A serious game to promote information security awareness by utilising simulated experiences among the youth

CC Croucamp

 **orcid.org 0009-0002-6421-422X**

Dissertation accepted in fulfilment of the requirements for the degree *Master of Science in Computer Science* at the North-West University

Supervisor: Prof GR Drevin

Co-supervisor: Prof L Drevin

Graduation: July 2025

Acknowledgements

I would like to express my sincere gratitude to everyone who has helped and guided me along the way of finishing my thesis. Your belief in me, your knowledge, and your support, have been priceless.

Above all, I owe a great deal to Prof. Gunther Drevin and Prof. Lynette Drevin for their outstanding direction, tolerance, and invaluable insights. Their knowledge and their mentoring have been invaluable in guiding my research; I truly value their help throughout this academic process and my academic career that has grown out of the time spent working with them.

Japie Spoelstra Snr. deserves particular gratitude, since his inspiration and mentoring has significantly shaped my academic development and altered my life path. I am truly grateful for all your help and guidance and your support and knowledge inspire me to go beyond my own expectations.

I also would like to thank Hester Spoelstra for opening her heart and home. Always making sure I was healthy and ready to take on the next day. Elmien, Japie Jnr, and Corlene Spoelstra thank you for your friendship and encouragement. I truly value these connections and realise that without them it would not have been possible to be where I am.

I also really appreciate my family and friends. Maliza Smit, I appreciate your constant support, patience, and belief in me throughout the course of this journey. To my parents, Chrissie Botha and Duane Botha; your love, direction, and relentless encouragement have been priceless.

Finally, thank you to everyone who has helped me both personally and academically, either directly or indirectly. I shall always be grateful for your help and your belief and confidence in me, as these have made this journey possible.

Abstract

Information security has emerged as a critical concern, particularly for the youth who are immersed in technology from a young age. The increasing prevalence of cyber threats and the need for effective awareness of information security among the youth have highlighted the limitations of traditional training methods. However, there is a pressing need to rethink the approach to information security education and awareness, moving beyond passive learning to more interactive and immersive experiences. The aim of this research is to develop and implement a serious game called "Cyber Cadet: Threat Defender" using simulated experiences to promote information security awareness. The Design Science Research Process was used to guide the development of the game. The study provides a comprehensive background on the current landscape of information security education, the identified challenges, and the potential benefits of adopting a serious game-based approach. A scoping literature review on information security awareness among the youth was performed. The results showed that serious games have the potential to provide hands-on training, improve security awareness, and foster the development of critical thinking and problem solving skills. The game was tested and evaluated by parents, teachers, and industry experts in order to provide feedback on the effectiveness of the game to promote cyber security awareness among the youth.

Keywords: Information security; Awareness; Simulated experience; Serious game

Contents

List of Figures

List of Tables

Table of abbreviations

A table containing a list of abbreviations that will be used throughout the text.

AES	Advanced Encryption Standard
APT	Advanced Persistent Threats
CIA	Confidentiality, Integrity and Availability
CSRF	Cross-Site Request Forgery
DDoS	Distributed Denial of Service
DoS	Denial of Service
DSRP	Design Science Research Process
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
MFA	Multi-Factor Authentication
MitM	Man-in-the-Middle
PII	Personally Identifiable Information
POPI Act	Protection of Personal Information Act
RAID	Redundant Array of Independent Disks
RBAC	Role-based Access Control
RSA	Rivest–Shamir–Adleman
SETA	Security Education, Training and Awareness
SIEM	Security Information and Event Management
TCP	Transmission Control Protocol
TEE	Trusted Execution Environment
TTP	Tactics, Techniques, and Procedures
XSS	Cross-Site Scripting

Chapter 1

Introduction

As the digital era continues to evolve, information security has emerged as a critical concern, particularly for the youth who are immersed in technology from a young age. Traditional training methods, such as phishing awareness campaigns, training videos, and assessments, have been shown to be less effective at engaging and educating this audience over time (Sendjaja et al., 2024). There is a pressing need to rethink the approach to information security education and awareness, moving beyond passive learning to more interactive and immersive experiences (Scherb et al., 2023).

Serious games have been identified as a promising approach to address this challenge. These games offer the opportunity to simulate real-world information security scenarios, allowing participants to engage with and learn from simulated experiences. By incorporating gamification elements, serious games have the potential to captivate and motivate the youth audience, fostering a deeper understanding of information security concepts and promoting sustainable behavioural change (Gáliková et al., 2021; Hart et al., 2021).

In this research, the aim is to develop and implement a serious game called "Cyber Cadet: Threat Defender" designed to promote awareness of information security among the youth. The study will provide a comprehensive background on the current landscape of information security education, the identified challenges, and the potential benefits of adopting a serious game-based approach.

The chapter begins with a basic background that will form the foundation upon which the study is built. This section is then followed by the problem statement, research question, and aims and objectives that identify the gap on which this study

is focused and what requirements are necessary for the research to be successful. The methodology is then discussed, and the chapter ends with an overview of the chapters found in this dissertation.

1.1 Background

The exponential growth and widespread adoption of digital technologies have revolutionised the way the youth interact with information and interact with online environments. Although this digital transformation has brought numerous advantages, it has also exposed the youth to a number of information security threats, ranging from phishing attacks and malware infections to data breaches and identity theft.

Organisations and educational institutions have launched several training courses and awareness initiatives to address this growing challenge. But since they are passive and lack the immersive and interactive components that today's youth want (Scherb et al., 2023), these conventional approaches sometimes fail to adequately educate and include the youth. However, serious games present a unique opportunity to close the gap between good awareness initiatives and immersive experiences. While still keeping the lure and intrigue aspects of classic games, these games are aimed primarily at education, training, and the raising of awareness. Serious games can offer hands-on training, raise information security awareness, and help to develop critical thinking and problem-solving ability by modelling real-world information security problems.

Studies have indicated that in the context of information security education, serious games can be rather successful (Gáliková et al., 2021). Since players in these interactive and dynamic games actively participate in the learning process, they might subsequently better grasp and remember the information security principles. Previous studies have shown that major games have the ability to affect player decisions on information security issues, emphasising the need for more research in this field (Hart et al., 2021; Jaffray et al., 2021).

Building on this foundation, the proposed solution looks at the development and implementation of a serious game designed to promote awareness of information security among the youth using simulated experiences (Micallef and Arachchilage, 2017).

1.2 Overview of the problem

The increasing prevalence of cyber threats and the need for effective awareness of information security among the youth have highlighted the limitations of traditional training methods. Although there are many serious games for information security education, they often follow a similar approach of showcasing the effects of a cyber attack on the system of an individual or an organisation (Hart et al., 2021; Micallef and Arachchilage, 2017; Scherb et al., 2023). However, it is necessary to explore the design and implementation of a serious game that goes beyond this traditional approach and focusses on immersing youth in simulated experiences to improve their understanding and participation in the concepts of information security.

To address this gap, the goal of this research is to develop and evaluate a serious game that uses simulated experiences to promote awareness of information security among the youth. Simulated experiences are an effective method of learning through experience (Francia et al., 2014).

In order to design the simulated experiences in the game, a detailed understanding of the various threats experienced by users is necessary. Examples of these threats are as follows:

Privacy attacks are designed to breach the security of a system's data and collect sensitive information covertly. Unlike attacks that aim to harm or compromise the integrity of a system, these attacks are considered passive in nature, as they blend into the system to collect data discreetly (Padmavathi and Shanmugapriya, 2009).

Denial-of-Service attack occurs when an attacker overwhelms a target system or network with an excessive volume of connection attempts or data requests. This exceeds the capacity of the targeted service, which makes it unable to respond to legitimate user requests. The traffic onslaught can cause the server to crash or completely stop operating (Whitman and Mattord, 2022).

Back door attacks are when malicious actors gain unauthorised access to a system or network by exploiting well-known or recently discovered entry points. Developers occasionally create these backdoor access points for their own needs, which are then left unresolved when the product is released. These covert entry points can be used to further compromise the system or introduce harmful malware that impacts the system or network (Whitman and Mattord, 2022).

Malware attacks or malicious software is intentionally developed to cause harm.

Its purposes can range from infiltrating and disrupting a system to manipulating a browser to display advertisements (Whitman and Mattord, 2022).

Password attacks are considered acts of espionage or unauthorised access, since the malicious party is trying to obtain data that do not belong to them. Cracking, the process of trying to decipher or guess a password, encompasses various techniques that can be employed for this purpose (Whitman and Mattord, 2022).

Phishing is a technique that uses various deceptive methods to persuade users to disclose private information, compromise online accounts, systems, or other individual/corporate IT resources. These attacks are commonly perpetrated through emails to target users unaware of the associated risks. Phishing has become one of the most prevalent forms of cyber crime (Whitman and Mattord, 2022).

The following two are not considered threats in the same context as the previous threats, but require a mention as they focus on human interactions that have a large impact on incidents as they are exploited in the threats already discussed.

The human aspect of information security is a significant vulnerability, as unaware individuals often fall prey to various attempts to gain access to personal or organisational data. Lack of fundamental knowledge about information security poses a critical risk within the current information security landscape (Sabillon, 2021).

Social engineering is the manipulation of a person to take an action that may or may not be in their best interest (Hadnagy, 2018).

These security incidents are prevalent across various forms of cybercrime and remain a significant challenge as our world becomes increasingly digitised. In addition, cybercriminals have taken advantage of the continuous development of new technologies and tools to expand their capabilities. One such recent advancement is the use of artificial intelligence as a means for cybercriminals to orchestrate attacks on a larger scale (Shetty et al., 2024; Truong et al., 2020). Due to the expansion of criminal capabilities, the need for better and more effective awareness education will continue to increase. This leads to the research question discussed in the following section.

1.3 Research question

A serious game, "Cyber Cadet: Threat Defender" that incorporates simulated experiences designed to promote information security awareness through experience will be created. In this dissertation, the related literature, design aspects, and evaluation elements will be discussed and examined, specifically the effectiveness of the approach. The research attempts to answer the following question:

How can a serious game utilising simulated experiences promote information security awareness among the youth?

The following secondary research questions will be also investigated:

- What were the methods used in recent cyber attacks?
- What simulated experience methods exist?
- What game design principles exist, and how can these principles be incorporated into a serious game?

To answer these questions an artefact will be designed and given to two groups of testers. The first is a pilot group to evaluate the first iteration of the game, to allow changes and corrections to be made to the game. Secondly, the game will be presented to parents, teachers, and industry experts, to test and evaluate the effectiveness of the games in educating the youth.

A detailed literature study will be conducted on topics such as information security, serious games, and simulated experiences. These topics will be researched to obtain a deeper understanding of the connection between them.

1.4 Aim and objectives

The aim of the study is to create a serious game that promotes information security awareness by incorporating simulated experiences into the game. The objectives of the study, which are needed to achieve the aim, are as follows:

- To obtain an understanding of recent cyber attacks;

- To obtain an understanding of existing simulated experiences and how they can be implemented;
- To obtain an understanding of existing game design principles and how to incorporate the principles into a serious game;
- To deliver a serious game utilising simulated experiences to promote information security awareness; and
- To evaluate the serious game by having parents, teachers, and experts in the field of information security and gaming play the game and provide feedback.

1.5 Methodology

In this dissertation, the Design Science Research (DSR) methodology is used. This methodology emphasises the creation and evaluation of artefacts designed to solve identified problems. It is particularly relevant in the field of Information Systems (IS) research, where it serves as a framework for developing innovative solutions that address real-world challenges. The DSR methodology is characterised by its focus on producing prescriptive knowledge through the design and evaluation of artefacts such as models, frameworks, and processes (Ylijoki et al., 2018).

The DSR process typically follows a structured approach that includes several key steps. According to Peffers et al. (2007), the DSR methodology consists of six steps:

1. Problem identification and motivation;
2. Definition of the objectives for a solution;
3. Design and development;
4. Demonstration;
5. Evaluation; and
6. Communication.

This structured approach ensures that the research is systematic and that the resulting artefacts are rigorously evaluated for their effectiveness and utility. The evaluation phase is particularly important as it assesses the quality and efficacy of the designed artefacts, ensuring that they meet the intended objectives.

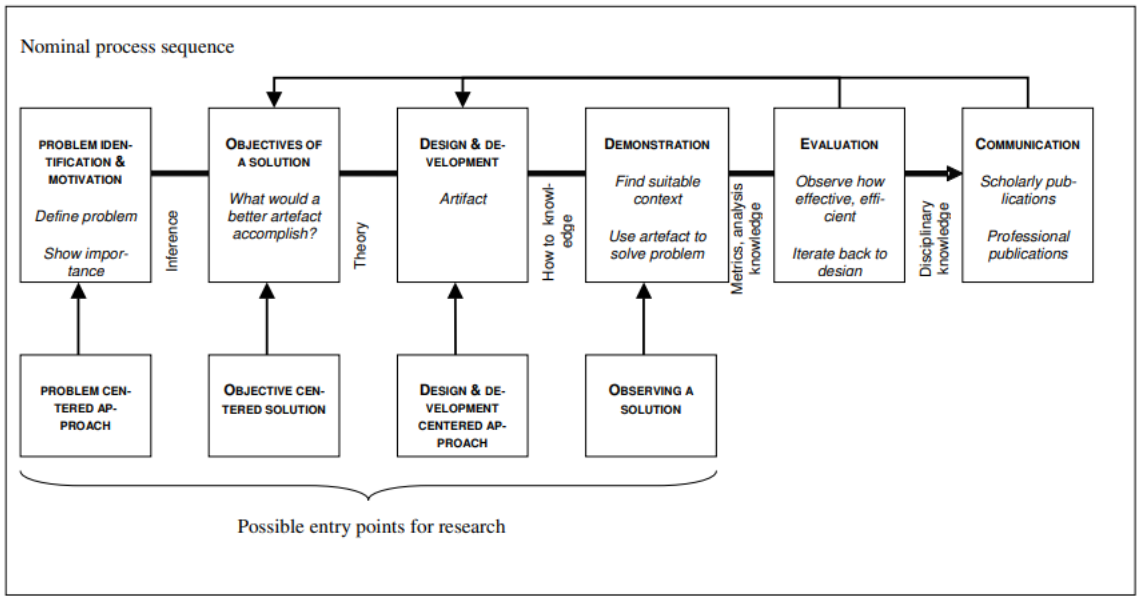


Figure 1.1: Design Science Research Process (DSRP) model by Peffers et al. (2007)

This methodology fits the nature of this research as an artefact will be created to educate a selected group of people on the importance of having information security awareness. The six steps referred to by Peffers et al. (2007) will be used to identify a problem, define objectives, design the game "Cyber Cadet: Threat Defender", demonstrate and evaluate the artefact using parents, teachers, and industry experts, and document and communicate the final findings. Figure 1.1 shows the process associated with DSR.

Using this methodology as the basis of this research, the following process will be followed:

- **Phase 1 (Problem identification and motivation):** This phase involves conducting a literature review to identify the research problem and establish the motivation for the study, presented in Chapter 1.
- **Phase 2 (Definition of objectives for a solution):** This phase defines the objectives of the proposed solution by evaluating existing research (Chapters 2, 3, and 4) to determine whether a serious game that incorporates simulated experiences can effectively improve information security awareness among the youth.
- **Phase 3 (Design and development):** Using a game engine, a game will be developed that incorporates the understanding obtained with regard to cyber attacks, simulated experiences, and principles of serious games. These three

aspects will then be introduced and combined to create a serious game that promotes information security awareness among the youth. (Chapter 5)

- **Phases 4 and 5 (Demonstration and Evaluation):** Parents, teachers, experts in security, and users from the gaming community will play the game and review the effectiveness of the product. These reviews will be captured and processed to be used in the communication phase. (Chapter 6)
- **Phase 6 (Communication):** This phase focuses on communicating the final findings, incorporating reviewer feedback, and documenting the conclusions. The findings of this phase will be presented in Chapter 7.

1.6 Ethical considerations

Ethical considerations represent pivotal components of all research endeavours. To ensure compliance with the relevant ethical standards, an ethics clearance request was submitted and subsequently approved, documented under the ethics number NWU-01435-23-A9. The approval document can be found in Appendix F. The ethical considerations relevant to this investigation include informed consent, anonymity, and confidentiality, as well as the rigour and integrity of the process and data.

To ensure informed consent, prospective participants received an invitation explaining the objective of the project: Improving information security awareness through an educational game and subsequently acquiring information via a questionnaire found in Appendix E. The invitation emphasised that participation was entirely voluntary, that no remuneration was provided, and that participants was free to withdraw from the study at any juncture without consequence. This transparent communication ensured that the participants fully understood the rationale for their participation in the study and how their participation would contribute to the overarching goals of increasing information security awareness among the youth.

To protect anonymity and confidentiality, all acquired information, including both gameplay data and questionnaire responses, was anonymised and securely stored. The data was used exclusively for research purposes and was not be disseminated beyond the confines of this scholarly pursuit. The protection of the identities of the participants by maintaining confidentiality further upholds ethical standards by respecting individual privacy.

To ensure the rigour and integrity of the process and data, the necessary mea-

sures were enacted to ensure that the data, once obtained, remained unchanged and faithfully represented. The conclusions derived from the research were based on the analysis of the evidence collected, thus strengthening the credibility of the study results. The focus on precise data management and honest reporting illustrates a strong commitment to academic integrity.

These ethical considerations are imperative and were consistently adhered to throughout the research process to preserve the study's integrity.

1.7 Chapter overview

In Chapter 2 the fundamental concepts of information security are discussed using the literature to provide a solid foundation on which to build the remainder of this study.

Chapter 3 focuses on the literature related to serious games and how to effectively integrate the core elements associated with serious game design.

In Chapter 4 a literature review on simulated experiences is done detailing what a simulated experience is and how to effectively create a serious game that incorporates the aspects.

In Chapter 5 the design process of "Cyber Cadet: Threat Defender" is detailed, examining each challenge created and the methods used to implement them.

In Chapter 6, the demonstration and evaluation processes for "Cyber Cadet: Threat Defender" is explained. This involves presenting the game to parents, teachers, security experts, and members of the gaming community, collecting their feedback, and analysing the results to assess the effectiveness of the game. These findings will then inform the subsequent communication phase.

Finally, in Chapter 7 conclusions are drawn,the research objectives are revisited, recommendation are presented and an overview of possible future work is provided.

Chapter 2

Information security

Information security is a critical discipline that aims to protect information from unauthorised access, use, disclosure, disruption, modification, or destruction (Andreassen et al., 1988). In today's digital age, where information is an asset for individuals and organisations alike, the importance of securing this information cannot be overstated (Waddington, 1995). In this chapter, the fundamentals of information security will be explored, delving into the threats and vulnerabilities faced by the youth, the current state of youth awareness and strategies necessary to mitigate these risks.

Section 2.1 explores the fundamentals of information security, establishing a strong foundation for the discussion. Section 2.2 examines human factors in information security, highlighting the role individuals play in maintaining security. In section 2.3, the threats and vulnerabilities that affect the youth are analysed, followed by Section 2.4, which reviews the current state of information awareness and educational programmes available to young people. Finally, Section 2.5 provides a summary of the chapter.

2.1 Fundamentals of information security

The fundamentals of information security are critical in understanding how to protect information effectively (Caballero, 2013). In this section, insights from key texts in the field will be used to outline the primary principles and practices in information security.

2.1.1 Core principles of information security

As described in "Principles of Information Security" by Whitman and Mattord (2022), information security is based on three core principles: confidentiality, integrity, and availability (CIA). These principles form the CIA triad, a model designed to guide information security policies within an organisation. With these principles creating the foundation of information security, they can be defined as follows (Whitman and Mattord, 2022):

- **Confidentiality**: Guarantees that only those with permission can access sensitive information.
- **Integrity**: Ensures the accuracy and reliability of the data.
- **Availability**: Guarantees that, when needed, information is available to authorised users.

Whitman and Mattord (2022) also expand on these core principles by adding to the model:

- **Accuracy**: Guarantees that all data are error-free and that the value is as expected.
- **Authenticity**: Guarantees that information is authentic rather than fake.
- **Utility**: Ensures that the user can use the data and that pertinent information is shown, rather than unsorted data.
- **Possession**: Ensures that the data belong to the legitimate owner.

The illustration in Figure 2.1 depicts the expanded CIA triad, further delving into the concept that security is like an onion that has various layers to ensure effective security practices. Understanding these core principles is essential to understanding how information security awareness can be approached.

2.1.2 Key practices in information security

Looking at the growing technological environment and understanding the core principles required for information security, these key practices have been identified

Figure 2.1: Expanded CIA triad based on Whitman and Mattord (2022)

to promote information security. A structured security approach, including security policies, processes, procedures, and organisational structures, is essential to effectively protect information resources (Arbanas and Hrustek, 2019). To further promote a culture of information security awareness among employees, an organisation should internalise information security policies and align them with compliance standards, ensuring compliance with required security practices (Park and Chai, 2018). Some of these key practices that should be addressed are discussed next.

Strong authentication and access control

By requiring more than just a password to gain access to a system, strong authentication increases security by using multiple factors to verify a user's identity. Biometrics, such as fingerprint or facial recognition, are popular strong authentication methods that provide high security levels and simplicity (Bhargav-Spantzel et al., 2006). Biometric identification and smart cards have also been used to improve user authentication in a variety of systems, such as wireless communications and mobile phones (He et al., 2011; Lu et al., 2015).

Access control is the other aspect that is required to be implemented to ensure information security. Access control consists of mechanisms that limit user access to resources and ensure that users can only carry out authorised operations within a system (Yang et al., 2023). An approach to large-scale access control is role-based access control (RBAC), which assigns access to information according to the clearance level of the individual (Ferraiolo et al., 2001).

Modern security frameworks must include strong authentication and access control, with a variety of technologies and techniques used to ensure safe and approved access

to systems and resources.

Regular software updates

Software systems must undergo regular updates to remain stable, secure, and functional. Updates are required to resolve security flaws, correct bugs, improve functionality, and provide new features (Hof and Carle, 2017). Users tend to ignore critical updates, not understanding the importance of regular updates or the threats associated with not updating (Fagan et al., 2015).

For software systems to remain functional and secure and to perform well, regular software upgrades are essential.

Encryption

A crucial concept in computer science and information security is encryption. This is the process of transforming data from plaintext to ciphertext in order to prevent illegal access or interception. Various encryption techniques and algorithms have been developed to ensure data confidentiality and integrity.

The process of encrypting and decrypting data requires cryptographic keys. The Advanced Encryption Standard (AES) and other symmetric encryption algorithms employ the same key for both encryption and decryption. Rivest–Shamir–Adleman (RSA) and other asymmetric encryption methods use a set of public and private keys (Whitman and Mattord, 2022).

These encryption methods are essential to protecting data, by encrypting the information even if unauthorised access has been gained without the key, the data can not be accessed. Encryption is a cornerstone of modern information security, encompassing various techniques and algorithms to safeguard data confidentiality and integrity.

Data backup and recovery

Data backup and recovery are essential processes that aim to protect data against loss and ensure its restoration in case of any mishap. Backup involves creating copies of data to prevent permanent loss, while recovery focuses on restoring the data to their original state after a loss event (Minhas et al., 2013). Maintaining the availability and integrity of the data depends on how these two processes interact (Deka and Barua, 2010).

Data backup and recovery are essential parts of data management plans that guarantee the availability, resilience, and integrity of data. Organisations can improve their overall data security capabilities and reduce the risks associated with data loss

by using cutting-edge technologies and implementing efficient backup plans.

Incident response planning

In the realm of information security, incident response planning is essential to maintain an organisation's information security strategy. It involves systematic methods and procedures set up to efficiently manage different security issues, cyberthreats, and data breaches (Suleman and Liaquat, 2022). Incident response planning is essential for ensuring business continuity by enabling a rapid and adequate response to security incidents (Imamverdiyev, 2018). Preparation, detection, containment, eradication, recovery, and feedback for future preparation are the usual six stages of this strategy (Grispos et al., 2017).

Incident response planning in information security is a multifaceted process that involves proactive preparation, organised response techniques, automation, collaboration, and integration with digital forensics readiness strategies. By implementing robust incident response plans, organisations can effectively mitigate the impact of security incidents and protect their critical information systems.

Network security

Network security involves protecting network systems and data from accidental or malicious threats, such as destruction, disclosure, or alteration, ensuring normal system operation and uninterrupted network services (Zhu et al., 2016). It includes protecting the hardware, software, and data of network systems to prevent unwanted access and maintain data availability, confidentiality, and integrity (Wan, 2012).

In general, network security is a multifaceted discipline that requires a combination of encryption, authentication, secure routing, intrusion detection, and prevention mechanisms to mitigate risks and safeguard sensitive information transmitted over computer networks.

Physical security

In information security, physical security refers to the protection of data through the defence of the hardware and infrastructure used for data processing, transmission, and storage. The purpose of this system is to prevent unauthorised access, damage, or theft of physical assets such as servers, data centres, and networking equipment. Providing a complete security approach includes technical security measures such as encryption, access controls, and physical security (Lombardi et al., 2020).

Regular security assessments

Information security assessments on a regular basis are crucial procedures that companies use to analyse and control threats to their systems. This should be done

regularly to ensure that the organisation is fully protected at all times. These assessments involve systematically analysing potential security risks, evaluating the impact of these risks, and implementing measures to mitigate or eliminate them (He and An, 2016).

By giving businesses insights into their security threats, empowering them to make wise decisions, and strengthening their overall security posture, regular security assessments are essential to information security management.

Policy and compliance

To protect their technology and information assets against security risks, companies must prioritise policy and compliance in the field of information security. Compliance with information security policies involves employees adhering to the rules and regulations set forth in the organisation's information security policy to improve data protection (Alassaf and Alkhalifah, 2021).

In order to effectively protect information assets within businesses, policy and compliance in information security combine to create elements that call for a complex strategy encompassing organizational culture, management support, employee attitudes, and the establishment of a compliance culture.

Security awareness training

Information security awareness training attempts to educate and encourage people to think about the significance of information security measures (Wang, 2022). It involves enhancing employee perceptions, attitudes, and motivations towards learning and maintaining appropriate behaviours related to information security (Ghazvini and Shukur, 2017). Security awareness is defined as the understanding users have about the significance of information security, their responsibilities, and their actions to exercise adequate levels of information security control to safeguard the data and networks of an organisation (Legárd, 2020).

Security Education, Training and Awareness (SETA) programmes play a vital role in increasing awareness of information systems security among individuals. With these programmes being a focus area in organisations, the working individual is exposed to the required information to have a safe cyber footprint. In later chapters, security awareness will be examined to further define the role of these youth SETA programmes.

Having a good understanding of these key practices in information security is becoming more important as security threats advance with the evolution of technology. These practices will not ensure that an organization or individual is completely safe,

but they will reduce the risk. Although being aware of the problems will lead to better security awareness, not being able to identify threats and vulnerabilities will reduce the effect that being security aware has. In the following sub-section, the theoretical underpinnings of information security will be examined.

2.1.3 Theoretical underpinnings

To clearly understand the risk involved with unsafe security practices, an individual first needs to understand what information security is and what common threats and vulnerabilities there are. In this section the following questions will be discussed:

- What are threats?
- What are vulnerabilities?
- What are attacks?

What are threats?
Information security threats encompass a wide range of risks that can compromise the confidentiality, integrity, and availability of information systems. These threats can be categorised into physical, human and system-related factors. Physical threats include risks such as unauthorised access to facilities or hardware, natural disasters, and power outages (Masrek et al., 2021). Human threats involve actions which can be both deliberate and accidental, taken by an individual that compromised information or data (Wall, 2012). System-related threats are risks such as malware, vulnerabilities, and cyber attacks (Yevseiev et al., 2021). Understanding each of these three threat categories is essential in order to develop a realistic overview of what is required to protect information.

Physical Threats: Information security concerns that directly affect the physical components of systems and infrastructure are referred to as physical threats. These dangers have the potential to cause major problems, safety risks, and operational failures. One key aspect of physical threats in information security is the deep integration of smart grid information with physical systems, which can result in network attacks affecting the security and stability of physical systems (Zhu et al., 2019). Furthermore, cyber-physical threats—like highly connected malware vectors—raise worries about operational disruptions and public safety risks (Bhusal et al., 2020). Physical threats found in Table 2.1 pose a serious threat to all security systems and should not be seen as a less important factor of security. These physical threats all

pose danger to one of the core principles and could affect confidentiality, integrity, and availability.

Table 2.1: List of physical threats and their explanations

Threat	**Explanation**
Natural Disasters	Events such as floods, power outages, or fires that can cause significant damage to infrastructure and operations.
Theft	The unauthorised taking of property or information which can result in financial loss and security breaches.
Vandalism	The intentional destruction or defacement of property which can lead to financial loss and operational disruptions.
Surveillance	Monitoring and recording of activities, often covertly, which can lead to privacy breaches and unauthorised data collection.
Power Failures	Disruptions in the electrical supply that can halt operations, cause data loss, and damage equipment.
Environmental Threats	Factors such as pollution, extreme temperatures, or hazardous materials that can impact health and safety.
Sabotage	Deliberate actions aimed at damaging or disrupting operations, often by insiders with access to critical systems.

This table summarizes various physical threats and provides brief explanations for each.

Human Threats: Information security risks posed by people include a broad range of acts and behaviours that might jeopardize the availability, confidentiality, and integrity of data and systems.These threats are becoming more widely acknowledged as major obstacles to upholding effective security measures (Xu and Guo, 2019). Most successful cyber attacks are caused by human error (Alsharif et al., 2022). The need for security awareness is critically important for individuals and organizations (Shojaifar et al., 2020).

With human threats to information security being one of the leading causes of incidents, it is very important to understand the role that the individual plays in having a safe online footprint.

System-related Threats: Can be defined as a potential threat or risk to the infrastructure of a system that targets confidentiality, integrity, or availability. Threats are commonly found in systems and affect the operation of systems. Some common threats are malware, denial of service, Man-in-the-Middle and other threats that

Table 2.2: List of human-related threats in information security

Threat	**Explanation**
Insider Threats	Malicious intent or mistakes by employees or contractors that compromise security, such as intentionally stealing data or accidentally clicking on phishing emails.
Social Engineering	Methods like phishing, spear phishing, pretexting, baiting, and tailgating that manipulate individuals into divulging confidential information or granting unauthorised access.
Human Error	Mistakes such as misconfiguring security settings, using weak passwords, or accidentally leaking data that can lead to security breaches.
Lack of Training and Awareness	Not enough education about security practices and policies, leading to vulnerabilities due to unawareness of threats and countermeasures.
Third-party Risks	Security weaknesses in other systems connected to personal systems that have vulnerabilities.
Physical Security Breaches	Unauthorised physical access, theft of devices, or dumpster diving that can compromise sensitive information and infrastructure.

This table summarizes various human-related threats in information security and provides brief explanations for each.

use software or programming vulnerabilities to disrupt or exploit a system for gain (Hadziosmanovic et al., 2012).

Table 2.3: List of system-related threats in information security

Threat	**Explanation**
Malware	Malicious software, such as viruses, worms, trojans, ransomware, and spyware, that can damage systems, steal data, or disrupt operations.
Denial of Service (DoS)	Attacks that overwhelm systems, networks, or applications with a flood of traffic, causing them to become slow or unavailable to legitimate users.
Man-in-the-Middle (MitM)	Attacks where an attacker intercepts and potentially alters communication between two parties without their knowledge.
SQL Injection	Code injection technique that exploits a vulnerability in the database layer of an application, allowing attackers to execute arbitrary SQL commands.
Cross-Site Scripting (XSS)	Injection of malicious scripts into websites that are then executed in the browsers of unsuspecting users, leading to data theft or session hijacking.
Unpatched Software	Vulnerabilities in software that remain unaddressed due to a lack of updates or patches, making systems susceptible to exploits.
Zero-Day Exploits	Attacks that target previously unknown vulnerabilities in software, for which no patches or fixes are available.
Configuration Errors	Mistakes in system or network configurations that can create security vulnerabilities, such as open ports, default passwords, or excessive permissions.
Insufficient Logging and Monitoring	Lack of proper logging and monitoring can lead to undetected breaches and delayed response to security incidents.
Advanced Persistent Threats (APT)	Prolonged and targeted cyber attacks where attackers gain and maintain access to a network to steal data over an extended period.

This table summarises various system-related threats in information security and provides brief explanations for each. (ISCAfrica, 2025; Steele, 2025)

These threats can be seen as a tool that malicious entities use to disrupt systems. It is very important to understand these threats to further protect yourself from the risk resulting from using the Internet everyday.

What are vulnerabilities?
Information Security vulnerabilities are weaknesses or flaws in a system, network, application, or process, that are exploitable by threats to impact confidentiality, integrity, and availability (Whitman and Mattord, 2022). These vulnerabilities can be found in hardware, software, organisational processes, or human behaviour (Kizza, 2013; Pouransafara and Maroop, 2013). Vulnerabilities in information are a big concern in the digital era we are in because the systems are always changing, and these new systems might provide a vulnerability to exploit by malicious entities. Some common vulnerabilities are highlighted in Table 2.4.

These vulnerabilities can be exploited by threat actors to gain access to a system, disrupt a system, or steal valuable data, and can be compared to leaving the gate open, allowing anyone who walks by to enter your property even if they were not meant to be there.

What are attacks?
This now leads to attacks that can be defined as deliberate actions taken by malicious entities to exploit vulnerabilities, gain unauthorised access, disrupt operations, steal data or cause damage to information systems and networks (Whitman and Mattord, 2022). Taking into account Table 2.5, we can clearly start to connect the attack vectors to the vulnerabilities found and the present threats.

All three factors contribute to an unsecured environment, and a clear understanding of these concepts could lead to better security awareness among individuals.

2.1.4 Data protection

Data protection is one of the main objectives of information security and involves protecting data for unauthorised access, modification, or destruction (Winkler and Danner, 1974). This can be done by using security techniques such as encryption, access control, and anonymisation (Fayayola et al., 2024). These techniques that where briefly highlighted in earlier section provide the means to protect data and by protecting the data confidentiality, integrity, availability, accuracy, authenticity, utility and possession can be ensured. Looking at each of these aspects and understanding how data protection is related can further expand a person's awareness.

- **Confidentiality:** Data protection ensures confidentiality by using encryption techniques to protect sensitive information from unwanted access. An example of an encryption technique is hardware memory encryption within

Table 2.4: List of vulnerabilities in information security

Vulnerability	**Explanation**
Bugs and Coding Errors	Flaws in software code that can be exploited by attackers, such as buffer overflows, input validation errors, and race conditions.
Unpatched Software	Failure to apply updates or patches that fix known security issues, leaving systems open to exploitation.
Configuration Issues	Incorrect settings or misconfiguration that create security holes, such as default passwords, open ports, or overly permissive access controls.
Firmware Weaknesses	Flaws in the firmware of hardware devices that can be exploited to gain control or cause malfunctions.
Physical Access	Lack of physical security measures, allowing unauthorised individuals to access hardware and potentially compromise it.
Insecure Protocols	Use of outdated or insecure communication protocols that can be intercepted or tampered with, such as HTTP instead of HTTPS.
Weak Network Segmentation	Inadequate separation of network segments, making it easier for attackers to move laterally within a network.
Open Ports	Unnecessary open ports that can be exploited to gain unauthorised access.
Weak Passwords	Use of easily guessable or weak passwords that can be cracked by attackers.
Lack of Multi-Factor Authentication (MFA)	Absence of additional authentication factors, making it easier for attackers to gain access with stolen credentials.
Privilege Escalation	Flaws that allow users to gain higher access levels than intended.
Cross-Site Scripting (XSS)	Injection of malicious scripts into web applications, affecting users who visit the compromised site.
SQL Injection	Injection of malicious SQL code into queries, allowing attackers to manipulate databases.
Cross-Site Request Forgery (CSRF)	Exploiting the trust of a web application in the user's browser, causing unauthorised actions.
Social Engineering	Techniques that exploit human behaviour to gain unauthorised access or information, such as phishing or pretexting.
Lack of Security Awareness	Insufficient training and awareness among employees regarding security best practices and threat recognition.
Insider Threats	Malicious or negligent actions by insiders, such as employees or contractors.
Inadequate Security Policies	Lack of comprehensive security policies and procedures to guide and enforce security practices.

This table summarizes various vulnerabilities in information security and provides brief explanations for each. (Fortinet, 2025)

Table 2.5: List of attacks in information security

Attack	**Explanation**
Virus	Malicious software that spreads by attaching to other programs.
Worm	A self-spreading malicious program that moves across networks.
Trojan Horse	Malicious software that pretends to be something useful to trick you into installing it.
Ransomware	Software that locks your files and demands money to unlock them.
Spyware	Software that secretly monitors and collects your personal information.
Phishing	Fake emails that try to trick you into giving away personal information.
Spear Phishing	Personalised phishing attempts targeting specific people or organizations.
Denial of Service (DoS)	Overwhelming a system with traffic to make it unavailable.
Distributed Denial of Service (DDoS)	A DoS attack from many computers at once.
Man-in-the-Middle (MitM)	Intercepting and altering communication between two parties.
SQL Injection	Injecting harmful code into a database query to access data.
Cross-Site Scripting (XSS)	Adding malicious scripts to web pages to steal information.
Brute Force	Guessing passwords until the correct one is found.
Password Cracking	Using tools to recover passwords.
Advanced Persistent Threats (APT)	Long-term, targeted attacks aimed at stealing data.
Zero-Day	Exploiting unknown software vulnerabilities before they are fixed.
Social Engineering	Tricking people into revealing confidential information.
Insider Threats	Harmful actions by trusted people within an organization.
Drive-by Download	Automatically installing malware when visiting an infected website.
Credential Stuffing	Using stolen login details to access multiple accounts.
IoT Attacks	Exploiting security flaws in smart devices.
Eavesdropping	Listening to private communications to steal information.

This table summarises various attacks in information security and provides brief explanations for each. (Fortinet, 2025; ISCAfrica, 2025)

a Trusted Execution Environment(TEE), ensuring data confidentiality (Feng et al., 2024). Cryptography is another technique that can help guarantee the confidentiality of data (Qiang et al., 2016). We use these techniques to ensure that any data are mutated to a state that cannot be used by malicious entities when gaining access to the data. This protects the individual/organization and adds an extra layer of defence. Data protection also ensures that sensitive information is accessed by only those with the right clearance.

- **Integrity:** By utilising data protection techniques we can prevent data tampering which could result in the loss of integrity. Data integrity being an important aspect of storage and network security (Ghaeb et al., 2011), the role that data protection plays is crucial to ensuring that integrity. There are various techniques, like TCP Checksum, encrypted transfers, RAID, and erasure coding, that offer integrity assurance at different levels, but these still have some drawbacks (Rynge et al., 2019). The protection of integrity is an ongoing process and as new ways of manipulating data become available, there will also have to be new ways of ensuring integrity.

- **Availability:** Data should be safeguarded against any disruption. This should ensure that data are available, no matter the circumstance. In a network there should be mechanisms to prevent, detect, and react to any denial-of-service attacks. There should be backups in place to ensure a system can be restored in cases where natural disaster has damaged the infrastructure or malicious entities have locked the system. There should always be fail safes to ensure availability (Whitman and Mattord, 2022).

- **Accuracy:** By having proper data protection methods in place, the accuracy of the data can be ensure. By ensuring data are accurate, these data can be used to make better decisions and improve organizational performance (Biasin, 2021). This accuracy of data also plays a important role in preventing misrepresentation and discrimination (Biasin, 2021). By ensuring data accuracy we can be certain the quality of decision made is better.

- **Authenticity:** is essential to ensure the integrity and originality of data. In data protection this involves verifying that data are genuine, unaltered, and originate from a known and trusted source (Johnson et al., 2001). Compromised data authenticity can lead to problems like unauthorised access, data manipulation, and a loss of trust in the data. Authenticity is important to data protection because it forms the basis of trustworthiness and reliability of data.

- **Utility:** Protecting data ensures that the data remain useful and relevant for their intended purpose (RajeshwariN and SowmyaraniC., 2016). This is a fine balancing process that is important because there needs to be optimization between privacy protection and data utility (Biswas et al., 2022), with some efforts to protect subject information leading to data that are not useful affecting research outcomes (Raturi et al., 2021). Finding methods to determine the level of data protection required while ensuring data utility is essential (BinJubier et al., 2022).

- **Possession:** The protection of data also ensures that the data that are being utilised rightfully belongs the entity using it. Recognising data ownership enables a more precise analysis of data and ensures data integrity (Tai, 2018). This is becoming more important with the growth of cloud computing, demanding attention to ensure secure data storage and management (Liu et al., 2011)

- **Compliance:** Many industries are subject to rules and regulations for protecting data such as the POPIA act introduces in South Africa. This means that organizations need to focus on building data protection capabilities that fall within these rules and regulations (Labadie and Legner, 2022). Any efforts of compliance should be focused on the most critical data (Mladinić et al., 2023). These regulations are there to form a foundation of data protection that everyone has to abide by, ensuring that the standards needed to protect the data of an individual are upheld.

- **Reputation:** With proper data protection in place an organization can protect their reputation, because an incident can have a massive impact on the public's perspective and lead to reputation damage (Cheng et al., 2017).

- **Economic Impact:** The economic impact of an incident on an organisation can be extremely expensive and could have a long term effect. For example if an incident occurs there could be problems with all the aspects discussed so far: there could be fines because of compliance problems, long term loss of clients because of reputation damage or loss of income if the data required are not available anymore.

By understanding these fundamentals, from the core principles to the importance of data protection, individuals and organisations can better prepare themselves to face various threats in the cyber environment, ensuring that their information remains secure and their systems are resilient against attacks. This foundation is critical to exploring more specific aspects of information security, such as the vulnerabilities that different demographics, especially youth, face online.

2.2 Human factors in information security

The role of a human in information security is often seen as a critical component in protecting personal and organisational assets. With human errors or vulnerabilities often being cited as a significant contributor to information security breaches, up to 95% of cyber incidents can be attributed to human error (Nobles, 2018), highlighting the importance of understanding how the human factor impacts security practices. The need to understand this factor is critically important to ensure secure practices for the individual and the organisation. In this section, this factor will be examined.

2.2.1 Human vulnerabilities in security systems

Human vulnerability in information security is a critical area of concern. These vulnerabilities arise from human error and are often considered the weakest link in the security chain. Attackers are able to exploit human vulnerabilities to gain unauthorised access to sensitive data (Kelm and Volkamer, 2018) by manipulating human behaviour through deception and persuasion, and these exploits can lead to breaches in confidentiality, integrity, and availability (Wang et al., 2020).

With the implications of human vulnerabilities extending beyond data breaches that can result in significant financial or reputational damage, the importance of security awareness training cannot be adequately highlighted. But even comprehensive security awareness training may not completely eliminate vulnerabilities (Wang et al., 2020). This indicates that while training can mitigate risks, it cannot fully eliminate the potential for human error. Table 2.6 identifies some common human errors:

Moreover, the complexity of modern systems increases these vulnerabilities. As systems become more interconnected and integrated, the potential for human error increases (Limba et al., 2017).

Table 2.6: List of common human errors in information security

Threat	**Explanation**
Phishing Attacks	Employees may inadvertently click on malicious links or attachments in phishing emails, leading to the installation of malware or unauthorised access to sensitive information.
Weak Passwords	Using weak or easily guessable passwords (e.g., "password123" or "admin") can make it easier for attackers to gain unauthorised access to systems.
Misconfiguration of Security Settings	Incorrectly configuring security settings, such as leaving ports open or not properly setting up firewalls, can create vulnerabilities that attackers can exploit.
Accidental Data Deletion or Modification	Employees might accidentally delete or modify critical data, leading to data loss or corruption.
Inadequate Patch Management	Failing to apply security patches and updates in a timely manner can leave systems vulnerable to known exploits.
Improper Handling of Sensitive Information	Employees might accidentally share sensitive information via unsecured channels or with unauthorised individuals, leading to data leaks.
Plugging in Unknown USB Drives	Connecting unknown or unauthorised USB drives to a computer can introduce malware into the network, compromising security.
Falling for Social Engineering	Employees may unknowingly provide sensitive information to attackers posing as legitimate entities through social engineering techniques.
Inadequate Training and Awareness	Lack of proper information security training can result in employees being unaware of security best practices, leading to poor decision-making.
Over-sharing Information on Social Media	Employees might share too much personal or work-related information on social media, which can be used by attackers to craft targeted attacks.

This table identifies some common human erros in information security. (Fortinet, 2025)

Taking this into account, human vulnerability in information security is a multi-faceted issue that requires an understanding of both the technical and human aspects of information security, highlighting the importance of effective strategies to limit human error.

2.2.2 Impact of technological advancements on information security

With the development of technology advancing at a rapid rate, malicious entities have exploited the unpreparedness of users, making information security awareness programs essential. But with the rapid growth of technology, these programmes will need to adapt to the current environment and be flexible in what is being taught.

There is a connection between information security and humans that cannot be ignored (Hughes-Lartey et al., 2021), and technology offers innovative solutions for information security. It also presents new challenges that must be addressed through approaches that include organisational, technological, and human factors. With research indicating that users decision-making abilities in relation to information security are largely influenced by their awareness of potential threats and their role in security (Johri and Kumar, 2023). One way to address this problem is to start awareness programmes for youth. The next section will look at the threats and vulnerabilities experienced by youth.

2.3 Threats and vulnerabilities facing the youth

The youth today face a large number of threats and vulnerabilities in information security, mainly arising from their interactions with digital technologies and social networks. These threats can be categorised into several key areas, including cyberbullying, privacy concerns, and lack of information security awareness. In this section, we will explore each of these areas.

2.3.1 Overview of youth specific threats and vulnerabilities

With the youth having access to digital technologies from an early age, they are also exposed to information security threats and vulnerabilities. These threats can take

many forms, from cyberbullying to phishing attacks. Moreover, social influences, including peer pressure, can lead the youth to engage in risky online behaviour, such as sharing passwords or personal information as a display of trust among friends (Furnell et al., 2021). This behaviour not only compromises their security, but also sets a precedent for future interactions that may further endanger their online safety. The key areas identified will now be further explored.

Cyberbullying: One significant threat is cyberbullying, which has become increasingly prevalent among the youth. Research indicates that many young people experience aggressive behaviour online, leading to severe psychological impact, such as depression and anxiety (Amankwa, 2021; Makarova and Makarova, 2019), and anonymity on the Internet can further increase these problems. In addition, the psychological vulnerability of teenagers, particularly those with low self-esteem, makes them more susceptible to the harmful effects of online harassment (Amankwa, 2021; Zhou, 2021), and this harassment can lead to them sharing personal information. This in turn can lead to information security vulnerabilities, where young users expose important information that could lead to other dangers.

Privacy Concerns: With many youths lacking awareness on the importance of protecting their personal information online, and studies showing that teenagers often share sensitive information on social networks without understanding the risk (Maryani et al., 2020; Zhao et al., 2022), this behaviour not only exposes them to identity theft, but also targets malicious entities that exploit these vulnerabilities to gain access to more secure networks, such as those used by their parents (Siyed, 2023). The implications of this are significant, as compromised home networks can lead to breaches of corporate security, highlighting the connection between personal and organisational security (Siyed, 2023).

Lack of awareness: Furthermore, the general lack of information security education among teenagers contributes to their vulnerability. Many youths do not possess the knowledge or skills required to protect themselves in the cyberenvironment. Research indicates that while teenagers are increasingly responsible for their online security, they often lack the necessary understanding of effective information security practices, such as the importance of using strong passwords and the recognition of phishing attempts (Choong et al., 2019; Nicholson et al., 2021).

Highlighting that initiatives to improve information security awareness among the youth are crucial, but they are often poorly implemented in schools (Alemany et al., 2020; Amankwa, 2021).

Considering the threats and vulnerabilities facing the youth, parents and educators must make renewed efforts to ensure a safer online environment for the youth. With a user, decision-making abilities are largely influenced by their awareness of potential threats and their roles in security.

2.4 Current state of information awareness and education programmes for the youth

The current state of information security awareness programmes for young people reflects a growing recognition of the importance of educating young people about information security risks and safe online practices. Recent studies indicate that there is a significant gap in awareness of personal information security among young people, which can lead to vulnerabilities in the digital landscape. For example, Rajkumar and Njenga (2022) emphasise that many young users are not adequately aware of the risks associated with the oversharing of personally identifiable information (PII) online, which exposes them to cybercriminal threats. This lack of awareness is particularly concerning given the rising number of threats associated with information security.

Venter argues that information security education should be prioritised as an essential part of the curriculum and should be seen in the same space as reading and mathematics (Venter et al., 2019). They advocate for a comprehensive approach to information security education that not only informs youth about risks, but also equips them with practical skills to navigate the digital world safely. In addition to formal education, various initiatives aim to improve information security awareness among the youth. For example, campaigns have been implemented to engage primary school students through contests and interactive activities, similar to efforts in other countries (Omorog and Medina, 2018). These initiatives are essential for building information security awareness among the youth.

Despite these efforts, challenges remain. The existing literature suggests that awareness levels are still inadequate, particularly among marginalised youth populations who may lack access to resources and information (Venter et al., 2019; Zenda et al.,

2020). Therefore, it is imperative that information security awareness programmes are tailored to address the specific needs and contexts of diverse youth. This includes leveraging the technology and social media platforms that are popular among young people to spread information effectively, and engaging them in discussions about information security risks and best practices. In the following sections, we will discuss the different recommended methods that should be used in information security awareness programmes.

2.4.1 Leveraging evidence-based programmes

Leveraging evidence-based programmes to promote awareness of information security among young people presents several advantages that can significantly improve their understanding and behaviour regarding information security. These programmes are designed to provide structured, validated approaches that not only educate but also motivate young people to adopt secure practices in their digital interactions.

One of the primary advantages of evidence-based programmes is their ability to create a security-positive culture among the youth. According to de Casanove et al. (2022), Security Education, Training and Awareness (SETA) programs are essential for equipping individuals with the knowledge and motivation necessary to comply with security policies when faced with risks. This proactive approach fosters a mindset where security becomes a shared responsibility, encouraging young people to actively engage in protecting their information and that of others. Evidence-based programmes are also grounded in psychological theories that improve their effectiveness. The research by Khan et al. (2011) highlights that awareness programmes based on psychological models can significantly influence individuals' understanding of security risks and their subsequent behaviours. By integrating psychological principles into training, these programmes can address emotional factors that affect decision-making, such as anticipated regret, which has been shown to motivate people to adopt security measures (Chen and Li, 2017). This suggests that a well-structured programme can lead to deeper internalisation of security practices among youth, making them more vigilant against potential threats.

2.4.2 Tailoring content to educational needs

To effectively tailor content for the educational needs of the youth in information security awareness programs, it is essential to consider several key factors: the existing knowledge gaps, the relevance of the content, the engagement strategies employed, and the continuous evolution of cyberthreats.

The relevance of the content delivered in information security awareness programmes is important and should be designed to connect with the experiences and challenges faced by the youth. This can be done by incorporating real-world scenarios and case studies that make the content more relatable and applicable to current youth (Legárd, 2020). Furthermore, the use of gamification and interactive learning methods has been shown to significantly increase information engagement and retention among younger audiences (Gjertsen et al., 2017; Letica, 2020). Such approaches not only make learning enjoyable, but also encourage active participation, which is crucial for effective knowledge transfer (Gjertsen et al., 2017).

The continuous evolution of cyberthreats requires that educational content be regularly updated to reflect the latest trends and challenges in information security. Programmes should include ongoing assessments and feedback mechanisms to adapt to the changing landscape of threats and to reinforce learning (Bauer et al., 2017; Brehmer et al., 2024). This approach ensures that the youth are not only aware of current threats, but also equipped with the skills to respond effectively (Maathuis et al., 2024).

It is critically important to keep information security awareness programmes relevant and up-to-date with the current state of the cyber environment.

2.4.3 The role of the parent

The role of parents or other caregivers in ensuring that their children are aware of information security is critical in the digital landscape nowadays. Parents act as the primary instructors of their children's online experiences, which includes educating them about information security risks and safe practices. Research indicates that many parents recognise their responsibility to guide their children through the complexities of digital environments, as they are often the first line of defence against potential cyber threats (Mian and Alatawi, 2023; Quayyum et al., 2021; Wang and Chen, 2022). This responsibility does not only involve monitoring their children's

online activities, but also fostering an environment where open discussions about digital safety can occur (Muir and Joinson, 2020; Sun et al., 2021).

One significant aspect of parental participation is the need for parents to improve their own digital literacy. Studies have shown that parents' understanding of information security directly influences their children's online safety (Banić and Orehovaki, 2024; Prior and Renaud, 2023). When parents are well informed about the risks associated with digital technologies, they are better equipped to implement effective strategies to protect their children. This includes setting appropriate boundaries, encouraging responsible internet use, and actively engaging in conversations about the potential dangers of the online world.

2.5 Summary

As highlighted in the chapter the threats and attacks in cyber-space are ever present and always advancing. This leads to the need for effective information security measures like strong authentication and access control or security awareness training. This research focuses on one of these security measures, security awareness training, focussing on the human aspect of information security. The goal is to educate the next generation by providing fun, interactive, and achievement-based awareness which will teach the youth about the threats faced.

The following chapter will highlight one method of information security awareness training in the form of a serious game and explain how the effective use of gaming can lead to a cyber-savvy youth of the future.

Chapter 3

Serious games

Serious games can be defined as games designed for a purpose other than entertainment, they are often used as educational, training, or therapeutic tools. These serious games leverage the engaging nature of gaming to facilitate learning, skills development, and behavioural changes across various fields, including education, healthcare, environmental management and information security training.

The difference between serious games and traditional games lies in intention and application. While traditional games are mainly focused on entertainment, serious games are designed to achieve educational or training goals. For example, Lau et al. (2017), emphasise that serious games can effectively target mental health outcomes, demonstrating their feasibility and effectiveness in cognitive training contexts. Olgers et al. (2022), report valuable learning experiences using a serious game to emphasise the utility of serious games in medical education, with a focus on ultrasound skills. This illustrates the potential of serious games to improve technical skills in a controlled and engaging environment.

In this chapter, the concept of serious games, particularly in the context of educating youth on information security awareness is explored. Section 3.1 examines the educational impact of serious games on young learners, highlighting their cognitive, motivational, and psychosocial benefits. It discusses how serious games improve engagement, improve knowledge retention, and provide interactive learning experiences that address the challenges facing marginalised youth. Section 3.2 explores the core elements that contribute to the effectiveness of information security awareness games, focussing on interactivity, real-world relevance, feedback mechanisms, and gamification principles. The subsections further break down essential aspects, such as learning goals and objectives, design principles for engagement, and embedded

information security concepts. Finally, Section 3.3 provides a summary of the chapter, consolidating key insights on how serious games can be effectively designed and implemented to improve information security education among the youth.

3.1 The educational impact of serious games for the youth

The educational impact of serious games on young people is large and varied and includes cognitive, motivational, and psychosocial aspects. Serious games have been shown to significantly improve learning outcomes compared to standard educational methods. A meta-analysis by Wouters et al. (2013) indicates that serious games are more effective in improving cognitive skills and knowledge retention, further suggesting that the benefits of serious games extend beyond immediate learning to long-term retention of information. This is particularly relevant for marginalised youth, who often face challenges in conventional educational settings. Research has shown that serious games can foster higher levels of motivation and engagement among these groups, thus addressing their underperformance in formal education (Hasanah and Baars, 2023).

The design features contribute much to the effectiveness of serious games. Aspects such as rapid feedback, goal setting, and the ability to fail without severe consequences promote exploration and experimentation (Abraham et al., 2019; Bellotti et al., 2010). "Stealth learning", where players are so focused on the game that they do not realise that they are learning, has been highlighted as an important aspect of serious games over traditional instruction methods (Haoran et al., 2019). Another aspect is to make sure that fun as well as educational content is present and important to maintaining user engagement (DeSmet et al., 2014; Schwarz et al., 2020).

In addition to cognitive benefits, serious games promote psychosocial skills among the youth, by providing a platform for collaborative learning and decision making, which in turn develops interpersonal skills and teamwork (Rumeser and Emsley, 2018). An example in health education where a serious game has shown positive effects on self-management and lifestyle choices among children, promoting healthy behaviours (Abraham et al., 2019; Andrew et al., 2022). The flexibility of serious games allows for targeted educational experiences that can adapt to the needs of the youth (de Araujo Pistono et al., 2024; Farsi et al., 2021).

With this in mind, serious games present a powerful tool to be used to advance education outcomes among the youth. The ability for a serious game to be a fun and interactive experience that improves cognitive skills and motivation and develops problem solving skills make them a valuable assets in educational strategies. This can be further explored as a tool to be used for information security awareness training by identifying the core element needed to create an effective information security serious game.

3.2 Core elements of effective information security awareness games

For a information security awareness game to be effective, several core elements must be built into the game to improve learning and participation among the players. These elements include interactivity, relevance to real-world scenarios, feedback mechanisms, and incorporation of gamification principles. These elements are further explored below:

- **Interactivity** is a fundamental aspect of any successful information security awareness game. Games that allow players to actively engage with the content tend to promote better learning outcomes. Interactivity should also aim to immerse the players into the world to promote "stealth learning". The "Cybersecurity Awareness using Augmented Reality" (CybAR) game demonstrates how augmented reality can create immersive experiences that teach information security concepts while providing immediate feedback on the player's decisions (Alqahtani and Kavakli-Thorne, 2020). In the same way, serious games like "CyberHero" have shown that personalised and adaptive game play can improve engagement and learning, with players reporting high levels of new knowledge acquisition (Hodhod et al., 2023).

- **Relevance to real-world scenarios** is another critical element. Games that simulate actual information security threats and challenges help players understand the implications of their actions in a safe environment. The tabletop game "Riskio" exemplifies this by allowing players to assume the roles of both attackers and defenders, thus gaining insight into information security strategies and the consequences of various decisions (Hart et al., 2020). Another aspect is the format of the "Build your own adventure" game, where the

choices change the outcomes and engage the players in realistic scenarios, further improving their understanding of information security issues (Croucamp et al., 2022).

- **Feedback mechanisms** are essential to strengthen learning. Games that provide immediate feedback on players' actions help them understand the consequences of their decisions, which is crucial for developing information security awareness. For example, the "CybAR" game not only teaches concepts, but also demonstrates the results of cyber-attacks through real-time feedback (Alqahtani and Kavakli-Thorne, 2020). This immediate reinforcement helps solidify the knowledge gained during game play. Having immediate feedback provides the player with the relevant information to understand the problem as it is being experienced.

- **Gamification principles** have an important role in maintaining engagement and motivation. By incorporating points, levels, and rewards for actions and achievements in games, the player experience is enhanced. Research suggests that serious games that incorporate these elements can enhance engagement and participation in information security training (Shah and Agarwal, 2023; Yasin et al., 2019). These principles should also aim to make the game fun and encourage the player to continue playing and learning.

An effective information security awareness game must integrate interactivity, real-world relevance, robust feedback mechanisms, and gamification principles to improve learning and engagement. By focussing on these core elements, developers can create impactful educational tools that not only inform users about information security threats, but also empower them to take proactive measures in their digital lives. The following sections will examine these elements in more detail, focussing on learning goals and objectives, design principles for engagement, and embedded information security concepts.

3.2.1 Learning goals and objectives

Learning goals and objectives are an important aspect in promoting information security awareness training through serious games. Clear educational outcomes must be established in games that promote information security awareness to keep users engaged effectively, improve user understanding, and influence user behaviour toward a safer online presence. Serious games provide an interactive platform on which

players can learn about information security in a simulated environment, which has been shown to improve knowledge retention and the application of skills in real-world scenarios (Godejord and Godejord, 2023; Yasin et al., 2019).

The integration of learning goals into serious games allows for targeted educational experiences that can address specific knowledge gaps among players. For example, games can be designed to focus on particular aspects of information security, such as threat identification, risk management, or safe online behaviours. Research indicates that serious games can effectively convey complex information security concepts by simulating real-world cyber attacks and providing players with opportunities to experiment with defensive strategies in a risk-free environment (Godejord and Godejord, 2023). This allows players to make informed decisions about their information security practices (Andrews et al., 2023). In addition, serious games can serve as a bridge between theoretical knowledge and practical application. By setting clear learning objectives, developers can ensure that players not only acquire knowledge but also understand how to apply it in real-life situations. For example, games that simulate phishing attacks can teach players how to recognise and respond to such threats, thereby translating theoretical knowledge into skills (Hart et al., 2020). This practical focus is essential, as studies have shown that awareness alone is insufficient to change behaviour, it must be coupled with practical strategies and experiences that reinforce learning (Limna et al., 2023).

By having a clear and defined goal when creating a serious game to promote information security awareness, the designer can focus on what important information needs to be delivered to the user, and it allows the game to be catered towards the targeted audience. This allows the user to receive the planned material in a structured and informative way, promoting retention, and allowing the users to make the connection between the content and the real-world.

3.2.2 Design principles and engagement

Effective design principles and engagement strategies are important aspects in improving learning in information security awareness games. These strategies ensure that users are engaged with the content, further ensuring the retention of important information. The key strategies are progressive difficulty, challenge, and real-world relevance. In this subsection, these strategies will be further explored.

- **Progressive difficulty and challenge:** The concept of progressive difficulty is crucial in game design, as it allows players to gradually build their skills and knowledge. By starting with simpler tasks and advancing to more complex challenges, players can develop a deeper understanding of information security concepts without feeling overwhelmed. Research indicates that increasing the level of difficulty as players progress can enhance their learning experience by promoting critical thinking and problem-solving skills (Hamari et al., 2016; van Steen and Deeleman, 2021). For instance, a game that simulates a cyber-attack can begin with basic scenarios, such as identifying phishing emails, and evolve into more complex situations, like responding to a data breach. This gradual escalation not only maintains player engagement, but also reinforces learning through practice and repetition (Coenraad et al., 2020). The integration of challenges that require players to apply their knowledge in dynamic scenarios can significantly enhance engagement. Games designed according to this principle encourage players to experiment with different strategies and learn from their mistakes in a risk-free environment (Jin et al., 2018). In addition, by incorporating challenges that mimic real-world information security threats, players can better understand the implications of their decisions and the importance of proactive measures.

- **Relevance to the real-world:** Connecting game content to real-world scenarios is another vital design principle that enhances learning outcomes. When players can relate the challenges they face in the game to actual information security issues, they are more likely to see the value of what they are learning. For example, a game that simulates the consequences of a data breach can illustrate the potential impact on an organisation, thus highlighting the importance of information security awareness (Godejord and Godejord, 2023; Zeijlemaker et al., 2022). Research has shown that serious games that incorporate real-world relevance not only improve knowledge retention but also motivate players to adopt safer online behaviours (Andrews et al., 2023). The use of realistic simulations in games can help promote the understanding of complex information security concepts, making them more accessible to players. By presenting scenarios that reflect current cyber threats, such as ransomware attacks or social engineering tactics, players can gain insight into the nature of these threats and the strategies to protect against them (Alqahtani and Kavakli-Thorne, 2020; Hall et al., 2022).

With this in mind, developers of serious games should have a clear goal in mind and employ effective game design principles that are relevant to the current state of

information security and engage the player/user to continue playing. This in turn promotes better learning and retention of the information provided.

3.2.3 Embedded information security concepts

Integrating information security concepts into a serious game in a natural way is a challenge that needs to be further emphasised. The key to providing the player with an effective learning experience is to do it in a way that promotes learning without feeling like a chore. An approach is to design a "information security serious game" that tries to reproduce real-life security experiences. These games require strategic and critical thinking from the players (Gáliková et al., 2021) and promote the education of the players on a variety of information security topics such as penetration testing, network forensics, and incident response.

Three types of serious games have been identified with regard to information security: games without integrated information security content, those with multiple choice selections, and those that have integrated information security objectives into the core gameplay loop (Kayali et al., 2018). The last is considered the most effective method for learning (Kayali et al., 2018). Games should incorporate objectives that are seamlessly integrated within both their narrative structure and the gameplay mechanics. (Kayali et al., 2018; Pellicone et al., 2022). These games should also feature gamification elements such as scoring systems, leaderboards, and feedback, to enhance player engagement and reinforce learning. There are various benefits in embedding information security concepts into a serious game, such as improving learning and engagement. By providing hands-on experience, concepts are not just superficially memorised but are learnt and understood in a natural and engaging manner (Huynh et al., 2017).

There is also empirical evidence that highlights the effectiveness of serious information security awareness games. An example is the research done with "CyberHero" where a large percentage of participants reported learning new information and being engaged in the content (Hodhod et al., 2023). Another study further highlights this point by demonstrating that an augmented reality game effectively taught participants about information security concepts and consequences (Alqahtani and Kavakli-Thorne, 2020).

3.3 Summary

For information security awareness games to be successful, the concepts discussed in this chapter need to be effectively integrated and used. By having clear goals and objectives, the game has a purpose and end goal to work towards, and this keeps the user engaged. The game should also feature proper design principles found in mainstream games to promote a fun gaming experience that promotes learning while also providing a fun and engaging experience. The information security concepts that form part of the objectives should also be integrated within the game and not added as an extra on the side, this promotes learning to happen naturally instead of a feeling of being forced. One method to achieve this integration is the use of real-life scenarios to simulate attacks or scenarios in which the user gets to experience the threat in a controlled environment. The following chapter will explore the concept of simulated experiences.

Chapter 4

Simulated experiences

As highlighted in the previous chapter, for a serious game to be successful, interactivity, relevance to real-world scenarios, feedback mechanisms, and gamification principles are necessary. These core elements must be integrated in a way that promotes the main objective of the serious game which is the raising of awareness about information security among the youth. In this chapter, we will explore the relevance to real-world scenarios, using simulated experiences as the focus.

Simulated experiences can be defined as structured, organised, and controlled environments that replicate real-world scenarios, allowing individuals to engage with content without the risk. These simulated experiences are commonly found in medical and educational settings, where the goal is to improve learning outcomes and build the confidence of the participant. The core of simulated experiences lies in the ability to create safe spaces for users to practise skills, reflect on their actions, and develop competencies through experimental learning.

One key aspect of simulated experiences is the psychological safety provided. This safe space allows users to take risks and make mistakes without lasting consequences. Research indicates that psychological safety is crucial for effective learning in simulation-based environments, as it encourages participants to participate fully without fear of negative consequences (Klenke-Borgmann et al., 2022; Purdy et al., 2022; Turner and Harder, 2018). For example, Purdy et al. (2022) highlight how previous experiences and personal confidence levels significantly influence participants' perceptions of risk taking in simulations, emphasising the importance of a supportive environment.

Another key aspect is the impact of simulated experiences on the user's emotional

state and confidence levels. Studies have shown that repeated exposure to high-fidelity simulations can significantly reduce anxiety and improve confidence in medical students (Small et al., 2018; Yu et al., 2021). This is particularly relevant in nursing education, where simulations allow students to practice clinical skills in a controlled environment, thus enhancing their readiness for real-life patient interactions (Adamson and Prion, 2020).

The design and fidelity of the simulations play a critical role in their effectiveness. High-fidelity simulations that closely mimic real-life scenarios tend to produce more meaningful learning experiences (Welman and Spies, 2016). Using advanced technologies such as augmented and virtual reality can further enhance the user experience by creating immersive environments that promote engagement and facilitate deeper learning (Chou et al., 2022). However, it is important to balance the realism with the educational objectives of the simulation, as too complex scenarios can obscure key learning points (Winn et al., 2006).

In this chapter, the effectiveness of simulated experiences in improving information security awareness is explored through immersive and interactive gameplay scenarios. In Section 4.1 an overview of simulated experiences in information security awareness games is provided, highlighting the role of simulated experiences in teaching essential information security skills through immersive mechanics. In Section 4.2 various mechanics explicitly designed to improve a user's information security awareness are discussed. These include detecting social engineering tactics, classifying and handling sensitive data, securing personal and mobile devices, reporting security incidents, maintaining daily vigilance, and analysing real-world attack scenarios. In Section 4.3 strategies used to maintain user engagement and interaction within information security simulations are outlined, such as progressive complexity, collaborative and competitive elements, incentives, and replayability, all contributing to sustained participation and effective learning. Finally, in Section 4.4 the key points discussed throughout the chapter are summarised, reinforcing the importance of carefully designed simulated experiences integrated into gameplay. This introduces the next chapter, where the proposed serious game, "CyberCadet: Threat Detector", is presented as a practical design science artefact.

4.1 The role of simulated experiences in information security awareness education

The role of simulated experiences in information security awareness education can be recognised as a critical component in improving the understanding and preparedness of individuals against cyber threats. Simulated experiences, such as gamified learning environments and interactive training modules, provide a unique opportunity for users to engage with information security concepts in a practical and immersive manner. This approach not only fosters a deeper understanding of the material, but also encourages the development of critical thinking and problem solving skills which are essential in real-world information security scenarios.

One of the primary advantages of using simulations in information security education is their ability to create a safe environment for learners in which to experiment and make mistakes without real-world consequences. One such simulation game, CyberMoraba (Nkongolo, 2024), has been shown to effectively engage users while teaching important information security knowledge. CyberMoraba not only improves individual learning, but also promotes a culture of information security awareness, by encouraging knowledge sharing and adherence to best practices (Nkongolo, 2024). The interactive nature of such simulations allows learners to experience the dynamics of cyber threats and defences, thereby reinforcing their understanding of the implications of their actions in a digital environment. By allowing users to play the game in a controlled way, these same users get to experience the threats in a practical way that allows the user to learn from experience and not just from learning material. This experience further advances the retention of information security knowledge by users. A study by Abrahams et al. (2024) shows that interactive workshops and simulated phishing exercises lead to higher levels of participation compared to traditional lecture-based training methods. The use of these practical methods further provide users with practical skills that can be used in their daily life, either personal or professional. Simulated experiences comprise two key components: real-world replication and risk-free environments. Understanding the importance of these two aspects forms the basis for simulation experiences.

4.1.1 Authentic real-world scenarios

Using authentic real-world scenarios when creating a simulated experience is important because it provides the player with knowledge of real-world threats that they

could experience in their personal and professional life. An important advantage is the ability to create immersive learning environments that mimic the complexity of actual cyber incidents. By immersing players in these realistic contexts, serious games facilitate a deeper understanding of information security principles and the critical thinking necessary to navigate potential threats effectively (Gáliková et al., 2021). By experiencing these incidents in a controlled and safe environment, players can experiment and learn from mistakes made, allowing them to further adapt to these threats in the real-world. Some proposed examples of possible attacks that can be simulated are presented in Table 4.1.

All of these examples can be programmed into a serious game and experienced by the user in a safe and controlled environment. This hands-on approach could improve the information security awareness of users, and improve their understanding of exposure to these threats.

4.1.2 Risk-free environment

The importance of creating a risk-free environment is underscored by the findings of Kovaević et al. (2020), who emphasise that the context in which individuals learn significantly influences their information security behaviours and perceptions. This is particularly relevant in educational institutions, where students are often exposed to various online threats. Using simulated experiences, educational institutions can foster an environment in which students can safely explore information security concepts, thus enhancing their understanding and awareness of potential threats (Khamzina et al., 2022). Specifically in the current state of the world where everything is becoming more and more digital, the youth need to understand the threats that exist in this digital world. Another aspect to consider is the current rise of AI tools that can be used to create more advanced attacks (Jampani, 2025) like ChatGPT [1]. One simple example could be that a threat actor that creates phishing emails can use AI tools to make sure there are no grammar mistakes, making it harder to detect phishing emails without proper identification methods or experience.

A user of a simulated experience serious game should experience the scenarios in a manner that promotes learning and is as close to the real-world as possible. This ensures that the virtual environment is safe, which is critical for the success of the game. The user will only truly learn once these two aspects have been properly defined and incorporated. The role simulations play in information security edu-

[1] https://chatgpt.com/

Table 4.1: Proposed threats that can be simulated for a information security awareness serious game

Simulated Threat	**Explanation**	**Examples**
Phishing	A broad type of cyber attack that uses deceptive messages (emails, texts, or instant messages) to trick individuals into revealing sensitive information (e.g., passwords) or installing malware. Attackers often impersonate legitimate organizations or create a false sense of urgency.	A user receives an email claiming to be from a bank or official source, prompting them to click a malicious link and provide personal details (e.g., password, credit card).
Ransomware Attacks	Ransomware involves encrypting a victim's files and demanding payment (often in cryptocurrency) to decrypt them.	A user unknowingly opens a malicious invoice attachment, causing their system to lock and display a ransom note.
Malware/Trojan Attacks	Malicious software disguised as legitimate programs, granting attackers unauthorised access or causing harm.	A seemingly harmless game download installs a Trojan, compromising the system's security.
Pretexting	Attackers create a believable backstory to manipulate users into revealing information or taking an action.	An attacker, posing as IT support, calls a user to obtain their login credentials under the guise of fixing an urgent technical issue.
Shoulder Surfing	Observing someone's screen or keyboard input to obtain sensitive data, such as passwords or PINs.	An attacker stands behind a user at a busy café and watches them type their password.
Baiting (Malicious USB)	Attackers leave infected media (e.g. USB sticks) in public places, hoping someone will plug it in.	A user finds a USB labelled "Confidential Salaries" and, out of curiosity, inserts it into their work computer, triggering malware.
Man-in-the-Middle (MitM)	An attacker intercepts or alters communication between two parties without their knowledge.	Using unsecured public Wi-Fi, a user's credentials are intercepted by an attacker monitoring the network traffic.

This table lists proposed threats that can be used for a simulated information security awareness serious game.

cation has the potential to become a core educational tool that can truly promote information security awareness among all people, not just the youth - if properly and effectively used.

4.2 Designing simulated experiences for serious games

When designing simulated experiences for serious games, a couple of aspects that need to be considered. These include clearly defined learning outcomes, the construction of realistic scenarios, the integration of simulation with game mechanics, and immersive feedback systems (Gáliková et al., 2021). All of these aspects need to be carefully investigated when designing simulated experiences. In this section, we will further explore these aspects, focusing on how these aspects can be used to create an effective serious game.

4.2.1 Defining clear learning outcomes

Defining clear learning outcomes is an important step in creating a simulated experience and answers the question what the user should learn from the interaction. These learning outcomes also impact the design and development of the serious game. Hodhod et al. (2023) state that serious games should measure the effectiveness of the game within itself to maintain immersion and provide meaningful data. By establishing precise learning outcomes, developers can ensure that the content of the game is aligned with educational goals, thus maximising the potential for knowledge transfer and skill acquisition. The following outcomes are proposed:

Recognize and respond to phishing attempts (Jayakrishnan et al., 2022)

- *Description:* Learners can identify and properly handle deceptive messages (emails, texts, or instant messages) designed to trick recipients into revealing sensitive information or installing malware.
- *Possible Assessments:*
  - Simulated phishing emails or text messages
  - Tracking response rates and click-throughs

  - Immediate feedback on correct/incorrect actions

Practice safe browsing habits (Shillair et al., 2015)

- *Description:* Learners understand how to verify site authenticity (checking URLs, certificates) and avoid dangerous downloads or suspicious links.
- *Possible Assessments:*
  - Interactive website simulation
  - Monitoring learner actions when prompted to download files
  - Real-time security prompts

Strengthen password security and authentication (Micallef and Arachchilage, 2017)

- *Description:* Learners know how to create strong passwords/passphrases and use multi-factor authentication to protect accounts.
- *Possible Assessments:*
  - Password creation exercises
  - Simulated system login with MFA requirements
  - Automated feedback on password strength

Detect social engineering tactics (Beckers et al., 2016)

- *Description:* Learners can spot and resist social engineering methods (pretext calls, tailgating, impersonation) used by attackers to gain unauthorised access.
- *Possible Assessments:*
  - Role-play or AI-driven interactions
  - Scenario-based quizzes
  - Observation of learner decision points

Classify and handle sensitive data appropriately (Qorahman and Akbar, 2024)

- *Description:* Learners accurately classify data (e.g. public, internal, confidential) according to organisational policy, and apply the correct handling procedures.
- *Possible Assessments:*
  - Interactive data handling tasks
  - Grading for correct classification
  - Feedback on risky storage behaviours

Secure personal and mobile devices (Ahmadov, 2023)

- *Description:* Learners apply best practices for device security, including encryption, software updates, and safe network connections.
- *Possible Assessments:*
  - Simulated device configuration
  - Checklists for security settings
  - Real-time prompts for updates or patches

Report and escalate security incidents (Grispos et al., 2017)

- *Description:* Learners understand when and how to properly report threats or suspicious activities to the appropriate security channels.
- *Possible Assessments:*
  - Time-sensitive incident simulation
  - Tracking response times and reporting accuracy
  - Automated guidance on escalation steps

Demonstrate overall information security mindset (Douha et al., 2023)

- *Description:* Learners internalise that security is everyone's responsibility and adopt vigilant, proactive behaviours in daily routines.

- *Possible Assessments:*
  - Monitoring consistent actions (e.g., locking screens, avoiding shoulder surfing)
  - Observation of learner vigilance in various game scenarios
  - Peer or supervisor feedback

Analyse real-world scenarios to identify likely attacks (Insua et al., 2019)

- *Description:* Learners study documented cyber incidents, news stories, or case studies to determine the likely attack method (e.g., phishing, ransomware, social engineering) and discuss possible prevention or response strategies.
- *Possible Assessments:*
  - Reviewing real or simulated incident reports and classifying the type of attack
  - Writing a brief analysis on how the attack could have been prevented
  - Scenario-based quizzes requiring learners to match evidence to an attack type

By incorporating these learning outcomes into a serious game, the effectiveness of the game could increase because there is a clear endpoint that must be reached. This implies that if a user reaches these outcomes, they should have a better understanding of the content that, in turn, might increase their effectiveness in protecting themselves from any incidents.

4.2.2 Constructing realistic scenarios

The construction of realistic scenarios as simulated experiences in serious games is important for several reasons; focusing on enhancing user engagement, facilitating effective learning, and promoting the transfer of skills to real-world situations (Palada et al., 2024; Lim et al., 2024). Realistic scenarios serve as the backbone of serious games, providing context as well as relevance which are crucial for players to fully immerse themselves in the learning experience. This immersion is essential to achieve the educational objectives that serious games are designed to fulfil. Figure 4.1 shows the possible flow that could be followed when creating these realistic scenarios. By using this as a guideline, one can effectively build realistic scenarios. Each of the steps will be explored next:

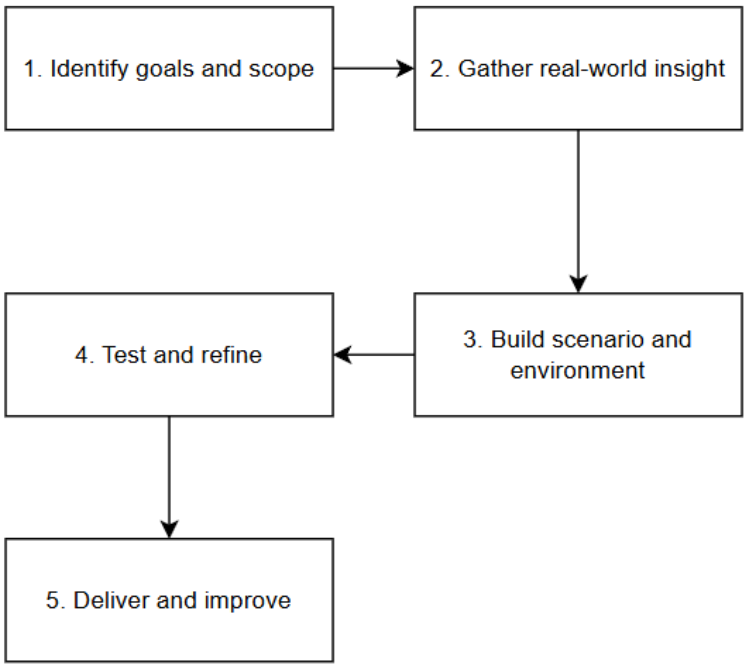


Figure 4.1: Scenario creation flowchart

Step 1: Identify goals and scope.

- **Define your training or exercise objectives:**
  - Determine the primary purpose of the scenario (e.g., phishing awareness, advanced incident response).
  - Align complexity to the skill level of participants (front-line employees, junior analysts, or security engineers).
- **Determine scenario boundaries:**
  - Decide on the technical scope (single system, entire enterprise, cloud services).
  - Set duration (a few hours, a full-day workshop, or a multi-day exercise).
  - Identify resource constraints (budget, staff availability, test environments).
- **Establish success criteria:**
  - Define metrics (e.g., detection speed, remediation effectiveness).
  - List desired learning outcomes (e.g. improved log analysis, improved threat detection).

Step 2: Gather real-world insights.

- **Research current hacking tactics (TTP):**
  - Follow threat intelligence feeds (e.g., blogs, forums, posts).
  - Note emerging attack trends (ransomware, supply chain compromises, IoT vulnerabilities).
- **Consult experts and case studies:**
  - Interview subject matter experts (penetration testers, red teamers, incident responders).
  - Study breach reports (public analyses of major incidents).
- **Synthesize key points:**
  - Build a reference list of common vulnerabilities (unpatched systems, weak credentials).
  - Map TTPs to your scenario goals (e.g., phishing for user awareness, lateral movement for network defence).

Step 3: Build scenario and environment.

- **Outline the narrative and timeline:**
  - Define an adversary profile (script kiddie, cybercriminal, hacktivist, nation-state).
  - Plan each attack phase (reconnaissance, initial compromise, privilege escalation, exfiltration).
- **Configure realistic systems:**
  - Decide on the technology stack (Windows, Linux, cloud services, or specialised systems).
  - Introduce relevant vulnerabilities or misconfiguration (e.g., outdated software, default passwords).
- **Create artefacts and clues:**
  - Prepare realistic logs (network traffic, SIEM alerts, endpoint detection logs).
  - Attempt phishing emails or malicious documents if social engineering is central.

Step 4: Test and refine.

- **Conduct a pilot run:**
  - Involve a small group of testers that match the skill level of your target audience.
  - Observe where they struggle or succeed to gauge the difficulty of the scenario.
- **Gather feedback:**
  - Use questionnaires or debrief sessions for direct participant feedback.
  - Validate technical accuracy with subject matter experts to confirm realism.
- **Refine scenario elements:**
  - Adjust complexity (add or remove attack steps, tweak vulnerabilities).
  - Improve clarity (revise instructions, improve, or simplify clues).

Step 5: Deliver and improve.

- **Run the final exercise:**
  - Provide a clear briefing on the context of the scenario, the available tools, and the rules of engagement.
  - Monitor participants' progress and decisions, noting how they respond to incidents.
- **Observe and guide:**
  - Offer clarifications or hints if participants get stuck, balancing learning with realism.
  - Track key metrics (time to detect or contain, overall collaboration).
- **Debrief, document, and evolve:**
  - Conduct a post-exercise debrief to identify what went well and where improvements are needed.
  - Use findings to update or create new scenarios, ensuring continuous evolution alongside emerging threats.

During the creation of the serious game related to this research, "CyberCadet", these steps were followed to identify and create scenarios for the game.

Another aspect that needs to be considered when creating these scenarios is the complexity of, and how a user will be guided through, the activity. For these activities, there should be guidance to ensure that the user has the opportunity to progress and learn and not get stuck without being able to complete the activity. The scenario should try to mirror real-world threats. This can be achieved using proper game design principles to simulate the environment of the scenario. Some effective methods are the introduction of visual information, story elements, or time pressure to create a sense of realism (Lim et al., 2024). Understanding these aspects and the reasons why they are important can further enhance the creation of simulated scenarios.

- **Visual information** is the incorporation of graphical representation, visual cues, and interactive elements. These aspects have a positive effect on the gaming experience of users, including enhancing user engagement, improving information retention, and fostering a deeper understanding of information security concepts. This in turn can make the learning experience more immersive and enjoyable (Gáliková et al., 2021; Hodhod et al., 2023).
- **Story elements** or storytelling serve as a powerful tool to engage users, enhance learning, and foster emotional connections to the material being presented. The narrative context provides a framework within which players can understand complex information security concepts, making the learning experience more relatable and memorable (Rikker and Sarmah, 2025).
- **Time pressure** refers to the constraints placed on players to make decisions within a limited time frame. This aspect is crucial to creating realistic and engaging scenarios that reflect the high-stakes environment of information security, where decisions often need to be made rapidly in response to evolving threats. The incorporation of time pressure can significantly influence a player's decision-making processes, enhancing the educational value of the game by simulating real-world conditions where timely responses are critical (Nkongolo, 2024).

Following the steps to create effective scenarios and using aspects such as visual information, story elements, and time pressure to enhance the experience, users get the opportunity to engage in the content being delivered. This creates a simulated

experience that allows the user to learn the required information in an enjoyable and interactive manner. This now raises the question of how to implement these scenarios in the serious game. This will be discussed in the following section.

4.2.3 Integration with game mechanics

An important aspect is to integrate these scenarios into the game loop without disrupting the immersion of the game. This can be achieved by building the game mechanics around the learning objectives. With this in mind in this section, the following mechanics are proposed based on the objectives highlighted above and relevant literature.

Scenario: Recognise and respond to phishing attempts (Jayakrishnan et al., 2022).

Mechanic: "Phishing?" inbox challenge

- **How it works:** The user receives a series of simulated emails or messages within the game interface. Some include telltale signs of phishing (e.g. suspicious links, poor grammar, urgent requests). The user must decide whether to open, report, or mark each message as phishing.
- **Assessments:** The system tracks correct identifications (flagging) vs. mistaken or missed attempts. Immediate feedback highlights missed red flags and reinforces correct phishing indicators.

Scenario: Practise safe browsing habits (Shillair et al., 2015)

Mechanic: Interactive "Safe surfing" browser simulation

- **How it works:** A simulated browser hosts multiple websites; some are benign, others contain malicious elements (e.g., phishing pop-ups, malware downloads). The user inspects the URLs and SSL certificates and decides whether to proceed with the downloads.

- **Assessments:** The simulation logs user actions, flagging risky clicks or downloads. Real-time pop-up warnings offer learning moments (e.g. "This certificate is expired, proceed?").

Scenario: Strengthen password security and authentication (Micallef and Arachchilage, 2017)

Mechanic: "Password creation and analysis challenge"

- **How it works:**
  - *Password creation:* The user is tasked with creating a strong password for a fictional account. As the user types, the system provides real-time feedback on the length, use of special characters, and avoidance of dictionary words or repeated patterns.
  - *Password analysis:* In addition to creating a password, the user is presented with a set of pregenerated passwords. A quick analysis tool (e.g., an estimated time-to-crack metric or a dictionary word scan) illustrates the strengths and weaknesses of each password.
- **Assessments:**
  - *Creation score:* The game evaluates the strength of the user-created password, using clear metrics such as length, character diversity, and resistance to brute-force attacks.
  - *Analysis score:* The user must classify each password provided as "weak," "moderate," or "strong" according to the tool analysis. The system logs how accurately the user identifies vulnerabilities in each sample password.
  - Demonstrates how strategic choices in password composition significantly improve security.
  - Reinforces best practices by letting the user see exactly how different factors (e.g., adding symbols, avoiding dictionary words) affect overall strength.
  - Encourages a deeper understanding of password vulnerabilities through direct comparison and feedback.

Scenario: Detect social engineering tactics (Beckers et al., 2016)

Mechanic: Role play and conversational scenarios

- **How it works:** The user engages with non-player characters (NPCs) employing social engineering ploys (e.g., tailgating, impersonation). Dialogue choices or scripted voice calls challenge the user to verify identities or protect sensitive info.
- **Assessments:** The game logs the choices at each decision point, highlighting when the user accidentally shares confidential details or allows unauthorised access.

Scenario: Classify and handle sensitive data appropriately (Qorahman and Akbar, 2024)

Mechanic: "Data sorting" mini-Game

- **How it works:** The user is presented with a set of fictional documents (e.g., emails, spreadsheets) each containing different sensitivity levels (public, internal, confidential). They drag and drop these items into appropriate classification folders and apply safeguards such as encryption where needed.
- **Assessments:** A scoring mechanism evaluates the correct classification and handling. If the user misclassifies a document, the game provides rationale for proper labelling.

Scenario: Secure personal and mobile devices (Ahmadov, 2023)

Mechanic: Virtual device configuration

- **How it works:** Within the game world, the user configures a simulated phone or laptop, enabling settings such as passcodes, automatic updates, and encryption. The periodic "OS update available" prompts to test whether they prioritise patching.
- **Assessments:** A checklist verifies the activation of crucial security measures. The game tracks the speed of the installation of the updates and notes any neglected patches.

Scenario: Report and escalate security incidents (Grispos et al., 2017)

Mechanic: Time-sensitive incident simulation

- **How it works:** During gameplay, a sudden "security breach scenario " occurs. The user must follow an in-game incident workflow (e.g., notifying the correct NPCs, logging the incident, escalating to higher authority) within a specific time limit.
- **Assessments:** The system records the response speed and accuracy (e.g., was the correct command chain followed?). Feedback highlights which steps the user missed or delayed.

Scenario: Demonstrate overall information security mindset (Douha et al., 2023)

Mechanic: "Daily vigilance" score and peer feedback

- **How it works:** The user navigates a persistent game environment populated with spontaneous security prompts (e.g. suspicious USB drives, shoulder-surfing attempts by NPCs). Taking correct actions increases the user's "Vigilance score."
- **Assessments:** Points accumulate for consistent good practices. Peer or AI-simulated supervisor feedback adds a social component (praise or guidance).

Scenario: Analyse real-world scenarios to identify likely attacks (Insua et al., 2019)

Mechanic: "Cyber investigator" case files

- **How it works:** The user reviews short narrative-based incidents reminiscent of real attacks, examining logs and clues to identify attack vectors. They propose prevention and response strategies in a quiz-like format.
- **Assessments:** The user must correctly classify each scenario (e.g., phishing, ransomware, social engineering) and articulate how it could have been mitigated.

Each mechanic above can be integrated into the core game play loop so that information security lessons feel organic to the story rather than a separate mandatory exercise. By designing the tasks to appear naturally in the user's in-game routine (e.g., checking email, working on projects, interacting with NPCs), the learning remains immersive, interactive, and highly practical.

4.2.4 Relevant feedback system

Using effective feedback systems is important because it facilitates learning (Ghani, 2015) in a way that simulates having a tutor give you feedback as they guide you through the task. Feedback serves as a mechanism for players to understand their performance, identify areas for improvement, and reinforce learning through responses to their actions within the game environment. The goal of this immersive feedback system would be to copy this approach, where feedback is given in a timely manner to allow the user to learn from the experience and not at a later stage. This feedback system can be achieved in various ways, some of which are score allocation, positive or negative feedback (notifications or indications of being right or wrong), and a review of performance.

An important aspect to remember is that the feedback system being used should be connected to the learning outcomes and should promote the goals of the scenario. For example, if using a point allocation system, the points should be given for a relevant aspect such as: The email is a phishing email, and the user correctly identifies that aspect. This system rewards the user for participating positively in the challenges found in the game.

Within this section, the construction of simulated scenarios was elaborated on, with a focus on how to create and implement these into a serious game. All of these aspects build up to another important part of a game, which is immersion. The goal of immersion is to create a game that keeps the user engaged without feeling like a chore, promoting learning while having fun. In the next section, these aspects will be explored.

4.3 Ensuring engagement and interactivity in simulated experiences

By incorporating effective engagement and interactivity aspects into the simulated experience, user understanding can be improved. This can be achieved with methods designed to promote learning and to keep the user engaged with the content; these methods are progressive complexity, collaborative elements, competitive elements, incentives, and replayability. These elements build on the foundation laid by aspects such as realistic scenarios and effective feedback systems by providing a method to realise these aspects. It is important to evaluate each of these elements and incorporate them into the design of a serious game.

4.3.1 Progressive complexity

The importance of ensuring progressive complexity in simulated experiences within information security awareness games cannot be overstated. As cyber threats evolve in sophistication, so must the training methods employed to combat them. Progressive complexity refers to the gradual increase in difficulty and level of tasks within a training programme, which is essential to effectively improve user skills and awareness of information security. This approach not only engages users, but also fosters deeper learning and retention of critical information security concepts. Filippidis et al. (2022) emphasise that as systems become increasingly complex, the human factor becomes a critical target for attackers, underscoring the need for training programmes that adapt to the evolving landscape of information security threats.

Incorporating progressive complexity into information security games allows for a customised learning experience that can accommodate varying levels of prior knowledge and skill among participants. This is particularly important, given that different users may have different levels of awareness and responsibilities regarding information security (Nkongolo, 2024). By designing scenarios that start with fundamental concepts and gradually introduce more complex scenarios, users can build confidence and competence over time. This aligns with the findings of Ertan and Yüzer (2024), who posit that awareness of information security responsibilities should be ingrained as a cultural element within organisations. Expanding on this to move outside the scope of organisations is important because the threats are not being experienced by organisations only. As threats evolve, proper inclusion of the general public in information security awareness campaigns needs to become a focus. This

ingrained cultural element should be taught to communities and the youth, creating a populace with a fundamental understanding of information security. This can be achieved by having customised progressive complexity scenarios that build on what the user already knows.

4.3.2 Collaborative elements

The integration of collaborative elements within simulated experiences is important to foster a solid understanding of security practices among participants. Collaborative gameplay not only enhances engagement, but also cultivates a shared sense of responsibility towards information security, which is essential in today's interconnected digital landscape. The importance of collaboration in information security awareness games can be understood through several dimensions, including the promotion of collective learning, the enhancement of problem solving skills, and the reinforcement of a security culture.

Collaborative elements in information security games facilitate collective learning, which is critical to developing a comprehensive understanding of information security threats and best practices. According to Nkongolo (2024), the inclusion of collaborative gameplay mechanics in information security awareness games fosters a culture of information security where knowledge is shared among participants, enhancing their collective resilience against cyber attacks. Shared experiences in a collaborative setting allow players to learn from one another, thereby strengthening their understanding of complex information security concepts. As highlighted by Teoh and Mahmood (2018), national information security strategies emphasise the importance of public awareness and collaboration among stakeholders to improve information security resilience. By engaging in collaborative gaming experiences, participants are more likely to internalise the importance of information security practices and the role they play in protecting their digital environments. This cultural shift towards a proactive stance on information security is essential, as it transforms participants from passive recipients of information into active contributors to their information security ecosystems.

In addition to these benefits, collaborative elements in information security awareness games also promote social interaction, which is vital to maintaining engagement and motivation among participants. Gwenhure and Rahayu (2024) note that the effectiveness of gamification in promoting information security awareness is closely related to the level of interaction and social participation within the game. When

players collaborate, they are more likely to remain engaged and motivated, leading to a deeper understanding of the material presented. This is particularly important in the context of information security, where the rapid evolution of threats requires continuous learning and adaptation.

4.3.3 Competitive elements

The integration of competitive elements into simulated experiences within information security awareness games is essential to improve engagement, knowledge retention, and practical skill application. The dynamic and immersive nature of these competitions prepares participants for the complexities of modern cyber threats while fostering a culture of continuous improvement and learning. As the information security landscape continues to evolve, leveraging competitive elements will be crucial to developing effective training programmes that equip users with the skills and knowledge necessary to navigate the challenges of the digital age.

By introducing competitive elements into a simulated experience, the user has the opportunity to apply their knowledge in a controlled and dynamic environment. One such competitive environment is the cybersecurity competition SANReN[2] CSC[3] (cybersecurity competition), where participants are challenged to compete against each other in a week-long competition. They are asked to complete various challenges that all count points, and each one tries to make the most points. Chindrus and Caruntu (2023) state that cybersecurity competitions provide a simulated battleground where defenders and attackers engage in a strategic encounter, preparing participants for the complexities of modern cyber threats. This competitive environment improves learning outcomes and promotes peer-to-peer interaction, which is vital for knowledge exchange and skill development. The immersive nature of these competitions allows participants to experience the pressure and urgency of real cyber incidents, thereby improving their situational awareness and response capabilities.

The integration of competitive elements into simulated experiences within information security awareness games is crucial to enhance engagement, knowledge retention, and practical skill application among participants. As the landscape of cyber threats evolves, traditional training methodologies often fail to prepare individuals for real-world scenarios. Incorporating competitive elements fosters a more immer-

[2]https://www.sanren.ac.za/
[3]https://www.csc.ac.za/

sive learning environment and encourages active participation, which is essential for effective information security education. In addition to enhancing participation, competitive elements in information security awareness games can lead to measurable improvements in knowledge retention and application. The survey of Balon and Baggili (2023) regarding information security competitions reports that gamification techniques, such as Capture the Flag (CTF) events, have been shown to yield positive learning outcomes. These competitions provide a platform for the application of practical skills and encourage participants to acquire new knowledge and skills to improve their performance, thus reinforcing the importance of continuous learning in the field of information security.

By ensuring that effective competitive elements are introduced into the game, one can make certain that users are motivated to engage in the content. This can come in various forms, from bragging rights to personal advancement.

4.3.4 Incentives

Incorporating incentives into simulated experiences within information security awareness games is crucial to enhance user engagement and promote effective learning outcomes. The integration of gamification elements, such as rewards and challenges, has been shown to significantly increase motivation among participants, leading to improved retention of knowledge and information security behaviours. By incorporating game mechanics that reward players for their achievements and progress, the game can effectively stimulate interest and participation, which are essential for successful learning in information security contexts (Nkongolo, 2024). When users are rewarded for completing tasks or achieving specific goals within a game, they are more likely to remain engaged and motivated to continue learning, providing the user with the tools to navigate cyberspace securely (Parvez et al., 2023). As users become accustomed to the game mechanics, their initial excitement may wane, leading to decreased participation and learning outcomes. Therefore, it is essential to continually innovate and introduce new challenges or rewards to maintain interest and motivation (Smiderle et al., 2020).

4.3.5 Replayability

Replayability in simulated experiences, particularly in information security awareness games, is crucial to enhance user engagement and retention of learning. By

allowing players to revisit scenarios with varying outcomes, these games can effectively emulate real-life cyberthreats in a safe environment, fostering a deeper understanding of information security principles. Incorporating interactive storytelling and customisable experiences not only maintains user interest but also reinforces learning objectives, making educational content more impactful (Croucamp et al., 2022; Rikker and Sarmah, 2025). Replayable games encourage players to experiment with different strategies, which is essential to understand the evolving nature of information security threats (Smith, 2014). As the landscape of cyberthreats evolves, the ability to adapt and learn through repeated gameplay becomes increasingly important, ensuring that users remain vigilant and informed.

4.4 Summary

Within this chapter, the aspect of what simulated experiences are was discussed, focusing on the role simulated experiences can have on information security awareness. With simulated experiences being recognised as a critical component in improving the understanding and readiness of users, it is further highlighted that effective implementation of simulated experiences is an important aspect of the simulations used in a serious game. These simulated experiences should be authentic real-world scenarios, created in a risk-free environment. They should also have clear learning outcomes that can better facilitate the goal of the serious game. The scenarios should be carefully designed to accommodate these learning outcomes, focusing on providing the best learning experience for the users. These simulated scenarios should also integrate seamlessly into the game mechanics to keep the user engaged with the content. This can be done by incorporating gamification components that further promote engagement. Some aspects like progressive complexity and competitive elements are key to creating a serious game that effectively achieved the goal of teaching the user to be more aware of their information security footprint.

With this in mind, we propose a serious simulation experience game called “Cyber Cadet: Threat Detector”, which will be discussed in the next chapter. This game was created to provide an artefact that can be used to test the effectiveness of simulated experiences in a information security awareness game.

Chapter 5

The Game

Within this chapter a detailed description and overview of the designed simulated experience information security awareness game "Cyber Cadet: Threat Defender" here after referred to only as "Cyber Cadet" will be presented. The design choices and relevance are discussed and examined. Further aspects of gamification are highlighted and explained. The aim of "Cyber Cadet" was to create a platform where users can play and experience authentic scenarios that are experienced in the real-world in a safe environment. Using the Scenario Creation flow chart shown in Figure 4.1 (page 50) as the foundation to build from, scenarios were created to be used in "Cyber Cadet". As stated in the previous chapters, an effective simulated experience will have clearly defined objectives. With this in mind, three scenarios were created and integrated into "Cyber Cadet". Each of these scenarios is explained using the first three steps of the scenario creation flowchart, while steps four and five will be discussed in the following chapter and will focus on the evaluation. The game can be accessed using the information found in Appendix A.

In section 5.1 the game engine used to create "Cyber Cadet" is discussed, followed by sections 5.2 to 5.4 where the three gaming challenges created to be used in "Cyber Cadet" are presented. In section 5.5 other gaming aspects are discussed to identify why incorporating these aspect are important. Finally, in section 5.6 a brief summary of the chapter is provided.

5.1 Game Engine

The game engine that was used to create the artefact is Godot[1] version 4.∗. Godot is a free open source game engine that allows the developer to create games without hidden expenses. It uses a programming language based on Python and other languages (Godot, 2024) and is designed to optimise aspects of game design, allowing the software to be used on any system and not just on high-end gaming systems. The system uses a style similar to object-orientated programming, where each scene found in the game is called a node, forming the player interface of the game. A typical game will consist of various scenes that interact with each other as the player progresses through the game. In Figure 5.1 the developer interface of the main menu scene for "Cyber Cadet" shows the similarity of the Godot development interface to other popular integrated development environments (IDEs), such as Visual Studio. This allows developers to quickly start programming without having to learn new features. This, and the fact that there are resources available to be used in the open source libraries, create an effective environment to create research-based games. In Figure 5.3, the simplistic code used to navigate to the other scenes from the main menu is shown.

This highlights basic functionality and familiarity with other coding languages.

Godot version 4 was selected as the software for this project due to ease of access and use. By using software that is easy to use, the developer is allowed to explore the goals and objectives of the game in more detail. In the following section the three scenarios that were incorporated into "Cyber Cadet" will be explored.

5.2 Password creation and analysis challenge

The first scenario that was integrated into "Cyber Cadet" was a password creation and analysis challenge. As a large number of incidents relate to the human aspect of information security; the importance of understanding effective password practices is essential to everyone. It is realised that with the advancement of technology, the complexity and strength of passwords need to increase to ensure that malicious entities cannot use weak password practices to compromise the user. In this section, the password creation scenario will be explained in more detail using the first three steps of the scenario creation flow chart (Figure 4.1, page 50).

[1] https://godotengine.org/

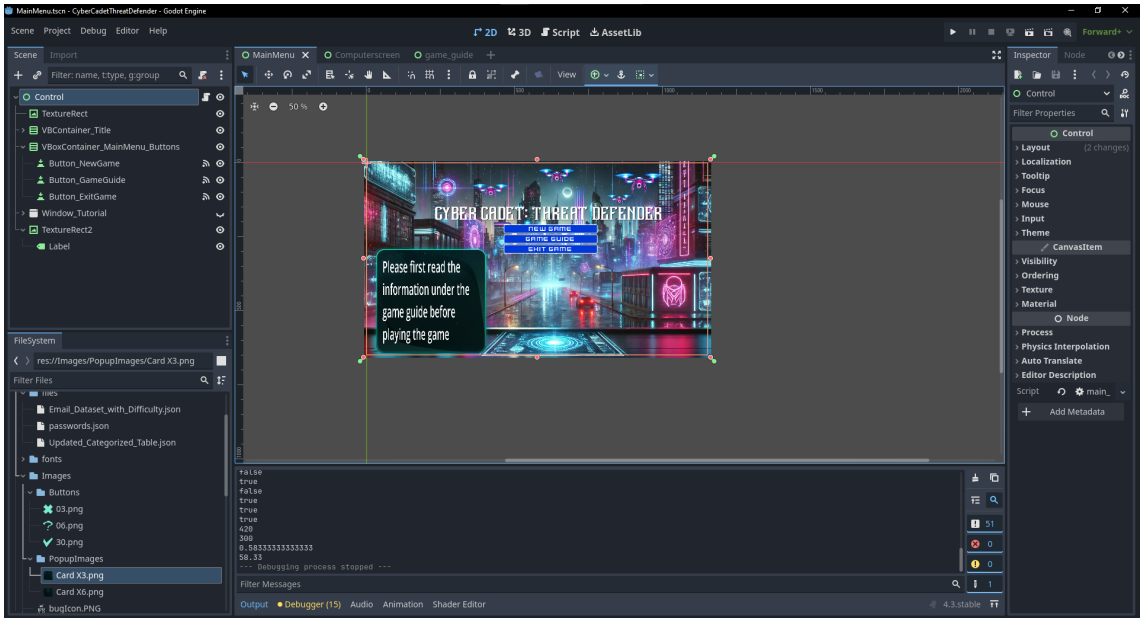


Figure 5.1: The developer interface for the main menu scene of “Cyber Cadet”

Figure 5.2: A screenshot showcasing the main menu

```gdscript
extends Control
var tutorial = true

# Called when the node enters the scene tree for the first time.
func _ready() -> void:
    pass

# Called every frame. 'delta' is the elapsed time since the previous frame.
func _process(delta: float) -> void:
    pass

func _on_button_new_game_pressed() -> void:
    get_tree().change_scene_to_file("res://Computerscreen.tscn")

func _on_button_exit_game_pressed() -> void:
    get_tree().quit()

func _on_button_game_guide_pressed() -> void:
    get_tree().change_scene_to_file("res://game_guide.tscn")

```

Figure 5.3: Code snippet for the main menu of "Cyber Cadet"

5.2.1 Step 1: Identify goals and scope

The proposed main objective of the "Password Creation and Analysis Challenge" is to educate and reinforce best practices for creating strong passwords by giving users hands-on real-time feedback on their choices. By having users both create their own passwords (and see immediate strength metrics) and analyse the strengths/ weaknesses of sample passwords, they gain a deeper understanding of why certain password components (length, character diversity, avoidance of common words or patterns) are critical to security. Using this objective as a starting point, the following proposed sub-objectives were also identified:

1. **Increase awareness of best practices:** By the end of the challenge, users should be able to explain why the use of a mix of uppercase, lowercase, numbers and symbols strengthens passwords.

2. **Demonstrate impact of common vulnerabilities:** Users should be able to identify which passwords are susceptible to dictionary attacks or repeated patterns, and explain how these factors weaken security.

3. **Develop hands-on password creation skills:** Each user should create a password that meets or exceeds specified strength metrics (e.g., length, complexity) as measured by the real-time feedback tool.

4. **Evaluate password strength accurately:** Given a set of sample passwords, users should classify them (weak, moderate, strong) with at least 80% precision, based on the criteria of the analysis tool.

5. **Promote lasting behavioural change:** After completing the challenge, users should commit to updating at least one of their actual real-world passwords to meet the newly reinforced standards.

5.2.2 Step 2: Gather real-world insights

This step involved looking at the common practices applied when determining what the characteristic of a strong password is. Four attributes were identified as important and integrated into the scenario; these attributes are:

Length: Length is one of the most important attributes in the strength of the password (Helble et al., 2019), because the number of possible combinations grows exponentially with each additional character added to the password. Some reason why length is important are:

1. **Exponential increase in combinations:** Each additional character in a password multiplies the total possible password combinations by the size of the allowed character set, leading to exponential growth in possibilities. For example, if each character is one of 10 digits, a 4-digit PIN has 10,000 combinations, and adding a fifth digit increases the possibilities to 100,000. This makes it drastically harder for automated tools (such as brute-force attacks) to guess the correct combination.

2. **Time to crack goes up:** Brute-force attacks test every possible combination. Longer passwords take significantly more time and computing power to crack, often making attacks impractical or impossible within a reasonable time frame.

3. **Offsets other weaknesses:** Even if a password has fewer special characters or predictable patterns, simply increasing its length can still improve its security (although the best practice is to combine length with complexity).

4. **Limits effectiveness of dictionary attacks:** Dictionary attacks usually rely on common words or phrases. A longer password, especially one that mixes random words or includes extra characters, makes it less likely to be found in any dictionary list.

Complexity: Complexity is a critical factor in password strength because it increases the difficulty of guessing or cracking a password by introducing a variety of

character types (Kävrestad et al., 2019). Some reasons why complexity is important are:

1. **Increases character variability:** Including a mix of uppercase and lowercase letters, numbers, and special character, significantly increases the total number of possible combinations, making passwords much harder to guess.
2. **Stops brute-force attacks:** Brute-force attacks rely on systematically trying all possible combinations. With increased complexity, the time and computational resources required to crack a password become impractical.
3. **Reduces vulnerability to dictionary attacks:** Simple passwords or those made up of common words are susceptible to dictionary attacks. Adding complexity makes passwords less predictable and less likely to be included in precompiled lists.
4. **Protects against pattern-based guessing:** Attackers often exploit predictable patterns (e.g., "1234" or "password"). Complexity reduces the likelihood that passwords are derived from predictable sequences.
5. **Enhances security for shorter passwords:** While longer passwords are generally better, adding complexity to shorter passwords can still provide a robust level of security by making them harder to predict.

Predictability: Predictability is a major weakness in password security, as attackers often exploit common patterns or sequences (Rodwald, 2019). Minimising predictability improves the strength of passwords by making it harder for attackers to guess passwords. Some reasons why reducing predictability is important are as follows.

1. **Prevents common pattern exploitation:** Attackers often guess passwords based on popular patterns such as "123456" or "password." Avoiding predictable sequences significantly reduces the chances of a successful guess.
2. **Increases resistance to dictionary attacks:** Predictable passwords are often included in precompiled wordlists used for dictionary attacks. Reducing predictability ensures that a password is not easily found in such lists.
3. **Avoids social engineering guesses:** Passwords based on personal information, such as birthdays or pet names, are highly predictable and easy for attackers to guess. Unpredictable passwords reduce this risk.

4. **Breaks brute-force efficiency:** Attackers may use algorithms to prioritise predictable combinations. Reducing predictability forces brute-force attacks to try more combinations, increasing the effort required.

5. **Encourages randomness:** A random mix of characters and symbols ensures that the password does not follow any logical or recognisable patterns, further enhancing its security.

Uniqueness: Uniqueness is essential for password security, as reusing passwords between multiple accounts creates significant vulnerabilities (Saleh, 2024). Ensuring that passwords are unique reduces the risk of widespread compromise. Some reasons why uniqueness is important are:

1. **Prevents credential stuffing:** If a password is reused across accounts, a breach in one system allows attackers to gain access to others. Unique passwords prevent this type of attack.

2. **Limits the impact of breaches:** Unique passwords ensure that the compromise of one account does not expose others, thereby limiting the damage of a data breach.

3. **Stops attacker assumptions:** Attackers often assume that users reuse passwords. Using unique passwords removes this advantage, making it harder for them to exploit leaked credentials.

4. **Promotes security best practices:** By using unique passwords for each account, users adhere to a fundamental principle of information security, reducing overall risk.

5. **Encourages the use of password managers:** The requirement of uniqueness often leads to the adoption of password managers, which help generate and store strong and unique passwords efficiently.

These four attributes were used in both the analysis and creation phases of the challenge and form the foundation to determine whether the user understands the concepts presented in the challenge. A dictionary list was also acquired to use as a data set for the password analysis phase of the challenge. This dictionary list contains over 3000 common passwords. Each of these passwords was analysed using the four attributes, namely length, complexity, predictability, and uniqueness, using a scoring system out of 10, adding up to a total out of 40. Table 5.1 shows examples

of passwords that have been analysed using this method. Some more examples can be found in Appendix B.

Table 5.1: Examples of passwords analysed

ID	Password	Length Score	Complexity Score	Predictability Score	Uniqueness Score	Total
224	666666	2	1	1	1	5
0	123456	2	1	1	1	5
1609	mustang1	5	2	2	3	12
1682	qwerty12	5	2	1	1	9
1161	Superman	5	1	1	2	9
1160	Sunshine	5	1	1	3	10
796	chester1	5	2	1	3	11
1485	jeffrey1	5	2	1	3	11
1447	heather2	5	2	1	3	11
970	nirvana1	5	2	1	3	11
1152	Password	1	1	1	1	4
624	phoenix1	5	2	2	3	12
1617	newyork1	5	2	1	2	10

This table shows examples of weak passwords and their analysed scores out of 40.

These four attributes and the password dictionary were used to create a challenge in which users would analyse a set of passwords and give it a score of 40. A calculation of how much the user's score deviates from the analysed password's score set is made to determine if the user effectively analysed the password. This provides the user with a score that will be discussed later in this chapter. In the next section, the process of building this scenario in the game will be explained.

5.2.3 Step 3: Build scenario and environment

The goal of the password creation and analysis challenge is to foster a good understanding of safe password practices. The scenario was designed to allow the user to evaluate various passwords using the four attributes discussed earlier. The user is presented with a password and must rate each of its attributes on a scale of 1 to 10. In Figure 5.4 the basic instructions given to the user when playing the game are presented; these basic instructions take into account that the user has already read the detailed instructions and awareness information found in the main menu. After the user has closed the instruction scene, the password analysis challenge will begin, as presented in Figure 5.5. Once the user gives a score, as seen in Figure 5.6, and clicks on the check mark icon at the bottom of the scene, a score based on the

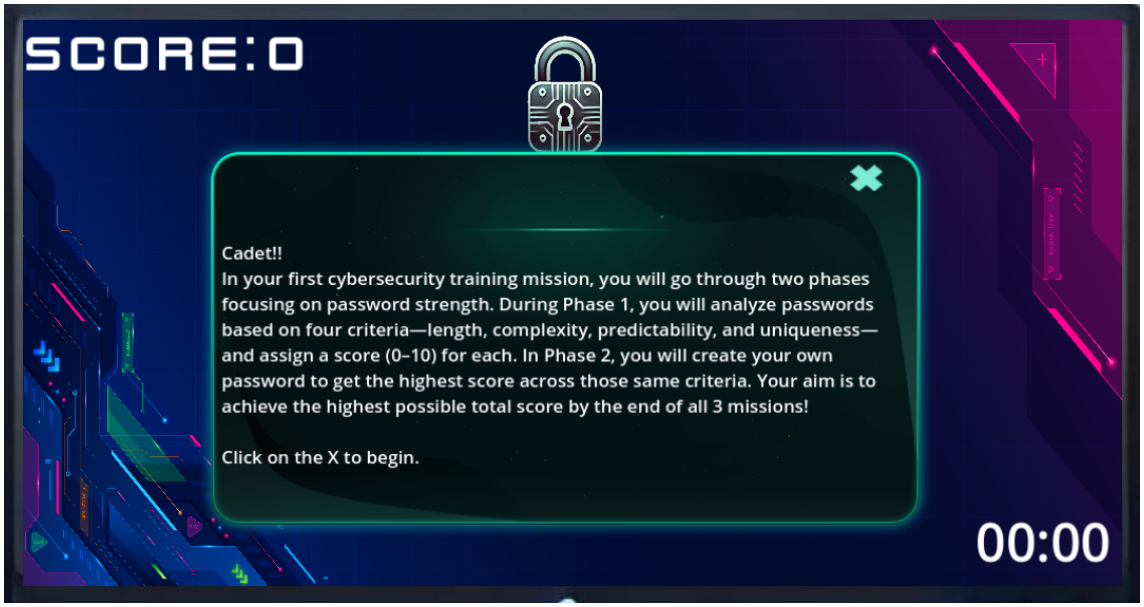


Figure 5.4: Ingame instruction for password challenge

deviation will be given to the user as part of a total score based on the calculations found later in this section. A new password is then revealed as seen in Figure 5.7.

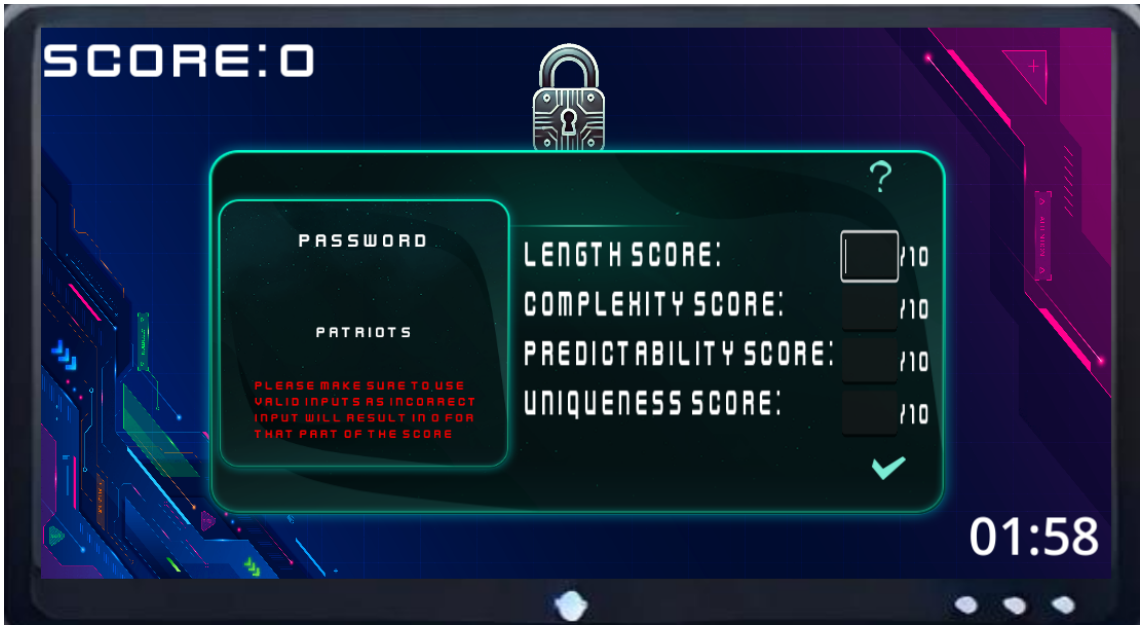


Figure 5.5: The password analysis challenge

Figure 5.6: User entered score for each attribute

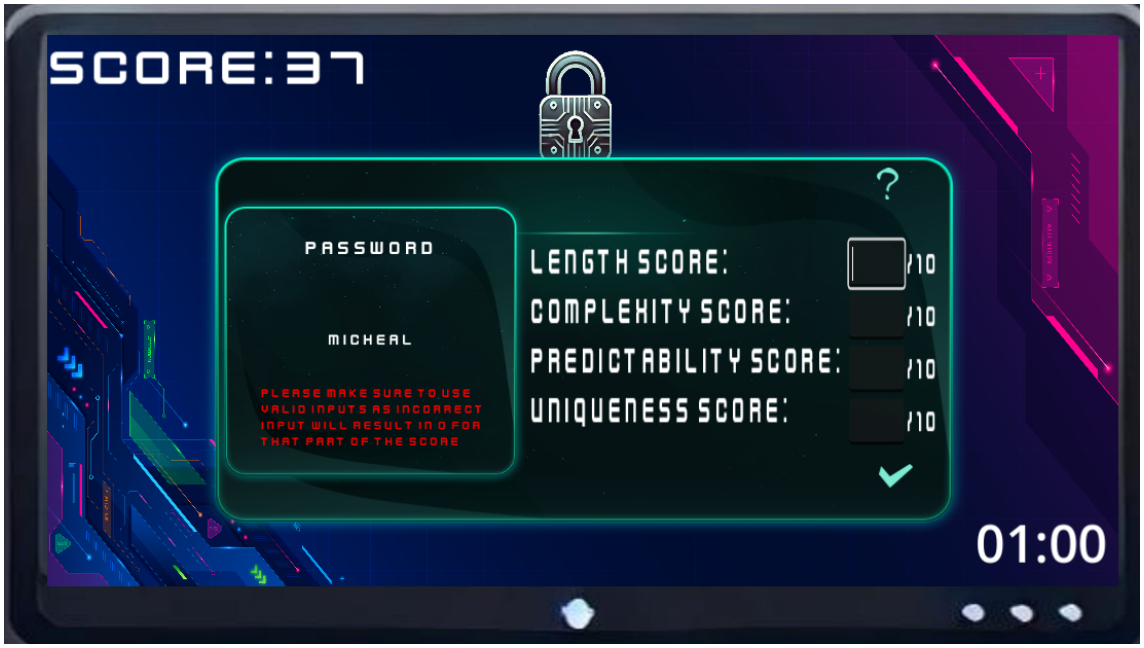


Figure 5.7: Score updated after clicking on check mark

The following parameters are used in the calculation of the deviation:

- P_{Length}: Password length input.
- $P_{\text{Complexity}}$: Password complexity input.
- $P_{\text{Predictability}}$: Password predictability input.
- $P_{\text{Uniqueness}}$: Password uniqueness input.
- total: Existing total score of the current password.
- difference: Absolute difference between the sum of inputs and the existing total.
- penalty: Calculated penalty based on the difference.
- max_score = 40: Maximum possible score.
- final_score: Final score after applying penalties.
- current_score: Current display score.
- calculated_score: Updated display score after adding the final score.

Sum of inputs:

$$\text{count} = P_{\text{Length}} + P_{\text{Complexity}} + P_{\text{Predictability}} + P_{\text{Uniqueness}}$$

Absolute difference:

$$\text{difference} = |\text{total} - \text{count}|$$

Penalty calculation:
If difference $= d$, then:

$$\text{penalty} = \sum_{i=1}^{d} i = \frac{d \times (d+1)}{2}$$

The penalty is capped at 40:

$$\text{penalty} = \min(\text{penalty}, 40)$$

If count $= 0$, then:

$$\text{penalty} = 40$$

Final Score:

$$\text{final\_score} = \text{max\_score} - \text{penalty}$$

Calculated score:

$$\text{calculated\_score} = \text{current\_score} + \text{final\_score}$$

Running Totals:

$$\text{Total\_Password\_Score\_Achieved} += \text{final\_score}$$
$$\text{Total\_Password\_Attempts} += 1$$
$$\text{Total\_Password\_Penalty} += \text{penalty}$$

The formula used to analyse the password compares the score assigned to a password with the score given to the same password by the user. If the user score is identical to the assigned score, the user will receive 40 points, which is added to their total

```
func calculate_password_analysis_score(current_password):
    # Validate that each input field has a valid intege
        var PLength: int = int(PasswordLengthInput.text)
        var PComplexity : int = int(PasswordComplexityInput.text)
        var PPredictability : int = int(PasswordPredictabilityInput.text)
        var PUniqueness : int = int(PasswordUniquenessInput.text)
        if(PLength<0 && PLength>=10):
            print(int(PasswordLengthInput.text))
            PasswordErrorText.visible = true
            PasswordErrorText.text = "Please enter a valid value for lenght"
        elif(PComplexity<0 && PComplexity>=11):
            PasswordErrorText.visible = true
            PasswordErrorText.text = "Please enter a valid value for complexity"
        elif(PPredictability<0 && PPredictability>=11):
            PasswordErrorText.visible = true
            PasswordErrorText.text = "Please enter a valid value for complexity"
        elif(PUniqueness<0 && PUniqueness>=11):
            PasswordErrorText.visible = true
            PasswordErrorText.text = "Please enter a valid value for complexity"
        else:
            var count = PLength + PComplexity + PPredictability + PUniqueness
            var totalText = current_password.Total
            var total = int(totalText)
            var difference = abs(total-count)
            var penalty = 0
            var max_score = 40

            for i in range(difference):
                penalty += i +1


            if(penalty >= 40):
                penalty = 40
            elif(count == 0):
                penalty = 40

            var final_score = max_score - penalty
            var current_score = int(DisplayScoreText.text)
            calcualted_score = current_score + final_score
            Total_Password_score_achieved += final_score
            Total_Password_attempts += 1
            Total_Password_Penalty += penalty
            DisplayScoreText.text = str(calcualted_score)
```

Figure 5.8: Code used to calculate password scores

score. On the other hand, the larger the difference between the user score and the allocated score, the fewer points the user will receive to a minimum of 0. The user has 120 seconds to complete the first challenge in order to accumulate the highest score for this challenge. This time limit adds a sense of urgency, as discussed in Chapter 4. By introducing a game mechanic that rewards the player, the user is actively given feedback on how well they are doing in the challenge. The goal of using these mechanics is to provide the user with a visible result, allowing the user to do the challenge again and see if there is any improvement. Figure 5.8 shows the code used to calculate these scores.

The first phase of the scenario encourages the user to carefully look at the passwords and determine if these are good or bad passwords. At the end of the two minutes, the scene transitions into a second phase, asking the user to create a password using

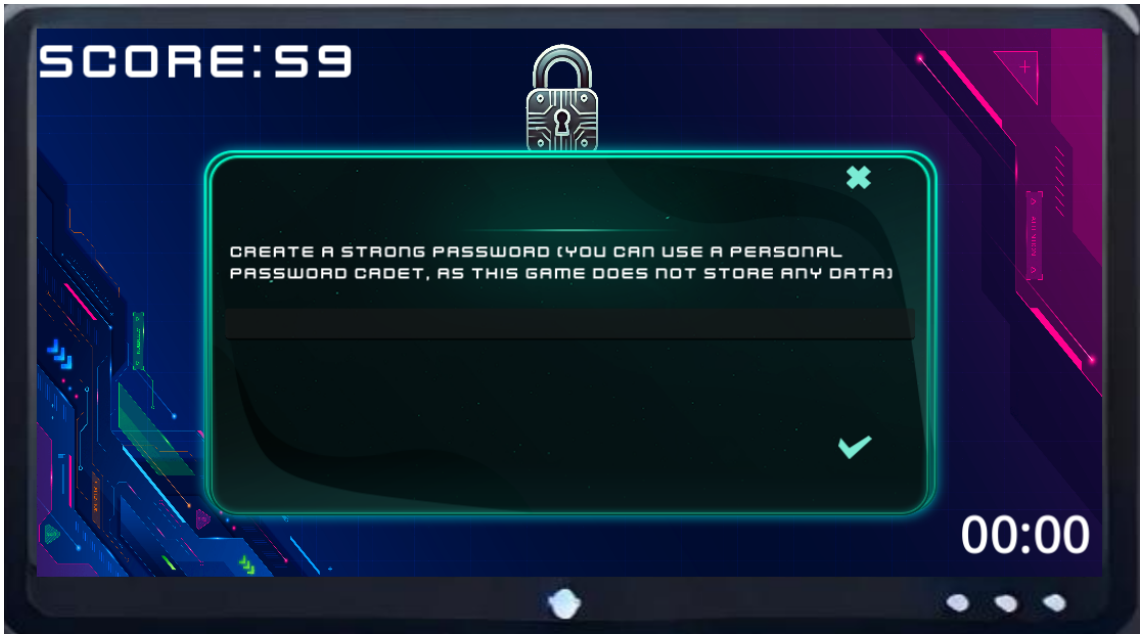


Figure 5.9: Phase 2: Password creation

what they have learnt from the previous phase, as shown in Figure 5.9.

The user can then create a password to try and receive additional points. The points given range from 0 to 200. The score is calculated by checking what the length of the password is, how many different character types were used, and if part of the password or the word as a whole is found in the password dictionary list. Figure 5.10 shows an example of a strong password that received the maximum points. The total score is then updated by double that to reward the user for doing well in this phase. This encourages the user to continue playing. The order of the challenge was chosen because providing the user with example passwords and having them create a password only afterwards, the user might learn from experiencing the weaknesses in the password analysis phase.

The user is then asked to use the X to exit the window and move on to the next challenge. Here, a brief description of the next challenge is explained to the user before having them move onto the second challenge, which is focused on email identification. The next section will deal with the creation and implementation of the second challenge.

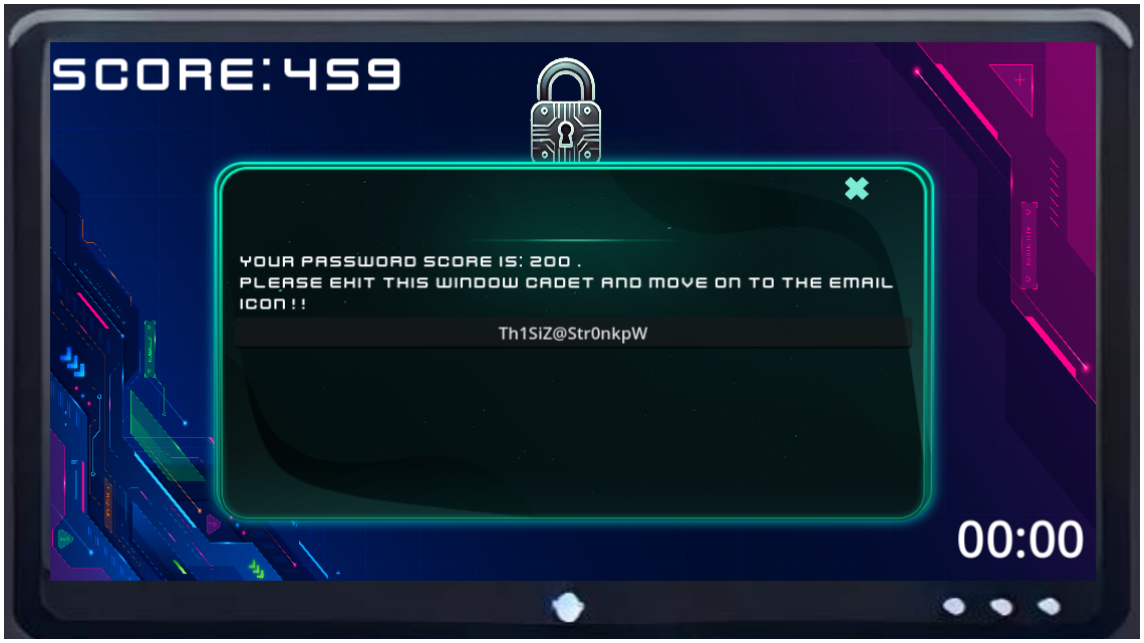


Figure 5.10: Example of a strong password

5.3 "Phishing?" inbox challenge

The second scenario that was integrated into "Cyber Cadet" was an email identification challenge, in which the user is required to look at emails and determine whether these emails are legitimate and safe or not. Nowadays the majority of people use emails daily, and tools to assist malicious entities to send out email scams of excellent quality are becoming more advanced. Subsequently the ability to identify and understand any threats is essential in present day life. This section will use the same steps as the previous challenge to clearly define a goal and outcomes, before looking at real-world examples and then the design aspect of creating this challenge.

5.3.1 Step 1: Identify goals and scope

The main goal of the "Phishing?" inbox challenge is to improve user awareness and practical skills in recognising and responding to suspicious communications. The main method of delivery in this challenge is via email simulations, but is applicable to other forms of communication as well, such as messages on other platforms. The proposed main objectives are:

1. **Increase awareness of phishing indicators:** By the end of the challenge, users should be able to identify common phishing signs such as suspicious

links, urgent requests, and poor grammar.

2. **Demonstrate understanding of appropriate responses:** Users should be able to correctly determine whether to report, mark as phishing or safely ignore simulated emails, based on the indicators provided.

3. **Develop decision-making skills in phishing scenarios:** Each user should achieve a minimum success rate (e.g. 80%) in correctly flagging phishing attempts and identifying legitimate messages by the end of the activity.

4. **Reinforce learning through deedback:** After completing the challenge, users should explain at least three red flags they missed during the activity and describe how they will recognise these in future scenarios.

5. **Promote long-term vigilance against phishing:** After the challenge, users must commit to regularly reviewing their email practices and applying the skills learnt to minimise the risks of falling for phishing attempts in real-world situations.

5.3.2 Step 2: Gather real-world insights

This step involved examining common email scams that were deployed to determine what suspicious communication looks like and how to clearly identify these threats. Four types of suspicious emails were identified to be used to provide the user with some common experiences that they may experience daily. The proposed email scams are credential-harvesting, malware, impersonation, and fraudulent offers (Dawkins, 2023). In this section, it is explained why it is important for a user to know about and be able to identify these scams.

Credential-harvesting: Credential-harvesting involves phishing attempts designed to steal sensitive information, often by tricking users into entering sensitive information on fake websites or forms (Fortinet, 2025). Understanding this type of attack is important to be able to:

1. **Protect against unauthorised access:** Stolen credentials can give attackers access to sensitive systems, personal accounts, or financial data. Recognising these attempts prevents such breaches.

2. **Reduce risk of identity theft:** Credential theft often leads to identity theft, where attackers misuse stolen information for fraudulent activities. Awareness helps users safeguard their identity.

3. **Prevent account takeovers:** Attackers frequently use harvested credentials to take over accounts, locking users out and causing significant disruption. Learning to spot these attacks can stop these takeovers.

4. **Defend against broader attacks:** Stolen credentials are often used in credential-stuffing attacks, where attackers try the same credentials across multiple accounts.

5. **Promote safe online practices:** Recognising fake login pages and suspicious links helps users adopt safer behaviours, such as verifying the authenticity of the website and avoiding suspicious attachments.

Malware: Malware refers to malicious software designed to harm devices, steal data, or disrupt operations (Fortinet, 2025). Recognising malware delivery methods is critical to be able to:

1. **Prevent system damage:** Malware can corrupt or disable systems, leading to data loss or downtime. Awareness helps users avoid downloading malicious software.

2. **Stop data theft:** Malware often steals personal or organisational data, putting privacy and security at risk. Identifying suspicious downloads or attachments minimises exposure.

3. **Block ransomware attacks:** Ransomware encrypts files and demands payment for decryption. Understanding how malware spreads can help prevent these costly attacks.

4. **Protect against unauthorised surveillance:** Some malware allows attackers to spy on users and capture sensitive information such as keystrokes. Recognising these threats ensures privacy.

5. **Reduce infection propagation:** Infected systems can spread malware to others within a network, increasing the impact. Educating users limits this cascade effect.

Impersonation: Impersonation involves attackers who pose as trusted entities, such as colleagues, friends, or organisations, to manipulate users into divulging information or performing harmful actions (Fortinet, 2025). Learning to identify impersonation attempts is important to be able to:

1. **Prevent manipulation:** Impersonators rely on trust to deceive users into revealing sensitive information. Awareness helps users verify identities before acting.

2. **Reduce financial loss:** Many impersonation attacks involve fraudulent payment requests. Recognising fake communications can save individuals and organisations from financial harm.

3. **Maintain professional integrity:** Attackers posing as executives or colleagues can damage reputations if sensitive information is leaked. Learning to spot these schemes protects integrity.

4. **Defend against social engineering:** Impersonation is a common form of social engineering. Understanding its tactics helps users resist manipulation.

5. **Improve verification practices:** Learning to validate requests and confirm identities enhances overall communication security.

Fraudulent offers: Fraudulent offers exploit users with enticing but false promises, such as winning a lottery, receiving a gift, or getting a discount (Fortinet, 2025). Understanding these schemes is important to be able to:

1. **Protect financial resources:** Many fraudulent offers aim to trick users into making payments or sharing payment details. Recognising these scams prevents financial loss.

2. **Avoid personal information theft:** Fraudsters often use fake offers to collect personal data, leading to identity theft. Awareness reduces this risk.

3. **Reduce exposure to malware:** Fraudulent links or attachments often contain malware. Understanding these tactics helps users avoid infection.

4. **Defend against emotional manipulation:** Fraudulent offers prey on excitement or urgency. Recognising these tactics allows users to pause and evaluate.

5. **Promote scepticism:** Learning about these schemes promotes a cautious approach to unexpected or unsolicited offers, reducing susceptibility to scams.

These four features described above are used in the challenge to create a scenario in which the user is presented with a short email and then asked if they think the

email received is safe or not. If the user does not think the email is safe, the user also needs to pick one of these features as a method of identifying the type of attack they think the email/message was. A list of short emails with errors was created. These emails were then categorised, assessed, and assigned a degree of difficulty. The following are four examples found in the list, and more examples are shown in Appendix C. This list was based on a dataset found on kaggle [2] a website that has various datasets available. The data were changed to remove any unwanted emails and make it relevant to the youth.

1.From: Amazon Security Team • **Email:** amazonsecurityteam11@notifications.net

- **Message:** Your account has been compromised. Click here to secure it: https://notifications.net
- **Safe:** No
- **Category:** Impersonation
- **Difficulty:** 4

2.From: Cathy3 Brown • **Email:** cathy3@notifications.net

- **Message:** Can you send me the report by tomorrow?
- **Safe:** No
- **Category:** Impersonation
- **Difficulty:** 2

3.From: Bank of America • **Email:** bankofamerica7@notifications.net

- **Message:** Urgent: Suspicious activity detected. Login to verify your identity: https://notifications.net
- **Safe:** No
- **Category:** Credential Harvesting
- **Difficulty:** 5

4.From: Cathy Johnson • **Email:** cathy@securemail.com

- **Message:** Can you send me the report by tomorrow?
- **Safe:** Yes
- **Category:** null
- **Difficulty:** 1

[2]https://www.kaggle.com/datasets/subhajournal/phishingemails

Figure 5.11: The email identification challenge

In the game a list of 200 fake emails was used to provide the user with emails. The user is then asked to determine whether the email is safe or not; if the user makes the correct choice, they are rewarded based on the difficulty of the email. The calculation and implementation of this challenge will be discussed in the following section.

5.3.3 Step 3: Build scenario and environment

The second challenge was created to follow the previous challenge. As the user closes the password creation phase of the first challenge, the user is provided with a new instruction page that briefly explains what to do in the challenge, as seen in Figure 5.11. It is explained to the user that they will receive a series of emails and need to decide whether the email is suspicious or not. If the user decides that the email is suspicious, they also need to decide in which category (described earlier) this email falls.

Some aspects of the previous challenge are used again, such as the scores that continue from the previous challenge without being reset to promote continuity. The timer is also reset, and the user has another two minutes to complete the challenge. In Figure 5.12 the first screen is shown after closing the instruction page. On this screen, the user is presented with the prompt “Is this email safe” and given a choice

Figure 5.12: A fake email given to the user to evaluate

between yes and no. If yes is selected and is correct, a base score of 25 is given and multiplied by the level of difficulty associated with the email; if the wrong answer is selected, a score of 0 is given. When the user selects no, indicating that they do not think this email is safe, the user also needs to choose the category to which they believe the suspicious email belongs, as shown in Figure 5.13. The scoring for this part starts the same as before, with 25 points being given for a correct no selection. A further 75 points are also given if the user chooses the correct category. This combined score is then multiplied by the difficulty assigned to the email. The score received for that email is then added to the total score in the top right of the screen, and a new email is provided to the user to analyse, as seen in Figures 5.14 and 5.15. In these figures, one can identify that the user has correctly analysed a fourth level of difficulty email and received a score of 400 added to their total.

In this section challenge two was designed to provide the user with a method where they can see example emails and how easy it can be to miss phishing attempts in emails. The objective is to improve users' awareness of their daily emails, enabling them to recognise any alterations that may indicate a suspicious message. The following section will look at the final challenge used in this study, that focuses on identifying different types of hacks based on the information received from short descriptions.

Figure 5.13: User selects that the email is not safe

Figure 5.14: Score before fourth level of difficulty email has been analysed

Figure 5.15: Score after fourth level of difficulty email has been analysed

5.4 "Cyber investigator" case files

For the final challenge, the user is presented with a small descriptive scenario detailing how an attack has affected a system, organisation or person. These are real-world attacks that have occurred, and the information can be found online at Jamcyber[3], a website that lists attacks that have occurred recently. The user must then use critical thinking to analyse and determine what type of attack was used to create the outcome. The Cyber Investigator activity challenges the user to analyse a scenario critically; this might also promote curiosity about the attacks that are experienced every day. In this section, the Cyber Investigator challenge will be explained in detail, and design strategies will be elaborated on.

5.4.1 Step 1: Identify goals and scope

The main objective of this challenge is to enable users to identify and classify information security threats based on a description of the scenario. This encourages critical thinking and exposes the user to real-world attacks. This exposure can have a positive effect because the user could realise the real risk associated with attacks. Below the proposed objectives are presented:

[3]https://jamcyber.com/discover/cyber-attacks/

1. **Enhance understanding of attack vectors:** By the end of the exercise, users should be able to correctly identify and classify common attack vectors, data breaches, ransomware, network intrusions, and system compromises with a success rate of 80% or higher.

2. **Develop critical thinking in incident analysis:** Users should demonstrate the ability to analyse the provided clues to pinpoint how an attack occurred, and articulate prevention strategies.

3. **Foster confidence in responding to cyber incidents:** By engaging in narrative-based incidents, users should feel more confident in identifying and addressing potential information security threats in real-world scenarios.

5.4.2 Step 2: Gather real-world insights

Real-world insights for this challenge were obtained by searching the Internet for the latest available attack information. The website Jamcyber has a list of malicious threats that are documented and categorised. There were 124 cases available that were used to create a dataset in the game. Real-world attack information from January 2024 to November 2024 was used. These cases were then categorised into five different types of hacks. The categories are: data breaches, network intrusion, ransomware, system compromise, and unauthorised access.

Data Breaches: Data breaches occur when sensitive information is exposed to unauthorised parties due to hacking, poor security measures, or insider threats (Jackson et al., 2019; Sarker, 2023). Understanding data breaches is critical to be able to:

1. **Protect sensitive information:** Awareness of how breaches occur helps users safeguard confidential data, such as financial records or personal details.

2. **Reduce financial and reputational damage:** Organisations and individuals suffer financial loss and reputation damage due to data breaches. Understanding these risks can help mitigate them.

3. **Promote proactive security measures:** Recognising vulnerabilities encourages the adoption of encryption, strong passwords, and secure authentication practices to prevent breaches.

4. **Help identify breach indicators:** Awareness enables users to detect signs of a breach, such as unauthorised access or unusual activity, and respond promptly.

5. **Support compliance with regulations:** Understanding data protection laws, such as the Protection of Personal Information Act (POPI Act) [4], ensures adherence to legal standards and reduces penalties for breaches.

Network Intrusion: Network intrusion refers to unauthorised access to computer networks by attackers looking to steal, modify, or disrupt data (Lam, 2021; Sarker, 2023). Recognising network intrusion is important to be able to:

1. **Prevent unauthorised access:** Understanding how attackers infiltrate networks helps users implement stronger security measures, such as firewalls and virtual private networks.

2. **Protect critical systems:** Detecting intrusions early prevents attackers from compromising essential infrastructure or sensitive information.

3. **Reduce spread of malicious software:** Many intrusions serve as entry points for malicious software. Awareness limits further infection and damage.

4. **Enhance incident response:** Recognising signs of an intrusion, such as unusual traffic or failed login attempts, allows users to respond quickly and minimise harm.

5. **Promote network monitoring:** Educating users about intrusion risks encourages regular monitoring of networks, ensuring proactive detection and prevention.

Ransomware: Ransomware is a type of malicious software that encrypts files and demands payment for decryption keys (Sarker, 2023; Temara, 2024). Understanding ransomware is critical to be able to:

1. **Prevent financial extortion:** Awareness of how ransomware spreads, such as through phishing emails, helps users avoid costly ransom demands.

2. **Protect data integrity:** Recognising ransomware risks ensures that users back up critical data regularly, minimising data loss.

[4] https://popia.co.za/

3. **Reduce system downtime:** Effective prevention strategies reduce the disruption caused by ransomware to operations or personal computing.
4. **Promote safe email practices:** Ransomware often spreads through malicious attachments or links. Educating users helps them identify and avoid such threats.
5. **Encourage layered security:** Awareness of ransomware risks promotes the adoption of strong antivirus software, firewalls, and patching practices to block attacks.

System Compromise: System compromise occurs when attackers exploit vulnerabilities to gain control over devices or systems (Bishop, 2018). Understanding system compromise is vital to be able to:

1. **Prevent loss of control:** Recognising signs of compromise, such as unauthorised changes or slow performance, ensures that users take immediate action to secure systems.
2. **Stop data theft or destruction:** Attackers often use compromised systems to steal or delete valuable data. Awareness helps users mitigate such risks.
3. **Minimize spread to other systems:** Compromised systems can act as launching pads for further attacks. Educated users limit damage by isolating affected devices.
4. **Promote patching and updates:** Many compromises exploit outdated software. Understanding these risks encourages regular updates to close vulnerabilities.
5. **Enhance forensic analysis:** Knowledge of system compromise indicators enables effective investigation and strengthens future defences.

Unauthorised Access: Unauthorised access refers to gaining entry to accounts, systems, or data without permission, often through weak passwords, stolen credentials, or exploits (Mijwil et al., 2023; Sarker, 2023). Understanding unauthorised access is essential to be able to :

1. **Secure sensitive accounts:** Recognising access risks helps users implement strong authentication methods, such as two-factor authentication.

2. **Reduce risk of privilege escalation:** Attackers often exploit unauthorised access to gain higher-level permissions. Awareness prevents this cascade effect.
3. **Protect against insider threats:** Unauthorised access is not always external; understanding internal risks improves overall security.
4. **Encourage password hygiene:** Many attempts at unauthorised access exploit weak or reused passwords. Educating users about strong password practices reduces this risk.
5. **Improve access control measures:** Learning about unauthorised access inspires better role-based access control and auditing of permissions.

These five categories were used as the selection choices given to the user. The user is presented with some information on an attack that has occurred; the user then needs to choose in which one of the five categories the attack falls. In the following section, more detail will be given on the process used to test this challenge.

5.4.3 Step 3: Build scenario and environment

The final challenge was created to spark some interest in what is really happening in the world. This challenge follows the second challenge, the score is added to the total score, and another two-minute timer is started. As the user completes the previous challenge, they are once again provided with a brief description of what is necessary for the next challenge, as seen in Figure 5.16. On closing the instruction screen, the user is confronted by the challenge screen, where they now need to decide what type of hack they think the scenario details were. As seen in Figure 5.17, Halliburton experiences an interruption of service. The user can then select his choice as seen in Figure 5.18, and based on whether the user is correct or wrong, they will receive or lose points in this challenge. The challenge has a streak system designed into the scoring system. The user will receive a base score of 25 points that is multiplied by the number of times the user was correct in a row; on the other hand, if the user was incorrect, they will lose 25 points from their total score.

The three challenges were specifically chosen to be used because they each had a different role to play in the creation of “Cyber Cadet”. The first two were there to provide some training in basic attacks, threats, and vulnerabilities that could be experienced by anyone, while the final challenge was chosen to allow the user to realise that these attacks are not just scare tactics and are happening everyday. In the next section, other gaming aspects used in “Cyber Cadet” will be discussed.

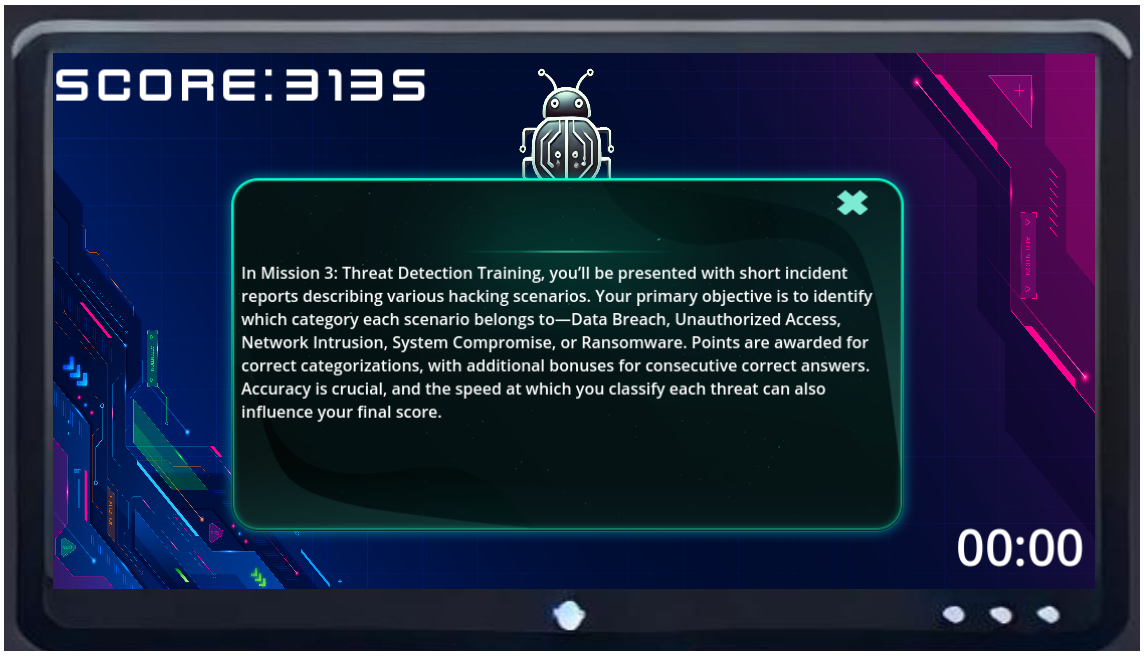


Figure 5.16: Hack analysis instructions

Figure 5.17: First screen for the hack analysis challenge

Figure 5.18: Hack analysis user selection

5.5 Other gaming aspects

This section will give an overview of the final screen that the user receives, and the other gaming aspects used will be discussed, focusing on why it was important to use these aspects in "Cyber Cadet". These aspects are a feedback system, time pressure, and a scoring system. Each of these systems has a specific goal in the design of "Cyber Cadet". This is important to make the serious game an effective gaming tool. With these aspects being used in "Cyber Cadet", a user is provided with an effective simulated environment to experience all the threats of cyberspace.

Feedback system: As discussed in Chapter 4, an effective feedback system is important because it allows the user to learn from what they played (Ghani, 2015). The feedback system in "Cyber Cadet" was designed to give subtle changes to the score as the user plays the game and then in the end give a detailed description on how the user performed in each challenge. This is achieved by keeping track of how the user performed in each challenge. In Figure 5.19 the user receives a detailed analysis and feedback on what they achieved during "Cyber Cadet". The screen is divided into four different sections, each focusing on one of the activities that the user had to complete. The first section takes a closer look at how the user performed in the password analysis part of the challenges. The score achieved for the password analysis part alone is given with a possible score. A percentage

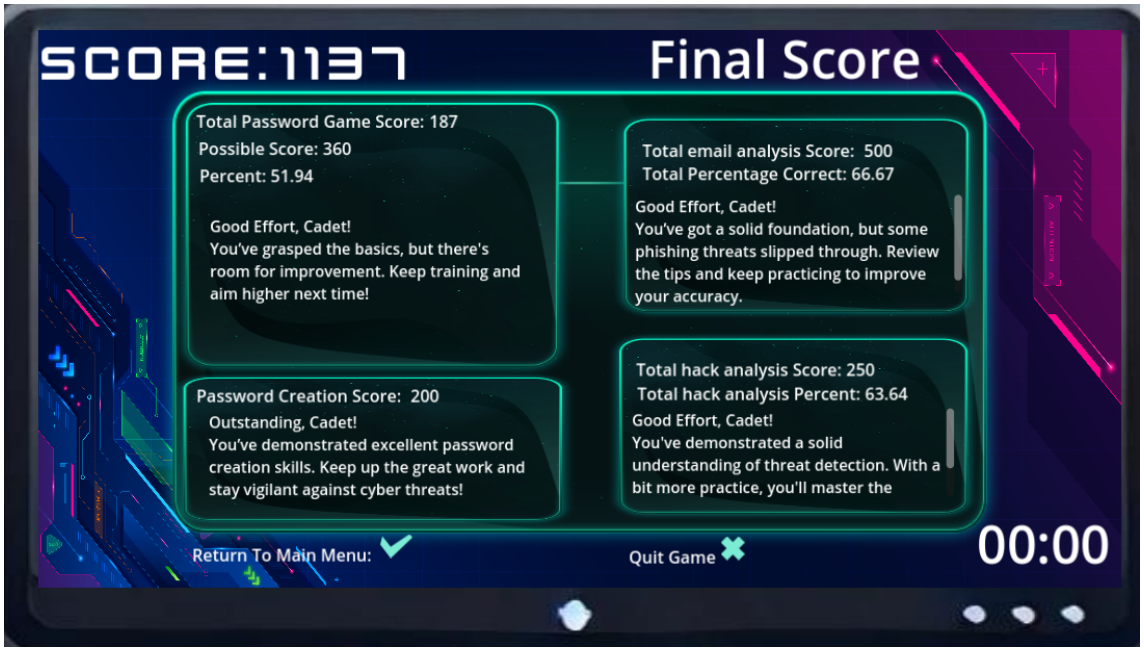


Figure 5.19: The final feedback screen

is also displayed that gives a good understanding of how well the user did in the challenge; by adding this to the result, a user is discouraged to just guess each password score without proper analysis. The second section provides the user with their score achieved for the password creation task. The third section provides an overview of the email analysis score, and the final section does the same for the hack analysis score. Adding the percentage was done to discourage a user from just trying to guess, encouraging the user to use critical thinking to complete the game.

Scoring system: The scoring system in "Cyber Cadet" was designed to create a clear progression indicator while the game is being played by continuously displaying the score and updating the score for every allocated point. This provides the user with their progression and continues the feedback that is important for a game to be effective as shown in Chapter 4. The scoring for each game was described in detail earlier in this chapter. In short, each challenge has a different scoring system to challenge the user in different ways. These different methods are used to keep the user engaged.

Time constraint: The time constraint found in "Cyber Cadet" is a set of three two-minute timers for each challenge. This constraint is intended to impose a time limit, prompting the user to work quickly and efficiently. This is implemented to create a experience similar to the pressure, as highlighted in Chapter 4, that

occurs when an attack is successfully perpetrated. In this case, whether personal or organisational, the attacked entity will quickly try to fix the problem and block any further misuse. This can be done by changing the password, or in extreme cases, switching off the service until a fix is found.

5.6 Summary

In this chapter, the process of choosing, researching, and designing effective simulation experiences was described. The three challenges: password analysis and creation; email analysis; and hack analysis, were clearly defined with goals and objectives to be achieved within "Cyber Cadet". The game was then designed with the focus on achieving these outcomes. But it is important to note that to create an effective serious game, it should also focus not only on the learning objectives, but also on the effective gaming aspects. These aspects need to create a flowing game in which the user is engaged with the content while also learning from what is experienced. This is a critical step in serious game design and only if these two aspects are correctly balanced will it create an effective learning tool (Charsky, 2010).

The next steps shown in the scenario creation flow chart in Figure 4.1 (page 50) are to test and refine, deliver and improve. The following chapter will focus on the processes associated with the testing phase within the Design Science Research Process.

Chapter 6

Game evaluation and results

The goal of the study was to determine whether a simulated experience serious game, called "Cyber Cadet" could positively promote information security awareness among the youth. The serious game was designed with three challenges included: these challenges are a password creation and analysis challenge focusing on secure password practices, the "Phishing" inbox challenge focusing on email safety, and the "Cyber Investigator" case files scenario challenges that focus on exposing the user to real-world incidents. As discussed in Chapter 1, to effectively evaluate an artefact, it needs to be presented to people to test. As seen in Figure 1.1 page 7, there are three phases after the design and development phase: which are demonstration, evaluation and communication. In this chapter, demonstration and evaluation will be discussed pertaining to "Cyber Cadet".

In this research, the demonstration and evaluation phases were done in two sessions. The first was a pilot study in which a smaller group of individuals tested the game to provide crucial feedback on the design elements and advice on improvements that could be made. After the pilot study, the game was modified, taking into account the feedback provided by the test group. After the changes had been made, a second testing phase was done. This was the final evaluation phase of the study, and was sent to various parents, teachers, and industry experts to test and review the game. The choice of first using adults was made to ensure that the information being presented is deemed suitable for the youth; this opens the possibility for future work to build on the findings and create a refined game that can be tested by the youth.

6.1 The pilot study

For the initial demonstration phase of the study, a pilot study was conducted by sending the game to a small group of people. This group consisted of eight people selected from different categories, namely parents, teachers, and industry experts. This study group received an early version of "Cyber Cadet" and were asked to complete a questionnaire related to the game. The questionnaire is provided in Appendix D. The aim of this pilot study was to get relevant feedback related to the experience, flow and gameplay of "Cyber Cadet". The participants were asked a set of questions related to these elements. The questions as well as the responses will be discussed in this section.

Question:"Are there any other topics you consider should be included in this game? Please name them."
Six out of the eight replied none or left no response, thereby indicating that at this stage of the game the content of the game was generally considered to be sufficient. One of the participants expressed the need for more advanced concepts for the above-average user as seen below.

P2: *"Yes. Identification of threats for "advanced users". The dangerous user that thinks he knows something."*

The last participant did not answer the question; instead making a comment related to a later question asked. With that, it was concluded that no new challenges needed to be added to the current state of the game and the focus should instead be on improving those that were already in "Cyber Cadet".

Question: "How engaging was the game's storyline?"
As seen in Figure 6.1, seven of the e participants gave the initial storyline 4 and above out of 5 while one participant gave 3. It could subsequently be deduced that the storyline was good as is for the current phase of the research, and no changes where made to that aspect of "Cyber Cadet"

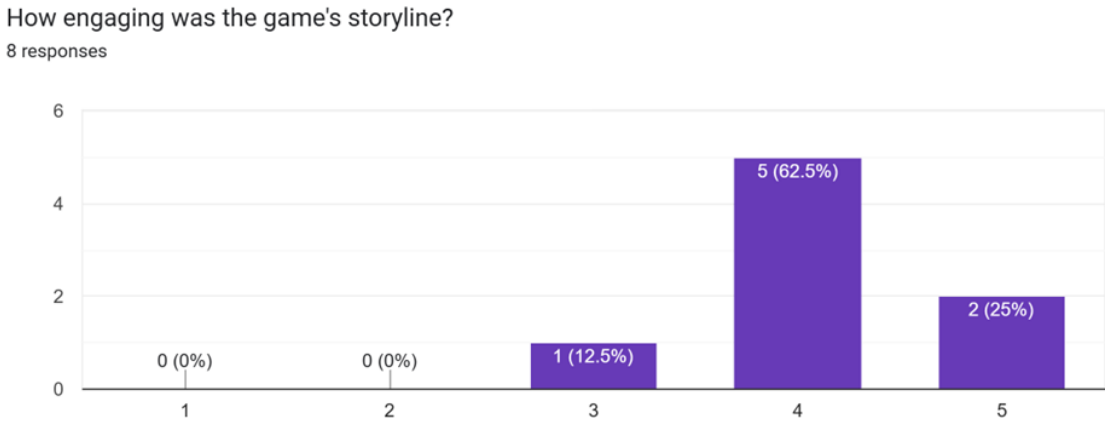


Figure 6.1: Engagement level of the storyline

Question: "Were the game objectives clear?
The next relevant question asked was whether the game objectives were clear and easy to follow. six out of eight gave the maximum score as seen in Figure 6.2 indicating that they felt the objective was clear. No changes were made to the objectives of the game. There was a person who gave the clarity of objective only a 2 out of 5. This could indicate that if one is not quite comfortable with a computer or with gaming, the objectives might not be clear.

Question: "Rate the effectiveness of the game's challenges and tasks in maintaining your interest."
This question was asked because for a serious game to be effective, players need to be engaged in the content of the game. If the content is boring or is seen as a chore, the players will lose interest and will not focus on the learning that can be achieved. As seen in Figure 6.3, seven of eight participants gave the initial state of the challenges an 4 or higher. The deduction can thereby be made that for the current state of the game the challenges are relevant and effective.

Question: "What suggestions do you have to improve the game's effectiveness in teaching information security awareness?"
This open ended question was asked to get some general feedback on the game and any changes that might be required. As shown below, the participants had some suggestions to improve "Cyber Cadet".

P1: *"Improve readability, size of text in scenarios is too small, which takes more time to read than answer."*

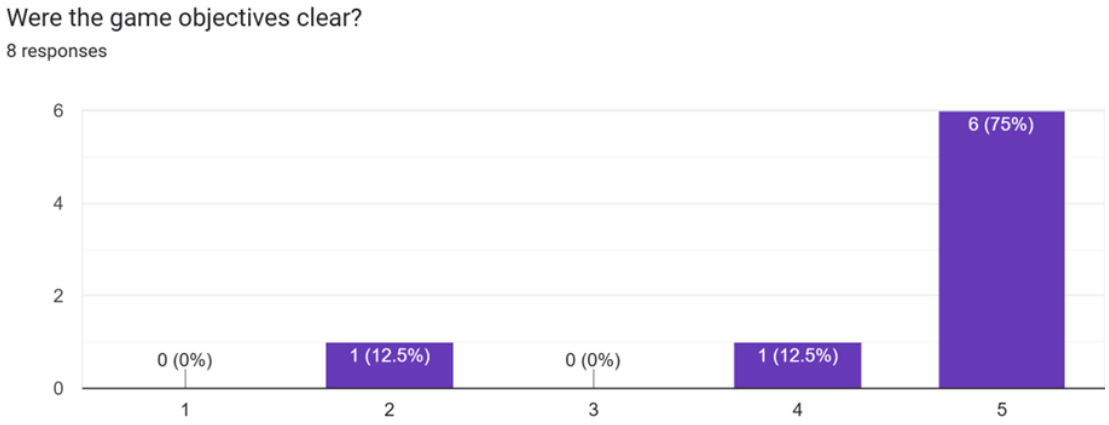


Figure 6.2: Clarity of objectives

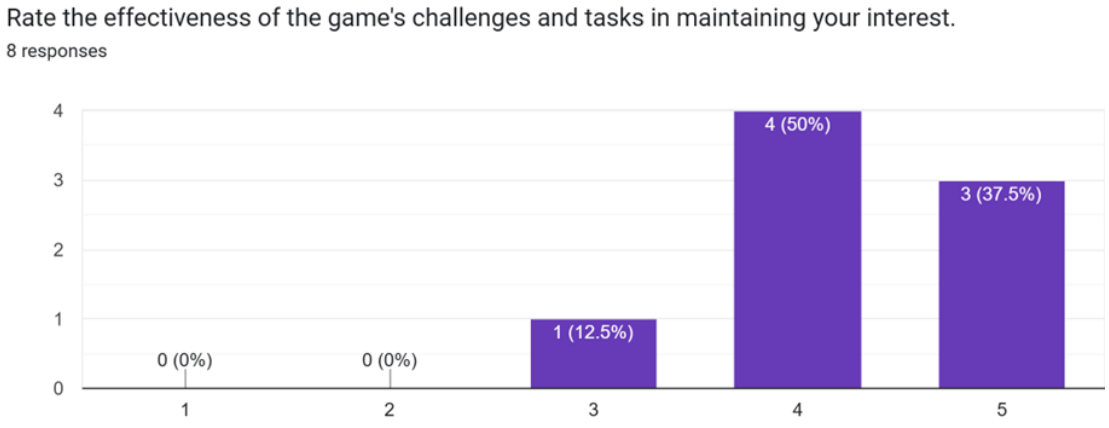


Figure 6.3: Effectiveness of game challenges

P2: *"Make the Introduction and instructions shorter and maybe expand the window to make it larger and clearer."*

P3: *"Extend the given time limit."*

P4: *"None."*

P5: *"None, the game draws attention well."*

P6: *"More time given to study the scenarios."*

P7: *"Give more feedback and learning opportunities. Also add some real valid emails to the email part. All of them were suspicious-looking ones. Most places will NOT ask you to log in using a link unless you asked for a link, in which case they will state that you did ask, and if you didn't, don't click."*

P8: *"Maybe a retry button?"*

Addressing this feedback, some changes were made to "Cyber Cadet".

- The instructions and the information on information security awareness were moved out of the gameplay loop and added to a main menu page called the game guide. This change can be seen in Figure 6.4, showing the instruction before each challenge and in Figure 6.5, showing the instructions as part of the game guide. The change was made to make it easier to read the instructions and also to create a space where information security awareness can be documented and read. This change was made to make the content of the game clear and also to promote information security awareness by providing the player with a reason to why it is important to understand password security, email security, and know about real-world incidents. Figure 6.6 shows the start of one of the sections that gives information on the importance of information security awareness.

- The next item to consider was the possibility of extending the time allocated to the challenge. The decision was made not to adjust the time. As discussed in Chapter 4, time pressure is an effective gamification method that creates a sense of urgency. By putting the player under this time pressure, they would need to adapt and learn to spot the key identifiers in the challenges, which promotes learning and effective identification of the attacks.

- The pilot feedback system only provided the user with a final score after completing all the challenges. A new feedback system was designed to provide

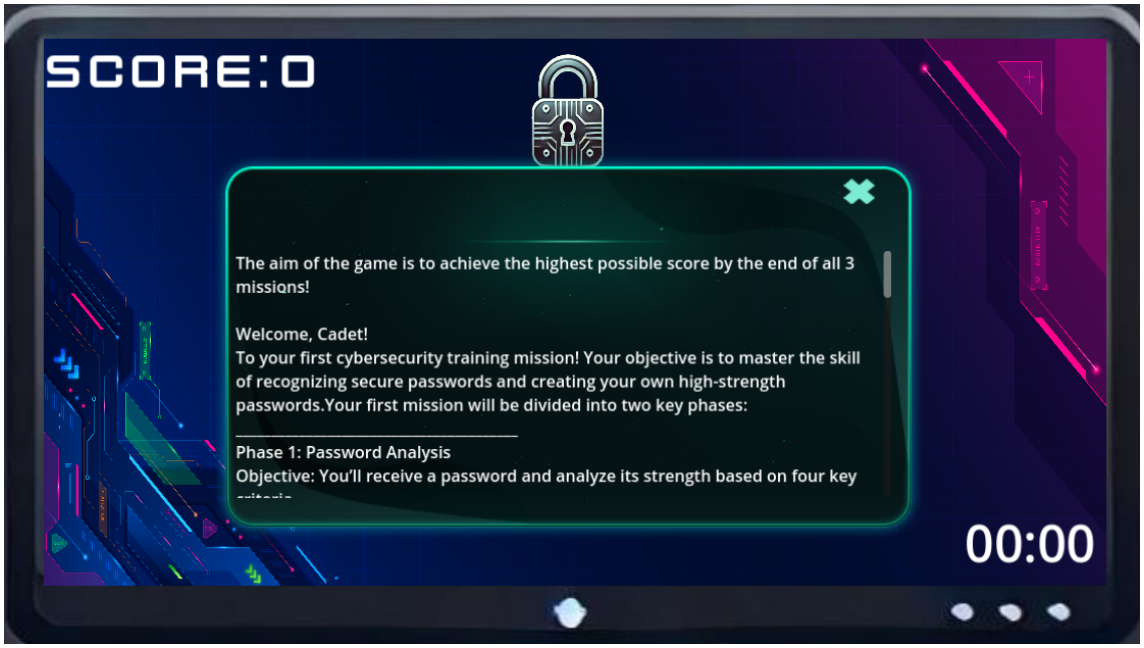


Figure 6.4: Instruction in the gameplay loop before moving to the game guide

the player with a detailed analysis of how they did in each challenge. This was done by giving the player feedback on each section and testing how they performed in those specific sections. This is shown in Figure 5.19

- A retry button. The choice was made to add "quit game" and a "return to the Main Menu" button to the final page to allow the user to exit the game if they wanted or to go back to the start and try again.

This initial pilot or demonstration phase of the DSRP is an important step to ensure that the quality of the final iteration is good and focused on the objective. This phase allows the researcher/developer to gain some outside perspective. This outside perspective is good for various reasons including a fresh take on the objective, an overview of effectiveness, and a critical eye on what changes need to be made to make the artefact reach the required level of effectiveness and engagement. After the pilot study, changes were made to "Cyber Cadet" before it was sent again to the reviewers for final evaluation and feedback.

6.2 Evaluation of research

In this section the data collected from the "Cyber Cadet" Questionnaire will be examined. This questionnaire evaluates the effectiveness of the game in improving

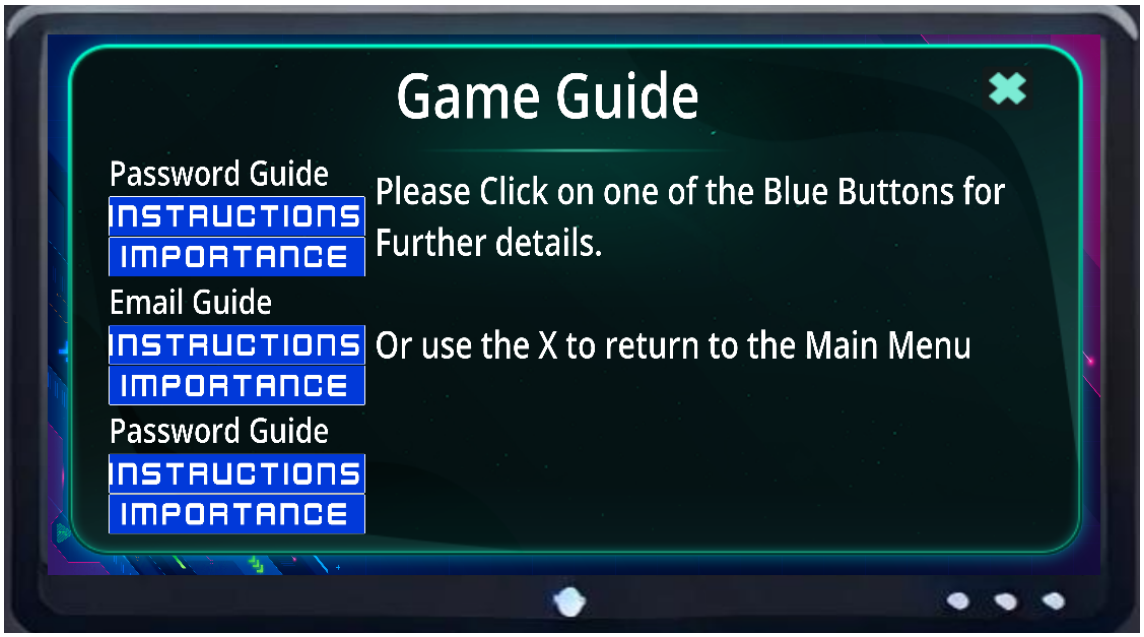


Figure 6.5: Instructions found in a separate game guide

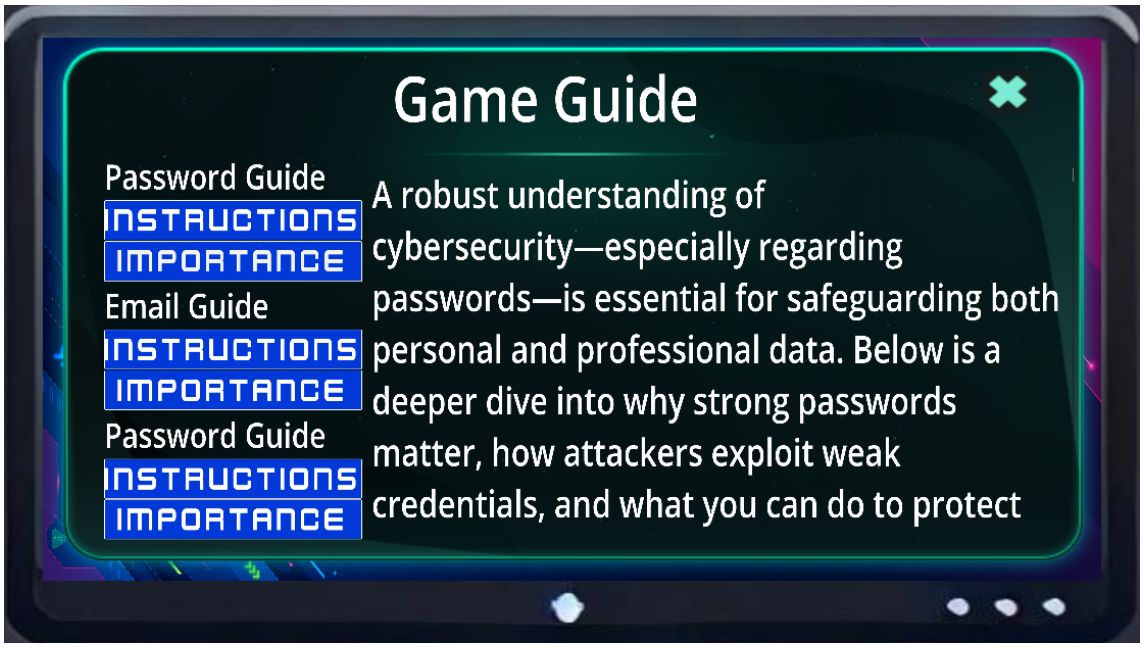


Figure 6.6: Example of important information being shared

Population	n=25				
Gender		**Cybersecurity Experience**		**Level of education**	
Male	44.00%	Novice	16.00%	Matric or Lower	8.00%
Female	56.00%	Moderate	52.00%	Certificate	20.00%
		Good	28.00%	Degree	36.00%
		Excellent	4.00%	Honours	32.00%
				Master +	4.00%
Age		**Groups***			
19-35	48.00%	Parent	48.00%		
36-60	44.00%	Teacher	52.00%		
61+	8.00%	Industry Expert	20.00%		
		Gaming Enthusiast/Expert	28.00%		
*A person can belong to of more than one group					

Table 6.1: Demographics of participants

information security awareness and is shown in Appendix E.

6.2.1 Demographic data and result analysis of the participants

A total of 25 participants reviewed the game. Table 6.1 provides an overview of the demographic composition. In addition, each participant was classified into one or more of the following categories: parent, teacher, industry expert, and gaming enthusiast/expert. These categories are highlighted below:

Parents: They have a close relationship with their children and care about the safety of their child;
Teachers: They have to educate and nurture the youth, creating valuable additions to society;
Industry experts: To evaluate the validity of the concepts being covered; and
Gaming enthusiast/experts: To evaluate the game design aspects of "Cyber Cadet".

Within this set of participants, 56% were female and the other 44% male. An interesting finding was that male participants performed better across the board, but specifically in the email analysis challenge as seen in Table 6.2. This could be a finding that can be further investigated, but will require a much larger population to effectively test. Participants were also asked to indicate their age category, with

	Phishing Challenge	Email Challenge	Hack Challenge
Female	51.98	41.54	59.51
Male	54.93	62.67	66.34
Average	53.28	50.83	62.52

Table 6.2: Average percentage correct for each of the three challenges for males and females

	Phishing Challenge	Email Challenge	Hack Challenge
19-35	51.45	55.85	62.52
36-60	58.60	48.89	63.37
61+	35.00	31.43	57.78
Average	53.28	50.83	62.52

Table 6.3: Average percentage correct for each of the three challenges for the different age groups

48% being 19-35, 44% being 36-60, and 8% being 61+. Some findings related to age were that those over the age of 60 generally did the worst in all three challenges, this as a result of various factors such as not being as tech-savvy as other participants. As seen in Table 6.3 for the password analysis challenge, the group between 36-60 did the best. A possible deduction can be made that these individuals had the opportunity to grow alongside the growth of technology and they had to learn how to securely use passwords. The younger generations are quickly moving towards using tools to manage their passwords.

Table 6.4, presents the percentage for each of the challenges according to the level of education of the participants. Some outliers were Master's and Higher, who got a poor percentage for the password challenge at 13.33%. This outlier does not accurately portray the effectiveness of these participants as only one participant had that qualification.

Another comparison that can be made would be to compare how the different participant classifications performed. In Table 6.5, the four categories (parents, teachers, experts, and gamers) can be compared. The gamers did best in the password challenge while the experts had the lowest score. For the email analysis challenge, the industry experts did the best and the parents had the lowest score. This could be interpreted as a solid argument for this study as these industry experts might have

	Phishing Challenge	Email Challenge	Hack Challenge
Certificate	59.36	35.54	50.35
Degree	53.82	64.04	67.84
Honours	55.42	50.20	66.65
Masters+	13.33	42.86	55.56
Matric or Lower	47.07	36.14	55.95
Average	53.28	50.83	62.52

Table 6.4: Average percentage correct for each of the three challenges for the different levels of education

	Phishing Challenge	Email Challenge	Hack Challenge
Parent	56.22	45.34	61.12
Teacher	50.31	51.59	66.09
Industry Expert	47.69	66.35	65.80
Gaming Enthusiast/Expert	57.36	57.51	61.64
Average	53.28	50.83	62.52

Table 6.5: Average percentage correct for each category

had more experience with these types of email and have learnt by doing. In the final challenge the teachers scored best and the parents had the lowest score, but the final challenge was closer between the different categories than the other two.

This demographic information is important to interpret because it could lead to a deeper understanding of the challenges faced around these topics. However, to effectively use these results, the number of participants would need to be increased to provide a better overview of each of these categories. In the next section"Cyber Cadet" is evaluated on the effectiveness of achieving information security awareness and the principles of game design.

6.2.2 Information security awareness and game evaluation

The evaluation of "Cyber Cadet" with regard to information security awareness and game design is an important step in the DSRP because it provides the developer/researcher with the necessary information to improve the experience and ultimately test whether the objective of the investigation was achieved. In this section, par-

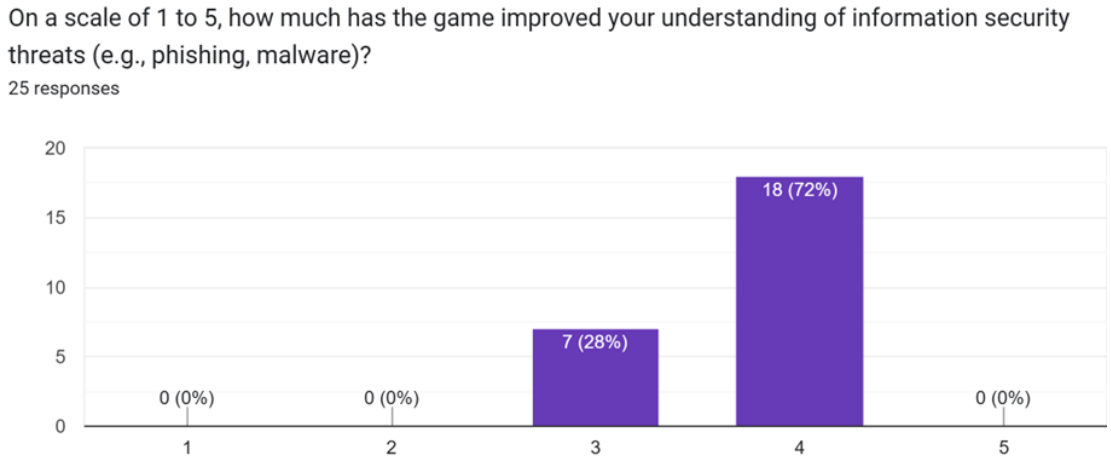


Figure 6.7: Improvement of understanding among participants

ticipants were asked to complete a set of questions based on their experience while playing "Cyber Cadet".

Question: "On a scale of 1 to 5, how much has the game improved your understanding of information security threats (for example, phishing, malware)?"
Participants were asked this question to identify whether they felt their understanding of information security threats had improved by playing the game. As seen in Figure 6.7, most of the participants felt that "Cyber Cadet" had improved their understanding with 72% giving this question 4 out of 5. The other 28% gave it a 3; this could indicate that for the majority of people "Cyber Cadet" would be efficient but could still require some improvements to get the participant to rate it 4 or 5.

Question: "How confident do you feel about identifying potential information security risks after playing the game?"
The next question focused on whether the participants felt they had received enough information to confidently apply it in real-world scenarios. In Figure 6.8 most of the participants once again gave "Cyber Cadet" a 3 (48%) or 4 (44%) out of 5. This could indicate that the information presented was effective for the general participant. Two (8%) participants gave a 2 out of 5 that could indicate that these challenges needed some more adjustment to properly provide the information.

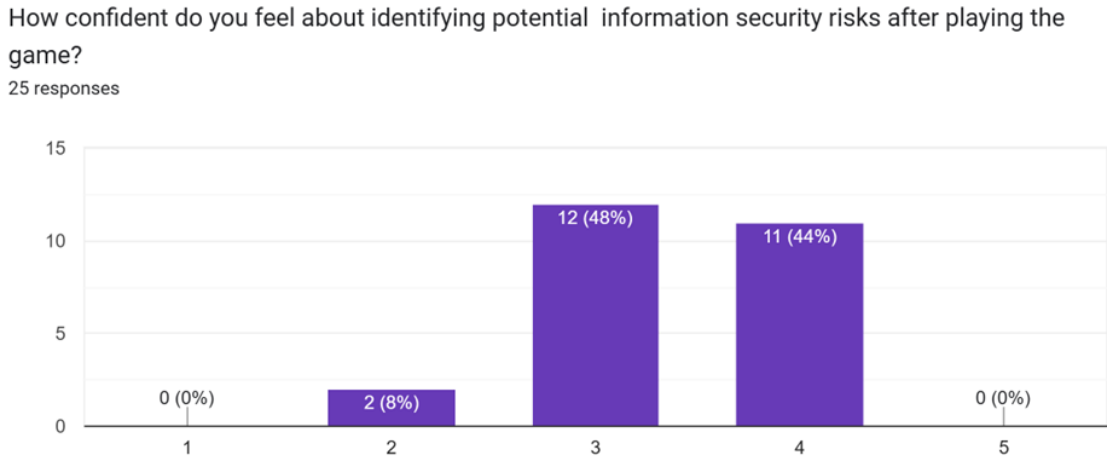


Figure 6.8: Confidence in identifying threats

Question: "Which, if any, of the threats experienced in the game have you also experienced in real life? Please name them; otherwise just reply "none"."

The next question was to gauge whether the participants had any experience with threats in the real-world. In Figure 6.9, the responses were grouped into categories, to give an overview of the feedback from the participants. These categories comprised anything related to email phishing and fraud, malicious software, and others included the rest of the replies like password weakness, etc. Of the participants, 35.3% experienced phishing, while 15.7% participants indicated that they experience fraud-related threats and 9.8% malware-related threats, and 39.2% of the participants experienced other threats. This highlights the need for effective email security and awareness.

Question: "How engaging was the game's storyline?"

This question was asked to determine whether the gameplay design centred on a storyline was engaging and interactive. Did it create interest in the objective of "Cyber Cadet", and did it keep the participant focused on what needed to be done. In Figure 6.10 one can see that 44% of the participants felt that the story was 4 or 5 out of 5. That shows that some participants felt that engagement was adequate. The other 66% gave "Cyber Cadet" a 2 or 3, indicating that the story would need some adjustments to be truly effective, especially in the case of the three participants who felt it was only a 2 out of 5.

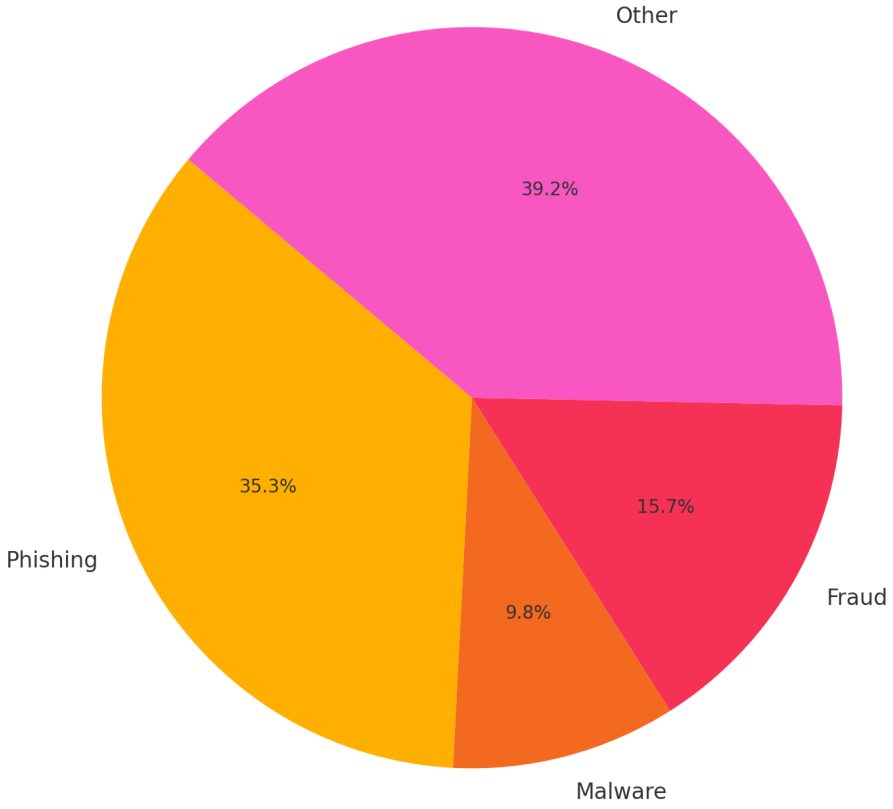


Figure 6.9: Threats experienced

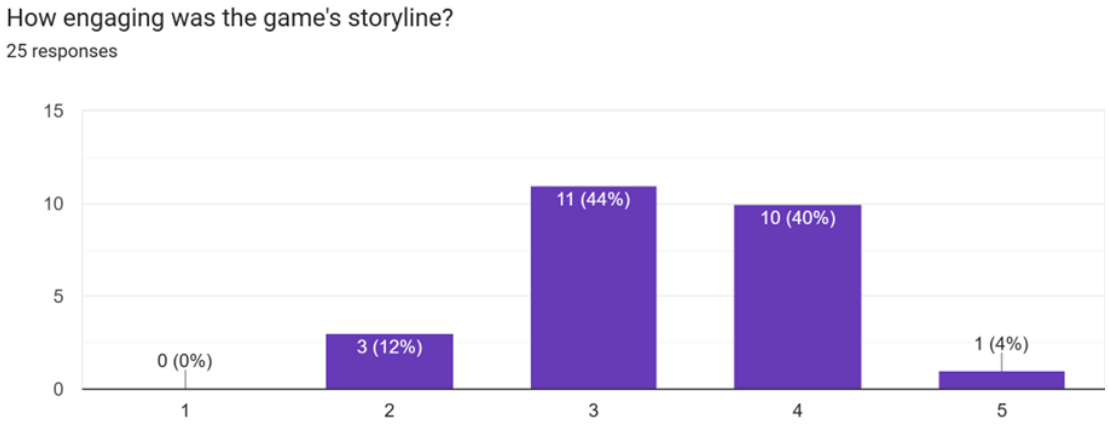


Figure 6.10: Engagement of the story

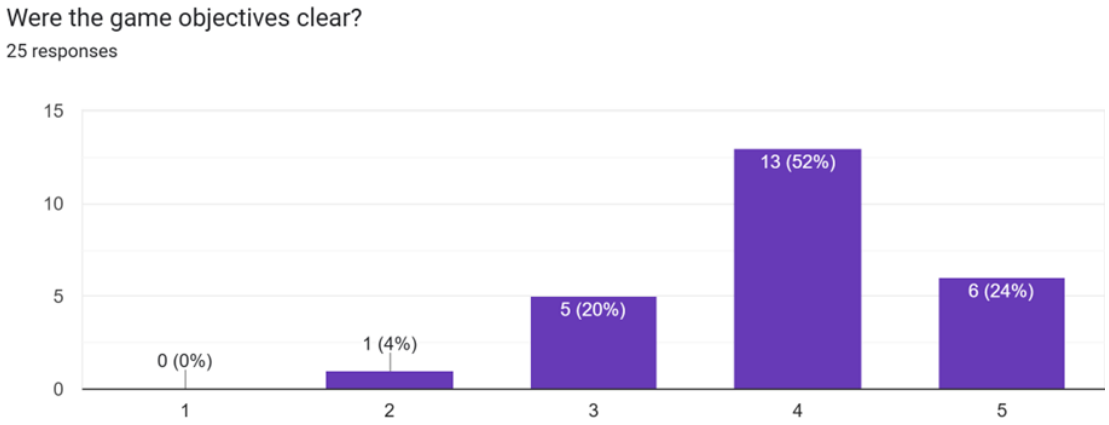


Figure 6.11: Are the objectives clear

Question: "Were the game's objectives clear?"
In the next question, participants were asked if the objectives were clear. With 76% giving the game and 4 or 5 out of 5 as seen in Figure 6.11, one can safely assume that the objectives of the game were clear and the users generally knew what to do to continue the game. Only 1 participant gave the objectives a 2 out of 5. Overall a deduction can be made that the objective were adequate.

Question: "Rate the effectiveness of the game's challenges and tasks in maintaining your interest."
The participants were then asked to rate how effective the game is at keeping the participants interest. As highlighted earlier, for a serious game to be effective, a player needs to be interested and engaged in the content, and thus learn by doing. In Figure 6.12 the result can be seen, and the participants generally feel that the game maintains enough interest.

Question: "Did the game's design elements (graphics, interface) enhance your learning experience?"
Based on the previous question, participants were also asked to rate elements of game design, such as the user interface and feel of "Cyber Cadet". As seen in Figure 6.13, most of the participants (92%) felt that these elements were adequate.

Question: "How realistic were the scenarios and situations presented in the game in depicting real-world information security issues?"
The participants were then asked if the challenges that were used were realistic enough. As seen in Figure 6.14, most of the participants felt very positive about the

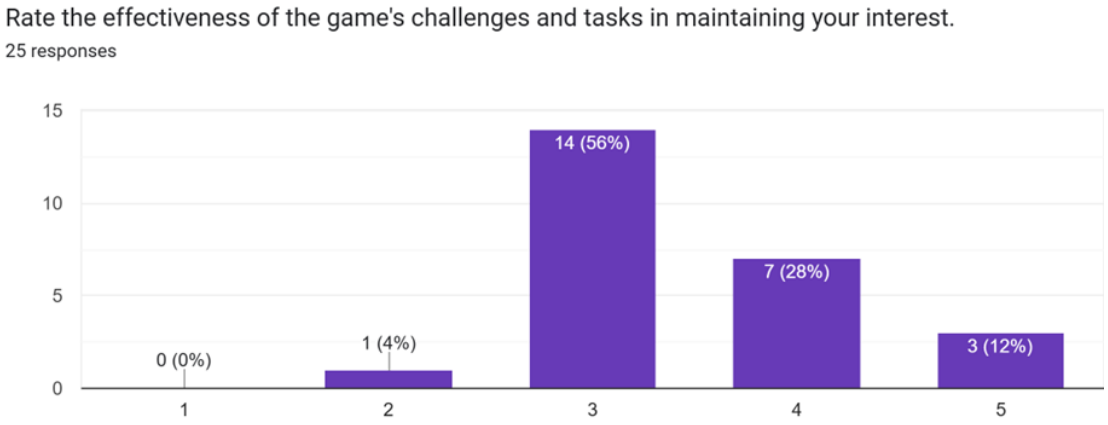


Figure 6.12: Effectiveness of keeping interest

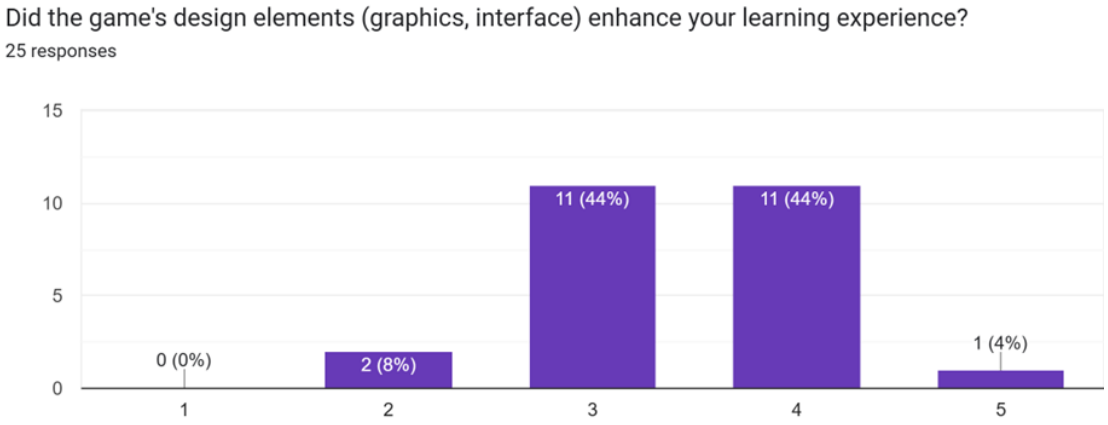


Figure 6.13: Rating of game design elements

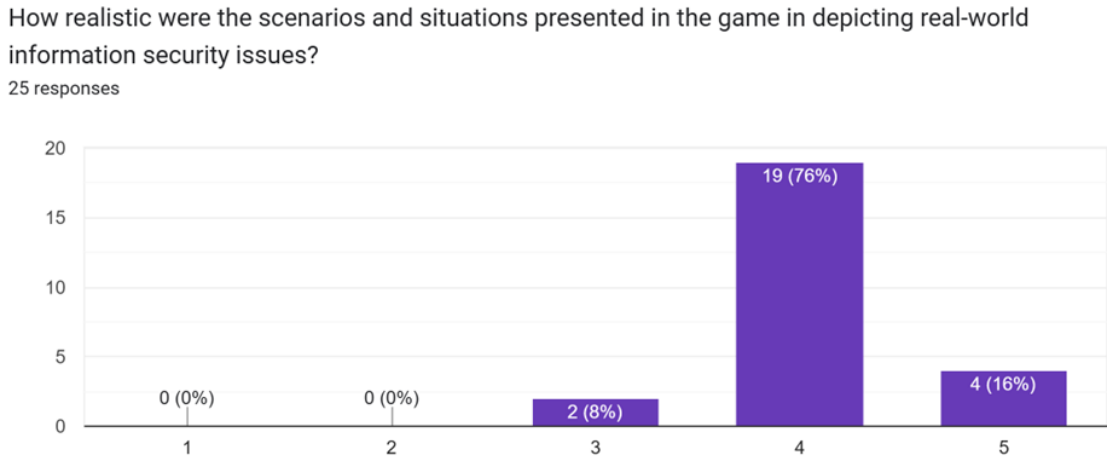


Figure 6.14: Realism of the challenges

realism introduced in "Cyber Cadet" as 92% gave the game 4 or 5 out of 5.

Question: "Did the game allow you to apply information security knowledge in simulated situations?"
Building on the previous question, the participant was also asked if the game allowed the participant to apply what they had learnt or already knew. In Figure 6.15, the participants generally indicated that the game adequately allowed the application of learnt or current knowledge as 60% gave the game 4 out of 5.

Question: "How well do you think the simulated experiences prepared you for handling actual information security threats?"
With the final question of this section, participants were also asked how well the game prepared them for actual information security threats. Most indicated that they were better prepared, as seen in Figure 6.16, with 88% indicating that the game had a positive effect on their preparedness.

In this section, participants were given the game to play and then asked to evaluate the game based on a series of questions. These questions were designed to clarify the effectiveness of the game in achieving the objective stated in the design. The general perception of "Cyber Cadet" was positive, with a high percentage of responses for each question being 3 out of 5 or higher in each of the questions. This could indicate that "Cyber Cadet" was successful in achieving the objective of promoting information security awareness. A deeper explanation on the findings will be discussed in Chapter 7 where the conclusions will be presented. In the next section, participants

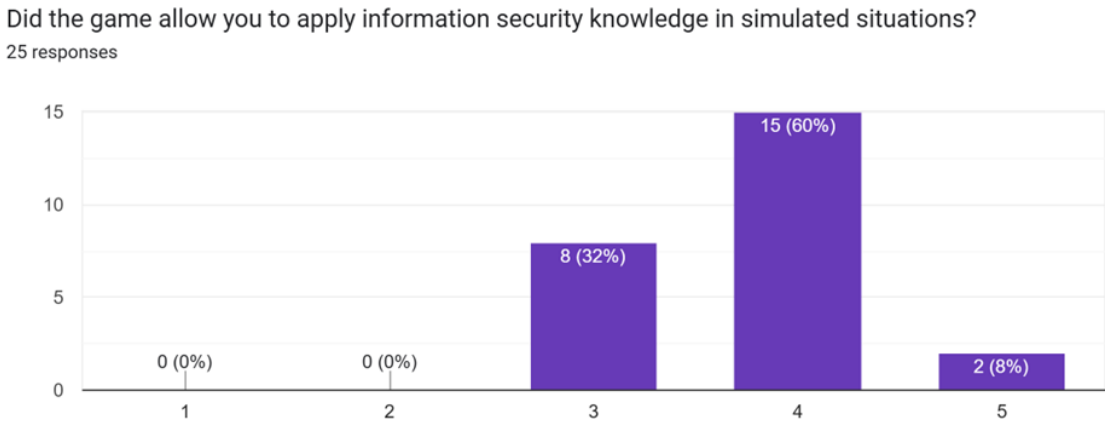


Figure 6.15: Allow applying information security knowledge

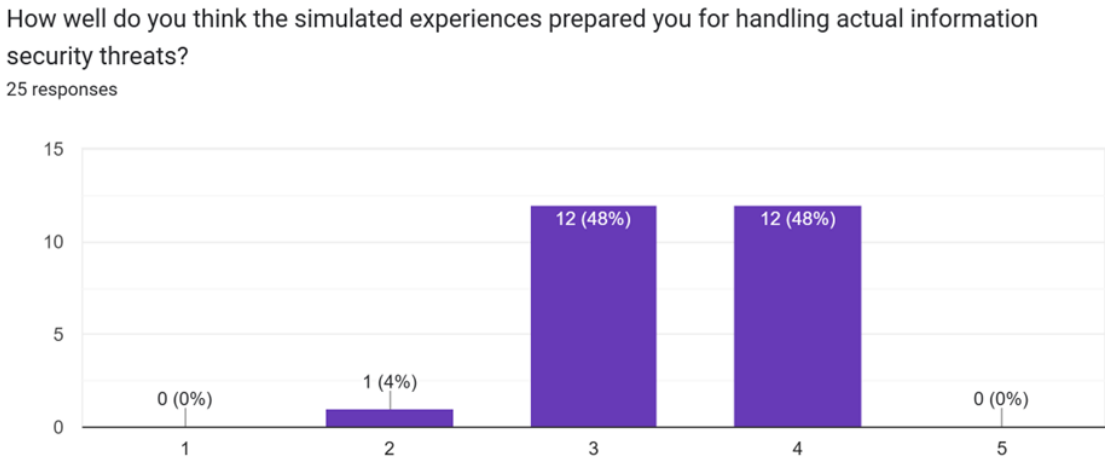


Figure 6.16: Preparedness for information security threats

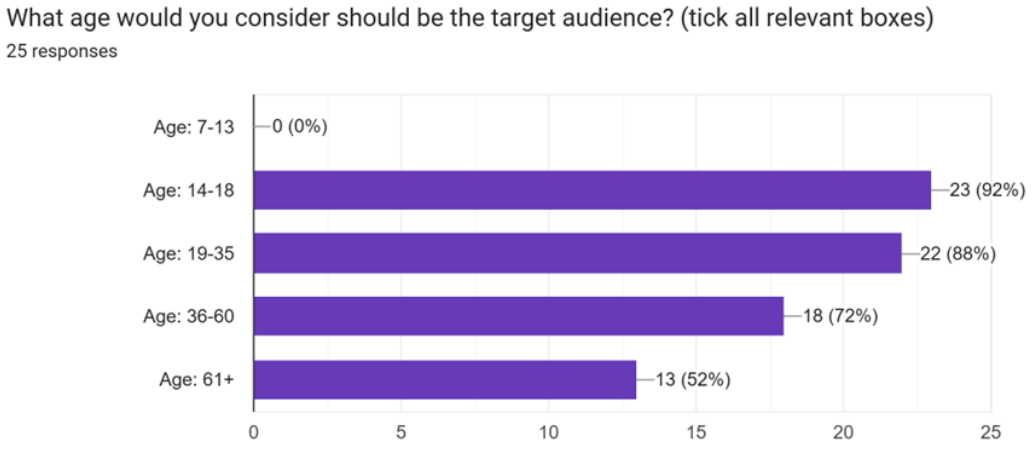


Figure 6.17: Age of target audience

provide feedback on "Cyber Cadet".

6.2.3 Participant feedback

For this section, participants were asked to indicate the age for which the serious game would be suitable and to provide general feedback on improving the game. In Figure 6.17, it can be seen that no participant felt that the game was suitable for anyone under the age of 13 years. This is an indication that this might be too advanced for that age group. The participants also felt that the game could be adapted to all the other age groups, with 92% believing that the 14-18 year olds are the optimal target audience. It should also be noted that one participant could choose multiple of these age groups, so the percentage is for all 25 participants. A general observation can be made that the majority of the participants felt that "Cyber Cadet" could be used to teach all ages older than 14 about cyber threats.

Some other feedback provided by the participants was largely based on the gamification elements that needed to be improved, as shown below. This feedback is important because these gaming elements will improve the general outcome of the game, and in turn improve user engagement, and also promote better information security awareness.

P1: *"Maybe make the game have a more detailed story"*

P2: *"Include Home network security and port forwarding mistakes"*

P3: *"maybe make it a more story driven challenge"*

P4: *"It would be interesting to add a voice over to read the instructions due to people not reading."*

P5: *"Extending the time"*

P6: *"Some more teaching mechanics that is not just reading instruction before playing the game, maybe a tutorial."*

P7: *"Move the focus to teaching and not self directed learning."*

P8: *"The challenges need to be expanded on to provide better understanding. An example would be to add more complex passwords to analyse"*

P9: *"Music and game sounds"*

P10: *"I believe the game would benefit from more gaming aspects."*

P11: *"Better guidance with the game"*

P12: *"Bit more time"*

P13: *"Use phases i e 123 in initial explanation "*

P14: *"More detail"*

P15: *"Better explanation on what to do"*

P16: *"More topics and a better gameplay loop"*

P17: *"A better feedback system that clearly indicates the score received for the previous analysis in all three games"*

P18: *"Better descriptions for the hack analysis "*

The above list indicates some of the verbatim feedback of participants - indicated by **Pn**. This can be taken into account for future changes to the game.

6.3 Summary

In this chapter, the game was tested and evaluated on two occasions, once by a smaller pilot group and a second by a larger selection of specific participants. These steps were used to effectively evaluate "Cyber Cadet" and get relevant feedback from the participants in both cases. Feedback was discussed and reflected upon with a focus on whether "Cyber Cadet" achieved the result of promoting information security awareness. The general results of both evaluation phases were positive and indicate that "Cyber Cadet" did indeed achieve the objective. In the following chapter, a conclusion will be presented. This will be done by ensuring that the study has achieved the research objectives and used the DSRP effectively.

Chapter 7

Conclusion

The purpose of this study was to create a serious game that promotes information security awareness. Simulated experiences were incorporated into the serious game. In order to achieve the desired result, the Design Science Research Process was used to guide the study. A detailed literature study on information security, serious games, and simulated experiences was conducted to identify key elements required to create an effective serious game that uses simulated experiences to promote information security awareness. The artefact: "Cyber Cadet: Threat Defender" was designed as a serious game using these key elements. The evaluation of the effectiveness of the game was conducted by reviews.

In Chapter 1, the background of the study was given as well as an overview of the problem, the research question and secondary research questions, aims and objectives, and an overview of the DSRP followed during this study.
Chapter 2 provided an overview of information security and the threats associated with cyberspace.
Chapter 3 focused on serious games and and their core elements.
Chapter 4 then provided a thorough literature study on simulated experiences and how to effectively implement these simulations in a game.
Chapter 5 provided the design elements of the game and the challenges found in "Cyber Cadet".
Chapter 6 presented the evaluation of the game, first summarising the pilot study and then providing feedback and results of the evaluation of the final game. These results indicated that "Cyber Cadet" using simulated experiences is an effective tool to promote information security awareness.

In the current chapter a summary of the study is given with a focus on evaluating the research objectives, evaluating the research process, pointing out the contribution that this study adds to the current body of knowledge, discussing the limitations of the study, proposing recommendations and finally presenting the possibilities of future work flowing from this study.

7.1 Evaluation of the research objectives

In order to answer the research question "How can a serious game utilising simulated experiences promote information security awareness among the youth?", five objectives were identified. In this section, an overview is given of how each of these objectives was achieved.

To obtain an understanding of recent cyber attacks
The first objective was to identify recent cyber attack trends that can be used in serious games to simulate real-world events. These cyber attacks could be identified from the literature and other sources of information. This objective was reached by conducting a literature review as shown in Chapter 2 and Chapter 4 (Sections 4.1 and 4.2). These cyber attacks were incorporated into the serious game in Chapter 5 as challenges to the players.

To obtain an understanding of existing simulated experiences and how they can be implemented
This objective was to identify simulated experiences and learn how they can be used in a serious game. This objective was reached in Chapter 4 where a detailed literature study was conducted on simulated experiences and how they can be implemented to be effective.

To obtain an understanding of existing game design principles and how to incorporate the principles into a serious game
This objective focuses on gaining an understanding of game design principles and how to effectively incorporate these principles to create a successful serious game. This objective was reached in Chapters 3 and 4, where a literature study was conducted on these principles and later incorporated into the design of the serious game in Chapter 5.

To deliver a serious game utilising simulated experiences to promote information security awareness

After the identification of the core principles needed to create an effective serious game using simulated experiences and real-world examples, a serious game called "Cyber Cadet: Threat Defender" was created to combine these three elements in a simulation environment that was safe for participants to use and experience. This objective was achieved by building this game and the design processes were discussed in Chapter 5.

Evaluate the serious game by having parents, teachers, and experts in the field of security and gaming, play the game and provide feedback
The final objective was to have a select group of adults play the game and evaluate the effectiveness of the game to improve information security awareness. This group of adults was used because they either had a connection to the youth by being a caregiver or they had relevant experience in information security or game design. It was important to ensure that these participants added value to the data collected and could evaluate the game with the youth in mind. This objective was achieved by having the participants evaluate the game and provide feedback on its effectiveness. This evaluation step was documented in Chapter 6.

By reaching these objectives, the study further answers the primary and secondary research questions, namely: how can a serious game utilising simulated experiences promote information security awareness among the youth? what were the methods used in recent cyber attacks? what simulated experience methods exist? what game design principles exist?, and how can these principles be incorporated into a serious game? The answer to the primary research question is that by using effective methods to identify clear objectives, a serious game can be created to simulate real-world events such as phishing, weak passwords and other malicious attacks in order to promote information security awareness in a safe environment. This safe environment creates a space where the user can explore and learn by doing, and this learning in turn allows the user to then apply what has been learnt in a real-world context.

7.2 Evaluation of the research process

The Design Science Research Process was followed and effectively implemented in the following way:

Problem identification and motivation
The first phase of the DSRP was achieved by conducting a literature review to identify the research problem and establish the motivation for the study (Chapter 1).

Definition of the objectives for a solution
The second phase was achieved defining the objectives of the proposed solution, by evaluating existing research (Chapters 2, 3, and 4) to determine whether a serious game that incorporates simulated experiences can effectively improve security awareness among the youth.

Design and development
The third phase was achieved by developing a simulated experience serious game that promoted information security awareness among the youth (Chapter 5).

Demonstration and evaluation
The fourth and fifth phases were achieved by having a group of participants evaluate and review the game (Chapter 6).

Communication
The final step of the DSRP is to communicate the findings. This can be done by writing scholarly publications or professional publications. This step is achieved with the documentation of the complete process as found in this dissertation.

By using the DSRP effectively, an artefact can be designed that achieves the objectives set out in the start of a study. If this artefact is an effective tool in solving the problem identified, it can lead to contributions to the field of study. The next section will identify the contributions this study makes to the field of research.

7.3 Contributions

The main contribution this study makes to the body of knowledge is an evaluated and effective serious game that uses simulated experiences to increase information security awareness among the youth. This game was developed as a proof of concept using core game design principles, real-world challenges, and simulated experiences to provide an effective method of promoting information security awareness. The study also provided secondary contributions that are:

- A literature review on information security, serious games, and simulated ex-

periences was performed and documented that could serve as a central source of information for future research.

- Simulated experience frameworks that were designed and these can be expanded and incorporated in future work.

7.4 Limitations

Due to ethical constraints, participation of the youth during the testing and evaluation phases of the study was not allowed. However, the evaluation was performed using adults associated with the youth and was an effective method to test the artefact. If the youth had been used during the test, a deeper and more focused assessment could have been done to identify the needs of the youth. This limitation is the most significant limitation related to this study. Another obstacle was to get participants who were willing to spend their time to evaluate the artefact, as a larger group of participants would have added value to the study. This value could have been in the form of more feedback to improve the artefact. The final limitation was the lack of manpower related to the study with regard to game design. To create an effective serious game, the developer needs to spend a lot of time on the development cycle. This development cycle requires expertise to be implemented effectively. Fully playable games that achieve all the goals and objectives set out by the developer take years to properly develop. This limits some of the gaming aspects that can be achieved if done in a larger team or over a longer period of time.

7.5 Recommendations

Based on the findings of this study, the following recommendations are proposed:

- **Integrate information security education into the school curriculum:** Integrating information security education into the school curriculum is an effective next step to ensure that the whole populace receives the required information security education.
- **Align game objectives with real-world needs:** When designing serious games that teach specialised information, collaboration with information security experts and educators is essential to identify current and critical threat

scenarios, ensuring that simulated experiences closely mirror current cyber risks.

- **Facilitate classroom and community integration:** These types of study should be expanded to ensure that the work that is being done reaches communities that require it.
- **Ensure serious games have a balance:** Serious games have to be balanced with respect to enjoyability and learning experience. If a game is not fun to play, the learning aspect will be ignored.

7.6 Future work

The main objective of the study was to identify how simulated experiences can be implemented in a serious game that effectively promotes information security awareness.
Future work could consist of further developing "Cyber Cadet" into a fully functional game that can be used to teach the youth and anyone willing to learn about information security awareness. Iterations can also be done on "Cyber Cadet" to expand on the already existing simulated experiences by incorporating other security threats.
Future work can also focus on finding effective methods of creating simulated experiences that can be used to improve the information security awareness of adults, as the results found in Chapter 6 indicate that the problem associated with information security awareness is not just faced by the youth, but is also evident in adult populations.

7.7 Summary

This study investigated the following question: "How can a serious game utilising simulated experiences promote security awareness among the youth?". In answer to this question, simulated experiences were designed and implemented in a serious game called "Cyber Cadet: Threat Defender" and presented to the participants to evaluate the effectiveness of these simulated experiences in the promotion of information security awareness. The result of the evaluation phase (Chapter 6) shows that a simulated experience game can be an effective method to increase

information security awareness, not only among young people but also among adults, as most of the participants felt the game was effective and suitable for anyone older than 14 years. To build an effective serious game to promote information security awareness among the youth, the game needs to have clearly defined objectives that create the framework for the rest of the game, have fun gameplay mechanics that keep the player entertained, and needs to simulate real-world scenarios that teach the player about the real consequences. These simulated experiences can provide everyone with the tools to effectively circumvent malicious threats and learn by experiencing these threats in a safe and controlled environment.

"Cyber Cadet: Threat Defender" highlights how a simulated experience serious game can information security awareness for both young people and adults. Through immersive simulations, players learn to identify, respond to, and protect against various digital threats in ways that traditional training methods may not be able to achieve. While the information security landscape continues to evolve, this study highlights the potential of serious games to keep pace with new attack vectors, empowering the next generation of digital citizens.

Bibliography

Abraham, O., Feathers, A. M., Grieve, L., and Babichenko, D. (2019). Developing and piloting a serious game to educate children about over-the-counter medication safety. *Journal of Pharmaceutical Health Services Research*, 10.

Abrahams, T. O., Farayola, O. A., Kaggwa, S., Uwaoma, P. U., Hassan, A. O., and Dawodu, S. O. (2024). Cybersecurity awareness and education programs: A review of employee engagement and accountability. *Computer Science & IT Research Journal*, 5:100–119.

Adamson, K. and Prion, S. K. (2020). Questions Regarding Substitution of Simulation for Clinical. *Clinical Simulation in Nursing*, 50:79–80.

Ahmadov, S. (2023). Enhancing BYOD mobile device security in a hybrid environment. *Sustainable Engineering and Innovation*, 5:247–260.

Alassaf, M. and Alkhalifah, A. (2021). Exploring the Influence of Direct and Indirect Factors on Information Security Policy Compliance: A Systematic Literature Review. *IEEE Access*, 9:687–705.

Alemany, J., Val, E. D., and García-Fornes, A. (2020). Assessing the Effectiveness of a Gamified Social Network for Applying Privacy Concepts: An Empirical Study With Teens. *IEEE Transactions on Learning Technologies*, 13:777–789.

Alqahtani, H. and Kavakli-Thorne, M. (2020). Design and Evaluation of an Augmented Reality Game for Cybersecurity Awareness (CybAR). *Information*, 11:121.

Alsharif, M., Mishra, S., and Alshehri, M. (2022). Impact of Human Vulnerabilities on Cybersecurity. *Computer Systems Science and Engineering*, 40:1153–1166.

Amankwa, E. (2021). Relevance of Cybersecurity Education at Pedagogy Levels in Schools. *Journal of Information Security*, 12:233–249.

Andreassen, A. L., Leighton, W. J., and Schreiber, D. F. (1988). Information security: An overview. *AT&T Technical Journal*, 67:2–8.

Andrew, L., Barwood, D., Boston, J., Masek, M., Bloomfield, L., and Devine, A. (2022). Serious games for health promotion in adolescents – a systematic scoping review. *Education and Information Technologies*, 28:5519–5550.

Andrews, G., Balakrishna, C., and Mikroyannidis, A. (2023). The need for game-based learning methods to address cyber threats. *European Conference on Games Based Learning*, 17:19–28.

Arbanas, K. and Hrustek, N. (2019). Key Success Factors of Information Systems Security. *Journal of Information and Organizational Sciences*, 43(2):131–144.

Balon, T. and Baggili, I. M. (2023). Cybercompetitions: A survey of competitions, tools, and systems to support cybersecurity education. *Education and Information Technologies*, 28:11759–11791.

Banić, L. and Orehovaki, T. (2024). A Comparison of Parenting Strategies in a Digital Environment: A Systematic Literature Review. *Multimodal Technologies and Interaction*, 8:32–60.

Bauer, S., Bernroider, E. W. N., and Chudzikowski, K. (2017). Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks. *Computer & Security*, 68:145–159.

Beckers, K., Pape, S., and Fries, V. (2016). HATCH: Hack And Trick Capricious Humans - A Serious Game on Social Engineering. *British Computer Society Conference on Human-Computer Interaction*, 30:1–3.

Bellotti, F., Berta, R., and Gloria, A. D. (2010). Designing Effective Serious Games: Opportunities and Challenges for Research. *International Journal of Emerging Technologies in Learning*, 5:22–35.

Bhargav-Spantzel, A., Squicciarini, A. C., and Bertino, E. (2006). Privacy preserving multi-factor authentication with biometrics. *Digital Identity Management*, 2:63–72.

Bhusal, N., Gautam, M., and Benidris, M. (2020). Cybersecurity of Electric Vehicle Smart Charging Management Systems. *North American Power Symposium*, 52:1–6.

Biasin, E. (2021). Why accuracy needs further exploration in data protection. *Proceedings of the 1st International Conference on AI for People: Towards Sustainable AI*, 1:1–6.

BinJubier, M., Ismail, M. A., Ahmed, A. A., and Sadiq, A. S. (2022). Slicing-Based Enhanced Method for Privacy-Preserving in Publishing Big Data. *Computers, Materials & Continua*, 72:3665–3686.

Bishop, M. (2018). A Design for a Collaborative Make-the-Flag Exercise. *Information Security Education – Towards a Cybersecure Society*, 531:3–14.

Biswas, S., Jung, K., and Palamidessi, C. (2022). Tight Differential Privacy Blanket for Shuffle Model. *ArXiv*, abs/2205.04410.

Brehmer, M., Steinherr, V. M., and Stöckl, R. (2024). Toward A Higher Resilience Against Cyberattacks. *Datenschutz und Datensicherheit*, 48:352–357.

Caballero, A. (2013). Information Security Essentials for IT Managers: Protecting Mission-Critical Systems. *Computer and Information Security Handbook*, 2:379–407.

Charsky, D. (2010). From Edutainment to Serious Games: A Change in the Use of Game Characteristics. *Games and Culture*, 5:177–198.

Chen, H. and Li, W. (2017). Mobile device users' privacy security assurance behavior: A technology threat avoidance perspective. *Information and Computer Security*, 25:330–344.

Cheng, L., Liu, F., and Yao, D. D. (2017). Enterprise data breach: causes, challenges, prevention, and future directions. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, 7:16–22.

Chindrus, C. and Caruntu, C. F. (2023). Securing the Network: A Red and Blue Cybersecurity Competition Case Study. *Information*, 14:587.

Choong, Y.-Y., Theofanos, M. F., Renaud, K. V., and Prior, S. (2019). "Passwords protect my stuff" - a study of children's password practices. *Journal of Cybersecurity*, 5:1–19.

Chou, C. Y., Chen, J., and Lin, S. (2022). Value cocreation in livestreaming and its effect on consumer simulated experience and continued use intention. *International Journal of Consumer Studies*, 46:2183–2199.

Coenraad, M., Pellicone, A. J., Ketelhut, D. J., Cukier, M., Plane, J. D., and Weintrop, D. (2020). Experiencing Cybersecurity One Game at a Time: A Systematic Review of Cybersecurity Digital Games. *Simulation & Gaming*, 51:586–611.

Croucamp, C., Drevin, G. R., and Snyman, D. P. (2022). Promoting cybersecurity awareness utilizing a "build your own adventure" serious game. *Proceedings of the International Conferences on Applied Computing 2022 and WWW/Internet 2022*, 1:212–216.

Dawkins, S. (2023). NIST Phish Scale User Guide. *National Institute of Standards and Technology*, TN2276:1–37.

de Araujo Pistono, A. M. A., Santos, A. M. P., Baptista, R. J. V., and Mamede, H. S. (2024). Framework for adaptive serious games. *Computer Applications in Engineering Education*, 32:1–34.

de Casanove, O., Leleu, N., and Sèdes, F. (2022). Applying PDCA to Security, Education, Training and Awareness Programs. *International Symposium on Human Aspects of Information Security and Assurance*, 658:39–48.

Deka, L. and Barua, G. (2010). On-line consistent backup in transactional file systems. *Asia Pacific Workshop on Systems*, 1:37–42.

DeSmet, A., Ryckeghem, D. M. L. V., Compernolle, S., Baranowski, T., Thompson, D. I., Crombez, G., Poels, K., Lippevelde, W. V., Bastiaensens, S., Cleemput, K. V., Vandebosch, H., and de Bourdeaudhuij, I. (2014). A meta-analysis of serious digital games for healthy lifestyle promotion. *Preventive Medicine*, 69:95–107.

Douha, N. Y.-R., Renaud, K. V., Taenaka, Y., and Kadobayashi, Y. (2023). Smart home cybersecurity awareness and behavioral incentives. *Information and Computer Security*, 31:545–575.

Ertan, S. and Yüzer, T. V. (2024). Examination of Cybersecurity in Open and Distance Learning within the Scope of Technical Support Services. *Journal of Educational Technology and Online Learning*, 7:254–272.

Fagan, M., Khan, M. M. H., and Buck, R. W. (2015). A study of users' experiences and beliefs about software update messages. *Computers in Human Behavior*, 51:504–519.

Farsi, Z., Yazdani, M., Butler, S. C., Nezamzadeh, M., and Mirlashari, J. (2021). Comparative Effectiveness of Simulation versus Serious Game for Training Nursing Students in Cardiopulmonary Resuscitation: A Randomized Control Trial. *International Journal of Computer Games Technology*, 6695077:1–12.

Fayayola, O. A., Olorunfemi, O. L., and Shoetan, P. O. (2024). Data privacy and security in IT: A review of techniques and challenges. *Computer Science & IT Research Journal*, 5:606–615.

Feng, D., Qin, Y., Feng, W., Li, W., Shang, K., and Ma, H. (2024). Survey of research on confidential computing. *The Institution of Engineering and Technology Communications*, 18:535–556.

Ferraiolo, D. F., Sandhu, R., Gavrila, S., Kuhn, D. R., and Chandramouli, R. (2001). Proposed NIST standard for role-based access control. *ACM Transactions on Information and System Security*, 4(3):224–274.

Filippidis, A. P., Lagkas, T. D., Mouratidis, H., Nifakos, S., Grigoriou, E., and Sarigiannidis, P. G. (2022). Enhancing information security awareness programs through collaborative learning. *European Conference on Games Based Learning*, 16:803–810.

Fortinet (2025). Cyberthreats. https://www.fortinet.com/topics/cyber-threats. Accessed: 22 January 2025.

Francia, G. A., Thornton, D., Trifas, M. A., and Bowden, T. (2014). Gamification of Information Security Awareness Training. *Emerging Trends in ICT Security*, 2024:85–97.

Furnell, S., Haney, J. M., and Theofanos, M. F. (2021). Pandemic Parallels: What Can Cybersecurity Learn From COVID-19? *Computer*, 54:68–72.

Gáliková, M., Vábenský, V., and Vykopal, J. (2021). Toward Guidelines for Designing Cybersecurity Serious Games. *Proceedings of the 52nd ACM Technical Symposium on Computer Science Education*, 52:1275.

Ghaeb, J. A., Smadi, M. A., and Chebil, J. (2011). A high performance data integrity assurance based on the determinant technique. *Future Generation Computer Systems*, 27:614–619.

Ghani, U. (2015). Effect of feedback mechanisms on students' learning in the use of simulation-based training in a computer engineering program. *QScience Proceedings, Engineering Leaders Conference 2014 on Engineering Education*, 59:1–6.

Ghazvini, A. and Shukur, Z. (2017). Information Security Content Development for Awareness Training Programs in Healthcare. *International Journal of Security and its Applications*, 11:87–96.

Gjertsen, E. G. B., Gjære, E. A., Bartnes, M., and Flores, W. R. (2017). Gamification of Information Security Awareness and Training. *International Conference on Information Systems Security and Privacy*, 3:59–70.

Godejord, P. A. and Godejord, B. J. (2023). Computer Games as a Pedagogical Tool for Creating Cyber Security Awareness. *European Conference on Games Based Learning*, 17(1):220–224.

Godot (2024). Godot, your free open-source game engine. https://godotengine.org/. Accessed: 05 February 2024.

Grispos, G., Glisson, W. B., and Storer, T. (2017). Enhancing security incident response follow-up efforts with lightweight agile retrospectives. *Digital Investigation*, 22:62–73.

Gwenhure, A. K. and Rahayu, F. S. (2024). Gamification of Cybersecurity Awareness for Non-IT Professionals: A Systematic Literature Review. *International Journal of Serious Games*, 11:83–99.

Hadnagy, C. (2018). *Social Engineering: The Art of Human Hacking*. Wiley & Sons, 2nd edition.

Hadziosmanovic, D., Bolzoni, D., Etalle, S., and Hartel, P. H. (2012). Challenges and opportunities in securing industrial control systems. *Complexity in Engineering (COMPENG). Proceedings*, 2012:1–6.

Hall, L., Paracha, S., Hagan-Green, G., Ure, C., and Jackman, P. (2022). Cyber Eyes Wide Open: Creative Collaboration between Artists, Academics & Cyber Security Practitioners. *Electronic Workshops in Computing*, 2022:1–10.

Hamari, J., Shernoff, D. J., Rowe, E., Coller, B. D., Asbell-Clarke, J., and Edwards, T. (2016). Challenging games help students learn: An empirical study on engagement, flow and immersion in game-based learning. *Computers in Human Behavior*, 54:170–179.

Haoran, G., Bazakidi, E., and Zary, N. (2019). Serious Games in Health Professions Education: Review of Trends and Learning Efficacy. *Yearbook of Medical Informatics*, 28:240–248.

Hart, S., Margheri, A., Paci, F., and Sassone, V. (2020). Riskio: A Serious Game for Cyber Security Awareness and Education. *Computers Security*, 95:101827.

Hart, S. R., Halak, B., and Sassone, V. (2021). MOTENS: A Pedagogical Design Model for Serious Cyber Games. *ArXiv*, abs/2110.11765.

Hasanah, A. and Baars, R. C. (2023). Serious Games, Motivation, and Learning: A Study on Marginalized Youth. *Creative Education*, 14:2747–2776.

He, D., Ma, M., Zhang, Y., Chen, C., and Bu, J. (2011). A strong user authentication scheme with smart cards for wireless communications. *Computer Communications*, 34:367–374.

He, M. and An, X. (2016). Information Security Risk Assessment Based on Analytic Hierarchy Process. *Indonesian Journal of Electrical Engineering and Computer Science*, 1:656–664.

Helble, S. C., Gartner, A. J., and McKneely, J. A. (2019). Increasing the Security of Weak Passwords: the SPARTAN Interface. *ArXiv*, abs/1905.08199.

Hodhod, R. A., Hardage, H., Abbas, S., and Aldakheel, E. A. (2023). CyberHero: An Adaptive Serious Game to Promote Cybersecurity Awareness. *Electronics*, 12:3544.

Hof, B. and Carle, G. (2017). Software Distribution Transparency and Auditability. *ArXiv*, abs/1711.07278.

Hughes-Lartey, K., Li, M., Botchey, F. E., and Qin, Z. (2021). Human factor, a critical weak point in the information security of an organization's Internet of things. *Heliyon*, 7:1–13.

Huynh, D., Luong, P., Iida, H., and Beuran, R. (2017). Design and Evaluation of a Cybersecurity Awareness Training Game. *International Conference on Evolutionary Computation*, 2017:183–188.

Imamverdiyev, Y. N. (2018). A model for optimal planning of information security incident response operations. *Problems of Information Technology*, 2:69–80.

Insua, D. R., Vieira, A. C., Rubio, J. A., Pieters, W., Labunets, K., and Rasines, D. G. (2019). An Adversarial Risk Analysis Framework for Cybersecurity. *Risk Analysis*, 41:16–36.

ISCAfrica (2025). Cybercrime. https://cybercrime.org.za. Accessed: 22 January 2025.

Jackson, S., Vanteeva, N., and Fearon, C. (2019). An Investigation of the Impact of Data Breach Severity on the Readability of Mandatory Data Breach Notification Letters: Evidence From U.S. Firms. *Journal of the Association for Information Science and Technology*, 70.

Jaffray, A., Finn, C., and Nurse, J. R. C. (2021). SherLOCKED: A Detective-themed Serious Game for Cyber Security Education. *International Symposium on Human Aspects of Information Security and Assurance*, 2107:4506.

Jampani, S. K. (2025). Social Engineering 2.0 Deepfake and Deep Learning-based Cyber-attacks (Phishing). *International Journal For Multidisciplinary Research*, 7:1–13.

Jayakrishnan, G., Banahatti, V., and Lodha, S. (2022). PickMail: a serious game for email Phishing Awareness training. *Usable Security and Privacy (USEC) Symposium*, 2022:1–13.

Jin, G., Tu, M., Kim, T., Heffron, J., and White, J. (2018). Evaluation of Game-Based Learning in Cybersecurity Education for High School Students. *Journal of Education and Learning*, 12:150–158.

Johnson, D. B., Menezes, A., and Vanstone, S. A. (2001). The Elliptic Curve Digital Signature Algorithm (ECDSA). *International Journal of Information Security*, 1:36–63.

Johri, A. and Kumar, S. (2023). Exploring Customer Awareness towards Their Cyber Security in the Kingdom of Saudi Arabia: A Study in the Era of Banking Digital Transformation. *Human Behavior and Emerging Technologies*, 2023:1–10.

Kävrestad, J., Eriksson, F., and Nohlberg, M. (2019). Understanding passwords - a taxonomy of password creation strategies. *Information and Computer Security*, 27:453–467.

Kayali, F., Schwarz, V., Purgathofer, P., and Götzenbrucker, G. (2018). Using Game Design to Teach Informatics and Society Topics in Secondary Schools. *Multimodal Technologies and Interaction*, 2:77.

Kelm, D. and Volkamer, M. (2018). Towards a Social Engineering Test Framework. 2018:38–48.

Khamzina, B., Roza, N., Zhussupbekova, G., Shaizhanova, K., Aten, A., and Meirkhanovna, B. A. (2022). Determination of Cyber Security Issues and Awareness Training for University Students. *International Journal of Emerging Technologies in Learning*, 17:177–190.

Khan, B., Alghathbar, K. S., Nabi, S. I., and Khan, M. K. (2011). Effectiveness of information security awareness methods based on psychological theories. *African Journal of Business Management*, 5:10862–10868.

Kizza, J. M. (2013). Computer Network Vulnerabilities. *Guide to Computer Network Security*, 2:89–105.

Klenke-Borgmann, L., Digregorio, H., and Cantrell, M. A. (2022). Role Clarity and Interprofessional Colleagues in Psychological Safety. *Simulation in Healthcare: The Journal of the Society for Simulation in Healthcare*, 18:203–206.

Kovaević, A., Putnik, N., and Toković, O. (2020). Factors Related to Cyber Security Behavior. *IEEE Access*, 8:125140–125148.

Labadie, C. and Legner, C. (2022). Building data management capabilities to address data protection regulations: Learnings from EU-GDPR. *Journal of Information Technology*, 38:16–44.

Lam, N. T. (2021). Detecting Unauthorized Network Intrusion based on Network Traffic using Behavior Analysis Techniques. *International Journal of Advanced Computer Science and Applications*, 12:4.

Lau, H. M., Smit, J. H., Fleming, T., and Riper, H. (2017). Serious Games for Mental Health: Are They Accessible, Feasible, and Effective? A Systematic Review and Meta-analysis. *Frontiers in Psychiatry*, 7:209.

Legárd, I. (2020). Building an effective information security awareness program. *Central and Eastern European eDem and eGov Days*, 338:189–200.

Letica, I. B. (2020). Some Correlates of Risky User Behavior and ICT Security Awareness of Secondary School Students. *International Journal of Electrical and Computer Engineering Systems*, 10:85–89.

Lim, W. M., Das, M., Sharma, W., Verma, A., and Kumra, R. (2024). Gamification for sustainable consumption: A state-of-the-art overview and future agenda. *Wiley*, 34:1510–1549.

Limba, T., Plėta, T., Agafonov, K., and Damkus, M. (2017). Cyber Security Management Model for Critical Infrastructure. *Entrepreneurship and Sustainability Issues*, 4:559–573.

Limna, P., Kraiwanit, T., and Siripipattanakul, S. (2023). The Relationship between Cyber Security Knowledge, Awareness and Behavioural Choice Protection among

Mobile Banking Users in Thailand. *International Journal of Computing Sciences Research*, 7:1133–1151.

Liu, Y., Ma, Y., su Zhang, H., yi Li, D., and Chen, G. (2011). A method for trust management in cloud computing: Data coloring by cloud watermarking. *International Journal of Automation and Computing*, 8:280–285.

Lombardi, M., Garzia, F., Fargnoli, M., Pellizzi, A., and Ramalingam, S. (2020). Application of Quality Function Deployment to the Management of Information Physical Security. *International Journal of Safety and Security Engineering*, 2020:727–732.

Lu, Y., Li, L., Peng, H., and Yang, Y. (2015). An Enhanced Biometric-Based Authentication Scheme for Telecare Medicine Information Systems Using Elliptic Curve Cryptosystem. *Journal of Medical Systems*, 39:32.

Maathuis, C., Janssens, F., and Rahimi, E. (2024). Design of a Disinformation Awareness Digital Game. *European Conference on Social Media*, 11:127–136.

Makarova, E. A. and Makarova, E. L. (2019). Aggressive Behavior in Online Games and Cybervictimization of Teenagers and Adolescents. *International Electronic Journal of Elementary Education*, 12:157–165.

Maryani, E., Rahmawan, D., Garnesia, I., and Ratmita, R. A. (2020). Management and Psychological Aspect: Teenagers' Awareness of Privacy in Social Media. *Jurnal Komunikasi Ikatan Sarjana Komunikasi Indonesia*, 5:168–178.

Masrek, M. N., Soesantari, T., Khan, A., and Dermawan, A. K. (2021). Examining the Relationship between Information Security Effectiveness and Information Security Threats. *International Journal of Business and Society*, 21:1203–1214.

Mian, T. S. and Alatawi, E. M. (2023). Investigating How Parental Perceptions of Cybersecurity Influence Children's Safety in the Cyber World: A Case Study of Saudi Arabia. *Intelligent Information Management*, 15:350–372.

Micallef, N. and Arachchilage, N. A. G. (2017). Involving Users in the Design of a Serious Game for Security Questions Education. *ArXiv*, abs/1710.03888.

Mijwil, M. M., Unogwu, O. J., Filali, Y., Bala, I., and Al-Shahwani, H. (2023). Exploring the Top Five Evolving Threats in Cybersecurity: An In-Depth Overview. *Mesopotamian Journal of Cyber Security*, 2023:57–63.

Minhas, T., Anamalamudi, S., Ning, X., and Jin, M. (2013). XML and NET Based GUI for Heterogeneous Database Backup System. *International Journal of Information and Education Technology*, pages 315–318.

Mladinić, A., Vukić, Z., and Ronević, A. (2023). GDPR compliance challenges in Croatian micro, small and medium sized enterprises. *Journal of Law*, 39:54–75.

Muir, K. and Joinson, A. N. (2020). An Exploratory Study Into the Negotiation of Cyber-Security Within the Family Home. *Frontiers in Psychology*, 11:424.

Nicholson, J., Terry, J., Beckett, H., and Kumar, P. (2021). Understanding Young People's Experiences of Cybersecurity. *Proceedings of the 2021 European Symposium on Usable Security*, 2021:200–210.

Nkongolo, M. (2024). Infusing Morabaraba Game Design to Develop a Cybersecurity Awareness Game (CyberMoraba). *Proceedings of the 19th International Conference on Cyber Warfare and Security*, 2024:240–250.

Nobles, C. (2018). Botching human factors in cybersecurity in business organizations. *Holistica – Journal of Business and Public Administration*, 9:71–88.

Olgers, T. J., van Os, J. M., Bouma, H. R., and ter Maaten, J. C. (2022). The validation of a serious game for teaching ultrasound skills. *The Ultrasound Journal*, 14:29.

Omorog, C. D. and Medina, R. P. (2018). Internet Security Awareness of Filipinos: A Survey Paper. *ArXiv*, abs/2012.03669.

Padmavathi, G. and Shanmugapriya, D. (2009). A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks. *ArXiv*, abs/0909.0576.

Palada, B., Chandan, V. S., Gowda, C. P., and Nikitha, P. (2024). The Role of Augmented Reality (AR) in Education. *International Journal for Research in Applied Science and Engineering Technology (IJRASET)*, 12(3):1400–1408.

Park, M. and Chai, S. (2018). Internalization of Information Security Policy and Information Security Practice: A Comparison with Compliance. *Hawaii International Conference on System Sciences*, 51:4723–4731.

Parvez, M. T., Alsuhibani, A. M., and Alamri, A. H. (2023). Educational and Cybersecurity Applications of an Arabic CAPTCHA Gamification System. *Ingénierie des Systèmes D Information*, 28:1275–1285.

Peffers, K., Tuunanen, T., Rothenberger, M. A., and Chatterjee, S. (2007). A Design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems*, 24:45–77.

Pellicone, A. J., Ketelhut, D. J., Shokeen, E., Weintrop, D., Cukier, M., and Plane, J. D. (2022). Designing a Game to Promote Equity in Cybersecurity. *European Conference on Games Based Learning*, 16:448–454.

Pouransafara, M. and Maroop, Z. I. M. C. N. (2013). Review of Information Security Vulnerability: Human Perspective. *The Society of Digital Information and Wireless Communications*, 2013:119–126.

Prior, S. and Renaud, K. V. (2023). Who Is Best Placed to Support Cyber Responsibilized UK Parents? *Children*, 10:1130.

Purdy, E. I., Borchert, L., El-Bitar, A., Isaacson, W., Bills, L., and Brazil, V. (2022). Taking simulation out of its "safe container" - exploring the bidirectional impacts of psychological safety and simulation in an emergency department. *Advances in Simulation*, 7.

Qiang, W., Zhang, K., Dai, W., and Jin, H. (2016). Secure cryptographic functions via virtualization-based outsourced computing. *Concurrency and Computation: Practice and Experience*, 28:3149–3163.

Qorahman, O. and Akbar, N. N. (2024). A bibliometric analysis of the of cybersecurity policy research. *Information: Journal of Library and Information Science*, 4:64–78.

Quayyum, F., Bueie, J., Cruzes, D. S., Jaccheri, M. L., and Vidal, J. C. T. (2021). Understanding parent's perceptions of children's cybersecurity awareness in Norway. *Proceedings of the Conference on Information Technology for Social Good*, 21:236–241.

RajeshwariN, O. and SowmyaraniC., N. (2016). Data utility measures - a survey. *2nd International Conference on Applied and Theoretical Computing and Communication Technology*, 2:722–725.

Rajkumar, K. and Njenga, K. N. (2022). Make personal information security great again: A case of users' perspectives on personal identifiable information in South Africa. *SA Journal of Information Management*, 24:1526.

Raturi, V., Hong, J., McArthur, D. P., and Livingston, M. (2021). The impact of privacy protection measures on the utility of crowdsourced cycling data. *Journal of Transport Geography*, 92:103020.

Rikker, V. and Sarmah, D. K. (2025). An Adversarial Risk Analysis Framework for Cybersecurity. *Computing in Higher Education*, 37:248–272.

Rodwald, P. (2019). Using Gamification and Fear Appeal Instead of Password Strength Meters to Increase Password Entropy. *Scientific Journal of Polish Naval Academy*, 217:17–33.

Rumeser, D. and Emsley, M. W. (2018). Can Serious Games Improve Project Management Decision Making Under Complexity? *Project Management Journal*, 50:23–39.

Rynge, M., Vahi, K., Deelman, E., Mandal, A., Baldin, I., Bhide, O., Heiland, R. W., Welch, V., Hill, R. L., Poehlman, W. L., Feltus, F. A., da Silva, R. F., and Mayani, R. (2019). Integrity Protection for Scientific Workflow Data: Motivation and Initial Experiences. *Proceedings of the Practice and Experience in Advanced Research Computing on Rise of the Machines Learning*, 17:1–8.

Sabillon, R. (2021). Delivering Effective Cybersecurity Awareness Training to Support the Organizational Information Security Function. *Research Anthology on Privatizing and Securing Data*, 1:284–309.

Saleh, H. A. (2024). BANK OF PASSWORDS: a secure Android password manager implemented based on specific requirements. *Al-Kitab Journal for Pure Sciences*, 8:40–62.

Sarker, I. H. (2023). Multi-aspects AI-based modeling and adversarial learning for cybersecurity intelligence and robustness: A comprehensive overview. *Security and Privacy*, 6:1–26.

Scherb, C., Heitz, L., Grimberg, F., Grieder, H., and Maurer, M. (2023). A Serious Game for Simulating Cyberattacks to Teach Cybersecurity. *ArXiv*, abs/2305.03062.

Schwarz, A., Huertas-Delgado, F. J., Cardon, G., and DeSmet, A. (2020). Design Features Associated with User Engagement in Digital Games for Healthy Lifestyle Promotion in Youth: A Systematic Review of Qualitative and Quantitative Studies. *Games for Health Journal*, 9:150–163.

Sendjaja, T., Irwandi, Prastiawan, E., Suryani, Y., and Fatmawati, E. (2024). Cybersecurity In The Digital Age: Developing Robust Strategies To Protect Against Evolving Global Digital Threats And Cyber Attacks. *International Journal of Science and Society*, 6:1008–1019.

Shah, P. R. and Agarwal, A. (2023). Cyber Suraksha: a card game for smartphone security awareness. *Information and Computer Security*, 31:576–600.

Shetty, S., Choi, K.-S., and Park, I. (2024). Investigating the Intersection of AI and Cybercrime: Risks, Trends, and Countermeasures. *International Journal of Cybersecurity Intelligence & Cybercrime*, 7:28–53.

Shillair, R., Cotten, S. R., Tsai, H.-Y. S., Alhabash, S., LaRose, R., and Rifon, N. J. (2015). Online safety begins with you and me: Convincing Internet users to protect themselves. *Computers in Human Behavior*, 48:199–207.

Shojaifar, A., Fricker, S., and Gwerder, M. (2020). Automating the Communication of Cybersecurity Knowledge: Multi-case Study. *Information Security Education. Information Security in Action*, 579:110–124.

Siyed, Z. (2023). A New Cyber Risk: How Teens Expose Corporations in WFH Era. *Journal of Information Security*, 14:396–421.

Small, S. P., Colbourne, P. A., and Murray, C. L. (2018). High-Fidelity Simulation of Pediatric Emergency Care: An Eye-Opening Experience for Baccalaureate Nursing Students. *Canadian Journal of Nursing Research*, 50:145–154.

Smiderle, R., Rigo, S. J., Marques, L. B., de Miranda Coelho, J. A. P., and Jaques, P. A. (2020). The impact of gamification on students' learning, engagement and behavior based on their personality traits. *Smart Learning Environments*, 7:3.

Smith, G. (2014). Understanding procedural content generation: a design-centric analysis of the role of PCG in games. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 14:917–926.

Steele, G. (2025). *Top 50 cybersecurity Threats*. Splunk, 1 edition.

Suleman, T. and Liaquat, N. (2022). The Cyber Security Incident Response and Reverse Engineering. *International Journal for Electronic Crime Investigation*, 6:19–38.

Sun, K., Zou, Y., Radesky, J. S., Brooks, C., and Schaub, F. (2021). Child Safety in the Smart Home: Parents' Perceptions, Needs, and Mitigation Strategies. *Proceedings of the ACM on Human-Computer Interaction*, 5:1–41.

Tai, E. T. T. (2018). Data ownership and consumer protection. *Journal of European Consumer and Market Law*, 7:136–140.

Temara, S. (2024). The Ransomware Epidemic: Recent Cybersecurity Incidents Demystified. *Asian Journal of Advanced Research and Reports*, 18:1–16.

Teoh, C. and Mahmood, A. (2018). Cybersecurity workforce development for digital economy. *The Educational Review USA*, 2.

Truong, T. C., Diep, Q. B., and Zelinka, I. (2020). Artificial Intelligence in the Cyber Domain: Offense and Defense. *Symmetry*, 12:410.

Turner, S. and Harder, N. (2018). Psychological Safe Environment: A Concept Analysis. *Clinical Simulation in Nursing*, 18:47–55.

van Steen, T. and Deeleman, J. R. A. (2021). Successful Gamification of Cybersecurity Training. *Cyberpsychology, Behavior and Social Networking*, 24:593–598.

Venter, I. M., Blignaut, R. J., Renaud, K., and Venter, M. A. (2019). Cyber security education is as essential as "the three R's". *Heliyon*, 5.

Waddington, P. A. J. (1995). Information as an asset: the invisible goldmine. *Business Information Review*, 12:26–36.

Wall, D. S. (2012). Enemies within: Redefining the insider threat in organizational security policy. *Security Journal*, 26:107–124.

Wan, H. (2012). Research of Network Security and Information Encryption. *International Journal of Education and Management Engineering*, 2(2):74–80.

Wang, B. and Chen, J. (2022). Parental intervention strategies and operating mechanism on adolescent social media use - The concept of literacy improvement based on interaction. *Frontiers in Psychology*, 13.

Wang, X. (2022). Exploring Chinese College Students' Awareness of Information Security in the COVID-19 Era. *European Journal of Education*, 5:19–33.

Wang, Z., Sun, L., and Zhu, H. (2020). Defining Social Engineering in Cybersecurity. *IEEE Access*, 8:85094–85115.

Welman, A.-M. and Spies, C. (2016). High fidelity simulation in nursing education: Considerations for meaningful learning. *Trends in Nursing*, 3.

Whitman, M. and Mattord, H. (2022). *Principles of information security*. CENGAGE Learning Custom Publishing, Boston, USA, 7th edition.

Winkler, S. and Danner, L. (1974). Data security in the computer communication environment. *Computer*, 7:23–31.

Winn, W., Stahr, F. R., Sarason, C. P., Fruland, R. M., Oppenheimer, P., and Lee, Y.-L. (2006). Learning Oceanography from a Computer Simulation Compared with Direct Experience at Sea. *Journal of Research in Science Teaching*, 43:25–42.

Wouters, P., van Nimwegen, C., van Oostendorp, H., and der Spek, E. V. (2013). A meta-analysis of the cognitive and motivational effects of serious games. *Journal of Educational Psychology*, 105:249–265.

Xu, Z. and Guo, K. H. (2019). It ain't my business: a coping perspective on employee effortful security behavior. *Journal of Enterprise Information Management*, 32:824–842.

Yang, H., Yu, J., Tang, S., and Hu, Y. (2023). Overview of security access control mechanisms. *2nd International Conference on Applied Statistics, Computational Mathematics and Software Engineering*, 12784:127843E.

Yasin, A., Liu, L., Li, T., Fatima, R., and Wang, J. (2019). Improving software security awareness using a serious game. *The Institution of Engineering and Technology Software*, 13:159–169.

Yevseiev, S., Melenti, Y., Voitko, O., Hrebeniuk, V., Korchenko, A., Mykus, S., Milov, O., Prokopenko, O., Sievierinov, O., and Chopenko, D. (2021). Development of a concept for building a critical infrastructure facilities security system. *Eastern-European Journal of Enterprise Technologies*, 111:63–83.

Ylijoki, O., Sirkiä, J., Porras, J., and Harmaakorpi, V. (2018). Innovation capabilities as a mediator between big data and business model. *Journal of Enterprise Transformation*, 8:165–182.

Yu, J. H., Chang, H. J., Kim, S. S., Park, J. E., Chung, W. Y., Lee, S. K., Kim, M., Lee, J., and Jung, Y. J. (2021). Effects of high-fidelity simulation education on medical students' anxiety and confidence. *PLoS ONE*, 16.

Zeijlemaker, S., Rouwette, E. A., Cunico, G., Armenia, S., and von Kutzschenbach, M. (2022). Decision-Makers' Understanding of Cyber-Security's Systemic and Dynamic Complexity: Insights from a Board Game for Bank Managers. *Systems*, 10:49.

Zenda, B., Vorster, R., and da Veiga, A. (2020). Protection of personal information: An experiment involving data value chains and the use of personal information for marketing purposes in South Africa. *South African Computer Journal*, 32:113–132.

Zhao, D., Inaba, M., and Monroy-Hernández, A. (2022). Understanding Teenage Perceptions and Configurations of Privacy on Instagram. *Proceedings of the ACM on Human-Computer Interaction*, 6:1–28.

Zhou, S. (2021). Status and Risk Factors of Chinese Teenagers' Exposure to Cyberbullying. *SAGE Open*, 11.

Zhu, B., Deng, S., Xu, Y., Yuan, X., and Zhang, Z. (2019). Information Security Risk Propagation Model Based on the SEIR Infectious Disease Model for Smart Grid. *Information*, 10:323.

Zhu, M., Luo, Y., Yang, J., shun Xing, M., and Zhao, J. (2016). Research on Security Issues and Protection Strategy of Computer Network. *The Open Automation and Control Systems Journal*, 7:2097–2101.

Appendix A

Cyber Cadet download information

This download serves as the archive for **Cyber Cadet**, a serious game developed as part of a Master's research project at the School of Computer Science and Information Systems, North-West University (South Africa). The game is designed to promote cybersecurity awareness among the youth by simulating real-world challenges—including password security, phishing detection, and hack analysis—to provide an engaging and interactive learning experience.

Key components of the repository include:

- **Game Downloads:**
  - **Both the Windos and Mac versions can be found at: https://l1nk.dev/F8jsM**
  - **To use the game in Windows just download the zip and run the application found in the folder. Further guidance can be found in the game guide section in the main menu of "Cyber Cadet"**
  - **To use the game on a Mac. You are required to first install the Godot game engine and then import the Mac version of "Cyber Cadet" into Godot and run it from their using the play button.**
- **Interactive Gameplay:** Players face realistic cybersecurity scenarios through timed activities, immediate feedback, and a dynamic scoring system that reinforces best practices.

- **Academic Context:** Developed as part of an academic study at North-West University, the game evaluates the effectiveness of game-based learning in enhancing cybersecurity knowledge. The repository contains detailed background information, contact details for the researcher and supervisors, and supporting materials.
- **Confidentiality and Research Integrity:** All study data was managed in accordance with ethical standards, ensuring participant anonymity and secure data handling.

Appendix B

Partial password dictionary with analysis

ID	Password	Length Score	Complexity Score	Predictability Score	Uniqueness Score	Total
3150	t-bone	2	3	10	9	24
2523	e-mail	2	3	10	8	23
3390	x-men	2	3	10	7	22
3194	x-files	2	3	10	6	21
3264	a	1	1	1	1	4
3463	i	1	1	1	1	4
3401	e	1	1	1	1	4
3451	aa	1	1	1	1	4
3426	m	1	1	1	1	4
3498	go	1	1	1	1	4
3432	y	1	1	1	1	4
3301	22	1	1	1	1	4
2454	1	1	1	1	1	4
2026	1q2w3e4r	5	3	3	8	19
2045	q1w2e3r4	5	3	3	8	19
2041	1qaz2wsx	5	3	3	7	18
3443	Front242	5	5	1	9	20
1897	1234qwer	5	3	1	7	16
3316	Geronimo	5	3	1	7	16
3409	sample123	5	3	1	6	15

ID	**Password**	**Length Score**	**Complexity Score**	**Predictability Score**	**Uniqueness Score**	**Total**
2054	princess1	5	3	1	6	15
3323	Montreal	5	3	1	5	14
3322	Metallic	5	3	1	5	14
2629	johanna1	5	3	1	4	13

Appendix C

List of created emails

1. **Amazon Security Team** • **Email:** amazonsecurityteam@supportcenter.com
   - **Message:** Urgent: Suspicious activity detected. Login to verify your identity: https:www.aMazon.net
   - **Safe:** No
   - **Category:** Credential Harvesting
   - **Difficulty:** 5

2. **PayPal Support** • **Email:** paypalsupport@supportcenter.com
   - **Message:** Your account has been compromised. Click here to secure it: https:www.paypalsupport.io
   - **Safe:** No
   - **Category:** Impersonation
   - **Difficulty:** 4

3. **Cathy Johnson** • **Email:** cathy@securemail.com
   - **Message:** Can you send me the report by tomorrow?
   - **Safe:** Yes
   - **Category:** N/A
   - **Difficulty:** 2

4. **PayPal Support** • **Email:** paypalsupport@notifications.net
   - **Message:** Your subscription is expiring. Update your payment information: https:www.PayP@l.com
   - **Safe:** No
   - **Category:** Impersonation
   - **Difficulty:** 5

5. **Bank of America** • **Email:** bankofamerica@notifications.net
   - **Message:** Your account has been compromised. Click here to secure it: https:www.banker.com
   - **Safe:** No
   - **Category:** Impersonation
   - **Difficulty:** 4

6. **Netflix** • **Email:** netflix@alerts.com
   - **Message:** Your account has been compromised. Click here to secure it: https:www.netflix1@alerts.com
   - **Safe:** No
   - **Category:** Impersonation
   - **Difficulty:** 4

7. **Netflix** • **Email:** netflix1@alerts.com
   - **Message:** Your account has been compromised. Click here to secure it: https:www.Netflix.org

- **Safe:** No
- **Category:** Impersonation
- **Difficulty:** 5

8. Amazon Security Team • **Email:** amazonsecurityteam@alerts.com
- **Message:** Urgent: Suspicious activity detected. Login to verify your identity: https:www.amazonian.net
- **Safe:** No
- **Category:** Credential Harvesting
- **Difficulty:** 3

9. Amazon Security Team • **Email:** amazonsecurityteam@notifications.net
- **Message:** You have won a a 3000$ prize. Claim it now by providing your details.
- **Safe:** No
- **Category:** Fraudulent Offers
- **Difficulty:** 5

10. Alice Smith • **Email:** alice@securemail.com
- **Message:** The meeting is scheduled for 3 PM in the conference room.
- **Safe:** Yes
- **Category:** N/A
- **Difficulty:** 1

11. Amazon Security Team • **Email:** amazonsecurityteam1@notifications.net
- **Message:** Urgent: Suspicious activity detected. Login to verify your identity: https:www.amazon.org
- **Safe:** No
- **Category:** Credential Harvesting
- **Difficulty:** 4

12. Bank of America • **Email:** bankofamerica@securemail.com
- **Message:** Urgent: Suspicious activity detected. Login to verify your identity: https:www.TheBankOfAmerica.com
- **Safe:** No
- **Category:** Credential Harvesting
- **Difficulty:** 3

13. Bank of America • **Email:** bankofamerica1@notifications.net
- **Message:** Your account has been compromised. Click here to secure it: https:www.bankofamerica.co.za
- **Safe:** No
- **Category:** Impersonation
- **Difficulty:** 4

14. PayPal Support • **Email:** paypalsupport1@notifications.net
- **Message:** Urgent: Suspicious activity detected. Login to verify your identity: https:www.paypal.org
- **Safe:** No
- **Category:** Credential Harvesting
- **Difficulty:** 3

15. Amazon Security Team • **Email:** amazonsecurityteam2@notifications.net
- **Message:** Your account has been compromised. Click here to secure it: https:www.secure.io
- **Safe:** No
- **Category:** Impersonation
- **Difficulty:** 4

16. Bob Miller • **Email:** bob@alerts.com
- **Message:** The meeting is scheduled for 3 PM in the conference room.
- **Safe:** Yes
- **Category:** N/A
- **Difficulty:** 2

17. **Cathy Brown** • **Email:** cathy@alerts.com
    - **Message:** The meeting is scheduled for 3 PM in the conference room.
    - **Safe:** Yes
    - **Category:** N/A
    - **Difficulty:** 1

18. **Amazon Security Team** • **Email:** amazonsecurityteam3@notifications.net
    - **Message:** Urgent: Suspicious activity detected. Login to verify your identity: https:www.amazon.io
    - **Safe:** No
    - **Category:** Credential Harvesting
    - **Difficulty:** 3

19. **PayPal Support** • **Email:** paypalsupport1@supportcenter.com
    - **Message:** Your account has been compromised. Click here to secure it: https:www.paypal.io
    - **Safe:** No
    - **Category:** Impersonation
    - **Difficulty:** 5

20. **Alice Miller** • **Email:** alice@supportcenter.com
    - **Message:** Can you send me the report by tomorrow?
    - **Safe:** Yes
    - **Category:** N/A
    - **Difficulty:** 2

21. **Bob Johnson** • **Email:** bob@supportcenter.com
    - **Message:** Can you send me the report by tomorrow?
    - **Safe:** Yes
    - **Category:** N/A
    - **Difficulty:** 1

22. **Amazon Security Team** • **Email:** amazonsecurityteam@securemail.com
    - **Message:** Your account has been compromised. Click here to secure it: https:www.Amason.net
    - **Safe:** No
    - **Category:** Impersonation
    - **Difficulty:** 4

23. **PayPal Support** • **Email:** paypalsupport2@supportcenter.com
    - **Message:** Your subscription is expiring. Update your payment information: https:www.paypal.org
    - **Safe:** No
    - **Category:** Impersonation
    - **Difficulty:** 5

24. **Amazon Security Team** • **Email:** amazonsecurityteam@updates.org
    - **Message:** Your subscription is expiring. Update your payment information: https:www.amazpnpayments.net
    - **Safe:** No
    - **Category:** Impersonation
    - **Difficulty:** 5

25. **PayPal Support** • **Email:** paypalsupport2@notifications.net
    - **Message:** Your subscription is expiring. Update your payment information: https:www.subcriptions.io
    - **Safe:** No
    - **Category:** Impersonation
    - **Difficulty:** 3

Appendix D

Pilot questionnaire

Cyber Cadet Threat Detector Questionnaire : Pilot study

Please consider taking part in my academic study.
This study involves your participation in a serious game designed to promote information security awareness through simulated experiences. The target audience for this study is the youth, and the goal is to evaluate the effectiveness of the game in enhancing cybersecurity knowledge. Your participation will be greatly appreciated and will contribute significantly to my Master's research!

Purpose of Study:

- The purpose of this Master's study is to design and assess a serious game that uses simulated experiences to educate youth on

  information security awareness. If you have any questions regarding this study, you may contact me or my supervisor (contact details are provided below).

General Information about the Study:

- Participation in this study is voluntary.
- The study involves playing the game and completing a short questionnaire afterward.
- You are unlikely to experience any discomfort or risks during the study.
- No compensation will be provided for participation.

Confidentiality:

- All information collected will remain anonymous and confidential. Data will be used solely for research purposes and stored securely.

Contact details of Researcher:

- **Full Name:** Christo C. Croucamp
- **School:** School of Computer Science and Information Systems
- **University:** North-West University
- **Country:** South Africa
- **Email:** 32177186@mynwu.ac.za

Contact details of Supervisor #1:

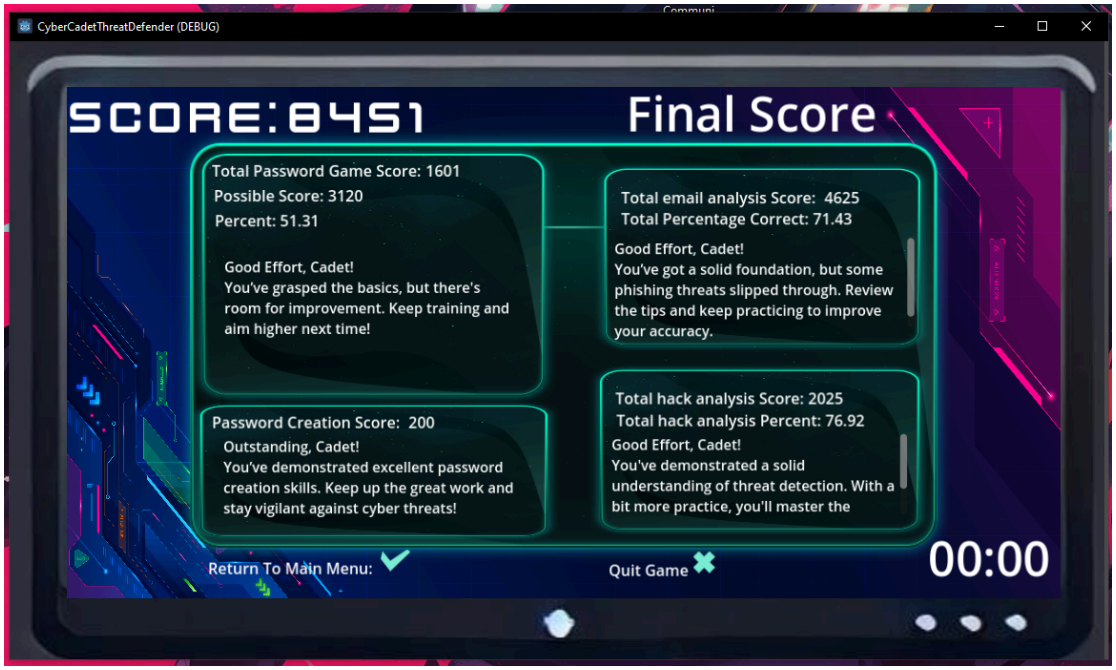
- **Full Name:** Gunther R. Drevin
- **School:** School of Computer Science and Information Systems
- **University:** North-West University
- **Country:** South Africa
- **Email:** gunther.drevin@nwu.ac.za

Contact details of Supervisor #2:

- **Full Name:** Lynette Drevin
- **School:** School of Computer Science and Information Systems
- **University:** North-West University
- **Country:** South Africa
- **Email:** lynette.drevin@nwu.ac.za

* Indicates required question

Please download and access the game from: Cyber Cadet Threat detector
You need to play the game before starting the questionnaire. It is also important to note that for the final question you should upload a screenshot of the finale scoreboard that looks like this: (This can be achieved by pressing WindowsKey+Shift+S and then dragging a box around the game)



1. Do you give consent to be apart of the research project? *

   Mark only one oval.

   - ◯ Yes *Skip to question 2*
   - ◯ No

Biographical and Awareness Information

This section contains non identifiable question to create an biographical and awareness level profile.

2. What is your gender? *

Mark only one oval.

- Male
- Female
- Prefer not to say

3. Which age group do you fall in? *

Mark only one oval.

- <19
- 19-35
- 36-60
- 61+

4. How would you classify your cybersecurity awareness level? *

Mark only one oval.

- Novice
- Moderate
- Good
- Excellent

5. What is your level of education achieved? *

Mark only one oval.

- Matric or Lower
- Certificate
- Degree
- Honours
- Masters+

General

This will be questions based on the game and your experience while playing.

6. On a scale of 1 to 5, how much has the game improved your understanding of information security threats (e.g., phishing, malware)? *

Mark only one oval.

	1	2	3	4	5	
Not	◯	◯	◯	◯	◯	Very much

7. How confident do you feel about identifying potential information security risks after playing the game? *

Mark only one oval.

	1	2	3	4	5	
Not	◯	◯	◯	◯	◯	Extremely confident

8. Which, if any, of the threats experienced in the game have you also experienced in real life? Please name them otherwise just reply none. *

9. Which information security concepts presented in the game did you find most valuable or memorable? *

10. Are there any other topics you consider should be included in this game? Please name them. *

11. How engaging was the game's storyline? *

Mark only one oval.

	1	2	3	4	5	
Not	◯	◯	◯	◯	◯	Extremely engaging

12. Were the game objectives clear? *

Mark only one oval.

	1	2	3	4	5	
Not	◯	◯	◯	◯	◯	Very

13. Rate the effectiveness of the game's challenges and tasks in maintaining your interest. *

Mark only one oval.

	1	2	3	4	5	
Very	◯	◯	◯	◯	◯	Very effective

14. Did the game's design elements (graphics, interface) enhance your learning experience? *

Mark only one oval.

	1	2	3	4	5	
Not	◯	◯	◯	◯	◯	Very much

15. How realistic were the scenarios and situations presented in the game in depicting real-world information security issues? *

Mark only one oval.

	1	2	3	4	5	
Not	◯	◯	◯	◯	◯	Extremely realistic

16. Did the game allow you to apply information security knowledge in simulated situations? *

Mark only one oval.

	1	2	3	4	5	
Nev	◯	◯	◯	◯	◯	Always

17. How well do you think the simulated experiences prepared you for handling actual information security threats? *

Mark only one oval.

	1	2	3	4	5	
Not	◯	◯	◯	◯	◯	Extremely prepared

18. What age would you consider should be the target audience? (tick all relevant boxes) *

Check all that apply.

- [ ] Age: 7-13
- [ ] Age: 14-18
- [ ] Age: 19-35
- [ ] Age: 36-60
- [ ] Age: 61+

19. What suggestions do you have to improve the game's effectiveness in teaching information security awareness? *

Appendix E

Final questionnaire

Cyber Cadet Threat Detector Questionnaire : Full Study

Please consider taking part in my academic study.
This study involves your participation in a serious game designed to promote information security awareness through simulated experiences. The target audience for this study is the youth, and the goal is to evaluate the effectiveness of the game in enhancing

information security knowledge. Your participation will be greatly appreciated and will contribute significantly to my Master's research!

Purpose of Study:

- The purpose of this Master's study is to design and assess a serious game that uses simulated experiences to educate youth on information security awareness. If you have any questions regarding this study, you may contact me or my supervisor (contact details are provided below).

General Information about the Study:

- Participation in this study is voluntary.
- The study involves playing the game and completing a short questionnaire afterward.
- You are unlikely to experience any discomfort or risks during the study.
- No compensation will be provided for participation.

Confidentiality:

- All information collected will remain anonymous and confidential. Data will be used solely for research purposes and stored securely.

Contact details of Researcher:

- **Full Name:** Christo C. Croucamp
- **School:** School of Computer Science and Information Systems
- **University:** North-West University
- **Country:** South Africa
- **Email:** 32177186@mynwu.ac.za

Contact details of Supervisor #1:

- **Full Name:** Gunther R. Drevin
- **School:** School of Computer Science and Information Systems
- **University:** North-West University
- **Country:** South Africa
- **Email:** gunther.drevin@nwu.ac.za

Contact details of Supervisor #2:

- **Full Name:** Lynette Drevin
- **School:** School of Computer Science and Information Systems
- **University:** North-West University
- **Country:** South Africa
- **Email:** lynette.drevin@nwu.ac.za

* Indicates required question

If using a windows computer,
Please download and access the game (CyberCadetThreatDefender_Windows_V05.zip) from: Cyber Cadet Threat detector

If using a mac,
Please download and access the game (Godot_v4.3_WithCyberCadetForMac-V05.zip) from: Cyber Cadet Threat detector

You need to play the game before starting the questionnaire. It is also important to note that for the final question you will be asked about the score you achieved please use the screenshot as a reference and note down your score achieved like this:

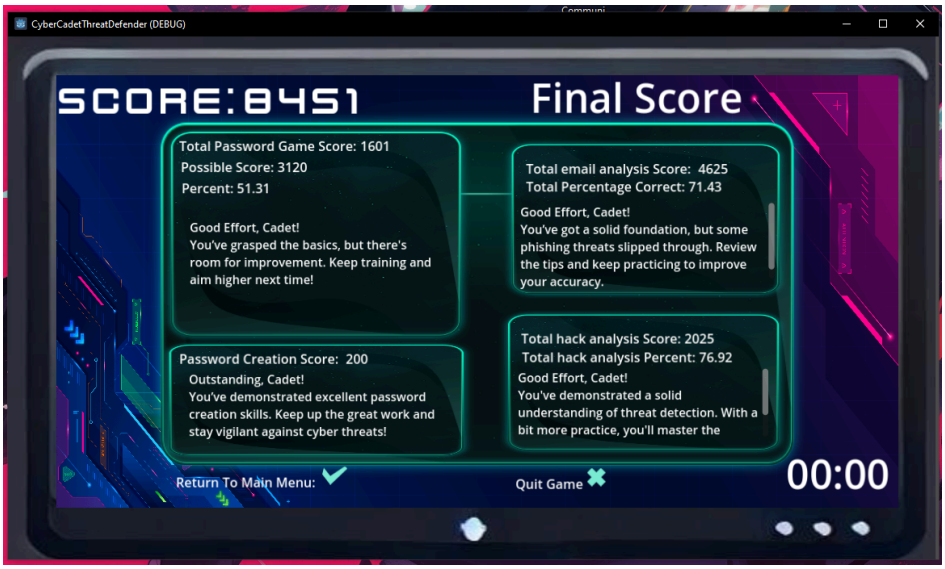
Total password game score = 1601
Possible Score = 3120
Percent = 51.31

Password Creation Score = 200

Total email analysis score = 4625
Total percentage correct = 71.43

Total hack analysis score = 2025
Total hack analysis percent = 76.92

Use this as an example. The final question will ask you to provide the scores.



1. Do you give consent to be apart of the research project? *

   Mark only one oval.

   - ◯ Yes *Skip to question 2*
   - ◯ No

Biographical and Awareness Information

This section contains non identifiable question to create an biographical and awareness level profile.

2. What is your gender? *

   Mark only one oval.

   - ◯ Male
   - ◯ Female
   - ◯ Prefer not to say

3. Which age group do you fall in? *

   Mark only one oval.

   - ◯ <19
   - ◯ 19-35
   - ◯ 36-60
   - ◯ 61+

4. How would you classify your information security awareness level? *

   Mark only one oval.

   - ◯ Novice
   - ◯ Moderate
   - ◯ Good
   - ◯ Excellent

5. What is your level of education achieved? *

Mark only one oval.

- ◯ Matric or Lower
- ◯ Certificate
- ◯ Degree
- ◯ Honours
- ◯ Masters+

6. In which of the following groups do you fall(Please indicate all relevant ones)

Check all that apply.

- ☐ Parent
- ☐ Teacher
- ☐ Industry Expert(Computer scientist, Developer, Security expert etc.)
- ☐ Gaming Enthusiast/Expert

General

This will be questions based on the game and your experience while playing.

7. On a scale of 1 to 5, how much has the game improved your understanding of information security threats (e.g., phishing, malware)? *

Mark only one oval.

	1	2	3	4	5	
Not	◯	◯	◯	◯	◯	Very much

8. How confident do you feel about identifying potential information security risks after playing the game? *

Mark only one oval.

	1	2	3	4	5	
Not	◯	◯	◯	◯	◯	Extremely confident

9. Which, if any, of the threats experienced in the game have you also experienced in real life? Please name them; otherwise just reply "none". *

10. Which information security concepts presented in the game did you find most valuable or memorable? *

11. Are there any other topics you consider should be included in this game? Please name them. *

12. How engaging was the game's storyline? *

Mark only one oval.

	1	2	3	4	5	
Not	◯	◯	◯	◯	◯	Extremely engaging

13. Were the game objectives clear? *

Mark only one oval.

	1	2	3	4	5	
Not	◯	◯	◯	◯	◯	Very

14. Rate the effectiveness of the game's challenges and tasks in maintaining your interest. *

Mark only one oval.

	1	2	3	4	5	
Very	◯	◯	◯	◯	◯	Very effective

15. Did the game's design elements (graphics, interface) enhance your learning experience? *

Mark only one oval.

	1	2	3	4	5	
Not	◯	◯	◯	◯	◯	Very much

Appendix F

Ethics approval

NORTH-WEST UNIVERSITY
NOORDWES-UNIVERSITEIT
YUNIBESITI YA BOKONE-BOPHIRIMA

Private Bag X1290, Potchefstroom
South Africa 2520

Tel: 018 299-1111/2222
Fax: 018 299-4910
Web: http://www.nwu.ac.za

Senate Committee for Research Ethics
Tel: 016 910 3446
Email: Feziwe.Mseleni@nwu.ac.za

ETHICS APPROVAL LETTER OF STUDY

Based on approval by the **Faculty of Natural and Agricultural Sciences Ethics Committee (FNASREC)**, the Faculty of Natural and Agricultural Sciences Ethics Committee hereby **approves** your study as indicated below. This implies that the North-West University Senate Committee for Research Ethics (NWU-SCRE) grants its permission that, provided the special conditions specified below are met and pending any other authorisation that may be necessary, the study may be initiated, using the ethics number below.

Study title: A serious game to promote information security awareness by utilizing simulated experiences, among the youth.
Study Leader/Supervisor: Prof GR Drevin
Student: CC Croucamp

Ethics number:

N	W	U	-	0	1	4	3	5	-	2	3	-	A	9
Institution				Study Number						Year			Status	

Status: S = Submission; R = Re-Submission; P = Provisional Authorisation; A = Authorisation

Application type: Single **Risk Category:** **Minimal**

Commencement date: 30/11/2023
Expiry date: 28/02/2025

Approval of the study is initially provided for a year, after which continuation of the study is dependent on receipt and review of the annual (or as otherwise stipulated) monitoring report and the concomitant issuing of a letter of continuation.

Special in process conditions of the research for approval (if applicable):

- The following documentation are archived by FNASREC and should be complete and kept up to date:
  - Research proposal
  - Signed approval from the scientific committee indicating the proposed risk category
- All researchers involved in the study should submit signed NWU code of conduct statements annually.
- All researchers of low risk studies should submit proof of relevant ethics training every two years.
- All researchers that take part in activities that pose a safety and security threat to the researchers or the environment should submit a risk assessment form annually.
- All research involving human interaction should follow best ethical practise and keep documents as proof. This includes informed consent, questionnaires, incorporation of risk-benefit, and responsible data management.
- Any research at governmental or private institutions, permission must still be obtained from relevant authorities and provided to the FNASREC. Ethics approval is required BEFORE approval can be obtained from these authorities.

Special conditions:
The best practices with regards to interviews should be implemented, including proper negotiation of access to participants; representative sampling; documented informed consent that includes the important elements; alignment of information collected with research questions; anonymization of collected information, ensuring the integrity and security of all data collected.

General conditions:
While this ethics approval is subject to all declarations, undertakings and agreements incorporated and signed in the application form, the following general terms and conditions will apply:

- *The study leader/supervisor (principle investigator)/researcher must report in the prescribed format to the FNASREC:*
  - *annually (or as otherwise requested) on the monitoring of the study, whereby a letter of continuation will be provided, and upon completion of the study; and*
  - *without any delay in case of any adverse event or incident (or any matter that interrupts sound ethical principles) during the course of the study.*
- *The approval applies strictly to the proposal as stipulated in the application form. Should any amendments to the proposal be deemed necessary during the course of the study, the study leader/researcher must apply for approval of these amendments at the FNASREC, prior to implementation. Should there be any deviations from the study proposal without the necessary approval of such amendments, the ethics approval is immediately and automatically forfeited.*
- *Annually a number of studies may be randomly selected for an external audit.*
- *The date of approval indicates the first date that the study may be started.*
- *In the interest of ethical responsibility, the NWU-SCRE and FNASREC reserves the right to:*
  - *request access to any information or data at any time during the course or after completion of the study;*
  - *to ask further questions, seek additional information, require further modification or monitor the conduct of your research or the informed consent process;*
  - *withdraw or postpone approval if:*
    - *any unethical principles or practices of the study are revealed or suspected;*
    - *it becomes apparent that any relevant information was withheld from the FNASREC or that information has been false or misrepresented;*
    - *submission of the annual (or otherwise stipulated) monitoring report, the required amendments, or reporting of adverse events or incidents was not done in a timely manner and accurately; and / or*
    - *new institutional rules, national legislation or international conventions deem it.*
- *FNAS-REC can be contacted for further information or any report templates via Roelof.Burger@nwu.ac.za 018 299 4269*

The FNASREC would like to remain at your service as scientist and researcher, and wishes you well with your study. Please do not hesitate to contact the FNASREC or the NWU-SCRE for any further enquiries or requests for assistance.

Yours sincerely,

Prof Roelof Burger
Chairperson Faculty of Natural and Agricultural Sciences Ethics Committee (FNASREC)

H C Sieberhagen — *Translator and Editor*
SATI no 1001489 — *082 3359846*
hettiesieb@gmail.com — *018 264 2309*

CERTIFICATE
OF LANGUAGE EDITING

ISSUED ON 19 MARCH 2025

This serves to certify that I have edited the language

of the dissertation

A serious game to promote information security awareness by utilising simulated experiences among the youth

by

C C Croucamp

orcid.org 0009-0002-6421-422X

Dissertation submitted in fulfilment of the requirements for the degree

***Master of Science* in Computer Science**

at the **North-West University**

Supervisor: Prof GR Drevin

Co-supervisor: Prof L Drevin

Examination: March 2025

Student number: 32177186

The responsibility to effect the recommended changes remains with the student

H C Sieberhagen
SATI no 1001489

19 March 2025