Giske Naper Freberg

Designing Software to Raise Cyber Security Awareness in Developing Countries

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

Master's thesis

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

NTNU
Norwegian University of
Science and Technology

Giske Naper Freberg

Designing Software to Raise Cyber Security Awareness in Developing Countries

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

The introduction of ICTs and digital tools has been an accelerator for innovation and development for the past decades. In less-developed countries, the availability of digital tools and access to the internet is increasing. The Covid-19 pandemic illustrated how ICTs could impact sectors like education and health. However, negative aspects within the field of cyber security emerge with increasing online access. Cyber security challenges are well recognised in developed countries. However, cyber security awareness has not been prioritised in less-developed countries. An increased online presence demands increasing attention to the risks that online presence presents, to which the younger generations in developing nations are especially exposed.

The objective of this master thesis project is to investigate the current status of research within the field of cyber security awareness in developing nations and to design and develop an application for raising cyber security awareness for young people living in these areas. By introducing an application for this purpose, its impact and limitations can be explored.

A systematic literature review was conducted in the preliminary phase to analyse related literature within the field of research. The literature review identified 18 primary studies. To accompany the findings from the systematic literature review, semi-structured interviews with experts within the field of research were conducted. Based on the findings from the preliminary phase, a working prototype for a digital platform was designed and developed through a collaboration with Leap Learning. The prototype was then tested on participants representing the project's target group. The data generation methods used for evaluating the prototype were observations and interviews.

The findings show that the developed prototype did provide participants representing the target group with new knowledge and a higher awareness level of cyber security. Additionally, four factors for successfully educating cyber security awareness in developing countries were identified. Future research can apply these recommended factors when conducting research in a developing country context.

Keywords: *Cyber Security Awareness, Developing Countries, Adolescents, Young Adults, Digital Literacy, Software Development, Systematic Literature Review*

Sammendrag

Innføringen av IKT og digitale verktøy har vært en akselerator for innovasjon og utvikling de siste tiårene. I utviklingsland er tilgjengeligheten av digitale verktøy og internettilgang økende. Koronapandemien illustrerte hvordan IKT kan påvirke sektorer som utdanning og helse. Med økende digital tilgang, dukker imidlertid negative aspekter forbundet med cyber sikkerhet opp. I velutviklede land er utfordringer knyttet til cybersikkerhet anerkjent. Den samme bevisstheten har imidlertid ikke blitt prioritert i utviklingsland. En økt tilstedeværelse på internett, krever økt oppmerksomhet rundt risikoene som aktivitet på internett utgjør. Særlig er de yngre generasjonene i utviklingsland utsatt.

Målet med dette masterprosjektet er å undersøke statusen for forskning innen bevissthet rundt cybersikkerhet i utviklingsland, samt å designe og utvikle en applikasjon for å øke bevisstheten rundt cybersikkerhet for unge mennesker i utviklingsland. Ved å introdusere en applikasjon med dette formålet, kan dens innvirkning utforskes.

Et systematisk litteraturstudie ble gjennomført i den innledende fasen av prosjektet, for å analysere litteratur relatert til forskningsfeltet. Litteraturstudiet identifiserte 18 primærstudier. For å akkompagnere funnene fra litteraturstudiet, ble det gjennomført semistrukturerte intervjuer med eksperter innenfor forskningsfeltet. Basert på funnene fra den innledende fasen, ble en fungerende prototype for en digital plattform designet og utviklet gjennom et samarbeid med Leap Learning. Prototypen ble deretter testet på deltakere som representerte prosjektets målgruppe. Observasjon og intervju ble brukt som datagenereringsmetoder for å evaluere prototypen.

Funnene viser at den utviklede prototypen ga deltakerne ny kunnskap og et høyere bevissthetsnivå for cybersikkerhet. I tillegg ble det identifisert fire faktorer for å sikre en vellykket opplæring av cybersikkerthetbevisshet i utviklingsland. Fremtidig forskning kan anvende disse anbefalt faktorene når forsking på cybersikkerhet i en kontekst med utviklingsland utføres.

Nøkkelord: *Cybersikkerhetbevisshet, utviklingsland, ungdom, unge voksne, digital kompetanse, programvareutvikling, systematisk litteraturstudie*

Acknowledgment

I would like to express my gratitude to my supervisor, Professor Letitia Jaccheri, for being a great support and guidance provider throughout this master thesis project. Her enthusiasm and commitment to my project has been indispensable. Additionally, I would like to thank my co-supervisor, PhD. Candidate Farzana Quayyum, for all the valuable feedback and idea sharing she has provided to this project.

This master project was done in collaboration with Leap Learning. I would like to thank Leap Learning, especially the CEO Marit Olderheim, for the close collaboration through the last two semesters. Discussions, idea sharing, and providing access to resources have given this project great value. I would also like to thank the Leap Learning representatives who contributed to the data collection in Gambia.

Furthermore, I would like to thank Save the Children Norway for sharing their knowledge and experiences and contributing to this project.

Lastly, I would like to express gratitude to all the students involved in the *Software for a Better Society* research collective for all the great feedback, discussions, and idea sharing during the weekly meetings over the last two semesters.

Preface

This master thesis was written at the Department of Computer Science The Norwegian University of Science and Technology (NTNU), as part of the course *TDT4900 - Computer Science, Master's Thesis*. The work has been performed under the supervision of Professor Letizia Jaccheri with co-supervision of PhD. candidate Farzana Quayyum.

Contents

Abstract . . . . **iii**

Sammendrag . . . . **v**

Acknowledgment . . . . **vii**

Preface . . . . **ix**

Contents . . . . **xi**

Figures . . . . **xv**

Tables . . . . **xvii**

Acronyms . . . . **xix**

1 Introduction **1**

1.1 Motivation 1

1.2 Research Questions 3

1.3 Research Objectives 3

1.4 Collaboration with Leap Learning 3

1.5 Thesis outline 3

2 Background **5**

2.1 Cyber Security 5

2.2 Developing Countries 6

2.3 Available Digital Resources and Digital Skills 7

2.4 Education in Cyber Security Awareness 8

3 Methodology **11**

3.1 Design and Creation strategy 11

3.2 Data generation 12

3.2.1 Interviews 13

3.2.2 Observation 14

3.2.3 Participant recruitment 15

3.2.4 Guide for observations and interviews 16

3.3 Data analysis 16

3.3.1 Analysis of interview data 16

3.3.2 Analysis of observation data 17

3.4 Ethics 17

4 Systematic Literature Review **19**

4.1 Research Method 19

4.2 Results 23

4.2.1 General findings 23

4.2.2 Cyber security risks 24

4.2.3 Approaches for raising Cyber Security Awareness 25

4.3 Conclusion of SLR 26

5 Collaborative Efforts and Expert Interviews 29

5.1 Collaboration With Leap Learning 29

5.2 Interviews With Experts 30

5.2.1 The goal of the organisations and areas of operation 30

5.2.2 Working with digital expertise and security in developing countries 30

5.2.3 Introducing digital tools for children and adolescents in developing countries 31

5.2.4 Risks young people in developing countries face in the digital world 32

5.3 Takeaways from interviews with experts 33

6 Design and Development 35

6.1 Leap Learning App Universe 35

6.1.1 Technology stack 36

6.1.2 Development Platform 36

6.1.3 Design template elicitation 37

6.2 Content and Functionality elicitation 38

6.2.1 Content elicitation 39

6.2.2 Functionality elicitation 40

6.2.3 Illustrations 42

6.3 App hierarchy of working prototype 42

7 Results 45

7.1 Demographics 45

7.1.1 Age of participants 45

7.1.2 Country of Origin 46

7.1.3 Gender of participants 46

7.1.4 Access to digital devices, internet and social media 46

7.2 Observations 47

7.2.1 Functionality and interaction 47

7.2.2 Language, words and unfamiliar terms 48

7.3 Interviews 49

7.3.1 Participants' reflections from the apps 50

7.3.2 Participants' real life experiences 52

8 Discussion 53

8.1 Designing a digital platform to inform adolescents and young adults in developing countries about cyber security 53

8.2 Factors to consider when educating cyber security awareness in underdeveloped areas 56

8.2.1 Adapting to specific cultures 56

8.2.2 Literacy and language level adaption 57

8.2.3 Introducing cyber security terms 58

8.2.4 Functionality measuring learning outcome 58

8.3 Implication for Research and Practice 58

8.4 Limitations 59

8.5 Future work 60

8.5.1 Implementation of additional CSA topics 60

8.5.2 Modifications and new functionality 60

8.5.3 Distribution through Leap Learning 60
9 Conclusion 63
Bibliography 65
A Data Extraction Form 69
B Consent form 71
C User testing guide 77
D Miro boards 83

Figures

2.1 Map of the Least Developed Countries 6

3.1 Design and Creation research strategy process 12

4.1 Study selection process 21
4.2 Number of papers per publishing year 23
4.3 Number of papers per country 23

6.1 Leap Learning Logic Apps 35
6.2 Snippet of the Leap Learning development platform 37
6.3 Literacy and logic apps using the children-targeted template 38
6.4 Informative and quiz apps using the adult-targeted template 38
6.5 Structured content for "Sharing Private Information" topic in Miro 40
6.6 "About Online Strangers" app views 41
6.7 "Select Sentence" app views 41
6.8 "Priority" app views 42
6.9 Implemented app hierarchy 43

7.1 Distribution of country of origin and gender amongst the participants . . . 46

D.1 Miro board with ideas for "Online Strangers Quiz" 84

Tables

3.1 Expert interview questions 13
3.2 Target group questions 14

4.1 Search string applied in Scopus database 20
4.2 Final papers included in SLR 22
4.3 Cyber security risks addressed in the included SLR papers 25
4.4 Approaches for raising CSA addressed in the included SLR papers 26

7.1 Overview of participants' age and country of origin 45
7.2 Digital device and internet access overview 47
7.3 Distribution of tested apps among participants 47
7.4 Observed words and terms participants struggled with 49
7.5 Reported learning outcome from each participant 50
7.6 Participants' reported pre-existing knowledge 51

A.1 Data extraction template 70

Acronyms

CS Computer Science. 1, 20

CSA Cyber Security Awareness. 1–3, 5, 8, 9, 11, 25–27, 31–33, 38–40, 47, 50, 54–59, 61, 63, 70

GDP Gross Domestic Product. 6

ICT Information and Communication Technologies. 1, 2

ITU International Telecommunication Union. 5

LDC Least Developed Countries. 2, 6, 7, 9, 46, 54, 56, 57, 59

MENA Middle East and Northern Africa. 23

NSD National Centre for Research Data. 17, 18

NTNU The Norwegian University of Science and Technology. ix, 18

RQ Research Question. 3, 13, 19, 20, 53

SBS Software For A Better Society. 1, 3

SDG Sustainable Development Goals. 1, 2

SLR Systematic Literature Review. 3–5, 8, 11, 12, 19–21, 23, 24, 26, 30, 38–40, 53–55, 58–60, 63

SSA Sub-Saharan Africa. 3, 6, 7, 29, 30, 53

UN United Nations. 1, 6

Chapter 1

Introduction

The accessibility of digital devices and online access are increasing across the globe. Over the past two decades, Information and Communication Technologies (ICT)s has become an indispensable part of everyday lives, and the technologies conduce innovation and development. ICTs have the potential to accelerate development in areas such as education and health care in developing countries. While digital development and ICTs can help to improve development and living standards, numerous risks arise with the usage of digital devices and online resources. The risks associated with cyberspace and online presence are well recognized in developed countries, and initiatives have been introduced to provide education and awareness to the public. On the contrary, similar initiatives are lacking in developing nations.

This master thesis explores the design and use of digital tools to raise awareness of the dangers connected to online presence and cyber security, with adolescents and young adults in developing nations as the target group. Through a collaboration with Leap Learning[1], a working prototype of a digital platform teaching Cyber Security Awareness (CSA) was developed. Test sessions consisting of observations and interviews of prototype with target group representatives were conducted in Gambia and Norway.

1.1 Motivation

Cyber security is a subset within the field of Computer Science (CS), emphasizing security measures in the development and usage of software systems. The term "cyber security" is a broad term, which will be further explained in Section 2.1. In this thesis, an emphasis is put on end-user education of cyber security[2] through the use of CS principles, including app development and use of methodologies for researching information systems.

This master thesis is part of the research collective Software For A Better Society (SBS), led by Professor Jaccheri[3]. The research conducted by SBS has a focus on targeting the United Nations (UN)'s Sustainable Development Goals (SDG)[4]. Especially SDG

[1] https://leaplearning.no/

[2] https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security

[3] https://sbs.idi.ntnu.no/

[4] https://sdgs.un.org/goals

number 3 [5] and SDG number 5 [6] are in focus in their research. SDG number 3 concerns health and well-being whilst SDG number 5 concerns gender equality. Their research aims to:

> "*Establish new knowledge about opportunities and challenges posed by the rapidly accelerating pace of technological advances and how they impact the economic, political, environmental, social and technological aspects of society*"[7].

Providing access to digital and online resources is a key factor for progression and growth in developing countries. Concerning SDG number 3, the Covid-19 pandemic revealed the importance of the use of technologies for various health benefits, including remote doctor consultations, contact tracing, digital testing, and digital certificates [1] [2]. In Least Developed Countries (LDC), there exists a gender gap in technology access, ownership and skills [2], which addresses SDG number 5. Another SDG relevant to this thesis is SDG number 9, addressing industry, innovation and infrastructure [8]. The sub-target goal number 9.c aims to:

> "*Significantly increase access to information and communications technology and strive to provide universal and affordable access to the Internet in least developed countries by 2020*"[9].

According to a study by Maoneke *et al.* [3] on cyberspace risks for adolescents in Namibia, pornographic content, exposure to harmful, user-generated content, violent videos, cyberbullying and threatening messages are among the risks that adolescents face online. Initiatives for promoting cyber security awareness amongst this group are lacking in less-developed countries. In less-developed countries, the introduction of CSA to this group of adolescents as they enter the online world could be an effective method to avert future cyber-attacks and threats. ICTs could play a crucial role in children's and adolescents' development opportunities.[4] [5]. However, as the usage of digital technologies expands, the need for increased awareness around online behaviour and cyber security emerges. The drawback of the Internet's rapid advancement is that legislation governing cybercrime, computer literacy, and education has lagged, leaving all internet users vulnerable to cyber attacks and online threats, according to Von Solms and Von Solms [6]. In recent years, research on ICTs in the African region has been concentrated on their abilities to promote developmental projects, with little attention paid to its potential drawbacks. The detrimental implications of children's usage of ICTs are abundantly demonstrated in studies from European, American, and Asian countries [3] [4].

[5] https://sdgs.un.org/goals/goal3

[6]

[7] https://sbs.idi.ntnu.no/

[8] https://unstats.un.org/sdgs/report/2021/goal-09/

[9] https://unstats.un.org/sdgs/metadata/?Text=Goal=9Target=9.c

1.2 Research Questions

The following Research Questions (RQs) will be addressed in this master thesis:

1. **RQ1:** What is the current "State of the Art" of cyber security awareness in developing countries?
2. **RQ2:** How to design a digital platform to inform adolescents and young adults in developing countries about cyber security?
3. **RQ3:** What factors should be considered when educating cyber security awareness in underdeveloped areas?

1.3 Research Objectives

The objective of this master thesis project is to investigate how digital tools can contribute to raising awareness of cyber security in less-developed countries. To provide an overview of previous research conducted on the research topic, a Systematic Literature Review (SLR) was conducted as a part of the course *TDT4501 Computer Science, Specialization Project*. Based on the findings from the SLR, this master thesis project will design and develop an IT artefact through a working prototype of an application aiming to educate CSA to adolescents and young adults in developing countries. In this thesis, *adolescents and young adults* refer to people of all genders between 13 to 30 years of age.

User testing of the working prototype on relevant target users was conducted, both in Norway and in Gambia. From the user test sessions, observations and feedback from the participants were collected. Gaining insights into the target user's digital accessibility and online habits was also an ambition. The findings from user testing and interviews conducted with experts within the research field were used in order to answer the RQs presented in the latter section.

1.4 Collaboration with Leap Learning

This master thesis project was conducted in close collaboration with Leap Learning[10]. Leap Learning is a Norwegian company that develops and distributes digital and analogue tools for education, focusing on children and adults in less-developed areas. They are mainly present in Sub-Saharan Africa (SSA). Leap Learning has collaborated with SBS and acted as a stakeholder in multiple previous research projects.

1.5 Thesis outline

The thesis consists of nine chapters. Chapter 1 is an introduction of the project, including motivation and presentation or research questions and research objectives. Chapter 2 presents background information and concepts as well as related work. In Chapter 3, the research methodology and chosen research strategy are presented and explained.

[10] https://leaplearning.no/home

Chapter 4 provides a summary of the SLR which was conducted in the specialization project, and includes methodology description as well as presentation of findings. Chapter 5 presents collaborative efforts as well as findings from interviews with experts within this field of research. Chapter 6 explain the development process of the IT artefact and explain design choices. Chapter 7 presents the results from the observations and interviews with target group participants, which lays the foundation for the discussion in Chapter 8. Finally, a conclusion is provided in Chapter 9.

Chapter 2

Background

The concepts presented in this chapter are built upon the work presented in the specialisation project, which was conducted in the Autumn semester of 2021 [4]. The project consisted of an investigation of the current research on cyber security awareness in developing countries through a SLR. The results from the SLR are presented in the next chapter. This chapter presents background theory, related work, and concepts.

2.1 Cyber Security

Cyber security is a broad term used to address both risks and security measures to which internet users are exposed. Terms like "online security", "online safety" and "internet security" are used interchangeably in the literature [5]. According to the International Telecommunication Union (ITU), cyber security can be defined as:

> "*The collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to protect the cyber environment and organisation and user's assets. Cyber security strives to ensure the attainment and maintenance of the security properties of the organisation and user's assets against relevant security risks in the cyber environment*".[1]

In this thesis, a focus will be put on the end-user aspect of cyber security. The most unpredictable cyber security aspect, namely people, is addressed through end-user education [2]. Cyber security is also a term that is commonly used to address the practice of protecting systems and networks from various digital attacks [7]. However, in this master thesis, the term does not refer to the technical aspect of security in systems and networks.

Cyber Security Awareness (CSA) is a term which will be referred to consistently through this master thesis. The term "awareness" refers to "knowledge that something exists, or understanding of a situation or subject at the present time based on information or experience"[3]. This thesis investigates different approaches for knowledge and

[1] https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx

[2] https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security

[3] https://dictionary.cambridge.org/dictionary/english/awareness

understanding of risks and preventive measures that can be taken to avoid dangerous situations in a digital, online environment.

2.2 Developing Countries

A "developing country" is a collective designation for countries that suffer from a weak economy and other difficulties that constrain the population's prosperity and welfare [4]. In a developing country, poverty is a widespread problem.

"Developing countries" can be further divided into sub-categories, with LDC being one of them. According toUN, LDCs are categorized as "States that are deemed highly disadvantaged in their development countries for structural, geographical and historical reasons"[5]. They are sensitive to environmental and economic shocks, and their human development levels are poor [4]. Currently, there are 46 countries which are listed as a LDC, which comprises around 880 million people. This equals 12 % of the world's population. In contrast, LDCs account for less than two per cent of the world's Gross Domestic Product (GDP) and around one per cent of world trade [4].

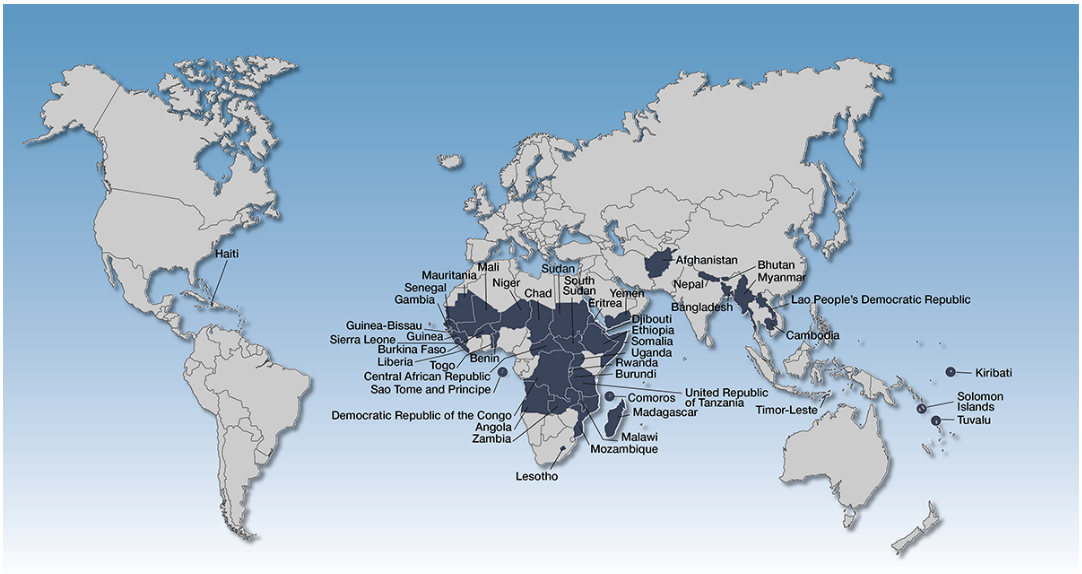


Figure 2.1: Map of the Least Developed Countries Source: https://unctad.org/topic/least-developed-countries/map

The majority of the countries listed as LDCs, 28 in total, are located in the Sub-Saharan region in Africa. All countries south of the Saharan desert are included in Sub-Saharan Africa (SSA). The term is used to describe the current stage of digitisation in low- and developing-income nations in the following section.

[4] https://snl.no/utviklingsland

[5] https://unctad.org/topic/least-developed-countries/recognition

2.3 Available Digital Resources and Digital Skills

There were 260 million estimated internet users in the LDCs in 2020, which accounts for almost a doubling of internet users since 2016, when the estimation was 132 million internet users[6]. 260 million internet users accounts for 25% of the population in LDCs. The average internet penetration rate across the world was estimated to be 63% in 2021, which leaves LDCs with less than half of the world's average penetration rates[7]. By 2025, more than 170 million people across the SSA region will have started using mobile internet for the first time, taking the penetration rate to just under 40% of the population[8]. In the region of SSA, over 40% of the population is under the age of 15. Young consumers owning a mobile phone will be the primary source for mobile growth in the future [9][4].

The gap in smartphone ownership between developed and developing countries are becoming more narrow as many directly move from not owning a phone at all to having a smartphone [8]. A survey conducted by Poushter *et al.* [8] in 2018 shows that internet usage is much more common among young users than older users. In Ghana, Kenya, Nigeria, Senegal, South Africa and Tanzania, the reported internet and smartphone use amongst adults aged 18-36 years were between 49-73%, whilst between 17-44% for adults older than 37 years old. The use of social media in developing countries is also on the rise. The latter survey also reported a 12% increase in the use of social media platforms in Ghana, Senegal, and South Africa between 2015 and 2017 [8].

In a paper published in April 2022, Aruleba and Jere [9] has explored the challenges of digital transformation in rural areas in the wake of the Covid-19 pandemic. The Covid-19 pandemic accelerated the technology use and development worldwide and underlined the importance of less-developed and rural areas not being left further behind in the digital gap. Aruleba and Jere [9] state that it is not enough to provide rural areas with digital equipment and connectivity. Although it is a crucial step in the right direction, training, adapting and learning the correct usage of the digital are just as important. Digital connected living has the potential for improving education, social well-being, health and alleviation of poverty. The systematic review of empirical studies by Arubleba et al. is conducted with the target being rural communities in South Africa. However, the findings are transferable to other less-developed and rural areas across the SSA region.

The statistics presented in the latter sections signify a rapid rise in internet usage in countries where cyber security legislation and online awareness programs are not prioritised. In LDCs, the internet users often only hold rudimentary digital skills and are prone to cyber threats, online abuse, misinformation and other negative impacts. The first meeting people have with the internet is often through a social media platform where they learn the minimum skills from friends and family. Lack of security training leaves users vulnerable. These countries are facing an immense challenge in providing digital literacy, and security training for their populations [2].

[6] https://www.itu.int/en/myitu/Publications/Connectivity-in-the-Least-Developed-Countries-Status

[7] https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

[8] https://www.gsma.com/mobileeconomy/wp-content/uploads

[9] https://www.gsma.com/mobileeconomy/wp-content/uploads

2.4 Education in Cyber Security Awareness

Quayyum *et al.* [5] conducted a SLR to map out cyber security risks faced by children and different approaches used in raising cyber security awareness for children. The paper presents a thorough study of 56 papers selected through a SLR process. The findings from the literature review revealed a broad spectre of cyber security risks to which children can be exposed. Amongst the risks were: online privacy risks, online harassment, content-related risks, sexual solicitation, password practices, technology-based threats and social engineering.

The paper also presents various approaches for raising cyber security awareness from the findings in the SLR. Game-based learning, training, intervention, gamification, and a warning approach are amongst the approaches found. A particular focus is paid to cyber security training and game-based learning methods [5].

As the SLR by Quayyum *et al.* [5] addresses similar issues to the objectives of this master thesis, it has value as related work. It also represents a great example of how to conduct an adequate SLR. However, the vast majority of the papers included in the SLR are based on research conducted in well-developed countries. Also, the paper focuses on cyber security awareness for children, whereas the target group of this master thesis are adolescents and young adults from 13-30 years of age.

Svabensky *et al.* [7] conducted an SLR to discover what topics are commonly researched and what topics are underrepresented in educational papers about cyber security. The SLR also presents findings of common cyber security teaching practices. The majority of the papers in the findings were related to data security, but the findings also included topics related to privacy, societal impact, authentication and cyber-attacks. In 54 of the 71 examined papers in the SLR, the target group were college or university students in the United States [4].

Grobler *et al.* [10] evaluated the level of CSA in rural communities in South Africa in 2011. The data collection was done through a series of exploratory surveys. Based on findings from the surveys, Grobler et al. proposed a CSA program for educating basic computer security and safe online habits to beginner internet users [10]. The study concluded that the findings in the surveys pointed toward low levels of awareness of the consequences of participation in social networks. Further awareness training in rural districts was necessary in order to improve the level of CSA. The target goal and methods implemented in this paper are similar to the objectives of this master thesis project. However, the study was conducted in 2010, and the findings could be considered outdated in light of the rapid technological development over the last decade.

Teaching CSA is not a new phenomenon and has been a focus in western and well-developed countries for many years. There are several tools, games, courses, and other learning activities available to educate people on the dangers of using the internet. Children and teenagers are the focus of a vast number of available courses and resources. One example of this is the prevalent teaching framework *Be internet Awesome*, created by Google [10]. The program consists of an interactive online game called "Interland", as well as a curriculum framework for teachers [11]. The program teaches children about cyberbullying, online privacy and password habits.

Programs like *Be internet Awesome* are contributing to helping teachers, parents and

[10] https://beinternetawesome.withgoogle.com/en$_u$$s$/

children navigate and create a safer environment online. However, most programs like these are aimed at an audience located in well-developed countries. Many children in these regions have grown up in a digital world, with digital devices easily accessible. People in LDCs, on the other hand, may not have had the same upbringing and may encounter the digital world for the first time without any prior knowledge. There exists many studies on CSA conducted in well-developed countries, such as the studies by Quayyum *et al.* [5] and Svabensky *et al.* [7]. However, only a limited amount of research is conducted on cyber security and CSA with target groups from less-developed countries.

Chapter 3

Methodology

In this chapter, the research strategy and applied methods are presented. The *Design and Creation* research strategy following the principles of Oates [12] was chosen. The data generation methods consist of semi-structured interviews and observations.

3.1 Design and Creation strategy

The Design and Creation strategy is a research strategy which focuses on the development of IT products, which could also be referred to as *IT artefacts*. For a project which develops a new computer-based product to be considered as research, not only technical skills are to be demonstrated but also academic qualities such as analysis, explanation, argument justification and critical evaluation, according to Oates [12]. The project is intended to contribute to new knowledge.

According to Oates [12], research within the Design and Creation field could consist of research where the IT artefact is the main focus in itself. It could also consist of research where the IT artefact acts as an instrument for contribution to knowledge. The main objective of the Design and Creation strategy is to investigate what happens when an IT artefact is used in a real-life context. In this project, both of the research types are transferable. The project's objectives are to raise knowledge about cyber security through a digital application and investigate how the application in itself contributes to this purpose.

A design and creation should, according to Oates [12], follow a five step process consisting of the following steps:

1. **Awareness:** recognizing and identification of a problem which needs to be solved.
2. **Suggestion:** a tentative solution to the problem.
3. **Development:** developing the design of the suggested solution.
4. **Evaluation:** examination of the designed artefact.
5. **Conclusion:** description of results from the design and development process, to evaluate to what degree the artefact contributed to solving the problem.

In this project, the awareness and suggestion steps were conducted during the specialisation project in the autumn semester of 2021, which included a Systematic Literature Review (SLR) on Cyber Security Awareness (CSA) in a context of youth and developing countries. Based on the results from the SLR, a suggestion of cyber security themes which should be included in the application was found. Oates [12] underlines that the five steps included in the Design and Creation strategy must not be followed in a rigid, step-wise fashion but should follow an iterative cycle. To accompany the information and results provided in the SLR, an expert interview was conducted in February 2022. The methodology applied to conduct the SLR is described in section 4.1.

Prototyping was chosen as the preferred system development methodology, addressing the third step in the five-step process of the Design and Creation strategy. Due to the possibility of developing a prototype through iterations and exploring new possibilities throughout the development phase, prototyping was considered the best-fitted system development methodology. In this project, the result is a *working prototype*, meaning that even though it is a prototype, it is implemented and could be used in a real-life context. The prototyping phase and implementation will be further described in chapter 6. Figure 3.1 visualises the study process of this thesis, following the five steps in the Design and Creation strategy and including the applied data generation methods in each step.

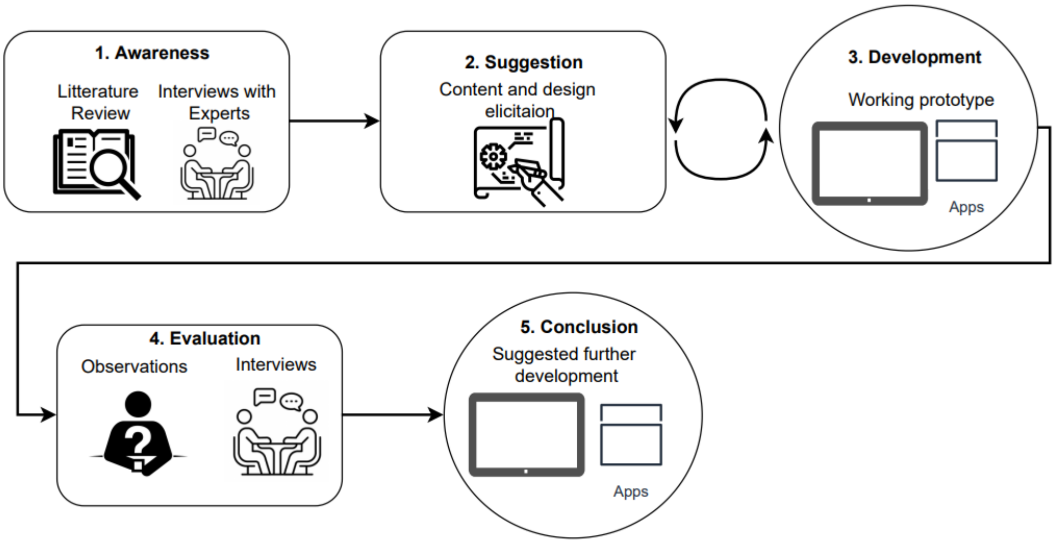


Figure 3.1: Design and Creation research strategy process

3.2 Data generation

According to Oates [12], evaluating the developed IT artefact in a real-world context to some degree is expected in Design and Creation, addressing the fourth step in the five-step process. Design and creation research often uses data generation methods such as interviews, observations, or questionnaires to evaluate the developed artefact. This section describes the method for collecting data for this project.

3.2.1 Interviews

Interviews were chosen as the preferred data generation approach to gather additional insights pre-development through expert interviews and to gain insights into target users' evaluations of the generated IT artefact post-development.

Interviews are a suitable generation method when the goal is to obtain detailed information about complex and sensitive issues. Oates [12] describes that by collecting data for requirement specification and eliciting user feedback on a finished design, interviews can 'top-and-tail' a design and creation strategy, which are the two purposes interviews were used for in this project.

Expert Interviews

The expert interviews were held in a semi-structured manner, following the definition of Oates [12]. A pre-defined list of questions was prepared prior to the interview, but it was not acquired to follow the order of the questions rigorously. Additional questions were asked when the interviewee brought up issues that the interviewer initially had not prepared for. The purpose of using this semi-structured approach is for the interviewee to speak their minds, leading to the discovery of new perspectives. The questions were derived based on the RQs and aimed to address and encourage discussion around the three RQs. Questions regarding the organisations' experiences with online risks aimed to address RQ1. Questions addressing the organisations' reflections and experiences with the introduction of digital tools in developing countries and rural areas, applied to RQ2 and RQ3. Table 3.1 contains the complete list of questions prepared for the expert interview sessions.

The expert interviews were conducted digitally, and both video and sound were recorded. After the interviews, the sound files were transcribed into text. As the interviews were semi-structured, not all of the answers were relevant to the theme of this master thesis. Extraction of the relevant answers was carried out, and the results are presented in chapter 5.

Questions
What is the main goal of your organization?
In what areas does your ogrnization operate?
What does your organization do in terms of working with digital expertise and/or digital security in developing countries?
What do you consider the positive and negative aspects of introducing online tools to children/adolescents in developing countries?
Do you have any experience introducing digital tools in areas with low digital literacy?
What to you think are the biggest threats facing young people in developing countries in the digital world today?
Do you think there are any special considerations which should be taken based on gender, and whether the content of the application should be adapted in relation to it?
Do you have any other input or tips that might be relevant to the master project?

Table 3.1: Expert interview questions

Interviews of participatory target users

As part of evaluating the working prototype of the developed IT artefact, test sessions on participants from the relevant target group were conducted. The sessions consisted of observing the participant interacting with the application, followed by an interview. The observation method is described in subsection 3.2.2.

The interviews were held in a semi-structured manner. Some of the interviews were conducted by representatives from Leap Learning on behalf of the author of this master thesis. In order to validate the results, each participant needed to be asked the same questions. When analysing results from multiple participants, the data has to be generated based on the same basis. However, there was room to ask follow-up questions if the interviewer saw it as necessary or for the interviewer to reformulate the question if the participant did not understand the initial formulation of the question. Thus, compared to the expert interviews, where there was more room for follow-up questions and discussion, the interviews with participants had to follow a more structured approach.

The purpose of the follow-up interviews was to provide demographic information about the participant and the participants' feedback and reflections on the tested application. Demographic information included age, country of origin, the users' previous experience with online tools, and obtaining the participants' feedback after interacting with the working prototype. Table 3.2 contains the questions included in the follow-up participant interview.

Questions
How old are you?
What is your country of origin?
What gender do you identify as?
Do you have any access to digital devices and Internett in your life?
Have you received any training education on cyber security awareness before?
Do you have an email account?
Do you have any sort of social media account? Like WhatsApp, Facebook or Instagram?
Did you learn anything new when using the application? If yes, can you mention something you learned?
Was there any information that you were presented with in the app that you knew from before? If yes, what did you already know?
Did you have any difficulties understanding how to use any of the applications?
How you find the language in the app? Was it difficult to understand?
Which part of the application did you enjoy the most?

Table 3.2: Target group questions

3.2.2 Observation

Observation can be used in the early design stages in order to understand the target user's needs or later in the design and development phase in order to examine to what degree a prototype meets the target user's needs [13]. In this project, the observation method was chosen to test the latter. However, the goal of testing and observing was also to understand users' needs for future development.

To gain insights and evaluate how the participants interacted with the applications, 'overt' observation of participants was used as a data generation method. Oates [12] explains 'overt' research as observation where the participant knows that they are being observed. Allowing the participant to consent to be part of the research is critical in this master thesis project due to privacy considerations. The opposite of 'overt' research is 'covert' research, where the participants are not aware that they are being observed [12]. The 'covert' observation approach did not apply to this study due to the ethical issues that arise when the participant cannot consent to participation.

A systematic observation approach was used to observe the participants testing the functional prototype. In a systematic observation, pre-defined events are observed, and each participant is asked to perform the same tasks. A facilitator, who also holds the role as the observer, is responsible for explaining the test's purpose and giving the participants tasks to perform. The role of the facilitator also includes observing and documenting the participant's behaviour and other events when solving the given tasks. The approach consisted of a participant and a facilitator, where the participant conducted a user test on parts of the working prototype. Prior to the observation sessions, participants were asked to read and think out loud, following the principles from Ericsson and Simon [14]. Documenting observations becomes easier for the facilitator when the participants say their thoughts aloud, as the observer can gain insights into their thought processes. The facilitator documented the behaviour and interactions of the participant by taking notes in an observation table, which is provided in the user testing guide in Appendix C.

3.2.3 Participant recruitment

When beginning the master project in the autumn of 2021, the initial idea was to travel to a developing country to perform user testing. By travelling to a developing country, one would be able to best reach the target group in a realistic setting and most likely get the most accurate results in observation and user testing. However, the COVID-19 pandemic was still raging worldwide during this time, making it challenging to plan travels. When the Omicron virus variant occurred in South Africa in late November of 2021, travel plans were put on hold. Instead, other options had to be considered.

Participants in Norway

Options for conducting user tests in Norway on the relevant target group were planned out. In search of participants who had recently arrived in Norway from a developing country, different education centres for adolescents and young adults, which offers primary and high school level teaching for immigrants and refugees, were contacted.

After contacting different education centres in Trondheim and Oslo, a meeting at one of the Education Centres in Oslo was held. This centre was already working with Leap Learning through their physical Leap Learning Labs [1] they had implemented in their school. Thus, the teachers were already familiar with Leap Learning and showed

[1] https://leaplearning.no/learning-labs

eagerness to contribute to the project. A date was set for conducting the user testing in April 2022, and recruiting of relevant participants was initiated.

Participants in Gambia

In the spring of 2022, a new opportunity of testing in a developing country presented itself as some representatives from Leap Learning were going to travel to Gambia and stay at one of their collaborative education centres. Considering the author of this master thesis could not travel herself, it was decided that the Leap Learning representatives could conduct the user testing in her stead. As the application development was conducted in close collaboration with Leap Learning, they already had insights and knowledge about the project. Thus, it was considered feasible and sound to let representatives conduct the user testing in Gambia.

The participants in Gambia were students at one of Leap Learning's partner schools, and Leap Learning representatives recruited participants through conversations with students.

3.2.4 Guide for observations and interviews

Representatives from Leap Learning held the role of facilitators for the testing in Gambia. They needed to be provided with a consistent and straightforward guide for the tasks for the observation sessions. Oates [12] mentions that one of the advantages of using systematic observation is that it is possible to include assistants in your research, as the tasks are the same for all of the participants. However, the procedures must be clear to everyone involved. Prior to the testing in Norway and Gambia, a meeting between involved parts was held, where the Leap Learning representatives had been provided with a user testing guide in advance. The guide contained clear instructions on what to do before, during and after the testing. During the meeting, the representatives got to ask questions concerning the guide, which resulted in minor changes and clarifications. By having this discussion meeting, all involved parts were on the same wavelength before conducting the testing. This was very important to obtain the most correct and unbiased results possible. The user testing guide can be found in Appendix C.

3.3 Data analysis

The collected data consisted of notes and comments from the observation phase and audio files from the interviews. From the expert interviews, audio files were recorded.

The data from the participatory target group and interviews with experts were mainly analysed using qualitative analysing methods. Qualitative analysis was chosen as the primary analysis approach due to the type of collected data. According to Oates [12], qualitative data analysis involves abstracting the verbal, visual or aural themes and patterns which are believed to be important to the research topic.

3.3.1 Analysis of interview data

The raw audio transcriptions were the starting point for the interviews, followed by identifying key themes in the transcription. Identification of key themes follows the approach suggested by Oates [12] and consists of segmenting the data into three parts:

1. Segments that bear no relation to the overall research purpose (not needed for this specific study)
2. Segments that provide general descriptive information that will be needed in order to describe the research context (e.g. location of the organisation, the organisation's main goal)
3. Segments that appear to be relevant to the research questions.

The expert interviews were held in a semi-structured manner, causing off-topic discussions. These discussion parts were removed from the results. The remaining results were then organised with the answers from both interviews and categorised under a relevant theme. The analysis presented in Section 5.2, which addresses the findings.

No data was removed for the interviews of target users as the interviews were more structured and contained fewer topic derailments. Each answer was added to a structured analysis sheet, making it easier to analyse the contents. Quantitative analysis of qualitative data, such as recording the age of each participant and numerically displaying the participant's demographic data, was conducted. This analysis was conducted to document that the participant fit the target user and discover other findings such as the user's digital level.

Preece *et al.* [13] suggests conducting content analysis which aims to make "collections" of answers which illustrate or address similar issues. After testing the applications, this method was used to analyse the participant's impressions. A focus was also on analysing the participants' real-life experiences, as they could address issues that the direct questions might not apprehend.

3.3.2 Analysis of observation data

For the data from the observations, qualitative categorisation analysis as described in Preece *et al.* [13] was conducted. This approach involves looking for incidents and patterns in the observation notes of each participant. A pattern or incident could, for example, be critical incidents where a participant is struggling with a task. Another incident could be comments made by participants during the test session.

A quantitative analysis of qualitative data was conducted to numerically display common issues such as pressing the wrong button or other interaction issues.

3.4 Ethics

When collecting data from experts in the field and target users for research purposes, following ethical principles is essential. Prior to the expert interviews and user testing sessions, each participant was introduced to the purpose and objectives of their participation. They were also informed about their right to withdraw from the process.

All participants signed a consent form following the standards from National Centre for Research Data (NSD). The form explained the purpose of the research, why they were asked to participate, how the collected data would be stored, and their withdrawal rights. A research application for both data collection groups was approved by the NSD. The consent form for participation can be found in Appendix B.

As the target user group included adolescents under the age of 18 years as well as it was desirable to document each participant's ethnically background, strict guidelines required by the NSD had to be followed. Obtaining consent from participants younger than 16 required a parent or guardian consent signature.

Following the requirements from NSD, Microsoft Teams[2] was used to store the collected data such as audio files and transcripts. NTNU has a processor agreement with Microsoft[3], and all access to the private channels which contained the sensitive data was password protected. This sensitive data will be deleted when the master thesis is submitted and graded.

[2] https://www.microsoft.com/nb-no/microsoft-teams/group-chat-software

[3] https://www.microsoft.com/nb-no/about

Chapter 4

Systematic Literature Review

In the specialization project conducted in the Autumn semester of 2021, a SLR was conducted as a contribution to answering the following research questions:

1. **RQ1:** What is the current "State of the Art" of cyber security awareness in developing countries?

The term "State of the Art" refers to the current contributions and newest development in the field of research. The following sections summarize the methods and results of the SLR.

4.1 Research Method

A prerequisite for conducting a study using the Design and Creation strategy is the necessity of relevant and unbiased information on the field. A systematic and thorough mapping of existing literature following the principles and guidelines presented by Kitchenham and Charters [15]: *Guidelines for performing systematic literature reviews in software engineering* was thus considered the best fitting approach.

Kitchenham et al.'s method consists of the following five-step approach:

Step 1. Data collection
Step 2. Inclusion and exclusion strategy
Step 3. Manual search
Step 4. Quality assessment procedures
Step 5. Data analysis

Data collection

To collect relevant research data, the academic citation database Scopus[1] was chosen as the preferred source. Formulating the best-fit search string that would yield an acceptable result in terms of size and relevancy was critical. The applied search string and the number of papers in the search result are presented in Table 4.1.

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

Database	Search string applied	Result
Scopus	(cyber OR online) AND develop* AND countr* AND security	1 185

Table 4.1: Search string applied in Scopus database

The results from the Scopus search were then filtered to be associated with the Computer Science (CS) field. After a brief comparison of the results with and without the filter applied, it was decided that applying the filter was reasonable. After the filtering, 672 results remained. The references from these results were downloaded to the reference management tool Endnote[2]. Each downloaded reference included the title and abstract. Then followed multiple filtering rounds on the papers in the results, using the grouping functionality in Endnote. The filtering rounds were based on the relevance of the title, followed by the relevance of the abstract.

Inclusion and Exclusion Criteria

For the final round of filtering, exclusion and inclusion criteria were formulated. The criteria were formulated based on the RQs, following the example of Kitchenham and Charters [15][4]:

Exclusion:

1. Studies not written in English
2. Studies focusing on governmental cyber security and cyber security policies/infrastructure
3. Studies on cyber security in businesses and organizations
4. Studies focusing on cyber-warfare

Inclusion:

1. Study focusing on cyber security awareness in developing countries
2. Study focusing on cyber threats for adolescents and young adults in developing countries
3. Studies on existing applications supporting cyber security awareness in developing countries
4. Studies proposing approaches for implementing awareness programs in developing countries
5. Presented empirical (qualitative or quantitative) data on cyber security awareness research in developing countries

The inclusion criteria provided in Quayyum *et al.* [5] were used as inspiration for the criteria in this SLR.

Quality Assessment

The final step in the study selection process was to assess the quality of the included studies. Based on the quality attributes suggested by Kitchenham and Charters [15]:

[2] https://endnote.com/

rigorous, credible and relevant, the following criteria had to be fulfilled in order to be included as a selected paper in the SLR:

1. The study is based on research
2. There is a clear statement of the aim of the study
3. There is a well-described context and methodology that is easy to follow

Figure 4.1 shows a visualization of the study selection process. The final 18 selected studies are presented in Table 4.2.

Data Analysis

A data extraction form was created to extract data from each included paper systematically. The extraction form contained fields for general information about the paper, as well as fields for type of research methodology, data collection instrument, data analysis, and findings. The extraction form template is included in Appendix A.

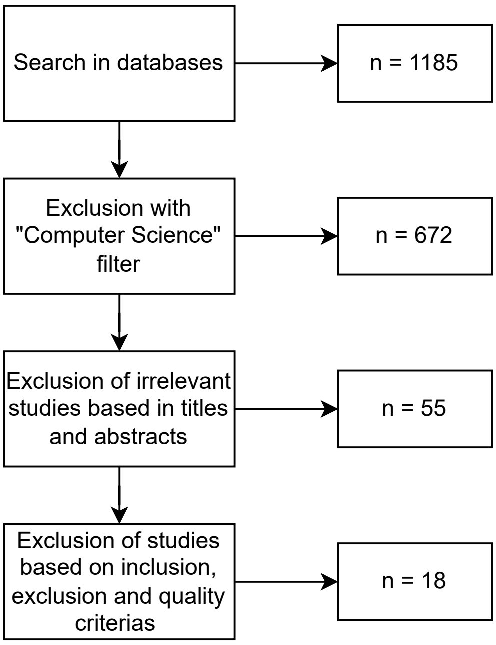

Search in databases
n = 1185
Exclusion with "Computer Science" filter
n = 672
Exclusion of irrelevant studies based in titles and abstracts
n = 55
Exclusion of studies based on inclusion, exclusion and quality criterias
n = 18

Figure 4.1: Study selection process

Study	Year	Title
Adelola *et al.* [16]	2015	*The urgent need for an enforced awareness programme to create internet security awareness in Nigeria*
Oyelere *et al.* [17]	2015	*Cybersecurity issues on web-based systems in nigeria: M-learning case study*
Von Solms and Von Solms [6]	2015	*Cyber safety education in developing countries*
Onwuka *et al.* [18]	2016	*Survey of on-line risks faced by internet users in the Nigerian telecommunication space*
Alotaibi *et al.* [19]	2017	*A survey of cyber-security awareness in Saudi Arabia*
Ahmed *et al.* [20]	2018	*Cybersecurity awareness survey: An analysis from Bangladesh perspective*
Maoneke *et al.* [3]	2018	*ICTs use and cyberspace risks faced by adolescents in Namibia*
Rho *et al.* [21]	2018	*Differences in online privacy and security attitudes based on economic living standards: A global study of 24 countries*
Visoottiviseth *et al.* [22]	2018	*POMEGA: Security game for building security awareness*
Calderwood and Popova [23]	2019	*Smartphone cyber security awareness in developing countries: A case of Thailand*
Owusu *et al.* [24]	2019	*Preliminary insights into the concerns of online privacy and security among millennials in a developing economy*
Chang and Coppel [25]	2020	*Building cyber security awareness in a developing country: Lessons from Myanmar*
Dassanayake *et al.* [26]	2020	*AwareME: Public awareness through game-based learning*
Datta *et al.* [27]	2020	*Data Analysis of Cyber Security for Women in Haryana*
Herkanaidu *et al.* [28]	2020	*Towards a Cross-Cultural Education Framework for Online Safety Awareness*
Jawad and Tout [29]	2020	*Introducing a Mobile App to Increase Cybersecurity Awareness in MENA*
Reichel *et al.* [30]	2020	*'I have too much respect for my elders': Understanding South African mobile users' perceptions of privacy and current behaviors on facebook and WhatsApp*
Veiga *et al.* [31]	2021	*Cyber4Dev-Q: Calibrating cyber awareness in the developing country context*

Table 4.2: Final papers included in SLR

4.2 Results

The results from the data extraction of the included papers consisted of general findings, cyber security risks addressed in the papers as well as approaches presented in the papers.

4.2.1 General findings

The studies included in the SLR were published between 2015-2021. Figure 4.2 displays an overview of the number of papers per publishing year. Figure 4.3 displays the countries in which the research in the papers was conducted.

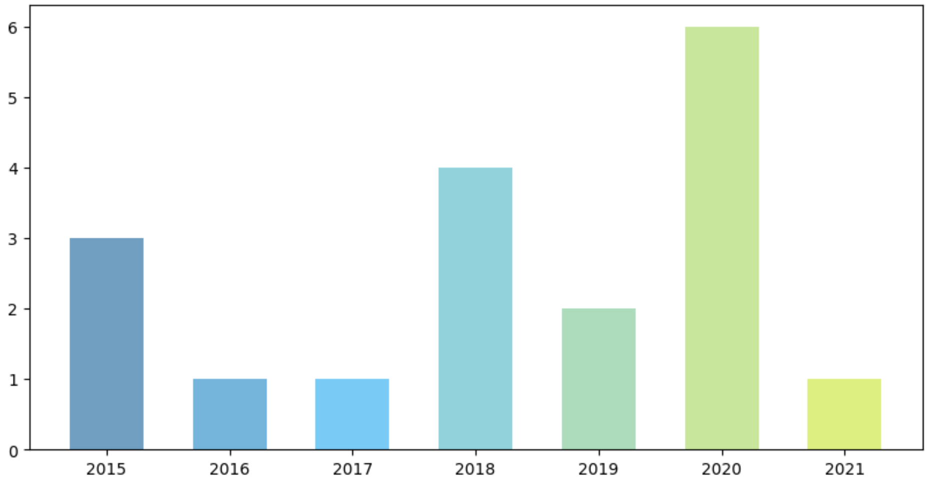
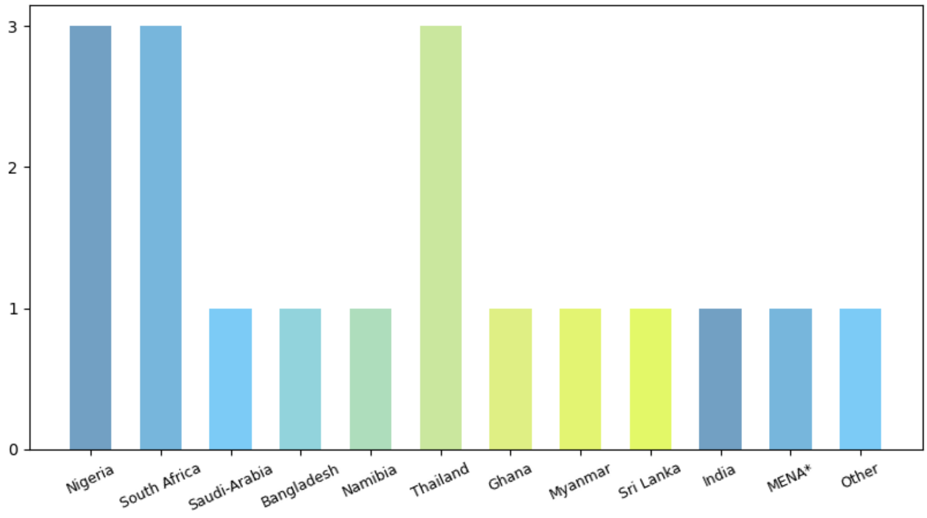


Figure 4.2: Number of papers per publishing year

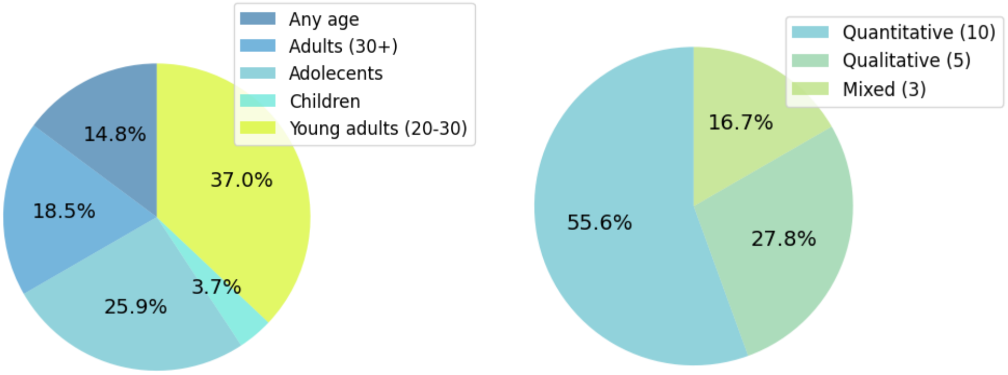


**Middle East and Northern Africa (MENA)*

Figure 4.3: Number of papers per country

Figure 4.4a displays the distribution of different age groups in the studies. Adolescents and young adults constitute a target group in the majority of the studies included in the SLR. However, there were only a limited amount of studies where this group was targeted, and thus studies with other target groups were also included.

Figure 4.4b displays the distribution of research methodology among the studies included in the SLR. The studies mainly used Design and Creation and Surveys as research strategies, where interviews and questionnaires were the most used data generation methods.



(a) Age distribution of participants in the studies

(b) Methodology distribution

4.2.2 Cyber security risks

As a part of the "State of the Art" of cyber security awareness, the risks addressed in the 18 included studies were systematically mapped out. The risks addressed in each paper were categorized under the four categories formulated by Von Solms and Von Solms [6]:

1. **Technology-based threats**, including the spreading of malware, spyware and hacking.
2. **Content-related risks**, where a person is subjected to harmful or offensive content, or where a person is influenced to produce and distribute such content.
3. **Threat of harassment**, which includes any form of unwanted contact or attention.
4. **Exposure-related threats** that include any situation where personal or sensitive information is exposed.

The results are summarized in Table 4.3. This result made up the foundation of what topics would be addressed in the IT artefact.

Category	**Studies**	**Risks**
Techology-based threats	[16], [17], [6], [18], [19], [20], [23]	Malware infection/software, weak antivirus knowledge, use of unprotected networks, hacking, email spoofing, DoS attacks, spam, IRC crime
Content related risks	[6], [18], [20], [3], [28], [30]	Pornography, child pornography, online violence, hatered and religious extremism materials, human rights violations, hate speech, obscene or offensive content, online game addiction, Exposure to sites discussing; committing suicide, self-harm, drugs, sexual content, promotion of eating disorders and hate messages aimed at particular groups and individuals
Threat of harassment	[6], [18], [3], [25], [28], [30], [31]	Cyberbullying, unwanted sexting, "being nasty to others", catfishing, online ’friends’, unwanted messages on social media, online stalking, net extortion, fraud via social media, child soliciting and abuse
Exposure related threats	[17], [18], [19], [20], [3], [21], [22], [23], [24], [25], [26], [28], [30], [31]	Sensitive data storage, weak passwords, use of personal info in passwords, no regular change of passwords, phishing emails, identity theft, oversharing personal/private information

Table 4.3: Cyber security risks addressed in the included SLR papers

4.2.3 Approaches for raising Cyber Security Awareness

Methods for raising CSA which were presented or tested in the included studies were mapped out. The different approaches and test results gave insights and ideas for developing the planned IT artefact.

Table A.1 displays an overview of the different approaches each paper describes. 7 out of the 18 collected papers presented and evaluated approaches for raising CSA in developing countries. The approaches varied from concrete guidelines for creating awareness programs, social media campaigns, and digital applications such as mobile security game apps and learning platforms. Storytelling, quizzes, cartoons and videos were amongst the methods used to educate CSA.

Study	Year	Approach
Von Solms and Von Solms [6]	2015	YouTube videos with follow up questionnaires
Visoottiviseth *et al.* [22]	2018	Online awareness app using gamification Contains six main functions: user record, game storytelling, tutorial, evaluation, certificate, and the hall of fame
Chang and Coppel [25]	2020	Social media campain "Cyber Baykin" Story telling through comic characters
Dassanayake *et al.* [26]	2020	Mobile game-based learning platform "AwareME" for public awareness Puzzle, quiz and an interactive UI
Datta *et al.* [27]	2020	Workshops on cyber security awareness
Herkanaidu *et al.* [28]	2020	Process for creating a awareness program tailor-made for a country
Jawad and Tout [29]	2020	Mobile app to educate cyber security and increase awareness of information assurance and cyber crimes

Table 4.4: Approaches for raising CSA addressed in the included SLR papers

4.3 Conclusion of SLR

15 of the 18 papers pointed out existing risks and disclosed that attempts had been made to map our cyber security concerns in recent years in developing countries. Although the studies had been conducted in 12 different developing countries, the level of digital literacy greatly varied among the participants in the different studies. The level of awareness of cyber security risks was reflected in the level of digital literacy [4].

From the various risks which were addressed in the papers included in the SLR, there were risks within several categories which were more prominent. In this master thesis, an emphasis will be put on addressing risks within these categories. The following CSA risk categories should be addressed in the IT artefact:

- Harmful content
- Interaction with strangers online
- Cyberbullying
- Password habits
- Sharing private information online
- Phishing attacks
- Identity theft

Guidelines and frameworks, as well as social media campaigns and game-based applications, were used to raise CSA. A common focus in the papers was the importance of customization of the contents to fit the target user. In order to achieve this, it is critical to map out the target user's digital literacy level [4].

Reviewing of the different approaches applied in the studies revealed several different methods used to disseminate information within the CSA field. Storytelling and use of gamification elements in order to challenge and measure the user's progress and CSA level will be of relevance when developing the IT artefact in this thesis.

Chapter 5

Collaborative Efforts and Expert Interviews

In this chapter a presentation of the collaboration with Leap Learning and a summary of the findings from the interviews with experts is provided.

5.1 Collaboration With Leap Learning

The partnership with Leap Learning[1] began during the specialisation project in the Autumn semester of 2021. Leap Learning held role as a stakeholder in this master thesis project and contributed with technical resources, knowledge, and experience after many years of working with education and operating in rural areas in developing countries. Their expertise and experience with introducing digital services in rural areas for educational purposes made them a fitting stakeholder and partner in this project.

A part of the collaboration with Leap Learning was developing and implementing the IT artefact through their platform. The final artefact designed and developed in this master thesis project would thus become a part of the "Leap Learning App Universe"[2], which is the collection of the applications which Leap Learning offers. The app universe is further explained in Section 6.1.

There are several reasons for this decision. Firstly, using the resources of Leap Learning would provide access to a well functional development platform, which would drastically shorten the time from suggestion to production. Another reason was the audience the apps in the Leap Learning App Universe could reach, with their presence in numerous developing countries, mainly in the Sub-Saharan Africa (SSA) region.

Developing a working prototype made it possible to quickly create an application that could be used in a real-life setting. When the application was ready to be built, it could be distributed in the Leap Learning App Universe and made available to users rapidly. It also allowed the project to test the working prototype and interview participants in the target group in a real-life setting, which was highly valuable.

[1] https://leaplearning.no/home

[2] https://leaplearning.no/apps

5.2 Interviews With Experts

To accompany the results from the SLR, interviews with experts within the field of cyber security, developing countries, and adolescents were conducted. The interviews were conducted early in 2022 with representatives from Save the Children Norway and Leap Learning. The goal of the expert interviews was to obtain further insights into the theme of the master thesis by learning more about the organisations and their operations worldwide. Another purpose of conducting expert interviews was to gain additional insight into how they have previously worked with introducing digital services in developing countries and rural areas. The interview method is described in Section 3.2.1. A summary of the findings from the two interviews is presented together in the following sections.

5.2.1 The goal of the organisations and areas of operation

The main goal of Leap Learning is to change how education happens in the world through innovative solutions. They believe in an approach of teaching children and adults in developing countries to "learn to learn". They operate mainly in the African region and Sub-Saharan Africa (SSA). In addition, they provide their "Leap Learning Labs" in some schools in Norway. Their long term goal is to reach all parts of the world.

The overall goal of Save the Children Norway is to work to fulfil children's rights, with a particular focus on safety, survival and the right to education. Save the Children Norway is an organisation under the large *Save The Chidren* alliance, consisting of 120 member countries. Save the Children focus on children in the most vulnerable situations, whether this is climate disasters, was zones or disabled children. In the Norwegian section, they also work with providing support for programs in other countries. Through funding from donors like Norad[3], The Ministry of Foreign Affairs[4] and other large institutions, as well as private donations from individuals. The donations are spent on projects in other countries, where they cooperate with Save the Children offices in other countries.

5.2.2 Working with digital expertise and security in developing countries

Leap Learning explained that they do most of their work and training by providing their students with a tablet. The students learn to use and navigate a tablet, interacting with the "Leap Learning App Universe" educational apps. However, they have not addressed security in their educational programs yet, which is their motivation to participate in this master thesis project.

Save the Children explains that any questions about how children's rights are transferred to the digital space. The digital space is where countries may not have legislation to ensure children's rights are fulfilled. They work towards figuring out:

> "What do children's rights mean online?".

[3] https://www.norad.no/

[4] https://www.regjeringen.no/no/dep/ud/id833/

In this, they underline how protecting children's rights became a challenge during the Covid-19 pandemic when education and school were abruptly moved into the digital space:

> "Who is responsible for safeguarding their rights when home-schooled?"

They work for the accountability of relevant authorities, whether that is the government, schools or aid organisations.

In Save the Children's educational programs, they use digital tools as an integrated part, and they work towards providing awareness among the users, including both children and adults. However, they admit that they are lagging behind and that they only recently have shifted their focus from education teachers and adults to targeting the children. They are working towards applying CSA into all their work and explain that they got a push with the arrival of the Covid-19 pandemic:

> "We have a bias, which has taken time to acknowledge, that children are digital users also in developing countries. Now we understand how many children are online and occasionally use digital components. Just because there is no internet in a rural village does not mean that the children are not using a digital device occasionally."

Save the Children work structurally with the authorities to put in place suitable systems that provide a safety net for children online. They also work with parents to raise awareness among parents and other adults around the children. They underline the importance of working directly with the children, as they are the ones who can tell what the challenges are and what dangers and opportunities exist. It is critical to understand it through the children's experiences.

5.2.3 Introducing digital tools for children and adolescents in developing countries

Save the Children points out the importance of facilitation and providing digital access for children and youth in developing countries. If children and youth in developing countries are not provided access, they fall further behind in development. For example, they point out politically active youth and how social media provides them with a platform for spreading their political message. However, being politically visible on social media can also pose a threat. Save the Children illustrates this with an example:

> "In a country in Asia, we have been working with politically active youth. They have been involved with politicians on Facebook, similarly to politically active youth in Norway. Then suddenly, a military coup happens, and then all this information about them online poses a big risk as it is no longer ok to be politically active. Then our role becomes to help them by trying to delete their online activity tracks and personal data."

Leap Learning explains that they have a lot of competence and experience introducing digital tools in rural areas. The experience is mainly due to their use of tablets in their educational programs. In Gambia, Leap Learning also provide PCs and coding clubs. They have, until now, mainly worked with their tablets in offline mode so that the students are not able to surf online. However, they plan to expand online and include communication functionalities in their educational programs in the long run. The Leap Learning representative also mentions that they have experienced an apparent increase in accessibility of phones and the internet. In Gambia, when the students reach the age of 15, 16, and 17, they often get their own phones.

Save the Children explains that during the pandemic, they have worked a lot with the continuation of school and education via mobile phones using social media platforms like WhatsApp and Facebook. When doing so, challenges arise, questioning whether or not this is a suitable platform for educational purposes. Also, they underline the importance of introducing alternative analogue methods.

5.2.4 Risks young people in developing countries face in the digital world

Leap Learning underlines the high level of naivety which exist among youth in rural areas and the importance of understanding how ground-level their CSA knowledge is, as many of them have zero experience with digital devices:

> "They do not know what is out there. They do not understand the consequences of the actions they take. If someone online gives them an opportunity, they could believe it is an entrance to happiness and money. They can send pictures to strangers in good faith because they have no idea about the consequences."

Leap Learning gives a further recommendation for addressing the lack of experience amongst the target group of this project. Information within the field of CSA should be conveyed in a straightforward manner, preferably including visualisation and audio elements. Testing the user to investigate whether or not they have comprehended the provided information is also emphasised. Another aspect mentioned that the youth in these areas are concerned with pleasing their teacher:

> "They are often more concerned with pleasing you, or a teacher, than understanding what they are reading. They often answer "yes" to be polite. They will always answer what they think you want them to answer. Be creative in the way you ask questions."

Save the Children says that they are worried and concerned about the limitlessness that exists online. They have experienced everything from girls being bullied over Instagram in a remote, rural village in Latin America to online sexual abusers. A common phenomenon is that sexual predators can sit behind the screen anywhere and abuse children and youth on the other side of the globe. They also describe how children and sexual predators meet on new platforms, which adults and authorities have yet to discover:

> "Unfortunately, when a new platform arrives, children are good at using it first, and abusers are also good at being there. No one is better at exploiting loopholes than those who have evil intentions."

Another threat which Save the Children highlights is the criminals who recruit youth into criminal networks online. They underline that this type of recruitment happens outside the digital sphere as well, but online recruitment is more invisible, frequent and abruptly more severe. It is a form of exploitation of children and youth who are already in a very vulnerable situation.

5.3 Takeaways from interviews with experts

Leap Learning and Save the Children both highlight the importance of involving the children and having more focus on them in terms of CSA education. Until now, this has not been a priority for either of them. The rapid increase in the introduction of digital and online tools during the Covid-19 pandemic was an accelerator.

When asked about threats facing young people in developing countries online, Leap Learning focuses on naivety and the lack of consequence thinking. This naivety is a consequence of the lack of experience with digital tools and online behaviour.

Save the Children focuses more on the outside threats and how it has become frighteningly easy for criminals to get a hold of young people through social media platforms. They mention sexual predators and criminal networks as criminal actors mainly present on the online recruitment scene. In countries with no laws, regulations or protection from the government, online activity can cause danger. Save the Children illustrates this by talking about politically active youth in an Asian country and how it became hazardous for them when a military coup happened, and digital footprint and activities were suddenly considered illegal.

Leap Learning is experienced in providing education to children and youth in underdeveloped and rural settings. In the interview, they gave concrete recommendations for teaching a thematic with which the target audience has no prior experience. The recommendation included disseminating the information in an uncomplicated and visual way and providing a testing aspect to measure the level of comprehension of the target user.

Chapter 6

Design and Development

This chapter presents the design and development of the working prototype. A presentation of the Leap Learning App Universe, including the technology stack, development platform and design templates, is followed by a presentation of the content and functionality elicitation.

6.1 Leap Learning App Universe

Leap Learning's App Universe[1] is a collection of educational apps which offers over 500 unique apps for literacy, numeracy, logic and entrepreneurship. The apps are available for iOS, Android and web apps. Figure 6.1 shows a collection of logic apps from the App Universe.

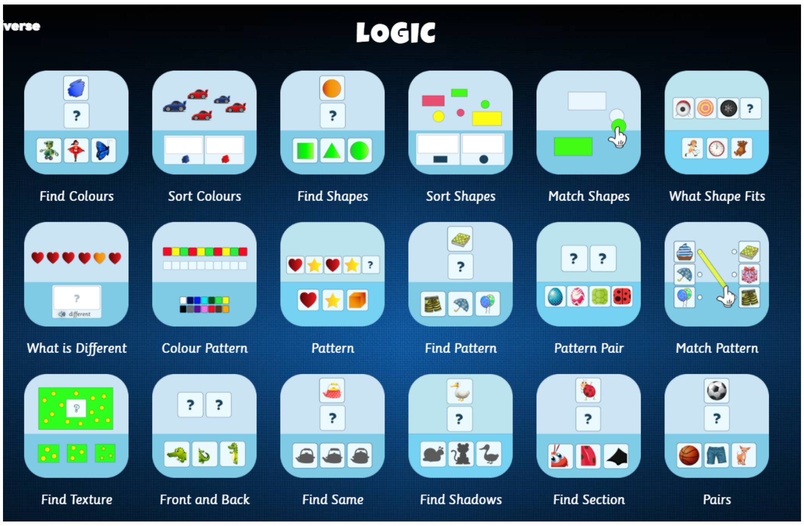


Figure 6.1: Leap Learning Logic Apps

[1] https://leaplearning.no/apps

6.1.1 Technology stack

The apps are based on the solar 2D game engine [2]. The frontend is written in Kotlin/Swift and React for the web application version.

Four components control the app universe; "Apptrack", "Translate", "Webapps", and "Autobuild". "Apptrack" is written in Python [3] and organizes all apps, versions, and categories. "Translate" is written in Elixir[4]/Python and organizes the content of each app as well as translations, illustrations, and sounds. When adding content to the apps in this project, it is done through the "Translate" platform. "Webbapps" is written in Elixir and serves web apps and APIs to the platform client. "Autobuild" is written in Python and automatically builds the apps.

The apps are hosted through the HashiCorp[5] stack with Nomad[6], Consul[7] and Vault[8], which orchestrates the deployment, service networking and security, respectively. The code base is managed in a private GitHub repository by Leap Learning.

6.1.2 Development Platform

The IT artefact prototype in this thesis was implemented in the form of apps in Leap Learning's development platform. In collaboration with software developers from Leap Learning, app templates were added to the platform. These templates contained functionality which was pre-existing in the app universe. After implementing the templates in the development platform, the next step was to add content and illustrations to each app. In addition to adding content, changes could be made to each app, such as the number of tasks, levels and placement of features. Figure 6.2 displays the development environment in the platform, using a snipped from one of this thesis' implemented apps as an example. This development environment uses a "Select Sentence" template.

[2] https://solar2d.com/

[3] https://www.python.org/

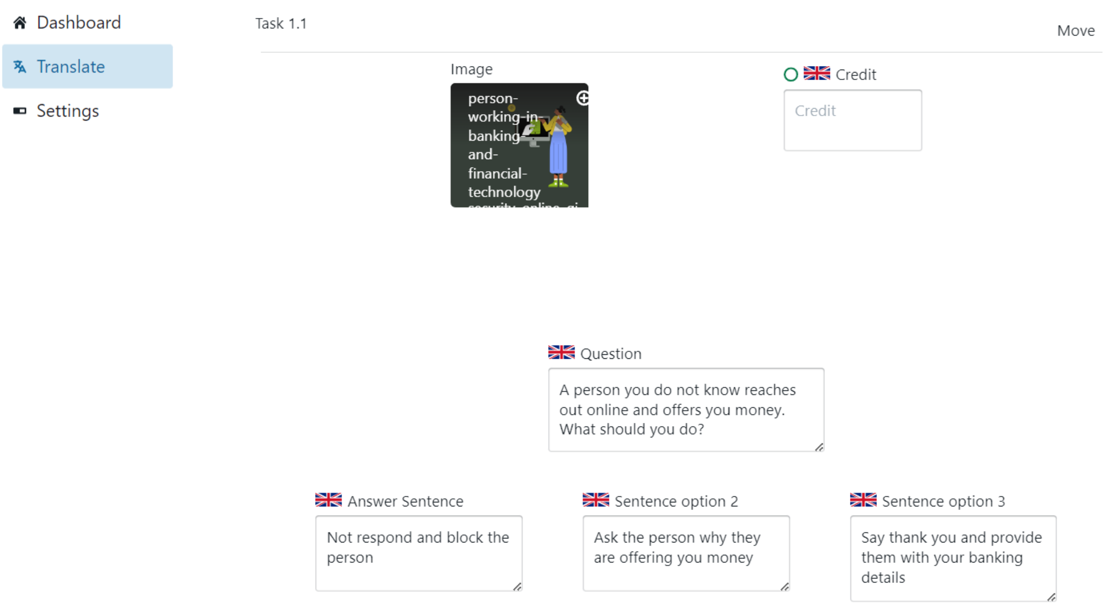
[4] https://elixir-lang.org/

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

[6] https://www.nomadproject.io/

[7] https://www.hashicorp.com/products/consul

[8] https://www.hashicorp.com/products/vault



Credit

Question

A person you do not know reaches out online and offers you money. What should you do?

Answer Sentence

Not respond and block the person

Sentence option 2

Ask the person why they are offering you money

Sentence option 3

Say thank you and provide them with your banking details

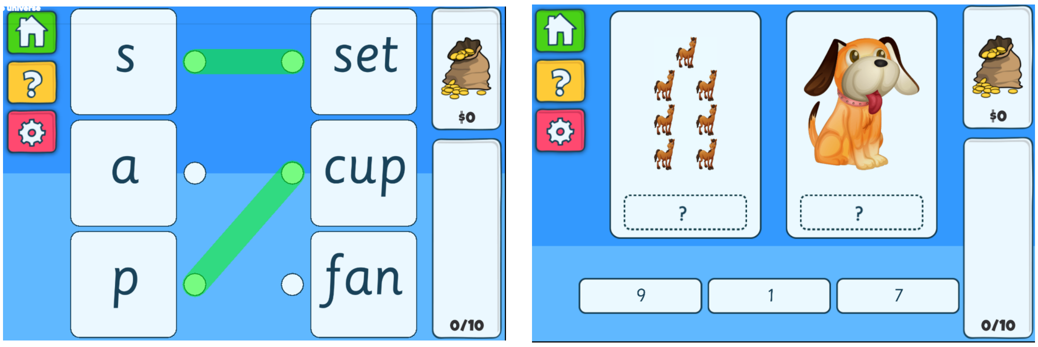
Figure 6.2: Snippet of the Leap Learning development platform

6.1.3 Design template elicitation

Developing apps using Leap Learning's platform meant that app functionalities and design templates were restricted to the design guides of Leap Learning. Leap Leaning's App Universe operates with two different design templates; one which targets children and one which targets adults. The children-targeted design template is used for literacy, numeracy and, logic educational apps. These apps are colourful and playful and rely heavily on illustrations. Figure 6.3 displays examples of a literacy and logic app for children.

The adult-targeted apps are used for educational programs which aim to empower and teach adults in rural areas within different fields. This includes topics concerning entrepreneurship and farming, amongst others. The adult-targeting apps follow a more informative approach but also include interactive functionality in order to test the user. Figure 6.4 displays examples of educational apps for adults.

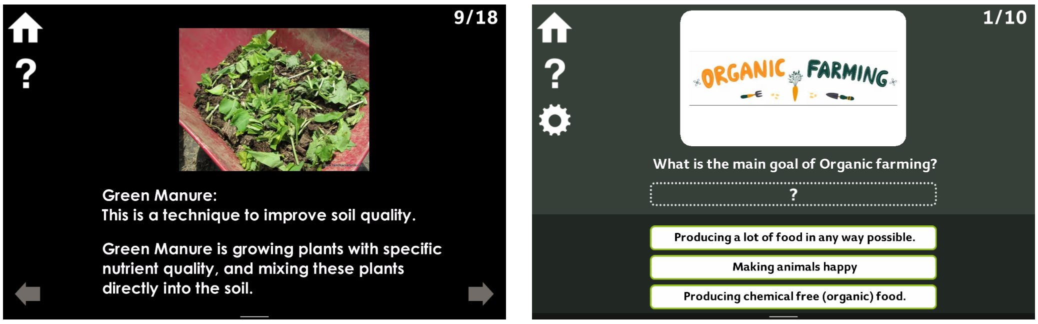
Due to the target group in this master thesis project being 13-30 years old, as explained in Section 1.2, it was decided that the template targeting children would not fit the purpose of the project. Additionally, cyber security awareness addresses many serious themes with topics considered incompatible with a cheerful design. Thus, the informative, adult-targeting template was considered the most fitting for the applications.



(a) Match letter-word app

(b) Match number-figures app

Figure 6.3: Literacy and logic apps using the children-targeted template


9/18

Green Manure:
This is a technique to improve soil quality.

Green Manure is growing plants with specific nutrient quality, and mixing these plants directly into the soil.

1/10

What is the main goal of Organic farming?

?

Producing a lot of food in any way possible.

Making animals happy

Producing chemical free (organic) food.

(a) Organic Farming informative app

(b) Organic Farming quiz app

Figure 6.4: Informative and quiz apps using the adult-targeted template

6.2 Content and Functionality elicitation

English was chosen as the language for the prototype due to the official language in Gambia, where user testing was conducted, is English. Based on the findings from the SLR in Section 4.2 and expert interviews in Section 5.2, the following seven CSA topics were planned to be addressed in the application:

- Harmful content
- Interaction with strangers online
- Cyber bullying
- Password habits
- Sharing private information online
- Phishing attacks
- Identity theft

Following the principles of iterative cycles in the Design and Development research strategy, described in Section 3.1, it was decided that not all seven topics would be focused on in this iteration cycle. Thus, three of the seven CSA topics were chosen to be addressed in the development of the working prototype. The chosen topics were: "Interaction with strangers online", "Password habits", and "Sharing private information online".

6.2.1 Content elicitation

As the application aimed to hold an informative approach, the content chosen to be presented was important. During the selection process, findings from the SLR studies were used as inspiration. Another sources utilized, was the CSA curriculum by Google [32], described in Section 2.4.

The content elicitation process consisted of the three following steps:

1. Brainstorming
2. Creating suggestions for content to be included
3. Implementing in development platform

A Miro[9] dashboard was actively used in the content elicitation process. Miro is a visual collaboration platform where one can create whiteboards and visually display ideas. Even though there was no one else than the master thesis student using the Miro board, it was chosen as an appropriate tool due to its scalability and visualization abilities. In the Miro dashboard, a whiteboard was created for each CSA topic mentioned in the previous section. In the brainstorming process, content suggestions for each CSA theme were added to a whiteboard. These could be suggestions for functionality for different tasks, quiz questions or scenarios.

Following the brainstorming process, a more structured phase where the type of application functionally and content for this was suggested. Figure 6.5 shows a snipped of the structured content suggestion for the "Sharing private information" CSA topic. A full Miro board for the planning of the "Online Strangers" quiz app is included in Appendix D in Figure D.1.

[9] https://miro.com/

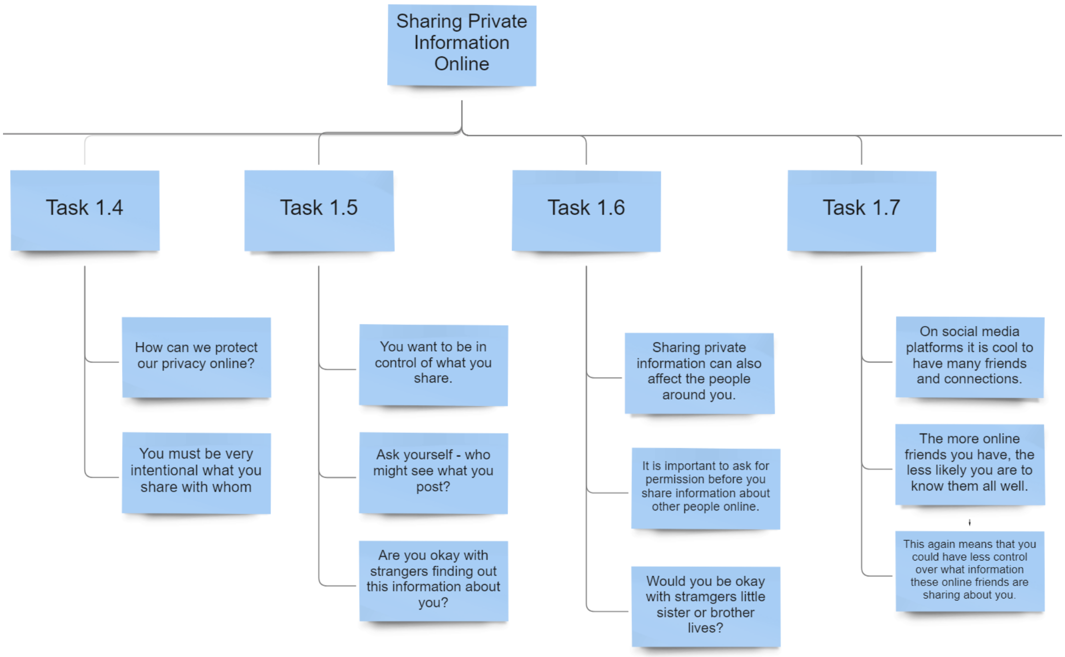

Sharing Private Information Online
Task 1.4
Task 1.5
Task 1.6
Task 1.7
How can we protect our privacy online?
You must be very intentional what you share with whom
You want to be in control of what you share.
Ask yourself - who might see what you post?
Are you okay with strangers finding out this information about you?
Sharing private information can also affect the people around you.
It is important to ask for permission before you share information about other people online.
Would you be okay with stramgers little sister or brother lives?
On social media platforms it is cool to have many friends and connections.
The more online friends you have, the less likely you are to know them all well.
This again means that you could have less control over what information these online friends are sharing about you.

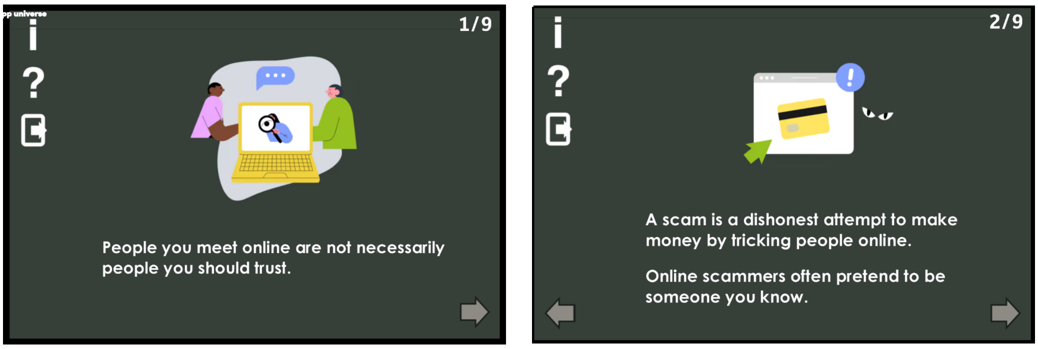
Figure 6.5: Structured content for "Sharing Private Information" topic in Miro

6.2.2 Functionality elicitation

In the findings from the SLR, different approaches of functionality were applied in order to present information and practice CSA. Storytelling, quizzes, visualization and inclusion of gamification elements were amongst the functionalities and practices applied, as presented in Section 4.2.3. From the expert interviews, the expert from Leap Learning underlined the importance of using various methods and testing the user on the learning material. The app functionalities elicited for the prototype are based on these findings and presented in this section.

Informative apps

In order to inform the user about each cyber security topic, an informative app presenting fundamental knowledge was included. This app format includes short sentences accompanied by an illustration and aims to explain a relevant aspect in a concise, descriptive manner. Figure 6.6 displays two app views from the working prototype of the informative app functionality.



People you meet online are not necessarily people you should trust.

A scam is a dishonest attempt to make money by tricking people online.

Online scammers often pretend to be someone you know.

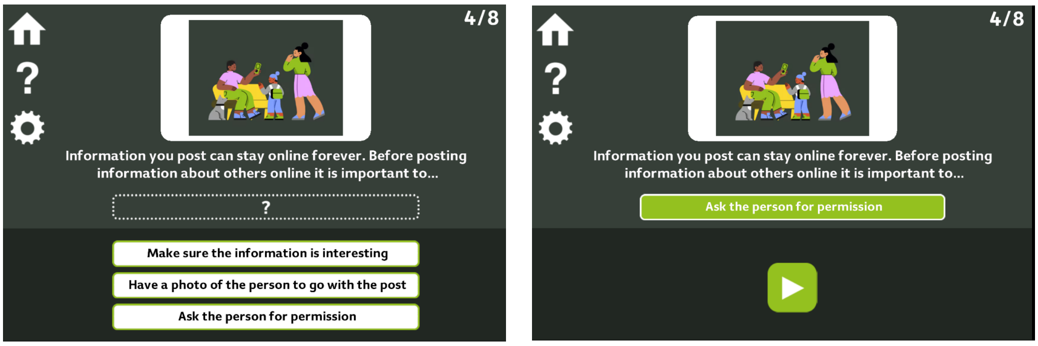
(a) Informative app view 1

(b) Informative app view 2

Figure 6.6: "About Online Strangers" app views

Quiz apps

In order to challenge the user and test if they have understood and learned from the informative app, a quiz-inspired "Select Sentence" app was included. This app asks the user a question, and the user is given three alternative answers, where one is correct. This app uses a drag-and-drop functionality where it is only possible to drag the correct answer onto place. When the right answer is dragged to the answer field, it will turn green, and a celebrating sound will be played. Figure 6.7 displays the view of an implemented task before and after choosing the correct answer.



Information you post can stay online forever. Before posting information about others online it is important to...

?

Make sure the information is interesting

Have a photo of the person to go with the post

Ask the person for permission

Information you post can stay online forever. Before posting information about others online it is important to...

Ask the person for permission

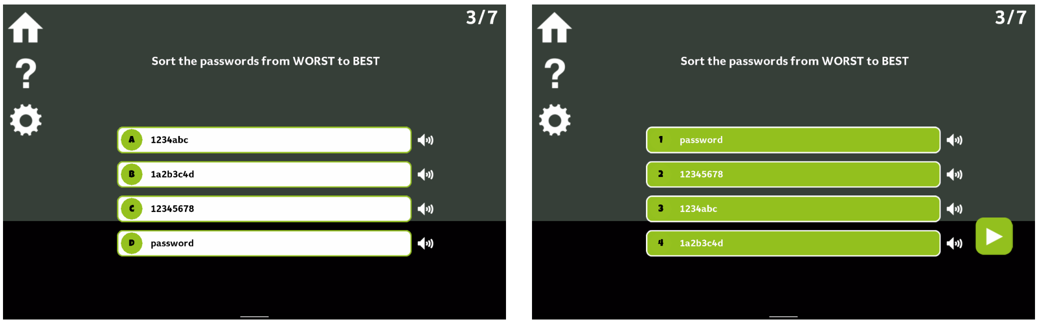
(a) Select Sentence view before answer

(b) Select Sentence view after answer

Figure 6.7: "Select Sentence" app views

Priority apps

The third and final app functionality included in this prototype iteration is a priority app, where the user should prioritize the alternatives from "best to worst" or "worst to best". This, too, incorporates drag-and-drop functionality. Figure 6.8 displays an implemented view of a priority task before and after the correct prioritization.



3/7

Sort the passwords from WORST to BEST

A 1234abc

B 1a2b3c4d

C 12345678

D password

(a) Priority app before answer

3/7

Sort the passwords from WORST to BEST

1 password

2 12345678

3 1234abc

4 1a2b3c4d

(b) Priority app after answer

Figure 6.8: "Priority" app views

6.2.3 Illustrations

Designstripe[10], an online illustrator program, was used to create the illustrations. The online tool provides pre-designed illustrations that the user can alter and customize. Designstripe offers a broad selection of characters from different cultures and colours and themes that may be used to personalize each illustration.

6.3 App hierarchy of working prototype

Figure 6.9 displays the apps in the working prototype implemented in the Leap Learning App Universe hierarchy. In total, seven apps were included in this working prototype iteration. These apps were built and distributed in the Leap Learning testing environment.

[10] https://designstripe.com/

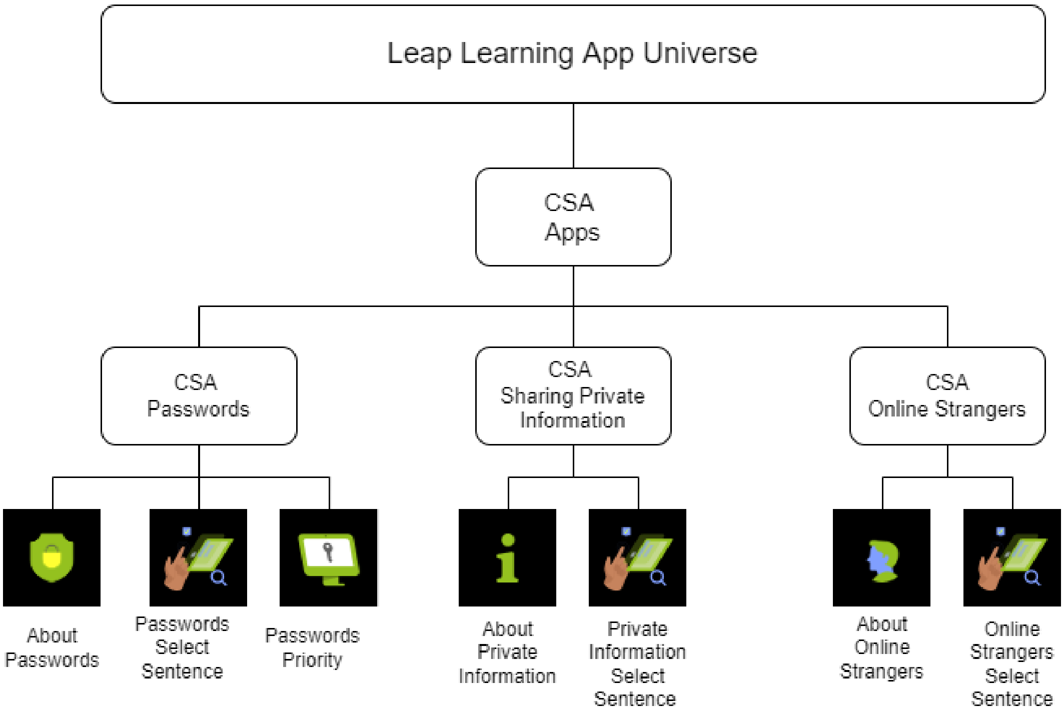

Leap Learning App Universe
CSA Apps
CSA Passwords
CSA Sharing Private Information
CSA Online Strangers
About Passwords
Passwords Select Sentence
Passwords Priority
About Private Information
Private Information Select Sentence
About Online Strangers
Online Strangers Select Sentence

Figure 6.9: Implemented app hierarchy

Chapter 7

Results

This chapter presents the results from the observations and interviews conducted in Norway and Gambia. In total, ten participants were observed and interviewed. However, one participant withdrew their participation, and another did not fit the age range of the target group. The data from these two participants were not included in the analysis of the results.

7.1 Demographics

Eight participants contributed to the observation and interview data. Six of them participated in Gambia, and two participated in Norway.

7.1.1 Age of participants

All the participants fit into the age range of the target group, which was between 13-30 years old. None of the participants was below the age of 16 because the participant aged 13-15 required a signature of a consent form from a parent or guardian, which proved to be difficult to obtain. Both adolescents and young adults were represented, with 37.5 % teenagers and 62.5 % older than 20 years old. Table 7.1 displays the age distribution of the participants.

Participant	Age	Country
P1	16	Gambia
P2	18	Gambia
P3	17	Gambia
P4	23	Gambia
P5	23	Gambia
P6	30	Gambia
P7	23	Syria
P8	30	Eritrea

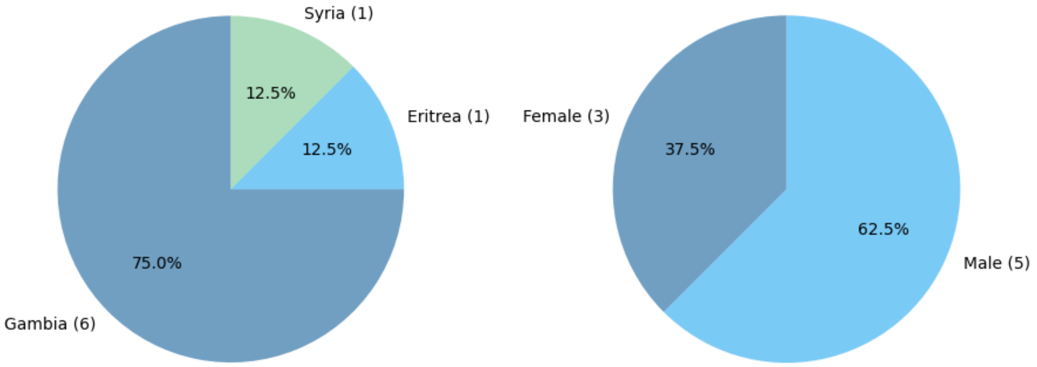
Table 7.1: Overview of participants' age and country of origin

7.1.2 Country of Origin

As most of the participants who contributed to the user testing were recruited in Gambia, it is not surprising that 75 % of the participants originated from Gambia. The two participants who contributed in Norway originated from Syria and Eritrea. Gambia and Eritrea are both countries listed on the UN's list of LDCs, whilst Syria is listed as a developing country[1]. Figure 7.1a displays the distribution of country of origin amongst the participants.

7.1.3 Gender of participants

The distribution of female and male participants was three to five, respectively. Figure 7.1b displays the gender distribution amongst the participants.



(a) Distribution of participant's country of origin **(b)** Gender distribution among participants

Figure 7.1: Distribution of country of origin and gender amongst the participants

7.1.4 Access to digital devices, internet and social media

The participants were asked about their digital habits and whether or not they had access to digital devices and the internet in their daily life. Most of the participants owned a smartphone and had various social media accounts. The full results are presented in Table 7.2.

[1] https://www.worldbank.org/en/country/syria/publication/economic-update-april-2022

Participant	Age	Access digital device	Internet access	Social media	Email
P1	16	No*	Only at school	No	No
P2	18	Smartphone	Yes	Facebook, WhatsApp, Twitter	No
P3	17	Phone, computer	Yes	Instagram, WhatsApp, Twitter, Google	Yes
P4	23	Phone	Yes	No	Yes
P5	23	Phone, computer	Yes	Facebook, WhatsApp, Instagram	No
P6	30	Phone, computer	Yes	Instagram, Facebook, WhatsApp, Snapchat	Yes
P7	23	Smartphone, computer**	Yes	WhatsApp, Facebook	Yes
P8	28	Smartphone, computer***	Yes	Facebbok, WhatsApp, Google	Yes

* Had access to a computer in school.
** Did not have any access in Syria, only the family's house phone. Got a smartphone in 2016
*** Only had an old cellular phone in Eritrea, no Internet. Got a smartphone in 2016.

Table 7.2: Digital device and internet access overview

7.2 Observations

In the user testing guide, which can be found in Appendix C, it was encouraged that each participant tested all apps with two CSA topics. In Gambia this was followed, and all six participants tested apps within two topicss. In Norway, the two participants tested apps within only one topic due to time restrictions. Table 7.3 shows the number of times each app was tested and by whom.

App observed	Participant
"About passwords"	P2, P3, P4, P6, P7
"Password Select Sentence"	P2, P3, P4, P6, P7
"Password Priority"	P2, P3, P4, P6, P7
"About Private Information"	P1, P5, P8
"Private Information Select Sentence"	P1, P5, P8
"About Online Strangers"	P1, P2, P3, P4, P6
"Online Strangers Select Sentence"	P1, P2, P3, P4, P6

Table 7.3: Distribution of tested apps among participants

7.2.1 Functionality and interaction

This section presents the most prominent findings regarding the participants' interactions with the apps' functionality during the observation sessions. The observations are structured under each type of app functionality, following the functionality types presented in Section 6.2.2.

The informative apps

Overall, the participants interacted with the apps on the tablet seemingly well. The participants spent some time reading the information in the "About" apps but found the "next"-button and navigated to the next task without issues. The main issue which appeared in the "About" apps was the understanding of certain words and terms, which will be further presented in Section 7.2.2.

The quiz apps

Most of the participants who tested the "Select Sentence" apps understood the "drag-and-drop" concept. Participant 5 seemed to find the functionality engaging and expressed a "yes!" when a question was answered correctly. However, participants 2, 4 and 7 spent some time understanding the "drag-and-drop" functionality and tried to push the answers instead of dragging them to the marked "answer" box. Participant 7 expressed, "It turns green, but I do not know why" when getting the answer correct.

The functionality of the "Select Sentence" apps required a correct answer before giving the user the next task. This requirement occasionally led to participants trying all three of the response alternatives until they got it right, and the answer turned green. All participants managed to navigate to the following tasks without noticeable issues.

The "Priority" app

The priority functionality was only implemented in the "Password" topic and was thus tested by five participants. All five of the participants struggled to understand how the functionality worked. All participants tried to press the buttons instead of dragging them into the correct order. Participant 4 expressed that "it is not working", but all participants seemed to get it after some trial and error. However, the order of alternatives was occasionally placed in correct priority from the beginning. The alternatives had to be moved back and forth to turn green and registered as correct in these cases. This functionality confused the participants. Participant 7 disagreed with a few of the answers and expressed: "I do not know what happened?" and "I cannot control... Why can I not change them after they turn green?".

Finding the exit button

In five out of eight observation sessions, the observer reported issues with participants exiting the application. Participants 1, 2, 3, 4 and 8 did not understand the exit symbol on the button. Participant 8 pressed the information button marked with an "i" when trying to exit the application. This participant ended up closing the whole application. When asked to exit their current application the second time around, the participants seemed to have learned the exit functionality and managed to exit without issues.

7.2.2 Language, words and unfamiliar terms

The language level of the participants varied. Some participants did not seem to struggle with understanding the content, whilst others struggled with certain words and terms. Participant 4 struggled with the reading and did not seem to understand the content in the "About" apps. At one point in the session, the facilitator had to read the text aloud to the participant, as the participant understood oral English well but struggled with reading comprehension. Another general observation was that some participants seemed to focus on reading the text aloud correctly and focusing less on actually understanding the content.

Two participants in the Gambia needed an explanation for the terms addressing financial and bank services. "Social security number" was also an unfamiliar term. The facilitator in Gambia reported that few people in the rural areas in Gambia own a bank account. They also reported that native Gambians seldom have a social security number, as it is only needed if they apply for passports or specific jobs.

The term "friend request" had to explain to participant 1. This participant did not have any form of social media. Having a pet is a phenomenon that does not exist in rural parts of Gambia and was an unfamiliar term for participant 1.

There were also a collection of words that some participants struggled with in pronunciation and meaning. "Malicious", "extortion", and "catfishing" are examples of words the participants found difficult. Table 7.4 displays a complete list of terms and words each participant found difficult.

App	Participant	Difficult words and terms
"About Private Information"	P1	Bank account, bank details, privacy, financial, financial fraud
	P5	Online privacy, location services, financial fraud
"Private Information Select Sentence"	P1	Pet, switched on/off, friend request
"About Online Strangers"	P1	Scam, cruel, malicious, extortion, blackmail, abusers, criminal network
	P2	Catfishing, malicious, potentially, extortion, persuade, explicit
	P5	Identity, Catfishing, "hiding behind screen", malicious, curel intentions, blackmail
"Online Strangers Select Sentence"	P1	"Offers you money", bank details
	P5	Nude
"About passwords"	P2	Security measure, sensitive, digital footprint, characters
	P6	Social security number
	P7	Characters, regularly
"Password Priority"	P7	Purpose

Table 7.4: Observed words and terms participants struggled with

7.3 Interviews

The interviews conducted after the participants had tested and interacted with the working prototype aimed to apprehend the participants' impressions and reflections. The results from the interviews are presented in the following sections.

7.3.1 Participants' reflections from the apps

The opinions expressed by the participants were diverse. Some participants provided thorough reflections of their experiences, while others were more reserved in their responses. When asked if they had previously received any cyber security training or education, all eight participants answered "no". As a result, their interactions with the apps were their first encounter with the CSA topic in an educational setting.

Reported learning outcomes

The participants were asked whether they had learned something new during the test session, where all participants answered "yes". However, the answers varied when asked to mention specific new information they had learned. Some participants explained specifics from the information they had gotten when using the apps, whilst others answered a simple "yes" without further reflections about their learning outcomes. The participants' answers are summarized in Table 7.5.

The participants were also asked whether there was any information presented in the apps they were familiar with prior to testing them. These findings are summarized in Table 7.6.

Participant	Reported learning outcomes
P1	*It taught me if I meet someone online or social media and it is a stranger, the he asked me to send him my nude photos I should block the person and never respond.* *If a stranger online, like someone you used to chat to, if they said "Do you want to meet somewhere?" You don't have to go and meet with the person.* *You don't have to send your password or your bank details or photos*
P2	*Yes I learned so many things here, about when scammers trick people, I learned also about this password. And so on. There are many things.*
P3	*Yes, it looks very simple and I did not know much of it before, but now I do.*
P4	*Yes I learned...* (Does not explain further)
P5	*Definitely. I learned a lot of things. I think they show like they are real, they just play role like they're real* (people on SoMe). *And then they're not real. And they just try to fake on the social media. Just to fool you. They just want something out of it. Yes definetly it is bad. And they just want to have your information so I just ignore it.*
P6	*So things new with regards to like my password combinations, and how to react based on certain instances with regards to like catfishing and sharing my personal information.*
P7	*I learned that it is the like the passwords it should be more more difficult for most things like. Yeah, I so. So here is 1234 or maybe the date when you are born. I used that before. Especially that 12345678. That one is the easiest and everybody can for example, if they had the phone (my phone) in their hands they can't try with that numbers 123456. So it's really easy. We have to never use it.*
P8	*Yes a little bit. Information about keeping information to your self and not share with friends.*

Table 7.5: Reported learning outcome from each participant

Participant	Pre-existing knowledge
P1	*Like you don't have to give your number to a person you don't know.*
P2	*Yes passwords. My phone has a password.*
P3	*You cannot share your password anyone apart from family member or only just you your private.*
P4	*Yes* (Does not explain what)
P5	*Yeah, about those hackers. Sometimes I meet them on Facebook. When I just read the message that they send II just kdefinitely know that this is something fake it is not good, they just try to keep your account details and stuff like that just to fool you.*
P6	*I knew how to possibly detect certain things when it comes to like scamming because, like I've experienced it, so yeah. Like people send me random emails.*
P7	*I learned that it is the like the passwords it should be more more difficult for most things like. Yeah, I so. So here is 1234 or maybe the date when you are born. I used that before. Especially that 12345678. That one is the easiest and everybody can for example, if they had the phone (my phone) in their hands they can't try with that numbers 123456. So it's really easy. We have to never use it.*
P8	*No.*

Table 7.6: Participants' reported pre-existing knowledge

When asked about their favourite part of the application, all five participants who had tested the password apps responded that this had been their favourite topic. In particular, the "Password Priority" was mentioned as a favourite by multiple participants. Participant 6 said, "When it came to finding the rating from the least to the most important, I found that really interesting because it was testing me, and it was a little difficult". Participant 7 expressed that "It is more fun and has more information about learning how to use the passwords".

Other participants gave more general reflections like participant 5, who commented, "Questions and answers are important, as you read and then try to fill the gaps".

Participants' perception of usability

When asked if they had any difficulties using the different apps, five of the participant were quick to respond "No" and "No, it was not difficult. Very simple". Participant 6 did respond that there were a few difficulties but provided no further explanation when asked. Participant 8 reported that there were some struggles figuring out how to enter and exit the application.

Participant 7 provided more detailed feedback regarding the "Password Priority" functionality. The participant found it strange that once he had chosen one alternative and everything turned green, he could not go back and change his answer. He also explained that he would have liked to have more feedback when getting the answers correct: "like an OK or something".

Participants' perception of language level

The majority of the participants reported that "there were a few words I did not know" when asked about how they found the language in the apps. Participant 6 pointed out a spelling mistake in one of the apps. The general response was that the sentences were "not too long and difficult". Participant 4, for whom the app's contents had to be read aloud throughout the test, said the language was "really easy".

7.3.2 Participants' real life experiences

During the interview sessions, some of the participants unsolicited told and reflected on their experience with online threats. Although these reflections were not direct answers to the interview questions, their experiences were relevant to the project. Thus, it was decided that they should be presented as results. In Table 7.6 experiences from participant 6 and 7 are presented. Participant 2 told a story about a time she experienced a scam attempt online. The following are outtakes from her story:

I was on Facebook, it was 5 PM around here, so one man added me on Facebook. I accepted him just as a friend, but he texted me on Messenger later on. He had put a white person on his profile picture. And he said his name, he said his name was Alex, but I forgot his surname. He told me, "I live in the US, but we have a ship in Italy, so we pack luggage. So we spent almost three months inside the water. When I arrive in Rome, I'll call you."

Unfortunately, the time he got to Rome, he did not call, but he texted me. He said, "We are going to have our money or three months' salary. So when I receive that, I'm going to do something for you."

I told him: "Wow, have you ever known me? You want to do something?" He said: "Yes, I just feel like doing something for you.!" And he said: "What do you want?"

I said: "Anything that you intended to give it from from the bottom of your heart, just give it to me. But, I will not require I to say that I need this, I need this, no."

He said he would buy a laptop, he'd buy a phone, he'd buy dresses, he'd buy a handbag for me. He sent pictures to me and said: "By tomorrow, this luggage will return to your country."

I said "OK", but then he said: "Before you get the luggage, you have to send me 30 US dollars."

Equivalent to Gambian money, I think, is 6650 Dalasi, something like that. He sent me the account number."

He asked me first: "Do you have Western Union?" I said, "Yes", and he said: "You go to Western Union. You send through this account number. "I told him: "Yes, OK, I will send it to you."

I sit and think I said: "hope this person is a good person, hope is it not a bad person?". Later on, I called my uncle. I explained everything to him, and he told me: "If you are a fool, go and send money to him", as he informed me I didn't even have money. Then I'm thinking of my family and how I can help my parents much more than to send 6000 dalasis. That is big money here. So later on, I ignore the person, and then I block it.

Chapter 8

Discussion

This chapter presents a discussion regarding the findings from data collections in this master thesis project. The discussions evolve around themes connected to the RQs. Additionally, implications of research and practice, limitations, and further work are presented in the following sections.

8.1 Designing a digital platform to inform adolescents and young adults in developing countries about cyber security

In order to see the purpose of introducing a digital platform to teach cyber security awareness, one fundamental attribution is that the target audience has access to digital devices and the internet. According to Poushter *et al.* [8], the smartphone ownership gap between developed and developing nations is narrowing. As presented in 2.3, it is projected that young people in Sub-Saharan Africa (SSA) who owns a mobile phone for the first time will be the dominant source of digital growth in the foreseeable future[1]. These findings were reflected in the access the participants in Gambia had to digital devices, the internet and social media. Five out of the six participants in Gambia owned a smartphone and had internet access outside of school. One participant did not own a phone and only had access to a computer in school. The two participants in Norway both owned a smartphone and had Internet access, which was not surprising as 96%[2] of people living in Norway own a smartphone. However, the two participants reported that neither had online access nor owned a smartphone prior to arriving in Norway. An observation made by one of the Leap Learning representatives who had been in Gambia three years prior illustrates the rapid increase in the availability of internet, social media and digital devices. During the representative's last visit, the children and adolescents danced and sang traditional folk songs and dances. Now, she observed that they were singing and dancing to viral TikTok songs. This observation illustrates how the rapid introduction of digital devices, the internet and social media in rural areas can cause changes.

The findings in the SLR laid a foundation for what cyber security topics should be addressed in an informative digital platform aimed at adolescents and young adults

[1] https://www.gsma.com/mobileeconomy/wp-content/uploads

[2] https://www.ssb.no/teknologi-og-innovasjon/faktaside/internett-og-mobil

in developing countries. The prominent topics were: *harmful content, interaction with strangers online, cyberbullying, password habits, sharing private information online, phishing attacks, and identity theft*. The SLR also explored different approaches for raising CSA. Although the studies covering this aspect were limited, some approaches were found, including storytelling, gamification elements, quizzes, social media campaigns and workshops. The findings from the SLR highlighted the necessity of additional research within the field of CSA and developing countries. The 18 papers extracted in the study selection process in the SLR were considered relevant enough to this thesis' research topic. In comparison, the SLR conducted by Quayyum *et al.* [5] included 56 studies. Quayyum et al. focused on a similar CSA aspect as this thesis but did not restrict the research to developing countries. The imbalance of the number of included studies, 18 to 56, illustrates efforts being put towards CSA in well-developed nations compared to under-developed nations.

Expert interviews with representatives from Save the Children Norway and Leap Learning provided further insights into the research topic and shed light on other aspects of the vulnerable position children and young adults in developing countries are in the digital world. The findings from the expert interviews also provided insights into cultural differences and how this can affect online behaviour. One key takeaway from the interviews is the level of naivety among people in rural areas due to their lack of experience with digital tools. This finding is in alignment with the findings in the study report by ITU [2], where statics show that people from Least Developed Countries (LDC) often have their first interaction with the internet through a social media platform lacking the rudimentary digital skills needed. Save the Children were clear that although cyber security and children's online safety are of the highest importance, there are also positive sides to being connected online. Aruleba and Jere [9] also addressed the positive aspect of digital connection and discussed how the Covid-19 pandemic has accelerated the use of digital tools and how digital connectivity has many positive consequences for improving education, health care and social well being.

Both Leap Learning and Save the Children explained how they lag on digital security and cyber security training initiatives. They admit that it has taken too long to realize that cyber security also involves children. One of the Save the Children representatives stated:

> "We have previously started with teachers and other partners, but now we focus properly on children as users. We have a bias, and it has taken time to acknowledge that children are digital users also in developing countries."

When compared, Save the Children seems to have a broader focus on what can be done to fight cybercrime and raise cyber security awareness, whilst Leap Learning has a more concrete and specific vision toward education. Save the Children are working towards the involvement of higher authorities on the matter, whilst Leap Learning are more focused on how cyber security training can be incorporated into their teaching programs. This distinction is expected as Save the Children is a worldwide organization with partnerships all across the globe, and Leap Learning is a company on a much smaller scale.

In this master thesis project, a working prototype of a digital platform in the form of apps in the Leap Learning App Universe was developed. The content, design and functionality were created based on the findings from the SLR and expert interviews. Three CSA topics were prioritized to be addressed in this prototyping iteration. The working prototype consisted of seven apps which addressed the following cyber security topics: *password habits, interaction with strangers online and sharing private information online*, as presented in Chapter 6. The content for cyber security topic was created with inspiration from the studies in the SLR, such as *POMGEA - Security Awareness Game* by Visoottiviseth *et al.* [22] and *AwareME* by Dassanayake *et al.* [26]. In addition, the teaching framework *Be Internet Awesome* by Google [32] was used as inspiration. As the apps had an informative approach, the content elicitation was important.

The functionality of the working prototype is presented in Chapter 6 and includes informative apps which explain and present information of relevance for each cyber security topic. In order to test and evaluate whether or not the user understood the provided information, apps with a quiz-inspired functionality, "Select Sentence", were included. The method consisting of presenting the user with information followed by testing their understanding of the provided information is similar to the approach used by Visoottiviseth *et al.* [22] in their *POMGEA Security Awareness Game*. However, Visoottiviseth *et al.* [22] uses storytelling and fictional characters in order to portray and present their cyber security topics. This approach contrasts with how the information is presented in the prototype in this thesis. The informative apps present factual information, teach relevant terminology and encourage and discourage certain behaviours online. The study by Visoottiviseth *et al.* [22] targets young adults in the age group 19-23 years old, which is partly the same target group as this master thesis project.

This master thesis study used qualitative methods to evaluate the developed working prototype. The evaluation was conducted by observing users testing the prototype, followed by interviews where the participants gave their reflections on the apps they tested. This evaluation method differs from the data generation and analysis methods used in the papers in the SLR, as the majority were quantitative studies. Visoottiviseth *et al.* [22] and Dassanayake *et al.* [26] both conduct usability tests in their studies. However, they do not include participants' perceptions and opinions of the application post-testing. The data collection method used in this master thesis appears to be distinct from other studies conducted on CSA in developing countries.

As the representative from Leap Learning explained in the expert interview, her experience is that Gambian youth are concerned with answering the questions in a manner that they believe is pleasing for the interviewer:

> "They always answer what they think you want them to answer".

In some cases, this was evident in the observation where the participant found it difficult to use some of the features or answer questions. However, when asked about the struggles in the interview, they do not reflect on this. They express that no issues occurred and that the process was "easy".

Another example is participant 1 (P1), who recited some text from the app word by word when asked about her learning outcomes. However, she did not reflect upon what she had read and the context of the information. This could indicate that she was more concerned with remembering the words and sentences by heart than comprehension when she was reading. This behaviour can be linked to the "Hawthorn Effect" described by Oates [12], which could be a disadvantage of 'overt' research. The participant may modify their behaviour when being observed due to stress. An effect is that the observed participant may become uncomfortable if they suspect that the observer does not approve of their answers or behaviour.

Some of the participants unsolicited told about experiences with meeting scammers on social media platforms. Participant 2 (P2) in Gambia told a story about an episode when she almost got scammed by a stranger on Facebook. Outtakes from the story is included in 7.3.2. The participant was eager to tell this because she recognized similarities to what the information in the app had presented. Two other participants also mentioned previous experiences with hackers and scammers they had encountered on Facebook and through email.

These stories and reflections of previous experiences underline the importance of teaching CSA in rural and underdeveloped areas. They show that the dangers of online presence exist even in rural villages. These stories also confirm the statement from Save the Children during expert interviews:

> "It has become frighteningly easy for criminals to get a hold of young people through social media platforms".

8.2 Factors to consider when educating cyber security awareness in underdeveloped areas

Both the findings from the expert interviews, observation and participant interview sessions highlighted aspects which should be considered when education CSA in developing countries. Four key factors are presented in this section.

8.2.1 Adapting to specific cultures

An aspect drawn from the findings from the test sessions in Gambia, is the importance of cultural and local adaption of content when disseminating new information. There were several examples of terms used in the applications to draw a picture related to a cyber security topic, which the participants struggled to understand because they could not relate to it. One example is how one of the participants did not understand what a "pet" was. Others could not relate to the terms used concerning banking and financial services or did not know what a "social security number" was. One of the participants asked what "nude photos" meant, and when explained, still could not relate to it.

Another important aspect to consider is using formulations, language or jargon that the interviewee may not understand, as Preece *et al.* [13] emphasizes when conducting interviews. This aspect became evident when the participants were asked the following question:

> "What gender do you identify as?"

In developed countries and particularly in western culture, formulating a question about gender in this manner is expected and considered "correct". However, in rural communities in an LDC like Gambia, the cultural traditions are far more conservative and less developed. Gender roles and identification has not been challenged in these countries, and thus a question formulated in this manner was very unfamiliar to the participants. The question had to be repeated and reformulated for each participant to understand.

These terms do not categorize as special cyber security terms but rather terms which describe societal phenomenons and constructions. However, these constructions and phenomenons do not apply to a rural village in a developing country like Gambia. Gambians often live by strict Muslim traditions[3], and thus topics that deal with nudity, dating, sexuality and gender identification are rarely or never a topic of conversation. Having a pet in a household is not a common phenomenon. These terms referred to phenomena and constructions common in societies in developed countries.

The paper by Herkanaidu *et al.* [28] addresses this aspect in the proposal of a framework and process of creating a CSA program. Their objective is to provide an educational program that is locally relevant, which can lead to better success instead of transposing a program from another country.

8.2.2 Literacy and language level adaption

As addressed in Section 7.2.2, the language abilities of the participants varied. Some participants encountered few issues reading and understanding the information provided in the apps, whilst others struggled with reading and comprehending. English is the official language in Gambia, and thus the majority speaks and understands English orally to a certain level. However, in 2015 the literacy rate of youth aged 15-24 years old was 67%[4]. A reflection provided by a Leap Learning representative in Gambia was that within the age group of the participants in this study, the knowledge and literacy levels are not necessarily correlated to their age. To a greater extent, it depends on how much schooling they have received throughout their lives. The observations of participant 4 represent this reflection. This participant struggled to read to a level where the facilitator had to read the text aloud to the participant. When given the apps' contents orally, the participant understood significantly better.

To address the gap between oral understating and literacy levels, including sounds and audio of written contents could be part of the solution. Sound could accompany the text, giving illiterate people equal access. Generally, illiteracy is an issue in all LDCs[5]. This issue was also addressed in the findings from the expert interviews.

For the participants in Norway, their first language was their mother tongue, and Norwegian was their second language. They were taught English at a secondary-school level, and it was observed that they had to concentrate on the language barrier when reading. This barrier could have come at the expense of their comprehension. The comprehension of the presented information might have been better if it had been presented in Norwegian or their mother tongue. Adapting the language to the target user would also contribute to a higher learning outcome.

[3] https://www.state.gov/reports/2019-report-on-international-religious-freedom/the-gambia/

[4] https://data.worldbank.org/indicator/SE.ADT.1524.LT.ZS?locations=GM

[5] https://data.worldbank.org/indicator/SE.ADT.LITR.ZS?locations=XL

8.2.3 Introducing cyber security terms

Cyber security is an area where special terminology is often present. These terms may be familiar or unfamiliar to the target user, depending on prior knowledge. For the participants in Gambia, the majority struggled with at least one cyber security related term, as displayed in Table 7.4. "Scam", "malicious", "catfishing", "blackmail", "extortion" and "digital footprint" are examples of cyber security terms the participants struggled to interpret. However, these terms are important to include when teaching CSA due to their relevance to the topic. Thus, the challenge is to find ways to present the key information and terms in a manner which was understandable to the target audience. This could, for example, be through using examples from a real-life setting when explaining a difficult term, as the Leap Learning representative emphasized in the expert interview.

8.2.4 Functionality measuring learning outcome

One of the key takeaways from the study by Adelola *et al.* [16], which was included in the SLR, was the importance of measuring and testing the users' knowledge and ability level. By including testing for comprehension, the aim is to engage the user to reflect upon the information provided. In addition, it can give an indicator to the educator whether or not the information fits the target audience.

The functionality implemented in the working prototype included a "Select Sentence" functionality and prioritization functionality, intended to work with a drag-and-drop behaviour. Both functionality types aimed to test whether or not the user comprehended the information provided in the informative apps. For the participant to proceed to the next task, they had to complete the task by providing the correct answer. As explained in Section 6.2.2, the app gave user feedback in the form of fields turning green when the correct answer or solution was given. However, this functionality "forced" the user to give the correct answer to proceed to the next task. During the observation sessions, it was discovered that this encouraged some users to try different alternatives until they got the correct answer instead of taking a moment to reflect before choosing an answer. A suggested solution to avoid this issue could be to give the user one or two chances to provide the correct answer before proceeding to the next task. After all the tasks are finished, the user could get feedback or score on which tasks they got right and wrong. This approach could also be more motivating and encourage concentration and reflection.

8.3 Implication for Research and Practice

The SLR conducted in the specialization project investigated the "State of the Art" of CSA in developing countries. The SLR revealed that limited research had been conducted within the field. No previous research specifically targeted adolescents and young adults within the age range of 13 to 30 years in developing countries.

This research has identified factors which should be considered when educating CSA in developing countries. These factors can also apply to other scenarios involving introducing digital platforms and tools for educational purposes in rural areas. Researchers can keep these factors in mind when conducting future research in developing countries.

An IT artefact in the form of a working prototype was developed in this master thesis project. Further research could develop and advance the working prototype and evaluate the solution in a broader context. A quantitative investigation could be conducted by expanding the investigations to a larger group of developing countries.

This thesis can be a basis of knowledge and influence for Leap Learning in their work towards providing education within the field of CSA. The research also provides Leap Learning with valuable feedback regarding the design of features and functionality in their application, which can be used for future improvement. The process and findings in this master thesis can also inspire other practitioners and organizations to develop digital tools to teach in developing countries, specifically targeting rural areas.

8.4 Limitations

To gather enough studies in the SLR, some of the studies in the final selection had target groups which did not reflect the target group of the specialization project and master thesis, namely adolescents and young adults between 13 to 30 years of age. The studies included other target groups, such as children and adults older than 30. The inclusion of other target groups was necessary due to the limited amount of studies conducted within this exact field of research. It also emphasizes the need for further research within this field.

Throughout both the expert interviews, it was evident that children were the group of focus, which does not target the correct target group in this master thesis. However, the term "children" refers to all human beings under 18 years old, and adolescents can also be categorized under the "children" term.

The data collection presented in Chapter 7 is based on findings from observation and interview sessions with a total of eight participants. A higher number of participants would have been ideal. Due to recruitment complications for testing in Norway as well as time restrictions of the project, eight participants became the final participant selection. Nevertheless, all the participants who contributed to the project fit well into the target group requirements, as they were all within the age gap range and originated or lived in a country which fit either into the LDC or "developing country" category. The participants in Gambia came from the same village and community, and thus it can be assumed that they would have similar backgrounds and experiences going into the test sessions. In contrast, the two participants in Norway lived in a well-developed country for several years and thus had a different background going into the test sessions.

The results from the observations are based solely on the notes made by the facilitators and Leap Learning's representatives. According to Oates [12], systematic observation enables the possibility of delegating the observation to multiple observers. Still, there is a possibility that the observer may have missed some observations or misinterpreted a participant's actions. The observation results are thus a reflection of the observer's interpretation.

As presented in Section 5.1, Leap Learning acted as a stakeholder and close collaboration partner throughout this master thesis project. The working prototype was developed through their platform, and the observations and interviews conducted in Gambia were conducted in collaboration with Leap Learning. Having Leap Learning as a stakeholder and collaboration partner provided many possibilities for the master thesis project and posed some limitations. Firstly, the technology stack could not be changed, and the application had to be implemented using the technologies already used in the platform. It also meant that design guides and pre-existing functionality set some constraints on the design and functionality of the application. The technical stack and design functionality choices were presented, and Chapter 6. Despite these restrictions, the pre-existing templates and functionalities were designed to fit the needs of people living in rural areas in developing countries, which can justify the reuse.

8.5 Future work

The research conducted, in particular through testing and evaluation of the working prototype, has revealed several ideas for future development and improvement.

8.5.1 Implementation of additional CSA topics

Initially, it was concluded from the results from the SLR and expert interviews that the seven cyber security topics, presented in Section 6.2, should be addressed in the application. Three topics were chosen for the first prototype iteration following the principle of multiple iteration cycles of the Design and Creation strategy. The three chosen topics were: *Interaction with strangers online, Password habits, and Sharing private information online*. As the remaining four topics are considered equally as important to educate, the following topics should be included in the application in future iterations:

- Harmful content
- Cyberbullying
- Phising attacks
- Identity theft

8.5.2 Modifications and new functionality

By observing and testing the apps included in the working prototype, several ideas for modifications and improvement of existing functionality were revealed. As discussed in Section 8.2.4, giving the user one or two attempts to complete a single task before proceeding to the next was one of them. If the user fails to answer a question correctly, the user will receive feedback. When all tasks in an app are completed, the user could receive a score saying how many were completed correctly and which tasks the user failed.

A gradual introduction of the terms is suggested to address the issue of complex cyber security terms. By dividing the information into levels based on complexity, the user could process the information gradually. The preliminary levels would explain the basics, avoiding using complex terms. The introduction of complex terms could unfold at higher levels when the user has built up basic knowledge on a cyber security topic.

8.5.3 Distribution through Leap Learning

The working prototype is implemented through Leap Learning's platform, and thus the apps will remain in their possession after this master thesis project is finished. Further development is thus dependent on a continued partnership with Leap Learning. Their ambitions when entering this project was to contribute within the field of CSA in developing countries, and they aim to continue this work.

Chapter 9

Conclusion

The Systematic Literature Review (SLR) conducted in the specialization project laid a foundation for aspects of cyber security that should be addressed in an informative digital platform aimed at adolescents and young adults in developing countries [4]. The thorough study of "State of the Art" within the field of Cyber Security Awareness (CSA) in developing countries highlighted the cyber security risks which were most prominent for adolescents and young adults in developing countries. *Harmful content, interaction with strangers, cyberbullying, password habits, sharing private information, phishing attacks, and identity theft* were identified as the most prominent risk factors in the SLR.

Expert interviews contributed to knowledge from representatives who had in-the-field experience with education and the introduction of digital tools in rural communities in developing countries. Based on the findings from the SLR and expert interviews, a working prototype to educate adolescents and young adults between the ages of 13-30 was developed in collaboration with Leap Learning[1]. The prototype consisted of multiple apps that aimed to provide information about different cyber security topics and test the users' comprehension and learning output of the information received. Testing of the prototype was done through observation and interviews with users within the target group. The findings from the test sessions revealed that the apps in the prototype did provide the participants with knew knowledge and awareness within the cyber security field. Additionally, four key factors to successfully educate CSA in a developing country context were identified. The factors were: adapting the country to specific cultures, conveying information adapted to the language and literacy levels, introducing cyber security terms and using functionality which measures the user's learning outcome.

Future work includes addressing CSA topics which were not included in the first iteration of the working prototype, as well as modifications and additional functionality to fit the four key factors presented.

[1] https://leaplearning.no/home

Bibliography

[1] E. Richardson, D. Aissat, G. A. Williams, N. Fahy *et al.*, 'Keeping what works: Remote consultations during the covid-19 pandemic,' *Eurohealth*, vol. 26, no. 2, pp. 73–76, 2020.

[2] ITU. 'Connectivity in the least developed countries: Status report 2021.' (2021 [cited 2022 Apr 30]), [Online]. Available: `https://www.itu.int/en/myitu/Publications/2021/09/17/11/46/Connectivity-in-the-Least-Developed-Countries-Status-report-2021`.

[3] P. B. Maoneke, D. F. B. Shava, A. M. Gamundani, M. Bere-Chitauro and I. Nhamu, 'Icts use and cyberspace risks faced by adolescents in namibia,' *ACM International Conference Proceeding Series*, pp. 109–117, Dec. 2018. DOI: `10.1145/3283458.3283483`.

[4] G. N. Freberg, *Designing software to raise cyber security awareness in developing countries: A systematic literature review*. [Online]. Available: `https://sbs.idi.ntnu.no/master`.

[5] F. Quayyum, D. S. Cruzes and L. Jaccheri, 'Cybersecurity awareness for children: A systematic literature review,' *International Journal of Child-Computer Interaction*, p. 100 343, 2021.

[6] R. Von Solms and S. Von Solms, 'Cyber safety education in developing countries,' 2015.

[7] V. Svabensky, J. Vykopal and P. Celeda, 'What are cybersecurity education papers about? a systematic literature review of sigcse and iticse conferences,' in *Proceedings of the 51st ACM Technical Symposium on Computer Science Education*, 2020, pp. 2–8.

[8] J. Poushter, C. Bishop and H. Chwe, 'Social media use continues to rise in developing countries but plateaus across developed ones,' *Pew Research Center*, vol. 22, pp. 2–19, 2018.

[9] K. Aruleba and N. Jere, 'Exploring digital transforming challenges in rural areas of south africa through a systematic review of empirical studies,' *Scientific African*, vol. 16, e01190, 2022.

[10] M. Grobler, J. Jansen van Vuuren and J. Zaaiman, 'Evaluating cyber security awareness in south africa,' 2011.

[11] Google, The Net Safety Collaborative, Internet Keep Safe Coalition, 'Digital safety and citizenship curriculum,' 2021.

[12] B. J. Oates, *Researching information systems and computing*. Sage, 2005.

[13] J. Preece, Y. Rogers and H. Sharp, *Interaction Design: Beyond Human-Computer Interaction*, 4th ed. Wiley, 2015.

[14] K. A. Ericsson and H. A. Simon, *Protocol analysis: Verbal reports as data.* the MIT Press, 1984.

[15] B. Kitchenham and S. Charters, 'Guidelines for performing systematic literature reviews in software engineering,' 2007.

[16] T. Adelola, R. Dawson and F. Batmaz, 'The urgent need for an enforced awareness programme to create internet security awareness in nigeria,' in *17th International Conference on Information Integration and Web-Based Applications and Services, iiWAS 2015 - Proceedings*. DOI: 10.1145/2837185.2837237.

[17] S. S. Oyelere, D. I. Sajoh, Y. M. Malgwi and L. S. Oyelere, 'Cybersecurity issues on web-based systems in nigeria: M-learning case study,' in *CYBER-Abuja 2015 - International Conference on Cyberspace Governance: The Imperative for National and Economic Security - Proceedings*, pp. 259–264. DOI: 10.1109/CYBER-Abuja.2015.7360510.

[18] E. N. Onwuka, D. O. Afolayan, W. Abubakar and J. I. Ibrahim, 'Survey of on-line risks faced by internet users in the nigerian telecommunication space,' in *CEUR Workshop Proceedings*, vol. 1830, pp. 28–33.

[19] F. Alotaibi, S. Furnell, I. Stengel and M. Papadaki, 'A survey of cyber-security awareness in saudi arabia,' in *2016 11th International Conference for Internet Technology and Secured Transactions, ICITST 2016*, pp. 154–158. DOI: 10.1109/ICITST.2016.7856687.

[20] N. Ahmed, U. Kulsum, M. I. Bin Azad, A. S. Z. Momtaz, M. E. Haque and M. S. Rahman, 'Cybersecurity awareness survey: An analysis from bangladesh perspective,' in *5th IEEE Region 10 Humanitarian Technology Conference 2017, R10-HTC 2017*, vol. 2018-January, pp. 788–791. DOI: 10.1109/R10-HTC.2017.8289074.

[21] E. H. R. Rho, A. Kobsa and C. Nguyen, 'Differences in online privacy and security attitudes based on economic living standards: A global study of 24 countries,' in *26th European Conference on Information Systems: Beyond Digitization - Facets of Socio-Technical Change, ECIS 2018*.

[22] V. Visoottiviseth, R. Sainont, T. Boonnak and V. Thammakulkrajang, 'Pomega: Security game for building security awareness,' *Proceeding of 2018 7th ICT International Student Project Conference, ICT-ISPC 2018*, Nov. 2018.

[23] F. Calderwood and I. Popova, 'Smartphone cyber security awareness in developing countries: A case of thailand,' in *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST*, vol. 260, 2019, pp. 79–86. DOI: 10.1007/978-3-030-05198-3_7.

[24] A. Owusu, J. Broni F. E. and P. K. Akakpo, 'Preliminary insights into the concerns of online privacy and security among millennials in a developing economy,' *Journal of Theoretical and Applied Information Technology*, vol. 97, no. 11, pp. 3063–3076,

[25] L. Y. C. Chang and N. Coppel, 'Building cyber security awareness in a developing country: Lessons from myanmar,' *Computers and Security*, vol. 97, 2020. DOI: 10.1016/j.cose.2020.101959.

[26] D. K. M. P. M. M. Dassanayake, S. N. Wijesinghe, T. L. C. Jayasiri, K. A. R. T. Keenawinna, W. H. Rankothge and N. D. V. Gamage, 'Awareme: Public awareness through game-based learning,' in *IEEE Region 10 Annual International Conference, Proceedings/TENCON*, vol. 2020-November, pp. 662–666. DOI: 10.1109/TENCON50793.2020.9293720.

[27] P. Datta, S. N. Panda and S. Bajaj, 'Data analysis of cyber security for women in haryana,' in *ICRITO 2020 - IEEE 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)*, pp. 763–767. DOI: 10.1109/ICRITO48877.2020.9197788.

[28] R. Herkanaidu, S. M. Furnell and M. Papadaki, 'Towards a cross-cultural education framework for online safety awareness,' in *IFIP Advances in Information and Communication Technology*, vol. 593 IFIPAICT, 2020, pp. 47–57. DOI: 10.1007/978-3-030-57404-8_4.

[29] H. M. Jawad and S. Tout, 'Introducing a mobile app to increase cybersecurity awareness in mena,' in *2020 3rd International Conference on Signal Processing and Information Security, ICSPIS 2020*. DOI: 10.1109/ICSPIS51252.2020.9340128.

[30] J. Reichel, F. Peck, M. Inaba, B. Moges, B. S. Chawla and M. Chetty, ''i have too much respect for my elders': Understanding south african mobile users' perceptions of privacy and current behaviors on facebook and whatsapp,' in *Proceedings of the 29th USENIX Security Symposium*, pp. 1949–1966.

[31] A. da Veiga, M. Loock and K. Renaud, 'Cyber4dev-q: Calibrating cyber awareness in the developing country context,' *Electronic Journal of Information Systems in Developing Countries*, 2021. DOI: 10.1002/isd2.12198.

[32] Google. 'Be internet awesome curriculum.' (2022 [cited 2022 May 1]), [Online]. Available: https://storage.googleapis.com/gweb-interland.appspot.com/en-us/hub/pdfs/2021/BIA_Curriculum_June-2021_EN_PDF-Version.pdf.

Appendix A

Data Extraction Form

1. Study overview	
Study identifier	Unique ID for the study
Extraction date	
Bibliographic reference	Author, Title, Year, Publication Source, Abstract, Pages
2. Design of the study	
Study type	Qualitative, Quantitative, Mixed
Research Methodology	Case Study, Experiment, Action research, Interview, Survey, Other
Research questions	
Research context	What are the aims and objectives of the study?
Research country	
Target audience (age)	
Target gender	
3. Cyber security risks	
What risks has been addressed and focused on?	
4. Approaches for raising CSA	
What is the approach?	
Description of how the approach has been used	What kind of activities has been used?
Effect of the approach	Successful/ failure/ effective ?
Type of elements in the approach	Game elements, intervention, informative
5. How has the level of CSA been measured?	
What has been measured	
Parameters used	
6. Data collection and analysis	
Data collection instrument	
Sample size	
Data analysis (qualitative/quantitative)	
Data analysis method	
7. Data collection and analysis	
Fidnings	
Threats to validity/ limitaions	

Table A.1: Data extraction template

Appendix B

Consent form

Do you want to participate in the research project

”Raising Cyber Security Awareness for Adolescents and Young Adults in Developing Countries”?

This is a question for you to participate in a research project where the purpose is to investigate how to design and develop software to increase awareness and knowledge about cyber security for adolescents and young adults in developing countries. In this consent form, you get information about the goals of the project and what participation will mean for you.

Purpose

The project is a master's thesis at the Department of Computer Science and Informatics (IDI) at the Norwegian University of Science and Technology (NTNU). The master's thesis is part of the NTNU project “Software For A Better Society”, led by Professor Letizia Jaccheri. The thesis focuses on how to use software to inform adolescnets and young adults in developing countries about how to safely navigate the Internet. The goal is to implement an application for this purpose. Development and testing of the application will be done in collaboration with the company Leap Learning, who have many years of experience in developing and implementing applications for learning purposes in areas where digital competence is low.

Who is responsible for the resesearch project?

The master thesis is performed by master student at Computer Science, Giske Naper Freberg, and supervised by Professor Letizia Jaccheri at IDI NTNU. PhD candidate Frazana Quayyum is the co-supervisor of the master thesis project.

Why are you asked to participate?

You will be asked to participate due to your age, geographical and ethnic background. Your participation will contribute to increased insight into the needs of young people and young adults in developing countries in the face of the Internet and digital tools. The information you provide will contribute to the content and user insight into the planned application.

What does it mean for you to participate?

If you choose to participate, you will participate in a user test of the application, as well as a follow-up interview. Audio recordings of user testing and interviews will be taken, which will be used to transcribe and analyze the obtained data afterwards.

It is voluntary to participate

It is voluntary to participate in the project. If you choose to participate, you can withdraw your consent at any time without giving any reason. All your personal information will and data then be deleted. It will not have any negative consequences for you if you do not want to participate or later choose to withdraw.

Your privacy - how your information is stored and used

The information about you will only be used for the purposes described in this article. The information is treated confidentially and in accordance with the privacy regulations. Only the master's student and the supervisors, as mentioned earlier, will have access to the information.

Names and contact information about you will be replaced with a code that is stored on a separate list of names separate from other data. The data material is stored on Microsoft OneDrive. NTNU has a data processing agreement with Microsoft, and all services are password protected. The student who conducts and transcribes the interviews will be the only one with access to the audio recordings from the interviews.

Participants will not be recognized in the publication.

What happens to your information when the research project ends?

When the project is completed / the master's thesis is approved, which according to the plan is approx. 31.12.22, the data material will be anonymised. All audio and video recordings will be deleted.

What gives us the right to process personal data about you?

We process information about you based on your consent.

On behalf of NTNU, NSD - Norwegian Center for Research Data AS has assessed that the processing of personal data in this project is in accordance with the privacy regulations.

Your rights

As long as you can be identified in the data material, you have the right to:

- Insight into what information we process about you, and to receive a copy of the information
- To correct information about you that is incorrect or misleading
- To have personal information about you deleted
- To send a complaint to the Norwegian Data Protection Authority about the processing of your personal data

If you have questions about the study, or want to know more about or exercise your rights, please contact:

NTNU - Norges teknisk-naturvitenskapelige universitet by student Giske Naper Freberg per email (giskenf@stud.ntnu.no) or phone number: +47 951 97 732

NTNU - Norges teknisk-naturvitenskapelige universitet by supervisor Letizia Jaccheri by email (letizia.jaccheri@ntnu.no) or phone: +47 918 97 028

NTNUs privacy representative by Thomas Helgesen at thomas.helgesen@ntnu.no

If you have questions related to the Privacy Services' assessment of the project, you can contact:
Privacy services by email (personverntjenester@sikt.no) or by phone: +47 53 21 15 00.

If you have questions related to NSD's assessment of the project, you can contact:

- NSD – Norwegian Center for Research Data AS by email (personverntjenester@nsd.no) or by phone: +47 55 58 21 17.

With Kind Regards

Letizia Jaccheri	Giske Naper Freberg
Project resposible	Project participant
(Professor)	(Master student)
	Giske N. Freberg

18.04.2022

Summary of consent form

In this consent form the purpose of your participation to the master thesis project is explained. You are asked to participate in the project beacuse of your age, ethinical and geographic backgrond. All data collected during the user test and interview will be anonomized, and and you have the right to withdraw your participation at any time. The data collected from you will then be deleted.

Declaration of Consent

I have received and understood information about the project "Raising Cyber Security Awareness for Adolescents and Young Adults in Developing Countries", and have had the opportunity to ask questions. I agree to participate in a semi-structured interview where audio recordings are made, as well as user testing and that my information is processed until the project is completed, approx. 31.12.22.

(Signed by project participant, date)

Appendix C

User testing guide

User testing guide - Gambia

This is a guide for conducting user testing and interviews of the apps ”Cyber Security Awareness” (CSA) in the Leap Learning App Universe. The user testing will consist of two parts. The first will be a usability test with a facilitator, followed by an interview of the participant.

Target group

The target group of this project are teenagers and young adults from developing countries within the age group 13-30 years old. Between 5 to 10 participants with different ages and gender are preferable, but selection of the participants depends on their availability and the facilitators schedule. .

Before beginning the user testing

1) Introduce yourself (the facilitator).
2) Explain the purpose of the test: “The purpose of this test is to investigate whether the apps can contribute to better cyber security habits and to uncover possible improvements.”
3) Explain the outline of the test: “The test consists of two parts: first you will test the apps where you are asked by the facilitator to perform different tasks. The second part is an interview where you will be asked some general info followed by questions about how you experienced interacting with the applications”.
4) Signing of consent form: Each participant **must sign** the consent form (attached in this guide), so that the data can be included in the master thesis report. Each participant will be anonymized, and can at any point during or after the testing withdraw his/hers consent. The data will then be deleted and not included in the master thesis report. It is important that this is communicated clearly to the participant. **NB! If the participant is under 16 years old a parent will have to sign the form on their behalf.**
5) Encourage the participants to **think aloud** during the user testing.
6) Ask the participant if they have understood everything and if they have any questions before beginning the test.

During user testing

In this part of the user testing the facilitator will give the participants tasks to perform and observe the participant’s interaction with the apps. It is important to underline that you as facilitator have an observing role, meaning you are not going to help the participant perform the tasks, only give instructions. Encourage the user to say what they are thinking out loud. If you see the participant struggling or becoming silent during a task, try to encourage them by kindly asking “What are you thinking?”.

Write down your observations as the participant works on tasks. This is easier to do if you are two people, so one can present the task and interact with the participant whilst the other one writes down the observations. You can record the audio if you find that easier, but the observations that are not possible to record must be written down.

Types of observations which should be written down:

- The thoughts that the participants are saying aloud.
- Participants struggling to understand what they are reading.
  - Are they spending a lot of time trying to understand what they are reading?
- Participants struggling to understand how to interact with the interface in the apps.
  - What are they struggling with?
  - Are they pressing the wrong buttons?
- Participants who do not seem to have struggles with the apps. This should be noted too.

All observations must to connected to a specific participant. Here is an example of how you can document your observations:

Participant no.	App observed	Observations
1	"About Passwords"	- Participant reads the information out loud without much problems. - Participants is able to navigate the slides with the arrow buttons. - On the fourth slide the participant takes more time reading, and is struggling.
	"Passwords Priority"	- The participant uses some time to slide the different options up and down. - The participant does not understand how to exit the app.

Each participant should test <u>all the apps in at least one of the different CSA themes (Passwords, Online Strangers or Private Information). P</u>referably they should be tested in two themes. However, if testing of one theme takes a long time it is ok to only test one. The following tasks should be given each participant:

<u>Questions for testing "Passwords apps":</u>

1) Click on the "About Passwords" app.
2) Read the text on the screen. Read aloud if you want to.
3) When finished reading, navigate to the next task.
4) Repeat point 2) and 3) until all tasks are read through.
5) Exit the application.

6) Click on the "Select Sentence" app.
7) Answer the question by choosing what you believe is correct.
8) Navigate to the next task
9) Repeat point 7) and 8) until all tasks are performed.

10) Exit the application.

11) Click on the “Password Priority”
12) Read the task and solve it
13) Navigate to the text task
14) Repeat point 12) and 13) until all tasks are performed
15) Exit the application.

Questions for testing “Online Strangers apps”:

1) Click on the “About Online Strangers” app.
2) Read the text on the screen. Read aloud if you want to.
3) When finished reading, navigate to the next task.
4) Repeat point 2) and 3) until all tasks are read through.
5) Exit the application.

6) Click on the “Select Sentence” app.
7) Answer the question by choosing what you believe is correct.
8) Navigate to the next task-
9) Repeat point 7) and 8) until all tasks are performed.
10) Exit the application.

Questions for testing “Private Information apps”:

1) Click on the “About Online Strangers” app.
2) Read the text on the screen. Read aloud if you want to.
3) When finished reading, navigate to the next task.
4) Repeat point 2) and 3) until all tasks are read through.
5) Exit the application.

6) Click on the “Select Sentence” app.
7) Answer the question by choosing what you believe is correct.
8) Navigate to the next task.
9) Repeat point 7) and 8) until all tasks are performed.
10) Exit the application.

After user testing

After the user testing is finished the participant will be interviewed. For the interview you can record the audio during the interview.

Interview guide

Demographic data/ general info:

1. What is your first name? (Only to distinguish the participants, will not be included in master thesis report)
2. How old are you?
3. What is your country of origin?
4. What gender do you identify yourself as?
5. Do you have access to digital devices and internet service in your daily life?
   a. If yes, what type of digital device(s) do you use?
6. Have you received any training education on cyber security awareness before?
7. Do you have any sort of social media account? Like WhatsApp, Facebook or Instagram?
8. Do you have an email account?

About the application:

1. Did you learn anything new when using the application?
   a. If yes, can you mention something you learned?
2. Was it information that you were presented in the app that you knew from before?
   a. If yes, what did you already know?
3. Did you have any difficulties understanding how to use any of the applications?
   a. If yes, what was difficult to understand?
4. How did you find the language in the application?
   a. Was the level of English difficult to understand?
   b. Were the sentences too long and difficult?
5. Which parts of the application did you enjoy the most?

Appendix D

Miro boards

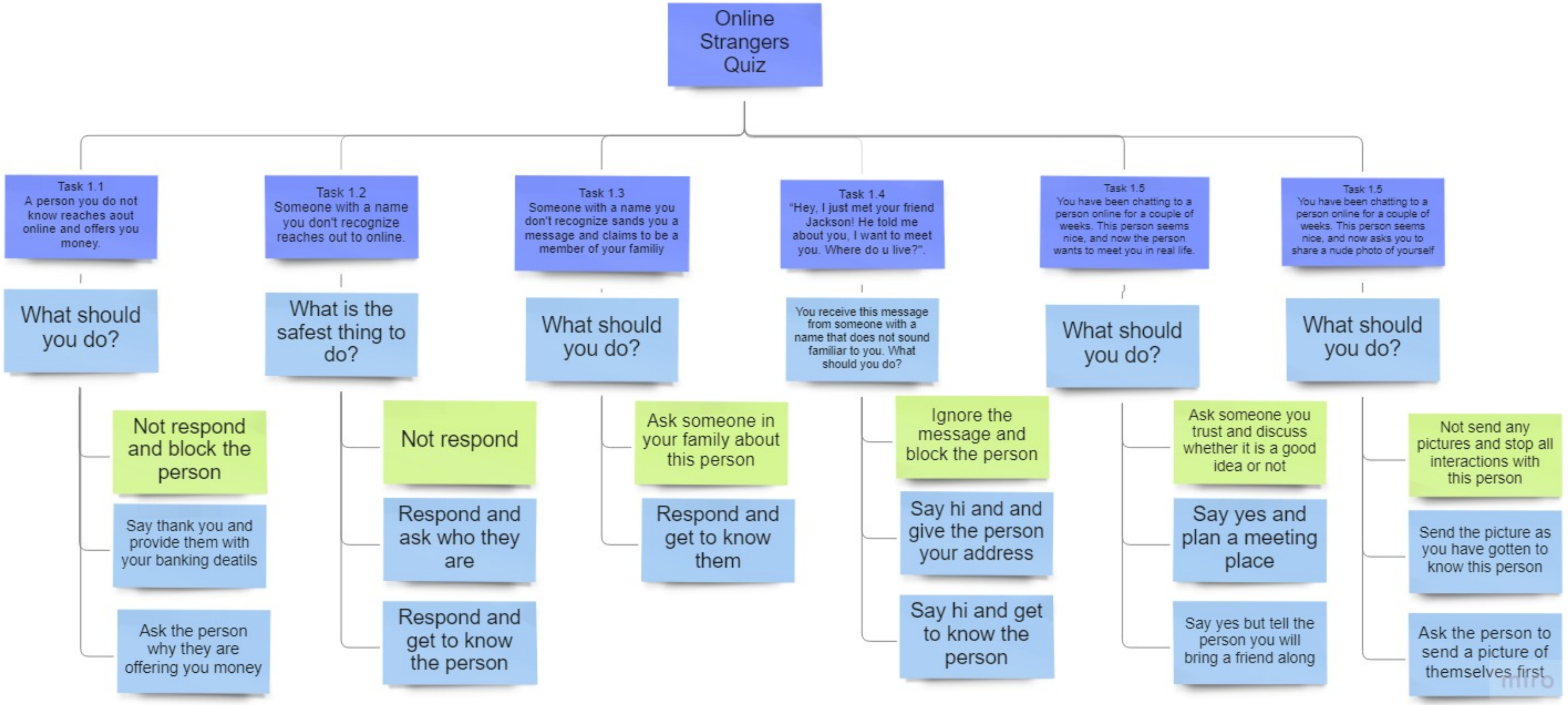

Online Strangers Quiz
Task 1.1 A person you do not know reaches aout online and offers you money.
What should you do?
Not respond and block the person
Say thank you and provide them with your banking deatils
Ask the person why they are offering you money
Task 1.2 Someone with a name you don't recognize reaches out to online.
What is the safest thing to do?
Not respond
Respond and ask who they are
Respond and get to know the person
Task 1.3 Someone with a name you don't recognize sands you a message and claims to be a member of your familiy
What should you do?
Ask someone in your family about this person
Respond and get to know them
Task 1.4 "Hey, I just met your friend Jackson! He told me about you, I want to meet you. Where do u live?".
You receive this message from someone with a name that does not sound familiar to you. What should you do?
Ignore the message and block the person
Say hi and and give the person your address
Say hi and get to know the person
Task 1.5 You have been chatting to a person online for a couple of weeks. This person seems nice, and now the person wants to meet you in real life.
What should you do?
Ask someone you trust and discuss whether it is a good idea or not
Say yes and plan a meeting place
Say yes but tell the person you will bring a friend along
Task 1.5 You have been chatting to a person online for a couple of weeks. This person seems nice, and now asks you to share a nude photo of yourself
What should you do?
Not send any pictures and stop all interactions with this person
Send the picture as you have gotten to know this person
Ask the person to send a picture of themselves first
miro

Figure D.1: Miro board with ideas for "Online Strangers Quiz"

Giske Naper Freberg

Designing Software to Raise Cyber Security Awareness in Developing Countries

NTNU
Norwegian University of
Science and Technology