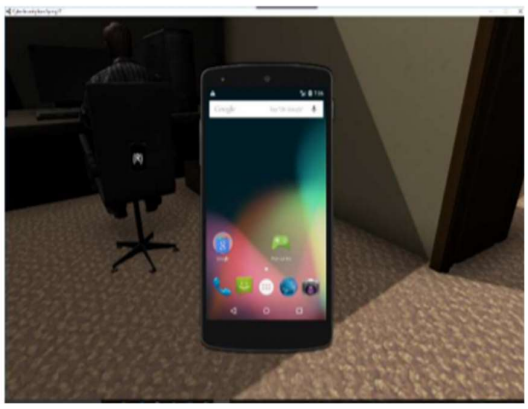
CybAR is an android platform mobile application game. Mobile application games provide an easy avenue of disseminating security awareness knowledge to players in a world with fast-emerging cyber security threats. The game implements role-playing and quiz game genres. CybAR game uses augmented reality and develops players' security awareness using technology threat avoidance theory (TTAT). TTAT seeks to influence players' motivation and behaviour by altering players' threat perception. Threat avoidance motivation is affected by a perceived threat, safeguard effectiveness, safeguard cost, self-efficacy, perceived severity, and perceived susceptibility. Individual differences such as demography, personality, risk, and decision-making affect threat avoidance behaviour. The game's interactivity and presentation of consequences of careless security behaviour can change a player's behaviour (Alqahtani & Thorne 2020).

Gameplay involves providing players with a sequence of tasks based on scenarios. Players are required to select the right option in each scenario. The game uses protection motivation theory (PMT) to trigger positive security behaviour amongst the players after each task. The game triggers positive behaviour by giving players coping messages after each successful implementation of a task. Coping messages alert players to the fact that cyber-attack risks are minimized by selecting the right options. When players select the wrong option in a scenario, the game gives players fear messages. Fear messages warn players of vulnerabilities associated with the bad options selected (Alqahtani & Thorne 2020).

8.28 3D virtual reality (VR) game

3D VR game consisting of 4 modules that develop players knowledge and skills in various topics (Jin et al., 2018). The 4 game modules are:

- 3D social engineering game – this module is implemented using 3D animation of characters. The game's genre is role-playing and it simulates an office environment. The game introduces players to social engineering techniques such as tailgating, piggybacking, and mantrap. Players interact with the game characters in simulation scenarios. During these simulation scenarios, players are required to select the appropriate action in each scenario as shown in figure 24 (A) below (Jin et al., 2018).
- 3D secure online behaviour game – this module of the game is implemented using 3D technology. The game either simulates a high school computer lab or bedroom environment as shown in figure 24 (B) below. The game introduces players to phishing emails, secure and insecure web links, phoney phone calls, and personal information protection. Players are required to correctly handle emails, weblinks, and phone calls on various devices such as computers, laptops, cell phones, and networked game consoles (Jin et al., 2018).



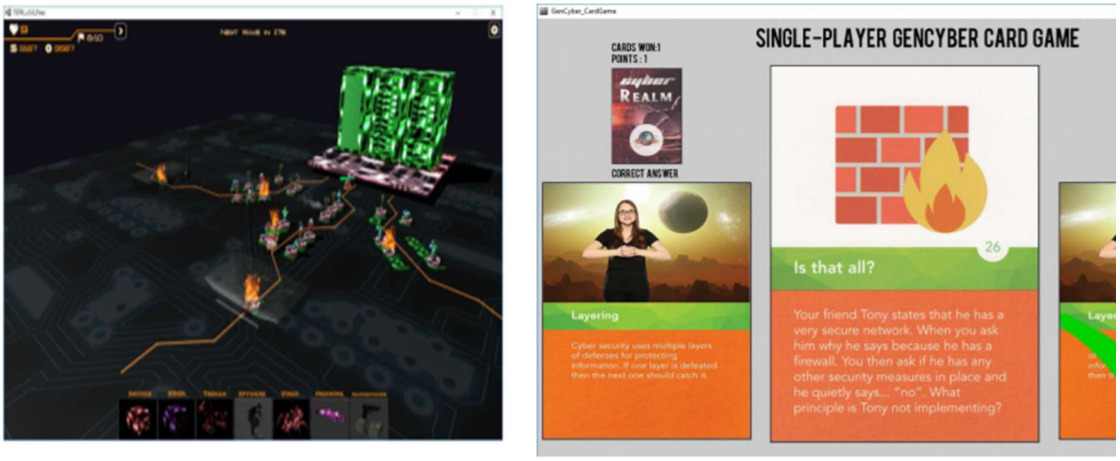


Figure 24: Game screen showing (A) Social engineering game (B) Secure online behaviour game (C) Defence tower game (D) 2D single-player card game (Jin et al., 2018)

- 3D cyber defence tower game – this module requires players to defend their virtual computer server from waves of attacks by placing correct defensive measures along the path of attack as shown in figure 24 (C) above. The virtual server is faced with attacks such as viruses, phishing, trojan, spyware, ransomware, DDoS, and sniffers. The defence measures available to the virtual server include anti-virus, password, system update, encryption, firewall, and secure cyber behaviour. As the game advances the frequency of attacks increase and the attack combination varies making defence of the virtual server more challenging (Jin et al., 2018).
- 2D GenCyber Card Game – this module is a card game that introduces players to 10 cyber security principles. The physical card game is played by 2 players face to face and the computer card game is played by 1 player. Gameplay involves drawing a card from the card deck which has a question as shown in figure 24 (D) above. Players are required to draw a card at hand that answers the question (Jin et al., 2018).

8.29 CyberNEXS

CyberNEXS is a security awareness platform implemented on a client-server architecture. The architecture has different operation models and gaming is implemented on the competition model. The game introduces players to cyber defence, penetration testing, and cyber forensics skills (Nagarajan et al., 2012). The 5 gaming modes in CyberNEXS are:

- CyberNEXS-CDN (Computer Network Defence Centralized) – is a cyber defence game where the blue team is responsible for ensuring network security and availability against the red team's attack. The blue team is also required to detect network attacks by the red team and deploy countermeasures against these attacks. At the end of the game, the blue team reports their finding to the white team i.e. administrator (Nagarajan et al., 2012).
- CyberNEXS-CDN Lite – is similar to CyberNEXS-CDN although, in this game, the blue team is not required to detect and deploy countermeasures against red team attacks (Nagarajan et al., 2012).
- CyberNEXS-Forensic – given cyber forensic challenges to players. Players are required to discover evidence of intrusion, find malware, analyze packet payload, and track attackers based on network logs. At the end of the game, players report their findings to the white team (Nagarajan et al., 2012).
- CyberNEXS-CNA (Computer Network Attack) – requires players to look for vulnerabilities in the network and exploit these vulnerabilities. Players exploit these vulnerabilities to get administrative control of the network. Players are required to report their successful network access exploits to the white team (Nagarajan et al., 2012).
- CyberNEXS-CTF – requires players to look for network vulnerabilities and exploit them to access and control some hosts in the network. Once hosts are under a player's control the player is required to defend these hosts against attacks while ensuring the host's critical services remain available (Nagarajan et al., 2012).

8.30 Capture the Flag (CTF)

Capture the Flag (CTF) game provides players with access to a virtual network containing virtual servers as shown in figure 25 below. The game's genre is capture the flag and quiz. Quizzes develop players' knowledge of cyber security terminology. CTF enables players to apply their skills in exploiting vulnerabilities and defending networks. The game introduces players to network configuration, network vulnerabilities, passwords, privilege escalation, phishing, and network snooping (Leune & Petrilli 2017).

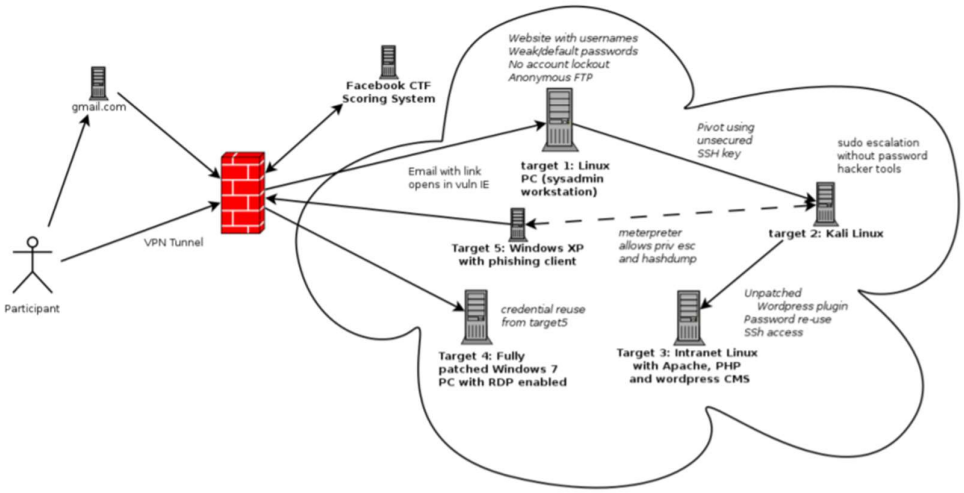


Figure 25: Virtual network showing servers and PC that contain flags (Leune & Petrilli 2017)

Gameplay consists of quizzes, CTF scavenger hunt, and CTF king of the castle game module. Players work in teams on each of the modules. In the quiz module players answers questions. Players score points for every correct answer to a quiz question. In the CTF scavenger hunt game module, players are required to gain access to a network and access the file that contains the flag by exploiting network vulnerabilities. Players score points for each flag collected and are required to document their activities. They are also required to provide recommendations on countermeasures to harden the network against their exploits. In the CTF king of the castle game module players are required to defend a network's server against attacks. Players score points for successfully defending a server and the scores are posted on a Facebook CTF scoring system (Leune & Petrilli 2017).

An evaluation of the game shows increased self confidence amongst players in their abilities to exploit network vulnerabilities and defend the network against attacks. Players also developed practical skills and found the game to be engaging and enjoyable (Leune & Petrilli 2017).

8.31 Class Capture the Flag (CCTF)

Capture the Flag (CTF) games require extensive preparation, coding skills, and security knowledge. This may discourage beginners from participating in CTF

competitions. Class Capture the Flag (CCTF) is a game that seeks to support and engage beginners of CTF competition. The small scope of the game offered in a classroom setting provides beginners with hands-on CTF experience. CCTF is implemented on a testbed accessible via a browser. Players are organized into teams with similar skills and play alternate offensive and defensive roles in different scenarios. CCTF introduces players to cryptography, intrusion, denial of service, and domain name system (Mirkovic et al., 2015).

The gameplay involves the blue team defending the server against various cyber-attacks deployed by the red team. Teams receive scores according to how successful they are at defending or deploying attacks against the server. After each CCTF session, there is a postmortem analysis done led by an instructor. During this session, players discuss and learn about their failures and successes. Successful teams share their strategies with other teams. After the postmortem analysis team conduct another CCTF session where the teams implement the recommendations discussed. Several iterations of CCTF sessions are conducted to enable teams to apply all the lessons learned from previous sessions (Mirkovic et al., 2015).

Players can assess their performance under stress during CCTF sessions. Players can also benchmark their performance against competitors, therefore, determining their operational security skills. An evaluation conducted on the game shows improved security awareness skills amongst the players. Players also found the game to be engaging (Mirkovic et al., 2015).

8.32 Hardware CTF

Capture the Flag games focus on application layer security and often neglect hardware-level security. Hardware-level security forms the basis for cyber security, all other layers are compromised if the hardware level is compromised. Hardware CTF game is designed to provide players with hardware security awareness. The game can either be implemented on digital hardware design representation, physical hardware devices, or an electronic design automation tool. The game requires players to use their hardware knowledge to identify, mitigate and exploit hardware vulnerabilities to capture a flag. Players are organized in teams while participating in the game modules. Hardware CTF game consists of a training module, jeopardy competition module, attack, and defence competition modules (Prinetto et al., 2020).

Gameplay begins with training where players are introduced to hardware security concepts. The game and its mechanics are also introduced to the players during training. The game's jeopardy module requires teams to exploit hardware vulnerabilities to capture a hidden flag. Teams do not compete against each other in this module. The challenge for the teams in this module is to simply capture the flag. The attack and defence module require teams to first play defence. Teams do this by identifying and fixing hardware vulnerabilities to prevent other teams from accessing their flag. Thereafter teams play offensive by probing their opponent hardware for unfixed vulnerabilities as they try to capture their flags. Teams score points for capturing opponents' flags and successfully defending their flags (Prinetto et al., 2020).

The game introduces players to cyber security topics in the following manner (Prinetto et al., 2020).

- Hardware Trojans are inserted on digital hardware and players are required to identify and exploit the trojan to capture the flag.
- Unprotected test infrastructure where players can capture the flag by exploiting the hardware's test infrastructure.
- Undocumented functions and features where players are provided with hardware documentation missing some features. Capturing the flag can only occur by players exploiting the missing feature's vulnerability.
- Design bugs and flaws where players have hardware with design flaws that result in vulnerabilities. Players are required to exploit these vulnerabilities to capture the flag.
- Side-channel attacks where players are given hardware vulnerable to side-channel attacks. Players are required to perform side-channel attacks to capture the flag.
- Weak implementation of hardware-based security module where the hardware has some security vulnerabilities. Players exploit this security vulnerability to get the flag.