Master's thesis

NTNU
Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Department of Computer Science

Rolf Erik Sesseng Aas
Sigurd Røstad Augdal

Raising cybersecurity awareness among children and parents using gamification

Master's thesis in Computer Science
Supervisor: Maria Letizia Jaccheri
Co-supervisor: Farzana Quayyum
July 2022

NTNU
Norwegian University of
Science and Technology

Rolf Erik Sesseng Aas
Sigurd Røstad Augdal

Raising cybersecurity awareness among children and parents using gamification

Master's thesis in Computer Science
Supervisor: Maria Letizia Jaccheri
Co-supervisor: Farzana Quayyum
July 2022

Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Department of Computer Science

NTNU
Norwegian University of
Science and Technology

Abstract

As more and more of people's daily life revolves around being online, the need to be aware of the risks one is exposed to is more important than ever. Through their inexperience and naiveté, the younger generations are at a higher risk of experiencing harassment and crime online. Therefore, adults have to raise awareness regarding cybersecurity risks from an early age, such that their children can grow up to become safe online. However, research has shown that adults have limited knowledge on cybersecurity threats themselves. This knowledge gap needs to be addressed, and this thesis will explore the potential game-based learning has regarding cybersecurity awareness. By using a Systematic literature review (SLR) as a foundation, we conducted expert interviews and a workshop. Then we planned and developed a working prototype of a cooperative game between children and parents. User testing with seven participants shows that all participants enjoyed playing the prototype, and the majority enjoyed the cooperative aspect. All participants also wanted to play the game again if more features, levels, and challenges are added. Furthermore, the user test displays an increase in cybersecurity knowledge and awareness among the children.

Keywords: *Cybersecurity, children, parents, family, game, game based learning*

Sammendrag

Ettersom mer og mer av vår moderne hverdag omhandler det å være på internett til enhver tid, er det viktigere enn noen gang å være oppmerksom på truslene som finnes på internett. Den yngre generasjonen, med sin naivitet og uerfarenhet, er spesielt utsatt for trakkasering og kriminelle handlinger på nett. For at barna skal kunne vokse opp til å bli trygge på nettet, må vi voksne gå inn for å øke oppmerksomheten og kunnskapen rundt risikoene fra en tidlig alder av. Forskning viser imidlertid at mange voksne har begrenset med kunnskap om denne typen trusler. For å angripe denne problematikken er det et behov for å øke kunnskapsnivået til de voksne. Denne masteroppgaven utforsker potensialet til spillbasert læring med tanke på trygghet på internett. En systematisk kunnskapsoversikt ble brukt som grunnlag, og sammen med ekspertintervjuer og en workshop, planla og utviklet vi en fungerende prototype av et samarbeidspill for barn og foreldre. Innledende brukertester viser at samtlige deltakere satte pris på å prøve spillet, og flesteparten like samarbeidsaspektet. Samtlige ønsket å prøve spillet igjen dersom det hadde blitt utvidet med flere nivåer, utfordringer og funksjoner. Brukertesten viste også en økning i kunnskap og oppmerksomhet rundt nettvett hos barn.

Nøkkelord: *Cybersikkerhet, barn, foreldre, familie, spill, spillbasert læring*

Acknowledgements

Thank you to our amazing co-supervisor Farzana for all your support, hard work and helpful feedback throughout the year. Your organisation skills, thoroughness and attention to detail has helped us getting this thesis finished in time.

We would also like to thank Professor Letizia Jaccheri for her guidance, insights, support, encouragements and invaluable feedback throughout the process.

Furthermore, we would like to express our gratitude to the Software for a better society group, as their insights and discussions has been a big help for us during this process.

Also, all participants and interviewees have our thanks for taking their time to contribute to our research.

Thanks to our employer for letting us use a lot of time on our thesis while still keeping us employed.

Thank you to ***Zotero*** and ***Overleaf*** for being awesome pieces of software, easy to use, and free, making our jobs less difficult.

Lastly, we are eternally grateful for the unreserved support we have received from our better halves, who have endured our absence and lack of focus for greater parts of the last 12 months. Thank you!

Preface

The following master thesis was written during the spring semester of 2022 under the supervision of Professor Letizia Jaccheri and co-supervisor PhD. candidate Farzana Quayyum at the Department of Computer Science at the Norwegian University of Science and Technology (NTNU). The master thesis was a part of the *TDT4900 - Computer Science, Master's Thesis* course.

Contents

Figures

Tables

Code Listings

Acronyms

ARCS Attention, Relevance, Confidence, Satisfaction. 11, 26, 31, 77

ATMSG Activity Theory Model for Serious Games. 12

BRT Bloom's Revised Taxonomy. 12

BYOD Bring Your Own Device. 22, 63

CAPEC Common Attack Pattern Enumeration and Classification. 12

CCI Child Computer Interaction. 20, 21, 23, 25, 83

CD/CI Continuous Delivery/Continuous Integration. 46, 47, 53

CKC Cyber Kill Chain. 12

COFELET Conceptual Framework for e-Learning and Training. 12

FPS First-person shooter. 13

GUI Graphical User Interface. 16

HCI Human Computer Interaction. 20, 21, 23, 25, 83

LCMS Learning Content Management System. 12

NCWF National Cybersecurity Workforce Framework. 12

NSD Norwegian Centre for Research Data. 19, 23

PMT Protection Motivation Theory. 16

RDBMS Relational Database Management System. 48, 50

RPG Role-playing game. 13

RQs Research questions. 3, 9, 10, 76

SLR Systematic literature review. iii, xv, xvii, 1–3, 9–11, 17, 19–21, 28, 32, 36, 45, 77, 83, 92

SQL Structured Query Language. 48

UN United Nations. 1

Chapter 1

Introduction

Since its initial creation, the World Wide Web has seen a tremendous growth in popularity, especially since the rise of social networks in the mid 2000s. As seen in Figure 1.1 the use of the Internet has steadily grown across the globe, and younger and younger audiences are accessing it daily[1]. The United Nations (UN) stated in 2020 that "*digital technologies have profoundly transformed society. They offer unprecedented opportunities and new challenges*"[2], and some of these challenges are the cybersecurity risks the younger generation face when they venture online.

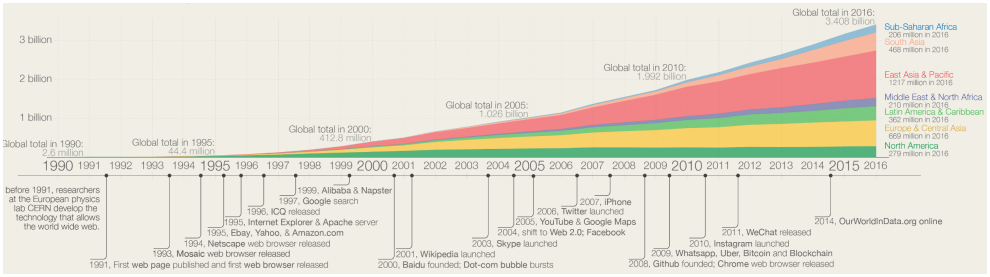


Figure 1.1: Total number of people using the Internet[3]

As more and more of our daily life revolves around being online at all times, more and more people with less honourable intentions does too. As such, it is vital that the general populous gain enough knowledge and know-how on how to spot, deter and deflect these bad actors. Children, as with other aspects of life, are especially vulnerable towards cybersecurity risks. Be it because of their limited experience or naivete, it is of the utmost importance that the older generations take action and work to enhance the children's cybersecurity awareness. This importance is stated in the Declaration on the Commemoration of the Seventy-fifth Anniversary of The United Nations: "*We must ensure safe and affordable digital access for all*"[2].

In 2021, Quayyum *et al.* [4] conducted an SLR outlining the current research into which cybersecurity risks children are exposed to, and how this is

being addressed. Furthermore, they looked at which approaches has been used to raise cybersecurity awareness, and how researchers have evaluated the cybersecurity awareness approaches for children. They found that there are several risks the younger generation faces online. Among these risks are: invasion of privacy, online harassment and content-related dangers. There lacked insight and research on other risks such as stranger danger. It is evident that the younger generation face these risks daily.

Moreover, Chigada and Madzinga [5] conducted an SLR that researched how the COVID-19 pandemic affected cyber attacks and threats. Businesses did not have the proper security routines and -measures in place such that employees could securely connect to their workplace remotely. They state that the number of cyber attacks and threats grew at an exponential rate during the pandemic, and there was no sign of stopping as of the time of writing the report.

Combining the above increase in cyber threats and lack of solutions for raising the cybersecurity awareness of children with the fact that humans are the weakest link in the security pipeline[6], the need for proper cybersecurity awareness training is evident. As such we see the dire need for applications and solution to battle this problem.

To be able to raise the awareness around cybersecurity in a younger audience one has to meet the children where they are already comfortable. As depicted in Figure 1.2 over 75% of children between 9 and 18 years old play video games on a regular basis. As such, using a game-based approach for raising cybersecurity awareness makes it possible to reach out to a larger part of the target audience.

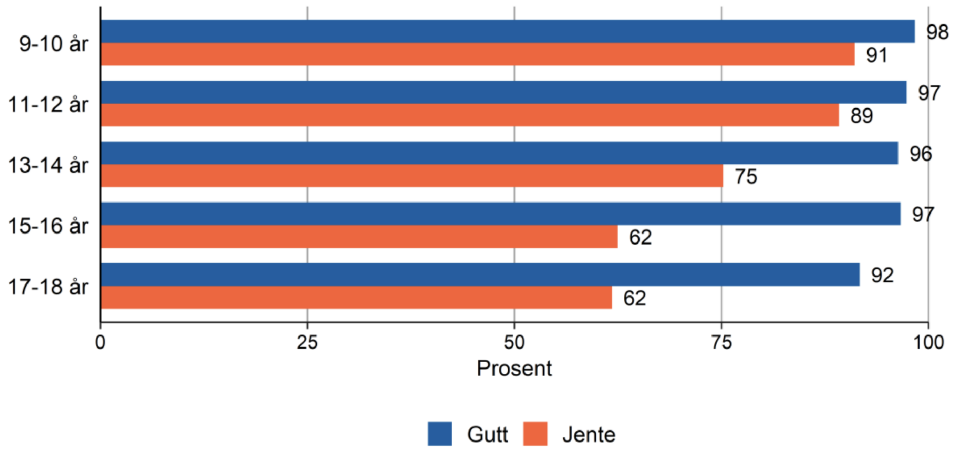


Figure 1.2: Percentage of youths playing video games based on age and gender 2020 (blue: boys, orange: girls)

[1]

The main goal of the project was to create a working prototype of a cooperative game that can enhance cybersecurity awareness among children. The development of the prototype was built on several preliminary activities, including a thorough Systematic literature review (SLR), expert interviews and a workshop. The prototype was tested within the target audience, and the results showed that a game-based approach for raising cybersecurity awareness is a viable solution. The prototype is available at `cybsecmaster.herokuapp.com`.

1.1 Research Questions

The thesis will address the following Research questions (RQs):

- **RQ1:** How can a game be designed such that cybersecurity awareness is raised for both children and adults?
  - **SRQ1.1:** Which game designs are appropriate?
  - **SRQ1.2:** What are the essentials in the design of a game to appeal to both children and adults?
- **RQ2:** How can one combine adult and child learning to raise awareness of cybersecurity?

1.2 Thesis Outline

This thesis consist of nine parts. Chapter 1 is this introduction. Chapter 2 outlines the background, and the motivation for the thesis. Chapter 3 summarises the SLR[7] conducted by us in the fall of 2021. Chapter 4 presents the different methodologies used throughout this project. Chapter 5 outlines and presents the expert interviews and workshop conducted for data collection. Chapter 6 describes the design and development of the prototype. Chapter 7 presents the resulting prototype, and the results from the user testing. Chapter 8 outlines the discussion of the aforementioned results, while chapter 9 concludes the report.

Chapter 2

Background

There have been several attempts on raising cybersecurity awareness in children in recent years. Reid and Van Niekerk [8], Baciu-Ureche *et al.* [9] and Giannakas *et al.* [10] all presented findings that their solutions increased cybersecurity awareness in their target audience. These findings are further supported by Tioh *et al.* [11] who showed that several games do increase cybersecurity awareness. However, as argued by Köhler *et al.* [6] most existing games only focus on remembering, understanding and applying knowledge. While this is a good step in the correct direction, they argue that evaluation of knowledge, as well as creation from knowledge are important to raise the awareness to an adequate level.

Furthermore, Quayyum *et al.* [4] uncovered the lack of research concerning the involvement of parents in the existing solutions. As parents often are a child's main caregiver until they become adults, it is vital to include them in the process. The importance is emphasised by the findings of Quayyum *et al.* [12] as it was apparent that parents lack the necessary knowledge themselves to teach their own children. Based on these finding, one can argue that including parents in the learning process is beneficial to the child.

This chapter outlines the different key areas and definition this master thesis is based on, followed by the motivation and inspiration for writing it.

2.1 Cybersecurity

There are several definitions of cybersecurity within the research domain. The most common definition is that of *computer security* which Merriam-Webster define as follows:

> *Measures taken to protect a computer or computer system (as in the Internet) against unauthorised access or attack*[1]

[1] https://www.merriam-webster.com/dictionary/cybersecurity

However, cybersecurity does not only concern the computers on the Internet. It also encompasses the users of the Internet, but to avoid confusion with *computer security*, the terms *digital wellness* and *digital competence* have been used. Digital wellness can be described 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*"[13]

While the Norwegian Government has defined *digital competence* as such:

> *Digital competence is the ability to relate and use digital tools and media in a safe, evaluative and creative way. Digital competence encompasses both knowledge and skill, as well as attitudes online. [...] Digital judgement, such as privacy, source criticism and information security are also an important part of the digital competence.*
> (translated)[14]

These two definitions highlights the personal aspect of the above stated cybersecurity definition, and when cybersecurity is mentioned in this report, the latter definitions are being used.

2.2 Game Based Learning

Game based learning, or gamification of learning, is a technique where elements from games are applied to the context of learning in order to encourage engagement and increase interest. This technique can both help engage children and improve their knowledge retention, as stated by Reid and Van Niekerk [8]. In the context of teaching or raising cybersecurity awareness among children the technique has been used in several papers and studies. Examples of these include *SecurityEmpire* by Olano *et al.* [15], *A Wolf, Hyena, and Fox game* by Snyman *et al.* [16], *The adventures of ScriptKitty* by Baciu-Ureche *et al.* [9] and *CyberSIEGE* by Irvine and Thompson [17]. In addition to the previously mentioned games, game based learning can in general be found in both paid and free mobile applications and games, as well as now outdated flash-games and other online games[18]. Many of the games or solutions that are part of research projects share a common limitation, namely that they seldom go past the phase of prototyping and/or user testing. In most cases with development of game based learning solutions for cybersecurity awareness, the solutions are not maintained after the papers they are part of have been published, and hence the games are not available to play outside the research process. The fact that the solutions (and source code) are unavailable after the end of the research projects makes it difficult for other researchers wanting to investigate similar topics in the future.

2.3 Motivation and Inspiration

As many as 640000 people on average access the Internet for the first time any given day[3], and with them there are several bad actors wanting to take advantage of the naivety of people with good intentions. The constant rise in number of people online leads to an increase in cyber attacks, cyber scams, identity theft, financial scams and defacing on a daily basis. As such we see the importance that the general population are aware of, and ready to face these cyber threats.

Since children are the world's future, it is even more important that they are aware of the different threats that exists online, and more so how to evade or overcome them if they are exposed to them.

There is a trend towards an increasing amount of young people playing video games in their free time[1]. In order to reach the children with information regarding safe practices and raising cybersecurity awareness, it is important to increase the engagement, by for instance approaching the children in a setting they are familiar with, such as games. In combination with the above mentioned threats this gave us confidence that a game-based learning platform on cybersecurity for children is a viable solution. Moreover, as the parents themselves lack the knowledge and experience to properly teach their children about how to spot and deter dangers online[12], and the research is lacking in this regard[4], we want to incorporate the parents in this solution.

By creating a web based game with a Mobile First design strategy[2] the accessibility is considerably enhanced. As Medietilsynet [1] concluded in their report, 97% of children between 9-18 years of age have their own mobile phone. More specifically, 87% of children aged 9-10 have their own mobile device. These statistics reinforces the notion that a web based game that is accessible from any device is a viable solution.

[2] `https://medium.com/@Vincentxia77/what-is-mobile-first-design-why-its-important-how-to-make-it-7d3cf2e29d00`

Chapter 3

Literature review

During the fall of 2021, we conducted a Systematic literature review (SLR) as preparatory work for this master thesis. The aim of the SLR was to build a foundation of knowledge such that we can develop a learning game aimed at children where the parents are an active part of the gameplay and learning process. To be able to reach this goal, we constructed the following Research questions (RQs):

- **RQ1**: How can children learn from using games focusing on cybersecurity?
- **RQ2**: What kind of game mechanics have been used to raise cybersecurity awareness among children?
- **RQ3**: Which kind of games exists for cybersecurity learning?
- **RQ4**: What does existing research say regarding involving parents in children's cybersecurity awareness?

The literature search was conducted using Scopus[1], an abstract, citation and bibliographic database, to find relevant papers to answer the above RQs. We used the following three search strings:

1. *("Cybersecurity" OR "Cyber security" OR "Digital security") AND "Game*" AND "Learn*"*
2. *"Game" AND "Design*" AND ("Child" OR "Children") AND ("Cybersecurity" OR "Cyber security" OR "Digital security") AND ("Awareness" OR "Understanding")*
3. *"Parent*" AND ("Inclusion" OR "Include*") AND ("Child" OR "Children") AND ("Cybersecurity" OR "Cyber security" OR "Digital security") AND ("Awareness" OR "Understanding")*

We were able to find a total of 327 papers that matched one or more of the search queries. By using the reference management software Zotero[2], 34 duplicates were found and excluded, which lead to 293 titles and abstracts to

[1] https://www.scopus.com

[2] https://www.zotero.org

be reviewed. 259 papers were excluded in this step as neither their titles nor their abstracts were relevant for the aforementioned RQs. As such, 34 papers were to be fully read and included based on the pre-defined inclusion criteria. As 15 papers did not pass our quality assessment, 21 papers were analysed for the SLR. The whole SLR process can be seen in Figure 3.1.

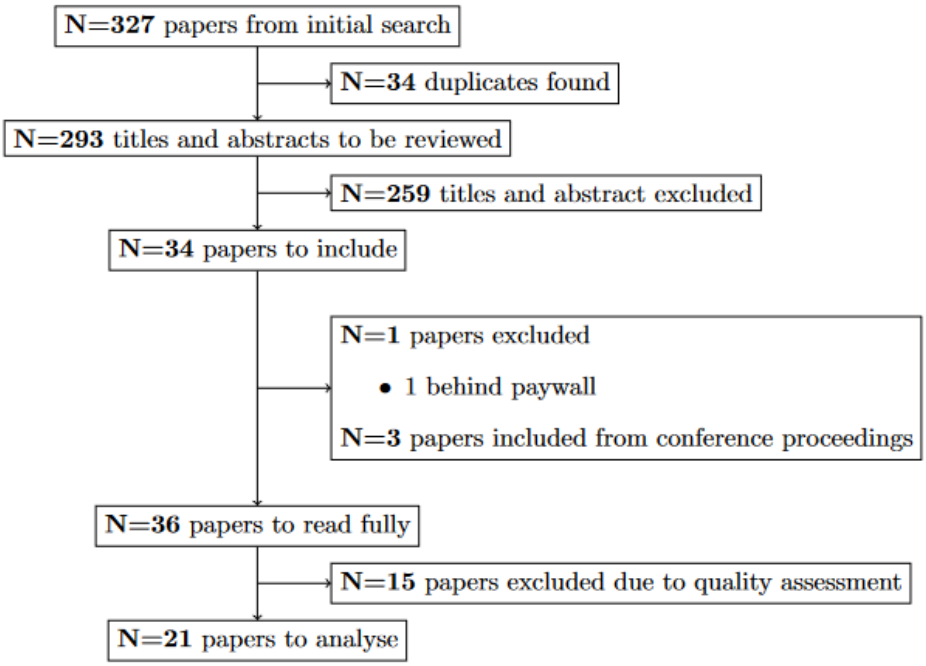
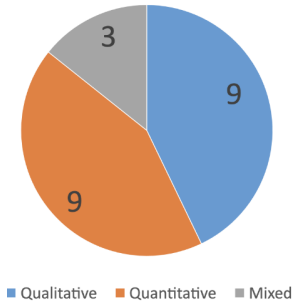


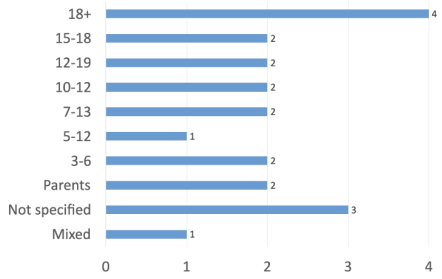
Figure 3.1: Paper selection process[7]

The collection of 21 papers consisted of a variety of research types, research methodology and target audiences. As shown in Figure 3.2a, nine papers were qualitative, nine were quantitative, while three where of mixed research types. There were five surveys, five experiments, five case studies, two analysis, one evaluation, one interview and two which used two or more different types of methodology. This distribution is depicted in Figure 3.2c. Lastly the different target audiences are summarised in Figure 3.2b. As one can see, most of the papers focused on youths in the age of 10-18, while both younger and older age groups were also present.

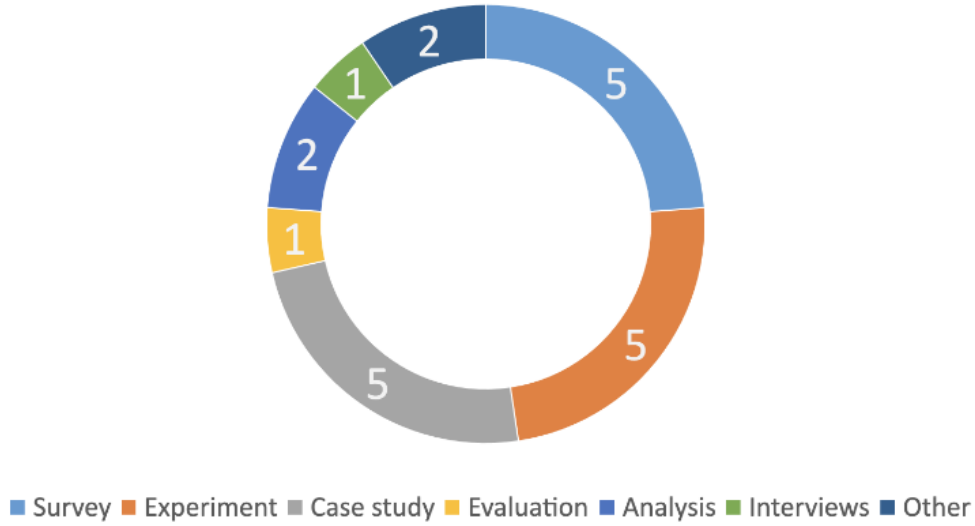
As one can see this SLR was diverse and covered several different research types, methodologies and target audiences. As such we deemed the SLR to be a valid ground for our future work. The next section will present and discuss the findings of the SLR.



(a) Research types



(b) Target audience



(c) Research methodologies

Figure 3.2: The different research types and methodologies, as well as the target audience of the papers reviewed in the SLR[7]

3.1 Findings

In this section we will discuss the different findings of the SLR. First the different learning frameworks used in the papers will be presented, followed by the different technologies used to create cybersecurity games for children and adults. Further, the most used and most popular game genres will be discussed, while the important game elements and design decisions are presented thereafter. Lastly the contributions this SLR has to the research domain will be propounded.

3.1.1 Learning Frameworks

The Attention, Relevance, Confidence, Satisfaction (ARCS) model of motivation([19]) is a learning framework, with the aim to enhance the retention and

recollection of knowledge by fulfilling these four concepts. The framework was used both in a cybersecurity awareness app [20] and a learning platform [10].

Another framework used in several of the examined papers [10], [21], was Bloom's Revised Taxonomy (BRT)([22]). BRT orders 6 cognitive skills: *remembering*, *understanding*, *application*, *analysis*, *evaluation*, and *creation*, in a hierarchical pyramid, where each level is theorised to establish the foundation for the level above. Being able to remember theory is seen as the lowest level, and creation of new theory the highest.

Conceptual Framework for e-Learning and Training (COFELET), presented by Katsantonis *et al.* [23], is based on an amalgamation of several other frameworks: Activity Theory Model for Serious Games (ATMSG), Common Attack Pattern Enumeration and Classification (CAPEC), Cyber Kill Chain (CKC) and National Cybersecurity Workforce Framework (NCWF), with focus on learning cybersecurity. By combining such specific frameworks, the result is both effective and relevant when used in cybersecurity education.

3.1.2 Techonologies

Among the examined papers, the two main identified technologies used to create cybersecurity solutions were mobile and web-based technology. The technology used does without a doubt govern the reach and availability of the solution. A mobile game only requires the user to use a mobile phone and a web-based solution can be reached by anyone with an internet connection.

As such, with an ever increasing use of the Internet world-wide, web-based technologies can be argued a great solution to efficiently reach a huge audience. Five of the solutions from the examined papers were developed with web-based technology. *Security Empire*, an online multiplayer tycoon-style adventure game was developed by Olano *et al.* [15] using LAMP and AJAX, while *Cyber-Hero* by Qusa and Tarazi [24] is a maze-escape game with focus on password security, built on a web-based platform for creating games using HTML5. Giannakas *et al.* [10] developed a Learning Content Management System. The game *A Day in the Life of the JOs* by Maqsood and Chiasson [25] is an extensive story-based game with focus on several different areas of cybersecurity. It is a web-application developed with HTML, CSS and JavaScript. The last game, *The Adventures of ScriptKitty* by Baciu-Ureche *et al.* [9] is a web-based game where the players use a Raspberry Pi to perform the tasks. The solution is not described in too much detail when it comes to the web-technology used, but they do use Kali Linux on the Raspberry Pi. In general there were very few similarities when it came to framework, platform, programming language or hardware used in the different solutions. This divergence demonstrates the enormous amount of options to choose from when it comes to developing a web-based solution.

Mobile phones have become a common possession among both adults and children in large parts of the world. Almost all Norwegian children, aged 9-18,

have their own mobile phones[1], and usage is increasing. Six of the papers (Snyman *et al.* [16], Allers *et al.* [13], Giannakas *et al.* [10], Giannakas *et al.* [20], Scholefield and Shepherd [26] and Alqahtani and Kavakli-Thorne [27]) used mobile technology in development or analysis, resulting in four mobile games aiming at raising cybersecurity awareness.

3.1.3 Game Genre

The *genre* of a game can be defined as a classification based on the way is is played, rather than the visual style or narrative presented. Examples of well known genres in games are: adventure, RPG, FPS, puzzle, quiz, simulations, racing and many more. The choice of game genre is another aspect that has to be considered carefully when designing and implementing a game, as how popular the different genres are depends on both age and other demographics. The chosen genre can affect the appeal and reception of the game within the target audience. The two most used game genres among all the games found from the papers were puzzle and quiz, and adventure.

The puzzle and quiz game genre seemed to be the most used genre from the examined papers. It often has a similarity to the well known format of test and quizzes conducted in a school setting, which means it is something children are familiar with. The games presented by Giannakas *et al.* [10], Snyman *et al.* [16] and Allers *et al.* [13] presented theoretical concepts, followed by a quiz, and a relevant mini-game based on the same concepts as reward upon completing the quiz. This repetition and different ways of presenting the same information is highlighted by Giannakas *et al.* [10], who presents their solution has an increase in learning outcome of 20%. Snyman *et al.* [16] and Allers *et al.* [13] did not conduct any form of evaluation of their solutions on their target audiences, but expert reviews deemed the games appropriate for the target age groups. The paper by Hattingh and Eybers [21] found that, on average, over 70% of participants felt the game made a contribution to a positive learning experience. Alqahtani and Kavakli-Thorne [27] went a different way with their solution, splitting the game into two separated parts: a set of learning materials and an actual game, where the materials acts as a supplement to the game. They concluded that the use of post-game questionnaires gave a motivational boost for learning about cybersecurity to the players, and that the game was a fun way to learn about the presented topics.

The three games developed by Olano *et al.* [15], Baciu-Ureche *et al.* [9] and Maqsood and Chiasson [25] can all be categorised under the adventure genre. Olano *et al.* [15] conducted a survey on their test subjects as part of the analysis of their game *SecurityEmpire*. From this analysis they deduced that several of the aspects relating to the genre used was positively received. Baciu-Ureche *et al.* [9] found that their game, *The Adventures of ScriptKitty*, made the test-participants more confident in computer usage, and saw an increase in use of best practice when it came to online safety after going through the testing.

Maqsood and Chiasson [25] showed a different level of comprehensiveness in developing their game. The game was developed, designed, tested and evaluated through an iterative process, including several rounds of user studies, use of pre- and post-test questionnaires, interviews, eye-tracking and recordings of the participants. They found that their solution led to improvements in both immediate and sustained cybersecurity literacy among the participants, and the feedback from both children and teachers were positive.

3.1.4 Game Elements and Game Design

When developing a game, one has to consider both what game design and what game elements to use. For a game aimed at children, the chosen elements and designs can be used to engage the players, and make it as appealing as possible. In their paper, Göbl *et al.* [28] state that "*Game design is difficult to quantify as likes and dislikes are subjective*". The following is a presentation of the different element- and design-choices identified in the reviewed papers.

A widely used type of game element is stress and time limits, which uses the temporal dimension in the gameplay. These elements can be implemented in many different ways, but examples include encouraging the swift progress of the player through the game by either penalising using more time or rewarding spending less. From the questionnaire conducted by Göbl *et al.* [28] they found that a time constraint of 15 minutes can be effective to increase reaplayability and player engagement. Five games from the reviewed papers implemented some type of stress or time limit. Giannakas *et al.* [10] implemented a time limit in the mini-game part of their solution, but not in the quiz part. The time limit was only used in the fun and rewarding secondary game component. Avoiding use of a time limit in the main part of the game moves the focus more to the quiz, and lets the player use time on reflection when answering questions, which in turn can increase the learning outcome. Qusa and Tarazi [24] on the other hand chose to implement a 90 second time limit for each "level" of their maze, constricting the time the player can use to find tips and answer questions. They point out that the time limit is used to induce retention of the information. In a similar way, Hattingh and Eybers [21] set a limit of 30 seconds for each answer in their game, with the intention of maximising the number of questions for each 30 minute session. They did however note that the sessions were too short to give the participants the full potential benefits of their game. In contrast, Tioh *et al.* [11] used a "stress meter" as a remedy to induce stress for the player in addition to function as a visual feedback of the progress in the game. Olano *et al.* [15] used a similar strategy, with a fast-paced gameplay to preserve both the interest and focus of the player, in addition to increase the engagement of the player. Trough semi-structured interviews and open-ended questions after the gameplay, the researchers got positive feedback from their test subjects regarding the use of the stress element.

Another much used element is rewards and/or punishment, which can be

an easy way to give the player feedback on how they are doing. A player that is given a reward as a result of an action is more likely to repeat the same action if the same situation or challenge occurs. Similarly, punishing a player based on an action makes it less likely that the action is repeated. Four of the papers implemented rewards in their games, while only one used punishment as a tool. In their games *Cyber-Hero* Qusa and Tarazi [24], *Cybar* by Alqahtani and Kavakli-Thorne [27] and *Data Science Pursuit* by Hattingh and Eybers [21], reward systems were implemented, based on the belief that punishments used in a game for children would inhibit the players tendencies to take risks and learn from mistakes. The form of rewards used were gaining levels or points upon completing an action correctly. In contrast, Scholefield and Shepherd [26] used a both punishment and rewards in their game, where the health points of the player and the opponent was reduced if the answers were incorrect and correct respectively. They noted that the use of this element increased the stress level among players.

The presentation of information as well as the amount thereof can also be considered an important element, especially when children is the target group of a cybersecurity game. Presenting long sections of text or using complicated language can make it harder to understand, and impact both enjoyment, attention, retention, interest and the learning outcome of the players. Zamri and Al Subhi [29] explains that in any application the informative element is necessary, and has to be essential. Among the papers five games were identified to use the amount and presentation of information as a tool. In their game, Reid and Van Niekerk [8] used colours, and kept their information short and concise. Snyman *et al.* [16] and Allers *et al.* [13] implemented both visual and auditory elements in order to communicate the information as well as present the information in the form of poems, making it easier to remember what was presented. In addition, they included the option of getting the poems conveyed through audio, which increases both the availability and information retention of the game, and makes it more universal. Another way of presenting the information was done by Köhler *et al.* [6], who argue that the knowledge of the player will increase through presenting explanations and relevant examples after completing all the challenges of their game. They mention that the balance of where to place the information, as well as the amount is hard to decide, since it can both negatively and positively affect the engagement level of the player, and in turn the learning outcome. They state that the use of a human facilitator could solve the engagement problem. In the case of the game by Scholefield and Shepherd [26] the participants expressed that they felt the presented information was lacking. One participant complained that the correct answer was not presented if they answered incorrectly, which indicates that this kind of informational feedback is a key technique when using quiz-style game elements. In contrast Baciu-Ureche *et al.* [9] found that their presentation of information was too much, with the text being too technical in nature, resulting in some participants failing to read all the information.

When making a game it is often necessary to apply a set of rules, to give the players explicit instructions on what is possible and not. They can also be said to be an important game element due to laying the foundation for fair gameplay. Even though most of the games from the reviewed papers implemented some set of rules, the majority of them only had implicitly defined rules from descriptions in various sections of their papers. Reid and Van Niekerk [8] and Hattingh and Eybers [21] implemented physical board games inspired by "*Snakes and ladders*" and "*Trivial Pursuit*" respectively, and were the only two who explicitly discussed the rules of the gameplay in their papers. Hattingh and Eybers [21] used a set of rules very similar to the original game they took inspiration from, whose rules are known to most children. In addition the difficulty and complexity of the game is almost entirely based on the questions presented to the players, and hence allows for rapid change and deployment. In a similar way Reid and Van Niekerk [8] also had rules taken from the original "*Snakes and ladders*, which in essence is a board game made for children. Using well known games as inspiration increases the possibility that the players know the rules from before, and it requires little extra effort and time to play.

Another type of game element that can be very powerful when making a game for children is the design element. For example, colours and animations can be used to convey information in a more visual way, to engage players, increase retention of information and better the replay value. The design of characters in the game, interfaces that are easy to use, and playful use of colours can all contribute to an enhanced experience for the player. There can also be certain differences based on the choice of platform, as the available design elements and GUI of a mobile phone can be more restrictive than on a desktop application for a computer. Five of the reviewed papers took note of the importance of using design as a tool. Reid and Van Niekerk [8] made use of colours to engage the younger players, while both Allers *et al.* [13] and Snyman *et al.* [16] used a combination of colours and animals to increase the appeal of their games. The remaining two, Olano *et al.* [15] and Scholefield and Shepherd [26] used the design element of animations to improve their game, noting that this was well received by participants in their user testing.

The last game element identified in the reviewed papers was statistics and feedback. These tools can give a player a good idea of the quality of their actions during the game. Baciu-Ureche *et al.* [9] points out that having the feedback be concise and to the point is important, and that long textual feedback is disadvantageous. Alqahtani and Kavakli-Thorne [27] implemented PMT on feedback to players after completing a task, which they argue is a good choice for how and when feedback is delivered. Feedback was also implemented by Olano *et al.* [15] through short-, medium- and long-term goals throughout the game, as well as feedback on the player's progress to these goals based on the actions of the player. As mentioned earlier, the participants in the evaluation of the game by Scholefield and Shepherd [26] noted the lack of feedback, and as

such could have improved their game by using this element. They did however implement a leaderboard indicating how the player compared to everyone else after playing through the game.

3.2 Contributions

The contributions from the SLR will be summarised in this section.

3.2.1 Increased Awareness

The papers that were reviewed in the SLR revealed that there have been many previous attempts at creating games to raise cybersecurity awareness among children, and many of the papers take notice of how the frameworks, techniques and tools used affect the quality, reach, and efficacy of their games. Two of the papers, Köhler *et al.* [6] and Tioh *et al.* [11], conducted SLRs. Together with our SLR[7] these will be a good starting point for other researchers investigating the current state of the research domain.

Three papers, Zamri and Al Subhi [29], Göbl *et al.* [28] and Kritzinger [30] researched the design and development of game based learning applications. There findings can be a good basis for development of new games or improvements for existing solutions for raising cybersecurity awareness. Furthermore, Shabe *et al.* [31], Al-Naser *et al.* [32] and Quayyum *et al.* [12] examined the risks children are exposed to online, the children's preparedness to handle the risks, and the role of the parents in this regard.

In total, 13 ([20], [10], [6], [16], [13], [33], [24], [26], [15], [25], [27], [9], [8] and [21]) out of all the reviewed papers described development and evaluation of their own game, with goals to teach and raise cybersecurity awareness. The findings showed both that there are certain genres and techniques that have been used more than others, that there are several potential choices for platform, game genre, game design, or game elements to choose when creating a game for raising cybersecurity awareness, and that game based learning in fact can increase cybersecurity awareness. However, the results presented in some of the papers are based on a small quantity of test subjects, and some papers lack sufficient quantitative evidence. These limitations are consistent with the findings from the paper by Tioh *et al.* [11], who also point out the small size of the test subject groups, and that it is not possible to conclude with a definitive answer to whether or not game-based learning increases cybersecurity awareness. The results can still be a good starting point for those wishing to raise cybersecurity awareness using game-based learning, even though more quantitative evaluations and research for such solutions should be carried out.

3.2.2 Parents as Stakeholders

Parents are in many cases the child's main source for attitudes and knowledge, and in many cases very influential in a child's life. Taking this into consideration, parents play an essential role in the process of raising cybersecurity awareness among their children. However, the papers studied showed that there was little focus on the role of parents in games for raising cybersecurity awareness. Quayyum *et al.* [12] supports this further, drawing attention to parents having limited knowledge within the cybersecurity domain, and not taking an active part in their children's cybersecurity education. Quayyum *et al.* [12] also found that it is challenging for parents to oversee all the online activity of their children, while Al-Naser *et al.* [32] points to a divide between current technology and parent's understanding and technical awareness.

Chapter 4

Methodology

In this chapter we will present the different research methods that have been applied as part of our project. The work done in this project is partly based on the SLR we conducted in the fall of 2021[7]. An overview of the utilised research methods can be seen in Figure 4.1, which is a visual representation of a research process created by Oates [34]. In section 4.1 we will discuss the use of semi-structured interviews with academics and professionals. Further in section 4.2 the workshop that was done with children and their parents will be described. Third, the design and creation of a prototype, including user testing of the prototype, will be outlined in section 4.3, followed by the process of applying to Norwegian Centre for Research Data (NSD) in section 4.4. Finally the qualitative data analysis will be detailed in section 4.5.

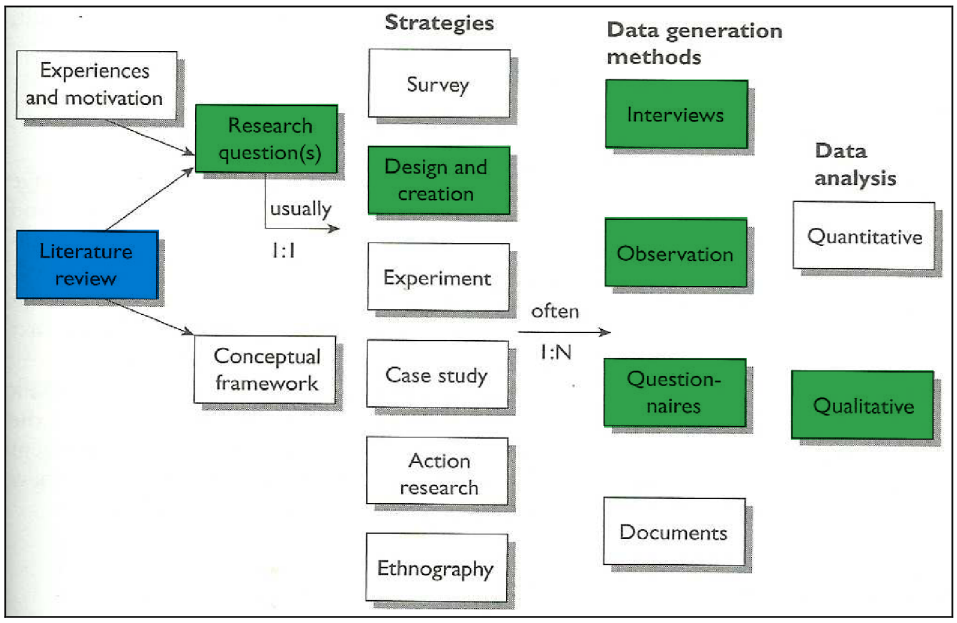


Figure 4.1: Overview of the used research methods based on the figure by [34]

4.1 Expert Interviews

As part of the research process, we conducted three expert interviews: two of which with Academics - participants with expert knowledge within the fields of HCI, CCI, game design and game development. The third participant represented a company specialising in raising cybersecurity awareness and teaching best practices and cybersecurity etiquette among adult employees within the businesses of their customers.

Conducting semi-structured interviews lasting between 40-60 minutes each with industry and academic professionals, allowed us to gather invaluable data. Combining this data with the findings of the previously mentioned SLR and a workshop within the target audience, created the foundation which a prototype could be built upon.

The interviews were conducted during March of 2022, and were done in Norwegian. Later, we transcribed the recordings in Norwegian, followed by translating them to English before analysis. As Norwegian was both our and the interviewees' native tongue, conducting the interviews in Norwegian improved the quality of both the questions and answers.

The interview subjects were selected based on their area of expertise and experience within their relative fields. The first interviewee represented a company specialising in raising cybersecurity awareness and teaching best practices and cybersecurity etiquette among adult employees. The second and third in-

terviewees were academics with expertise within the field of HCI, CCI, game design and game development. These areas correlated directly to the aim of this master thesis, and as such their input and knowledge helped contribute to a foundation upon which to build the proposed prototype.

To help the interview subjects understand and prepare for the interviews, we created interview guides and consent forms that were sent in advance. The forms and guide are attached in Appendix B (English) and Appendix C (Norwegian). These forms included the purpose of the interview, the aim of the project as well as general information about the rights and privacy of the interviewees.

4.2 Workshop

As part of the planning stages of this master thesis, we conducted a workshop consisting of four children, each with one of their parents (eight participants in total). To be able to better understand the needs both parties have when it comes to playing games together, we made a simple maze for each parent-child pair to cooperate on completing. Each maze consisted of several challenges the pairs had to overcome to be able to proceed through the maze. The goal of the workshop was to observe and ask questions about playing games together with their family members, and get insight into what people are looking for in a game.

In addition to understanding the needs both children and parents have when it comes to playing games together, we wanted to understand how the participants cooperated when presented with challenges. This data was important for us, helping us to decide which game mechanics to use in the resulting prototype. The execution of the workshop will be presented in detail in section 5.2.

4.3 Design and Creation

A working prototype within the context of this project is a game prototype that incorporates most of the functionality of a finished game. In other words, a prototype that is implemented, and could be used in a real-life context. In this section we will discuss the design, creation and user testing of the working prototype.

4.3.1 "Working Prototype"

The planning of the prototype started early in the project, with brainstorming sessions to come up with ideas, and revisiting the SLR we conducted during the fall semester for inspirations. The plans for the prototype were changed continuously during the project, as new ideas emerged, and we gathered data from the interviews and workshop.

As part of the planning we looked into several different possibilities for frameworks, platforms and programming languages for game development. When we started developing, we ended up with starting "from scratch", as neither of us had any experience in using existing frameworks, and learning new frameworks would delay the development work too much.

For the game we planned to make a story-based adventure game, where the players navigate a maze and are presented with challenges in the form of questions within various cybersecurity topics. Given the short duration of the project, we set up to continuously work on the report, and on planning the user testing of the prototype alongside the development of the prototype. The user testing of the prototype is discussed more detailed in the following section.

4.3.2 User Testing the Prototype

To be able to evaluate our game within the target audience, we conducted a user test after the prototype was fully developed. We experienced some difficulties with recruiting suitable participants within the target group, and because of this, we decided to limit the number of obstacles for participating in our user testing. Since the prototype was developed as a web based game, it was accessible from any device as long as the device had an active internet connection. Consequently we invited potential participants to an online workshop, using a BYOD strategy. The participants chose the time and location for the user testing themselves, and we were available for assistance and support digitally. We had continuously communication with each participant throughout their gameplay, and as such got valuable running feedback. A final date for the user testing was set such that we had time to extract and analyse the data before the deadline of the report.

The data was mainly collected using a pre- and post-questionnaire the participants filled out before and after playing. These questionnaires were implemented as part of the gameplay to increase the accessibility of the user test. The results from both the questionnaires and the challenges within the game was stored in a database in real time as the participants submitted their answers.

By following the guidelines presented by Read and MacFarlane [35] the pre- and post-questionnaire had short questions formulated in a easy and understandable language, and presented enough information such that the player would not get confused by the questions. Furthermore, we wanted to limit the amount of writing and open-ended questions, and as such gave the players a series of multiple choice questions.

The pre-questionnaire contained basic demographic questions such as age and gender, followed by a series of questions regarding different cybersecurity risks. These cybersecurity questions were repeated in the post-questionnaire to be able to understand if the game had any impact on the players knowledge and awareness around cybersecurity. The post-questionnaire also asked the users to rate the game on a Likert scale from one to five, one being the lowest score, and

five the highest. These questions regarded the game itself and how the players felt while playing it, and were added as to gauge the player satisfaction after playing one session.

Recruitment was also done digitally, through us contacting the previous participants from the workshop, in addition to anyone in our social networks that were in the target age group. In some instances, there were parents who were willing to recruit participants among friends with similar aged children, or their children's classmates. Taken all the adjustments in the recruitment process and the implementation of the user testing into consideration, the recruitment was still laborious and difficult, and we had to work quite hard to get the number of participants we acquired.

4.4 NSD Application

As part of the data collection process of the project, we had to apply for approval from Norwegian Centre for Research Data (NSD), which was done in preparation for the conducted interviews. NSD has defined strict guidelines for data collection, storage and analysis for research projects. After getting our application approved, the interviewees were presented with, and signed, consent forms for collection of their data, and their rights in connection with their personal data being collected. This consent form can be seen in subsection B.2.4. Furthermore, they received an interview guide explaining the purpose of the project, the research questions relating to the interviews, and a set of preparatory questions for the semi-structured interviews. This interview guide is attached in Appendix B.

The user testing was designed in such a way, that the data was anonymised by default, and no identifiable information was collected from this activity. As such, no approval from NSD was necessary.

4.5 Data Analysis

To be able to draw conclusions and useful data from the interviews, workshop and user test, we had to plan which data analysis methods to use. This section presents and discusses the different method used in this master thesis. First, we will outline the method used for analysing the interview transcripts, followed by how we analysed the workshop data. Lastly, the analysis of the data collected during the user test are presented.

Interviews

When analysing the expert interviews we opted to use a qualitative thematic analysis with an inductive approach. We closely examined the data to identify common themes and ideas that related to CCI, HCI and game design. By using

an inductive approach we did not analyse the data with any preconceived ideas, theories or existing knowledge as to not becloud the views and experience of the interview subjects. As we had a limited number of interviewees we did not see the need to include coding in our analysis. However, we were interested in the different themes that came up between the transcripts. As themes are generally broader than codes and provide more of an overview of the field, it made more sense to focus on these in this project.

Workshop

The results from the workshop was a combination of observation notes taken, and recordings done during the workshop. As the number of participants were limited, we decided to analyse the data using a qualitative content analysis. To avoid getting lost in the data using this analysis method, it is important to start the analysis with a specific goal in mind. The goal of the workshop was to see the cooperation and interaction between parent and child when playing a game together, and how they view this activity. As such, we looked for trends and similarities between the observations and the group discussions to understand how the groups view cooperative game play.

User Testing

As with the workshop, the analysis of the data from the user testing was done using qualitative content analysis. According to Read and MacFarlane [35] it is important to "*avoid the temptation to apply statistical tests to children's responses, rather look for trends and outliers*". As such, we looked at the data to see if there existed any trends, and more importantly any outliers. By comparing the pre- and post-questionnaire answers these trends and outliers became easily recognisable. We conducted the analysis with several questions in mind, as to not get sidetracked or lost in the data. These questions ranged from "*how much did the participants enjoy the game and its features?*", "*did the participants learn anything from playing the game?*" to "*are there any trends in the knowledge regarding cybersecurity?*".

Chapter 5

Expert Interviews and Workshop

As a preliminary data collection before starting the planning and implementation of the prototype, we conducted a series of interviews with three experts in relevant fields, and a workshop with the intended audience for the prototype. This chapter outlines the process and findings from all interviews as well as the workshop. We will first describe and discuss the expert interviews, and secondly the workshop.

5.1 Interviews

As described in section 4.1, during March of 2022, we conducted three semi-structured interviews with professionals and experts in the fields relating to cybersecurity awareness, HCI, CCI, game development and game design. The aim of these interviews were to gather data from people who work within the relevant fields on a daily basis. Furthermore, each interview subject has several years of experience, and as such the data collected is of high quality. The finding from these interviews are compiled into five overall themes, and are presented in the following subsections.

5.1.1 Context and Culture

The developers of any game will, either wittingly or unwittingly, be influenced by their own culture when creating a game. As such it is vital to be aware of this fact, as cultures are vastly different across the globe. The context and culture a game is developed within will be reflected in the game in a numerous different ways, be it the graphical style, sound choices, obstacles and play style. "*The background for the choices made in development will have different impact on youths in for example Norway and Thailand*" one interview subject pointed out,

and as such the feedback given to the players has to accommodate the context and culture the players finds themselves in.

However, if the development team is aware of this effect, one can take steps towards making the game as inclusive as possible. By using feedback elements that are more universal, for example traditional contrasting sounds, bright and happy colours or similar, the game will entice a more diverse audience.

Furthermore, how people define the term cybersecurity varies between contexts as well. If one were to ask a computer class how they would define the term, one would most likely get a definition similar to *computer security*, which is defined in section 2.1. Also, what a group of people will think is important in regards to cybersecurity will vary. Some will say privacy is important, while others will say that awareness around scams and theft are more important. As such, the developers need to have the correct context and culture in mind when creating a game focused on learning cybersecurity.

As *relevance* is one of the corner stones of the ARCS model of motivation, explained in subsection 3.1.1, it is important to design the game such that the relevant context and culture of the target audience are incorporated.

5.1.2 Story

The part of a game that all interviewees agreed upon to be the most important was the story presented in the game. The story is the driving force behind the gameplay, and as such has to be engaging, understandable, relatable and relevant for the players. This importance is further solidified by Baciu-Ureche *et al.* [9] as they received feedback that "*students loved the storyline*".

Storytelling has been used thoroughly throughout human history in both an educational, entertainment and enlightenment setting, and as such story-driven games will inherently be familiar and engaging to a wide audience.

Engagement can be fostered through the story, especially if the story encourage exploration and experimentation. As two interviewees agreed upon, exploration and experimentation will pique the curiosity of the players, and as pointed out by Wang [36, Chapter 7] both sensory and cognitive curiosity is important to enhance the learning outcome of a game. Furthermore, curiosity will entice the player to explore and engage more with the game, and as such play the game for a longer period of time, as well as come back to play more. Player retention is a goal for all game developers, and is not any less important for a learning game as it is with a AAA[1] video game.

Since *attention* also is a corner stone of the ARCS model of motivation, the developers should strive to create and present a story that is engaging and curiosity enhancing for the target audience.

[1] https://en.wikipedia.org/wiki/AAA_(video_game_industry)

5.1.3 Game Elements

A video game consists of many pieces of different elements combined. These parts make up the game as a whole, and they are what the players see, hear and feel when playing the game. These game elements are heavily influenced by the aforementioned context, culture and story, and as such has to be made to target the intended audience. However, there are certain game elements that are universal, and should be used as such.

As mentioned in subsection 5.1.1 some sounds are recognisable across the board. These sounds should play on the intended emotions for the presented situation. One interview subject said:

> *Everything that has to do with sounds are based on emotions, and the player will remember the action and consequence better. The impact will be larger. [...] Sound is very important as it affects our emotions more than the visual.*

By using sounds that are recognisable and familiar to the player, one can achieve higher engagement, as well as possible retention of knowledge.

Feedback is another important game element that was stressed by all interviewees. The player should receive different auditory and visual feedback on different actions taken throughout the gameplay. One interviewee said that "*sound will drastically enhance the impact of the feedback, if applied correctly*". It is important that both the auditory and visual feedback makes sense in the context it is presented in. If it is not, the player may not be able to understand the result of their actions.

5.1.4 Game Mechanics

One can make a game using only a story and game elements such as described above. However, it is not a proper game if there are no game mechanics involved. Game mechanics are what drives a game. Everything from the core rules of the game, what actions a player can make, and how the game is supposed to react to these actions. They "*effectively specifies how the game will work for the people who play it*"[37].

As little research has been done earlier concerning involving parents in the process of raising cybersecurity awareness among children using games, a cooperative game where both the child and the parent actively play together is a good approach. This notion is reinforced by two of the interviewees as they believe that if both players have their own character, their own challenges and their own story within the game, it will increase engagement and knowledge retention for both parties. One of the interviewees suggested further that the players perform actions in turn, which again will affect both themselves, as well as the other player, in order to increase the interaction and encourage cooperation between the players.

5.1.5 Pitfalls

Developing a game can be difficult, and this was reiterated by the expert in game development during the interview. There are many parts that make a game, and they are all from different fields of expertise. There are sounds, graphics, story, mechanics and code, and as such, creating a game as two computer scientists can be challenging. As such, one has to constantly remember that context, culture, story, game elements and game mechanics has to make sense together as a whole. Decisions made in one of these areas impacts the possible decisions in other areas. As the interviewee said:

> "*Gamification is just silly, if there is no true meaning behind it. Gamification can create interest, and pique some activity in the beginning. But if people do not get anything out of it,* ***then there is no point****, 'it dies' out. But gamification can make a person who is not so interested in security think that: "Aah, now I'll get points. That was fun. It was fun and actually a little useful", and as soon as you get there, you can build on the experience of that it was in fact useful, that 'security might not be so stupid'.*"

5.2 Workshop

The workshop was conducted at a local library in Trondheim on a Sunday morning. The aim of the workshop was to understand the needs of both children and parents when it comes to playing a game together. The data collected from the workshop, alongside the interviews, explained in section 5.1, and the SLR, presented in chapter 3, laid the foundation for the creation of a cybersecurity awareness game for both children and parents.

The following sub-sections outlines and discusses the recruitment process and the execution of the workshop, followed by a rundown of what we found. Lastly, our remarks on the workshop are presented.

5.2.1 Recruitment

As the workshop was specifically aimed at people with children between the ages 10 and 12, the target audience was narrow to start with. Furthermore, as the time and place had to fit for all participants, the size of the potential participant group decreased. However, we and one of our supervisors reached out in our respective social circles, and gathered both known and unknown participants that fit the set criteria. While the original age range for the children was 10-12 years old, it was widened to 9-13 to accommodate available participants. We gave all the participants cinema gift cards as a token of gratitude for their time and participation.

5.2.2 Execution

At the beginning of the workshop, we introduced ourselves to the participants, followed by presenting a brief overview of the workshop plan and requesting the participants to fill out the demographic and consent forms. The main task was allotted 50 minutes followed by a short break, while the discussion and conclusion was allocated a total of 40 minutes. We allotted 50 minutes for the game task for there to be ample time for the participants to play the maze-game. Furthermore, parts of these 50 minutes could be used in other sections if needed, as it is important not to stress the participants if some tasks take longer than planned. The proposed timetable for the workshop can be seen in Table 5.1.

Task	**Estimated time**
Welcome and settle down	10:00 - 10:10 (10 minutes)
Fill out forms and introduction	10:10 - 10:20 (10 minutes)
Maze game	10:20 - 11:10 (50 minutes)
Snack break	11:10 - 11:20 (10 minutes)
Group discussion	11:25 - 12:00 (35 minutes)
Conclude	12:00 - 12:05 (5 minutes)

Table 5.1: Workshop timetable

As the main section of the workshop was playing a maze-game, we had to construct and design the actual maze. To simplify this process, as well as making the game accessible and easy to use, we opted to construct the maze using an online maze-generator[2], even though this resulted in somewhat basic and less artistic maze. By adjusting the variables in the maze-generator, a desirable maze was created. As the maze was supposed to be played by two people at the same time, as well as containing a specified amount of challenges each player had to overcome to reach the exit, the generated maze had to be modified to fit the criteria we had defined. An additional starting point was created, and possible side paths in the maze were walled off.

As seen in Figure 5.1 each player has to overcome at least 5 challenges to reach the goal. However, as it is possible to take a wrong turn, and encounter a sixth challenge, we constructed 6 challenges in total for each participant. These challenges were divided into a set of child-specific challenges, and a set of parent-specific challenges.

The child-specific challenges were of a more quizatorial nature, where they were presented with questions around a certain cybersecurity topic, and provided several choices they could choose from. Some challenges also had the option to give more than one answer.

Furthermore, the parent-specific challenges on the other hand, were more focused on the parents view and relation towards their own child's cybersecur-

[2] `https://mazegenerator.net`

ity knowledge and behaviour. The parents were presented with different scenarios they had to take a stand on, and each scenario was surrounding their own child and the various security risks they encounter online.

To get the most out of the workshop, the challenges were designed to reflect a variety of different cybersecurity concepts from both the child's and the parent's perspectives. The challenges were also tailored to fit within the themes that we and our co-supervisor were investigating.

To make the challenges more interesting and enticing to the younger audience, the challenges were printed in colour, and included simple graphics relevant to the respective cybersecurity risk. To more easily distinguish between the challenges for parents and children, they were colour coded. Examples of these challenges can seen in Figure 5.2 and Figure 5.3.

To gather more insightful data about the participants experience, as well as understanding how each participant felt about a cooperative game about cybersecurity, the group was divided in two smaller groups for the discussion. One consisting of the children, and one consisting of the parents. We wanted the unfiltered thoughts of both group without having the parents speak for their child. Two organisers gathered the children in a separate room, while the parents stayed behind with the other organisers. Each group was presented with different questions aimed at their role in the parent-child duo such that we got the best data possible. These questions can be viewed in Appendix E.

By the end of the allotted time, the groups were again gathered together and the workshop was concluded. Each participant was gifted a gift card at the local cinema as a thank you for participating.

5.2.3 What We Found

By combining the observations done by us, with the information gathered in the group discussions, several interesting topics were apparent. The parents believed their children did not want to play games with their parents, as the children often view their parents as "old" or "outdated". Furthermore, the parents are not used to play video games as their children are, so the basic understanding and expectations of a game are different between the two groups. A possible solution for this is to incorporate older siblings into the game, instead of only the parents, as they often have more in common with the child, which further increases the possible target audience of the game.

However, the parents felt a collaborative game could be helpful in increasing the cybersecurity awareness of their children, and is further reinforced by the observations done by us. Several of the parents took a more collaborative approach when playing the maze game with their children. They helped their child understand each challenge, but did not guide them towards what the most correct answers were. They discussed the challenges and the different options on each, and helped the child make their own decisions. Furthermore, the parents let their child provide help, even when the parents themselves did

not need it, and as such the child felt empowered. As presented in chapter 3, confidence is one of the four cornerstones in the ARCS model of motivation, and as such should be prioritised when collaborating with children.

On the other hand, other parents chose to utilise a more guiding approach when playing the maze game with their child. It was observed that the parents took the lead, and guided the child towards the correct answers instead of letting the child make their own conclusions. This approach does not necessarily correspond with any of the proposed learning frameworks presented in chapter 3. According to Utdanningsdirektoratet [38] a child's independence and confidence is increased when they understand their own learning processes and their own professional development, and as such a guiding approach is not the best approach when learning children about cybersecurity.

All participant, both children and parents alike, said the game was fun to play, and especially together with their own kin. Some participants did not usually play games together at home, and the workshop introduced them to a new past time. They did, however, feel it would not have been equally fun to play on their own accord at home, as the game had a more teaching element, rather than a fun and playful game element. Similar opinions are presented in section 5.1 where the experts remarks the importance of fun and playfulness in a game. As such the notion that a game should be fun is an important one.

Furthermore, the participants felt that a game-based approach to learning was exciting and interesting, and could make learning more interactive and engaging. A correlation can be seen to the findings in [8], [11], [10], [24], [27], [25] and [15], and as such should be deemed an important factor when creating a solution to raise the awareness around cybersecurity.

5.2.4 Remarks

It became apparent that the difference between a child that is 9 years old, and a teenager that is 13 years old is often huge. The age difference became apparent in both their experiences from real life, as well as their ability to think and grasp larger topics surrounding their online life. It was noted by us that the 9 year old children need more help and guidance through the maze, than what the 13 year old children needed.

Furthermore, during the group discussion, the 13 year old children were the ones who had thoughts and feedback, while the younger participants stayed mostly silent, which provided us with limited data from the group discussion with the children. Moreover, we felt we had little to no experience with engaging with children in the target age group, and as such it was difficult to engage the children in the discussion. If the participants had not been split up into two groups, the parents could have provided better feedback from their own child.

Furthermore, the size of the participant group was small, but due to time constraints and the difficulty in finding a time and location, as well as recruiting participants that fit the criteria, we are satisfied with the turn out.

By combining the findings in both the SLR in chapter 3 and the interviews in section 5.1 one can see common topics emerge. Topics such as fun and playful gameplay, cooperative play style, and the engagement a game can summon. Moreover, by providing a accessible platform to both parents and children they are more inclined to delve into a game together, whether it is to learn or have fun.

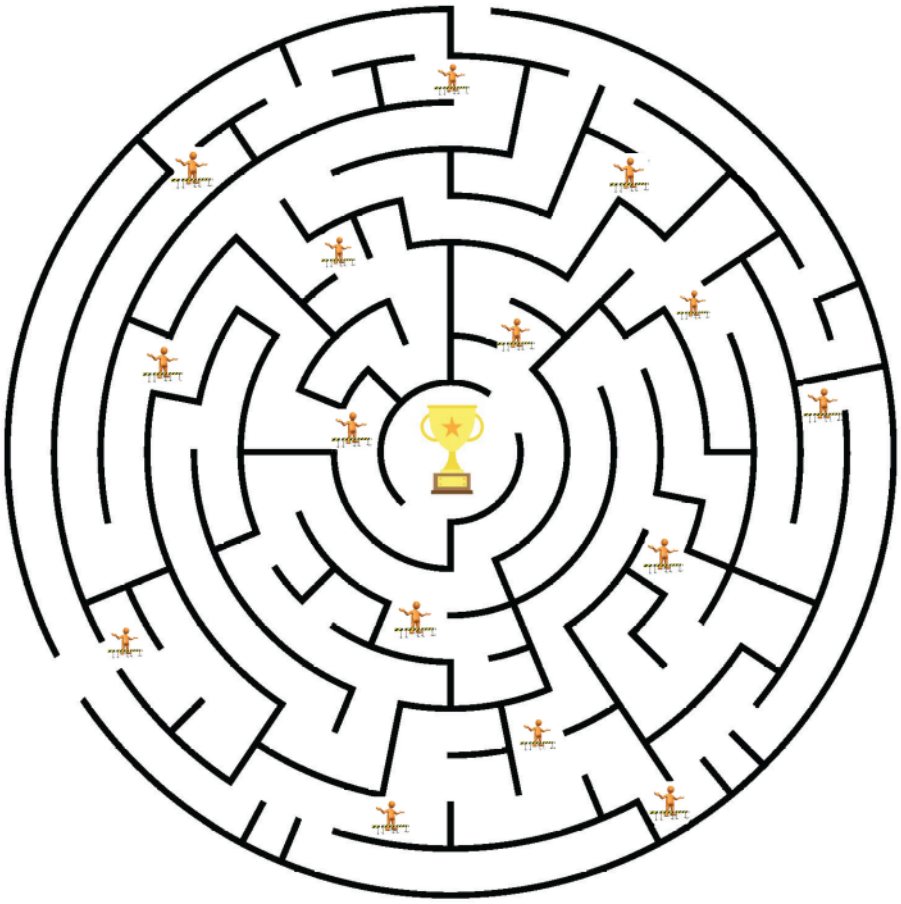


Figure 5.1: The maze used as the game-board for the workshop activity. The small figurines in the maze are the obstacles (challenge points), the goal is represented by the trophy in the middle, and there are two starting points (making the maze a 2 player game).

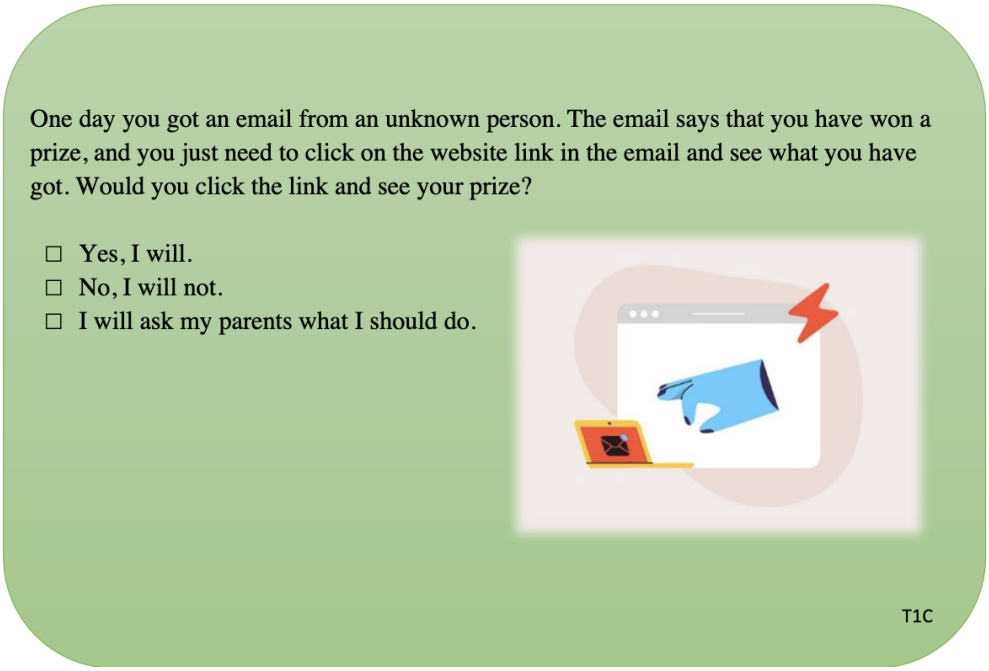


Figure 5.2: Child challenge about phishing risk

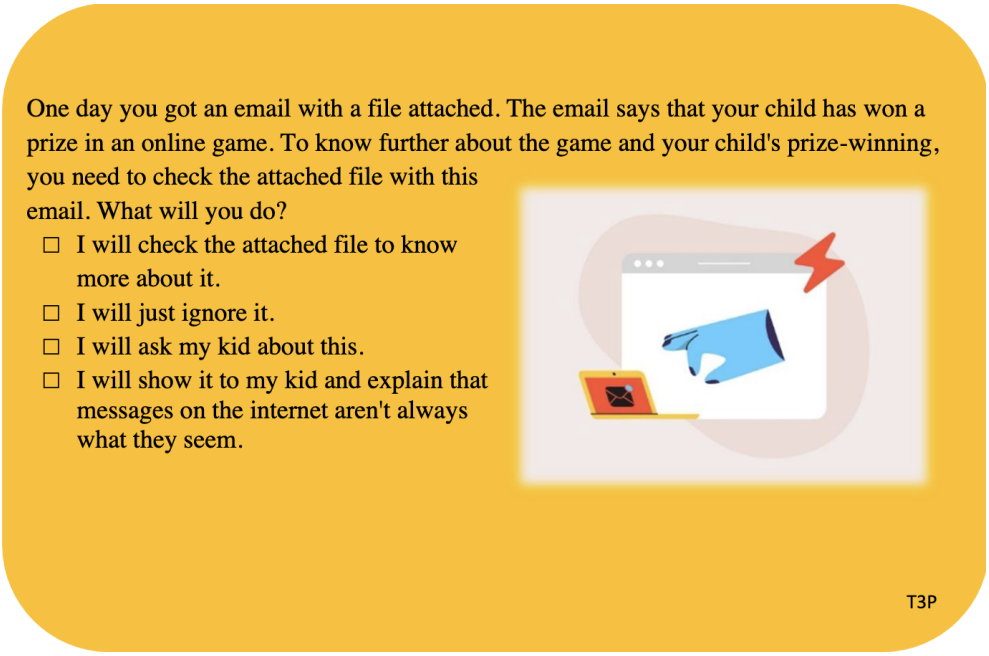


Figure 5.3: Parent challenge about phishing risk

Chapter 6

Design and Development

As with any production, a video game production undergoes several stages from start to finish. These stages vary from project to project but can be summarised as seen in Figure 6.1.

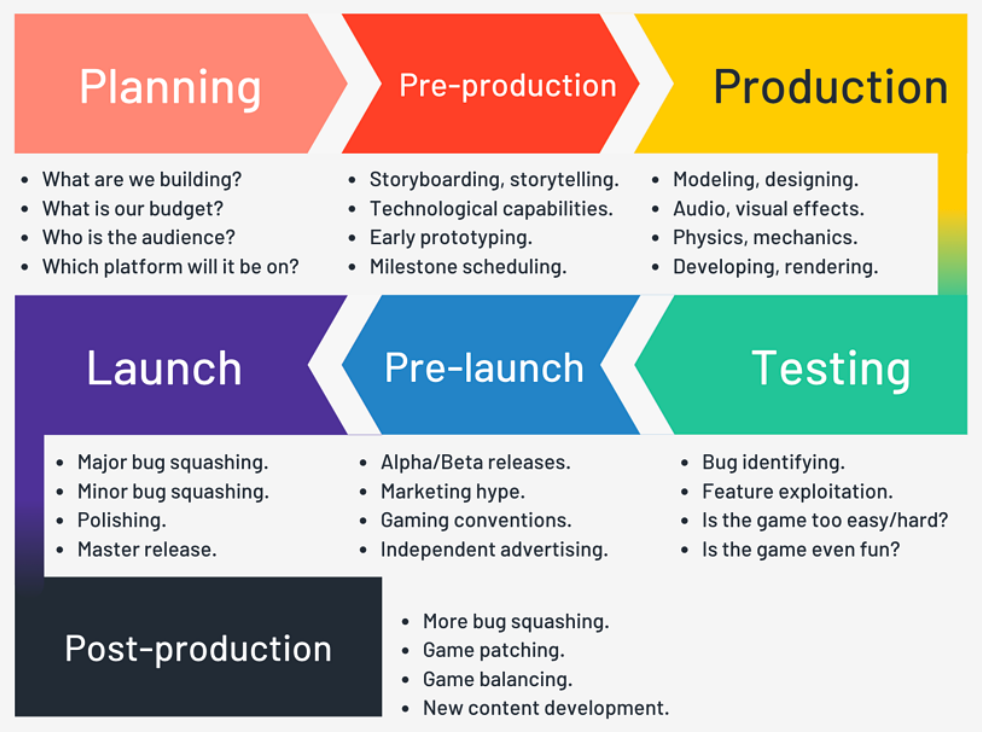


Figure 6.1: The stages of video game production[39]

As one can see this type of production is enormous, and consists of of several interdisciplinary tasks and objectives. As an AAA-game can have a budget on over 100 million dollars[40], a development period over several years, and a team of over 100 people, it should be understandable that the prototype

developed for this master thesis is of a much smaller scope, and does not implement all stages mentioned above.

By choosing the most relevant stages and sub-tasks within these, we had a more effective plan that fit the intended solution. We chose to focus on the planning stage, a combination of the pre-production and production stage, as well as the testing stage.

More specifically we planned what type of game to develop, who the target audience is and which platform the to develop the game for. Afterwards, we looked at the technical capabilities we had available as well as the capabilities we possessed. During the production stage we found relevant graphics and sounds, wrote code and tested alongside the development. At last we entered the testing stage where participants in our user testing group played and evaluated the game.

This chapter outlines the above mentioned steps in detail. Firstly the planning stage will be explained. Secondly both the functional requirements as well as the main quality attributes will be presented, followed by an overview of the technical design of the prototype. Afterwards, the development process is introduced, and lastly the implementation details are discussed.

6.1 Interaction Design

The interaction design phase of the planning stage is important as it defines the context and setting of the game, as well as the different game elements and game mechanics that influence how a player engages and interacts with the game. Furthermore, it sets several precedents that we have to follow as a change in the interaction design in a later stage has a big impact on all aspects of the game. Such a change requires stopping most of the development as re-planning and restructuring has to be done. However, by preparing for such changes that do eventually come up, we can handle changes more fluently and efficiently. Even though, this phase should be thoroughly planned and reiterated for the most efficient development process in later stages.

This section outlines the design choices made, both visual, auditory and game design is compromised here. First we will look at the story element of the game, followed by which theme and atmosphere the game should have. Thereafter, how player feedback will be implemented is presented, and lastly, we will look at the different game mechanics and game elements we decided to use as these are the driving force within a game.

6.1.1 Story

During the SLR, outlined in chapter 3, it became apparent that few solutions have implemented a proper story element to their cybersecurity awareness games. Several papers reviewed, did however discover that the adventure game

genre was one of the more popular amongst children, and as story is what drives an adventure game forward it is one of the core pillars of such a game.

We wanted to capture the feeling of adventure in our solution as Wang [36] mentions that exploration and curiosity are important factors for learning retention. These factors combined with the fact that all interviewees in section 5.1 expressed the further importance of story, makes the story element one of the more important aspects of a game-based learning solution.

It is easy to write a story, but it is exceptionally hard to write a good story. A good story should be engaging and complex, but at the same time be easy to understand and have a logical flow such that the listener can easily follow along. One can easily find story templates, or even free story generators, online but the story has to fit within the context and culture of the players as further explained in the interview findings.

The story also affects the games graphical theme, its game mechanics and the different game elements used, as all these parts has to fit together to make a cohesive and enjoyable experience for the player.

As this project is a prototype of a cybersecurity awareness game for children aged 9-13 and their parents, the story was kept simple without twists, turns or complex plots. When a player starts the game, they are greeted with a short description of why they are where they are in the game world. The player is trapped in a maze, and the goal is to reach the second door and unlock it, which enables to player to escape the maze. However, the doors are sealed, and in order to open them the player has to help the spirits of the world with challenges they have. By exploring the maze, the player can encounter such a spirit, and is prompted with a cybersecurity related challenges. Every correct answer to these challenges rewards the player with points. When the player has amassed enough points they are able to unlock a door and proceed.

As one can see the story is simple, yet engaging. By letting the players explore the maze on their own without them knowing when a spirit may decide to interact with them, as well as not showing the entire maze at once, entices the curiosity of the player. Further, by giving the players a concrete goal, it is easy for them to understand what to do, and how to do it.

6.1.2 Theme and Atmosphere

After the story is defined, one should look at what the overall feel and atmosphere a game should be. As with the story, the atmosphere should be related to both the context and the culture of the player and the game setting, while also conform with the story itself.

As the story has a mysterious element to it, the player is trapped in a fantasy world with spirits, the atmosphere should mirror this. As such, we wanted to have a mysterious atmosphere where both the graphical and auditory elements enhanced this feeling.

By using ambient sounds along side sound effects, one can achieve a more

immersive game while also keeping the effects of actions and consequences high. By also including suitable colour schemes one can enhance the players learning retention as well as keeping the game engaging.

However, as one interviewee said in section 5.1, it is important that all these elements include some familiarity for the player. If the whole game feels out of place for the player, it is more likely they will not engage in the intended manner, which could lead to players not finishing the game, and forgetting it soon afterwards.

6.1.3 Feedback

As explained in section 5.1, all interviewees mentioned that both auditory and visual feedback is important to get the best effect of a learning game. By focusing on three major components of auditory and visual feedback, we provide the players with proper feedback across an entire game session. These three, sound, graphics and animations, will be presented in turn below.

Sound

As one interviewer expressed in subsection 5.1.3 the player remembers the action and consequence better because the impact is larger when using proper sound feedback. It is, however, important to choose a audio profile that fits the content, setting and atmosphere of the game, as well as the context and culture the target audience is familiar with.

Since the genre of the game is adventure and the target audience is Norwegian pre-teenagers, we decided to use a lighthearted and slow piece of music as the background track.

Furthermore, different sounds were used when the player performed actions. When they encountered a spirit, a sound played and the challenge was displayed. This sound was short and more alarming than the background track, such that the player more easily understood that something is going on, and another action is required.

The last sound used was a more happy and encouraging sound that played when the player successfully opened a door to advance to the next level. This sound lasted as long as the door animation, and as such there is coherency between the auditory feedback, and the visual feedback, such that they enhance each other.

As neither of us are audio creators or audio designers, the sounds were open source and found on itch.io[1], an online archive of both free and paid games, game assets and tools. These creators are credited in the online repository of the game.

[1] `https://itch.io/`

Graphics

When creating a game one cannot ignore the requirement for graphical components as these are what the player sees, interacts with and often remembers a game from. Even if sounds are a more effective method of feedback, a game without graphics are often disengaging for younger audiences.

Furthermore, to conform with the context and story of the game, we chose a mystical graphical impression. As the player is trapped in a fantasy world, and the levels in the game are mazes, we saw it fitting to use mountains, grass and paths to represent this world. As with the sounds, we found a free tile and spritesheet set in itch.io called Mystic Woods[2], as seen in Figure 6.2, that fulfilled all our graphical requirements.

Figure 6.2: Mystic Woods asset pack

The art style is playful, but mysterious, just like we want to present our prototype. Moreover, the method we aimed to use to create the levels in combination with the asset pack, made the game unique and memorable for the players. The pack also has more tile sets than we need for the prototype, so it can easily be used to extend both the functionality and add different settings and biomes to the game.

The feedback the players receive from these assets include, but are not limited to, player movement, door interaction, and difference between rooms in the maze.

Animation

To be able to use visual assets properly when giving feedback to the user, one has to use animations. A static image can give a small amount of feedback, but by using animations this effect is greatly enhanced.

It is, however, important to not overuse animations, as they have to be relevant and fitting to enable a positive effect on the players. An out of place animation, or an animation that lasts either too short or too long, can be interpreted as a bug or a fault in the game, and as such will not be taken seriously.

To overcome the problems mentioned above, we carefully planned which animations to use, and where to use them. There were five situations where animations were most effective.

First, when the player moves we wanted to simulate movement from one square to the next, which made the movement feel more natural, and the player got the sense that they actually controlled the character on screen.

Secondly, we wanted the encounters with the different spirits to come as a surprise to the player. As such a pop-up box was implemented with the spirits

[2] `https://game-endeavor.itch.io/mystic-woods`

challenge contained within, and the pop-up animation was a smooth transition such that it did not "come out of the blue".

Thirdly, when answering a challenge, the correct and incorrect challenge options were animated with a suitable colour. If one option was correct, it gradually turned green, and if one option was incorrect, it gradually turned red, to both emphasise the answers, and enhance the learning outcome for the player.

Fourthly, the opening of the door was animated to reinforce that an action has triggered a consequence. The door fluently change between a locked door to a fully opened door. This animation told the player that they had finished the level, and were able to proceed to the next.

Lastly, we want the inaccessible parts of the maze to have variety. As the asset pack mentioned in section 6.1.3 contained both water tiles and water animations, it was possible to implement this. The water splashes against the shore, and the middle parts had a wave effect added to them. These small details greatly enhance the effect the game world had on the players.

Both the challenge pop-up and the door animations had relevant sounds associated with them to enhance the importance of the actions.

6.1.4 Game Mechanics

Game mechanics are defined as "*constructs of rules and feedback loops intended to produce enjoyable gameplay*"[41], and as such are important to implement correctly when creating any type of game. The game mechanics governs how the player interacts with the game, and how the game reacts to the players actions. These reactions has to conform with the overall theme of the game, such that it is logical for the player.

The tree main game mechanics to be implemented in our prototype are cooperation, rewards and the core game rules, and these are presented in turn.

Cooperation

Based on the feedback from both the interviews in section 5.1 and the workshop in section 5.2 we wanted to include the parents in the gameplay as we see it favourable to increase their awareness around cybersecurity risks as well.

As such, we wanted to developer a cooperative multiplayer game that enabled more than one player in one game session at a time. By doing this, we encourage cooperation and participation from both players. One interviewee suggested to have the players play in turn, but we wanted the game to be more active, so we opted for a real time multiplayer game. Both players can move at the same time, both players encounter spirits randomly and both have to answer the spirits challenges correctly to advance to the next level.

Furthermore, either player can ask the other player for help when stuck on a challenge. If one player requests help, the same challenge is displayed to both

players, and they can actively cooperate on the answer.

Moreover, to enable communication between the players, such to have the opportunity to play together even though they are not physically together, we wanted to implement a real time chat system within the game. The chat will be tied to that one game session so that only the players within that one session sees the relevant messages, which in turn enhances the cooperative feeling of the game.

Rewards

A reward system is a fundamental and widely used game mechanic. A reward can be anything from experience points to level up a character, in-game currency to buy equipment or bypass obstacles, or it can be a simple points system to enable competition between players.

We chose to implement a simple points system, where the player got points for answering correctly on a challenge. To advance to the next level, the player had to have amassed enough points to be able to open the locked door. A correct answer gives points ranging from 5-25 each. The amount of points vary based on what the best option is for that challenge. Incorrect answers reward zero points, and the player is presented with graphics indicating if their choices were correct or incorrect.

For this point system to make it more challenging when playing cooperatively with another person, we set the required points for each door accordingly. If a single player plays, the requirement is 60 points. If two players play, each player has to acquire 60 points each for the door to open. This requirement entices proper cooperation as both players have the same end goal.

The points are displayed at the top of the game screen such that it is easy for any player to see how many they have acquired so far, and how many they are missing. If points are missing to advance to the next level, they have to continue to search for more spirits to help.

Rules

For any game to function and work as intended by the creators, a set of basic rules has to be in place. Imagine Monopoly without rules. A gameplay session would be catastrophic as all players would disagree on how to play the game. However, these rules have to be easy to grasp and understand for the target audience, as too complex and intertwining rules are often misunderstood and can result in the player leaving the game early. Furthermore, these rules has to make sense within the game genre and context, as all aspects of the game has to conform with each other. If the game is not coherent in its whole, players lose engagement and player retention is lost.

As such we opted for a set of very simple, but effective rules for our game. The player, or players, are set within an unknown maze with limited visibility.

Figure 6.3: Fog-of-war in the open-source game Freeciv[3]. By Nybygger at English Wikipedia, CC BY-SA 3.0[4]

The players move around using the controls, and randomly encounter a spirit. To be able to move further into the maze, the player has to answer the challenge given by the spirit. As mentioned in section 6.1.4, correct answers reward points, while incorrect answers reward zero points.

The goal of the maze is to find the locked door, amass enough points to open it, and advance to the next level. The next level is another, but bigger maze they have to explore, and as with the first level, they have to collect points from helping spirits to be able to finish the game. When the player reaches and opens the second door, they are finished with the game.

Fog of War

To encourage exploration and pique the curiosity of the players, we wanted to implement a fog-of-war system in the game. Fog-of-war is a term used to describe a mechanic where the game map is not fully visible at all times. Fog-of-war is best represented using images, and as seen in Figure 6.3 the fog-of-war is the darker parts of the game screen. Usually this mechanic has three stages:

1. Unexplored - black in colour
2. Explored but not visible - visible game map but with a darker overlay
3. Visible - normal visible game map

We wanted to implement all three stages in our game as to keep a mysterious atmosphere within the maze. First we defined a light radius which is the number of squares a character sees in any direction, and by using Bresenham's Line Algorithm[42] we were able to find all intercepting squares between the player and the end of the light radius. If one of these squares was a wall, all squares behind it turned not visible. By not knowing what was around the next corner, it enticed the player to further explore the maze such that they got the full layout in the end.

6.2 Requirements

In this section we will discuss the requirements used in the development of the game. The requirements are a result of the planning and implementation done during the development process. First we will present the functional requirements, then we will take a closer look at the non-functional requirements, also known as *quality attributes*.

6.2.1 Functional Requirements

The development "team" consisted of two people and the project was inherently small in extent and complexity. Because of this combined with the somewhat nontraditional structuring of the development process, the way the functional requirements were defined can be described as fluid and flexible. The requirements were first discussed during planning of the game, but amended to and refactored throughout the development process. The resulting functional requirements can be seen depicted in Table 6.1, where each requirement is marked with it's corresponding priority. For the priorities, *high* corresponds to a requirement that must be implemented, *medium* is used for requirements that are "good to have", and those that are insignificant, and more of a bonus are categorised as *low* priority.

ID	**Requirement**	**Priority**
FR1	The player should be able to play cooperatively together with another player	High
FR2	The player should easily be able to find instructions for how to play the game	High
FR3	The player should be able to communicate with the other player	Low
FR4	The player should be presented with different challenges when navigating the maze	High
FR5	The player should be able to play alone	Medium
FR6	The player should be shown their score throughout the gameplay	Medium
FR7	The game should have several levels	Medium
FR8	The player should see a graphical representation of where the challenges are inside the maze	Low
FR9	The player should get visual and auditory feedback on actions and progress	High

Table 6.1: The identified functional requirements for the prototype

6.2.2 Quality Attributes

As the primary quality attribute for the game, we chose accessibility, which involves both how accessible the software is, as well as how easy the software is to use for the intended players. The secondary quality attribute chosen was usability: how inherently easy the functionality of the game is to learn, as well as how rewarding and easy it is to play. The reasoning for choosing these two attributes is tightly linked with our ambition to create a game that is available to as many people as possible, that is easy and fun to play in order to raise cybersecurity awareness. These quality attributes are described in detail through the various scenarios in the tables in the sections below.

Accessibility

The two scenarios for accessibility are shown in Table 6.2 and Table 6.3. The first describes a player being able to easily start a game using a different device than the other player, while the second details the ease of starting a single-player game.

ID	QA1
Source	Player
Stimulus	Wants to play multiplayer with two different devices/platforms
Artifacts	Game mechanics
Environment	Run-time/design-time
Response	The player should be able to use any device that has a browser and an internet connection to play the game
Response measure	$<$ 5 seconds

Table 6.2: Playing from any device

ID	QA2
Source	Player
Stimulus	Wants to play the game alone
Artifacts	Game mechanics
Environment	Run-time
Response	The player should be able to start a single-player game
Response measure	$<$ 5 seconds

Table 6.3: Play the game alone

Usability

For the usability quality attribute the two scenarios describes the straightforwardness of learning how to play the game, shown in Table 6.4, and effortlessly joining the game of another player, to play a multiplayer game, shown in Table 6.5.

ID	QA3
Source	Player
Stimulus	Wants to learn how to play the game
Artifacts	Game mechanics
Environment	Run-time
Response	The player should have easy access to instructions on how to play the game
Response measure	In less than 2 minutes the player should be able to get familiar with the game mechanics

Table 6.4: Learning how to play the game

ID	QA4
Source	Player
Stimulus	Wants to join a game started by another player
Artifacts	Game mechanics
Environment	Run-time
Response	The player should easily be able to join a multiplayer session in a game started by another player
Response measure	$<$ 30 seconds

Table 6.5: Joining a previously started game to initiate a multiplayer session

6.3 Technical Design

This section outline the overall architectural design of the solution, as well as the foundation the prototype will run on. First we will define what type of solution the prototype will be, followed by an explanation of how this solution will be hosted and available to the participants of the user testing. Lastly we will outline the system architecture of the entire solution.

6.3.1 Web Application

Based on the findings of the SLR, comments from interviews and Medietilsynet [1] we decided that a web application was the preferred platform for

a game-based learning solution. Furthermore, we already had extensive experience with creating web application, and as such a working prototype was feasible to implement within the project scope. Moreover, a web application is accessible from any type of device, be it a mobile phone, tablet, laptop or desktop computer, and as such the accessibility of the solution is enhanced, which again is one of the main quality attributes of the solution.

6.3.2 Cloud Hosting

To enable easy access for users, as well as good up-time and less maintenance needed from us, a cloud hosting provider was chosen for hosting the application. We had some criteria when choosing the hosting provider such as:

1. Support for the selected framework and platform
2. Support for Continuous Delivery/Continuous Integration (CD/CI)
3. Support for the selected database engine and server

After researching and comparing different providers, *Heroku* was chosen as it supported all requirements and it is free to use for non-commercial applications.

Heroku

Heroku is "*a platform as a service (PaaS) that enables developers to build, run, and operate applications entirely in the cloud*"[5]. As it has inbuilt support for the chosen language and framework, as well as a free basic plan for the chosen database, while also being free and easy to use for the scope of the project, it was a perfect fit for the solution. Furthermore, with the provided *Heroku CLI*[6] we were able to easily control and extract data from the user testing.

Continuous Delivery/Continuous Integration

A Continuous Delivery/Continuous Integration pipeline was set up to enable us to quickly deploy hot fixes as well as check how the solution worked in a production environment. A CD/CI pipeline gives the developer instant feedback if their code changes works or not, and is inherently secure as all production environment variables are only accessible within the production environment.

There are however some drawbacks with setting up such a pipeline. It can be time consuming to set up if the developer has limited experience with the technology. There are several steps that has to be enabled and work fluently together, and it is difficult to test the actual pipeline without deploying code directly to the pipeline target. Furthermore, it makes it more difficult to change to another hosting provider in the future, as the CD/CI pipeline is tightly integrated with the production environment.

[5] https://www.heroku.com

[6] https://devcenter.heroku.com/articles/heroku-cli

Despite these drawbacks, the advantages of a CD/CI pipeline outweighed the disadvantages as we already had experience with setting up such a pipeline, and the time frame of the project would not impose a change of hosting provider.

NTNU Assets Storage

Since a game usually has graphical and auditory assets, and these assets are large in file sizes, a separate asset storage solution had to be found. *Heroku* only allows a certain disk space usage on their platform, and this usage would be too little for the prototype. As such, we looked at several solutions to this problem, and decided to make use of the free could storage the university provides us as students. By storing the assets on the university's servers, and downloading them to the client when a player plays the game overcame the problem of disk usage at the hosting provider.

One drawback of such a solution is that the client has to download the assets, and since these files tend to be bigger in size, the game has a initial loading time. However, after testing this approach, it was a viable solution as it would let the players have time to read and understand the provided instructions for the game while they waited for the downloads to finish.

6.3.3 System Architecture

The system architecture of any software solution is important, as it ties into all parts of the solution. The architecture can limit the available frameworks, the available technology as well as the available storage solutions. However, the choice of system architecture can also be influenced by the choice of technology. If the developer has prior experience in on technology, it can be beneficial to choose the technology first, rather than the system architecture. As such the architecture has to conform with the choice of technology.

This is what we did in this project. As we had extensive experience in the chosen technology, we decided on technology first, rather than architecture. As such the architecture evolved from the choice of technology.

Server Side Rendering

As the prototype was a multiplayer game played in the browser from any device that had an active internet connection, we wanted to minimise the possible synchronisation issues between clients. As each client can have vastly different internet connection speeds, concurrency and latency can cause the players to feel that the game is unplayable or not enjoyable. To overcome these issues, we decided to utilise server side rendering as this would ensure that both the current state of the game, as well as all game logic and rules were handled by one central unit. As such, the clients would only be showing the current state

of the game and receive input from the players which in turn was sent to the server for processing.

There are, however, some drawback with using a server side rendering architecture. It does require that all clients have a relative good and stable internet connection, and as such this solution would be less ideal in rural location. The multiplayer aspect of the game would feel difficult to handle if the internet connection was to drop out, as the client would experience loss of concurrency with their co-player. Larger multiplayer production enables a more fluent experience by letting the client make predictions on what is going to happen next in the players field of view. While this could be implemented in the prototype, it is not prioritised because of time constraints.

Relational Database Management System

To be able to gather data directly from the prototype for evaluation, we wanted to use a Relational Database Management System (RDBMS) for data storage, enabling us with easy access to all stored data, as well as a powerful query language to structure and extract the relevant data collected in the user testing stage.

While NoSQL[7] are more preferred by developers in 2022[43], we already had prior knowledge and experience using a relational database and the Structured Query Language (SQL). As such the choice of data storage solution was done early on. The only requirement we had for the solution was that the language and framework used in development had proper support and easy implementation for the chosen RDBMS.

6.4 Implementation

The implementation details are important to understand how the plan and vision for the project went from ideas on paper to an actual working prototype. The details will serve both as information about the platform, structure and work flow during development, and as a guide on how to proceed with further development in the future.

We have created a simple architecture, chosen technologies that are easy to use, and set up a work flow such that any developer can extend the prototype with new features or fix possible bugs in the code with relative ease.

This section outlines in turn the process model followed, programming language, frameworks, middleware and database used in developing the prototype, followed by special programs used during the development stage as well as data extraction.

[7] https://en.wikipedia.org/wiki/NoSQL

6.4.1 Process Model

When choosing a process model to use in the development of the prototype we found two major limitations that needed consideration: The time constraint of the project, and the fact that the main goal of the project was to explore how a game should be made to increase cybersecurity awareness. In a regular development setting a more traditional process model would be more fitting, but given the scope and time span, we settled for a mixed process model, using elements from both the *code-and-fix* model, the *incremental* model and the *waterfall* model.

The *code-and-fix* model is a simple and effective approach. The model is advantageous for a smaller, less complex project, as it requires less planning, and there are fewer steps to follow for each component or feature that is developed. Using the model can make it harder to track progress, accommodate changes and assess quality, but we deemed these challenges to be less of a threat since we were the only two working in the development team, and we both had experience using a more agile and structured approach in our professional lives. From the *incremental* model we used the parallel development for parts of the process, where one person worked with a specific part of the game, while the other developed something else entirely. This separation allowed us to be a lot more effective in the development process, as we were able to double the amount of work done in a time period. The *waterfall* model is a process model where a set of phases are followed one after another. On the basis of the limited time and resources, we utilised a limited version of these, using only the design, implementation and testing phases.

6.4.2 Elixir

"*Elixir is a dynamic, functional language for building scalable and maintainable applications. [...] Elixir is successfully used in web development [...] across a wide range of industries*"[8], and as we already had extensive knowledge of the language, the choice was made early on. As the language is easy to learn, and requires little boiler plate code to make a functional demo, it was the perfect fit for this prototype.

By using the provided frameworks and tools, one can have a simple web application up and running in a production environment in a matter of hours.

Phoenix LiveView

Phoenix is a web-framework for Elixir[9] which enables the developer easy access to functions and tools to make the development of a fully functional web backend in no time. `LiveView` "*provides rich, real-time user experiences with*

[8] `https://elixir-lang.org/`

[9] `https://www.phoenixframework.org/`

server-rendered HTML"[10] which provides the developer the neccessary tools to create server-side rendered web applications. Using these two frameworks together lets the developer create a full-fledged web application in one language and one code base. There is no need to differentiate the front- and backend code as they are tightly intertwined.

PubSub

"*PubSub is a realtime publisher/subscriber service for Phoenix web-apps*"[11] which enables the Phoenix Framework to send and receive messages from multiple clients at once. According to the Phoenix community, one single Phoenix instance is able to handle 2 million concurrent websocket connections while still keeping a 1 second broadcast time between the connected clients[44].

As the prototype was both a single player game, and a two player cooperative game, some communication between connected clients had to occur. When player 1 moved, this had to be replicated on player 2's screen, such that the experience would be that of a cooperative game. PubSub delivered this functionality by having the clients that were playing on the same instance of the game subscribe to the same topic. When one player moved, PubSub broadcasts this movement to all other clients on the same topic, and a *handle_info* function replicates the movement for these clients. This program flow can be seen in Figure 6.4.

Ecto

As the game stored the answered questionnaire questions, as well as the challenge answers, a static storage solution had to be implemented. However, as the data collected inherently relates to one and other, that being the player ID with the answered questionnaire questions, or the player ID with the answered challenge questions, a Relational Database Management System had to be supported in the chosen language and framework.

This is provided in Elixir by using the standard database framework, complete with drivers for the most popular RDBMS, called Ecto[12]. By using Ecto with the chosen RDBMS, described in section 6.3.3, the only implementation the developer needs to do is set up the relevant `schemas` and database queries.

6.4.3 PostgreSQL

"*PostgreSQL is a powerful, open source object-relational database system [...] strong reputation for reliability, feature robustness, and performance*". By using a robust and easy to use database system to store collected data from the user testing, it will be manageable to structure and export the data as we see fit.

[10] `https://hexdocs.pm/phoenix_live_view/Phoenix.LiveView.html`
[11] `https://hexdocs.pm/phoenix_pubsub/Phoenix.PubSub.html`
[12] `https://hexdocs.pm/ecto/Ecto.html`

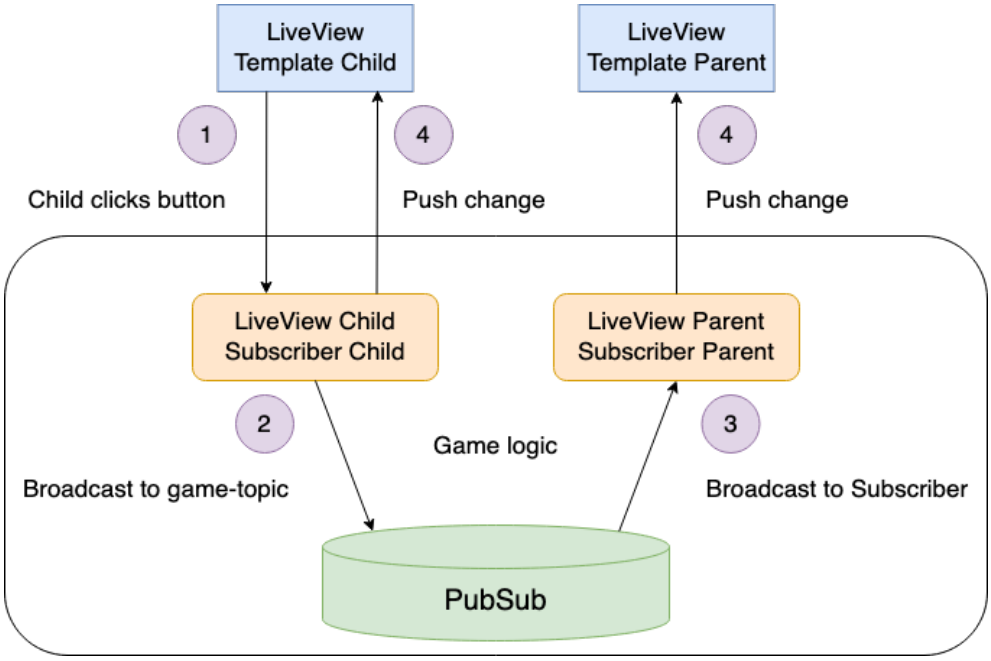


Figure 6.4: Game loop and control flow of the prototype

However, a good database system is only as good as the table structure we create. As such we planned the structure carefully to be able to extract the relevant data in a controlled and proper manner. The proposed database structure can be seen in Appendix F.

6.4.4 Heroku PSQL

The Heroku PSQL CLI gave the developer access to the remote PostgreSQL database from the terminal. It functions like a locally installed PostgreSQL CLI, and is meant to be used for database management and data extraction without having to install third party tools.

We constructed several queries to extract the data needed for this thesis. Code listing 6.1 shows an example where we extracted the combined set of the answers given in the pre-questionnaire with the answers given in the post-questionnaire. As we only wanted to see the development from before and after gameplay, we only extracted the answers from player who submitted both questionnaires.

Code listing 6.2 however, shows the `SQL` query for extracting only the game feedback questions with the amount of answers for each option.

Code listing 6.1: Extraction of pre- and post-questionnaire answers

```
select max(qq.questioneer_type) as type,
       qq.header                as question,
       qa.answered_value        as answer,
       qqo.id                   as option_id,
       qqo.text                 as option_text,
       count(*)                 as total
from questioneer_question as qq
inner join questioneer_answer as qa
  on qa.questioneer_question_id = qq.id
inner join questioneer_question_option as qqo
  on qa.questioneer_question_option_id = qqo.id
inner join game_player as gp
  on qa.game_player_id = gp.id
where gp.id in
(
  select gp.id
  from game_player as gp
  inner join questioneer_answer as qqa1
    on qqa1.game_player_id = gp.id and
       qqa1.questioneer_type = 'PRE'
  inner join questioneer_answer as qqa2
    ON qqa2.game_player_id = gp.id and
       qqa2.questioneer_type = 'POST'
  group by gp.id
) and
(qq.id in (
  select qqpre.id
  from questioneer_question qqpre
  inner join questioneer_question qqpost
    on qqpre.header = qqpost.header
  where qqpre.questioneer_type = 'PRE' and
        qqpost.questioneer_type = 'POST'
  group by qqpre.id, qqpost.id
) or qq.id in (
  select qqpost.id
  from questioneer_question qqpre
  inner join questioneer_question qqpost
    on qqpre.header = qqpost.header
  where qqpre.questioneer_type = 'PRE' and
        qqpost.questioneer_type = 'POST'
  group by qqpre.id, qqpost.id
))
group by qq.header, qa.answered_value, qqo.id, qqo.text
order by qq.header
```

Code listing 6.2: Extraction of game feedback

```
select qqpost.id          as question_id,
       max(qqpost.header) as question,
       qo.id              as question_option_id,
       qo.text            as question_option,
       count(*)           as count
from questioneer_question qqpost
left join questioneer_question qqpre
  on qqpre.header = qqpost.header and
     qqpre.questioneer_type = 'PRE'
inner join questioneer_answer qa
  on qa.questioneer_question_id = qqpost.id
inner join questioneer_question_option qo
  on qo.id = qa.questioneer_question_option_id
where qqpre.id is null
group by qqpost.id, qo.id;
```

6.4.5 Version Control

To be able to easily share the code between us, as well as enabling version control and support for the CD/CI discussed in section 6.3.2, we chose to use `git`[13] through the premium version of `GitLab`[14] provided by the university. By using this platform, our supervisor and co-supervisor could easily see the progress done throughout the development phase. Furthermore, it enables the continuation of the prototype after the project is finished.

6.4.6 Visual Studio Code

Any development phase needs a good and reliable code editor to be efficient and structured. We normally use Visual Studio Code[15] on a daily basis, and it was an easy choice for this project. The application is tightly integrated with both git and a numerous of programming languages, enabling fast and easy code completion.

[13] `https://git-scm.com/`
[14] `https://about.gitlab.com/`
[15] `https://code.visualstudio.com/`

Chapter 7

Results

This chapter presents the results from this master thesis. First the prototype will be presented in its entirety as it stands at the time of writing, and how it conforms with the design decisions explained in section 6.1, and how the different requirements and quality attributes, presented in section 6.2, were used in the final product. Afterwards, the results from the user testing is presented and evaluated.

7.1 Prototype

This section presents the prototype as it is at the time of writing this report. We will first describe a full playthrough of the game, where each step is explained through both text and imagery. Afterwards, we will look at how the prototype compares to the initial plans described in chapter 6.

7.1.1 Playthrough

The prototype can be viewed, tested and played at `cybsecmaster.herokuapp.com`, and it is available on any device with an active internet connection. By utilising the Mobile First design strategy, as discussed in section 2.3, the game is playable on all mobile, tables, laptops and desktop computers. The game screen as seen on a mobile device is depicted in Figure 7.1, on a tablet in Figure 7.2, and on a desktop in Figure 7.3. One can easily see that it is usable and enjoyable on all screen sizes. All further images of the game in this report will be screenshots from an iPhone 11 Pro.

When first navigating to the game URL, the player is presented with the welcome screen seen in Figure 7.4a. This screen contains information on how to play the game cooperatively with another player, as well as general information about the project. The full consent form of the game can be viewed in Appendix G. The players is prompted to enter their game name as well as a optional game ID. The game ID is used to connect to an existing game to enable cooperative play.

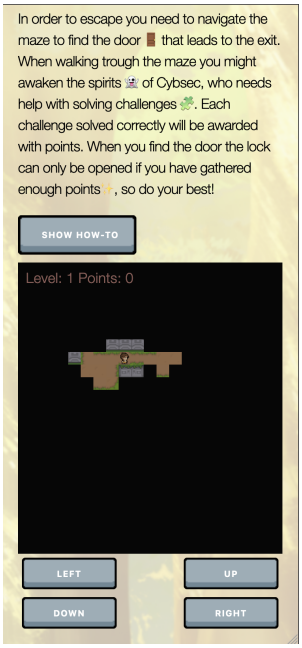


Figure 7.1: The game screen as seen on a mobile device

After entering their chosen name and game ID, the user is sent to a loading screen, as seen in Figure 7.4b. The game is now loading in the necessary assets to be playable, such as the music and sound effects. When the loading is finished, the pre-questionnaire is presented, which can be seen in Figure 7.4c. The player answers and fills out this questionnaire before the gameplay starts. The pre-questionnaire is the first data collection we do, and it is used to get the general demographic of the testers, as well as to be able to see if the game enhanced the players knowledge and awareness around cybersecurity risks.

When all questions are answered, the player is prompted to enter the game by clicking a button at the bottom of the page. The player is sent to the main game screen, depicted in Figure 7.1, Figure 7.2 and Figure 7.3, depending on the device the game is played on. The main game screen is where the player actually plays the game, and it is done by either using the arrow keys on a keyboard, or pressing the direction keys directly below the game screen. While navigating around the maze, there is a chance that the player will encounter a spirit. Each spirit has their own unique challenge they need help with. When such an encounter happens, the challenge pop-up is displayed, which is shown in Figure 7.4d.

The player reads the challenge, and chooses what they think is the most correct answer. After submitting an answer, the game tells the player which of the provided choices were correct, and which were incorrect. The correct choices are coloured green with a check mark trailing them, while the incorrect choices are coloured red with an *X* trailing them. The feedback is depicted

Figure 7.2: The game screen as seen on a tablet

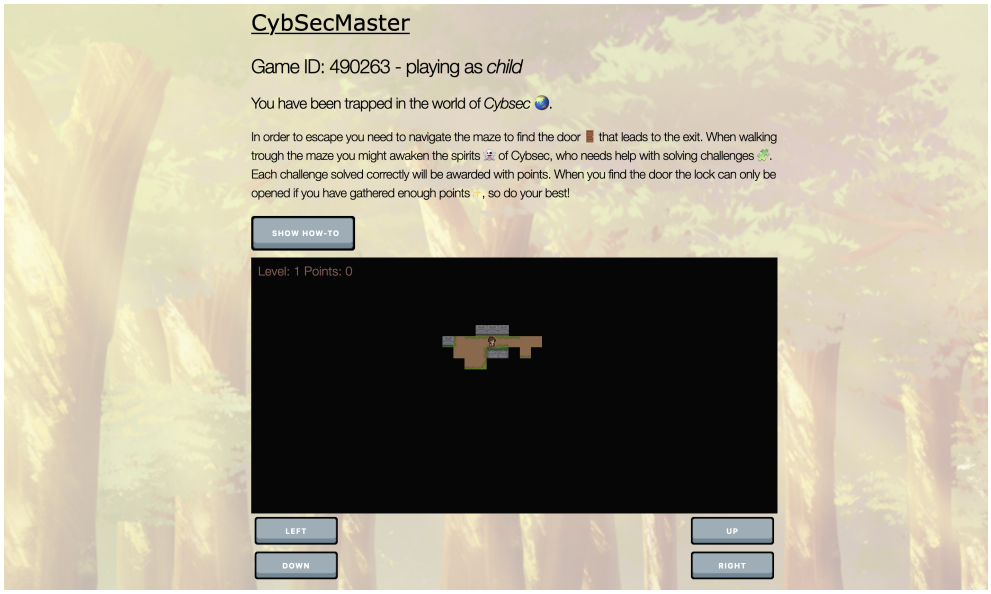


Figure 7.3: The game screen as seen on a laptop or desktop computer

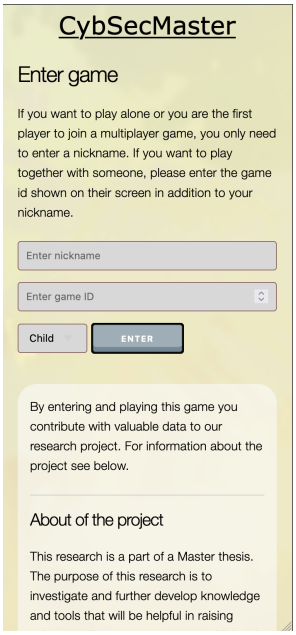
in Figure 7.5a. The answers given on these challenges are the second data collection within the game. The challenge pop-up disappears when the player presses the "OK" button, and they are free to move within the maze again.

For each correct answer given on a challenge, the player is rewarded with points. When the player has amassed a total of 60 points, they can navigate to the door located at a random spot within the map. When near the door, a sound will play and the door slowly opens, which enables the player to proceed to the next level.

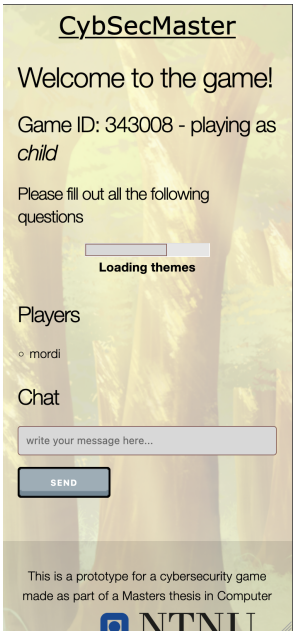
The process described above is the main game loop, and the player has to amass 60 new points in level 2 to finish the game. After completing enough challenges to open the door in the second level, the game is finished. The player is then presented with the post-questionnaire which encourages the player to reflect on their game session. This questionnaire can be seen in Figure 7.5b. The post-questionnaire is the last data collection we conduct.

7.1.2 Plan vs. Execution

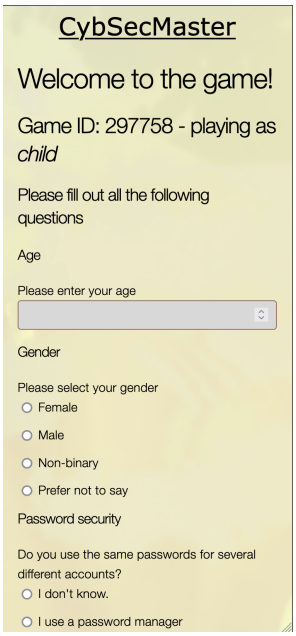
As the scope of the project was limited in both time and resources we did not manage to implement all elements discussed throughout chapter 6. The following sections will look at each element in turn, and evaluate the planned implementation with the finished prototype.



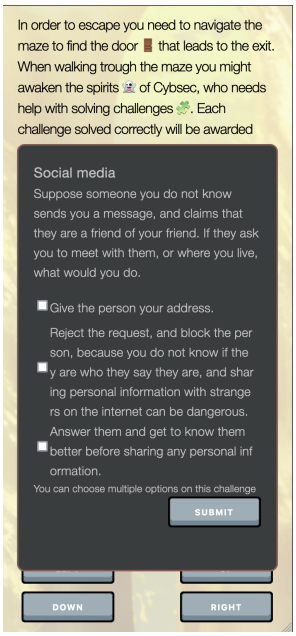
(a) Game: welcome screen



(b) Game: loading screen

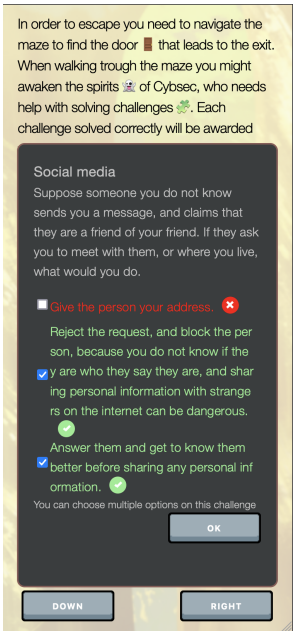


(c) Game: pre-questionnaire screen

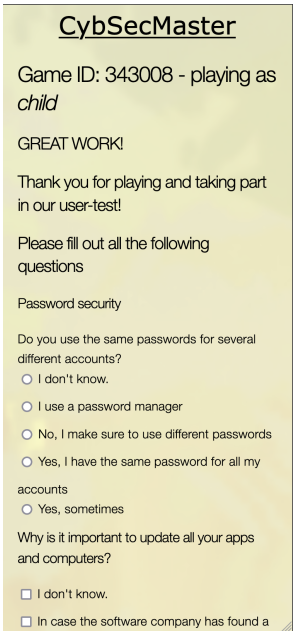


(d) Game: challenge screen

Figure 7.4: Game screens 1



(a) Game: challenge screen answers



(b) Game: post-questionnaire screen

Figure 7.5: Game screens 2

Story

The story was kept short and simple, and did not exclude nor include parts not mentioned in subsection 6.1.1. As the story was mysterious, but not outright scary, it conformed with the target audiences context. The story did not contain any unfamiliar elements, or complex twists such that the story made sense within the rest of the game.

Theme and Atmosphere

As with the story, the theme and atmosphere had mysterious elements to it. The layout of the maze was unknown, the chosen colour scheme was gloomy, and the spirits roaming the maze created a suspense for the players. However, we initially wanted to implement actual roaming spirits within the maze that the player had to actively search for, but as this task proved to be difficult to manage within the set time frame, the encounters were decided at random for each move.

Feedback

It was mentioned in both section 5.1 and subsection 6.1.3 that both visual and auditory feedback is important for the immersion and playability of a game. The sounds chosen fit the context of the game, and using different sounds for

different actions enhanced the variety of the game. Furthermore, by implementing animations on both the challenge pop-up and the opening of a door reinforced the player that their actions have meaning and consequences. However, as mentioned in section 7.1.2, time constraints limited us on how many animations and sounds we could implement. As such we decided to implement the most impactful and visible feedback to get the most out of the time we had.

Game Mechanics

Since game mechanics are what drives a game, they got the highest priority during development. By focusing on having a stable and working cooperative option, we enabled the parents or guardian, and the child to play together and experience the game as a team. Furthermore, by having simple and easy to understand rules, the younger parts of the target age group were not ostracised from the game, and their parent could assist when needed. Lastly, by implementing a fog of war system, described in section 6.1.4, the player would be encouraged to explore the maze, and the system contributed to keep the mysterious atmosphere of the game.

Requirements

In a more traditional setting, a natural counterpart to the list of functional requirements is a test-report. Given the scope of this project the number of functional requirements was quite low, and the test-report is summarised in Table 7.1.

ID	Requirement	Priority	Status
FR1	The player should be able to play cooperatively together with another player	High	Implemented
FR2	The player should easily be able to find instructions for how to play the game	High	Implemented
FR3	The player should be able to communicate with the other player	Low	Implemented
FR4	The player should be presented with different challenges when navigating the maze	High	Partly implemented
FR5	The player should be able to play alone	Medium	Implemented
FR6	The player should be shown their score throughout the gameplay	Medium	Implemented
FR7	The game should have several levels	Medium	Implemented
FR8	The player should see a graphical representation of where the challenges are inside the maze	Low	Not implemented
FR9	The player should get visual and auditory feedback on actions and progress	High	Partly implemented

Table 7.1: The functional requirements of the prototype and their implementation status

Similarly, the test-report for the quality attribute scenarios is shown in Table 7.2, highlighting the responses, response measures and implementation status.

ID	Response	Response measure	Status
QA1	The player should be able to play cooperatively together with another player	< 5 seconds	Implemented
QA2	The player should be able to start a single player game	< 5 seconds	Implemented
QA3	The player should have easy access to instructions on how to play the game	Familiarised with game mechanics in less than 3 minutes	Implemented
QA4	The player should easily be able to join a multiplayer session in a game started by another player	< 30 seconds	Implemented

Table 7.2: Implementation and testing status of the quality attribute scenarios

7.2 User Testing

The user test of the prototype was conducted during the spring of 2022. The participants played the game and answered the questionnaire online, as to increase the number of participants. The test utilised a Bring Your Own Device (BYOD) strategy where the participants played the game on the device that suited them best. This section presents the results from the user test. We will first look at the demographic data collected, such as gender and age, followed by the general feedback we received from the participants on what they thought and felt about the game. Lastly, we will present the answers from the pre- and post-questionnaire.

7.2.1 Demographic

There were a total of seven participants that completed one whole play through of the prototype during the user testing, which entails that they answered the pre-questionnaire, followed by completing both level 1 and 2. Lastly, the testers completed and submitted the post-questionnaire.

As seen in Table 7.3, there were four children and two parents or guardians that completed the user test, as well as one who did not want to disclose their age. All children were within the target age group, and the two guardians completed the game with their child in a cooperative manner.

Participants	**Age**
1	9
3	12
1	37
1	46
1	Not disclosed

Table 7.3: Age of participants

Of these seven participants, Table 7.4 shows that five were male, and two were female. One of the parents were male, and the other was female, such that four children were male, and the remaining child was female.

Participants	**Gender**
5	Male
2	Female

Table 7.4: Gender distribution among participants

7.2.2 Game Feedback

During the post-questionnaire we asked the participants to rate aspects of the user test and prototype using a five-point Likert scale. The ratings are presented as star-ratings in Figure 7.6.

As seen in Figure 7.6a the game received positive feedback on what the users thought of the game after playing it. Three users thought it was neither good nor bad giving the game three stars, while two gave it four star, while the last two gave the game all five stars.

Looking at how fun the players felt the game was, Figure 7.6b shows that a majority felt it was averagely fun to play, while one participant thought it was not fun at all, giving the game one star. However, the last participant felt the game was very fun to play, and gave it the maximum amount of stars.

When the participants rated how fun the cooperative element of the game, the results were mixed. As shown in Figure 7.6c, two participants stated they played alone which makes the cooperative element moot. However, one user gave the multiplayer aspect all five stars, while another participant gave it four stars. These participants liked playing together with their child or parents. Two other participants felt the cooperation was average, using three stars, while one participant did not care much for it and gave it two stars.

We were also interested in how much the players felt they had learned by playing the game. As such, we asked them to rate their own learning outcome as shown in Figure 7.6d. The majority of participants submitted four stars, meaning they felt they had learned a good amount from playing the game. One participant rated their learning outcome with only one star, which could indicate that they did not learn anything new, or learn anything at all from the prototype. The last two participants gave this question two and three stars respectively, which indicated that one felt they learned more than the other.

To measure player retention to our solution, we tasked the user testers with rating how much they would like to play the same game again, but with more added features, challenges and levels. This question received overwhelmingly positive feedback, as five participants have the question four stars, while one other gave it all five stars. Only one participant submitted a three star answer.

As seen in the above discussed feedback on the game from the participants, the game was enjoyable for the majority of testers. The testers felt it was fun to play and that they learned from it. Moreover, all participants were positive to playing the game another time if it was further developed with more features, challenges and levels. This positive feedback bodes well for gamified cybersecurity learning among children.

However, as the cooperative element received the most mixed feedback of all questions, it will be a good idea to have a game with optional multiplayer.

(a) What did you think of the game?

(b) How fun was the game?

(c) How much did you enjoy playing with your parent/sibling/child?

(d) How much do you feel you learned by playing this game?

(e) How much would you like to play this game again, but with more features, challenges and levels?

Figure 7.6: Feedback on the game from user testing

7.2.3 Questionnaires

The main data collection in this thesis was the pre- and post-questionnaires. As explained in subsection 4.3.2 the pre-questionnaire was presented to the player before starting the game and consisted of demographic questions as well as questions regarding different cybersecurity risks. The post-questionnaire was presented after the player had finished level 2 and contained the questions discussed in subsection 7.2.2 followed by a repeat of the cybersecurity questions in

the pre-questionnaire. These questions were repeated to enable us to see if the game had improved the players cybersecurity knowledge and awareness. All of the repeated questions were multiple choice questions. This section presents the results from these specific questions in turn.

Figure 7.7 and Figure 7.8 depicts all the results from these questionnaires. The blue bars represent the pre-questionnaire answers, while the orange bars represent the corresponding post-questionnaire answers.

Looking at Figure 7.7a we can see that one participant learned that large social media companies always knows something about a person as they changed their answer from "*They know nothing about me*" to another answer. However, we see a reduction in the option containing the most information.

The results on the question regarding password security, seen in Figure 7.7b, suggest that there is almost no change between before and after playing the game. However, we see that one participant changed his answer to "*I dont't know*". While there is little change in these answers, it is surprising to see that several participants use a password manager as this is the most secure and recommended form of password security.

Regarding what happens to the pictures when one deletes them from social media sites, we can see that most participants are aware that the pictures are not entirely removed from the internet when they are deleted. Most participants know that social media companies keeps the pictures while hiding them from you, while two participants believe they are deleted if they cannot see them. It does, however, look like the game put forth the notion that the companies sell the pictures as the answer count for this option rose by one. Lastly, one participant answered "*I don't know*" in the post-questionnaire.

A majority of the participants knew that by giving out a lot of personal information can be used against you. According to the results shown in Figure 7.7d five participants believed people can order fake ids and set up fake accounts in your name, while four participants believed one could more easily guess their passwords if they were weak. However, we do see a concerning rise in the more incorrect answers in the post-questionnaire as one fewer participant chose the more correct answers above, and one believed that the people could not do much by having your personal information. Furthermore, the "*I don't know*" option was chosen by one participant in the pre-questionnaire, while two participants chose this option in the post-questionnaire.

To further gauge the safety awareness among the participants, we asked them to choose which of the given methods were considered multi-factor authentication methods. As we can see in Figure 7.8a there was no change between the pre- and post-questionnaire. Four participants knew that a one-time code received through SMS or email was a multi-factor authentication method, while one participant knew that a biometric scanner was another. However, one participant thought that a strong password was enough to be considered multi-factor, while two participants did not know.

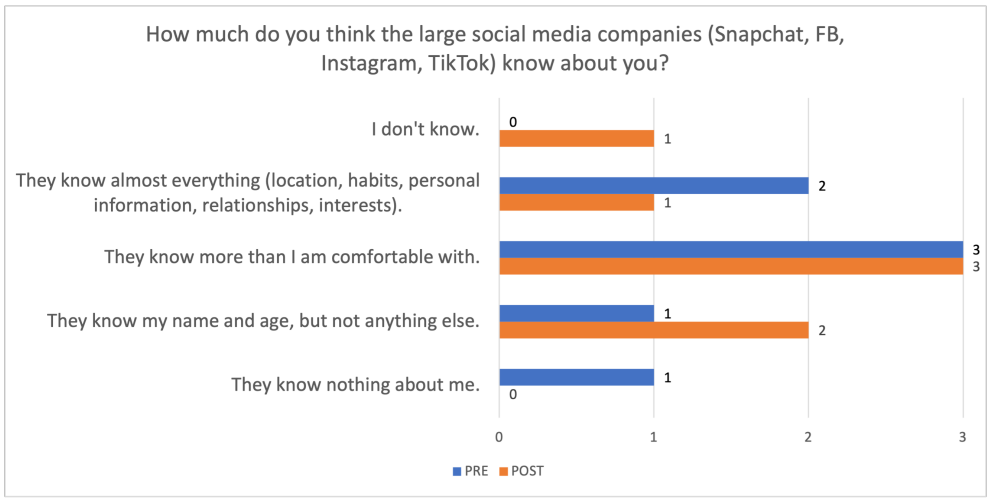
Figure 7.8b shows why the participants believe it is important to keep their

devices and apps up to date. We can see that the majority of the participants knew that the software company delivered updates to patch security issues in their software, and two participants updated their apps to get the newest features. Both of these options saw an increase with one answer in the post-questionnaire compared to the pre-questionnaire. Non of the participants believed that it was not important to update their apps, while one participant answered "*I don't know*" on both questionnaires.

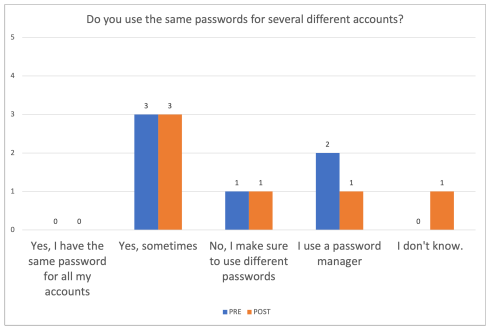
Lastly, we asked the participants what they though was correct about people they did not know online, and this question had some interesting results. As seen in Figure 7.8c five participants believed that most people are not bad, but there are always someone who can be evil, which is reflected by three participants believing some people online can have criminal intentions. Both of these options were chosen by the same number of participants in both the pre- and the post-questionnaire. However, the three remaining options were chosen by one participant each in the post-questionnaire. One participant thought people online are usually friendly, while another believed they had bad intentions. Lastly, one participant did not know what they thought was correct about people they do not know online.

Figure 7.9 and Figure 7.10 shows the same diagrams as above, but they contain only the answers given by the children who finished the game, while Figure 7.11 and Figure 7.12 depicts the parents answers. We can see that the children fluctuate more between their pre- and post-questionnaire answers than the parents. The parents are stable, and usually chooses the same option for each question. Looking at Figure 7.9a more participants chose the more correct options in the post-questionnaire, which is also true for all Figure 7.10a, Figure 7.10b and Figure 7.10c. The diagrams shown in Figure 7.9b and Figure 7.9d are unchanged between the pre- and post-questionnaire, while Figure 7.9c shows that one participant believed the social media companies sell their pictures in the post-questionnaire. There is, however, one change in all but two of the children's diagrams and that is the fact that one participant answered "*I don't know*" on all questions.

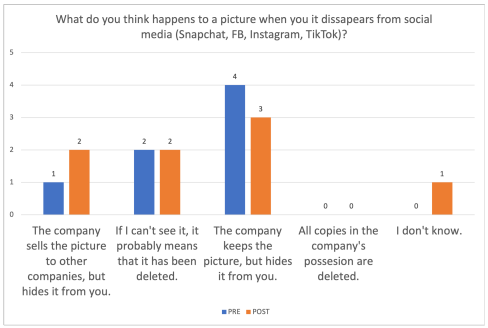
As mentioned above, the parents answers are unchanged throughout the questionnaires. However, it is apparent that one adult participant did not complete the entire post-questionnaire as some questions are lacking enough answers compared to the corresponding pre-questionnaire question.



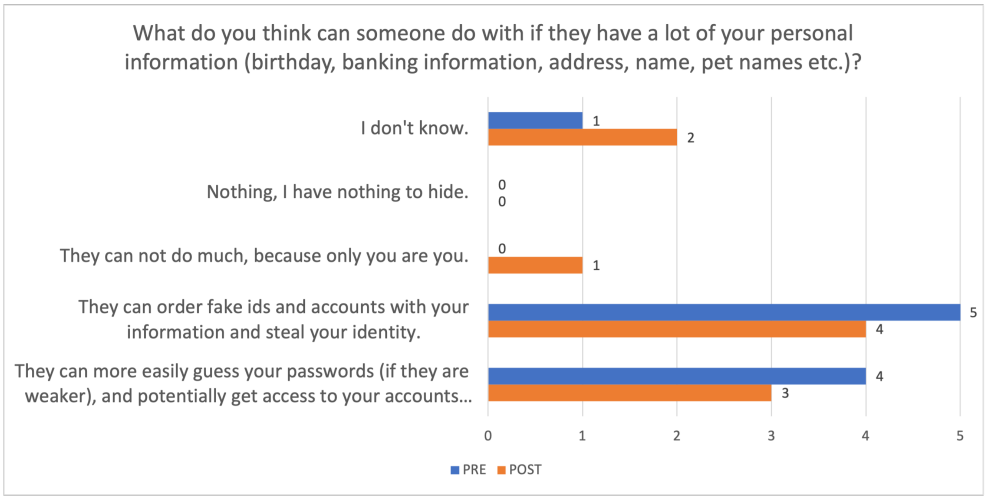
(a) Answers relating to social media



(b) Answers relating to password security

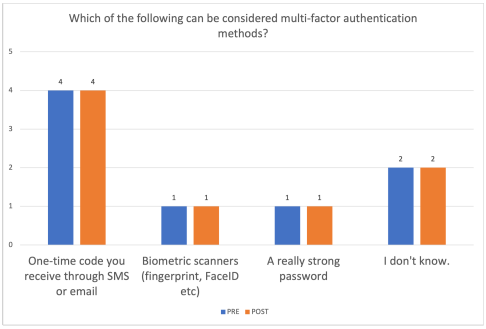


(c) Answers relating to privacy and social media

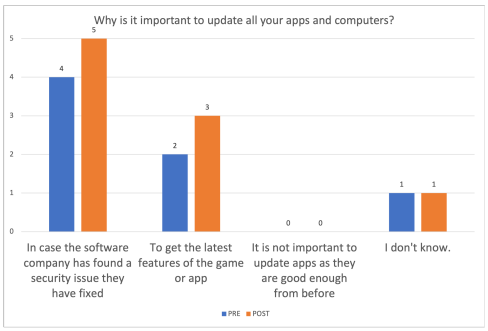


(d) Answers relating to privacy

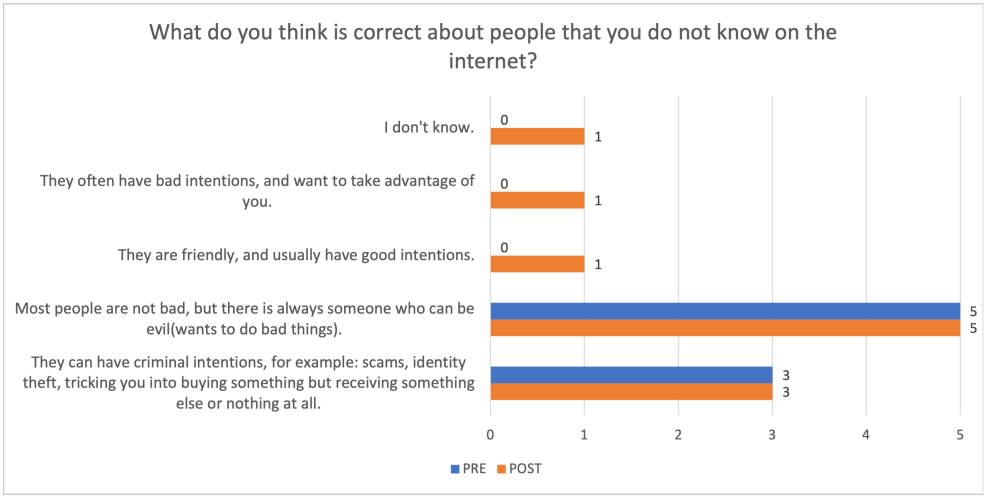
Figure 7.7: Result set 1 of all pre- and post-questionnaire answers



(a) Answers relating to multi factor authentication

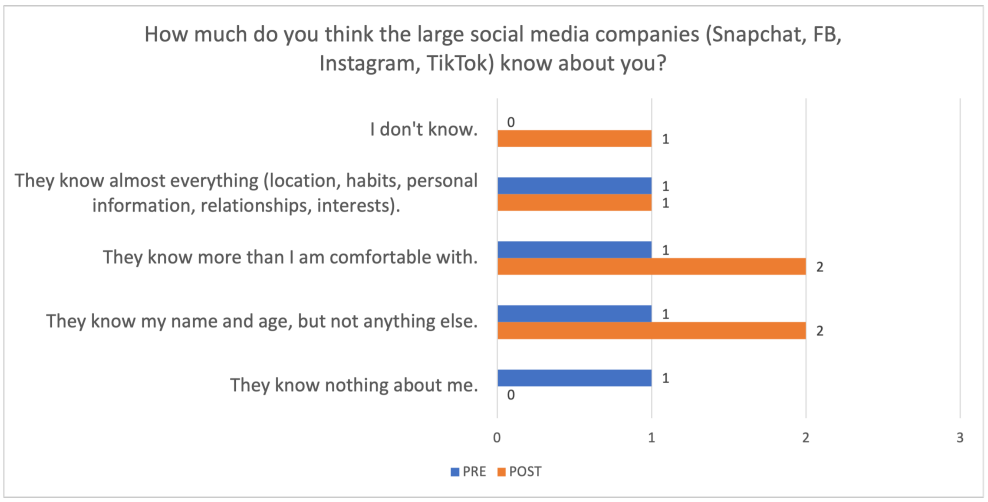


(b) Answers relating to updates and patches

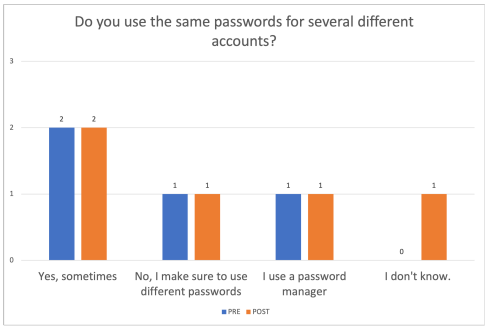


(c) Answers relating to stranger danger

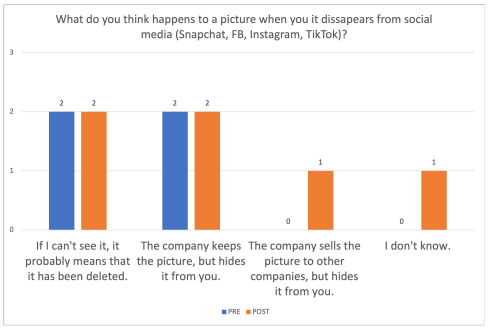
Figure 7.8: Result set 2 of all pre- and post-questionnaire answers



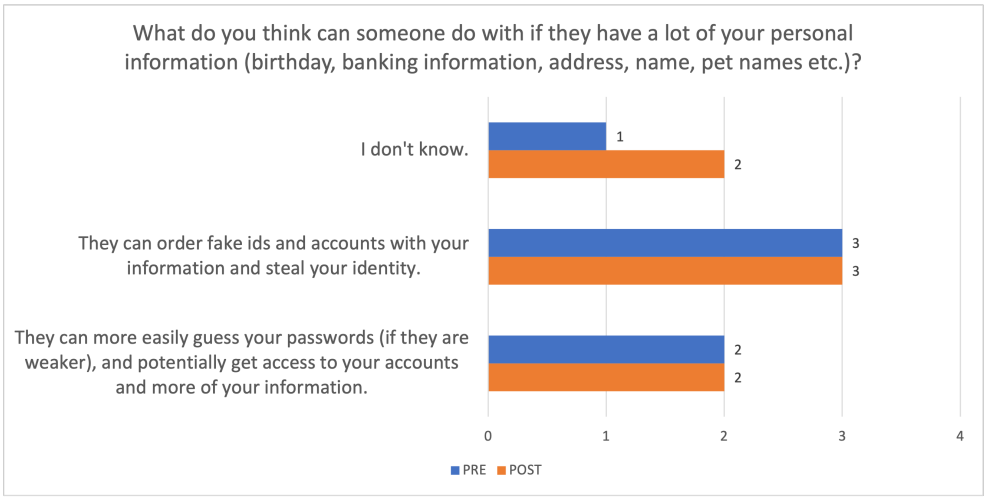
(a) Children's answers relating to social media



(b) Children's answers relating to password security

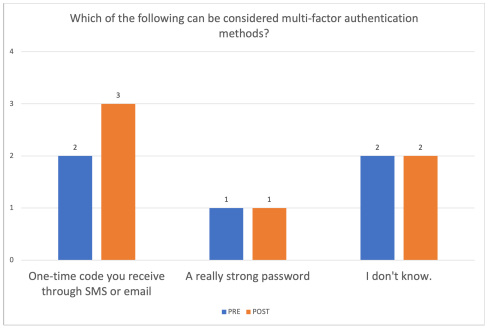


(c) Children's answers relating to privacy and social media

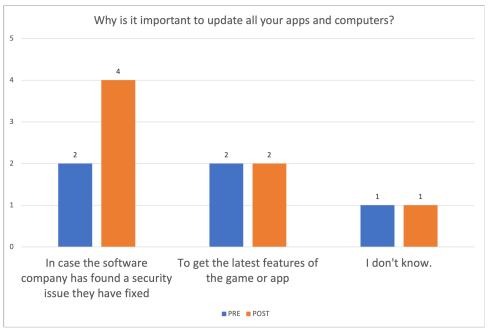


(d) Children's answers relating to privacy

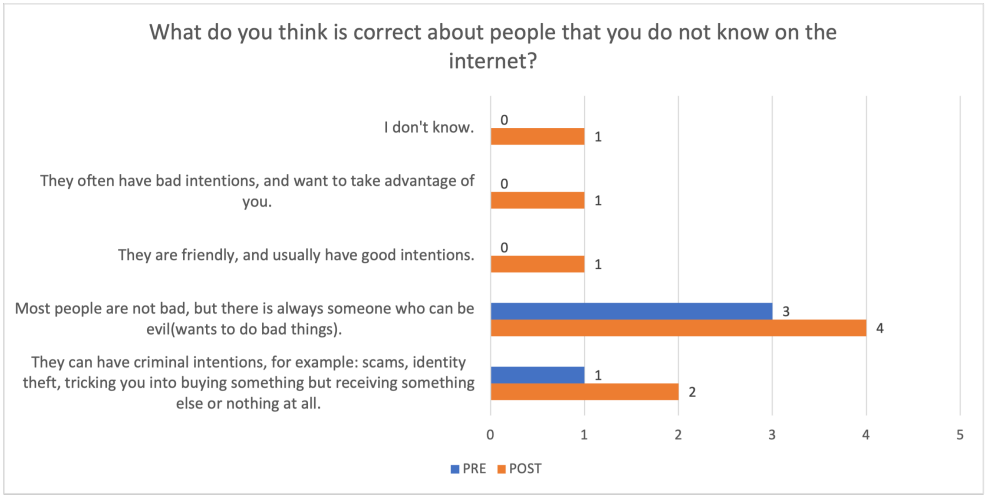
Figure 7.9: Result set 1 of pre- and post-questionnaire answers from children



(a) Children's answers relating to multi factor authentication

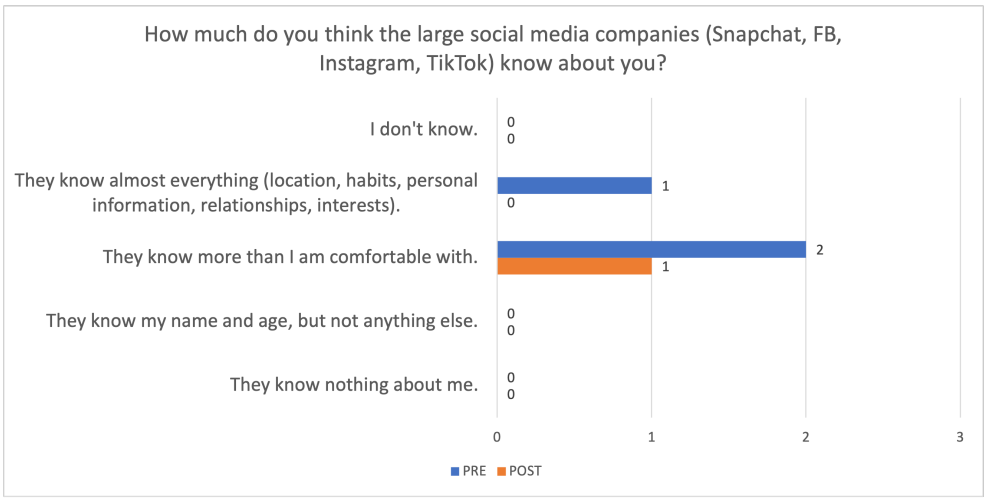


(b) Children's answers relating to updates and patches

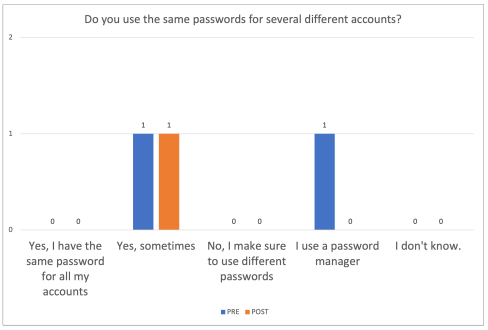


(c) Children's answers relating to stranger danger

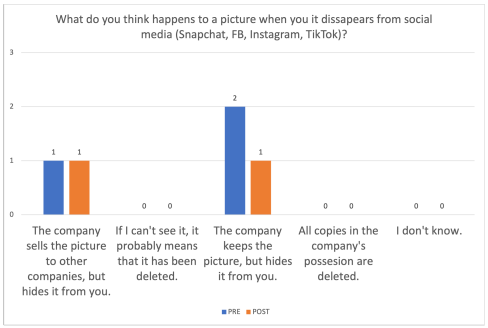
Figure 7.10: Result set 2 of pre- and post-questionnaire answers from children



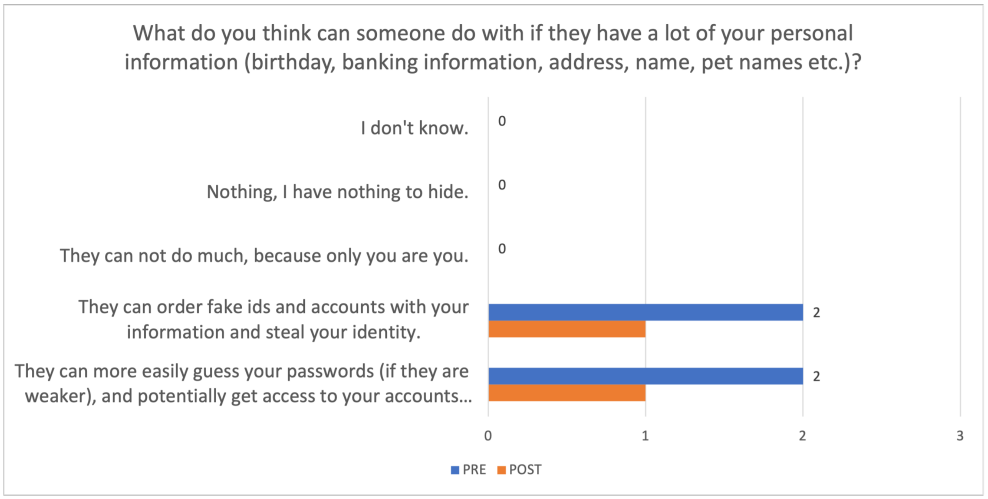
(a) Parent's answers relating to social media



(b) Parent's answers relating to password security

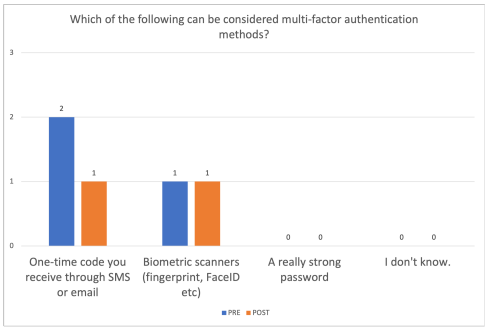


(c) Parent's answers relating to privacy and social media

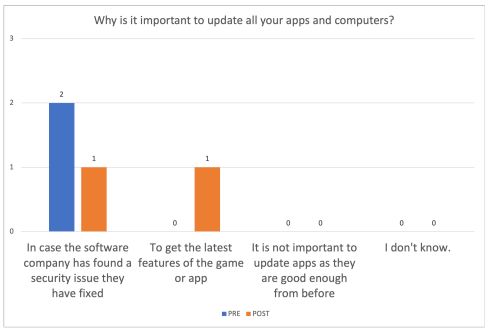


(d) Parent's answers relating to privacy

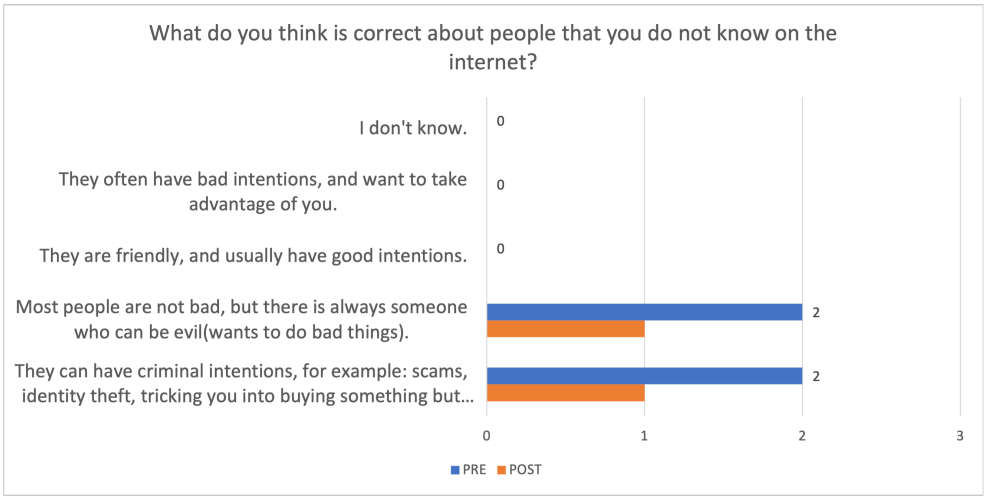
Figure 7.11: Result set 1 of pre- and post-questionnaire answers from parents



(a) Parent's answers relating to multi factor authentication



(b) Parent's answers relating to updates and patches



(c) Parent's answers relating to stranger danger

Figure 7.12: Result set 2 of pre- and post-questionnaire answers from parents

Chapter 8

Discussion

In this chapter we will discuss the ethics, RQs, results, struggles and challenges, and limitations of the project.

8.1 Ethics

Article 12 in the United Nations *Convention on the Rights of the Child* states that "*States Parties shall assure to the child who is capable of forming his or her own views the right to express those views freely in all matters affecting the child, the views of the child being given due weight in accordance with the age and maturity of the child*"[45]. Since part of the target audience for our prototype were children between 9 and 13 of age we wanted to include the children in the research process. However, as Prevention of Cruelty to Children [46] outlines: "*there must be a balance between the needs of the research and the need to protect children from harm*", and as such we had to take great care in how we involved the children. When conducting research regarding the younger generation, it is important to assess the potential harmfulness and impact the research will have on their lives. As the research done in this master thesis is focused on children playing a game with their parents, we see no indication of harmfulness in the process. The questions served to the children were non-agitating, neutral and used a non-offensive language. Furthermore, the art style and audio were mysterious and pleasant. Based in the feedback from the children, they liked the game.

Furthermore, Bratteteig and Wagner [47] states that "*the biggest ethical challenge for researchers working with children is the disparities in power and status between adults and children*". As these disparities were present during both the workshop and the user testing, we took great care on levelling with the children and doing the process on their term while using their language. We gave as much information as we had, and as much attention as the children needed. By also having the parents present at all times, the child felt safe and not uneasy in the testing situation. Moreover, researching and user testing a

game meant for children is difficult if the target audience is not present in the process.

8.2 Designing a Game to Raise Cybersecurity Awareness for Both Children and Adults

As this thesis is grounded in the RQs presented in section 1.1, we want to clearly present the findings for each of these. This section presents the answers for **RQ1** and its related **SRQ**s.

It is difficult to create a game that is accessible and enjoyable for a large audience, and as children and parents are form very different generations, this age gap is substantial. As such the game design has to be universal, familiar and relevant for the whole target audience. However, by instructing the parents that this is for their child's own good, they will be encouraged and enticed to contribute as they want the bast for their own children. Furthermore, one can market the game as a family game, such as Monopoly, and express that the game is for all ages.

One can also include the children's older siblings or friends in the process, as a replacement for the parents. The age difference between the target children and their older sibling or friends is lower than that between the child and their parent, and as such the game feel more relevant to the older sibling.

Appropriate Game Designs

To make the game appropriate for children and adults alike, it is important to focus on what is appropriate for the children in the target audience. The children are young and as such what is appropriate for them is more narrow than what is appropriate for their parents. As such, one has to understand the context and culture the target children are from and are used to. Furthermore, as one wants the children to learn from the game, it is important to increase player engagement such that the players plays the game for a longer period of time, and increase learning retention such that what is learned actually is remembered by the player.

The game has to pique the interest and curiosity of the player to enable exploration and experimentation. As such, information given has to be presented in bits and pieces, and let the player stitch the pieces together themselves, which will again increase the players confidence in themselves for solving problems within the game.

Furthermore, it is important to reward the player generously when they do a correct action, and not punish them severely when doing an incorrect action. It is, however, useful for the player if they are notified that the action they preformed was incorrect, as to deter them from doing it later.

By anchoring the game in the ARCS model of motivation, the player engagement will increase the players attention, context and culture will increase the relevance of the game, problem solving will increase the players confidence, and rewarding points will increase the players satisfaction with the game.

Essential Game Design

The game designs mention in section 8.2 are a collection of appropriate game designs, however, there are some designs that are essential for creating a successful cybersecurity awareness game for children and adults alike.

By focusing on choosing game elements and game mechanics that conform with the target audiences culture, one can derive a set of elements and mechanics that will fit within the target audience. Furthermore, by understanding the context the game will have within the culture, one is able to know what is familiar to the audience.

With this familiarity, one has to derive a fitting story that conforms with the context and culture mentioned above. A familiar story the target audience can relate to and understand, will increase player engagement and the learning retention will be enhanced.

To make the game interesting, it is further important to use game elements, such as graphics, sounds and animations, that the player can relate to and understand. These factors will make the players feel more comfortable with the setting of the game, and see the game more as a game, rather than a learning platform.

As the mechanics chosen for the game is the underlying set of functions that makes the game run, they are equally important to focus on. Using familiar and relatable mechanics will increase the satisfaction the player has with the game.

All of the above mentioned culture, context, game elements and mechanics has to be familiar and conform with each other. Otherwise, the game will feel out of place for the players, and they will not engage with the game. All parts of the game has to become one whole together, such that all parts makes sense in the bigger picture.

8.3 Combining Adult and Child Learning to Raise Cybersecurity Awareness

To answer **RQ2** we have to look at the findings from both the SLR from chapter 3 and the results from the interviews and workshop presented in chapter 5.

As it became apparent in the workshop, it is very difficult to create a game that appeals to both children and adults while also including a learning aspect, where both groups can acquire knowledge. Many games made for adults are often too graphic or include content making the games inappropriate for children. Furthermore, many games made for children are too "childish", easy or

boring for adults.

Moreover, based on the findings of the workshop and the user testing, parents generally do not play games together with their children. Several of the parents sat with their children while the child played the game, and contributed passively.

To overcome the aforementioned obstacles, one can attempt to tailor the game experience, such that the challenges, obstacles, tasks or quests are relevant for each player based on if they are a child or a parent. On the other hand, there exists examples of universal games, made for both old and young people. As seen in Figure 8.1 Nintendo has created games that cover a wide range of ages. However, these games do not usually focus on the learning aspect of a game. Furthermore, they are created by huge corporations with decades of knowledge, experience and research within game development.

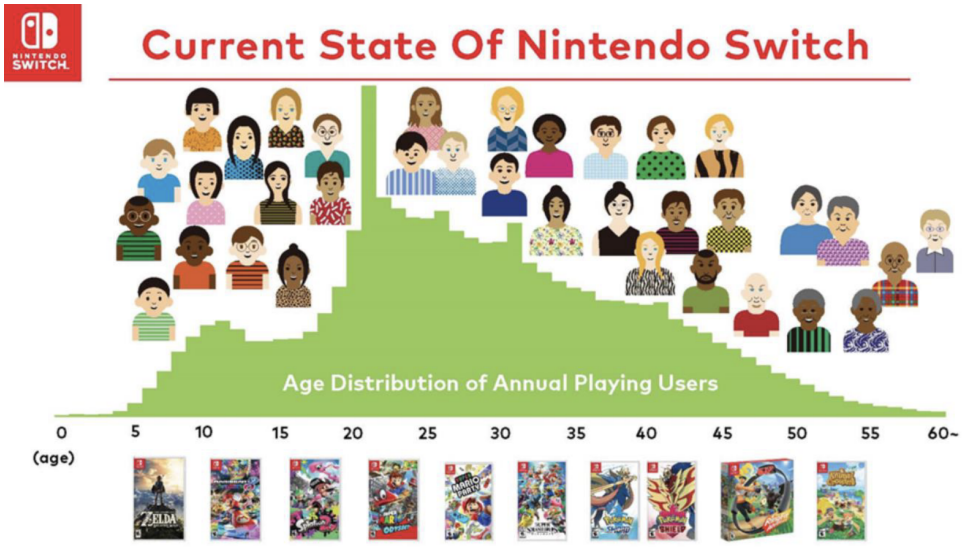


Figure 8.1: Age distribution of annual playing users [48]

8.4 Regarding the Results

This report has three main parts: the collection of data by conducting interviews and a workshop, the planning and development of a prototype, and the testing of said prototype. As the interviews, section 5.1, and the workshop, section 5.2, has already been discussed in their respective sections, this section will focus on the working prototype, and the results from the user testing. First we will discuss the prototype, followed by the user testing results.

Prototype

Taking the scope of this thesis and the time constraint we had into consideration, we are satisfied with the prototype we have developed. Using a familiar development process and technical stack enabled us to start developing faster, and get more features completed in less time than we would have used if the technology was unknown. As it is only the creativity that can stop such a development process, there are many more features, game mechanics and improvements to explore regarding the prototype.

However, as the game was just a prototype, some bugs and issues are to be expected. We received comments throughout the user testing, and worked hard to assist and fix game breaking bugs such that the participants were able to participate.

As experienced in the workshop, the younger part of the target age group may not have their own mobile device. As such we see it would have been beneficial to also have a game version that ran on different gaming consoles. Several of the participants in both the workshop and the user testing commented on this, and said that their child had access to a Nintendo Switch, Xbox or PlayStation, but not a mobile device. As such, some of the participants used their parents device to play the prototype. However, by choosing to develop a web-application using mobile first design principles, we mitigated parts of the above mentioned issue as these types of apps are inherently accessible via the internet. Furthermore, developing and supporting multiple versions of the same game is often twice the amount of work, as the platform and technologies does not necessarily conform with each other.

User Testing

By looking at the game feedback in Figure 7.6 in subsection 7.2.2, the majority of participants gave the gameplay and experience positive reviews. The only question that had no clear majority was the one regarding cooperative play, seen in Figure 7.6c. As only one parent completed the user test in its entirety, the responses to this question could mean that the parents did not actively play with their child in the same game session, but looked at and guided the child while the child played. Based on the findings of the workshop in section 5.2, the children would rather cooperatively play with their parents, rather than having them over their shoulder while playing. As such, the parents should have been guided to play alongside their children in the same game session.

But why did the parents only passively partake in the user test, rather than playing an active part? There are many possible answers to this, and to name a few we can look at other findings from the workshop. The parents believe their children want to play alone, as playing a game is the child's own hobby. This belief could lead the parents to let the child play alone, without asking if they could join. Furthermore, since not all children possess their own mobile device, they may have had to borrow their parents device, and as such hindered the

parents from actively playing. Moreover, it could be that our test instructions were lacking when expressing the importance of active participation from both child and parent. Since the user test was conducted online, we did not have the option to properly address the issue as it occurred. However, the feedback from the participants were not only negative regarding cooperation. Over 50% gave the cooperative question three stars or more, and as such shows that this is a viable solution for integrating parents in the cybersecurity learning process of children. Furthermore, all participants were eager to play the game another time, if more features, challenges and levels were added. This feedback indicates that the prototype has potential, and should be explored further.

Looking more closely on the answers given in the questionnaires, we can see that many participants already had good knowledge regarding cybersecurity risks. One even used a password manager for storing their passwords. As such, this type of game could have limited effect. However, looking at the other answers to the same password security question, seen in Figure 7.9b, the children do not practice the best password hygiene as two participants reuse the same password for multiple accounts. Children may not have the same relationship with user accounts and logins as older generations do. The parents may have set up the account without the child present, and chosen a password that would be easy for the child to remember. As such, the child could reuse the same password when they created another account themselves. This notion is further supported by the children's answers regarding multi-factor authentication as seen in Figure 7.10a. Only two in the pre-questionnaire and three in the post-questionnaire knew that a one-time code is considered a viable multi-factor authentication method, while non opted for the biometric option.

There is one trend in the children's results that stand out. One participant consequently answered "*I don't know*" on all questions in the post-questionnaire. There could be several reasons for this, and the two most likely are either that the child got bored of the game and just wanted to finish the user test, or that their parent was not present when they completed both levels to help them through the questions. As one participant was only nine years old their knowledge of English could be lacking. We experienced the same in the workshop with the younger participants. They needed more translation help and guidance then their older counter parts, and as such was too young to participate.

All of the above mentioned problems regarding the questionnaire answers could have a common reason behind them. Read and MacFarlane [35] stated that "*because a survey is, by definition, designed, it will always be restrictive*" and as such is difficult to create such that the answers are not the ones the designer of the survey wanted to get. Furthermore, we are not specialists in survey creation, and as such could be part of the problem. However, we did follow the guidelines presented by Read and MacFarlane [35] to make the questionnaire as accessible and understandable for the children as we could. Furthermore, questionnaires and surveys are a great way to collect a larger amount of structured data, and since we had limited time to collect and analyse this data, the

questionnaires became invaluable for our research.

8.5 Struggles and Challenges

All researchers encounter their own struggles and challenges at some point, and we are not different. The scope of this project became bigger than expected, and as such each struggle and each challenge were noticeable. Most of what was done during this master thesis was new to us. Everything from the required processes to the different methodologies used.

Before we could conduct the interviews with experts, we had to get clearance from the Norwegian Centre for Research Data, as explained in section 4.4. This process was cumbersome, as there was a lot papers to create and choices to make. Furthermore, due to NSDs processing time, we did not get an answer before three weeks had passed. This uncertainty made it difficult to set a time and place for the interviews as the interviewees were generally busy during the daytime.

Another challenge we encountered were the amount of work needed after the interviews were held. As we wanted the interviews to be as effortless as possible, we conducted them in Norwegian. The recordings each contained 45-60 minutes of interviews held in the local dialect of the interviewee. Having the recordings in Norwegian made the automatic transcript tool struggle, and we had to go through most of the interviews manually. Furthermore, as the analysis had to be done on English transcripts, we had to translate them after transcribing. The automatic translation tool worked better than the transcription tool, but we had to manually correct these as well. As such, the interview process was time consuming.

As stated in subsection 6.1.1 the story element of a learning game is highly important. As neither of us had the knowledge or skill to construct a compelling and fitting story, it was difficult to address this. Furthermore, we lacked the artistic skill do be able to construct a vibrant and engaging graphical world, but we are satisfied with the end product. As the scope of this thesis is limited, it was important to limit the scope of the prototype accordingly.

8.6 Limitations

We have seen several limitations emerge from the methods used in this project. The first, and perhaps most significant one, is the low number of participants in the workshop. Since children (and their parents) in the selected age group are often busy with recreational activities on week-day evenings, we aimed for conducting the workshop during a weekend, but the timing of the workshop meant that several of the weekends in question overlapped with national holidays, increasing the chances of people being occupied. Having only four participant groups made it possible for us to facilitate them more closely, but

it also limited the possibilities for quantitative data analysis and weakens the basis of our findings.

For the user testing we went for a different approach, designing it in a way that enabled the participants to test it whenever and wherever, as long as they had a device with a browser and an internet connection. Choosing this approach made the process of recruiting participants easier, but it also introduced a new limitation. By not requiring the participants to meet physically, the testing was done more or less without facilitation. Hence we ended up with most participants playing in the presence of their parent, but without their parent actively playing together with the child, resulting in only one complete data point for parents from the user testing. However, given the struggles we experienced with recruitment for the workshop, we think we managed to gather more data using this strategy for the user testing than what we would have accomplished with requiring physical attendance.

In addition, the user testing was done without any way for the participants of giving free-form feedback, outside the predefined questions and answer options. Offering the participants to give such feedback would have made it possible to extract a form of qualitative data from the participants, other than the questionnaires and fun-scale.

Finally, another limitation that emerged is that since both cybersecurity threats, and the way children interact and relate to technology is under constant development, and these changes are not possible to predict, some of our work is undoubtedly bound to the time under which it was done, and as any research, further development and exploration is necessary to keep up with the development.

Chapter 9

Conclusion and Further Work

This chapter concludes this master thesis, and will first present the general conclusion to the thesis, followed by a presentation of the potential further work on both the research domain and the prototype.

9.1 Conclusion

The combination of the SLR conducted in the fall of 2021, and the expert interviews and workshop laid the foundation for creating a working prototype of a game to raise the cybersecurity awareness among children. By using the limited number of relevant litterateur on inclusion of parents in the process, such a game was developed during this master thesis.

By conducting interviews with experts in the fields of CCI, HCI, game development and game design, we got invaluable insight and resources on how a game should be made such that it is appealing to children. Understanding that all aspects of a game a tightly knit together made us realise that developing a game is difficult, but manageable if careful planning is done in advance.

Using the data collected in the workshop, we took into account how the target audience viewed gamification and cooperative play with their family members.

The prototype was planned using the collected data and information, and developed using current technologies and development processes. The resulting game was a working prototype, hosted online and available from any device with an active internet connection. A user test was conducted remotely, and data collected through questionnaires. The results showed that the participants enjoyed the game as a whole, as well as playing with their family members. Furthermore, they wanted to play the game again if it had more features, levels and challenges. There was also a rise in awareness in several of the presented cybersecurity risks among the children.

9.2 Further Work

There are several aspects of both the research domain and the prototype that needs further work. While this thesis explore the inclusion of parents in a game-based cybersecurity solution, it is unique in it's kind, as limited research exists on the topic. Including parents in this setting needs to be addressed, as the parents, guardians or siblings of the younger generation are a vital part of the child's life, and as such would be beneficial to include in their learning process. As everyone ventures online frequently, it is important to accustom the upcoming generations to the life online. This life is becoming equally important to the real, and must be safe guarded.

Regarding the prototype, we had many ideas for expansion and enhancement but had to limit the scope due to time constraint. As such we will present these as potential further work. As mentioned in section 8.5, we did not have the skill or knowledge to meet the importance of a proper story within the game. The lack of story has to be addressed, such that player engagement and retention is increased. By using the results from the interviews in section 5.1, workshop in section 5.2 and this thesis, it is possible to gain the foundation to create such a story. Furthermore, by enhancing the graphical profile of the game a more enjoyable game session will be possible The graphics has to be relevant to the culture and context of both the game and the target audience, and as such has to be properly planned and executed.

Expanding on the story and the graphics, the setting and challenges within the game needs more diversity. As the game stands at the time of writing, it has one setting, and a handful of challenges. By introducing new settings, new biomes and new ambient sounds, the players will meet a more living world, which in turn would be more enticing and engaging.

On the more technical side, the game will benefit from the introduction of a proper game loop. At the time of writing, the game loop is event based, such that one player has to preform an action for the game world to update. An event based game loop is an outdated method of running a game, as most games have a main game loop that keeps track of all changes in the game world in real time. This game loop can be implemented using Elixir's provided `GenServer`[1] whose responsibility would be to have an internal ticker that broadcasts the current game state to all connected clients at a fixed interval. Using such a game loop, one can implement more living animations, other characters or enemies, floating spirits to interact with and more.

Lastly, we want to open source the code repository, as to facilitate further development from the open source community. Before this can be done, however, we want to clean up the code, make the project easier to set up and use, and write a more comprehensive guide on how the flow of the game is.

[1] `https://hexdocs.pm/elixir/1.13/GenServer.html`

Bibliography

[1] Medietilsynet, 'Barn og digitale medier 2020,' Norwegian, 2020. [Online]. Available: https://www.medietilsynet.no/globalassets/publikasjoner/barn-og-medier-undersokelser/2020/201015-barn-og-medier-2020-hovedrapport-med-engelsk-summary.pdf.

[2] United Nations, 'Declaration on the commemoration of the seventy-fifth anniversary of the united nations,' 2020. [Online]. Available: https://www.un.org/pga/74/wp-content/uploads/sites/99/2020/06/200625-UN75-highlight.pdf (visited on 14/06/2022).

[3] H. R. Max Roser and E. Ortiz-Ospina, 'Internet,' *Our World in Data*, 2015, https://ourworldindata.org/internet.

[4] F. Quayyum, D. S. Cruzes and L. Jaccheri, 'Cybersecurity awareness for children: A systematic literature review,' *International Journal of Child-Computer Interaction*, vol. 30, p. 100 343, 2021, ISSN: 2212-8689. DOI: https://doi.org/10.1016/j.ijcci.2021.100343.

[5] J. Chigada and R. Madzinga, 'Cyberattacks and threats during COVID-19: A systematic literature review,' en, *South African Journal of Information Management*, vol. 23, pp. 1–11, 2021, ISSN: 1560-683X. [Online]. Available: http://www.scielo.org.za/scielo.php?script=sci_arttext&pid=S1560-683X2021000100001&nrm=iso.

[6] K. Köhler, M. Wolf, v. drury vincent, R. Röpke and u. meyer ulrike, 'A Pond Full of Phishing Games - Analysis of Anti-Phishing Education Games,' Sep. 2020.

[7] R. E. S. Aas and S. R. Augdal, *Development of cybersecurity awareness solutions for children, using gamification: A systematic literature review*, Dec. 2021. [Online]. Available: https://studntnu-my.sharepoint.com/personal/marhh_ntnu_no/Documents/Projects/Rolf-Sigurd.pdf.

[8] R. Reid and J. Van Niekerk, *Back to basics: Information security education for the youth via gameplay*, English. Springer New York LLC, 2013, vol. 406, Journal Abbreviation: IFIP Advances in Information and Communication Technology Pages: 10 Publication Title: IFIP Advances in Information and Communication Technology, ISBN: 9783642393761 (ISBN). DOI: 10.1007/978-3-642-39377-8_1.

[9] O.-G. Baciu-Ureche, C. Sleeman, W. Moody and S. Matthews, 'The adventures of ScriptKitty: Using the Raspberry Pi to teach adolescents about internet safety,' English, in *SIGITE - Proc. Annu. Conf. Inf. Technol. Educ.*, Association for Computing Machinery, Inc, 2019, pp. 118–123, ISBN: 9781450369213 (ISBN). DOI: 10.1145/3349266.3351399.

[10] F. Giannakas, A. Papasalouros, G. Kambourakis and S. Gritzalis, 'A comprehensive cybersecurity learning platform for elementary education,' English, *Information Security Journal*, vol. 28, no. 3, pp. 81–106, 2019, Publisher: Taylor and Francis Inc., ISSN: 19393555 (ISSN). DOI: 10.1080/19393555.2019.1657527.

[11] J.-N. Tioh, M. Mina and D. Jacobson, 'Cyber security training: A survey of serious games in cyber security,' English, in *Proc. Front. Educ. Conf. FIE*, Journal Abbreviation: Proc. Front. Educ. Conf. FIE, vol. 2017-October, Institute of Electrical and Electronics Engineers Inc., 2017, pp. 1–5, ISBN: 9781509059195 (ISBN). DOI: 10.1109/FIE.2017.8190712.

[12] F. Quayyum, J. Bueie, D. Cruzes, L. Jaccheri and J. Vidal, 'Understanding parents' perceptions of children's cybersecurity awareness in Norway,' English, in *GoodIT - Proc. Conf. Inf. Technol. Soc. Good*, Journal Abbreviation: GoodIT - Proc. Conf. Inf. Technol. Soc. Good, Association for Computing Machinery, Inc, 2021, pp. 236–241, ISBN: 9781450384780 (ISBN). DOI: 10.1145/3462203.3475900.

[13] J. Allers, G. Drevin, D. Snyman, H. Kruger and L. Drevin, 'Children's awareness of digital wellness: A serious games approach,' in Jul. 2021, pp. 95–110, ISBN: 978-3-030-80864-8. DOI: 10.1007/978-3-030-80865-5_7.

[14] S. Holden, B. Abelsen, H. Jordell, H. E. Stokke, L. Akkaraju, R. Nersten, B. Søgaard, B. K. Barvik, L. Sannes, J. Sørbø, T. Bergene, T. Skjerve, A. Turmo, K. Bjorvatn, T. H. Sollien, M. Tønnessen, H. Børrestuen, R. E. Stangeland, L. Nerdrum, K. G. Dalbak, I. B. Krüger, M. O. Nygaard and H. Ytteborg, 'Nou 2019: 2 - fremtidige kompetansebehov ii — utfordringer for kompetansepolitikken,' Feb. 2019. [Online]. Available: https://www.regjeringen.no/no/dokumenter/nou-2019-2/id2627309/?ch=1 (visited on 03/11/2021).

[15] M. Olano, A. Sherman, L. Oliva, R. Cox, D. Firestone, O. Kubik, M. Patil, J. Seymour, I. Sohn and D. Thomas, 'SecurityEmpire: Development and evaluation of a digital game to promote cybersecurity education,' English, in *USENIX Summit Gaming, Games, Gamification Secur. Educ., 3GSE*, Journal Abbreviation: USENIX Summit Gaming, Games, Gamification Secur. Educ., 3GSE, USENIX Association, 2014.

[16] D. P. Snyman, G. R. Drevin, H. A. Kruger, L. Drevin and J. Allers, 'A Wolf, Hyena, and Fox Game to Raise Cybersecurity Awareness Among Preschool Children,' en, in *Human Aspects of Information Security and As-*

surance, S. Furnell and N. Clarke, Eds., ser. IFIP Advances in Information and Communication Technology, Cham: Springer International Publishing, 2021, pp. 91–101, ISBN: 978-3-030-81111-2. DOI: 10.1007/978-3-030-81111-2_8.

[17] C. Irvine and M. Thompson, 'CyberCIEGE Scenario Design and Implementation,' Aug. 2014.

[18] S. Jansen, *Lær barna nettvett med medietilsynets nettspill*, Sep. 2020. [Online]. Available: https://www.barnevakten.no/stjernekolonien/.

[19] J. M. Keller, 'Development and use of the arcs model of instructional design,' *Journal of instructional development*, vol. 10, no. 3, pp. 2–10, 1987.

[20] F. Giannakas, G. Kambourakis, A. Papasalouros and S. Gritzalis, 'Security education and awareness for K-6 going mobile,' English, *International Journal of Interactive Mobile Technologies*, vol. 10, no. 2, pp. 41–48, 2016, ISSN: 18657923 (ISSN). DOI: 10.3991/ijim.v10i2.5473.

[21] M. Hattingh and S. Eybers, 'Towards Understanding How Game Based Learning Can Enhance Flipped Learning,' in Sep. 2017, ISBN: 978-3-319-71083-9. DOI: 10.1007/978-3-319-71084-6_12.

[22] T. Staff, *Bloom's taxonomy is a hierarchical framework for cognition and learning objectives*, [Online; accessed 11-December-2021], 2021. [Online]. Available: https://www.teachthought.com/learning/what-is-blooms-taxonomy/.

[23] N. Katsantonis, I. Kotini, P. Fouliras and I. Mavridis, 'Conceptual framework for developing cyber security serious games,' English, in *IEEE Global Eng. Edu. Conf., EDUCON*, Ashmawy A.K. and Schreiter S., Eds., vol. April-2019, IEEE Computer Society, 2019, pp. 872–881, ISBN: 9781538695067 (ISBN). DOI: 10.1109/EDUCON.2019.8725061.

[24] H. Qusa and J. Tarazi, 'Cyber-Hero: A Gamification framework for Cyber Security Awareness for High Schools Students,' English, in *IEEE Annu. Comput. Commun. Workshop Conf., CCWC*, Paul R., Ed., Institute of Electrical and Electronics Engineers Inc., 2021, pp. 677–682, ISBN: 9780738143941 (ISBN). DOI: 10.1109/CCWC51732.2021.9375847.

[25] S. Maqsood and S. Chiasson, 'Design, Development, and Evaluation of a Cybersecurity, Privacy, and Digital Literacy Game for Tweens,' English, *ACM Transactions on Privacy and Security*, vol. 24, no. 4, 2021, Publisher: Association for Computing Machinery, ISSN: 24712566 (ISSN). DOI: 10.1145/3469821.

[26] S. Scholefield and L. Shepherd, *Gamification Techniques for Raising Cyber Security Awareness*, English. Springer Verlag, 2019, vol. 11594 LNCS, Journal Abbreviation: Lect. Notes Comput. Sci. Pages: 203 Publication Title: Lect. Notes Comput. Sci., ISBN: 9783030223502 (ISBN). DOI: 10.1007/978-3-030-22351-9_13.

[27] H. Alqahtani and M. Kavakli-Thorne, 'Design and evaluation of an augmented reality game for cybersecurity awareness (CybAR),' English, *Information (Switzerland)*, vol. 11, no. 2, 2020, Publisher: MDPI AG, ISSN: 20782489 (ISSN). DOI: 10.3390/info11020121.

[28] B. Göbl, D. Hristova, S. Jovicic and H. Hlavacs, 'Serious Game Design for and with Adolescents: Empirically Based Implications for Purposeful Games,' in Jul. 2020, pp. 398–410, ISBN: 978-3-030-50163-1. DOI: 10.1007/978-3-030-50164-8_29.

[29] K. Y. Zamri and N. N. Al Subhi, '10 user interface elements for mobile learning application development,' in *2015 International Conference on Interactive Mobile Communication Technologies and Learning (IMCL)*, Nov. 2015, pp. 44–50. DOI: 10.1109/IMCTL.2015.7359551.

[30] E. Kritzinger, 'A Curriculum Approach to Improving Cyber Safety in South African Schools,' in Jan. 2017, pp. 95–105, ISBN: 978-3-319-71083-9. DOI: 10.1007/978-3-319-71084-6_11.

[31] T. Shabe, E. Kritzinger and M. Loock, 'Scorecard Approach for Cyber-Security Awareness,' in Jan. 2017, pp. 144–153, ISBN: 978-3-319-71083-9. DOI: 10.1007/978-3-319-71084-6_16.

[32] A. Al-Naser, A. Bushager and H. Al-Junaid, 'Parents' awareness and readiness for smart devices' cybersecurity,' English, in *IET Conf Publ*, vol. 2019, Institution of Engineering and Technology, 2019.

[33] J.-N. Tioh, D. Mina and D. Jacobson, 'Cyber Security Social Engineers An Extensible Teaching Tool for Social Engineering Education and Awareness,' English, in *Proc. Front. Educ. Conf. FIE*, vol. 2019-October, Institute of Electrical and Electronics Engineers Inc., 2019, ISBN: 9781728117461 (ISBN). DOI: 10.1109/FIE43999.2019.9028369.

[34] B. J. Oates, *Researching Information Systems and Computing*, en. SAGE, 2006, ISBN: 978-1-4129-0224-3.

[35] J. C. Read and S. MacFarlane, 'Using the fun toolkit and other survey methods to gather opinions in child computer interaction,' en, in *Proceeding of the 2006 conference on Interaction design and children - IDC '06*, Tampere, Finland: ACM Press, 2006, p. 81. DOI: 10.1145/1139073.1139096.

[36] A. I. Wang, 'Hvordan kan dataspill fremme faglig motivasjon i klasserommet?' In *Mediepedagogikk - Refleksjoner om teori og praksis*, 2012.

[37] S. Boller, 'Learning game design: Game mechanics,' 2017. [Online]. Available: http://www.theknowledgeguru.com/learning-game-design-mechanics/ (visited on 31/05/2022).

[38] Utdanningsdirektoratet, *Overordnet del – verdier og prinsipper for grunnopplæringen*, Jun. 2022. [Online]. Available: https://www.udir.no/lk20/overordnet-del/ (visited on 13/06/2022).

[39] D. Pickell, 'The 7 stages of game development,' 2019. [Online]. Available: https://www.g2.com/articles/stages-of-game-development (visited on 23/06/2022).

[40] Wikipedia, *List of most expensive video games to develop — Wikipedia, the free encyclopedia*, http://en.wikipedia.org/w/index.php?title=List%20of%20most%20expensive%20video%20games%20to%20develop&oldid=1085494592, [Online; accessed 23-June-2022], 2022.

[41] J. Kumar, 'Gamification at work: Designing engaging business software,' Jul. 2013, pp. 528–537, ISBN: 978-3-642-39240-5. DOI: 10.1007/978-3-642-39241-2_58.

[42] J. E. Bresenham, 'Algorithm for computer control of a digital plotter,' *IBM Systems Journal*, vol. 4, no. 1, pp. 25–30, 1965. DOI: 10.1147/sj.41.0025.

[43] S. Overflow, '2022 developer survey,' 2022. [Online]. Available: https://survey.stackoverflow.co/2022 (visited on 24/06/2022).

[44] G. Rennie, 'The road to 2 million websocket connections in phoenix,' Nov. 2015. [Online]. Available: https://www.phoenixframework.org/blog/the-road-to-2-million-websocket-connections (visited on 02/02/2022).

[45] United Nations, '11. convention on the rights of the child,' vol. 1, Nov. 1989, ch. 4.

[46] N. S. for the Prevention of Cruelty to Children, 'Research with children: Ethics, safety and avoiding harm,' 2020. [Online]. Available: https://learning.nspcc.org.uk/research-resources/briefings/research-with-children-ethics-safety-avoiding-harm (visited on 08/03/2022).

[47] T. Bratteteig and I. Wagner, 'Unpacking the Notion of Participation in Participatory Design,' en, *Computer Supported Cooperative Work (CSCW)*, vol. 25, no. 6, pp. 425–475, Dec. 2016, ISSN: 1573-7551. DOI: 10.1007/s10606-016-9259-4. (visited on 08/02/2022).

[48] 'Second quarter financial results and corporate management policy briefing for fiscal ending march 2022,' *Nintendo Co., Ltd. - Investor Relations Information*, Nov. 2021. [Online]. Available: https://www.nintendo.co.jp/ir/pdf/2021/211105e.pdf.

Appendix A

SLR Papers

Pub. Year	Authors	Title
2015 [29]	Zamri, Khairul Yusri; Al Subhi, Nada Nasser	10 user interface elements for mobile learning application development
2019 [10]	Giannakas, F.; Papasalouros, A.; Kambourakis, G.; Gritzalis, S.	A comprehensive cybersecurity learning platform for elementary education
2017 [30]	Kritzinger, Elmarie	A Curriculum Approach to Improving Cyber Safety in South African Schools
2020 [6]	Köhler, Klemens; Wolf, Martin; drury, vincent; Röpke, René; meyer, ulrike	A Pond Full of Phishing Games - Analysis of Anti-Phishing Education Games
2021 [16]	Snyman, Dirk P.; Drevin, Gunther R.; Kruger, Hennie A.; Drevin, Lynette; Allers, Johann	A Wolf, Hyena, and Fox Game to Raise Cybersecurity Awareness Among Pre-school Children
2013 [8]	Reid, R.; Van Niekerk, J.	Back to basics: Information security education for the youth via gameplay
2021 [13]	Allers, J.; Drevin, G.; Snyman, Dirk; Kruger, Hennie; Drevin, Lynette	Children's Awareness of Digital Wellness: A Serious Games Approach
2019 [33]	Tioh, J.-N.; Mina, D.M.; Jacobson, D.D.W.	Cyber Security Social Engineers An Extensible Teaching Tool for Social Engineering Education and Awareness
2017 [11]	Tioh, J.-N.; Mina, M.; Jacobson, D.W.	Cyber security training: A survey of serious games in cyber security
2021 [24]	Qusa, H.; Tarazi, J.	Cyber-Hero: A Gamification framework for Cyber Security Awareness for High Schools Students
2020 [27]	Alqahtani, H.; Kavakli-Thorne, M.	Design and evaluation of an augmented reality game for cybersecurity awareness (CybAR)
2021 [25]	Maqsood, S.; Chiasson, S.	Design, Development, and Evaluation of a Cybersecurity, Privacy, and Digital Literacy Game for Tweens
2019 [26]	Scholefield, S.; Shepherd, L.A.	Gamification Techniques for Raising Cyber Security Awareness
2019 [32]	Al-Naser, A.E.; Bushager, A.; Al-Junaid, H.	Parents' awareness and readiness for smart devices' cybersecurity
2017 [31]	Shabe, Tsosane; Kritzinger, Elmarie; Loock, Marianne	Scorecard Approach for Cyber-Security Awareness
2016 [20]	Giannakas, F.; Kambourakis, G.; Papasalouros, A.; Gritzalis, S.	Security education and awareness for K-6 going mobile
2014 [15]	Olano, M.; Sherman, A.; Oliva, L.; Cox, R.; Firestone, D.; Kubik, O.; Patil, M.; Seymour, J.; Sohn, I.; Thomas, D.	SecurityEmpire: Development and evaluation of a digital game to promote cybersecurity education
2020 [28]	Göbl, Barbara; Hristova, Dayana; Jovicic, Suzana; Hlavacs, Helmut	Serious Game Design for and with Adolescents: Empirically Based Implications for Purposeful Games
2019 [9]	Baciu-Ureche, O.-G.; Sleeman, C.; Moody, W.C.; Matthews, S.J.	The adventures of ScriptKitty: Using the Raspberry Pi to teach adolescents about internet safety
2017 [21]	Hattingh, Marie; Eybers, Sunet	Towards Understanding How Game Based Learning Can Enhance Flipped Learning
2021 [12]	Quayyum, F.; Bueie, J.; Cruzes, D.S.; Jaccheri, L.; Vidal, J.C.T.	Understanding parents' perceptions of children's cybersecurity awareness in Norway

Table A.1: List of papers included in the Systematic literature review by Aas and Augdal [7]

Appendix B

Interview Guides

B.1 Professionals

B.1.1 Research Questions

- **RQ1**: How can one combine adult and child learning to raise awareness of cybersecurity?

B.1.2 Questions for Interview

- **Q1**: What is the best way for people to learn about good cybersecurity etiquette?
  - **Q1.1**: In your experience: which methods are proven to be most successful? (activities, lectures, videos, quizzes, games etc)
  - **Q1.2**: In your experience: are there any differences between the way we act professionally (at work) and in private (at home) when it comes to cybersecurity etiquette? If so: are we more aware of the risks at work or at home? Why could this be?
  - **Q1.3**: Which challenges have you experienced when educating adults on cybersecurity?
- **Q2**: Do you have any experience teaching children about cybersecurity?
  - **Q2.1**: In your experience: which methods are proven to be most successful? (activities, lectures, videos, quizzes, games etc)
  - **Q2.2**: Which challenges have you experienced when educating children on cybersecurity, and how is it different from educating adults?
- **Q3**: Which cybersecurity risks (phishing, stranger danger, password hygiene etc.) are easiest to educate people on?
  - **Q3.1**: Why do you think it is so?
- **Q4**: Which cybersecurity risks (phishing, stranger danger, password hygiene etc.) are the most difficult to educate people on?

- **Q4.1**: Why do you think it is so?

- **Q5**: Does a lack of technological insight reduce the outcome of the lessons and activities you provide?

B.1.3 Subject Selection

Role	Comment	Suggested by
CEO of a company specialised in education of cybersecurity. Experience with educating the public about cybersecurity.		Co.supervisor

Table B.1: Subject selection

B.2 Academics

B.2.1 Research Questions

- **RQ1**: How can a game be designed such that cybersecurity awareness is raised for both children and adults?
  - **SRQ1.1**: Which game designs are appropriate?
  - **SRQ1.2**: What are the essentials in the design of a game to appeal to both children and adults?
- **RQ2**: How can one combine adult and child learning to raise awareness of cybersecurity?

B.2.2 Questions for Interview

- **Q1**: How should one design a game such that both children and their parents have a positive learning experience?
  - **Q1.1**: Which game elements are frequently used to enhance learning outcomes for children?
  - **Q1.2**: Which game elements are frequently used to enhance learning outcomes for adults?
- **Q2**: Should one aim to have a more fast-paced game play for children?
  - **Q2.1**: If so: how could one combine a fast-paced game play, while retaining good learning outcomes?
- **Q3**: Which game genres should one consider opting for when creating a fun learning experience for children and adults?
  - **Q3.1**: Are there game genres that appeal to both children and adults?

- **Q4**: How does one manage to keep the attention of children in a learning game?
  - **Q4.1**: What design techniques and game elements are proven to be successful in achieving this goal?
- **Q5**: Which challenges/obstacles and/or advantages/gains do you see for designing a cybersecurity game aimed at both children and adults?
  - **Q5.1**: Can you think of special consideration one should make?
  - **Q5.2**: Do you know any strategies one can use to avoid the challenges/obstacles?

B.2.3 Subject Selection

Role	Comment	Suggested by
Professor at Department of Computer Science at NTNU. Has experience in game development.		–
Professor at Department of Computer Science at NTNU - Academic interest in the field of child-computer interaction.		Co-supervisor
Professor at Department of Computer Science at NTNU - Academic interest in the field of human-computer interaction.		-

Table B.2: Subject selection

B.2.4 Consent Form

The research is conducted by two master students at the Department of Computer Science at the Norwegian University of Science and Technology (NTNU). The results from this interview will be analysed, used and presented in their final master thesis. The goal is to gain insight into the fields of game design and human-computer interaction, as well as get a better understanding of which aspects to consider and prioritise when developing a game prototype for raising cybersecurity awareness among children and parents alike.

The master students, Rolf Erik Sesseng Aas (reaas@stud.ntnu.no) and Sigurd Røstad Augdal (sigurdra@stud.ntnu.no), are responsible for, and will be conducting, the interview. The interviewee is selected as they have expertise within the relevant research domain, and will be beneficial to understanding the domain, possibilities and limitations within said domain. The interviewee was proposed by the researcher's co-supervisor, or by the researchers themselves.

Consent to take part in research

- I _____ voluntarily agree to participate in this research study.
- I understand that the interview will take up to 1 hour.
- I understand that even if I agree to participate now, I can withdraw at any time or refuse to answer any question without any consequences of any kind.
- I understand that I can withdraw permission to use data from my interview within two weeks after the interview, in which case the material should be deleted.
- I have had the purpose and nature of the study explained to me in writing and I have had the opportunity to ask questions about the study.
- I understand that participation involves answering questions regarding cybersecurity, children and game design relating to these topics. My participation will help the researchers gain insight into the fields of game design and human computer interaction, and help them to get a better understanding of which aspects to consider and prioritise when developing a game prototype for raising cybersecurity awareness among children and parents alike.
- I understand that I will not benefit directly from participating in this research.
- I agree to my interview being audio-recorded.
- I understand that all information I provide for this study will be treated confidentially.
- I understand that in any report on the results of this research my identity will remain anonymous. This will be done by changing my name and disguising any details of my interview which may reveal my identity or the identity of people I speak about.
- I understand that disguised extracts from my interview may be quoted in the final master thesis, as well as the final dissertation.
- I understand that if I inform the researchers that myself or someone else is at risk of harm they may have to report this to relevant authorities - they will discuss this. with me first but may be required to report with or without my permission.
- I understand that signed consent forms and original audio recording will be retained in NTNU's private OneDrive with strict user access until the exam board confirms the results of the researchers dissertation.
- I understand that a transcript of my interview in which all identifying information has been removed will be retained for two years from the date exam board confirms the results of the researchers dissertation.
- I understand that under the freedom of information legalisation I am entitled to access and/or change the information I have provided at any time while it is in storage as specified above.
- I understand that under the freedom of information legalisation I am entitled to notify the Norwegian Data Protection Authority (Datatilsynet)

regarding misuse or other details about the information stored about me.
- I understand that I am free to contact any of the people involved in the research to seek further clarification and information. The researchers can be contacted using either of the following:
    - Rolf Erik Sesseng Aas
    - Masters in Computer Science at NTNU
    - reaas@stud.ntnu.no
    - Sigurd Røstad Augdal
    - Masters in Computer Science at NTNU
    - sigurdra@stud.ntnu.no
    - Letizia Jaccheri
    - Professor at Department of Computer Science at NTNU
    - letizia.jaccheri@ntnu.no

Signature of research participant	Signature of researcher
_____	_____
Date	Date
_____	_____

B.3 Workshop participants

B.4 User test participants

Appendix C

Intervjuguide

C.1 Industrieksperter

C.1.1 Forskningsspørsmål

- **RQ1**: Hvordan kan man kombinere læring for voksne og barn for å øke bevissthet rundt cybersikkerhet?

C.1.2 Intervjuspørsmål

- **Q1**: Hva er den beste måten for folk å lære om god cybersikkerhets etikette?
    - **Q1.1**: I dine øyne(?) (Fra din erfaring) Etter det du har erfart: hvilke metoder har vist seg å være mest vellykkede? (aktiviteter, forelesninger, videoer, quiz, spill osv.)
    - **Q1.2**: Etter det du har erfart: er det forskjeller på måten man opptrer i profesjonell (på jobb) og privat (hjemme) kontekst når det kommer til cybersikkerhet? I så fall: er vi mer bevisste på risikoene på jobb eller hjemme? Hva kan dette skyldes?
    - **Q1.3**: Hvilke andre utfordringer har du opplevd når det kommer til å lære voksne cybersikkerhet?
- **Q2**: Har du erfaring med å lære barn cybersikkerhet?
    - **Q2.1**: Etter det du har erfart: hvilke metoder har vist seg å være mest vellykkede? (aktiviteter, forelesninger, videoer, quiz, spill osv.)
    - **Q2.2**: Hvilke utfordringer har du opplevd når det kommer til å lære barn om cybersikkerhet, og hvordan skiller det seg fra å lære bort til voksne?
- **Q3**: Hvilke cybersikkerhetsrisikoer (phishing, fremmedfare(stranger danger), passordhygiene osv.) er enklest å lære folk om?
    - **Q3.1**: Hva kan være grunnen til dette?

- **Q4**: Hvilke cybersikkerhetsrisikoer (phishing, fremmedfare(stranger danger), passordhygiene osv.) er vanskeligst å lære folk om?
  - **Q4.1**: Hva kan være grunnen til dette?
- **Q5**: Ser du en sammenheng mellom mangel på teknologisk innsikt og resultatene av timene og aktivitetene du gjennomfører?

C.1.3 Utvalg av intervjuobjekter

Rolle	Kommentar	Foreslått av
Daglig leder for et selskap som spesialiserer seg på cybsersikkerhetsutdanning og- opplæring. Erfaring med å lære bort cybersikkerhet.		Medveileder

Table C.1: Utvalg av intervjuobjekter

C.2 Akademikere

C.2.1 Forskningsspørsmål

- **RQ1**: Hvordan kan man designe et spill på en måte som øker bevisstheten rundt cybersikkerhet for både barn og voksne?
  - **SRQ1.1**: Hvilke spilldesign er passende?
  - **SRQ1.2**: Hva er det essensielle nå man skal lage spill som appelerer til både barn og voksne?
- **RQ2**: Hvordan kan man kombinere læring for både voksne og barn for å øke bevissthet rundt cybersikkerhet?

C.2.2 Intervjuspørsmål

- **Q1**: Hvordan bør man designe et spill slik at både barn og voksne kan ha en positiv læringsopplevelse?
  - **Q1.1**: Hvilke spillelementer er oftest brukt for å forbedre læringsutbytte for barn?
  - **Q1.2**: Hvilke spillelementer er oftest brukt for å forbedre læringsutbytte for voksne?
- **Q2**: Bør man ha som mål å ha et mer fartsfylt spill for barn?
  - **Q2.1**: I så fall: hvordan kan beholde et godt læringsutbytte for et fartsfylt spill?
- **Q3**: Hvilke spillsjangre bør velge når man skal skape en morsom læringsopplevelse for både barn og voksne?

    - **Q3.1**: Finnes det spillsjangre som appellerer til både barn og voksne?
- **Q4**: Hvordan kan man holde på oppmerksomheten til barn i et læringsspill?
    - **Q4.1**: Hvilke designteknikker og spillelement har vist seg å være vellykkede for å oppnå dette målet?
- **Q5**: Hvilke utfordringer/hindringer og/eller fordeler/gevinster ser du ved å designe et cybersikkerhetsspill rettet mot både barn og voksne?
    - **Q5.1**: Kan du tenke deg spesielle hensyn man bør ta?
    - **Q5.2**: Vet du om strategier man kan bruke for å unngå de nevnte utfordringene/hindringene?

C.2.3 Utvalg av intervjuobjekter

Rolle	**Kommentar**	**Foreslått av**
Professor Institutt for datateknologi og informatikk ved NTNU. Har erfaring innen spillutvikling.		–
Professor Institutt for datateknologi og informatikk ved NTNU. Akademisk interesse innenfor CCI-feltet (barn-maskin-interaksjon).		Medveileder
Professor Institutt for datateknologi og informatikk ved NTNU. Akademisk interesse innenfor HCI-feltet (Menneske-maskin-interaksjon).		-

Table C.2: Utvalg av intervjuobjekter

C.2.4 Samtykkeskjema

Forskningen utføres av to masterstudenter ved Institutt for datateknologi og informatikk ved Norges teknisk-naturvitenskapelige universitet (NTNU). Resultatene fra dette intervjuet vil bli analysert, brukt og presentert i masteroppgaven deres. Målet er å få innsikt i feltene spilldesign og menneske-maskin interaksjon, samt få en bedre forståelse av hvilke aspekter man bør vurdere og prioritere når man utvikler en spillprototype for bevisstgjøring av cybersikkerhet blant barn og foreldre.

Masterstudentene, Rolf Erik Sesseng Aas (reaas@stud.ntnu.no) og Sigurd Røstad Augdal (sigurdra@stud.ntnu.no), er ansvarlige for, og skal gjennomføre, intervjuet. Intervjuobjektet er valgt på grunnlag av sin kompetanse innenfor det aktuelle forskningsdomenet, og vil kunna bidra til forståelse for mulighetene og begrensningene innenfor nevnte domene. Intervjuobjektet ble foreslått av forskernes medveileder.

Samtykke til å ta del i forskning

- Jeg _____ velger frivillig å delta i dette forskningsprosjektet.
- Jeg forstår at intervjuet kan ta opptil 1 time.
- Jeg forstår at selv om jeg samtykker til å delta nå, kan jeg når som helst trekke tilbake mitt samtykke, eller nekte å svare på spørsmål uten noen form for konsekvenser.
- Jeg forstår at jeg kan trekke tilbake mitt samtykke til å bruke dataene fra dette intervjuet innen to uker etter gjennomført intervju, og da få slettet all data.
- Jeg har fått skriftlig forklart hensikten med forskningen og dens art, og jeg har hatt mulighet til å stille spørsmål om forskningen.
- Jeg forstår at deltakelse innebærer å svare på spørsmål som omhandler cybersikkerhet, barn og spilldesign relatert til disse emnene. Min deltakelse vil hjelpe forskerne til å få innsikt i feltene spilldesign og menneskelig datamaskininteraksjon, og hjelpe dem til å få en bedre forståelse av hvilke aspekter de bør vurdere og prioritere når de utvikler en spillprototype for å øke bevisstheten om cybersikkerhet blant barn og foreldre.
- Jeg forstår at resultatene og dataene som samles inn fra dette intervjuet kun vil bli brukt i forskernes masteroppgave.
- Jeg forstår at jeg ikke vil ha direkte nytte av å delta i denne forskningen.
- Jeg godtar at det blir gjort lydopptak av intervjuet.
- Jeg forstår at all informasjon jeg bidrar med vil bli behandlet konfidensielt.
- Jeg forstår at i enhver rapport om resultatene av denne forskningen vil min identitet forbli anonym. Dette vil bli gjort ved å endre navnet mitt og skjule alle detaljer i intervjuet som kan avsløre identiteten min eller identiteten til personer jeg snakker om.
- Jeg forstår at anonymiserte utdrag fra intervjuet kan siteres i masteroppgaven.
- Jeg forstår at hvis jeg informerer forskerne om at jeg eller noen andre er i fare for skade kan de måtte rapportere dette til relevante myndigheter - de vil diskutere dette med meg først, men kan bli pålagt å rapportere med eller uten min tillatelse.
- Jeg er innforstått med at det signerte samtykkeskjemaet og originalt lydopptak vil bli oppbevart i NTNUs private OneDrive med streng brukertilgang inntil eksamensstyret bekrefter resultatene av forskernes avhandling.
- Jeg forstår at en utskrift av intervjuet mitt der all identifiserende informasjon er fjernet kan bli oppbevart i to år fra datoen eksamensstyret bekrefter resultatene av forskernes avhandling.
- Jeg forstår at etter informasjonsfrihetslovgivning har jeg rett til å få tilgang til og/eller endre informasjonen jeg har gitt i tiden den er lagret som spesifisert ovenfor.

- Jeg forstår at jeg står fritt til å kontakte Datatilsynet ved eventuelle misbruk eller annet av informasjonen gitt til forskningsprosjektet.
- Jeg forstår at jeg står fritt til å kontakte personene som er involvert i forskningen for å stille spørsmål og få mer informasjon. Forskerne kan nås ved å bruke følgende kontaktinformasjon:
    - Rolf Erik Sesseng Aas
    - Master i Datateknologi fra NTNU
    - reaas@stud.ntnu.no
    - Sigurd Røstad Augdal
    - Master i Datateknologi fra NTNU
    - sigurdra@stud.ntnu.no
    - Letizia Jaccheri
    - Professor i Datateknologi hos NTNU
    - letizia.jaccheri@ntnu.no

Signatur forskningsdeltaker	Signatur forsker
_____	_____
Dato	Dato
_____	_____

Appendix D

Observation Guide

Observation guide

Observer name:
Time and date:
Points to focus:

**Remember to write down the participant team ID with the notes/observation. For example: CT1 (which means child from team 1), PT2 (the parent from team 2)*

1. The team
    a. How are the parent and child working as a team?
        i. Collaborative approach (helping each other, reciprocal or not)?
        ii. Guiding approach (parent tells the answers to the child or guide what to do)?
        iii. Who is helping whom to understand the security concepts or risks?
            A. Parent helps the child?
            B. Or the child helps the parent?
2. The communication
    a. Reciprocal? Or one way communication?
    b. Who is leading the communication? The parent or the child?
3. Other points
    - What questions did they have for us?
    - To what extent did everybody participate? What was the mood in the session? Were they open to try?
    - What worked well?
    - What was challenging?
    - Any feedback from the participants about the workshop organization?

Appendix E

Group Discussion Guide

Group discussion

Questions to ask/discuss:

1. What was good and what was challenging?
2. (parent) In your opinion, does involving parents in the game help the children to learn in a better way?
   - Why?
   - Why not?
3. (parent) What kind of roles can a parent play in an online security awareness game while playing with a child?
   a. If you are asked to play a learning game with your child what role you would like to play in the game?
      i. A co-player, as you have played now?
      ii. Compete against each other (competition)?
      iii. Would you like to suggest any other ways? Any new ideas?
4. (child) What kind of roles can children expect from their parents in an online security awareness game?
   a. If you need to play a learning game, how can your mom/dad help you with the game?
      i. Would you like to play with your mom/dad as you have played now (co-player)?
      ii. Would you like to go for a competition (against each other)?
      iii. Would you like to suggest any other ways? Any new ideas?

Appendix F

Database Diagram

Figure F.1: Database diagram of the prototype

Appendix G

Online Consent From

By entering and playing this game you contribute with valuable data to our research project. For information about the project see below.

G.1 About of the project

This research is a part of a Master thesis. The purpose of this research is to investigate and further develop knowledge and tools that will be helpful in raising cybersecurity awareness among children in a playful, engaging, and motivating manner.

This research aims to develop an online security awareness game for children incorporating parents' views and expectations.

G.2 Who is responsible for the research project?

The Department of Computer Technology and Informatics at NTNU is responsible for the project.

G.3 Why are you being asked to participate?

The researchers in the project team have compiled a list of people they know with children in the age group 9-13 years. We do not have any additional selection criteria, but the parents of these children are encouraged to play through the game together with them, aiming to examine the role of parents in safeguarding children's online security and how to empower both parents and children with online security knowledge and skills.

G.4 What does participation involve for you?

This research will conduct a user test of a game prototype with children (and their parents). The testing aims to assess how the different elements and techniques used in the game might contribute to raising cybersecurity awareness among children. Playing through the prototype takes approximately 30-45 minutes.

The participants will first answer a pre-test questionnaire. Then they will play through the game, and lastly answer a post-test questionnaire. The questionnaire includes questions related to cybersecurity and the game experience.

The answers to the questionnarie questions together with the answers from the challenges from the gameplay constitutes the collected data from the testing. Along with this information, we will collect some personal information, such as the gender and age of the participants, but no other indentifying data will be collected.

G.5 Your personal privacy – how we will store and use your personal data

We will only use your personal data for the purpose(s) specified in this information letter. We will process your personal data confidentially and in accordance with data protection legislation (the General Data Protection Regulation and Personal Data Act). Any data collected is inherently anonymised, and therefore can not be traced back to you.

- A group of five researchers from NTNU will have access to the data. Two master's students will facilitate the user testing and the data collection is built into the web-application. The data is anonymised by default.
- The data will be stored in a cloud service affiliated with NTNU (Microsoft services) and are password-protected so that no unauthorized persons have access.
- The Research Team consists of Professor Letizia Jaccheri, Professor Daniela Soares Cruzes, PhD student Farzana Quayyum, and two master's students Rolf Erik Sesseng Aas and Sigurd Røstad Augdal.

The participants of the study will not be recognizable in publications.

G.6 Where can I find out more?

If you have questions about the project or want to exercise your rights, contact:

- NTNU via PhD Candidate Farzana Quayyum (farzana.quayyum@ntnu.no)
- NTNU via Master student Rolf Erik Sesseng Aas (reaas@stud.ntnu.no)
- NTNU via Master student Sigurd Røstad Augdal (sigurdra@stud.ntnu.no)
- Our Data Protection Officer: Thomas Helgesen (thomas.helgesen@ntnu.no)

Thank you again for participating in our project! :)

R.E.S. Aas, S.R. Augdal

Raising cybersecurity awareness

NTNU
Norwegian University of
Science and Technology