A mobile serious game to promote digital wellness among pre-school children

J Allers

orcid.org/0000-0002-6896-4020

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

Supervisor:	Prof GR Drevin
Co-Supervisor:	Mr DP Snyman
Co-supervisor:	Prof HA Kruger
Assistant-Supervisor:	Prof L Drevin

Graduation May 2021

25847465

Acknowledgements

I thank the following people for their contributions, for without them, this study would not have been possible:

My supervisor, Prof GR Drevin

My Co-supervisors, Mr DP Snyman and Prof HA Kruger.

My Assistant-supervisor, Prof L Drevin.

The individuals that participated in this study.

My parents, Johan and Janet Allers for their unending love and support.

My girlfriend, Sonja Marx for her understanding, love and support.

And above all, I thank God for the ability and His grace.

Abstract

Children today are more exposed to cyberspace and cyber threats than any of the previous generations. Due to the ever-evolving nature of digital technologies, devices like cell phones and tablets are more accessible to both young and old and although technological advancements create many opportunities to its users, it also exposes them to many different threats. Young users are especially vulnerable to these threats, as they are rarely educated about these threats and how to protect themselves against it. One possible solution to this problem is to create a mobile serious game that promotes digital wellness among pre-school children. Digital wellness can be defined as maintaining a good mental and physical wellbeing when using digital and online technologies. This study aims to identify different critical elements that, when implemented into a mobile serious game, will result in a game that is fun to play, appropriate for pre-school children and will spread awareness of digital wellness among the pre-school children. The question that this study aims to answer is: "What critical elements should be implemented into a mobile serious game to effectively promote digital wellness among pre-school children?"

In order to answer the research question, a literature review was conducted to identify critical elements and these elements were then implemented in a mobile serious game. The game was reviewed by six experts in the field of pre-school education, to validate the identified elements and to identify any possible additional elements. The results of the expert review verified that all of the elements identified from the literature are critical elements and the reviewers identified five additional elements. The following critical elements were thus identified: structured challenge; fantasy; choice; rules; competition; clear and simple goals; aesthetics; quality feedback and rewards; appropriate interface; balanced simplicity and complexity; use of appropriate material for the target group; presenting of the material in an appropriate way; focusing on different topics of digital wellness; short playtime; balanced work and play; quality interactions and replayability.

Keywords: Digital wellness; serious games; cybersecurity awareness; cybersafety for children; digital wellness for pre-school children

Opsomming

Kinders word vandag meer blootgestel aan die kuberruimte en kuberbedreigings as enige van die vorige generasies. As gevolg van die aanhoudende ontwikkelende aard van digitale tegnologieë, is toestelle soos selfone en tablette toegankliker vir beide jonk en oud en alhoewel tegnologiese vooruitgang baie geleenthede vir gebruikers bied, stel dit hulle ook bloot aan baie bedreigings. Jong gebruikers is veral kwesbaar vir hiervoor, aangesien hulle selde ingelig word oor hierdie bedreigings en hoe om hulself daarteen te beskerm. Een moontlike oplossing vir hierdie probleem is om 'n mobiele speletjie te skep wat digitale welstand onder voorskoolse kinders bevorder. Digitale welstand kan gedefinieer word as die handhawing van 'n goeie geestelike en fisiese welstand terwyl digitale en aanlyn tegnologieë gebruik word. Die doel van hierdie studie is om kritieke elemente te identifiseer wat, wanneer dit in 'n mobiele speletjie geïmplementeer word, sal lei tot 'n speletjie wat lekker is om te speel, toepaslik is vir kleuters en wat bewustheid van digitale welstand onder die kleuters sal bevorder. Die vraag wat hierdie studie beoog om te beantwoord, is: "Watter kritieke elemente moet in 'n mobiele, ernstige speletjie geïmplementeer word om digitale welstand onder voorskoolse kinders effektief te bevorder?"

Om die navorsingsvraag te beantwoord, is 'n literatuuroorsig gedoen om kritiese elemente te identifiseer, en hierdie elemente is dan in 'n mobiele, ernstige speletjie geïmplementeer. Die speletjie is deur ses kundiges op die gebied van voorskoolse onderwys hersien om die geïdentifiseerde elemente te bevestig en om addisionele elemente te identifiseer. Die resultate van die oorsig deur die kundiges het bevestig dat al die elemente wat uit die literatuur geïdentifiseer is, kritieke elemente is en vyf addisionele elemente is geïdentifiseer. Die studie het die volgende kritieke elemente geïdentifiseer: gestruktureerde uitdaging; fantasie; keuse; reëls; kompetisie; duidelike en eenvoudige doelwitte; estetika; kwaliteit terugvoer en belonings; toepaslike koppelvlak; gebalanseerde eenvoud en kompleksiteit; gebruik van toepaslike materiaal vir teikengroep; materiaal wat op 'n gepaste manier aangebied word; fokus op verskillende onderwerpe van digitale welstand; kort speeltyd; gebalanseerde werk en spel; kwaliteit interaksies en herspeelbaarheid.

Sleutelwoorde: digitale welstand; ernstige speletjies; bewustheid oor kuberveiligheid; kuberveiligheid vir kinders; digitale welstand vir voorskoolse kinders

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Background

Cyberspace is an artificial world with infinite possibilities that allow humans to navigate an information-based space (Benedikt, 1991). With the high growth of the internet, social media, online communication, internet of things, etc., most humans are connected to cyberspace, whether they want to be or not. According to Von Solms and Fischer (2017), most of the technological advancement that takes place in Africa and especially in South Africa, is in the mobile sphere. The main reasons why this is true, is because young people are currently the main clients of the digital uptake in developing countries and therefore mobile devices are easier and cheaper to acquire than other digital devices. (Phyfer et al., 2016; South African Broadcasting Corporation & The Henry J. Kaiser Family Foundation, 2007). This means that younger generations have more exposure to technology than previous generations and thus the younger generations provide a big driving force for technological advances in developing countries.

This technological advancement holds many advantages to developing countries and it also presents many new opportunities for the younger generations, but with these advantages, there are also many dangers. One issue that arises from this exposure to cyberspace, is that young people are much more likely to be exposed to negative online experiences and cyber threats than other groups. The reason why these individuals are more likely to have negative experiences is because they are exposed to cyberspace without knowledge of how to maintain a good digital wellness (Phyfer et al., 2016).

Digital wellness can be defined as being healthy in a digital society. This involves being able to distinguish between dangers and opportunities in the digital realm, acting responsibly in online situations and aligning online behaviour with offline values, thereby to ensure digital safety and security (Von Solms & Fischer, 2017). Digital wellness thus does not only mean avoiding threats to data, assets and security, but it also means maintaining

a physical and mental wellbeing.

Individuals especially at risk to the dangers of cyberspace are pre-school children. Pre-school children are exposed to cyberspace and all of its dangers from a very young age and the children usually do not possess the skills and knowledge to protect themselves from these dangers (Von Solms & Fischer, 2017). Although there are a lot of educational material and awareness strategies that focus on the awareness of cybersecurity and education about it, these methods rarely address educating a young audience of pre-school children about how to protect themselves against cyber threats. These resources are not suitable for pre-school children, because pre-school children have different and specific requirements when it comes to learning. One of these requirements is to present information in different ways and to include different methods of learning, because most pre-school children are not able to read or write. Another requirement is that the content should be presented in an easily understandable and fun way, to ensure that the pre-school children will be interested and motivated to participate.

Although the increasing number of pre-school children using mobile devices to access cyberspace creates security risks, it also creates an opportunity to educate them about cyber threats and the dangers of cyberspace. Because children learn through playing games (Yogman et al., 2018), using a serious game on a mobile platform could be considered to be a viable method of promoting the different concepts of digital wellness among pre-school children.

A serious game is an application that presents serious aspects with utilitarian functions, as a video game (Alvarez & Djaouti, 2011). By using a serious game which appeals to pre-school children, on mobile devices that they are familiar with, the youth of developing countries could be educated about the dangers that exist in cyberspace. Also how to defend themselves and act against these dangers.

Although using a mobile serious game is a viable method of promoting digital wellness among pre-school children, the success of such a game is not guaranteed (Callaghan & Reich, 2018). However, there are certain factors that can be considered and elements that can be implemented that will increase the game's chance of success. By identifying these different factors and critical elements, it becomes possible to create a mobile serious game that contributes to the goal of spreading awareness of digital wellness among pre-school children.

1.2 Research question

This study is about the use of a mobile serious game as a viable method of promoting awareness of digital wellness and cybersecurity among pre-school children. To increase the viability of this medium as a tool for spreading digital wellness awareness, this study will focus on identifying elements that, when implemented into a mobile serious game, will result in a game that is fun to play, appropriate for pre-school children and will spread awareness of digital wellness among pre-school children.

The research question of the study is as follows:

"What critical elements should be implemented into a mobile serious game to effectively promote digital wellness among pre-school children?".

1.3 Research objectives

The primary goal of this study is to identify different elements that, when implemented into a mobile serious game, will result in a game that promotes digital wellness among pre-school children. If these elements are implemented, the resulting game should satisfy the following criteria: The game should be fun; the game should be suitable for pre-school users; and the game should promote digital wellness.

To achieve the main goal, the following secondary objectives have been set:

1. Identify critical elements from literature that, when implemented in a mobile serious game, will satisfy the criteria mentioned above;
2. Develop a mobile serious game that implements the elements identified in the literature;
3. Use expert reviews to validate the elements implemented in the mobile serious game and to identify additional elements; and
4. Evaluate and list all of the elements identified from literature and the expert reviews.

1.4 Research design

This study is conducted using the positivist paradigm with a design science methodology.

Positivist research aims to discover rules and laws that govern the universe and it is generally informed by realism, idealism and critical realism. When using a positivist paradigm, the ontological assumption can be made that there is one reality that is knowable within probability. Data is gathered using questionnaires, observations, tests and experiments and the nature of

the knowledge gained using a positivist paradigm is objective and based on verifiable observation and measurement (Kawulich, 2001).

The purpose of design-science research is to obtain knowledge and understanding of a problem or problem domain, through the development of an artefact. The following list shows the 7 guidelines for design science research (Hevner et al., 2004):

1. Design as an artefact - Design-science research must produce a viable artefact;

2. Problem relevance - The objective of design-science research is to develop technology-based solutions to important and relevant business problems;

3. Design evaluation - The utility, quality, and efficacy of a designed artefact must be rigorously demonstrated;

4. Research contributions - Effective design-science research must provide clear and verifiable contributions;

5. Research rigour - Design-science research relies upon the application of rigorous methods in both the construction and evaluation of the designed artefact;

6. Design as a search process - The search for an effective artefact requires utilizing available means to reach desired ends while satisfying laws in the problem environment; and

7. Communication of research - Design-science research must be presented effectively both to technology-oriented as well as management-oriented audiences.

1.5 Chapter outline

For this study the process is as follows:

In Chapter 2, a broad overview of cyberspace and cybersecurity are given. This includes an explanation of what cyberspace and cybersecurity is, as well as a brief look at the different dangers that exist in cyberspace and how to defend against them. This chapter is also used to briefly discuss the topic of cybersecurity awareness campaigns.

The concept of digital wellness is explored in Chapter 3. This concept is further explained by listing the different elements of digital wellness. Digital wellness for pre-school children is also discussed in this chapter, followed by an overview of the “Digital wellnests” book and digital wellness awareness for children.

Chapter 4 defines the concept of serious games. First, the concept of play is explained, followed by a clarification of different types of games and the classification of these games. This chapter finally identifies different elements of good games and elements necessary for pre-school children.

In Chapter 5, the technical aspects of the created mobile serious game is discussed. This is done by listing the different elements identified from literature that should be implemented, explaining what technologies were used in the development phase and giving a complete overview of the application and the elements implemented.

Chapter 6 presents a compilation of the results and a conclusion. In this chapter, the results of the expert review is analysed to verify the elements implemented in the application and to identify new elements. These elements are finally summarized and presented as an answer to the research question.

Finally, Chapter 7 a conclusion to the study is presented. In this chapter an overview of how the research objectives were met is given, followed by a list of limitations that the study encountered. In this chapter the contributions of this study to the existing body of knowledge is discussed and suggestions are made for future work.

1.6 Summary

With the increase of young users of cyberspace, it becomes necessary to implement a strategy to spread awareness of the dangers of cyberspace, especially among the youngest users. One approach for promoting awareness is to create a mobile serious game aimed at pre-school children. This study focuses on identifying core elements that can increase the success of a mobile serious game to promote digital wellness among pre-school children, so that these elements can be used as a baseline in future work.

In this chapter an introduction to and substantiation of the current study was given. The background of the problem was explained, the research question, research goal and research design was introduced, followed by a brief overview of the remaining chapters. In the next chapter, a review of the literature on cyberspace is given.

Chapter 2

Cyberspace

In this chapter the required background on cyberspace, cybersecurity and basic defensive measure that can be taken to defend against various cyber threats, is presented.

In Section 2.1 cyberspace and the history of cyberspace is discussed, followed by Section 2.2, where the concept of security in the cyber realm is further defined. After these concepts are explained, some of the different threats that exist in cyberspace are listed and briefly discussed in Section 2.3 and next the different safety measures and defences that can be used to protect users from these threats and dangers are explored in Section 2.4. This chapter ends in Section 2.5 with a brief overview of cybersecurity awareness and the different elements necessary for a successful awareness campaign.

2.1 Defining cyberspace

Data is everywhere. In modern society, most people's lives are irreversibly interwoven with technology and our daily operations are drastically influenced by the complex environments created by the ongoing development of information technology (Stolterman & Fors, 2004).

2.1.1 The origin of cyberspace

The origin of cyberspace had an immeasurable impact on society as we know it today and it has not only influenced every human living today, but it will almost certainly affect all generations to come. Even though the creation of cyberspace has had this huge impact, it is difficult to exactly pinpoint a date or even an event that triggered the creation of cyberspace (Andersen, 2019). Many people believe that the origin of cyberspace was due to the founding of the World Wide Web in 1990 by the British scientist, Tim Berners-Lee (McPherson, 2009), but others may believe that the origin of cyberspace

started with the first use of the word.

The first ever mention of cyberspace was made by two Danish artists, Susanne Ussing and Carsten Hoff (Andersen, 2019; Ning et al., 2018). Ussing and Hoff first used this word in the 1960's when naming their art studio, Atelier Cyberspace. When asked, Hoff confirmed that the word did not refer to anything digital or virtual, but that it rather referred to "sensory spaces". Hoff further defined these "sensory spaces" as a room that physically exists, but senses humans and then adapt to them (Kryger & Mathias, n.d.). The use of the word cyberspace in the context of art and artworks did however not make any lasting impact and thus perished, until it was used again in 1982 in the context that we are familiar with today (Andersen, 2019).

2.1.2 Defining cyberspace

In 1982 the American-Canadian fiction writer and essayist, William Gibson, used the term cyberspace in his short stories "Burning Chrome" and "Neuromancer". Not only did Gibson coin this term, he also envisioned the existence of both the internet and virtual reality long before either of these concepts were created. Gibson is widely viewed as the individual who, by creating these short stories and envisioning these futuristic concepts, created the initiative for making these fantasies a reality (Andersen, 2019).

In 1991 Benedikt explored several different definitions and approaches to cyberspace. In his paper, Cyberspace: first steps, (Benedikt, 1991) Benedikt does an in-depth study of these approaches until he finally reaches the conclusion with reference to the researchers whose definitions he had studied:

> "Indeed, the very definition of cyberspace may well be in their hands (or yours, dear reader)." (Benedikt, 1991, p.23)

Since the creation of the word cyberspace in 1982, the term has become an everyday word, not only being used by scholars, researchers and professionals, but also by the layperson. As the concept of cyberspace became a reality and evolved past anyone's expectations, the very definition of the word also evolved and changed to a point where there is not one clear definition, but rather a collection of definitions that are often debated about. Even though the definitions given above were satisfactory at the time they were written, a modern definition is needed to define the concept of cyberspace as it is today. It is however clear that a single definition will not be adequate for defining the concept of cyberspace, as cyberspace is ever changing and evolving to adapt to the billions of humans that come into contact with it every day.

For the sake of this study, the following statement by Ning et al. (2018) will be accepted as a broad definition of cyberspace:

> "Generally speaking, the concept of space in cyberspace tends to be abstract and mathematical, without the quality of volume. Therefore, the cyberspace in the conventional sense is merely a virtual, digital world created, based on various infrastructures such as computers, networks, data and information, hardware and software, etc., which we call conventional cyberspace or cyberspace in short." (Ning et al., 2018, p.1843)

This definition is accepted, because it does not attempt to define the evolving possibilities and applications of cyberspace, but rather connects the term to the infrastructure that it is based on. It also clearly states that cyberspace is a virtual and digital realm that is removed, but not disconnected from our reality.

Investigating the modern concept of cyberspace, one finds that one of the most prominent characteristics is that of interconnectedness (Ottis, 2011). Because cyberspace is based on different infrastructures that are all connected (Ning et al., 2018), one of the inherent features of cyberspace is its communication capabilities. These capabilities enable cyberspace to be used as a social platform that connects not only hardware and software across the world, but also connects the billions of users of these different infrastructures. These users' lives have become intertwined with modern cyberspace, meaning that cyberspace has become a part of modern society (Ramlakhan, 2011).

Although cyberspace has changed the average human life for good mostly, cyberspace cannot be defined as inherently good or bad. I.e. it can be used for both of these purposes (Balvin & Tyler, 2006; Latour, 2002). This fact ultimately leads to misconduct in cyberspace. Due to the fact that cyberspace is ever-evolving and social in nature, a lot of threats can persist in this cyber realm and because of modern society's dependence on cyberspace, these threats, although digital, can have irreversible, real world effects (Abomhara & Køien, 2015). For protection against these threats, it is important to be mindful of security, but given that these threats exist in a digital realm, normal security measures will not be effective and it is thus necessary to apply cybersecurity.

In this section, a definition of cyberspace was given as it applies to this study. This was achieved by discussing the evolution of cyberspace from the first time it was mentioned. From this exploration of cyberspace and its evolution, it became clear that there is no universally accepted definition for cyberspace, but a definition that is applicable to this study was outlined. This information led to the conclusion that there are threats in cyberspace and that a digital form of security is needed to ensure the safety of users in the cyber realm.

2.2 Cybersecurity / Digital security

While defining cyberspace in Section2.1, it became clear that cyberspace is a constantly growing social environment, with near infinite different uses. Therefore, cyberspace has become a vital and irreplaceable part of modern society, hosting not only billions of users daily, but also data and information of people, companies and governments. This information includes, but is not limited to sensitive data, personally identifiable information, protected health information, personal information, intellectual property and governmental and industrial information systems.

A threat that exists in cyberspace can therefore not only affect personal and private information, but it can also directly or indirectly affect a user's physical and mental well-being. Therefore, one can conclude that a form of digital security must be implemented and upheld by users of cyberspace to ensure that a safe cyber environment is maintained. When discussing digital security, there are two main topics that both describe a certain form of digital security. These two topics are information security and cybersecurity. Although many consider these two words to mean the same thing, a distinct difference exists between information security and cybersecurity.

2.2.1 Information security

As the name would suggest, information security involves securing information from numerous types of threats. In an attempt to define the entirety of information security, the international standard, ISO/IEC 27002 (2005), has identified three critical elements of information that should be preserved. These elements are the confidentiality, integrity and availability of information, also commonly referred to as the CIA triangle (Disterer, 2013).

- Confidentiality: Access to information must be controlled.
- Integrity: Information must be trustworthy and unchanged.
- Availability: Reliable and constant access to information should be provided.

In an attempt to improve on the CIA triangle, experts have proposed four more critical elements, namely accuracy, authenticity, utility and possession (Whitman & Mattord, 2017; Parker, 2015).

- Accuracy: Information must be accurate and error free.
- Authenticity: Information should be verified as original and not a reproduction.
- Utility: A use or purpose for the information should exist.
- Possession: The possession of information should be controlled.

Upon further investigation of the critical properties of information security, as stated above, it becomes clear that there is no limitation on the medium in which the information is presented. This means that information security applies to all forms of information, both digital and hard copies, whether it is stored or in transit. As the problem stated in Chapter 1 focuses only on digital threats and cyberspace, it is not necessary to focus on the physical portion of information security. By disregarding the physical part of information security, we focus on the security of information and communication technology (ICT).

2.2.2 Information and communication technology security

The focus of ICT security is on information stored and transferred digitally. This means that ICT security focuses mainly on the protection of technology-based systems on which information is commonly stored and/or transmitted (Von Solms & Van Niekerk, 2013). As ICT security is a subset of information security, all of the critical characteristics that are needed to ensure information security, also apply to ICT security. There are, however, three more characteristics that apply to ICT security, that do not generally apply to information security as a whole. These are identified as non-repudiation, accountability and reliability (Von Solms & Van Niekerk, 2013; Dhillon, 2007).

- Non-repudiation: The validity of information cannot be denied.
- Accountability: Actions by an entity can be traced solely to that entity.
- Reliability: Information can be trusted to be true.

When considering the information given above, it is clear that information security, as well as ICT security, focus on the protection of data and information. Seeing that cyberspace exists in a digital world made up of data and information, ICT security might appear to be satisfactory to defend against threats in a digital realm, but there is one crucial aspect of cyberspace that ICT security does not take into account: threats to the user.

2.2.3 Cybersecurity

As discussed in Section 2.1, information is not the only vulnerable asset in cyberspace. Threats in cyberspace can, either directly or indirectly, have real world effects, that do not only extend to users, their safety and possessions, but also to entire societies (Von Solms & Van Niekerk, 2013). This makes it clear that information security is not an effective solution to the problem.

Unlike information security, cybersecurity is used as an all-inclusive term that does not only focus on protecting the data and information aspect of cyberspace, but also the technologies that it runs on and its many users. In other words, cybersecurity can be defined as a collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment, and also protect the user and user's assets (Von Solms & Van Niekerk, 2013).

The fact that cybersecurity is all inclusive when it comes to the protection of cyberspace, means that ICT security is not only a part of information security, but it is also a part of cybersecurity. This means that ICT security is the point where information security and cybersecurity converge (see Figure 2.1).

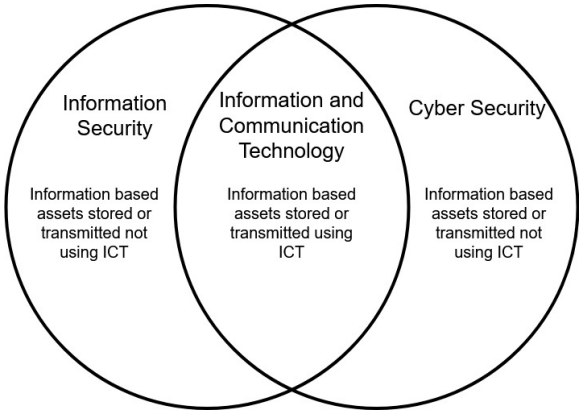

Figure 2.1: The relationship between information and communication security, information security, and cybersecurity.

Due to the fact that cybersecurity is so closely related to information security, the critical characteristics of information security, namely confidentiality, integrity and availability of information, accuracy, authenticity, utility and possession, are also the critical characteristics of cybersecurity. The critical difference however is cybersecurity's approach to protecting the users and their non-information-based assets.

In this section, the differences between information security, ICT security and cybersecurity are discussed by defining each of these securities' critical

characteristics, as well as the scope of what these different concepts attempt to protect. Before the different defences that cybersecurity offers can be discussed, it is firstly important to know what types of dangers users face in the digital realm. By defining different threats and their effects on users, not only will the potential dangers become clear, but also what users can do to protect themselves while visiting the digital realm.

2.3 Cyber threats

In an era of constant and exponential technological progression, where data is the user's most valuable asset, almost all users will be exposed to some form of cyber threat. The definition of cybersecurity, as given in Section 2.2, provides a general guideline of the different elements that need to be preserved in order for data to be considered safe and secure. Although these elements provide a good foundation for upholding cybersecurity, it would be of no use to any user, without understanding the different threats, attacks and vulnerabilities that exist in cyberspace.

2.3.1 Terminology

The following is a collection of different information security terms. It is necessary to know and understand these terms if one wants to defend oneself from the various dangers in the digital realm.

Assets

Assets are anything that has some form of value or importance to a user or system. Assets can be anything from data, information, systems, hardware, etc.

Vulnerability

According to the Glossary of Key Information Security Terms of NISTA (Kissel, 2013), vulnerability can be defined as a weakness in an information system that could be exploited or triggered by a threat source. Weaknesses can exist in the information system's security procedures, internal controls, or implementation. In other words, a vulnerability is a flaw or weakness in a system, that could possibly be exploited by an attacker (Abomhara & Køien, 2015). Weaknesses are not exclusive to either hardware or software. Both the hardware and the software of a system can be exploited by an intruder to gain access to the vulnerable system and to launch attacks and execute malicious commands (Bertino et al., 2010). The identification and repairing of hardware vulnerabilities are usually difficult tasks. The most common causes of hardware vulnerabilities are design flaws, hardware compatibility

and hardware interoperability. Software vulnerabilities can be present in any software in a system, such as its operating system, or its application and control software. The two biggest causes of software vulnerabilities are human errors and software complexity (Abomhara & Køien, 2015). Software component vulnerabilities can be divided into two categories (Bertino et al., 2010): Software defects, caused by inherent design flaws or errors in the code; and configuration errors, caused by unnecessary and dangerous services or misconfiguration in the system's access control.

Exposure

Exposure is a software weakness and it is very similar to vulnerability. The key difference between these two weaknesses, is that a vulnerability is caused by a software error that can be used to gain direct access to a system by an intruder, while an exposure can be either a software mistake or configuration error that does not jeopardize the system or its resources directly, but which can serve as an entry point for an attack (Bertino et al., 2010). Exposures can lead to unauthorised data capturing, modifying or replacing software on a system and many other forms of attack on the compromised system (Padmavathi & Shanmugapriya, 2009).

Threats

The Glossary of Key Information Security Terms of NISTA (Kissel, 2013) defines a threat as any circumstance or event that has the potential to negatively impact organizational operations, organizational assets, or individuals. This harm can be done to an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

Simply put, a threat is any action or event that is able to do harm to that system or any of its assets (Brauch, 2011). Therefore, threats are not always driven by humans, but it could also occur due to natural events (Abomhara & Køien, 2015; Rainer & Cegielski, 2010). Due to this fact, threats can be divided into two primary categories: natural threats and human threats. Natural threats are physical, natural events that can cause severe damage to a system and its assets. Natural disasters such as floods, hurricanes, earthquakes and even fires are examples of natural threats. The fact that these events can rarely be predicted or prevented means that the damage that they cause cannot be completely prevented, but it is possible to minimise that damage. By implementing disaster recovery countermeasures such as system backups and contingency plans, and by ensuring that all hardware are stored in secure locations, the damage caused by natural threats can be limited (Abomhara & Køien, 2015). Human threats are malicious actions taken by individuals or groups that aim to

harm or disrupt a system and its assets by exploiting vulnerabilities. Such individuals or groups are not always unauthorised outsiders attempting to do damage from outside the system, but they could also be internal users, with authorized access to the system. Human threats can further be divided into the following categories:

- Naive and accidental threats: Threats that are associated with human errors which is not intended to harm an organization or any of its assets (Parsons et al., 2014). Threats of this type usually stem from inside an organization and are seen as mistakes made by naive employees (Parsons et al., 2017);
- Unstructured threats: Threats from inexperienced individuals. The individuals can be seen as amateur hackers and they use easily accessible tools and frameworks; and
- Structured threats: Threats from experienced individuals or groups. Structured threats are posed by people who know system vulnerabilities and who understand, develop and exploit codes and scripts (Abomhara & Køien, 2015).

Attack

An attack (also called an exploit) is a type of human threat, where an individual or group (attacker) attempts to gain access to a system. The goal of this intrusion is usually to damage the system and its assets or to compromise the system's integrity (Bertino et al., 2010). According to Kissel (2013), an attack can be defined as any kind of malicious activity with the intent to collect, disrupt, deny, degrade, or destroy information, the resources of an information system or the information that resides on the system.

Attacks are carried out by the attackers, by intentionally exploiting a vulnerability in a system (Bertino et al., 2010). The different types of attacks and attackers will be further discussed in the following sections.

Figure 2.2 illustrates the relationship between threats, vulnerabilities and assets.

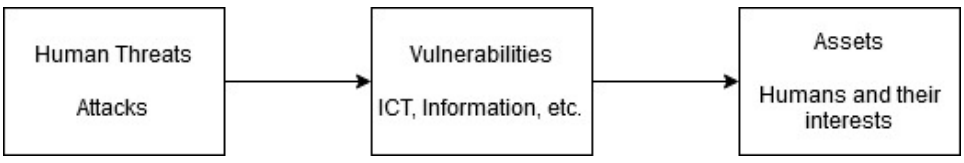

Figure 2.2: Relationship between threats, vulnerabilities and assets in cybersecurity.

In cyberspace, there are many different types of threats that can affect a user. One example of such a threat is an attack. These threats exploit the vulnerabilities in a system and by doing so, the integrity of the assets and interests of the user is compromised.

When defending assets in cyberspace, the user must be aware of the different threats and of defences against these threats. Even though natural threats can affect assets in cyberspace, these threats only occur in the physical world, meaning that it is not a cybersecurity threat and therefore, this study will not focus on different natural threats, but it will rather elaborate on the human threat of cyber attacks.

2.3.2 Attack types

In cyberspace, cyber attacks are occurring increasingly more frequent and defence against such attacks is becoming more intricate and difficult. One of the basic and most important defences against any form of cyber attack is being aware of the types of attacks that can occur and the dangers they pose to the user. The following is a brief overview of some of the most common types of attack. For the sake of this study, these attacks are divided into two groups: technical attacks and end-user attacks.

Technical attacks

The first group are technical attacks that indirectly affect the user by attacking servers and system. These attacks cannot be warded off by users.

Privacy attacks

Privacy attacks are specifically aimed at compromising the privacy of data and information that exist on or pass through a system or network. These privacy attacks are unique in the sense that they are the only type of attacks that are passive in nature. The reason for this is because the privacy attack does not attempt to damage a system nor does it attempt to compromise the integrity of data and information. It rather hides on a system and gathers information in anonymous manner (Padmavathi & Shanmugapriya, 2009). Common examples of passive privacy attacks are eavesdropping, traffic analysis and man-in-the-middle attacks.

- Eavesdropping - Like the name suggests, eavesdropping is a passive attack method that monitors and intercepts private communications in real time. This method does not send data to another device, but rather monitors the outgoing data from a user to a server. Even though this attack is passive, the intelligence gathered using this method can be used to cause immense damage to users and their assets (Grassi

et al., 2017; Teymourlouei, 2015; Kissel, 2013; Padmavathi & Shanmugapriya, 2009).

- Traffic analysis - Traffic analysis is a passive attack that analyses patterns and information about communications and traffic, rather than the content itself. Traffic analysis can be used to identify communication patterns and other useful data by analysing meta-data about traffic (such as durations and frequency of communications) without having to decrypt the content of the communications (Kissel, 2013; Padmavathi & Shanmugapriya, 2009).

- Man-in-the-middle attacks - A man-in-the-middle attack is a passive attack that enables the attacker to access data and information sent between devices or systems over a network. This attack is similar to the eavesdropping approach, with the main difference being that the man-in-the-middle attacker positions itself between the sender and receiver, disguised as a network node. Once the users exchange data, the attacker receives the data and then transmits to the receiver. Although this type of attack is usually passive, it can also be used to alter the received data before sending it, rendering it an active attack (Teymourlouei, 2015; Kissel, 2013).

Denial of Service attacks

A denial of Service (DoS) attack is a special kind of attack that attempts to overload a system or server (Teymourlouei, 2015). By using this method of overloading, the attacker can slow down the target system or even shut it down completely, meaning that the attacker can render the system or server unusable or unavailable to its intended users, hence, denying the services of the system to the users (Abomhara & Køien, 2015). DoS attacks are especially effective against time-critical operations and systems with low memory capabilities. Time-critical may be milliseconds or it may be hours, depending on the service provided (Kissel, 2013; Padmavathi & Shanmugapriya, 2009). DoS attacks can also be used to serve as a distraction from other vulnerabilities, possibly allowing other attacks to go unnoticed (Teymourlouei, 2015). One of the most widely used and effective types of DoS attacks is a Distributed Denial of Service (DDoS) attack. A DDoS attack is a DoS technique that uses multiple hosts or attacking nodes to target a system or server (Kissel, 2013). A common method of launching a DDoS attack, is by creating a network of bots or zombies. In DDoS attacks, a bot or a zombie is an infected system that, unbeknownst to its user, participates in the attack. The collection of these bots or zombies, called a botnet, launches a coordinated attack by flooding the target system with requests, ultimately forcing it to shut down (Rainer & Cegielski, 2010).

Because this attack is launched from multiple locations simultaneously, it can easily overload vulnerable systems and cause damage.

Back door attacks

A back door attack is a simple attack which can only be successfully executed if the system has a back door. A back door in a digital system is an undocumented way of gaining unauthorised access to a system. Back doors are usually hidden software or hardware mechanisms used to bypass security controls (Kissel, 2013). Back doors are commonly added to systems in the development phase, to allow developers to test specific functions or features in a system without passing all of the security measures. If a back door is not removed, it can cause serious security breaches to a system, by allowing unauthorised access to the system software (Rainer & Cegielski, 2010). When an attacker learns about the existence of a back door, it can be used to gain access to the system without triggering any of the security measures responsible for protecting the system.

End-user attacks

The second group of attacks is a list of attacks that directly affect the end-user. The users can defend against these threats to a certain degree.

Malware attacks

One of the most common tools used in cyber attacks is malware. Malware can be defined as any code that, when executed, causes malice on the user's device (Teymourlouei, 2015). Some of the most common functions or goals of malware is slowing or shutting down the infected system or even stealing valuable information. Because malware is such a broad term and because there are so many different types of malware, it is difficult to identify the core symptoms that they all share. However, the one defining characteristic of malware is its ability to quickly spread and infect multiple systems. The four most common forms of malware are spyware, viruses, worms and Trojan horses.

- Spyware - The primary goal of this type of malware is to steal valuable information from the infected computer. Once the spyware infects the system, it spies on the system and the activities of the user on that system (Teymourlouei, 2015).
- Viruses - Virus malware, similar to biological viruses, survive by attaching to a host. In the case of virus malware, the virus is a piece of code that attaches to another program on the system. The virus then uses the program to spread across the system and other devices,

slowly damaging or slowing it. The longer a virus is able to spread on a system, the more damage it will be able to do (Rainer & Cegielski, 2010).

- Worms - Malware worms are much like viruses. Worms also spread through a host system and performs malicious actions, but the one core difference is that a worm does not need a host program to replicate. This means that a worm is able to duplicate itself without requiring another program (Teymourlouei, 2015; Rainer & Cegielski, 2010).

- Trojan horse - A Trojan horse is a type of malware that, unlike most other kinds of malware, does not replicate itself. The primary function of a Trojan horse is to disguise itself as a useful or helpful program, until it is activated. Once the Trojan horse is active, it will start to execute its malicious code (Rainer & Cegielski, 2010).

Some of the most common methods for executing malware attacks include sending malware via email or a messaging system, uploading malware to websites that download when visited and embedding malware in different software. Another approach to malware attacks is using a blended attack. A blended attack attempts to spread malware on a target system using multiple delivery methods. These attacks will use multiple methods to spread malware such as spyware, viruses, worms and Trojan horses across a system.

Password attacks

A simple method of protecting assets from unauthorised access in a cyber realm is by using some form of identification to prove that the user, who is attempting to gain access, is indeed authorized to do so. The most common use of this method is setting up and using passwords. A password is a string of characters used to authenticate the identity of a computer system user or to authorize access to system resources (Kissel, 2013; Rainer & Cegielski, 2010). In simpler terms, a password serves as a key to gain access to a system and its assets and thus, any entity that has that key, has complete, authorised access to the system. Password attacks are methods used by attackers to uncover an authorised user's password and thus, gain access to the system (Raza et al., 2012). Many different password attack methods exist, each with its own applications and success rates. Three of the most popular methods include brute force attacks, dictionary attacks and shoulder surfing.

- Brute force attacks - A brute force attack is a straightforward, but time-consuming method of effectively guessing a password. This method involves attempting to apply all possible combinations of characters to the system as a password, until a valid password is uncovered (Rainer

& Cegielski, 2010). Brute force attacks are very resource intensive, meaning that it requires most of a system's computing resources, and, because these attacks have to search through all possible character combinations, they take exponentially longer to complete the longer the password is. The following is an example of how long a brute force attack can take as stated by Mudassar Raza (Raza et al., 2012, p.439) of the Comsats Institute of Information Technology:

> "For example a user enters a password of 8 characters and all characters are lower case letters. Then to break the password using the brute force attack it requires $(26)^8$, which is equal to 208827064576, combinations. If a single computer takes 1000 passwords to check in one second then total time will be 208827064576 / 1000 = 208827064.576 seconds which is equal to 58 007.52 hours."

This example illustrates that although brute force attacks may be effective when cracking short passwords, the time it takes to crack a password using the brute force method becomes exponentially longer as the password gets longer.

- Dictionary attacks - Similar to the brute force attack, the dictionary attack is also a password attack method that attempts to guess a valid password to a system. The core difference between these two methods is that where the brute force attack blindly attempts each possibility, the dictionary attack makes use of a type of dictionary to guess possible passwords based on words and combinations of words and characters (Kissel, 2013; Raza et al., 2012; Rainer & Cegielski, 2010). Because a dictionary attack only uses a set amount of words to crack a password, it is a much faster method of attack than the brute force method. The problem that the above-mentioned method has is that it is not guaranteed to crack every password. The dictionary attack requires that the attacker obtain or create a dictionary with commonly used words that the user might use as a password. When a dictionary attack is aimed at a specific user, the dictionary may be updated with information such as the user's name, surname, birthday, place of work or any other personal information that might be used to form the password. The dictionary is then applied to make an attempt to crack the password in a similar way to the brute force method. The biggest drawback of this method, is that it will not be able to crack a password if the password is not present in the dictionary itself (Raza et al., 2012).

- Shoulder surfing - Unlike brute force attacks and dictionary attacks, shoulder surfing is not an attack method that uses digital processing to crack a password, but it is rather a form of spying on a user in the physical world. In other words, shoulder surfing is a method of obtaining a user's password, or finding clues to what the password is, via observation (Raza et al., 2012). Common examples of this are hidden cameras that record the keyboard when a password is typed, or listening to the number of keys pressed when a password is entered, to narrow down the length of the password, or it can even be as simple as looking over someone's shoulder as they[1] are typing in their passwords.

Phishing attacks

When it comes to cybersecurity, one of the potentially biggest vulnerabilities of a system is the human factor. Due to the fact that most systems are digitally protected against threats, an attacker needs to outsmart the protection by using complex algorithms and methods. Opposite to the engineered, digital protection of a system, humans are much more susceptible to different forms of trickery and fooling. Phishing is a type of attack that does not attempt to access a user's personal assets or information by attacking a system, but rather by fooling a human to willingly produce the information (Grassi et al., 2017; Teymourlouei, 2015; Rainer & Cegielski, 2010). The most common method of doing this is by sending the user an authentic looking email or message from a seemingly trusted source. The email might directly ask for personal data from the user, or, in more sophisticated cases, the email may redirect the user to a website that requests this information (Kissel, 2013). Phishing attacks are aimed at large groups of people simultaneously and as a result of this, are very general and easy to identify. In an attempt to improve the success rate of phishing attacks, attackers started to personalise their messages and attacks to fit individuals. This method is called spear phishing. In a spear phishing attack, the attackers attempt to find as much information on the target as they possibly can and then use that information to send a personal phishing message. The increased amount of personal information in the message lends a type of credibility to it, with the result that more users will tend to cooperate and disclose their personal information.

[1] In this paper, the words 'they' and 'their' are often used in singular form as a gender neutral alternative to 'he', 'she', 'his' and 'her' (Swan, 1995, p.528)

2.3.3 Attackers and Motivation

Knowing the different cyber attacks that one can encounter is a good first step in preventing these attacks from happening and protecting one's assets. However, spreading awareness of these methods does not help one understand who launches these attacks or why they do it. If an attack is successfully executed, it can be very difficult to identify the entity responsible for the attack and thus, in many cases, these attackers are able to succeed in their attempt to enter, damage or steal from a user or system, without being identified. Even though these attackers may be difficult to identify, all attackers can be classified into certain categories based on their access, size and motives (Abomhara & Køien, 2015).

Access

Considering access, one can identify two basic types of attackers, namely insiders and outsiders.

- Insiders - An insider threat is caused by an entity that has authorised access to a system (Kissel, 2013). Simply put, an insider is an attacker that has access to a system and can thus launch an attack from inside the target system. Inside attackers are usually employees that have to use the system, which is why they have authorised access.

- Outsiders - As opposed to inside attackers, outside attackers do not have authorized access to the target system. These unauthorised attackers have to penetrate the defences of a target system before they can cause any damage to a system or its assets (Abomhara & Køien, 2015).

Size

When we mention the size of an attacker it refers to the number of people involved in the attack. By classifying attackers according to their size, three major categories can be identified. The three categories are individuals, organized groups and intelligence agencies (Abomhara & Køien, 2015).

- Individuals - Individual attackers are attacking entities that consist of only one member. Individuals work alone and usually have limited resources and expertise (Abomhara & Køien, 2015). They also usually target systems with low security that are easy targets (Sheldon, 2012). Individuals can range from amateurs to experts in attacking systems and their impact is usually less than that of the other categories.

- Organised groups - An organized group of attackers is, as the name suggests, a group of individuals, working in an organized manner to attack a target system. Organized groups usually consist of multiple professionals working together to reach their goal. They are usually more capable than individual attackers and their attacks have the potential to have a much larger impact (Abomhara & Køien, 2015). Organized groups are criminal groups or organizations, that migrated their operations to the digital realm, where they found an opportunity to continue their illegal activities on a new platform (Sheldon, 2012).
- Intelligence agencies - Unlike the individual attacker or the organized groups, intelligence agencies are massive organisations with many professionals, who execute large scale attacks. These attacks are usually attempts by agencies, from different countries, to probe the military systems of other countries (Abomhara & Køien, 2015). These agencies have organized structures and sophisticated resources to successfully execute their attacks.

Motivation

Unlike categorizing attackers by their access or size, categorizing attackers based on their motive is very difficult. The reasons behind an attack on a system may vary, but it can usually be traced back to either personal satisfaction or recompense (Abomhara & Køien, 2015). Abomhara and Køien (2015, p.77) summarised the different motivations for attacks as follows:

> "Government websites, financial systems, news and media websites, military networks, as well as public infrastructure systems are the main targets for cyber-attacks. The value of these targets is difficult to estimate, and estimation often varies between attacker and defender. Attack motives range from identity theft, intellectual property theft, and financial fraud, to critical infrastructure attacks. It is quite difficult to list what motivates hackers to attack systems. For instance, stealing credit card information has become a hacker's hobby nowadays, and electronic terrorism organizations attack government systems in order to make politics, religion interest."

2.4 Basic defences

Cyber attacks are ever-present threats that all users of cyberspace will face at some point in time and although these attacks cannot always be stopped completely, much can be done to limit their effectiveness. Being educated about these attacks and the dangers they pose can prove to be

very beneficial to the user when setting up defences and guidelines to avoid and limit damages caused by these threats. When setting up defences to protect one's assets against cyber threats, it is important to not rely on only one method or tool, but rather to use as much methods as possible, in order to defend against all forms of attacks and threats. The following is a list of basic defence methods and tools, commonly used to protect users and their assets in the cyber realm.

Passwords

Setting up and creating strong passwords is a very simple, yet crucial step in protecting assets in cyberspace. As stated in section 2.3.2, a password is used to prove that the current user is authorized to use or access a system or asset. This set of characters serve as a key that allows any user that has it to gain authorized access to a system and if this key were to fall in the wrong hands, attackers can gain full, authorized access to the system. (Teymourlouei, 2015). In 2017 the United States Department of Commerce's National Institute of Standards and Technology (NIST) updated their set of standards to ensure that passwords and their verifiers are strong and up to standard. These updated standards were published in the NIST Special Publication 800-63B (Grassi et al., 2017). Most of these standards and policies are targeted at password verifiers to ensure that users are assisted when creating a password, without forcing them to adhere to unreasonable password rules and policies, but in these standards three criteria of strong passwords are identified. These criteria are length, complexity and randomness.

- Length - The length of a password is the primary factor in characterizing password strength (Grassi et al., 2017). This is due to the fact that shorter passwords are easier to crack using brute force methods and dictionary attacks and it is thus important to ensure that a user's passwords are at least of a certain length. The minimum password length may vary between different passwords, as the minimum required length depends on the threat model that is being addressed. The commonly accepted minimum length for passwords is 8 characters. Users should be allowed and encouraged to make passwords as long as they want, but it is also important to define a maximum size that a password can be. Passwords that are longer are inherently more complex than shorter passwords, but it leaves more room for users to forget or mistype their passwords. The standard as set by NIST suggests that a maximum passwords length of 64 characters is acceptable.

- Complexity - The complexity of a password refers to the different types of characters, numbers and special characters that is used in the password, also referred to as the composition of a password. Using different character types when creating a password increases its complexity and makes it difficult to crack, but forcing users to follow composition rules can lead them to respond in a very predictable way. It is thus important that users are not forced to comply to composition rules. Users should be allowed and encouraged to use any ASCII or Unicode character, spaces included. Passwords that are forced to have a high complexity create another potential vulnerability, because they are less memorable and can thus be forgotten much easier. When creating a password, it is best to include complexity, without making it predictable or hard to remember.

- Randomness - When creating a password, users often use birthdays, names or locations that are memorable to them to ensure that they remember the password, but by doing this, the user's password is very vulnerable to dictionary attacks. By randomly creating or generating a password that is well distributed, one's password will be safe against both brute force and dictionary attacks.

Anti-malware software and tools

Malware can infect a system from many different sources. Malware can be hidden in an email attachment sent from either a known or unknown source. Malware can infect a system over an unprotected network. Malware can be transferred via an external storage medium. Malware can even infect a system by using trusted software as a method for spreading. It is very likely that a user's computer, device or system will be infected with some form of malware and thus, protecting against this malicious software is one of the most important tasks when protecting one's assets. The solution to this problem is using anti-malware software. Anti-malware software (also called antivirus software) is a specialized kind of software that searches for, detects, prevents, quarantines, and removes malicious computer programs from the system (Teymourlouei, 2015; Kissel, 2013). This protection software will routinely scan the entire system, or certain parts of the system (based on how it is configured) for any malicious code on the system. If malware is detected, the anti-malware software will warn the user of the threat and quarantine the malicious code. Modern anti-malware software can also be configured to scan emails and attachments, downloaded/downloading files and external storage mediums, and then quarantine any malicious code, even before the files are on the target system. Due to the fact that malware is constantly adapting and changing, anti-malware software is also often updated, ensuring that new forms of viruses do not go unnoticed. There

are many variations of paid and free anti-malware software available on the market and using one of these will significantly reduce the probability of malware infection.

Firewalls

A firewall is a device or program that monitors, controls and limits the flow of network traffic to and from the user's system (Kissel, 2013). A firewall can be viewed as a guard that monitors and assesses the traffic that enters and leaves a system in a network. If the firewall detects any suspicious activity or unauthorized connections, that communication is blocked and the user is notified. Using a firewall adds a defensive layer against almost all types of cyber attacks. All network traffic has to pass the firewall and therefore it will be difficult for attackers to get past, without being flagged as an untrusted communication. Most modern operating systems have a built-in firewall that automatically monitors communications, with little or no input from the user. Other firewall hardware and software are also available as free or paid products. Although many users find firewalls to be an inconvenience, it can usually be configured to adopt certain levels of security, based on the user's personal preference (Kumar et al., 2005).

Securing confidential information

As stated in section 2.3.2, many attacks succeed due to some form of human error. Sometimes preventing cyber-attacks is as simple as using common sense (Teymourlouei, 2015). When an attacker has access to the personal information of the user, the attacker can easily use this information to do harm to the user. In simple cases, attackers can use this information to send malware and launch other, small scale attacks, but in more extreme cases, leaking personal information can lead to serious crimes such as identity theft and fraud. By presenting an unsuspecting user's personal information as their own, attackers can gain access to certain real world assets (such as bank accounts) and commit fraud. By doing so, the attacker will not only damage the assets of a user, but they may also damage the user's reputation. This could lead to legal action, financial losses and other serious real world consequences. By simply not sharing personal information with individuals or seemingly suspicious organizations, users can reduce the chance of being affected by these criminal acts.

Connecting safely

A common method of gaining unauthorized access to mobile devices is via public, open Wi-Fi networks. Open Wi-Fi networks are unprotected and thus susceptible to threats. If an attacker were to attempt to gain access to a user's device or its communications via this network, the chance of

success will be rather high and the user will not easily be able to defend against this threat. The best method of defence against unprotected hot-spots is to simply avoid them and to not allow any connections to be made without user consent. Not all public Wi-Fi networks are dangerous and compromised, but by avoiding all of these networks, one's assets will be much safer. If it is necessary to use an unknown or public network, it is essential to avoid transactions or registering for anything that requires any input of personal information (Teymourlouei, 2015).

Browsing safely

In many cases, websites are set up in a way that attempts to protect both the users and the website itself, but unfortunately this is not true for all websites. Users should be wary of the websites that they browse and make sure that the website has a security certificate (most websites will link to this). Although many modern browsers warn users of unsecured websites, it is still valuable to be wary when browsing websites on-line. The following is a list of tips to browse securely as stated by Teymourlouei (2015):

- Disable the use of remembering passwords for sites in all browsers;
- Disable the use of remembering what was entered in a form;
- Make sure browsers are set to clear data when the browser is closed ;
- Block pop-ups for all browsers;
- Set the internet zone security level;
- Do not open unknown e-mail attachments or respond to unknown e-mails;
- Password protect all devices that are connected to the internet; and
- Do not respond to online requests for personal identifiable information.

Downloading safely

Just as it is important to be wary of the websites that one browses, it is also important to be cautious of the software and files that one downloads. Due to the fact that malware such as viruses attach themselves to certain software or files, it is very common that users unintentionally download different types of dangerous malware. This is especially true when downloading freeware from suspicious sites, downloading using Peer-to-Peer (P2P) methods, or downloading software or files illegally. Freeware is software that is free to download and use and usually, downloading freeware from trusted sources do not have any negative effects, but freeware from untrusted, suspicious

sources are very likely to contain malware (Kissel, 2013). Trusted sites are known to scan their files for any malware and thus this freeware can be confirmed as reputable and legitimate. In contrast to this, P2P downloads have no form of regulation or policy to ensure that files are safe and malware-free. P2P downloading is a method that allows users to share files on their devices and thus allow other users to download these files. This means that these users can easily spread malware to other users, possibly damaging their system seriously (Teymourlouei, 2015). Another reason why P2P downloading is cause for alarm, is that it is often a method of downloading files illegally. If one is caught downloading files illegally, serious legal action may be taken. It is thus important to only download from trusted websites and to never, under any circumstances, download any files or software illegally.

Updating software

As discussed in Section 2.3.1, it is common for software to have vulnerabilities and attackers will exploit these vulnerabilities to damage a system and its assets. Fortunately for the user, it is the responsibility of the maintenance section of each software development agency to identify possible vulnerabilities and breaches and then to create a patch or update to secure said vulnerability. Since no software is completely unbreachable, it is very important that these updates are constantly created and made available to the user. The responsibility of the user is to ensure that these updates are installed frequently. This is usually not a problem, as most software have the ability to update automatically or to even force the user to install updates before it is used, but it is essential that users are aware of the update status of their software and that they know how to manually update their software.

Create backups

No method of defence or even combination of methods has a 100% chance of protecting one's assets. Even when every other precaution is taken to secure one's digital assets, there is always a possibility that data will become corrupted, damaged or lost. This can be due to a successful attack, natural threats/disasters, corrupted software or even hardware failures. That is why it is always necessary to have recent backups of all-important data on a system. A backup is a copy of files and software to facilitate recovery, if necessary (Kissel, 2013). By using a backup, a user can minimise the damage caused by these threats and recover the data without much difficulty. Users are encouraged to have multiple backups on multiple mediums. A good backup policy is to always have three, recently updated backups: one physical disk on-site, one physical disk off-site and one digital copy, saved on a secure cloud storage or backup service.

2.5 Cybersecurity awareness

Creating awareness in the realm of cybersecurity refers to any activities intended to focus an individual's attention on a certain cybersecurity issue or issues. The purpose of cybersecurity awareness strategies is to allow individuals to recognise the different cybersecurity threats and concerns and then respond to them in the correct way (Kissel, 2013). It is important to note that cybersecurity awareness is for the end-users of a system and thus addresses the human element of cybersecurity.

Many different strategies, protocols and campaigns exist to improve cybersecurity awareness among users, but despite all efforts, cybersecurity attacks still happen on a daily basis (Kirlappos et al., 2014). Although the increased skill level of the attackers might be a possible reason for the number of attacks that succeed, despite all efforts to stop it, this cannot be the only reason (Bada et al., 2015).

2.5.1 Why cybersecurity awareness fails

In the past, the success of cybersecurity awareness campaigns was determined by the satisfaction level of the users, instead of measuring success by using some form of proof or metric. However, with time, this method of testing the success of awareness campaigns have been replaced with different methods of evaluation and the results of these evaluations suggest that cybersecurity awareness campaigns often fail (Ostrovsky, 2014). The following list, identified by Ostrovsky (2014), contains the six fundamental reasons why cybersecurity awareness activities fail:

- The given solutions or activities are not aligned with the business risk;
- The progress of the user and the value of the activities are not measured;
- The assumptions made about people and their motivations are often incorrect;
- User expectations are set unrealistically high;
- The focus is not placed on the correct skill; and
- Many users perceive awareness as background noise.

Knowing the reasons why these awareness campaigns fail is an important step to creating and implementing strategies that will more effectively spread awareness. It is also important to know how the success of these campaigns are measured, because then it might be possible to create a strategy with near perfect results.

2.5.2 Measuring the effectiveness of awareness campaigns

According to Timmermans and Cleeremans (2015), there are four types of measures when testing the effectiveness of an awareness campaign. These measures can be identified by the combination of two properties: Objective/Subjective; and Direct/Indirect.

- Direct/Indirect - This property indicates whether the information received from the tested individual was gathered directly (via direct contact, report or verbal) or indirectly (via observation or priming).
- Objective/Subjective - This property indicates whether the information received is of objective (not influenced by feelings) or subjective (based on, or influenced by feelings) nature.

Even though the effectiveness of measuring awareness has increased over time, these measures still face many issues that make them unreliable. Because the results of these measures rely on humans and their experiences, all forms of evidence are based on indirect observations or results that could be potentially influenced by people's subjective experience. These problems are called the observer paradox (awareness cannot be turned off) and the contamination problem (all measures can be influenced by conscious and unconscious contents) (Timmermans & Cleeremans, 2015).

As it is nearly impossible to successfully measure awareness, this study will measure the effectiveness of spreading awareness by using expert reviews. In an attempt to increase the effectiveness of spreading awareness by using a serious game, the elements of a successful cybersecurity awareness campaign will be discussed and employed.

2.5.3 Elements of a successful cybersecurity awareness campaign

To form and initiate a successful cybersecurity awareness campaign, there are many elements that have to be considered. In an attempt to outline a broad framework for a successful cybersecurity awareness campaign, a list of some of these important elements are identified from literature.

- Communication - Cybersecurity awareness campaigns directly communicate with the user in an attempt to improve the human element of digital security. Because these campaigns attempt to influence human behaviour, it is important that the user and whoever is driving the cybersecurity awareness campaign should communicate. Good communication in cybersecurity awareness campaigns can not only teach a user a new skill, but it can also assist those managing awareness campaigns to adjust their approach to best fit the users (Bada & Nurse, 2019; Ostrovsky, 2014).

- Avoid pitfalls - In order to effectively spread awareness on the topic of cybersecurity, there are certain pitfalls that must be avoided. The following is a list of avoidance methods as identified by Bada et al. (2015).

    1. Understanding what security awareness is;
    2. Understanding that a compliance awareness program does not always result in the desired behaviours;
    3. Using engaging and appropriate materials for the target group;
    4. Illustrating that awareness is a unique discipline;
    5. Using an assessment for the awareness program; and
    6. Focusing on an array of different topics in the field and using multiple training exercises to create a broad awareness, instead of focusing on only one topic.

- Simplicity - For an awareness campaign to be successful, it is important that the user feels in control of the situation and can follow specific behaviours (Ajzen, 2002). By keeping the rules simple and consistent, the user's perception of control will make it easier to accept the new behaviour (Bada & Nurse, 2019).

The elements listed above are essential to ensure that an awareness campaign succeeds. One of the objectives listed in Section 1.3 is to create a game that successfully promotes digital wellness, therefore these elements are to be implemented in the mobile serious game.

2.6 Summary

In this chapter the environment in which the problem exists, namely cyberspace, was described. The background of cyberspace was provided and defined as a virtual, digital world based on various infrastructures such as computers, networks, data and information, hardware and software, etc. This was followed by an explanation of the differences between information security; information and communication technology security; and cybersecurity and concludes by stating that this study focuses mainly on cybersecurity.

Next, the topic of cyber threats were discussed by first giving a brief overview of important terminology needed to understand the content of the section. This was followed by discussing different types of attacks that a user can encounter while using cyberspace and the different classifications of attackers in cyberspace. Then a short list of basic defences was provided. This list only defines a few important defensive measures as stated in literature,

to ensure safer use of cyberspace and better protection of a user's digital assets. Finally, a brief overview of cybersecurity awareness was given, and focusing on why these awareness campaigns fail and what elements should be used to ensure a successful cybersercurity awareness campaign.

Although the protection of assets is important, it is not the only thing that is in danger when making use of cyberspace. When a user is browsing in the cyber realm there are two important elements that need to be protected: one's assets, protected by cybersecurity and defensive measures as named in Section 2.4 and oneself or one's mental and physical well-being. The well-being of a user is in some cases even more important than any of the user's assets, but cybersecurity does not contain methods or policies to protect the well-being of the user in a digital realm. To be secure and safe in a cyber realm, cybersecurity is not enough. It is also necessary to employ and uphold methods and policies aimed at improving digital wellness. This is discussed further in Chapter 3.

Chapter 3

Digital wellness

In Chapter 2 the setting or environment of the problem addressed in this study (see Chapter 1), was defined. By better understanding what cyberspace is and how to protect one's assets, a solid foundation is created that is used to support the next important step in ultimately solving the problem. This step is defining and describing the content to be used to spread awareness among preschool children. This content is digital wellness.

In Section 3.1 the definition of digital wellness is provided. This is followed by Section 3.2 which lists the elements of digital wellness. Next, in Section 2.5 three attempts at spreading awareness among pre-school children are mentioned, followed by an overview of the book: Digital wellnests by Von Solms and Fischer (2017) in Section 3.4. The book, Digital wellnests, is discussed because it specifically addresses digital wellness for young children and it will be used as the content of the mobile game. Finally, in Section 3.5, the topic of digital wellness awareness for children is briefly discussed.

3.1 Defining Digital wellness

We live in a technological society (Ritchie, 2013). Whether it is used for work or play, technology is used in almost every part of our life. Due to the fact that almost all human lives are intertwined with these digital inventions, it makes sense that both the physical and mental health of modern society can be affected by these technologies.

Digital technologies can affect one's personal experiences in daily life with both positive and negative outcomes (Roquet & Sas, 2019). This ultimately means that these ever-evolving digital technologies have a direct and growing impact on the well-being of users. Just as it is important to maintain a good and healthy lifestyle to ensure a positive well-being in the physical realm, it is important to maintain a good and healthy lifestyle in the digital realm to ensure a positive well-being. This fact leads to the need for a new evaluation, measure or standard to determine the well-being of users in the digital realm

and that standard is called digital wellness (McMahon & Aiken, 2015).

Several definitions for the term digital wellness are found in literature McMahon and Aiken (2015, p.141). McMahon define digital wellness as follows:

> "We define digital wellness as incorporating all aspects of a person's well-being with regard to information technologies, including, but not limited to their propensity to search for health related information online, their online security and privacy cognitions, attitudes and behaviours, their use of and level of attachment to their devices, their impulsiveness in responding to device notifications, their multitasking patterns, cross platform and device behaviours, their screen time duration, their posture and so on. In sum, a person's digital wellness signifies how healthily, both physically and mentally, they relate to digital technology."

McMahon and Aiken continue to explain that their, and by implication digital wellness', approach to technology usage is centred more around usage in moderation, as opposed to the overwhelmingly positive approach of e-health. By reviewing this definition, it becomes clear that digital wellness is a measure of a user's well-being as affected by the use of digital technologies. As stated by McMahon and Aiken, this does not only refer to one's physical state of health, but also to the mental effects that the use of these technologies may have on a person.

Von Solms and Fischer (2017, p.156) also provide a definition of digital wellness. This definition reads as follows:

> "Digital wellness refers to the notion of 'being well in a digital society'. It is characterised by the ability of users to discern between the dangers and opportunities found in the cyberspace, act responsibly, and align their online behaviour with their offline values - to remain cyber safe."

When assessing the definition provided by Von Solms and Fischer, it becomes clear that digital well-being is not only dependent on how a person uses these digital technologies, but it is also affected by the user's ability to identify dangers in the cyber realm and how the user acts on these dangers. This means that digital wellness can be influenced by digital assets, digital threats and digital communications and thus to maintain a good well-being in the cyber realm, it is necessary to uphold cybersecurity protocols, while also maintaining a positive mental and physical health.

Royal et al. (2017, p.105) defined digital wellness as follows:

> "A way of life, while using technology, that promotes optimal health and well-being in which body, mind, and spirit are integrated by the individual to live more fully within the human, natural, and digital communities. Ideally, it is the optimum state of health and well-being that each individual using technology is capable of achieving."

In this definition it becomes clear that digital wellness refers to the digital lifestyle of a user and finding a balance between the user's body, mind and soul while using digital technologies. This means that maintaining a positive digital wellness does not mean to follow a set of rules and instructions, but to rather find the balance in which the user is happy, comfortable, healthy and safe in a digital realm.

From these three definitions it can be concluded that digital wellness is a measure of one's complete well-being in cyberspace. This means that digital wellness refers to how balanced one's mental and physical state is when using different digital technologies and how safe users and their assets are in the digital realm.

3.2 Elements of digital wellness

According to McMahon and Aiken (2015), the elements of digital wellness can be divided into three groups: physiological, behavioural and psychological. To better understand what it means to maintain a digitally healthy lifestyle, these three categories are discussed.

3.2.1 Physiological Elements

The physiological category of digital wellness refers to the physical well-being of a user. This means that the physiological elements of digital wellness are concerned with the health and safety of users. There are two main elements in the physiological category, namely screen time and technostress (McMahon & Aiken, 2015).

Screen time

Screen time refers to the amount of time that a user spends using digital technologies and thus in front of screens (Lubans et al., 2013; Sigman, 2012). This screen time is seen as a form of sedentary behaviour. Sedentary behaviour is a distinct class of behaviour characterized by little physical movement and low energy expenditure. Common examples of this behaviour

includes sitting, watching television and playing video games (Tremblay et al., 2011). Excessive screen time and sedentary behaviour is known to be detrimental to one's health. In a systematic review of sedentary behaviour and health indicators in school-aged children and youth, Tremblay et al. (2011) found that increased sedentary time (increased screen time) can be associated with negative outcomes on the following criteria:

- Body composition (overweight/obesity measured by body mass index, waist circumference, skinfolds, bio-impedance analysis, dual-energy X-ray absorptiometry)
- Fitness (physical fitness, physical conditioning, musculoskeletal fitness, cardiovascular fitness);
- Metabolic syndrome and cardiovascular disease risk factors (unfavourable lipid levels, blood pressure, markers for insulin resistance or type 2 diabetes);
- Self-esteem (self-concept, self-esteem, self-efficacy);
- Behavioural conduct/pro-social behaviour (child behaviour disorders, child development disorder, pro-social behaviour, behavioural conduct, aggression); and
- Academic achievement (school performance, grade-point average).

These findings are further supported by a similar systematic review focusing on the health indicators associated with screen-based sedentary behaviour among adolescent girls, done by Costigan et al. (2013). In this review the following results were found:

- Strong evidence for a positive association between screen-based sedentary behaviour and weight status
- A positive association between screen-time and sleep problems, musculoskeletal pain and depression
- Negative associations between screen time and physical activity/fitness, screen time and psychological well-being, and screen time and social support
- The relationship between screen-based sedentary behaviour and diet quality was inconclusive

These findings were not intended to advocate against the use of digital technologies, but rather to promote limiting the amount of screen time that a user is exposed to daily. It is important to find a balance between one's screen time, physical activity and interpersonal relationships to ensure a positive digital well-being.

Technostress

The term technostress was first introduced in 1984 by clinical psychologist, Brod (1984, p.16). Brod defined technostress as "a modern disease of adaptation caused by an inability to cope with the new computerworld technologies in a healthy manner". Simply put, technostress is a kind of stress or psychosomatic illness caused by the repetitive use of information and communication technologies (McMahon & Aiken, 2015; Yan et al., 2013). The following is a list of the five technostress triggers as identified in literature by Ragu-Nathan et al. (2008), Wang et al. (2008), and Tarafdar et al. (2007):

- Constant connectivity - Because users are always connected and can always be reached, this constant connectivity can potentially extend the workday. This constant exposure leads individuals to feel that they are never free of these technologies and that their time and space have been invaded. This can also be referred to as "Techno-invasion".
- Information overload - Users have access to multiple devices simultaneously and this can often lead to users being exposed to more data and a flood of information that is more than they can process at a time. This can often force users to feel that they have to do more work in a shorter amount of time and this is often referred to as "Techno-overload".
- New technologies - Technology is constantly evolving. Users often feel pressured to use state of the art technologies, but as these technologies evolve, they may become more complex and difficult to learn to use. This can also be applicable to applications, functions and jargon that seems intimidating to users, therefore causing stress. This is also known as "Techno-complexity".
- Job insecurity - Insecurity in technostress is associated with any situation in which users feel insecure about losing their job due to technology. This is also referred to as "Techno-insecurity".
- Lack of expertise - The constant change in technologies creates an environment in which users have to adapt to new technologies, but because new technologies have a short life cycle, users can rarely become adept at using new technologies before they become obsolete. This means that users often stress about the inability to master new technologies. This can be called "Techno-uncertainty".

The symptoms of technostress are very similar to regular stress, with the addition of symptoms unique to technostress caused by the technostress triggers as named above. Typical symptoms of stress include: headaches, irritability, gastrointestinal problems, insomnia, asthma, mental problems (depression, anxiety, addiction, mood changes, burnout, behavioural changes,

job dissatisfaction), musculoskeletal tension (carpal tunnel, back and lower back pain, shoulder pain) and in rare cases, diabetes, cancer, heart attacks, and multiple sclerosis (Berrios Rolon, 2014; Gendreau, 2007). The symptoms caused by the technostress triggers named above include: information overload, less down time or rest time, multitasking madness, memory issues, blurring of boundaries between family and work, computer anxiety, anger, work overload, addiction, and techno-insecurity (Berrios Rolon, 2014; Wang et al., 2008; Tarafdar et al., 2007).

There are two methods or strategies of limiting the effects of technostress on digital wellness. The first strategy is problem-focused, meaning that the user should attempt to improve the environment and stop the problem at the cause (Wang et al., 2008). This can be done by seeking information on what to do, holding back from premature actions or confronting the person that causes or contributes to the technostress. The second approach is emotion focused. This approach focuses on making the user feel better, rather than solving the problem (Wang et al., 2008). This can be done by simply avoiding thinking of the problem or distancing oneself from it, but this method is not recommended, as it could lead to more problems and contribute to technostress later on.

3.2.2 Behavioural Elements

The behavioural elements of digital wellness are concerned with the behaviour and actions of users. This means that the behavioural aspects of digital wellness focus on how the use of digital technologies affect one's habits, actions and performance both in the digital realm and in the real world. Two of the main elements that affect one's overall digital wellness are the problematic use of the internet and media multitasking (McMahon & Aiken, 2015).

Problematic use of technology

The problematic use of internet can be defined as the use of the internet which creates psychological, social, school, and/or work difficulties in the life of the user (Beard & Wolf, 2001). The problematic use of technology therefore refers to any form of misuse of digital technologies. The problematic use of technologies may vary based on the situation of the user. Although spending time browsing online might be acceptable while one is at home, using company resources to browse online while one is at work might be less so. While the problematic use of technology may refer to misuses such as internet procrastination (Thatcher et al., 2008) and visiting illegal or inappropriate websites, literature mostly associate the problematic use of technology and the internet with addictive behaviour (McMahon &

Aiken, 2015; Merlo et al., 2013; Thatcher et al., 2008; Davis et al., 2002). Although the problematic use of technology and the internet appears to be very similar to an addiction, professionals in the field are still divided on whether the problematic use of technology and the internet can be defined as an addiction or whether it is rather a behavioural manifestation of other things that may be problematic in their lives (Thatcher et al., 2008; Caplan, 2002). Some of the symptoms of the problematic use of technology and the internet include: needing to spend increasing amounts of time online, loss of control over the amount of time spent online, unsuccessful attempts to reduce the amount of time spent online, preoccupation with online activities, withdrawal symptoms, changes in mood or anxiety levels, denial or deception regarding the amount of time spent online and negative social, physical, financial or emotional consequences as a result of spending time online (Thatcher et al., 2008; Caplan, 2002; Davis et al., 2002; Beard & Wolf, 2001).

The following is a list of suggestions for avoiding the problematic use of technology (Király et al., 2020):

- Self-monitoring - Being conscious of one's usage and regulating it is an essential step to avoiding the problematic use of the internet (Király et al., 2020). If needed, one can reduce one's access and self-regulate when to have access and for what purpose to have access.

- Using digital well-being applications - Such apps spread awareness and can be handy for motivating users to avoid the problematic use of technology. By using these digital well-being apps, access can be limited and scheduled (Király et al., 2020).

- Use analogue technology - The use of analogue technologies can reduce the temptation for using digital technologies (Király et al., 2020). For example, using a clock instead of the mobile device to check the time, might avoid unnecessary use of a mobile device.

- Keeping in touch with friends and relatives - Keeping in touch with one's loved ones is important to reduce the feeling of loneliness (Király et al., 2020). This is also a pastime that could distract from excessive internet use.

- Seeking help - If the problem gets out of hand, it is important to seek help from a professional. There are multiple helplines and mental health professionals that are able to help someone to overcome the problem (Király et al., 2020).

Media multitasking

In a world that is saturated with streams of data and information, how to structure media usage can have real world implications. Media multitasking can be defined as the consumption of more than one item or stream of content at the same time (Lin, 2009; Ophir et al., 2009) and it is a trend that is becoming increasingly more popular. Although many believe multitasking and specifically media multitasking to be harmless, multiple studies have found evidence that proves otherwise. In a study summarising the findings of the effects of media multitasking on users, Melina R. Uncapher and Anthony D. Wagner (Uncapher & Wagner, 2018) identified the following effects:

- Working memory: Media multitasking users performed significantly worse than non-media multitasking users.
- Interference management: The findings of media multitasking's effect on interference management showed a negative relationship, meaning that media multitaskers performed worse that non-media multitaskers.
- Attention: Studies found that media multitasking has a negative effect on attention span. These studies found that media multitasking also has an effect on the speed at which tasks are completed.
- Managing task goals: Testing the management of task goals was divided into two factors, task switching and dual tasking. The results of these tests showed that no clear connection can be made between media multitasking and the management of tasks.
- Inhibitory control: Inhibitory control is thought to be a distinct form of cognitive control such as attention selection and sustained attention (Schutten et al., 2017). Studies found that media multitasking can affect inhibitory control or impulsiveness and that heavier media multitaskers were prone to show more signs of impulsiveness.
- Relational reasoning: Heavy media multitaskers performed significantly worse than lighter user counterparts when it comes to relational reasoning.
- Long term memory: While available data are quite limited, heavier media multitasking in adults was associated with poorer explicit and implicit long-term memory, but no effects were observed in adolescents.

The simplest method of avoiding the negative effects that media multitasking might have on a person, is to actively steer clear of using multiple devices or looking at multiple screens in short succession. By focusing on a single task on only one device at a time, the chances of being affected by these negative effects are limited.

3.2.3 Psychological Elements

The final group of elements of digital wellness concerns the user's mental or psychological well-being. In addition to the mental well-being of the user, the psychological elements of digital wellness also focus on the emotional state of the user. The two main elements of this group are on-line security and on-line disinhibition (McMahon & Aiken, 2015).

Online security

The online security and privacy element of digital wellness refers to protecting the user's assets in cyberspace (McMahon & Aiken, 2015). This element of digital wellness therefore directly deals with cybersecurity.

Online attacks and crimes can leave victims feeling helpless and these attacks can have real psychological impacts on users (Bada & Nurse, 2019; Modic & Anderson, 2015; Gandhi et al., 2011). The following is a list of the possible psychological and emotional effects that cyber attacks can have on a user (Bada & Nurse, 2019; Nurse & Nurse, 2019; Kirwan & Power, 2012):

- The victims of online attacks can suffer emotional trauma which can lead to depression;
- In some cases there are evidence of limited symptoms of acute stress disorder in victims of online crime;
- The emotional impact of attacks can include the user becoming distressed and feeling violated, betrayed, vulnerable, angry, powerless, outraged and anxious;
- Victims of cyber attacks might also develop a preference for security over liberty and these attacks might cause them to have little interest in adopting new technologies due to loss of confidence and a feeling of helplessness;
- Victims of cyber attacks and fraud may feel that they are at least partially to blame for the incident and that it may even lead to further incidents.

Although these cyber attacks pose a significant challenge to modern society (Nurse & Nurse, 2019), there are still steps that can be taken by users to avoid the psychological and emotional damages. Such actions are defined in Section 2.4 and include, but is not limited to, setting up strong passwords, using anti-malware tools and firewalls, securing confidential information, not connecting to unknown networks, browsing safely, downloading only from trusted sites, updating software and creating backups frequently.

Online disinhibition

According to Suler (2005), the online disinhibition effect is a phenomenon where people behave differently online than they do in the real world (Rose, 2014; Suler, 2005). These uninhibited actions can be divided into two categories, benign disinhibition and toxic disinhibition.

- Benign disinhibition - This refers to the unusual acts of kindness and generosity that users may display online. Such users will sometimes reveal suppressed emotions, fears and wishes online and may go out of their way to help others.
- Toxic disinhibition - In contrast to users that display benign disinhibition, users that display toxic disinhibition are prone to be rude, critical, angry, hateful and threatening. Such users might explore online places of perversion, crime and violence that they would never do in real life.

It is important to distinguish between benign and toxic disinhibition, as the distinction between these two forms of disinhibition may become ambiguous in some cases (Suler, 2005). Although benign inhibition appears to be much less harmful to oneself and others, cases may arise where certain users self-disclose inappropriately, making themselves feel exposed or ashamed and making others feel uncomfortable (Rose, 2014).

The cause of online disinhibition is still up for debate, but Suler (2005) identified the following six possible contributing factors: anonymity, invisibility, asynchronicity, solipsistic introjection (a sense that the textual conversation is with oneself rather than others), dissociative imagination (a sense that online interactions take place in an unreal online world), and minimization of status authority in the absence of the visual cues that typically distinguish authority.

One of the most common forms of online disinhibition is cyberbullying. Cyberbullying can be defined as an aggressive, intentional act carried out by an individual or by a group of by a people, using electronic forms of contact, repeatedly and over time against a victim who cannot easily defend him or herself (Smith et al., 2006).

The following are possible negative effects that cyberbullying can have on users (especially children and adolescents) (Hamm et al., 2015; Hinduja & Patchin, 2010; Hoff & Mitchell, 2009):

- Increased levels of anger, powerlessness, sadness, and fear;
- Loss of confidence, disassociation from friends and school, and a general sense of uneasiness;
- Reactive behaviour that could lead to physical harm, which is likely to escalate the situation further;
- Increased levels of anxiety and depression; and
- Self-harm or suicidal thoughts.

To avoid acting in an uninhibited way, it is important to self-monitor one's actions and discussions online (Király et al., 2020). Avoiding discussions and situations where a person might show signs of disinhibition, will reduce the opportunity and impulse to act in a way that the person normally would not behave. In situations where other users make a user uncomfortable, unsafe or unhappy, there are two recommended actions. The first is to avoid online contact with those users by blocking contact with them or avoiding websites or situations where they might make contact. The second option is to report these users to the corresponding authorities. These authorities may be the administrators of an application or website in an online capacity or the parents, guardians or teachers in the case of younger users (Von Solms & Fischer, 2017).

3.3 Digital wellness for preschool children

As stated in Chapter 2, cyberspace can be dangerous and therefore it is necessary that children be made aware of the dangers from a young age. This section identifies three attempts to increase awareness of digital wellness among preschool children.

Table 3.1: Digital wellness content for children

Author	**Title**	**Content**
Fischer and Von Solms (2016)	Digital wellnests: Let us play in safe nests	A book consisting of concepts, 14 poems and 14 messages set in the animal kingdom. The 9 identified digital wellness and cybersecurity morals are listed in Section 3.4.
Google (2019)	Interland: Be Inter-net awesome	A game and resources (that includes a curriculum for educators) which explores four different worlds teaching the user four different lessons about cybersafety: • Communicate Responsibly; • Know the Signs of a Potential Scam; • Create a Strong Password; and • Set an Example and take action against inappropriate behaviour.
Halpert (2014)	Savvy Cyber Kids	A book series consisting of three books identifying three elements of digital wellness and cybersecurity specifically for children: • Online anonymity (not sharing information online); • Online bullying (tell people you trust when someone is being bullied); and • Limit screen time.

When comparing the identified related work, the book, "Digital wellnests: Let us play in safe nests", aligns best with the goal of this study. This book identifies most digital wellness topics and is specifically aimed at preschool children. Both "Interland: Be Inter-net awesome" and "Savvy Cyber Kids" identify core digital wellness issues, but the number of issues is limited

compared to that of "Digital wellnests: Let us play in safe nests".

3.4 Digital wellnests

"Digital wellnests: Let us play in safe nests" [1] is an electronically available book created by Fischer and Von Solms (2016) with the goal to promote a cybersecurity culture amongst children. The book uses simple explanations and depict animals as the main characters. These animals are familiar to African children. In 2015, while this book was still in its developmental stage, it was presented at a workshop in Nairobi, Kenya. At this workshop the book received much praise for its clear approach and identifiable characters. Even the academia and civil society members present at the workshop proclaimed that it is successfully achieving the aims of giving the topic a local character (Von Solms & Fischer, 2017).

This book is discussed in this chapter, as it aligns with the goal of this study and it highlights a lot of critical elements of digital wellness aimed specifically at preschool children. The content of this book is also used in the mobile application developed in this study and therefore it is discussed and linked to the elements of digital wellness (as described in Section 3.2) in the rest of this section .

The book consists of four main sections. The first is a foreword and introduction that are primarily aimed at the parent, guardian or teacher. The second section of the book contains a few technology-related concepts that are both explained and illustrated by a drawn representation. The main content of the book is provided in the third section in the form of poems. Each of these poems features animals interacting with technology and ends with a moral lesson. The fourth and final section of the book consists of 14 short messages that serve as important cybersecurity-related lessons and are easy to remember (Von Solms & Fischer, 2017).

3.4.1 Concepts

The book describes the following 9 technology-related concepts:

1. Camera - Device that can take pictures;
2. Cell phone - Mobile device that is used to contact other people, by either phoning, texting or e-mailing;
3. Kindle - Mobile device which can be used to read electronic books (e-books);
4. E-mail - Electronic mail that is sent and received between people;

[1] https://www.up.ac.za/african-centre-of-excellence-for-information-ethics/article/2109737/digital-wellness-toolkit

5. Computer - Electronic device that is used to store, compile and distribute data;
6. Mouse - Electronic device used with computer to navigate the screen and content of the computer;
7. Signal Tower - Tower that sends and receives signals;
8. Social Media - Collective used to refer to online social networking sites and tools that enable the creation and sharing of information in an online social environment; and
9. Tablet - Mobile device with same functions as a computer, cell phone and e-book reader and has a touch-screen. Is bigger than a cell phone, but smaller than a computer and has more uses than an e-book reader.

3.4.2 Poems

The poems in the book serve as the main content and it is used to teach the reader a moral lesson regarding cybersecurity and digital wellness. The following is a list that provides the names of the 14 poems, their cybersecurity-related theme, their moral lesson and what element or elements of digital wellness they address.

The safety of nests

This first story follows a little bird that likes to use the internet. Although the little bird uses the internet frequently, he always listens to the guidance of his parents and teachers when using the internet and he honestly shares his experiences with them. The moral of the story therefore is to be honest when using the internet and this story addresses the problematic use of technology and the internet element of digital wellness.

Safety Snail's e-mails

In this story a snail receives an email from a stranger. Instead of opening and reading the e-mail, she decided to delete the message. The moral lesson of the story is to not open any suspicious e-mails (and other messages) from unknown sources. The moral of the story addresses the online security and privacy element of digital wellness as these suspicious e-mails may be a form of cyber attack.

Lucky the Fish

Lucky the fish received a text message that notified him that he won a prize. Although Lucky knew he did not enter any competition to win a prize, he wanted to click on the link provided, but his friend advised him to delete the message instead. The moral of this story is to not access or respond to any suspicious messages or links. This story addresses the problem of phising and/or malware attacks and therefore the digital wellness element of this story is online security and privacy.

Rabbit with the tablet

A rabbit and his monkey friends use his tablet to visit unsafe websites and these websites scare them. The rabbit then realises that there are many dangers on the internet and that they have to be careful online. The moral of the story is to be careful and safe while browsing online. This message can be associated with two digital wellness elements: online security and privacy, as dangerous websites might cause security threats; and the problematic use of technology and the internet, because the internet was used in an unsafe and irresponsible way.

Elephant and his shoe

In this story an elephant does not know how to tie his shoelaces. His friend, Rabbit, then uses the internet to help the elephant learn how to tie his shoelaces, but then Rabbit also advised the elephant that it is important to also play outside. The moral lesson of this story is that even though the internet is very useful, it is important to also play outside and spend time away from technological devices. The element of digital wellness that is emphasized the most in this story is screen time, as it motivates children to maintain a balance between the time that they spend with technology and time that they play outside with friends. The moral of the story can also be connected to the problematic use of technology and the internet element of digital wellness, as it clearly advocates the responsible use of technology and the internet.

Sheepish Shelly

A sheep named Shelly accepted a Facebook friend request from a stranger. Because Shelly posted a lot of personal information on Facebook, the stranger, who turned out to be a wolf with a fake profile, stalked and followed her. The moral of the story is to only accept friend requests from people that you know personally and to not share personal information online. The

digital wellness element that is addressed in this story is online privacy, as the story shows that not protecting one's personal information in an online environment can have serious, real world consequences.

Wolf, Hyena and Fox

Three friends, Wolf, Hyena and Fox discuss how to create strong passwords. Wolf recommends that they share each other's passwords and Hyena agrees, until Fox warns them to never share their passwords with others. The moral of the story is to create strong passwords and to keep these passwords a secret from others. Because the focus of the story is on creating strong passwords and keeping them secret, the digital wellness element can be identified as online security and privacy. Good password practices is a big part of cybersecurity and it is essential to improve one's online security.

Healthy Bear

In this story a bear wanted to play games on a laptop and received a warning from the anti-malware software to update it. The bear however chose to ignore the message and the laptop was then infected with malware. The bear's father then helped him remove the software and told him of the importance of updating anti-malware programs. The moral of the story is to keep anti-malware software up to date on all devices to protect it against viruses and other infections. The digital wellness element that is addressed in this story is online security and privacy. As stated in Section 2.3.2, malware is a kind of cyber attack that can damage a system and installing and updating anti-malware tools and software is an important step in protecting systems against these attacks.

Happy Hippo

A hippo received a mean text message from an unknown source and this message made him sad. The hippo did not want to report this, as he said that it is not physical bullying, but his friend the rhino told him that cyberbullying is real and then convinced hippo to report the incident to their teacher. The moral of the story is that if one is being bullied, whether it is online or physical, one should report the incident to a trusted person. The moral of the story directly coincides with the online disinhibition element of digital wellness and more specifically, toxic disinhibition.

Buffy the Bully

The story of Buffy the Bully follows a buffalo that feels sad and alone and acts out by sending cruel messages to his classmates online. After the class reports Buffy to the teacher, the teacher confronts the bully and tells him that he must speak about what is causing him to send the mean messages and the teacher tells him that bullying is not the solution to his problems. The moral of the story is that if one sees that someone is being a bully, it must be reported to a trusted adult. The moral of this story is related to the online disinhibition element of digital wellness as cyberbullying is a form of toxic disinhibition.

Identity Cricket

In this story a cricket was sad because he had no friends and he decided to share his personal information online in an attempt to make friends. His plan then backfired as dangerous animals used the information to locate the cricket. The moral of this story is that one should not make personal information available for others to see online. The actions of the cricket were a serious security breach and therefore the moral of the story addresses online security and privacy.

Cyber Cat

A cat that became skilled at using computers and writing code used his skills to steal money and gain illegal access to websites. The cat then got caught for his crimes and went to jail. The moral of the story is that hacking is an illegal activity and that one can be punished for online illegal activities. The two main elements of digital wellness that are being addressed are online security and privacy (because hacking and other illegal online activities are compromising cybersecurity). It illustrates the problematic use of technology and the internet.

Cannot see Chameleon

One day, King Lion held a competition to see which animal is the healthiest in the kingdom. The animals debate over the strongest and fastest animal, but the owl then points out that the healthiest animal is the chameleon, as the chameleon stays hidden from danger. This story is used as a metaphor for staying safe while using the internet by keeping your personal information hidden. The digital wellness element in this story is online security and privacy.

Zebra and his stripes

In this story, the zebra is used to refer to the zebra lines on roads. The zebra reminds the animals that just as it is important to look both ways before crossing a street, it is also important to think before posting something online. This story reminds children to think before they act on the internet by comparing the situation to the zebra stripes on a road. The moral of the story is online security and privacy.

3.4.3 Short messages from the animals

The final section of the book contains 14 short messages that convey cybersecurity-related lessons in a way that is fun and easy to memorize. Because the messages roughly match the lessons of the poem, these messages will not be listed in this section, but the following is an example of one of the messages given in the book (Fischer & Von Solms, 2016):

> "Remember the golden rule, Online, in a game or outside your school. Don't talk to a stranger. This will keep you safe from danger"

3.4.4 Digital wellness for children

By analysing the content of the book, we can identify the most important digital wellness elements for children as: screen time; the problematic use of technology and the internet; online security and privacy; and online disinhibition. The general morals of the stories and messages can be summarized as follows:

- Do not share personal information online (Sheepish Shelly, Identity Cricket, Cannot see Chameleon, Zebra and his stripes, message 2, message 7 and message 14);
- Delete messages and friend requests from unknown people and suspicious sources (Safety Snail's e-mails, Lucky the Fish, Sheepish Shelly, message 1, message 5 and message 6);
- Report cyberbullying to trusted adults (Happy Hippo, Buffy the Bully and message 3);
- Be honest when going online and do not visit dangerous or suspicious websites (The safety of nests, Rabbit with the tablet, message 8 and message 9)
- Balance using technology (screens) and playing outside (Elephant and his shoe and message 4);

- Always set up strong passwords and keep them a secret from others (Wolf, Hyena and Fox and message 10);
- Remember to use and update anti-malware tools and software (Healthy Bear and message 13);
- Do not engage in illegal activities when using technology or the internet (Cyber cat and message 12); and
- Do not physically meet strangers that you met online without adult supervision and consent (message 11).

3.5 Digital wellness awareness for children

To better understand how to spread awareness of cybersecurity among preschool children, the focus of this section is to identify how preschoolers learn and develop important skills. The early experiences that children have, play a big role in their overall development and exposing them to the concepts of digital wellness can have significant benefits (McCall et al., 2019).

Children, especially preschool children, are able to learn in five different ways (Raisingchildren.net.au, n.d. Matthews et al., 2007):

- Observation - Visual learning via observation and imitation;
- Listening - Auditory learning;
- Exploring - Investigative learning;
- Experimenting - Physical learning via trial and error; and
- Asking questions - Inquisitive learning.

Although this shows that children are capable of learning in different ways, it is important to note that not all children learn in the same way. Some children might respond better to teaching methods that involve observing and listening, while others might receive more stimulation from practical experimentation and asking questions. Fortunately, preschool children are still at the age of learning through play (Yogman et al., 2018). Play is a fun way for children to learn, regardless of their preferred method of learning. Play allows children the opportunity to observe, listen, explore, experiment and ask questions to solve problems, and leaving them the freedom to decide.

By using play as a tool for learning, the method of teaching is not limited to only one or two of the different ways of learning, but can instead be set up to include all of these methods. By creating a game specifically aimed at children, it is possible to stimulate all forms of learning using only one learning medium. The observation and listening methods of learning can be achieved by presenting information using both audio and visual

methods. The addition of audio and visual feedback can also contribute to the player's overall learning experience (Callaghan & Reich, 2018). By using different tasks and interactions, it is possible to include both the exploring and experimenting methods of learning and by adding thought provoking questions, the inquisitive learning method will also be included.

Another important factor that should not be overlooked when discussing the awareness of preschool children, is the involvement of the child's parent, teacher or guardian. When the parent, teacher or guardian of a child knows how the child learns best, they can guide the child to optimize learning and thus spread awareness effectively. By showing interest in what the child is doing, playing games with them, reading to them and spending time with them, the child's motivation and productivity will noticeably improve (Cheung & Pomerantz, 2015). This is especially important for inquisitive learning as children who learn by asking questions should feel comfortable to ask these questions of people whom they trust.

3.6 Summary

In this chapter the content that will be used to create a mobile serious game to promote digital wellness among pre-school children was discussed. The chapter started by defining digital wellness. This was then followed by listing the three categories and six elements of digital wellness. Each of these elements were defined, their negative effects were explained and a simple method of preventing these negative effects were given. Next, the book "Digital wellnests: Let us play in safe nests" was discussed and analysed. The content of this book was discussed by summarising the stories and their moral lessons and the element of digital wellness that it relates to was given. In the next section, the most important elements of digital wellness for children were identified and the nine digital wellness lessons that relate to children were summarised. Finally, digital wellness awareness for children was discussed by highlighting how children learn. The section ended with the conclusion that children learn through play and thus a game will be used to spread awareness among children.

Having discussed the content of information that should be conveyed to children, the focus of the study changes to the method that will be used to deliver the content to the children, i.e. games. More specifically, the following chapter will discuss serious games and the use of games as a method of learning.

Chapter 4

Serious games

In this chapter the subject of serious games is discussed. The goal of this chapter is to define the concept of a serious game and to explore how a serious game can be created to educate users.

In Section 4.1 the topic of games and play is discussed. Although the concept of play may seem obvious to many, creating a clear and universal definition of play is an important part of understanding games, and by extension, serious games. Section 4.2 is used to present the classification of games based on three criteria and it is followed by a discussion of optimal game development in Section 4.3. In Section 4.4, different serious games for children are discussed, followed by a list of critical elements for applications to pre-school children.

4.1 Defining games

Before a formal definition and classification of games will be given, the topic of play will be discussed. Defining play might not seem like a challenging feat, but many experts in different fields of science struggle with clearly defining the concept of play (Burghardt, 2011).

4.1.1 Play

When studying literature to define the concept of play, one realises that playing is not unique to humans, but it is also commonly observed in animals (Pellis & Pellis, 2013; Burghardt, 2005; Huizinga, 1938). This means that a definition must be created that does not only explain playing in children and adults, but also in all species of animals that is capable of play. Another challenge in conceptualizing play, is that most definitions have borderlines, gray areas and mislabelling. In the area of play for both children and animals, it is not uncommon to confuse play with certain behavioural actions, such as fighting, bullying, courtship and hunting (Pellis & Pellis,

2013; Burghardt, 2005). Play is usually seen as frivolous and foolish, but the players of a game are often focused and goal oriented. This means that play is not always a relaxed activity with focus on enjoyment, but it can also be structured, planned and almost compulsive (Huizinga, 1938).

Garvey and Lloyd (1990) defined play as a range of voluntary and intrinsically motivated movements or activities done for recreational and enjoyment purposes.

Another attempt to define play was made by Huizinga (1938, p.13) in his book titled *"Homo Ludens"* (man playing). Huizenga's definition of play is often referred to as the magic circle notion of play. This definition is stated in his book as follows:

> "Summing up the formal characteristic of play, we might call it a free activity standing quite consciously outside 'ordinary' life as being 'not serious', but at the same time absorbing the player intensely and utterly. It is an activity connected with no material interest, and no profit can be gained by it. It proceeds within its own proper boundaries of time and space according to fixed rules and in an orderly manner. It promotes the formation of social groupings that tend to surround themselves with secrecy and to stress the difference from the common world by disguise or other means." (Huizinga, 1938)

In layman's terms, the definition states that play is removed from normal, everyday actions and not serious in nature. It also describes play as a free activity that can immerse the player into an activity with its own boundaries and rules that is removed from reality to a certain extent.

Eberle (2014) does an in-depth philosophical analysis of the term play and defines the six elements of play as anticipation, surprise, pleasure, understanding, strength and poise. According to Eberle (2014), play begins in anticipation, when players look forward to the moment that play's arrival is announced. Anticipation then give way to surprise, that can act as a reward to players. Eberle's third element, pleasure, is seen as the most important element, as it is not only a defining trait of play, but it also acts as an incentive to keep playing (Eberle, 2014). Pleasure is also fleeting and only momentary, making it a perfect driving element for play. The fourth element, understanding, serves as emotional and intellectual bonuses by increasing the player's empathy and insight necessary for playing with other individuals (Eberle, 2014). According to Eberle (2014), mutuality and sensitivity are required credentials for play with others. The fifth element, strength, refers to strength of body and strength of mind. This is an outcome of the understanding element. Playing trains the player's physical skills, sharpens their mental abilities and deepens their insights into our ability to be social. The sixth element, poise, is the product of adding understanding to strength. Poise can be seen as a reward for players

who experience an increased amount of dignity, grace, composure, ease, wit, fulfilment and spontaneity. Using these six elements, Eberle proposes the following definition for play:

> "Play is an ancient, voluntary, 'emergent' process driven by pleasure that yet strengthens our muscles, instructs our social skills, tempers and deepens our positive emotions, and enables a state of balance that leaves us poised to play some more."

Similarly to Eberle, Burghardt defined five criteria of identifying play in the Oxford Handbook of the Development of Play (Burghardt, 2011, p.10). These five criteria are defined as follows:

> "Play is incompletely functional in the context in which it appears; spontaneous, pleasurable, rewarding or voluntary; differs from other more serious behaviours in form or timing; is repeated, but not in abnormal and unvarying stereotypic form; and initiated in the absence of acute or chronic stress."

The existence of so many definitions of play, created by different experts from their respective fields, is proof that the phenomenon of play is difficult to fully understand and define (Piaget, 2013). However, for the purpose of this study, the following simple definition for play is proposed: "Engaging in an activity guided by rules and constraints, for the primary goal of enjoyment and recreation".

This definition is proposed as it excludes all non-human participants while still including digital forms of play. Although the primary goal of play is enjoyment and recreation, this definition does not limit the goal to only these two elements.

4.1.2 Serious games, entertainment games and gamification

Games can be defined as a set of actions (play) that are restricted by rules and constraints with a certain objective or goal (Stenros, 2016). Computer games have had a transformational impact on how people play and spend their leisure time over the last half century and the interest in these games is still growing (Connolly et al., 2012). The popularity and use of games have grown so much that the primary goal of some games is no longer restricted to the original purpose of pure entertainment. To create a better understanding of some of the different types of games that extend past only being entertaining, the differences between entertainment games, serious games and gamification will now be discussed.

Entertainment games

As the name suggests, entertainment games are games that exist for the purpose of entertaining the user (player). In other words, entertainment games can be described as any game that is designed to give pleasure to the player (Nakatsu et al., 2015; Asgari & Kaufman, 2009). Although such games are not designed for the purpose of learning or training, players in some cases learn new information or discover new skills while playing. This is referred to as incidental learning (Asgari & Kaufman, 2009).

Serious games

Many different approaches to define serious games exist in the literature, but most of these approaches propose a simple definition: A serious game is a genre of video game that has the primary goal of combining the aspects of fun and play with a serious or utilitarian aspect (Dörner et al., 2016; Alvarez & Djaouti, 2011; Dibbell, 2011; Ritterfeld et al., 2009). In simpler words, serious games are video games that do not only aim to be fun and entertaining, but also have a serious or utilitarian motive, such as teaching the user something or spreading awareness on a certain topic. In contrast to entertainment games, learning new information and skills while playing serious games is the intended outcome. It is important to note that in this context, video games refer to all games that are played using a digital medium or on a digital platform.

Gamification

Gamification can be defined as the use of game design elements in a non-game context (Dörner et al., 2016; Brigham, 2015; Deterding et al., 2011). In other words, gamification is a method of adding game elements (such as scoring systems, challenges, rewards and badges) to a service that is otherwise not recognised as a game, with the goal to improve the user's motivation, experience and overall outcome (Matallaoui et al., 2017). The core difference that separates gamification from both entertainment games and serious games is the fact that gamification only employs gaming elements to improve user enjoyment, whereas entertainment games and serious games are complete games. Gamification still allows an application or service to be used to fulfil an operative task (similar to serious games), but the entertainment aspect of gamification is a secondary objective (Matallaoui et al., 2017).

Figure 4.1 is a visual representation of the core differences in the primary goals of entertainment games, serious games and gamification. The primary goal of entertainment games is to entertain the user, whereas the primary goal of gamification is to reach a more serious goal. Although gamification is also used to increase the entertainment of the user, it is not the primary

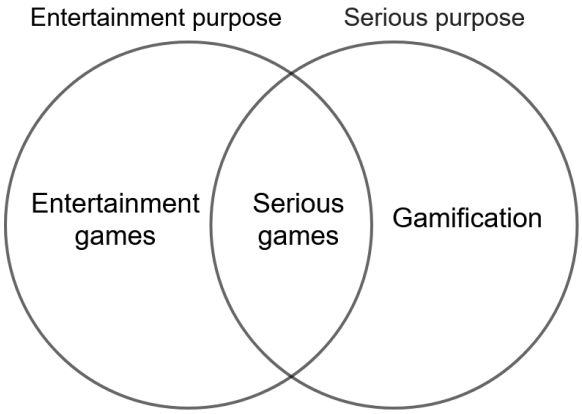

Figure 4.1: The classification of entertainment games, serious games and gamification based on purpose

objective of the service, but rather a method of encouragement. The final type of game, serious games, has the primary goal of presenting or addressing a serious topic in a way that is entertaining for the user, thus combining the entertainment with serious goals.

For the sake of this study a serious game was chosen to be used to promote digital wellness among preschool children. A serious game was chosen because promoting digital wellness is a serious goal, but it is important to entertain the preschool users in order to maintain attention and incentive.

4.2 Classifying serious games

Due to the fact that serious games have such a rich typology, identifying a classification system for these serious games is a necessary step (Alvarez & Djaouti, 2011). Several methods and tools have been used in an attempt to classify serious games, but most of these classification systems have not reached a level of general acceptance (Djaouti et al., 2011). Some of these methods include market-based classifications (classification based on the market that uses it); purpose-based classifications (classification based on the intention that each game was designed to satisfy); and multi criteria classification (classification based on both the market and purpose of the game).

As stated in Section 4.1.2, serious games are defined by the combination of serious aspects and game aspects, but the above-mentioned classifications focus only on the serious aspects and disregards the game aspects (Djaouti et al., 2011). In order to improve these classifications, it is necessary to include the game aspects. In an attempt to accomplish this, Djaouti et al. (2011) proposed a classification system that is valid for both the "serious"

and "game" dimensions. This system is called the G/P/S model and it classifies serious games using three criteria: gameplay; purpose; and scope.

4.2.1 Gameplay

The gameplay criterion refers to the type of gameplay used and is intended to provide information about the game structure and how it is played (Djaouti et al., 2011). The gameplay aspect focuses more on the "game" dimension of serious games.

Gameplay can be defined as the combination of the following five components: rules, the command modes and the spatial-, temporal- and dramaturgical structures (Alvarez & Djaouti, 2011). Although all five these elements are essential components of the definition of gameplay, the "rules" component is used for this classification as it is logical in nature and thus eligible for formal deconstruction (Alvarez & Djaouti, 2011; Djaouti et al., 2011). By deconstructing the "rules" element, two types of games can be identified:

Play-based

Play-based games refers to a more freeform kind of game. This means that the game lacks any rule defining goals and thus it cannot be won or lost. Because there is no formal goal to aim for, the performance of the player is not determined by the game, but rather by the players themselves (Djaouti et al., 2011); and

Game-based

Game-based games refers to a more structured form of game, with defining goals that allow the player to win or lose the game. These rules are used to provide the user with positive or negative feedback based on their actions (Djaouti et al., 2011).

4.2.2 Purpose

The purpose criterion refers to the designed purpose of the game (Alvarez & Djaouti, 2011; Djaouti et al., 2011). This purpose does not refer to the "entertainment" aspect of serious games, but rather to the "serious" goal that is addressed in the game.

The purpose of serious games can be traced to three main goals: Broadcasting a message; Training users; or Exchanging data (Alvarez & Djaouti, 2011; Djaouti et al., 2011). These purposes can be defined as follows:

Message-broadcasting

These games have the simple goal of broadcasting a message to the player. To further distinguish between the nature of the message that is being broadcast, four characteristics of these messages are defined.

1. Educative messages: These messages are used to transmit knowledge or education to the player and are also called "Edugames";
2. Informative messages: Informative messages are used to broadcast a neutral point of view to the player with the goal of informing them. These games are also called "Newsgames";
3. Persuasive messages: These messages use a strategy to influence the players opinions or viewpoint. Typical examples of these games are "Advergames" (games with the primary goal to advertise a product or service) and political games; and
4. Subjective messages: Subjective messages are used to broadcast an opinion. Typical examples of these games are military games and art games (Alvarez & Djaouti, 2011; Djaouti et al., 2011).

Training

Training games are designed to improve certain skills of the player. These training games usually improve the cognitive performance or motor skills of the player by either mental or physical exercise. These games can be classified in two categories: "Training and Simulation games" or "Games for health" (Alvarez & Djaouti, 2011; Djaouti et al., 2011).

Data exchange

Data exchange games are focused on collecting information from their players or encouraging them to exchange data. In other words, data exchange games are games designed as support for exchanging data between players or between the players and the publisher of the game (Alvarez & Djaouti, 2011; Djaouti et al., 2011). These games are less common than the other categories and these games are also called "Datagames".

4.2.3 Scope

The final criterion, scope (Djaouti et al., 2011) (also called Sector (Alvarez & Djaouti, 2011)), is used to classify serious games based on the target market or audience that use the application. This means that the scope criterion refers to both the individuals and the sectors that use the game and thus, the scope criterion can be divided into two levels: the market and the users (Alvarez & Djaouti, 2011; Djaouti et al., 2011).

Market

The market level refers to the target industry, market or sector that the game will be used in. This does thus not identify the individuals that will use the game, but rather the general area of expertise that the game is targeted at for intended use. It is important to note that the list of areas of applications must be updated regularly to reflect the emergence of new sectors, but the following is a list of commonly targeted sectors: State and Government, Military, Health, Education, Corporate, Religion, Art and Culture, Ecology, Politics, Humanitarian and charity work, Media, Advertising, Scientific Research and Entertainment (Alvarez & Djaouti, 2011; Djaouti et al., 2011).

Users

The user level refers specifically to the target audience within the target market. The user level identifies the group of people that will use the application in two ways, the player age and the player type.

The player's age is classified in several ranges inspired by both the ESRB and PEGI rating systems. Age is used to identify the age range of the players. The player type is used to differentiate between three categories: General public (any person); Professionals (the workers in the target system); and Students (people studying to become a professional) (Alvarez & Djaouti, 2011; Djaouti et al., 2011).

By using these three criteria in combination, it becomes possible to classify serious games not only based on the "serious" dimension, but rather based on a mixture of the "serious" dimension (Purpose and Scope) and the more entertaining "game" dimension (Gameplay). It is important to note that the classification as given above is only applicable to the original and intended use of these games, as serious games (and all other types of games) can be used in a way that was not intended by the designer. This classification method will therefore not be applicable to entertainment games that provide incidental learning nor will it apply to serious games that are used differently than intended (in a non-serious setting) (Alvarez & Djaouti, 2011).

When comparing the model above with the goal of this study (creating a mobile serious game to promote digital wellness among preschool children), it becomes possible to identify and classify the serious game that will be created. The gameplay of the mobile serious game will be structured and it will have defining goals, meaning that it will be classified as game-based. Game-based gameplay is used because it provides the player with better structure, simple rules and constructive feedback. The purpose of the mobile serious game is to spread a message to children. This aligns with the goal of the study to spread awareness rather than training the player to complete a

certain task. This message can be classified as educative. The target market of the game is the education sector, with the users being preschool children.

4.3 Optimal game development

Serious games have great potential to be used as a tool for education, but even with the market flooded with different educational games for children of all ages (Shuler et al., 2012), serious games are still not adopted into mainstream education. To better understand the reason for this, it is necessary to investigate why these games often fail.

4.3.1 Why serious games often fail

Serious games have been one of the least popular gaming genres to date. Klopfer et al. (2009) identified four barriers slowing the adoption and development of serious games:

- Barriers to adoption - These barriers include standardized curriculum requirements, parents' and educators' attitudes, the lack of class logistics and models to integrate games into the curriculum and the lack of support for teachers, lack of assessment possibilities, evidence of the effectiveness of learning games, and social and cultural structures;
- Barriers to design and development - This includes development costs and processes, the play-testing possibilities and limited sources of funding;
- Barriers to sustainability such as maintenance, update and support issues; and
- Barriers to innovation such as the limitation of data, pedagogical paradigms, research, and ambition.

Developing games requires both time and money, but because serious games are less popular, there are fewer financial rewards when creating a game in this genre. This causes developers to spend less time creating good serious games and consequently the quality of many serious games are below the standard of other genres (Klopfer et al., 2009). This in turn causes fewer people to buy serious games, resulting in even less money to create good quality games.

In an attempt to break the negative feedback loop of serious games, one can attempt to create more games of higher quality, by using optimal game development techniques.

4.3.2 Optimal game development

In literature, many individuals and teams have researched the topic of optimal game development (Mildner et al., 2015; Mitgutsch & Alvarado, 2012; Charsky, 2010; Hunicke et al., 2004; Kramer, 2000; Malone & Lepper, 1987; Malone, 1981). The goal of optimal game development is to implement certain design elements to create a game that will increase the motivation of the players and can objectively be classified as a good game. In table 4.1, 7 studies are listed with the game elements that they identified as necessary for game development.

Table 4.1: Optimal game development elements

Author	**Paper Title**	**Elements identified**
Malone (1981)	Toward a Theory of Intrinsic Instruction	- Challenge; - Fantasy; and - Curiosity.
Malone and Lepper (1987)	Making learning fun: A taxonomy of intrinsic motivations for learning	- Challenge; - Fantasy; - Curiosity; and - Control.
Kramer (2000)	What makes a game good	- Originality; - Freshness and Replayability; - Surprise; - Equal opportunity; - Winning chances; - No “Kingmaker effect”; - No early elimination; - Reasonable waiting times; - Creative control; - Uniformity; - Quality of components; - Target groups; - Tension; - Learning and mastering a game; and - Complexity and Influence.

Continued on next page

Table 4.1 – Continued from previous page

Author	**Paper Title**	**Elements identified**
Hunicke et al. (2004)	MDA: A Formal Approach to Game Design and Game Research	- Sensation; - Fantasy; - Narrative; - Challenge; - Fellowship; - Discovery; - Expression; and - Submission.
Charsky (2010)	From Edutainment to Serious Games: A Change in the Use of Game Characteristics	- Competition and Goals; - Rules; - Choice; - Challenges; and - Fantasy.
Mitgutsch and Alvarado (2012)	Purposeful by design?: A serious game design assessment framework	- Purpose; - Contents and information; - Game mechanics; - Fiction and narrative; - Aesthetic and graphics; - Framing; and - Coherence and cohesiveness of the game system.
Mildner et al. (2015)	From game characteristics to effective learning games evaluation of a component-based quiz game	- Competition and Goals; - Rules; - Choice; - Challenges; - Fantasy; and - Aesthetics/graphics.

For the purpose of this study the elements identified by Mildner et al. (2015) will be implemented. This approach is used because it builds on multiple previous studies of identifying critical elements that contribute to making a good game.

The first elements identified in this approach are challenge, fantasy and curiosity. These three elements were first identified by Malone (1981), and these three elements are widely regarded as core elements, with multiple studies extending or adapting this list. One example of such an adaption is the adaption by Charsky (2010), who removed the element of curiosity and added three elements to the list: competition and goals; rules; and choice.

In the approach by Mildner et al. (2015), the elements highlighted by

Charsky (2010) were identified as the core elements of good games, with the single addition of the aesthetics/graphics element identified by Mitgutsch and Alvarado (2012). The following is a list of all of the identified elements, each with a brief description of what that element entails.

Challenge

The challenge element describes the problem or issue that has to be resolved by the player (Mildner et al., 2015). In other words, challenges are the tasks or activities in a game that requires a certain level of skill from the player (Charsky, 2010; Malone & Lepper, 1987). It is important to have the correct level of challenge in a game, as a task that is either too challenging, or not challenging enough would have a negative effect on the player's motivation and enjoyment (Cowley et al., 2008).

Fantasy

Fantasy in games refers to the theme or setting of the game that distinguishes it from reality. Fantasy plays an important role in the motivation of players by making the player more involved (Malone, 1981). Fantasy can be either endogenous or exogenous (Charsky, 2010).

- Endogenous fantasy refers to using fantasy as a tool for expanding the knowledge of the player. When endogenous fantasy is used, there is little, or no connection between the challenge and the fantasy elements.
- Exogenous fantasy refers to using fantasy elements as a reward to the player. Thus, by completing set challenges, the player can be rewarded with more lore or other fantasy components.

Choice

Another critical element for any game is the element of choice (often referred to as control (Malone & Lepper, 1987)). The element of choice refers to the options that a player has prior to and in a game. Choices have to be made by the player for the game to progress. There are three forms of choice: Expressive choice; strategic choice; and tactical choice (Charsky, 2010).

- Expressive choices have little to no impact on the game. These choices are made by the player to express themselves and relate more to the game. An example of this type of choice is picking or creating an avatar that represents the player.
- Strategic choices are choices that directly influence how the game is played. This is often referred to as the game settings that can be adapted to fit the needs of the player. An example of this type of choice is selecting of a difficulty level for the game.

- Tactical choices are the choices that the player makes in the game. Some examples of this is choosing answers from multiple prompts or choosing between different paths to travel.

Rules

The rules of a game is a set of constraints that limit the actions that a player can and cannot take. In contrast to fantasy, the rules of a game anchors the game in reality and enables the lessons learned in the game to be translated to real life (Charsky, 2010). Rules also give structure to games and enable a fair gaming experience for the whole game community (Mildner et al., 2015).

Competition and goals

According to Charsky (2010), competition and goals form one of the most important elements of games, as almost every game incorporates this element. The goal of the game refers to the winning conditions, while competition refers to the obstacles on the way of reaching these conditions. In some games, the goal is the victory condition resulting from the competition. Competition and goal are intertwined as using competition in a game serves as motivation for the player to reach the goal.

Aesthetics

The aesthetics or presentation of a game is a motivating factor that is often overlooked. The aesthetics of a game refers to the overall presentation of the game and the visual and auditory appeal of the game. One of the first hurdles that any game must overcome is getting the player interested by presenting it in a appealing way. If it has a pleasing aesthetic, players will be more likely to play and complete the game (Mildner et al., 2015; Mitgutsch & Alvarado, 2012).

The game development elements that have been identified are essential for developing a game that is fun and objectively good. Due to the fact that one of the objectives listed in Section 1.3 is to create a game that is fun to play, these elements are to be implemented in the creating of the mobile serious game.

4.4 Serious games for preschool children

The fact that preschool children learn through play (Yogman et al., 2018) allows educators and parents to make use of games to assist in teaching children new skills and building on existing knowledge. When the idea of using games for teaching and spreading awareness is considered in the light

of children's growing exposure to digital technology (Callaghan & Reich, 2018), the idea of using digital games to spread awareness among children appears to be a viable approach. This has become evident by the number of serious games targeted directly at young children.

4.4.1 Similar games

A list of serious games targeted at young children with the goal of teaching or spreading awareness of digital wellness and cybersecurity is given in Table 4.2. The games listed here serve as a practical reference when creating a serious game for children about cybersecurity and digital wellness. Identifying and analysing these games also enables a better understanding of the physical implementation of the game elements identified in Section 4.3.2.

Table 4.2: Serious games for children

Author/developer	**Game name**	**Digital wellness topic**
Google (2019)	Interland: Be Internet awesome	- Communicate Responsibly; -Know the Signs of a Potential Scam; -Create a Strong Password; and -Set an Example and take action against inappropriate behaviour
Australian Department of Broadband Communications and the Digital Economy (2011)	Budd:e	- Staying safe online - Protection against viruses and malware - Using social networks responsibly
Carnegie Mellon University (2011)	Carnegie Cadets	- Staying safe online - Protection against viruses and malware - Using social networks responsibly
FBI (n.d.)	FBI Cyber Game	- Staying safe online
PBS - NOVA labs (n.d.)	PBS Cybersecurity Lab	- Staying safe online - Spotting scams - Defending against cyber attacks

4.4.2 Applications for preschool children

Serious games targeted at preschool children have become increasingly popular over time (Shuler et al., 2012). It is important to note that even though there are more games directed at preschool children, it does not mean that these games are optimised for this target audience. In an attempt to create a framework for games aimed specifically at preschool children, Callaghan and Reich (2018) identified the following design elements based on how preschool children learn:

Clear and simple goals

Children learn best with clear instructions and modelling which allows them to draw connections to existing beliefs (Cowley et al., 2008). By specifying clear and simple goals at the start of the game, the child will be less likely to become confused and overwhelmed, empowering them to complete their tasks with minimal disruptions;

Quality of feedback and rewards

Feedback is a powerful and important tool that encourages children and notifies them if they are doing something wrong. At preschool age, most children are not able to read and thus text feedback will not be of any help to the child. A better alternative is to combine both visual and auditory feedback that can be easily understood by the child;

Structure of challenge

When structuring a challenge, it is important to keep the level of performance of the target audience in mind. By adapting the level of challenge of an application to gradually increase in difficulty as the child understands more of the material, as well as decrease in difficulty when the child appears to struggle, it becomes possible to scaffold the child's learning. Adaptive scaffolding in applications can greatly influence the child's learning experience; and

Motion based interactions

Motion based interactions refers to different physical methods that children can use to interact with applications. These motion-based interactions can serve as an alternative to complex touch screen activities that might be too difficult for many children. By creating the game in such a way that it aligns with the physical capabilities of preschool children (e.g., touchable object sizes, simplified touchscreen motions at first, etc.), the overall experience of the child will improve. In most cases this element refers to the design of the game interface and therefore will be referred to as appropriate interface.

The four elements listed above is essential to ensure that a game is suited to a pre-school aged child. Because one of the objectives listed in Section 1.3 is to create a game that is suitable for pre-school children, these elements are to be implemented in the created mobile serious game.

4.5 Summary

In this chapter the topic of serious games was discussed. The first section was used to discuss serious games by first defining the concept of play, followed by pointing out the differences between serious games, entertainment games and gamification and giving a definition for each type of game. This section was followed by identifying a classification model based on the gameplay, purpose and scope of the game. This classification model is used to highlight the different types of serious games and to further aid in the creation of a mobile serious game that will promote digital wellness among preschool children. In this section it was concluded that the mobile serious game can be classified as a game that uses game-based gameplay, with the purpose of conveying an educative message to preschool children in the education market.

In the third section of this chapter, the topic of optimal game development was discussed. This section highlighted why serious games are often unsuccessful. Different game elements were identified which can be used to create a game that can be objectively classified as a "good" game. These elements were selected by identifying different studies from literature and comparing them to select an optimal development model. The final section was used to specifically highlight serious games for children. In this section a list of similar games was identified, followed by four elements identified from literature that can be used to ensure that a mobile game is suitable for preschool children.

In the next chapter, the technical aspects of the game design will be discussed.

Chapter 5

Discussion of the application

In this chapter, the technical aspects of the created mobile game is discussed. Section 5.1 lists the critical elements as identified from the literature. In Section 5.2, the different technologies used in the creation of the game is identified, followed by a brief motivation as to why these technologies were chosen. In Section 5.3 an overview of the created game is given. This overview describes the layout and functionality of the different scenes of the game, followed by an explanation of how each element identified from literature is implemented into the scene.

5.1 Elements identified from literature

As stated in Section 1.2, the goal of this study is to identify core elements that, when implemented in a mobile serious game, can serve as a method to promote awareness of digital wellness among pre-school children. When implementing these elements in a game, the resulting game should satisfy the following three criteria: the game should be (1) fun to play, (2) appropriate for pre-school children and (3) spread awareness of digital wellness. In the first phase of identifying elements that adhere to these criteria, the following elements were identified from existing literature:

1. Elements that ensure that a game is good/fun:
    - Challenge;
    - Fantasy;
    - Choice;
    - Rules;
    - Competitions and goals; and
    - Aesthetics.

2. Elements that ensure that a game is appropriate for children:
    - Clear and simple goals;
    - Quality feedback and rewards;
    - Structured challenges; and
    - Appropriate interface.
3. Elements that increase the effectiveness of a digital wellness awareness campaign:
    - Communication;
    - Simplicity;
    - Understanding digital wellness;
    - Using appropriate material for target group;
    - Present material in an appropriate way (methods of learning from Section 3.5);and
    - Focusing on different topics of digital wellness.

While developing the mobile serious game, only the elements listed under criteria 1 and 2 were directly implemented into the game. The elements listed in criteria 3 were not directly implemented due to the following reasons:

- Some elements are only focused on the content of the awareness campaign. These elements are not implemented directly into the game, but it is very important when picking content to be used or when creating new content (content selected in Section 3.3). These elements are: "Simplicity"; "Understanding digital wellness"; "Using appropriate material for target group"; and "Focusing on different topics of digital wellness";
- Certain elements are not applicable to a game medium. The "Communication" element is an example of this, because it is not possible for the developer to directly communicate with the user in an attempt to secure the human element of digital security; and
- One of the elements is implemented in games by default. This is the "Present material in an appropriate way" element (games allow learning via observation, listening, exploring, experimenting and asking questions).

The second phase of identifying core elements requires the knowledge and expertise of experts in the field of pre-school education. In this phase, the elements identified from literature is implemented into a mobile serious game for children. This game is then presented to experts to enable them to review the implemented elements and identify any additional elements that can contribute to the success of the application.

5.2 Technologies used

The technologies used to create the mobile game can be divided into three main categories: Game engine; Programming language; and Visual editing.

5.2.1 Game engine

The game engine used in the development of the game is the Godot game engine [1]. The Godot game engine is a free and open source game development engine, which provides a large collection of common tools that assist in the process of game development. Godot game engine supports multiple scripting options, including: GDScript (Godot's integrated scripting language), C#, C++, Rust, Nim, D, Visual scripting. etc.

Godot game engine was chosen as the game development platform for the following reasons:

- Multi-platform editing. This allows developers to develop games on any desktop operating system, regardless of whether the platform is a 32-bit or 64-bit version.
- Lightweight. Godot is a lightweight editor that is not resource intensive. The lightweight nature of the engine allows for easy setup and use on any system.
- Multiple platform deployment. Deployment and exporting to most platforms can be done using a single click. These platforms include Desktop (Windows, macOS, Linux, UWP, and BSD); Mobile (iOS and Android); Consoles (Nintendo Switch, PlayStation 4 and Xbox One, all via third-party providers); and Web (using HTML5 and WebAssembly).
- Separate 2D and 3D game engines. This allows for a smoother and more convenient 2D game development and deployment experience.
- Built in tools and resources. Godot provides ready to use tools and resources that can be used as building blocks or nodes to create an application.

5.2.2 Programming language

The application was written using the C# programming language. C# is an object-oriented programming language developed by Microsoft as a modern, general purpose language and it is commonly used in many applications and projects.

C# was chosen as the programming language for the application for the following reasons:

[1] https://godotengine.org/

- Object-Oriented programming. Object-Oriented programming is a modular computer programming model that allows code to be reused and provides the programmer with a lot of flexibility to solve problems effectively.
- Cross platform programming. C# allows programming across various platforms.
- Automatic garbage collection. This means that C# is efficient at managing the user's system, allowing most programs to run smoother.
- Speed. C# has a fast compilation and execution time.

5.2.3 Visual editing

The editing of the visual components of the application was done using two programs: Paint.net [2] and Synfig [3].

Paint.net is a free to use image manipulation and drawing program that provides multiple tools to edit and create visual resources. This software is simple to understand and easy to use, but still provides the user with enough tools and options to complete almost any task.

Synfig is a free and open-source program that is used for 2D animation. This software can be used to easily animate any image or 2D visual resource, by providing powerful vector tweening options. These vector tweening capabilities, combined with multiple layering tools, filtering options and other advanced controls allow easy 2D animation that can be used by users of any skill level.

5.3 Application overview

The resulting application/serious game consists of four main scenes. Each of these scenes contribute to the main goal of spreading awareness of digital wellness among pre-school children, by implementing some of the elements identified in Section 4.3.2 and Section 4.4.2. By implementing these elements, the overall fun factor of the game can be increased, adding to the overall motivation and enjoyment level of the children.

In this section, an overview of the application is given. This is achieved by explaining the layout and function of each scene and its components, followed by a brief summary of the different elements implemented in each of these scenes.

[2] https://www.getpaint.net/
[3] https://www.synfig.org/

5.3.1 Main Menu

The first scene that the user can interact with is the main menu screen. This scene primarily serves as a selection screen for picking the poem, quiz and game that the user will play. A screenshot of the main menu scene is given in Figure 5.1.

Figure 5.1: Application main menu

The following is a list of the different components of the main menu screen, with a brief description of their functions (as numbered in Figure 5.1):

1. Left navigation button - This navigation button is used to scroll counter clockwise through the available selection of stories. When the left button is tapped, all of the animations that represent a poem (3-5), will rotate one position counter clockwise.

2. Right navigation button - This navigation button is used to scroll clockwise through the available selection of stories. When the right button is tapped, all of the animations that represent a poem (3-5), will rotate one position clockwise.

3. Current selected poem - The current selected poem component is a selectable animation that corresponds to a certain poem. The current selected poem's animation is always playing. When this component is tapped, the next scene (poem scene) that corresponds to the selected

poem is displayed. When one of the navigation buttons is tapped, this element will move to position 4 or 5 (depending on the arrow tapped), and the animation will stop playing.

4. Previous poem - The previous poem component is a non-clickable and static animation that corresponds to a certain poem. This component is used to indicate what poem will become the selected poem if the left navigation button (1) is tapped.

5. Next poem - The next poem component is a non-clickable and static animation that corresponds to a certain poem. This component is used to indicate what poem will become the selected poem if the right navigation button (2) is tapped.

6. Settings - The settings button is used to display the game settings. The current version of the game has only two settings: volume control and a default level selector. More settings will be added in future versions (Multiple languages, age selection, username selection, etc.).

7. Selected poem title - This component displays the title of the currently selected poem.

In Table 5.1 the game elements identified in Section 4.3.2 and Section 4.4.2 are listed with a brief explanation of how these elements are implemented in the main menu scene.

Table 5.1: Implemented game elements in the main menu scene.

Game element	**Implementation**
Challenge	The challenge element is not implemented in the main menu scene.
Fantasy	The fantasy element is implemented and highlighted in the main menu scene through the use of the animal animations that the user must tap to select. The use of the fictional characters, the jungle background and the jungle themed music contributes to the fantasy feel of the scene.
Choice	The element that is most prominent in the main menu scene, is the element of choice. This scene allows the user to not only select a poem (expressive/strategic choice), but it also allows the user to change the game settings (strategic choice).
Rules	The rules of the main menu scene is enforced by forcing valid input (tapping arrows, settings and selecting a poem). This means that the user is not able make any mistakes in this scene.
Competition and goals	The competition and goals elements are not implemented in the main menu scene, as it does not yet allow the user to play.
Aesthetics	The aesthetic element of the game is enforced by using fun and colourful animations, a background that contributes to the fantasy, without drawing attention away from the important elements, big buttons, fitting music and audio feedback when components are tapped.
Clear and simple goals	Instructions to select a story is provided using both text and audio instructions.
Feedback and rewards	Audio feedback provided on buttons tapped.
Structured challenge	The structured challenge element is not implemented in the main menu scene.
Appropriate interface	The interaction for children is made easier by providing big icons that are easy to tap, audio feedback on buttons tapped, bright colours that are not overwhelming and a simple layout.

5.3.2 Poems

Once the user selects a poem in the main menu scene, the application will display the poem scene. In this scene the selected poem will be displayed on the screen and it will be read to the user. The user interacts with the screen by tapping anywhere to move to the next paragraph or page. The main goal of this scene is to educate the user and spread awareness of the dangers of cyberspace in an enjoyable way.

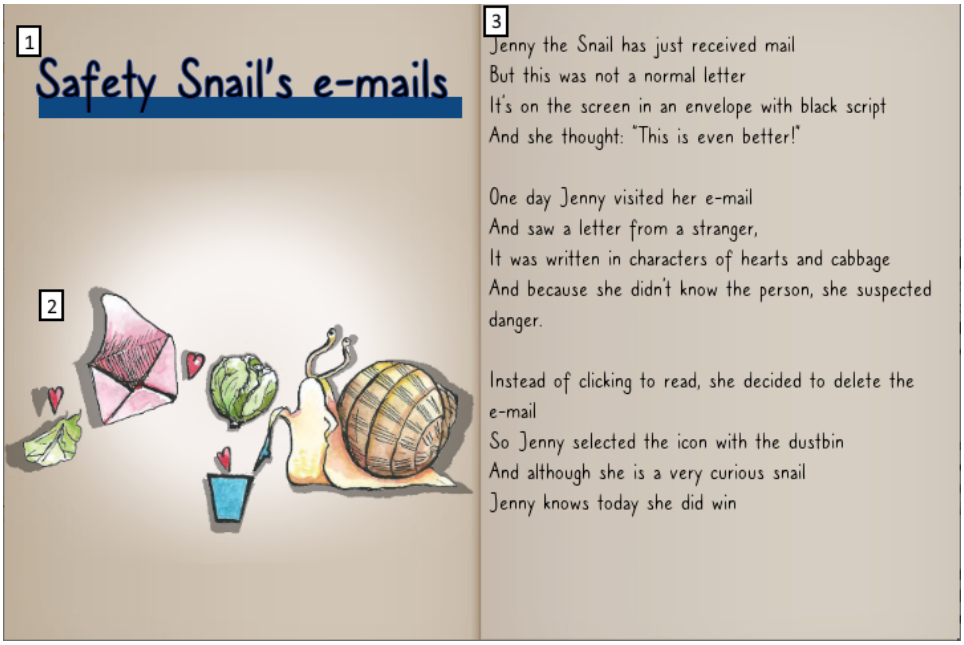

Figure 5.2: Poem scene

The following is a list of the different components of the main menu screen, with a brief description of their functions (as numbered in Figure 5.2):

1. Poem title - This component displays the name of the poem that is currently being read.

2. Story animation - The animation component is used to represent a part of the poem visually. This animation changes each time a new paragraph or page is being read.

3. Poem text - The poem text shows the content of the poem, the moral of the story and questions for the user to discuss with other people. Each time the user taps on the screen, the next paragraph on the page will slowly begin to appear. This also triggers the audio of each paragraph being read to start playing. When there is no more space

for text to appear on the page, an animation plays to simulate a page being turned.

In Table 5.2 the game elements identified in Section 4.3.2 and Section 4.4.2 are listed with a brief explanation of how these elements are implemented in the poem scene.

Table 5.2: Implemented game elements in the poem scene.

Game element	**Implementation**
Challenge	The challenge element is not implemented in the poem scene.
Fantasy	The poem scene is used to present information in a fun way and this was done by implementing endogenous fantasy elements. This scene advances the characters, lore and story of the fictional characters. The fantasy element is implemented by using the fictional story/poem and the animations representing each paragraph.
Choice	This scene does not implement choice as it is a poem that is being read.
Rules	This scene enforces rules by only allowing the continuation of the story to the next paragraph if all the text of the current paragraph has been shown. This encourages the user to read the poem without skipping the lessons and moral that the poem teaches.
Competition and goals	Competition and goals were implemented into the poem scene in the form of questions at the end of the poem. Although these questions are only meant to initiate a discussion between the user and other people about the topic, the question can spark an optional goal for the user. This goal is to have a discussion or deep thought about the topic and provide an answer that expands the user's knowledge about the topic.

Continued on next page

Table 5.2 – Continued from previous page

Game element	**Implementation**
Aesthetics	The visuals and background of the poem scene is basic, to avoid unnecessary distractions and to stimulate an environment of learning. The background is set to look like the inside of a book, with no extra colours. The jungle themed background music is reduced to a very low level and the only clear sounds are the poem being read and the sound of the page turning.
Clear and simple goals	The goal of this scene is clear and simple, as the user only needs to tap on the screen and listen to or read the poem.
Feedback and rewards	The poem scene use exogenous fantasy in the form of new and different animations for each paragraph as a way to reward the user for listening to or reading the poem.
Structured challenge	The structuring of the challenge of the quiz scene starts in the poem scene. Although the poem scene does not implement any form of challenge, it does structure the challenge of the next scene, by providing all of the necessary information to answer the questions in the quiz.
Appropriate interface	The interaction that this scene required is acceptable for pre-school children, as the only interaction needed is a tap on the screen to progress the story. This is an easier action to perform than tapping on specific buttons.

5.3.3 Quiz

The quiz scene is entered immediately after the user completes the reflection questions in the poem scene. The aim of this scene is to determine whether or not the user understands the problem described in the poem by motivating them to answer four questions about the topic. These questions are randomly chosen from a pool of questions to provide a form of replayability and to ensure that a pattern cannot be memorised when answering the questions. The quiz does not block progress if the user's results are subpar. The user's progress does not get blocked for two reasons: The goal of the game is not to educate children of the dangers, but rather to spread awareness on the matter; and the quiz is only meant to be used by parents, teachers and guardians as a tool to motivate the user keep track of their efforts and progression.

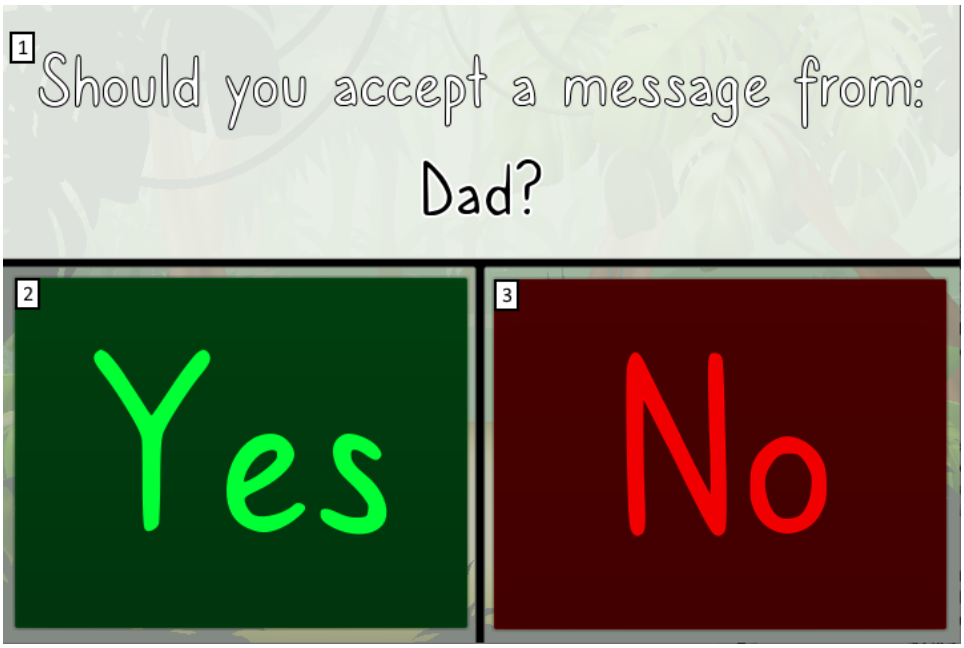

Figure 5.3: Quiz question screen

The following is a list of the different components of the quiz scene, with a brief description of their functions (as numbered in Figure 5.3 and Figure 5.4):

1. Question text - This component displays the current quiz question. The question is chosen randomly from a question pool and a total of 4 questions are asked per quiz. The quiz questions are also read out loud to the user.

2. Yes button - The "yes" button can be tapped to answer the given question. If this button is tapped, the user answers "yes" to the question. Once this button is tapped, the screen will either display a large check mark or a large cross to indicate whether the user's answer was correct or incorrect. This also triggers a sound effect to indicate whether the answer was correct or incorrect.

3. No button - The "no" button can be tapped to answer the given question. If this button is tapped, the user answers "no" to the question. Once this button is tapped, the screen will either display a large check mark or a large cross to indicate whether the user's answer was correct or incorrect. This also triggers a sound effect to indicate whether the answer was correct or incorrect.

4. Quiz results - This component provides visual feedback based on the number of questions that the user had correct. The result feedback

displays four silhouettes of a character (character changes based on poem chosen). Each of these silhouettes represent one question. For each question that the user answered correctly, one character silhouette will be filled in. The example in Figure 5.4 shows a result where the user answered three questions correctly.

5. Badge feedback - The badge component is used as feedback to motivate and reward the player. The badge that is displayed is dependent on how well the user does in the quiz, but it is also affected by a random element. How well the user does determine the pool of possible badges that the user can receive and a badge will be chosen randomly from the given pool. Each badge also has audio feedback to motivate the user.

6. Try again button - The try again button is only available after the quiz is completed. When this button is clicked, the quiz will start again with randomly chosen questions.

7. Continue button - The continue button is only available after the quiz is completed. When this button is clicked, the user is navigated to the game scene.

Figure 5.4: Quiz results

In Table 5.3 the game elements identified in Section 4.3.2 and Section 4.4.2 are listed with a brief explanation of how these elements are implemented in the poem scene.

Table 5.3: Implemented game elements in the quiz scene.

Game element	**Implementation**
Challenge	The challenge element is one of the key game elements in the quiz scene. The challenge of the quiz scene is to apply the knowledge gained from the poem scene by answering four questions from real life scenarios.
Fantasy	The fantasy element is less prominent in the quiz scene than in any other scene. The overall theme of the quiz is more serious than the other scenes in an attempt to make the user aware of the real world scenarios and implications thereof. Therefore, the fantasy element is only used in an exogenous way, to reward the user afterwards.
Choice	The quiz scene allows the user to make tactical choices by prompting the user to answer the given questions. These choices have a direct impact on the results that the user receive. The user is also given the choice to retake the quiz or continue to the game, allowing more freedom to the user.
Rules	The rules of the quiz are simple. The user is prompted to answer four questions in succession. Correct answers add to the user's score and wrong answers do not add to the user's score. The user is only allowed to select either "Yes" or "No" as an answer to the question.
Competition and goals	The goal of the quiz scene is to test the user's knowledge and understanding of the given topic. The user's goal is to answer the given questions correctly by applying the information given in the poem. The users compete against themselves and the scores they received in previous attempts.
	Continued on next page

Table 5.3 – Continued from previous page

Game element	**Implementation**
Aesthetics	As was the case for the fantasy element of the quiz scene, less emphasis is placed on the aesthetic element of the quiz. The visual layout of the quiz question screen is basic, with a dull background, clear question text and two large, coloured buttons that are easy to tap. The colours of the buttons are used to indicate the "Yes" (green) and "No" (Red) answers to the question. In contrast to the question screen, the result screen displays images of the characters in the poems, colourful buttons and a motivating badge.
Clear and simple goals	The goal of the quiz is clear and presented with both text and audio. The goal and mechanics of this scene is simple, as the user only has to answer yes or no to each question.
Feedback and rewards	Feedback on the quiz scene is done instantly, using both visual and audio effects. Each correct answer is rewarded with a green check mark and positive sound, whereas each incorrect mark receives a red cross with a negative sound. After the quiz is completed, the user is rewarded with a visual display of the number of questions that they answered correctly, a badge to congratulate them on their achievement and a positive audio feedback (positive tune and verbal feedback).
Structured challenge	Structured challenge is only implemented to a small degree in the quiz scene, because the difficulty level of the quiz is set. There are two reasons why the quiz challenge is not scaled: the first reason is that the goal of the quiz is not to teach the user new information, but rather spreading awareness of the dangers in cyberspace; and the second reason is that the content covered in the poem is very specific and already structured to the target audience.
Appropriate interface	The interaction is made suitable by using large buttons and visual effects, making buttons easy to use. The use of audio also accommodates users who are not yet able to read. Input and actions needed to use this scene are simple.

5.3.4 Game

The final scene of the application is the game scene. This scene allows the user to play a certain mini-game based on the poem that they have chosen. Each of these games are different and serves as the final reward for completing the poem and quiz scenes. Before the game starts, the instructions and goal of the game are displayed on the screen and it is read out loud (shown in Figure 5.5) . The user can then use the slider to pick a level and play the game.

Figure 5.5: Game menu

The first game (shown in Figure 5.6) is called Safety Snail's email game. The objective of the game is to move the different coloured envelopes to the same colour column before the envelope reaches the bottom. Twenty correct matches win the game and three incorrect matches lose the game. This game uses random colour placement and random slide sizes to increase replayability. This game is an exercise in small motor movement and colour matching. The game also has the underlying message of sorting through emails and either answering or ignoring the message based on its appearance. A higher difficulty level in the game increases the speed at which the envelopes fall, the number of different colours and the number of slides.

The second game (shown in Figure 5.7) is called the Happy Hippo game. The objective of this game is to tap on the bullies (buffaloes) as they appear, while avoiding tapping on the hippos. The game can be won by tapping on twenty bullies and the game is lost if three hippos are tapped. The bullies

Figure 5.6: Safety Snail's email game

and hippos spawn every few seconds at a random location that does not overlap other targets. This game is an exercise in small motor movement and reflexes. The message of the game is to take action against bullies by reporting them to an adult. A higher difficulty level increases the speed at which targets appear and disappear and the size of the targets.

The third game (shown in Figure 5.8) is called the Wolf, Hyena and Fox game. In this game the user has to flip over tiles to reveal the images underneath. Once two tiles are flipped, if their images do not match, they are flipped back. If the images do match, these tiles are turned facing upwards permanently. All of the images are spread randomly between the tiles and each tile has exactly one match. The goal of this game is to match each tile with an identical tile. This game does not have a scoring system and the game cannot be lost. The game is a exercise in memory and the theme of the message of the game is to remember the passwords that one create. A higher difficulty level increases the number of tiles that need to be matched.

When the game is finished, a message is displayed to notify the user whether they won or lost. This message is accompanied by a matching animation relating to the poem. The user is then given the option to play again or return to the main menu. If the user decides to play again, the user is redirected to the level selection screen.

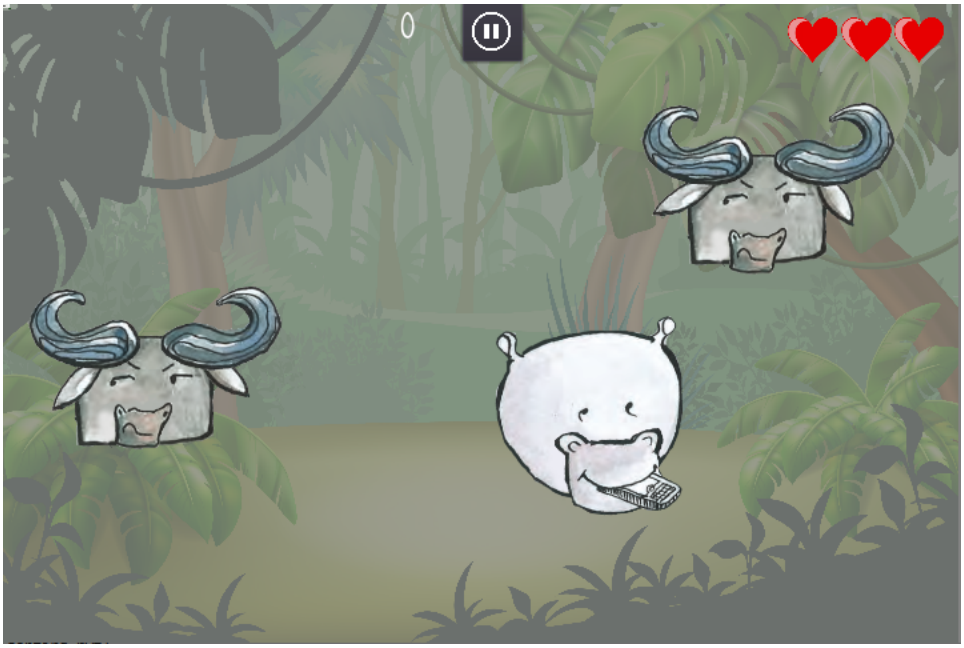

Figure 5.7: Happy Hippo game

Figure 5.8: Wolf, Hyena and Fox game

The following is a list of the different components of the game scene, with a brief description of their functions (as numbered in Figure 5.5 and Figure 5.6):

1. Game instructions - This component explains the rules and goals of the game. These instructions are also read out loud.
2. Level slider - The level slider is used to select the level of difficulty that the user wants to play on. The minimum level is level 1 and the maximum level is level 10.
3. Level indicator - This text is used to show what level is currently selected.
4. Play button - Once the user is ready to start the game, the user can tap the play button to start the game.
5. Score - The score component is used to show the user's current score. Each time the user completes an objective, the score is increased.
6. Pause button - The pause button can be used to pause the game.
7. Lives indicator - This component displays the user's current lives (chances to miss an objective). Each time the user makes a mistake, the lives indicator will display one less heart. This indicator starts with three hearts/lives and once it reaches zero hearts, the mini game will end.

In Table 5.4 the game elements identified in Section 4.3.2 and Section 4.4.2 are listed with a brief explanation of how these elements are implemented in the game scene.

Table 5.4: Implemented game elements in the game scene.

Game element	**Implementation**
Challenge	The challenge of the game scene is to play and win the different games as stated above. Each of the three games present their own unique challenge and it requires certain skills to overcome the challenge.
Fantasy	Exogenous fantasy elements are implemented in the game scene in two ways: the overall theme, audio and visual components that tie in with the jungle theme; and the animations that play at the end of the game to display whether the user won or lost.

Choice	Users are able to make both strategic and tactical choices in the game scene. The main strategic choices are level selection, the option to pause and the option to replay or return to the main menu. Although these strategic choices may appear to be insignificant to the user's overall enjoyment, allowing the user simple choices reduces the feeling of restrictiveness. The tactical choices refer to how the user plays the game and what tactics or strategies are used.
Rules	The rules of each individual game is stated above. These rules highlight the actions that the user can and cannot take.
Competition and goals	The goals of each individual game is stated above. These goals refer to the winning condition that the user has to reach. In Safety Snail's email game and the Happy Hippo game the goal is to reach twenty points without making three mistakes. The goal of the Wolf, Hyena and Fox game is to match all tiles. How to achieve this goal is stated in the rules of the game. Because the user has no opponents, the competition refers to the game itself. This means that the user is ultimately playing these games to win against the program or game itself.
Aesthetics	These games include both visual elements and audio elements that contribute to the overall aesthetic of the game. Safety Snail's email game uses bright colours to motivate the user. The Happy Hippo game attempts to contribute to the overall aesthetic through the moving animations of the targets. The Wolf, Hyena and Fox game has a smoother aesthetic that is less busy with more symmetry than the other games.
Clear and simple goals	The goals and rules of the games are presented at the beginning of the game using both text and audio. These instructions are clear and simple to follow.
Feedback and rewards	The feedback of the games is done with text, audio effects, audio feedback and visual feedback.

Structured challenge	The ability of the users to select a difficulty level allows them to structure the challenge based on their own skill level. This means that both experienced and inexperienced users will be able to play the games at a level that is difficult enough to be challenging, without it being so challenging that a user is unable to win. This method of structuring challenges gives the users a lot more freedom to explore and it allows the users to recognize their own skill level.
Appropriate interface	The large icons and buttons enable a child to easily interact with the different components of the game. The lower levels of the games have big components that are easy to click, drag and use. All of the required motions of the game are simple (tap, drag, release) and are designed for easy interaction.

5.4 Summary

In this chapter, the mobile serious game that was developed was discussed. The first section summarised the core elements that should be implemented as identified in the literature. In the second section the different technologies that were used to develop the game were discussed with a brief explanation of why these technologies were used. In the final section of this chapter, an overview of the mobile serious game which was developed, was given. This overview highlighted the different components of each of the four scenes of the application and the function of these components. After the layout of each scene was described, a brief explanation was given on how each of the identified elements were implemented in the scene.

After its creation, the serious game was sent to experts in the field of pre-school education, for review. The goal of this review was to validate the elements identified in literature and to identify more elements that could contribute to the effectiveness of a mobile serious game, to promote digital wellness among pre-school children. In the following chapter, the results of the expert review are given and analysed.

Chapter 6

Results

In the previous chapter, the technical aspects of the created mobile serious game were discussed. The mobile serious game was sent to experts in the field of pre-school education so that they could give their expert opinion about the developed game, about the elements identified from literature, and any other elements that they deem necessary for the overall success of the game. In this chapter the results of this expert review are discussed.

In Section 6.1, information about the experts is given, including their experience and knowledge of the given problem. The results of the validation of both the game and the identified elements are discussed in the Section 6.2. In Section 6.3, the elements that were identified by the experts are listed and briefly discussed. Finally, in Section 6.4, the research question stated in Section 1.2 is answered by listing all of the critical elements identified during this study.

6.1 Expert reviewers

Six experts were asked to review the game and the elements identified. The reviews were conducted using a questionnaire and it was followed up by a brief phone interview to gather more information. The questionnaire consisted of several questions regarding the reviewer's experience and opinion of the problem; a review of the mobile serious game and the elements implemented in the game; and questions about additional elements that could be identified. The follow up interview was used to gain a better understanding of how the reviewers reacted to each element implemented in the game and to gather more information on the additional elements that they have identified or clear up any issues. The questionnaire is given in Appendix A. The information about the reviewers, obtained from the questionnaire, is given in Table 6.1.

Table 6.1: Reviewer information.

Information	**Reviewers answers**
Years of experience	Total: 168, Average: 28
Age of children	Youngest: 3, Oldest: 9
Awareness of the dangers of cyberspace	4/5 (Good)
Children's exposure to digital and online technologies	4.3/5 (A lot - too much)
View of whether this level of exposure is a problem	Yes: 5, No: 1, Maybe: 0
Knowledge of existing resources that promote awareness of digital wellness to pre-school children	Yes: 1, No: 5
Use existing resources that promote awareness of digital wellness to pre-school children	Yes: 0, No: 6
View on parents' awareness of the dangers of cyberspace	2.16/5 (Poor - average)
View on parents' effectiveness teaching children of the dangers of cyberspace	1.5/5 (Very poor - poor)

The reviewers have a combined experience of 168 years working with pre-school children, resulting in an average of 28 years of experience. The age of the children that the reviewers generally work with ranged between 3 years old and 9 years old.

All six of the reviewers have indicated that they have either a good or very good understanding of the different dangers and threats of the cyberspace and digital technologies, but have also indicated that they believe that the parents of the children are not very aware of these dangers. When asked whether or not the reviewers believe that the parents effectively teach the children about these dangers, all responded negatively.

According to the reviewers, today's pre-school children have a lot of exposure to digital and online technologies and their accompanying dangers, but one of the six reviewers does not believe that the exposure level of the child is problematic. Even though five of the six reviewers indicated that they believe that the current level of exposure of children to digital technologies is problematic, none of the reviewers were aware of any resources that can be used to promote digital wellness and cybersecurity and none of the reviewers used any resources for this purpose.

6.2 Validation

The expert review required that the experts validate both the created game and the identified elements. In this section, the results of the validation process are discussed.

6.2.1 Validation of the game

The validation of the mobile serious game was conducted using a scoring system. After playing the game multiple times, the reviewers were asked to score the implementation of each applicable element on a scale of one to five, where one indicates poor to no implementation and five indicates excellent implementation. In Table 6.2 the average implementation score of each element is shown, with comments from the reviewers.

Table 6.2: Reviewer scores.

Game element	**Average score**	**Answer range**	**Comments**
Challenge	4	3-5	"The younger children might find the app too challenging." (from interview)
Fantasy	4.3	3-5	"It [the animal theme] was very fitting and the children will love it." (from interview)
Choice	4.5	4-5	"More stories" (on suggestion for further development)
Rules	4.5	4-5	N/A
Competition and goals	4.5	4-5	N/A
Aesthetics	4.3	3-5	"Was colourful.", "Visuals", "It is very interactive and colourful." (on which elements stood out most)
Clear and simple goals	4	3-5	"Perhaps clearer instructions on how the story works. (click to turn the page etc.)" (on suggestion for further development)
Feedback and rewards	4	3-5	"Good feedback, but more colours can be good." (Overall comments)
Structured challenge	4	3-5	"I love the different levels of play", "More difficult levels are too difficult (in envelope game)" (from interview)

Continued on next page

Table 6.2 – Continued from previous page

Game element	Average score	Answer range	Comments
Appropriate interface	4.3	3-5	"This application is very child friendly. I will not change a thing. " (on suggestion for further development)
Simplicity	4	3-5	"Do not over simplify it [the content of the game]", "Don't underestimate the children's intelligence" (from interview)
Appropriate materials	4.5	4-5	"It [the animal theme] was very fitting and the children will love it.", "The different concepts are explained to them (the children) very well." (from interview)
Appropriate method of presenting the materials	4.5	4-5	"I like that it [the game] uses sounds, pictures and words so everyone can understand it." (from interview)
Focusing on different topics	3.5	3-4	"More stories" (on suggestion for further development)

When reviewing the results in the above (table 6.2), it is evident that the reviewers believed that the implementation of each element was satisfactory, but there is still room for improvement. The reviewers concluded that the overall implementation of the different elements was done with great success.

To further validate the game, the reviewers were also asked to score the game based on the following three criteria: how much fun is the game; how suitable is the game for pre-school children; and how effective will the game spread awareness of digital wellness? All three of these criteria were awarded an average score of 4.5 out of 5 and a range of 4-5, meaning that the reviewers believed that the game would be an overall success.

6.2.2 Validation of the elements identified in literature

The validation of the elements identified from literature was done in the form of a discussion during interviews. The reviewers were asked which elements they felt were unnecessary or not critical elements and also which elements they deemed most important. The reason why these questions were asked, was to verify that the elements identified from literature can truly be considered to be critical elements.

According to the reviewers, all of the elements identified from literature

can be considered to be necessary and critical elements, contributing to the goal of spreading awareness of digital wellness among pre-school children. One reviewer noted that if even one of the elements were not implemented, the game would be dramatically less effective at spreading awareness. It can be concluded that all of the elements identified in the literature are critical elements, as this validation adds a second level of validity to the elements identified from literature.

Even though all of the reviewers indicated that each one of the identified elements are critical, they still pointed out certain elements that they felt were more important than others. The following is a list of the five most important elements according to the reviewers, ranking from most important to least important, where the number in brackets displays how many experts have identified the element as important:

1. Aesthetics (6/6) - According to the reviewers, the aesthetics of a game is the most important element that was identified. They claimed that in order to grab the attention of a child and maintain that attention long enough, it is necessary to use materials that are both visually and audibly pleasing. If this element is implemented well, it could lead to the success of the application, but if the element is not implemented, no child will attempt to play it.

2. Appropriate content (5/6) - In order to effectively spread awareness on any given topic, it is crucial that the content that is used is appropriate for the target audience. As stated in Section 1.1, one of the core reasons why it is a problem that children are exposed to cyberspace, is the lack of content that is appropriate for children.

3. Structured challenge (2/6) - The challenge element in any game is one of the biggest motivational factors, but it is important that the challenge does not overwhelm the player. Structuring challenges to fit the skill level of the player will ensure that the player is motivated to play and not discouraged from having to keep on trying.

4. Feedback and rewards (2/6) - Using quality feedback and rewards is an effective method of motivating the players and informing them of their progress. One reviewer stated that using feedback and rewards is an effective method of enforcing desired behaviours.

5. Appropriate interface (1/6)- In order for any game to be playable, it is important that the interactions with the game is appropriate for the target audience. This is especially true when the target audience is children. Young children have mostly underdeveloped coordination and motor skills and it is critical that any game aimed at children employs interfaces and interactions that are suitable for them.

It is important to note that the five elements listed above are not a complete list of critical elements, but rather just the elements that the reviewers felt contribute most to the final goal. The best results will be obtained when all elements are present.

6.3 Elements identified in expert review

One of the main goals of the expert review was to identify any critical elements that were not identified in literature. Even though most critical elements can be identified from literature, these elements are not always directly applicable to the given situation. The individuals that directly work with pre-school children on a daily basis is specifically tuned to the situation. During the expert review, each reviewer was asked to identify any additional elements, not listed from literature, that, when implemented in a mobile serious game, should result in a serious game that effectively promotes digital wellness among pre-school children. The following is a list of elements identified by the reviewers, with a brief explanation as to why each element is a critical element.

Balanced simplicity and complexity

During the interview phase, one of the reviewers pointed out that it is important that serious games are not oversimplified. According to the reviewer, the intelligence of children should not be underestimated, and they will quickly lose interest in anything that is oversimplified. This element replaces the original element of simplicity, and it may be seen as an extension of the original element.

Short playtime

Children have active brains and thus a short attention span. In order to optimize the effects of the awareness project, it is crucial that the child does not lose focus. According to a reviewer, there are two methods of achieving this: one is to use engaging visuals and audio to attract attention; and the other is to limit play time to the length of the child's attention span. The reviewer stated that in the case of this game, it would be more effective to limit the time of a single game to ensure that the child is engaged, without forcing attention.

Balanced work and play

During an interview, one reviewer mentioned that many serious games for children are overly focused on the serious (work) aspect of the game. This

may result in a game where the child feels forced to play without experiencing fun. When developing a mobile serious game for children, it is important that there should be a balance between the aspects of work and play to ensure that the game is both fun and effective.

Quality interactions

While playing a game, the only method of communication to and from the game is done via the interactions made available by the application itself. These interactions are the only way that information can be transferred from the player to the game and from the game to the player. For this reason, interactions are critical for the functioning of any application. In order to ensure that this communication is clear and effective, it is necessary that the interactions of an application are of a high quality and comprehensive.

Replayability

Although this element was mentioned in Section 4.3.2 and Table 4.1, it was not deemed as a necessary element to ensure that a game is fun and objectively good. This element was however highlighted by a reviewer as being critical to increase the effectiveness of the mobile serious game. The reason why this element can be seen as critical in this specific context, is because it increases the player's exposure to the content of the game. This increase in exposure will mean that the player is more likely to remember the content and apply it in real life.

It is important to note that the elements in this list was identified by the reviewers and that any overlapping elements will be mentioned in Section 6.4. The five elements identified by the expert reviewers can be considered to be critical elements. Although none of these elements were directly implemented in the game, some of these elements are present in the game in its current state.

6.4 List of identified critical elements

The research question of this study as stated in Section 1.2 reads as follows:

"What critical elements should be implemented into a mobile serious game to effectively promote digital wellness among pre-school children?".

In order to answer this question, critical elements were identified from both literature and via expert review. In Table 6.3 a summary of all identified critical elements is given:

Table 6.3: Identified critical elements.

Game element	**Description**
Structured challenge	Tasks and activities should be presented and scaled to the level of the player (This element is a combination of the "challenge" and "structured challenge" elements)
Fantasy	The game must have an appropriate theme or setting that engages and motivates players.
Choice	Players must be allowed to have sufficient control over their gameplay experience.
Rules	Constraints should be present to give structure to the game and enforce the game's limits.
Competition	Obstacles to achieving the goal must be present for increasing motivation (This element was originally part of the competition and goals element).
Clear and simple goals	The game must have a winning condition that is reachable. The goal should be stated clearly and it should not be too complicated for the player to understand (This element is a combination of the "goals" section of the competition and goals element and the "clear and simple goals" element).
Aesthetics	The game should be visually and audibly appealing to the target audience.
Quality feedback and rewards	A constant loop of feedback and rewards should be used to guide the player to making correct decisions.
Appropriate interface	The game should be playable by the target audience. Design should consider the abilities of the target audience.
Balanced simplicity and complexity	The serious content of the game should be simple enough to be understandable, but still complex enough to engage the player (This element is an adaption of the "simplicity" element, and is based on feedback from the expert reviewers).
Use appropriate material for target group	The content used in the game should be appropriate to the target audience.

Continued on next page

Table 6.3 – Continued from previous page

Game element	Description
Present material in an appropriate way	The game should enable learning in multiple different ways (via listening, observing, exploring, etc.).
Focus on different topics of digital wellness	Different topics should be discussed in the content of the game.
Short playtime	Limit the length of a single play session or round to adapt to the attention span of the player.
Balanced work and play	Maintain a balance between serious and play aspects to ensure that the game does not lose its fun factor.
Quality interactions	All interactions between the player and the game must be meaningful and of a high quality.
Replayability	Ensuring that a game is replayable will motivate players to play multiple times, thereby increasing their exposure to the game content.

This list of elements serves as an answer to the research question given above and satisfies the final secondary objective. It is important to note that the implementation of these elements does not guarantee that an application will be successful, but it can greatly increase the chances of success.

6.5 Summary

In this chapter, the results of the expert review were discussed. In the first section some details of the expert reviewers were briefly discussed. This section mentioned the experience of the reviewers, followed by a brief summary of the experts' view of the level of exposure that children have to cyberspace. The second section was used to summarise the results of the validation process of the serious game as well as of the critical elements identified from literature. This section concluded that the game satisfied all three criteria mentioned in Section 1.2 and that all identified elements can be considered to be critical elements. The next section of this chapter listed five additional critical elements identified by the expert reviewers, followed in the final section by a complete list of all elements identified in this study.

The next chapter concludes the study by answering the research question as stated in Section 1.2. This chapter will also present a reflection on the current study and suggest possible future studies.

Chapter 7

Conclusion

The aim of this study was to identify critical elements that, when implemented in a mobile serious game, will result in a game that effectively spreads awareness of digital wellness among pre-school children. In order to identify these critical elements, several elements were identified from literature and implemented in a mobile serious game. This game was sent to experts in the field of pre-school education for the validation of the elements identified from literature and for the identification of additional elements.

In Chapter 1, the background of the study was given. This chapter included the problems statement, research question, secondary objectives and research design for the study. Chapter 2 provides more background on the dangers of cyberspace and how to defend against them. In Chapter 3 the concept of digital wellness was discussed. This chapter mainly focused on defining digital wellness and discussing digital wellness specifically for children. The topic of serious games was discussed is Chapter 4. This chapter defined serious games, identified optimal elements that can be implemented to produce a good game and elements that can be implemented to make a game appropriate for pre-school children. The mobile serious game that was created was discussed in Chapter 5.3. This discussion highlighted the technologies used and the different elements that were implemented in each scene of the game. Chapter 6 summarised the results received from the expert review. These results validated the elements identified from literature and identified five additional elements.

In this chapter a summary of the study is given and suggestions are made for future work. A brief evaluation of the research goals as mentioned in Section 1.3 is given in Sections 7.1. Next, the contribution of this study to the current body of knowledge is discussed in Section 7.2, followed by a discussion of the limitations of the study in Section 7.3. Finally, the possibilities for further study is discussed in Section 7.4.

7.1 Evaluation of research objectives

In order to answer the research question as stated in Section 1.2, four secondary objectives were set. In this section a brief overview is given on how each objective was met.

1. Identify potential critical elements from existing literature.

The first objective was concerned with identifying critical elements from literature that, when implemented into a mobile serious game, will result in a game that is fun to play, will be appropriate for pre-school children and will spread awareness of digital wellness among users. This objective was reached by doing the literature review (reported in Section 2.5, Section 4.3.2 and Section 4.4.2) and the elements that were found were summarised in Section 5.1. The identification of these elements was fundamental for all further objectives.

2. Develop a mobile serious game that implements the elements identified in literature.

After the identification of the preliminary elements, a mobile serious game implementing these elements was created. The goal of this application was to serve as a proof of concept for the identified and implemented elements. The documentation for this application and the implementation of the different elements were reported in Section 5.3. A link to a playable desktop version of this game can be found in Appendix B.

The development of the game presented a practical demonstration of the application of the elements identified. The game could be used to evaluate the effectiveness of the identified elements and to identify missing elements.

3. Use of expert reviews to validate the elements implemented in the mobile serious game and to identify additional elements.

The third objective required that experts in the field of pre-school education evaluate both the elements identified during the completion of the first objective, and the serious game created during the completion of the second objective.

This objective had two sub-objectives. The first sub-objective was to validate if the elements identified from literature could be considered as critical elements. The reviewers confirmed that all of the elements identified from literature are critical elements and thus, none of the elements are deemed non-critical. The results of the evaluation of the elements identified from literature are summarized in Section 6.2.2.

The second sub-objective was to identify additional critical elements that were not identified during the completion of the first objective. The reviewers were able to identify five additional critical elements. Four of these elements were added to the list of critical elements and one reviewer element was used to modify an element identified from literature. The results of the identification of additional critical elements are summarised in Section 6.3.

The validation of the elements identified from literature added a level of validity to the elements and the additional elements identified by the reviewers contributed to the primary goal of the study.

4. Evaluate and list all of the elements identified from literature and from using expert reviews.

As a final step to reaching the main goal, the fourth objective consisted of a brief evaluation and compilation of the elements identified during the study. In order to accomplish this objective, the results of the expert reviews were used to modify the list of identified elements by making minor adjustments to certain elements and by adding the newly identified elements. The list that was formed as a result of the completion of this objective is given in Table 6.3.

This list of critical elements serves as the answer to the question: "What critical elements should be implemented into a mobile serious game to effectively promote digital wellness among pre-school children?".

7.2 Contributions

This study's main contribution to the current body of knowledge is a successful serious game for preschoolers that has been developed based on principles already proven (using the book by Von Solms and Fischer, 2017). This serious game has been tested and validated using expert opinions.

The secondary contributions of this study are:

1. Relevant information regarding digital wellness and cybersecurity specifically for pre-school children was summarized through a literature study. This summary may serve as a central source for future reference;

2. Several elements from literature regarding optimal game development, applications for children and cybersecurity awareness campaigns were identified and validated; and

3. The content of the book "Digital wellnests" was presented in an interactive medium, extending its reach and effectiveness as a tool for spreading awareness of digital wellness among pre-school children.

7.3 Limitations

Due to ethical constraints, the involvement of pre-school children during the testing and validation phases was not allowed. Although the experts were able to effectively test and validate the application and elements, involving children in this process can lead to a deeper understanding of both the critical elements and the needs of the children. These constraints are considered to be the biggest limitation of the study.

Another obstacle that the study faced was the limited number of experts that were both capable and willing to participate in the expert review. All participants were chosen based on their accessibility and expertise and therefore, only a limited number of individuals were able to participate. A larger group of reviewers would have added greater validity to the results and could have contributed to the identification of additional elements.

The final limitation that this study encountered was the lack of resources for formal testing. One of the core characteristics of design science is iterative design and evaluation phases. Due to the fact that the mobile serious game could only be tested internally, the number of iterations during the development phase was limited.

7.4 Future work

This study was conducted as a foundation for future work. The main goal of this study was to identify critical elements that will be used in future work to create mobile serious games that will promote digital wellness among pre-school children.

The future work could consist of the development of a full game that will be made available as a supplementary resource for parents and teachers. This game could contain all of the poems, concepts and messages that are portrayed in the book “Digital wellnests”.

Future studies may consider focusing on both the development and deployment of this mobile serious game. The effectiveness of this game can be compared to that of other, traditional methods of spreading awareness in order to validate if a mobile serious game is an effective tool to spread awareness of digital wellness among pre-school children.

Future studies may also consider streamlining the development of the game by including additional help with development and visuals and by employing iterative design. The development of a mobile serious game that is largely reliant on visual and audible interactions is a big endeavour and the development phase will benefit from multiple iterative design phases.

The validation of both the game and critical elements could be done by a more diverse group of experts from different, but relevant, fields (pre-school teachers, child psychologists, application developers etc.) and by observing

pre-school children while playing. The knowledge gained from observing the children playing the game could lead to a better insight of the needs of the children.

7.5 Summary

This study investigated the following question: "What critical elements should be implemented into a mobile serious game to effectively promote digital wellness among pre-school children?". As an answer to this question, this study identified seventeen different elements by examining existing literature, creating an application which incorporated these elements, and conducted an expert review by six experts in the field of pre-school education.

This study serves as a foundation for developing and deploying a complete mobile serious game that promotes digital wellness among pre-school children. The critical elements identified in this study will be implemented in the mobile serious game, to ensure that the game is objectively good or fun to play, appropriate for pre-school children and spreads awareness of digital wellness among them.

Bibliography

Abomhara, M., & Køien, G. M. (2015). Cyber security and the internet of things: Vulnerabilities, threats, intruders and attacks. *Journal of Cyber Security and Mobility*, *4*(1), 65–88.

Ajzen, I. (2002). Perceived behavioral control, self-efficacy, locus of control, and the theory of planned behavior. *Journal of Applied Social Psychology*, *32*(4), 665–683.

Alvarez, J., & Djaouti, D. (2011). Design science in information systems research. *Proceedings of the Serious Games & Simulation Workshop*, 10–15.

Andersen, T. R. (2019). Cyberspace Revisited: A Radial Reading of William Gibson's "Burning Chrome". *The Journal of American Culture*, *42*(2), 121–136.

Asgari, M., & Kaufman, D. (2009). Motivation, Learning, and Game Design. *Handbook of research on effective electronic gaming in education* (pp. 1166–1182).

Australian Department of Broadband Communications and the Digital Economy. (2011). Budd:e.

Bada, M., & Nurse, J. R. (2019). The social and psychological impact of cyber-attacks.

Bada, M., Sasse, A. M., & Nurse, J. R. C. (2015). Cyber Security Awareness Campaigns: Why do they fail to change behaviour? *International Conference on Cyber Security for Sustainable Society*, 118–131.

Balvin, N., & Tyler, M. C. (2006). Emotions in cyberspace: The advantages and disadvantages of online communication. *Organisational Psychologist*, *2007*(277), 5–8.

Beard, K. W., & Wolf, E. M. (2001). Modification in the Proposed Diagnostic Criteria for Internet Addiction. *CyberPsychology & Behavior*, *4*(3), 377–383.

Benedikt, M. (1991). *Introduction to cyberspace: First steps*. MIT Press.

Berrios Rolon, M. M. (2014). *A quantitative study to explore the relationship between technostress symptoms and technostress among Puerto Rican university students* (Doctoral dissertation). Capella University.

Bertino, E., Martino, L., Paci, F., & Squicciarini, A. (2010). *Security for Web Services and Service-Oriented Architectures*. Springer Berlin Heidelberg.

Brauch, H. G. B. (2011). *Coping with Global Environmental Change, Disasters and Security*. Springer International Publishing.

Brigham, T. J. (2015). An Introduction to Gamification: Adding Game Elements for Engagement. *Medical Reference Services Quarterly*, *34*(4), 471–480.

Brod, C. (1984). *Technostress: The human cost of the computer revolution*. Reading, Mass.: Addison-Wesley.

Burghardt, G. (2011). Defining and Recognizing Play. *The oxford handbook of the development of play* (pp. 9–18).

Burghardt, G. M. (2005). *The genesis of animal play: Testing the limits*. Mit Press.

Callaghan, M. N., & Reich, S. M. (2018). Learning, Media and Technology Are educational preschool apps designed to teach? An analysis of the app market. *An analysis of the app market, Learning, Media and Technology*, *43*(3), 280–293.

Caplan, S. E. (2002). Problematic Internet use and psychosocial well-being: Development of a theory-based cognitive-behavioral measurement instrument. *Computers in Human Behavior*, *18*(5), 553–575.

Carnegie Mellon University. (2011). The Carnegie Cyber Academy - An Online Safety site and Games for Kids.

Charsky, D. (2010). From edutainment to serious games: A change in the use of game characteristics.

Cheung, C. S.-S., & Pomerantz, E. M. (2015). Value development underlies the benefits of parents' involvement in children's learning: A longitudinal investigation in the United States and China. *Journal of Educational Psychology*, *107*(1), 309–320.

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

Costigan, S. A., Barnett, L., Plotnikoff, R. C., & Lubans, D. R. (2013). The Health Indicators Associated With Screen-Based Sedentary Behavior Among Adolescent Girls: A Systematic Review. *Journal of Adolescent Health*, *52*(4), 382–392.

Cowley, B., Charles, D., Black, M., & Hickey, R. (2008). Toward an understanding of flow in video games. *Computers in Entertainment*, *6*(2), 1–27.

Davis, R. A., Flett, G. L., & Besser, A. (2002). Validation of a new scale for measuring problematic internet use: Implications for pre-employment screening. *Cyberpsychology and Behavior*, *5*(4), 331–345.

Deterding, S., Dixon, D., Khaled, R., & Nacke, L. (2011). From game design elements to gamefulness: Defining "gamification". *Proceedings of the 15th International Academic MindTrek Conference: Envisioning Future Media Environments, MindTrek 2011*, 9–15.

Dhillon, G. (2007). *Principles of information systems security: Texts and cases*. John Wiley & Sons Incorporated.

Dibbell, J. (2011). *Serious games*. Springer International Publishing.

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for information security management. *Journal of Information Security*, *4*(1), 92–100.

Djaouti, D., Alvarez, J., & Jessel, J.-P. (2011). Classifying Serious Games: The G/P/S Model. *In handbook of research on improving learning and motivation through educational games: Multidisciplinary approaches* (pp. 118–136).

Dörner, R., Göbel, S., Effelsberg, W., & Wiemeyer, J. (2016). *Serious Games.* Springer.

Eberle, S. G. (2014). The elements of play: Toward a philosophy and a definition of play. *American Journal of Play*, *6*(2), 214–233.

FBI. (n.d.). FBI — Cyber Task Forces.

Fischer, R., & Von Solms, S. (2016). *Digital wellnests*. ACEIE.

Gandhi, R., Sharma, A., Mahoney, W., Sousan, W., Zhu, Q., & Laplante, P. (2011). Dimensions of cyber-attacks: Cultural, social, economic, and political. *IEEE Technology and Society Magazine*, *30*(1), 28–38.

Garvey, C., & Lloyd, B. (1990). *Play*. Harvard University Press.

Gendreau, R. (2007). The new techno culture in the workplace and at home. *Journal of American Academy of Business*, *11*(2), 191–196.

Google. (2019). Be internet awesome: Google Digital Literacy and Citizenship Curriculum.

Grassi, P. A., Fenton, J. L., Newton, E. M., Perlner, R. A., Regenscheid, A. R., Burr, W. E., Richer, J. P., Lefkovitz, N. B., Danker, J. M., Choong, Y.-Y., Greene, K. K., & Theofanos, M. F. (2017). *Digital identity guidelines: authentication and lifecycle management* (tech. rep.). National Institute of Standards and Technology. Gaithersburg, MD.

Halpert, B. (2014). Kids – Savvy Cyber Kids.

Hamm, M. P., Newton, A. S., Chisholm, A., Shulhan, J., Milne, A., Sundar, P., Ennis, H., Scott, S. D., & Hartling, L. (2015). Prevalence and effect of cyberbullying on children and young people: A scoping review of social media studies. *JAMA Pediatrics*, *169*(8), 770–777.

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly: Management Information Systems*, *28*(1), 75–105.

Hinduja, S., & Patchin, J. W. (2010). Archives of Suicide Research Bullying, Cyberbullying, and Suicide. *Archives of Suicide Research*, *14*(3), 206–221.

Hoff, D. L., & Mitchell, S. N. (2009). Cyberbullying: causes, effects, and remedies. *Journal of educational administration*, *47*(5), 652–665.

Huizinga, J. (1938). *Homo Ludens*. Routledge.

Hunicke, R., Leblanc, M., & Zubek, R. (2004). MDA: A formal approach to game design and game research. *AAAI Workshop - Technical Report*, *WS-04-04*, 1–5.

Kawulich, B. (2001). Selecting a research approach: paradigm, methodology and methods. *Doing social research: A global context* (pp. 1–21).

Király, O., Potenza, M. N., Stein, D. J., King, D. L., Hodgins, D. C., Saunders, J. B., Griffiths, M. D., Gjoneska, B., Billieux, J., Brand, M., Abbott, M. W., Chamberlain, S. R., Corazza, O., Burkauskas, J., Sales, C. M., Montag, C., Lochner, C., Grünblatt, E., Wegmann, E., … Demetrovics, Z. (2020). Preventing problematic internet use during the COVID-19 pandemic: Consensus guidance. *Comprehensive Psychiatry*, *100*(1), 152180.

Kirlappos, I., Parkin, S., & Sasse, M. A. (2014). Learning from "Shadow Security:" Why Understanding Non-Compliant Behaviors Provides the Basis for Effective Security. *Workshop on Usable Security*, 1–10.

Kirwan, G., & Power, A. (2012). *The Psychology of Cyber Crime*. IGI Global.

Kissel, R. (2013). Glossary of Key Information Security Terms. *NIST IR*, (Revision 2), 222.

Klopfer, E., Osterweil, S., & Salen, K. (2009). Moving Learning Games Forward - obstacles, opportunities & openness. *Flora*, *3*(December), 1–56.

Kramer, W. (2000). What makes a game good. *Game & Puzzle Design*, *1*(2), 84–86.

Kryger, J. L., & Mathias. (n.d.). The (Re)invention of Cyberspace.

Kumar, V., Srivastava, J., & Lazarevic, A. (2005). *Managing Cyber Threats: Issues, Approaches, and Challenges - Google Books*. Springer International Publishing.

Latour, B. (2002). Morality and Technology The End of the Means. *Theory, Culture & Society 2002*, *19*(5), 247–260.

Lin, L. (2009). Breadth-biased versus focused cognitive control in media multitasking behaviors.

Lubans, D., Lonsdale, C., Plotnikoff, R., Smith, J., Dally, K., & Morgan, P. (2013). Development and evaluation of the Motivation to Limit Screen-time Questionnaire (MLSQ) for adolescents. *Preventive Medicine*, *57*(5), 561–566.

Malone, T. W., & Lepper, M. R. (1987). Making learning fun: A taxonomy of intrinsic motivations for learning. *Conative and affective process analyses* (pp. 223–253).

Malone, T. W. (1981). Toward a theory of intrinsically motivating instruction. *Cognitive Science*, *5*(4), 333–369.

Matallaoui, A., Hanner, N., & Zarnekow, R. (2017). Introduction to Gamification: Foundation and Underlying Theories. *Introduction to gamification: Foundation and underlying theories* (pp. 3–18).

Matthews, D., Lieven, E., & Tomasello, M. (2007). How toddlers and preschoolers learn to uniquely identify referents for others: A training study. *Child Development*, *78*(6), 1744–1759.

McCall, R. B., Groark, C. J., Hawk, B. N., Julian, M. M., Merz, E. C., Rosas, J. M., Muhamedrahimov, R. J., Palmov, O. I., & Nikiforova, N. V. (2019). Early Caregiver–Child Interaction and Children's Development: Lessons from the St. Petersburg-USA Orphanage Intervention Research Project.

McMahon, C., & Aiken, M. (2015). Introducing digital wellness: Bringing cyberpsychological balance to healthcare and information technology. *Proceedings - 15th IEEE International Conference on Computer and Information Technology, CIT 2015, 14th IEEE International Conference on Ubiquitous Computing and Communications, IUCC 2015, 13th IEEE International Conference on Dependable, Autonomic and Se*, *2015*(October 2015), 1417–1422.

McPherson, S. S. (2009). *Tim Berners-Lee: Inventor of the World Wide Web*. Twenty-First Century Books.

Merlo, L. J., Stone, A. M., & Bibbey, A. (2013). Measuring Problematic Mobile Phone Use: Development and Preliminary Psychometric Properties of the PUMP Scale. *Journal of Addiction*, *2013*(1), 1–7.

Mildner, P., Stamer, N., & Effelsberg, W. (2015). From game characteristics to effective learning games evaluation of a component-based quiz game. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 51–62.

Mitgutsch, K., & Alvarado, N. (2012). Purposeful by design?: A serious game design assessment framework. *Foundations of Digital Games 2012, FDG 2012 - Conference Program*, 121–128.

Modic, D., & Anderson, R. (2015). It's All Over but the Crying: The Emotional and Financial Impact of Internet Fraud. *IEEE Security and Privacy*, *13*(5), 99–103.

Nakatsu, R., Rauterberg, M., & Ciancarini, P. (2015). *Handbook of Digital Games and Entertainment Technologies*. Springer International Publishing.

Ning, H., Ye, X., Bouras, M. A., Wei, D., & Daneshmand, M. (2018). General Cyberspace: Cyberspace and Cyber-Enabled Spaces. *IEEE Internet of Things Journal*, *5*(3), 1843–1856.

Nurse, J. R. C., & Nurse, J. R. C. (2019). Cybercrime and You: How Criminals Attack and the Human Factors That They Seek to Exploit. *The oxford handbook of cyberpsychology* (pp. 662–690).

Ophir, E., Nass, C., & Wagner, A. D. (2009). Cognitive control in media multitaskers. *Proceedings of the National Academy of Sciences of the United States of America*, *106*(37), 15583–15587.

Ostrovsky, A. (2014). *From Promoting Awareness to Embedding Behaviours* (tech. rep.). Information Security Forum.

Ottis, R. (2011). *A Systematic Approach to Offensive Volunteer Cyber Militia* (Doctoral dissertation). Tallinn university of technology.

Padmavathi, D. G., & Shanmugapriya, M. D. (2009). A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks. *International Journal of Computer Science and Information Security*, *4*(1), 1–9.

Parker, D. (2015). Toward a New Framework for Information Security? *Computer security handbook*, *3*(1), 31–34.

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. *Computers and Security*, *66*(1), 40–51.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers and Security*, *42*(1), 165–176.

PBS - NOVA labs. (n.d.). Cybersecurity Labs.

Pellis, S., & Pellis, V. (2013). *The playful brain: venturing to the limits of neuroscience*. Oneworld Publications.

Phyfer, J., Burton, P., & Leoschut, L. (2016). *South African Kids Online : A glimpse into children's internet use and online activities.* (tech. rep.). UNICEF.

Piaget, J. (2013). *Play, dreams and imitation in childhood*. Routledge.

Ragu-Nathan, T. S., Tarafdar, M., Ragu-Nathan, B. S., & Tu, Q. (2008). The consequences of technostress for end users in organizations: Conceptual development and validation. *Information Systems Research*, *19*(4), 417–433.

Rainer, R. K., & Cegielski, C. G. (2010). *Introduction to Information Systems, Supporting & Transforming Business*. John Wiley & Sons, Inc.

Raisingchildren.net.au. (n.d.). How children learn: learning at 0-5 years — Raising Children Network.

Ramlakhan, N. E. (2011). Ethical Implications of Third-party Cookies. *International Journal of the Humanities*, *9*(1), 59–68.

Raza, M., Iqbal, M., Sharif, M., & Haider, W. (2012). A survey of password attacks and comparative analysis on methods for secure authentication. *World Applied Sciences Journal*, *19*(4), 439–444.

Ritchie, R. (2013). *Primary Design and Technology: A Process for Learning*. Routledge.

Ritterfeld, U., Cody, M., & Vorderer, P. (2009). *Serious games: Mechanisms and effects*. Routledge.

Roquet, C. D., & Sas, C. (2019). Digital Wellbeing: Evaluating Mandala Coloring Apps. *CHI Conference on Human Factors in Computing Systems*, 9–12.

Rose, E. (2014). "Would you ever say that to me in class?": Exploring the Implications of Disinhibition for Relationality in Online Teaching and Learning. *Proceedings of the 9th International Conference on Information Technology, ITNG 2014*, *9*, 253–260.

Royal, C. W., Wasik, S. Z., Horne, R., Dames, L. S., & Newsome, G. A. (2017). Digital Wellness: Integrating Wellness in Everyday Life with Digital Content and Learning Technologies. *Handbook of Research on Transformative Digital Content and Learning Technologies*, 103–118.

Schutten, D., Stokes, K. A., & Arnell, K. M. (2017). I want to media multitask and I want to do it now: Individual differences in media multitasking predict delay of gratification and system-1 thinking. *Cognitive Research: Principles and Implications*, *2*(1), 8.

Sheldon, J. B. (2012). State of the Art Attackers and Targets in Cyber 2012. *Journal of Military and Strategic Studies*, *14*(2), 1–19.

Shuler, C., Levine, Z., & Ree, J. (2012). iLearn II: An analysis of the education category of Apple's app store. *Joan Ganz Cooney Center*, *2*(January), 1–32.

Sigman, A. (2012). Time for a view on screen time. *Archives of Disease in Childhood*, *97*(11), 935–942.

Smith, P., Mahdavi, J., Carvalho, M., & Tippett, N. (2006). *An investigation into cyberbullying, its forms, awareness and impact, and the relationship between age and gender in cyberbullying* (tech. rep.). Unit for School and Family Studies, Goldsmiths College, University of London.

South African Broadcasting Corporation, & The Henry J. Kaiser Family Foundation. (2007). *Young South Africans, broadcast media, and HIV/AIDS awareness: results of a national survey* (tech. rep.). n.a.

Stenros, J. (2016). The Game Definition Game: A Review. *Games and Culture*, *12*(6), 499–520.

Stolterman, E., & Fors, A. C. (2004). Information technology and the good life. *IFIP Advances in Information and Communication Technology*, 687–692.

Suler, J. (2005). The online disinhibition effect. *International Journal of Applied Psychoanalytic Studies*, *2*(2), 184–188.

Swan, M. (1995). *Practical English Usage*. Oxford University Press.

Tarafdar, M., Tu, Q., Ragu-Nathan, B. S., & Ragu-Nathan, T. S. (2007). The impact of technostress on role stress and productivity. *Journal of Management Information Systems*, *24*(1), 301–328.

Teymourlouei, H. (2015). Quick Reference : Cyber Attacks Awareness and Prevention Method for Home Users. *International Journal of Computer, Electrical, Automation, Control and Information Engineering*, *9*(3), 480–486.

Thatcher, A., Wretschko, G., & Fridjhon, P. (2008). Online flow experiences, problematic Internet use and Internet procrastination. *Computers in Human Behavior*, *24*(5), 2236–2254.

Timmermans, B., & Cleeremans, A. (2015). How can we measure awareness? An overview of current methods. *Behavioral methods in consciousness research* (pp. 21–46).

Tremblay, M. S., LeBlanc, A. G., Kho, M. E., Saunders, T. J., Larouche, R., Colley, R. C., Goldfield, G., & Connor, S. G. (2011). Systematic review of sedentary behaviour and health indicators in school-aged children and youth. *International Journal of Behavioral Nutrition and Physical Activity*, *8*(98), 1–22.

Uncapher, M. R., & Wagner, A. D. (2018). Minds and brains of media multitaskers: Current findings and future directions. *Proceedings of the National Academy of Sciences of the United States of America*, *115*(40), 9889–9896.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers and Security*, *38*(38), 97–102.

Von Solms, S., & Fischer, R. (2017). Digital Wellness : Concepts of Cybersecurity Presented Visually for Children. *Proceedings of the Eleventh International Symposium on Human Aspects of Information Security & Assurance (HAISA 2017) Digital*, *11*, 156–166.

Wang, K., Shu, Q., & Tu, Q. (2008). Technostress under different organizational environments: An empirical investigation. *Computers in Human Behavior*, *24*(6), 3002–3013.

Whitman, M. E., & Mattord, H. J. (2017). *Principles of information security*. Cengage Learning.

Yan, Z., Guo, X., Lee, M. K., & Vogel, D. R. (2013). A conceptual model of technology features and technostress in telemedicine communication. *Information Technology & People*, *26*(3), 283–297.

Yogman, M., Garner, A., Hutchinson, J., Hirsh-Pasek, K., & Golinkoff, R. M. (2018). The Power of Play: A Pediatric Role in Enhancing Development in Young Children. *Pediatrics*, *142*(3), e20182058.

Appendix A

Questionnaire

This is the questionnaire that was used to conduct the expert review.

Digital wellnests - Expert review

Thank you very much for agreeing to participate in this expert review. I am Johann Allers and I am currently studying to complete my Masters degree in Computer Science at the North-West University. The goal of my study is to promote digital wellness among preschool children, as well as their parents.

With the increase of the popularity of mobile technologies, children are exposed to cyberspace and the internet at a very young age. Many of these children do not know of the dangers of cyberspace and how to protect themselves against these threats. This can have a negative effect on a child's digital wellness.

Digital wellness refers to a person's well-being with regard to information technologies. This means that digital wellness is not only concerned with threats to one's digital assets, but also the person's physical and mental health. This means that digital wellness is not only focused on threats such as viruses and hackers, but also topics such as cyber bullying and limiting one's screen time.

In an attempt to spread awareness of digital wellness among preschool children, Rachel Fischer & Sune von Solms created the book: "Digital Wellnests" (https://www.cybersecurityhub.gov.za/cyberawareness/images/Booklets/boek-9-a4wire-landscape-kleur-bind-kort-kant_final.zp95232.pdf). This book contains different poems and messages to teach both parents and their children how to maintain good digital wellness. The content of this book was used to create a mobile game that further extends the effectiveness of the book.

The application as provided is not a full game, but rather a proof of concept, combining multiple elements to provide an experience that will highlight important safety measures to ensure digital wellness. In a full version of this game, all of the poems and messages of the "Digital Wellnests" book would be included, with extra language features, interactive games and quizzes. I thus ask that you take into consideration that the game, as presented, is only meant as a demonstration of future work and development.

All the personal information in this review is confidential and will not be made available to the public. Information such as the name, surname and preschool name will only be used to prevent duplicate entries.

* Required

1. Name and Surname *

2. School name *

3. What is your role in the above mentioned school? *

4. How many years of experience do you have working with children? *

5. What age group/s do you work with? *

6. I hereby agree to participate in the review of the application and permit the use of the information I provide *

Check all that apply.

☐ Yes

Expert view on the problem

This section is used to get your opinion and experience with the given problem

7. How aware are you of the different threats and dangers of cyberspace and digital technologies? *

Mark only one oval.

	1	2	3	4	5	
Not aware	◯	◯	◯	◯	◯	Very aware

8. In your experience, how much exposure do preschool children have to digital and online technologies? *

Mark only one oval.

	1	2	3	4	5	
Too little	◯	◯	◯	◯	◯	Too much

9. Do you view this level of exposure as a potential problem? *

Mark only one oval.

- ◯ Yes
- ◯ No
- ◯ Maybe

10. Please motivate your previous answer *

11. Are you aware of any resources that promote digital wellness or cyber security among preschool children? *

Mark only one oval.

- ◯ Yes
- ◯ No

12. Do you use any resources to promote digital wellness or cyber security among preschool children? *

Mark only one oval.

- ◯ Yes
- ◯ No

13. Please list these resources (if any)

_____

_____

_____

_____

_____

14. How aware do you think the parents of preschool children are of the dangers of cyberspace and digital technologies? *

Mark only one oval.

	1	2	3	4	5	
Not aware	◯	◯	◯	◯	◯	Fully aware

15. In your opinion, how effectively do parent teach their preschool children about the dangers of cyberspace? *

Mark only one oval.

	1	2	3	4	5	
Not effectively	◯	◯	◯	◯	◯	Very effectively

Application scoring

This section is used to rate the different elements and experience of the game

16. Is the difficulty level of the application fit for preschool children? *

Mark only one oval.

	1	2	3	4	5	
Not fitting	◯	◯	◯	◯	◯	Fitting

17. Is the application too easy or too difficult (if previous answer is not 4 or 5)?

Mark only one oval.

◯ Too easy
◯ Too difficult

18. How fitting is the presented animal theme for preschool children? *

Mark only one oval.

	1	2	3	4	5	
Not fitting	◯	◯	◯	◯	◯	Fitting

19. Does the application provide the player with enough choices? *

Mark only one oval.

	1	2	3	4	5	
Not enough	◯	◯	◯	◯	◯	Enough

20. How clear are the rules and goals presented? *

Mark only one oval.

	1	2	3	4	5	
Not clear	◯	◯	◯	◯	◯	Very clear

21. How effective do think the level selection of the games are for creating a structured challenge based on the player's abilities? *

Mark only one oval.

	1	2	3	4	5	
Not effective	◯	◯	◯	◯	◯	Very effective

22. How aesthetically pleasing did you find the application? *

Mark only one oval.

	1	2	3	4	5	
Not aesthetically pleasing	◯	◯	◯	◯	◯	Very aesthetically pleasing

23. How fitting do you think the interface and interaction is for preschool children? *

Mark only one oval.

	1	2	3	4	5	
Not fitting	◯	◯	◯	◯	◯	Very fitting

24. How would you rate the quality of feedback and rewards of the application? *

Mark only one oval.

	1	2	3	4	5	
Very bad	◯	◯	◯	◯	◯	Very good

25. How fitting is the level of simplicity of the content?

Mark only one oval.

	1	2	3	4	5	
Not fitting	◯	◯	◯	◯	◯	Very fitting

26. How appropriate is the content of the game for children?

Mark only one oval.

	1	2	3	4	5	
Not appropriate	◯	◯	◯	◯	◯	Very appropriate

27. How sufficient is the amount of topics covered by the game?

Mark only one oval.

	1	2	3	4	5	
Not sufficient	◯	◯	◯	◯	◯	Sufficient

28. How enjoyable do you think preschool children will find this application? *

Mark only one oval.

	1	2	3	4	5	
Not enjoyable	◯	◯	◯	◯	◯	Very enjoyable

29. How suitable is the game for pre-school children?

Mark only one oval.

	1	2	3	4	5	
Not suitable	◯	◯	◯	◯	◯	Very suitable

30. How effective do you think this application will be in spreading awareness of digital wellness among preschool children? *

Mark only one oval.

	1	2	3	4	5	
Not effective	◯	◯	◯	◯	◯	Very effective

Application comments

This section is used to get any further comments about the game. Any and all feedback will be greatly appreciated. Please use this section to express your feelings

regarding the game.

31. Which elements did you like the most in the application? (Pick up to 3) *

Check all that apply.

- [ ] Challenge
- [ ] Fantasy
- [ ] Choice
- [ ] Rules
- [ ] Competion and goals
- [ ] Aestetics
- [ ] Clear and simple goal
- [ ] Feedback and rewards
- [ ] Structured challenge
- [ ] Appropriate interface
- [ ] Simplicity
- [ ] Appropriate content
- [ ] Focusing on different topics
- [ ] Present material in an appropriate way

32. In your opinion, which elements are most important to the success of the game? (Pick up to 3) *

Check all that apply.

- [ ] Challenge
- [ ] Fantasy
- [ ] Choice
- [ ] Rules
- [ ] Competion and goals
- [ ] Aestetics
- [ ] Clear and simple goal
- [ ] Feedback and rewards
- [ ] Structured challenge
- [ ] Appropriate interface
- [ ] Simplicity
- [ ] Appropriate content
- [ ] Focusing on different topics
- [ ] Present material in an appropriate way

33. Which elements did you feel were missing or neglected? (Pick up to 3) *

Check all that apply.

- [ ] Challenge
- [ ] Fantasy
- [ ] Choice
- [ ] Rules
- [ ] Competion and goals
- [ ] Aestetics
- [ ] Clear and simple goal
- [ ] Feedback and rewards
- [ ] Structured challenge
- [ ] Appropriate interface
- [ ] Simplicity
- [ ] Appropriate content
- [ ] Focusing on different topics
- [ ] Present material in an appropriate way

34. Which elements did you feel were not critical to the success of the game? (Pick up to 3) *

Check all that apply.

- [ ] Challenge
- [ ] Fantasy
- [ ] Choice
- [ ] Rules
- [ ] Competion and goals
- [ ] Aestetics
- [ ] Clear and simple goal
- [ ] Feedback and rewards
- [ ] Structured challenge
- [ ] Appropriate interface
- [ ] Simplicity
- [ ] Appropriate content
- [ ] Focusing on different topics
- [ ] Present material in an appropriate way

35. What suggestions do you have to further develop the application? *

36. Comments and critique

Appendix B

Download instructions

The following link can be used to download a playable desktop version of the Digital wellnests game: https://cutt.ly/hhFtnG7

Instructions

1. Download the DigitalWellnests folder on the link given above.
2. Unzip and store the folder in a memorable location on the computer.
3. Open the downloaded folder.
4. Double click on the DigitalWellnests.exe file. The game should run in a few seconds.

If the DigitalWellnests.exe file does not exist in the DigitalWellnests folder after downloading, the DigitalWellnests folder should be whitelisted in the computer's anti-malware program. If the program cannot run, repeat the steps with the DigitalWellnestsx32.zip folder located using the same link.