Master's thesis

NTNU
Norwegian University of Science and Technology

Marit Sylstad

Chat Room safety

Keeping children safe in online environments

Master's thesis in Interaction design

October 2020

NTNU
Norwegian University of
Science and Technology

Marit Sylstad

Chat Room safety

Keeping children safe in online environments

Master's thesis in Interaction design
Supervisor: Professor Patrick Bours
Co-supervisor: Frode Volden
June 2021

Norwegian University of Science and Technology
Faculty of Architecture and Design
Department of Design

NTNU
Norwegian University of
Science and Technology

Abstract

Children and young people are spending more and more of their time on the internet. By the age of ten, almost all children have access to a smartphone. Nine out of ten children and young people aged nine to 18 use one or more social media, and the proportion increases with age. The development of the internet and social media in combination with children and young people's access to PC, tablet and other mobile devices offer great opportunities for people seeking to establish sexualised contact with children. Many of the websites, social media and online games intended for and used by children are also used by adults, who in various ways entice children into sexualised situations. Through grooming, an adult can build a relationship, trust and emotional connection with a child or young person, which they later can take advantage of to manipulate, exploit and abuse them. This study is intended to acquire insight into the knowledge of grooming and online sexual predators. Through this, the aim is to develop a way to warn children in live chat conversations.

The master thesis will be part of the AiBA (Author Input Behavioral Analysis) project, which monitors chat conversations through behavioural biometrics and text analysis to warn users about false identities and suspicious behaviour. The AiBA project is conducted by the Norwegian Biometry Laboratory, which is part of the Department of Information Security and Communication Technology at NTNU Gjøvik. The project aims to identify fake profiles in chat applications using a machine learning approach within the field of keystroke dynamics and stylometry, particularly for protecting children from sexual predators that find their victims online.

Sammendrag

Barn og unge bruker mer og mer av sin tid på internett. I en alder av ti har nesten alle barn tilgang til en smarttelefon. Ni av ti barn og unge i alderen ni til 18 bruker ett eller flere sosiale medier, og andelen øker med alderen. Utviklingen av internett og sosiale medier i kombinasjon med barn og unges tilgang til PC, nettbrett og andre mobile enheter gir store muligheter for mennesker som ønsker å etablere seksualisert kontakt med barn. Mange av nettstedene, sosiale medier og nettspill som er ment for og brukes av barn - brukes også av voksne som på forskjellige måter lokker barn til seksualiserte situasjoner. Gjennom grooming prosessen kan en voksen bygge et tillitsforhold og oppnå en følelsesmessig forbindelse med et barn eller en ungdom, som de senere kan dra nytte av for å manipulere, utnytte og misbruke dem. Denne oppgaven er ment å skaffe innsikt i kunnskapen om grooming og seksuelle overgripere på nettet. Gjennom dette er målet å utvikle en måte å advare barn på i live chat-samtaler.

Masteroppgaven vil være en del av prosjektet AiBA (Author Input Behavioral Analysis), som overvåker chattesamtaler gjennom atferdsbiometri og tekstanalyse for å advare brukere om falske identiteter og mistenkelig atferd. AiBA-prosjektet er gjennomført av Norsk biometri-laboratorium som er en del av Institutt for informasjonssikkerhet og kommunikasjonsteknologi ved NTNU på Gjøvik. Prosjektet har som mål å identifisere falske profiler i chatte-applikasjoner ved hjelp av en maskinlæringsmetode innen tastetrykkdynamikk og stylometri, spesielt for å beskytte barn mot seksuelle overgripere som finner ofrene sine online.

Preface

This Master's thesis constitutes the final assessment in the Master programme Interaction Design at NTNU in Gjøvik. It was mainly conducted during the spring semester of 2021 and is accredited with 30 ECTs. During the fall semester of 2020, the research for this thesis was planned, a literature review was also conducted. This work was accredited with 7,5 ECTs. It was realised as part of the AiBA project by the Norwegian Biometry Laboratory.

The thesis consists of five sections following the IMRaD structure and relate

to introduction and state of the art, description of the methodology, presentation of results as well as a discussion and conclusion part.

I would like to thank my supervisor Patrick Bours for letting me contribute to the AiBA project and providing me with excellent support during my thesis writing. I benefited greatly from his guidance and support, in addition to his contacts at local schools. On this note, I also want to thank Kopperud skole and Vestre Toten ungdomsskole for participating in my study. An extra big thank you to the 9th-grade students from Kopperud skole who participated in our focus groups during the spring of 2021. In addition, I would like to thank my fellow student Nakul Pathak for a good collaboration with the collection of data for this master thesis. There were many hours spent discussing various approaches, planning and creating guides and tasks for the interviews and focus groups. We also spend much time exploring and planning the questions and the design of our survey.

I also would like to thank my second supervisor Frode Volden who has given me valuable advice and great help in analysing a large amount of data from our survey. Frode was also the one who introduced me to Patrick and suggested a collaboration for my thesis.

I greatly appreciate the love and support that I have received from my family, especially my husband's patience during my three years as a master student. He has spent many a night putting the kids to bed while I was hard at work doing research or collaborating with other students.

Table of Contents

1 List of Figures xiii
2 List of Tables xiv
3 List of Abbreviations (or Symbols) xv
1 Introduction 17
1.1 Introduction to the topic 17
1.2 The corona pandemic 18
1.3 Keywords 19
1.4 Topics covered 19
1.5 Problem Description 19
1.6 Significance, Motivation, and Benefits 20
1.7 Research question and hypothesis 20
1.8 Terms and phrases relating to child sexual abuse 20
2 Background 23
2.1 The AiBA Project 23
2.2 Children and social media 24
2.3 Grooming 25
2.4 Online sexual grooming 26
2.5 Children's awareness and perceptions of online risks 30
2.6 Parental mediation 31
2.7 Risk communication 33
2.8 Warning design 35
2.9 Design guidelines 38
2.9.1 Usability Heuristics 38
2.9.2 Universal and accessible design 39
2.9.3 Use of colour 41
2.9.4 Visualisation 43
2.10 Government prevention efforts 44
3 9. Methodologies 45

3.1 The research process 45
3.2 Research participants 46
3.3 Semi-structured Interviews with parents 47
3.4 Survey for children 5th to 9th grade 49
3.5 Focus group and co-creation with 9th-grade children 50
3.5.1 Practical implementation 51
3.5.2 Purpose of exercise 52
3.5.3 Focus group design and conduction 52
3.5.4 Child persona 53
3.5.5 Design methods used 54
3.5.5.1 Brainstorming in Activity 1, 2 and 3 54
3.5.5.2 Crazy 8's in Activity 4 54
3.5.5.3 Dot Voting In activity 3 & 4 54
3.6 Expert and Heuristic Evaluation 54
3.7 Prototyping 56
3.7.1 Paper Prototyping 56
3.7.2 Digital Prototyping 56
3.7.3 Warning message and safety words 56
3.8 Ethical Considerations 57
4 10. Results 59
4.1 Semi-structured interviews 59
4.1.1 Thematic Analysis 59
4.1.2 The users 60
4.1.3 Mediation 62
4.1.4 Communication and awareness 65
4.1.5 Privacy 69
4.1.6 Feature requests and possibilities 70
4.2 Survey 72
4.2.1 About the population 72
4.2.2 Access to equipment and technology 73

4.2.3 What social media and chat apps do children use? 74
4.2.4 Experience with chat apps 75
4.2.5 Communicating with strangers online 76
4.2.6 Security and privacy 78
4.3 Focus groups 80
4.3.1 Questions about online risks 80
4.3.2 Activity 1 81
4.3.3 Activity 2 82
4.3.4 Activity 3 83
4.3.5 Activity 4 84
4.4 Initial prototypes 85
4.4.1 Paper prototypes 85
4.4.2 Initial digital prototypes 86
4.4.2.1 AiBA app prototype 87
4.4.2.2 AiBA child warning prototype 88
4.4.2.3 AiBA parents notification 88
4.5 Expert evaluation 89
4.5.1 Prototype: AiBA warning to children in chat 89
4.5.1.1 Were there any actions that did not work as expected? 90
4.5.1.2 Other comments 91
4.5.2 Prototype: AiBA warning to parents 91
4.5.2.1 Do you have any other comments? 92
4.6 Final prototypes 93
4.6.1 The AiBA app prototype 93
4.6.2 Notification from AiBA to parents prototype 93
4.6.3 Notification from AiBA to child prototype 93
5 Discussion and conclusion 94
5.1 Limitations 97
5.2 Further research 97
6 References 98

7 Appendices 111
7.1 NSD application 111
7.2 Information letter about the project and consent form 112
7.3 Interview Schedule – Semi-Structured Interviews 117
7.4 Interview guide - interview with parents 118
7.5 Survey questions 122
7.6 Focus group 130
7.6.1 Plan 130
7.6.2 Presentation for focus groups 131
7.6.3 Mock-ups by the teenagers 139
7.6.4 Crazy-8s 141
7.7 Expert evaluation - questionnaire 145

1 List of Figures

Figure 1 AiBA system structure (Source: https://AiBA.ai/) 24
Figure 2 Colour contrast check on primary design and text colours. 41
Figure 3 Adobe colour tool used to evaluate the colour scheme of the warning levels ... 43
Figure 4 43
Figure 5 43
Figure 6 Design Council's Double Diamond conveys a design process. The two diamonds represent a process of exploring an issue more widely or deeply (divergent thinking) and then taking focused action (convergent thinking)(Design Council, 2015) 46
Figure 7 Kopperud school 52
Figure 8 Child personas 53
Figure 9 Jakob Nielsen's ten usability heuristics that can help the designers to make applications intuitive. Source: (Langmajer, 2019) 55
Figure 10 An overview of the colour coded tags assigned to the data. 60
Figure 11 Word cloud of social media used by children 60
Figure 12 Word cloud of social media used by parents 61
Figure 13 Quote from a parent regarding their kids' view on Facebook 61
Figure 14 Quotes regarding parents' internet use 61
Figure 15 Mediation 62
Figure 16 Quotes regarding active mediation 63
Figure 17 Quotes from parents about restrictive mediation 64
Figure 18 Quotes from parents about technical mediation 64
Figure 19 Quotes from parents about monitoring 65
Figure 20 Information the parents want to receive 66
Figure 21 Awareness training comments from parents 66
Figure 22 Quotes regarding how parents communicate with their kids 67
Figure 23 Quotes regarding the parents main concerns 68
Figure 24 Quotes from parents regarding how to protect the kids online 69
Figure 25 Attitude to kids privacy 70
Figure 26 Parents' quotes about privacy 70
Figure 27 Design improvements and suggestions from the parents 71
Figure 28 Gender of the respondents 72
Figure 29 Which grade the kids are in 73
Figure 30 Kids' access to digital devices 73
Figure 31 When someone asks you to become "friends" 75
Figure 32 79 percent agree that they have a lot of contact with their friends on social media 75

Figure 33 I have a lot of contact with my friends on social media 76
Figure 34 84 percent of the children have had contact with strangers online 76
Figure 35 Crosstab: have you chatted with strangers online 77
Figure 36 Have you been asked to share 77
Figure 37 22 percent had been asked to share a sexual or nude photo 78
Figure 38 What did you do the last time you were asked for private information 78
Figure 39 "What do you need to feel safe while chatting on the internet or using a chat app" 79
Figure 40 The participants strongly believe that they have control over the information they share with their friends and followers 79
Figure 41 73 percent of the children state that they have been informed by their parents about the dangers of using chat apps 80
Figure 42. The teenagers generally feel safe online 81
Figure 43. teenagers themselves want to decide what should be shared with their parents 81
Figure 44. children reflect on what AiBA notifications should say 82
Figure 45. Post-its from activity 1 and activity 2 82
Figure 46. Possible features 84
Figure 47. Crazy 8s results 84
Figure 48 Paper prototypes and ideation 86
Figure 49 AiBA app prototype with basic features 87
Figure 50 AiBA child warning prototype 88
Figure 51 AiBA parents notification 88
Figure 52 experts were told to evaluate the warning steps 89
Figure 53 results from the heuristic evaluation AiBA warning to children 90
Figure 54 Evaluation of the warning steps 91
Figure 55 Heuristic evaluation AiBA warning to parents 92
Figure 56 All the expert rate the risk of online grooming as very high or high, they also rate the usefulness of the AiBA app as high or very high 93

2 List of Tables

Table 1 The EU Kids Online: Risks relating to children's internet use 22
Table 2 Overview mediation techniques 62
Table 3 a larger proportion of boys use Discord 74
Table 4 The most popular apps that the children use are by far Tiktok and Snapchat 74

3 List of Abbreviations (or Symbols)

NTNU	Norges Teknisk- Naturvitenskapelige Universitet Norwegian University of Science and Technology
AiBA	Author Input Behavioral Analysis
KRIPOS	Norway's National Criminal Investigation Service
NCIS	Norway's National Criminal Investigation Service
NKVTS	Norwegian centre for violence and traumatic stress studies
WHO	World Health Organisation
IWF	Internet Watch Foundation
OCSEA	Online child sexual exploitation and abuse
NSD	Norwegian centre for research data
UCD	User-centered design

1 Introduction

1.1 Introduction to the topic

Norway is one of the most digitised countries globally, and social media have become an integrated feature in the lives of most Norwegians, including children and young people. The internet provides access to websites and social platforms

central to children and young people's communication, knowledge exchange, and social arena (Aanerød, L. and Mossige, S, 2018). "Everything" happens online for children and young people today. Here they play games with each other, get invited to soccer practice through Spond, get to know new people on Instagram, hand in school assignments on Microsoft Teams, Snapchat with their friends and parents, watch movies on Netflix, and watch influencers on YouTube. The Internet is integrated into young people's lives and no longer something we can consider separate from children's 'real' lives or society in general. According to the "Barn og medier-undersøkelsen" from 2020, 97 percent of 9- to 18-year-olds have their own mobile phone. Eighty-seven percent of those aged 9-10 have their own phone – and at ages 13–14, practically all children own a mobile phone. In addition, 90 percent of 9-18-year-olds are on one or more social media. Half of the Norwegian nine-year-olds use social media, and 65 percent of teens (Medietilsynet, 2020).

The development of the internet and social media combined with children and young people's access to PC, tablet, and other mobile devices offers excellent opportunities for people to establish sexualised contact with children (Kripos, 2019b). The availability and opportunities to contact children are plentiful in today's society. "Barn og medier-undersøkelsen" from 2020 shows, for example, that 29 percent of children and young people aged 13–18 over the preceding year had received sexual comments online that they experienced as unpleasant or threatening. As many as two percent received sexual comments once or several times a week (Medietilsynet, 2020).

A recent Norwegian Broadcasting Corporation (NRK) article shows that more and more people are convicted of online child abuse. In 2015, NRK found 165 verdicts dealing with sexual offences against children on the internet. In 2019, the number had risen to 244. This is an increase of 48 per cent over five years (Hagen, 2020). Internationally, the World Health Organisation (WHO) defines sexual abuse towards children as one of the worlds significant public health problem and a grave violation of human rights ('WHO | Responding to children and adolescents who have been sexually abused', 2019).

Research figures from the Internet Watch Foundation (IWF), an organisation in the UK that removes child abuse imagery from the internet, indicate that girls aged between 11 and 13 are more at risk of being groomed by sexual predators on the internet than ever before. While young boys are also subjected to this form of abuse, the IWF sees an exponential increase in "self-generated" child sexual abuse content, created using webcams or smartphones and then shared online via a growing number of platforms. In some cases, children are groomed, deceived or extorted into producing and sharing a sexual image or video of themselves. The photos and videos predominantly involve girls aged 11 to 13 (Internet Watch Foundation, 2021). The predators groom, bully and coerce their victims into filming their sexual abuse on internet-enabled devices, often in the child's bedrooms in their family homes. The images and videos of this abuse are then shared widely online (IWF, 2021). Never before has it been so easy for offenders to come into contact with children over the internet. At the same time, police, policymakers and legal practitioners are struggling to keep up with technological developments within this area. The past few years have seen a dramatic increase in the number of reported cases of various forms of online child sexual exploitation and abuse (OCSEA) related offences perpetrated within Norway (Sylwander, Vervik and Greijer, 2021).

1.2 The corona pandemic

The global impact of the corona pandemic means people are spending more time online. This includes both children and adults. Adults working remotely are less able to spend time with their children, who are allowed greater unsupervised internet access. As a result, children are, among other things, more exposed to offenders through online gaming and the use of chat apps (Europol, no date).

This means that abusers are more online than before. "With more people spending more time online, predators are finding new ways to contact and manipulate children who are, in many cases, a captive audience at home with their devices. Lockdown has made this worse." - Internet Watch Foundation CEO Susie Hargreaves (Oppenheim, 2021). Children are at increased risk of being groomed online during the pandemic as they spend more time online and out of school. Children's everyday lives are already heavily digitalised. During the Corona pandemic, it may have been hyper digitised to meet adolescents' need for social contact and participate in compulsory school activities. This may have enabled online abuse of various kinds (Hafstad and Augusti, 2020). A nationwide survey of violence, abuse, and mental health among young people in Norway in the spring of 2020 conducted by The Norwegian Centre for Violence and Traumatic Stress Studies (NKVTS) shows that every sixth young person experienced at least one form of violence or abuse when the school was closed. Several experienced online sexual exploitation for the first time. Girls were much more vulnerable than boys (Hafstad and Augusti, 2020).

1.3 Keywords

Online sexual exploitation, online abuse, grooming, human factors, chat safety.

1.4 Topics covered

This thesis will be incorporated in the Author Input Behavioral Analysis (AiBA) thesis supervised by Patrick Bours. The AiBA project's overall goal is to protect children online from sexual predators, grooming, and cyberbullying through identifying and preventing grooming in online chat rooms. It aims at identifying fake profiles in chat applications through biometric, text, and media analysis. This study is intended to acquire insight into the knowledge of grooming and online sexual predators. Through this, the aim is to develop a way to warn children in live chat conversations about potential danger. Looking at how to warn parents about potential risks in online environments is an integral part of this thesis.

To investigate these themes Interaction design and user-centered design methods play an important role. To conduct a thorough user research this thesis makes extensive use of established design methods such as semi-structured interviews, surveys and focus groups. The gathered data is in turn evaluated by additional design methods such as thematic analysis, affinity diagramming, gamestorming and expert evaluation. Warning design is the overall theme that leads through the thesis, from researching information needs to the creation of a prototype. The thesis covers theories from several fields such as IT security, interaction design, and human factors. It can therefore be described as an interdisciplinary thesis that promotes cooperation and contributes to each area.

1.5 Problem Description

The AiBA (Author input Behavioral Analysis) project aims to protect children online from sexual predators by identifying and preventing grooming in online chat rooms. By being a part of this project, the overall goal is to protect children from sexual predators, grooming and cyber bullying. Making children and parents aware of sexual predators online and in chats will increase the possibility of them being more careful and knowing the right steps to take to get out of the situation. The design of the warning will be adapted to each recipient as kids will receive different, more reassuring information including steps to take to get out of the situation. While parents will receive a more neutral warning and then practical information on the advised next steps to take. In addition a suggestion for an easy user friendly set up of the AiBA app will be introduced where the parents are the target audience. The thesis will present a design suggestion for the warning aimed at children, the warning notification aimed at parents as well as a suggested starting point for the AiBA app.

1.6 Significance, Motivation, and Benefits

Teaching children and young people about healthy relationships and how to stay safe online can help prevent sexual exploitation. Children and young people who are not informed about the possible dangers of establishing contact with others online have an increased risk of experiencing negative aspects of such activity (Fleming *et al.*, 2006). According to The National Criminal Investigation Service (NCIS) in Norway, there is a need for research-based knowledge and appropriate measures on this topic (Kripos, 2019b). This thesis aims to provide a comprehensive understanding of online grooming and how to protect children from online grooming risks.

1.7 Research question and hypothesis

The thesis will work towards answering the following research question:

Can we design a way to warn children in live chat room conversations that they are/might be talking to a sexual predator?

To answer this question, several sub-questions need to be addressed:

- How do we communicate risk in a chat conversation and influence kids' behaviour in real-time
    - How do we inform the child about the risk profile in a chat environment?
    - How can we inform the child about the sexual predator's suspicious behaviour?
    - How to point to particular parts of the conversation that are suspicious.
- How can we help the parents (or guardians) monitor and keep their children safe from online predators?
- How can design notifications that inform the parents (or guardians) about a potential grooming situation?

The hypothesis is that if we alert and advise the children in a chat that they might be talking to a sexual predator, it will enable them to, depending on their age, either notify a trusted adult or take the necessary steps to stop, block and/or report the incident.

1.8 Terms and phrases relating to child sexual abuse

In international research, various terms are used, such as "online sexual victimisation", "online sexual solicitation", "online sexual harassment", and "online sexual exploitation". The most commonly used term is "online sexual exploitation". The term is used regardless of whether the activity is desired or not when children are involved (Aanerød, L. and Mossige, S, 2018).

The term online sexual exploitation of children will be used about the sexual abuse of children that takes place online. It can be illegal photo sharing, criminal chatting, or grooming via the internet. This research thesis focuses primarily on how to prevent online grooming in chat rooms.

There is no agreed definition of online sexual exploitation in international law. For the purposes of this document, online child abuse is defined as an umbrella term covering: Use of the internet, mobile phone, or other forms of information and communications technology (ICT) to bully, threaten, harass, groom, sexually abuse, or sexually exploit a child. Child sexual exploitation is a form of child sexual abuse.

Online sexual exploitation of children on the Internet can be divided into two main types:

1. Child lure, called "grooming". The child sexual abuser uses the internet to contact children to exploit them sexually.
2. Download abuse material. The abusers provide pictures and videos that show the sexual abuse of children. Some share them further.

In Table 1**,** there is an overview of how EU kids online have classified the various types of online risks. EU Kids Online is an international research network. It seeks to enhance knowledge of European children's online opportunities, threats, and safety (*EU Kids Online*, no date).

	Content Child as receiver	Contact Child as a participant (adult-initiated activity)	Conduct Child as actor (perpetrator / victim)
Aggressive	Violent / gory content	Harassment, stalking	Bullying, hostile peer activity
Sexual	Pornographic content	Grooming, sexual abuse on meeting strangers	Sexual harassment, “sexting.”

Values	Racist / Hateful	Ideological persuasion	Potentially harmful user-generated content
Commercial	Embedded marketing	Personal data misuse	Gambling, copyright infringement

Table 1 The EU Kids Online: Risks relating to children's internet use

There is no established definition of the term online abuse in Norway. The Norwegian police and Kripos use the formal term "Internet-related sexual exploitation of children" for criminal acts via the Internet that involve children. In this thesis, we use the term online abuse for practical purposes. The terms 'child sexual abuser', 'child sexual offender', or 'perpetrator of child sexual abuse are used to reflect the crimes committed more accurately, no matter what the child's age (Aanerød, L. and Mossige, S, 2018). In this thesis, the term "sexual predator" describes the adult who initiates and performs the grooming and sexual abuse directed at a child.

2 Background

2.1 The AiBA Project

The AiBA (Author input Behavioural Analysis) project aims to protect children online from sexual predators by identifying and preventing grooming in online chat rooms. This is done by using machine learning through keystroke dynamics and stylometry to detect sexual predators online. It is real-time, continuous, multimodal detection of sexual predators online. By observing a person's behaviour in chat rooms, online messaging forums, or social media, AiBA can determine the correctness of the user's profile. By analysis of the conversation, it detects if cyber grooming or harassment is taking place. How we write a text is a biometric characteristic, it is unique to each of us. By looking at how a person types on a keyboard, researchers can identify, for example, the gender, age, and mood of a person. AiBA results from several years of research conducted at the Norwegian Biometric Laboratory at the Department of Information Security and Communication Technology at the Norwegian University of Science and Technology (NTNU). The project started as a collaboration between Patrick Bours, professor of biometrics and information security, and Dorothee Beermann, professor of linguistics at NTNU. "The way you type reveals you. We measure when a key is pressed and comes up again and how long the key is down. In addition to how long it takes from one key goes down to the next", says Bours in an interview with NRK (Ness, 2018). He also states that "- With the help of artificial intelligence, computers can find patterns. This means that we can distinguish between a text written, for example, by a 14-year-old and a 32-year-old". AiBA can be applied in chat rooms, on the user's device, or to analyse large data sets in criminal investigations.

AiBA continuously monitors the typing rhythm behaviour and the content of conversations to detect false gender and age profile information (Figure 1). If AiBA detects potential cyber grooming, the dialogue will be red-flagged for moderators and subject to further investigation. This preselection will save resources and allow moderators to focus on the conversations that matter (NTNU, no date).

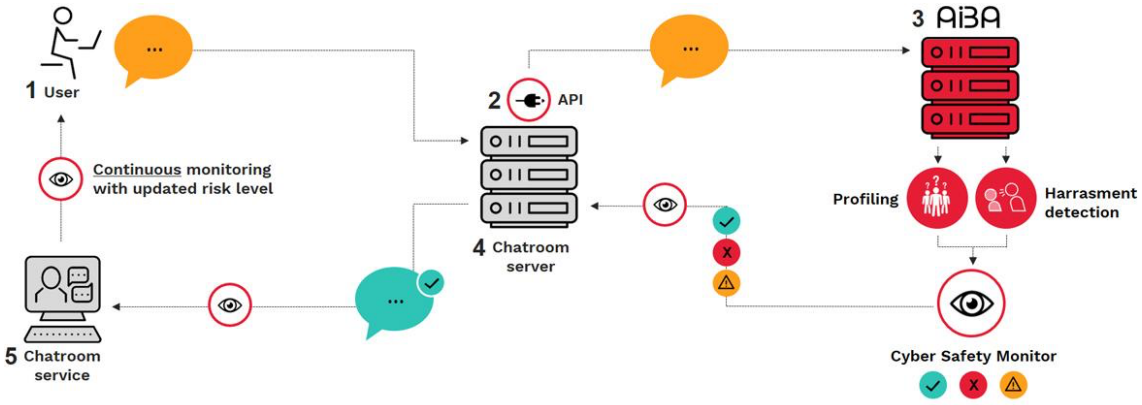


Figure 1 AiBA system structure (Source: https://AiBA.ai/)

It is envisioned that the algorithms will either be built into platforms and applications used by children, such as gaming platforms like Roblox, MovieStarPlanet, Discord or social media like Snapchat and Instagram, or will act as a standalone application that retrieves data from the chats.

2.2 Children and social media

In Norway, we have a law (the Privacy Information Act) that sets a 13-year limit for the use of social media. This means that it is not allowed to collect and use personal information for children under 13 years, but the law states that parents are allowed to give consent. Parents can therefore give children under the age of 13 permission to use social media. At the same time, Tiktok, Snapchat and Instagram and many other popular social media have a 13-year age limit, which means that a child that is younger than 13 must lie about their age when creating a profile (ReddBarna, 2020b).

A European study from 2020, published by the EU Kids Online network (Smahel *et al.*, 2020), states that children in Norway spend more time on the Internet than other European children, 3.6 hours compared with 2.8 hours being the average. This is supported by the "Children and Media 2020" survey published by the Norwegian Media Authority (Medietilsynet). This is a survey of 9–18-year-olds' digital media habits. Young people are spending more and more of their time on the internet. By the age of ten, almost all children have access to a mobile phone. Ninety percent of children at this age have their own smartphone. Nine out of ten children and young people aged 9 to 18 use one or more social media, and the proportion increases with age. From the age of 12 for girls and 13 for boys, just about everyone uses social media (Medietilsynet, 2020). In the age group 9–15 years, the average is two hours every day. The most popular apps are TikTok (previously Musical.ly) and Snapchat (Medietilsynet, 2020). Many children want to use social media even though they might be younger than the recommended age limit for the service, and they must have approval from their parents to establish a profile and

share personal data (Medietilsynet, no date). Furthermore, several websites, social media, and online games are designed for children and frequented by children and adults who induce children into sexual situations. For example, MovieStarPlanet is intended for ages 8-14.

Increased and more flexible access to the Internet also means that children and young people can now conduct their activity on the Internet more "under the radar" of their adult caregivers. While previously there was one PC for sharing stationed in the living room, the young people can now operate their smartphone alone and at all hours of the day (ReddBarna, 2020a).

Over the past decade, fewer and fewer young people spent most of their time out with friends. While four out of ten middle school students were out with friends at least two evenings a week at the beginning of the decade, that applies to three out of ten in 2018 (Bakken, 2019). Children and young people are more at home than before but have a lot of contact with each other on social media. Many spend a lot of their free time on digital activities. The proportion who spend a lot of time on digital screen activities has increased markedly over time. Since 2015, the ratio of those who use at least three hours in front of a screen has increased by between seven and thirteen percentage points. The increase is most significant among girls at the lower secondary level. Much of the increase in screen use is due to more and more people spending a lot of time on social media (Bakken, 2019).

2.3 Grooming

The word grooming has long been associated with child sexual abuse and has gained significant popularity in the last two decades (Burgess and Hartman, 2018). Many articles suggest definitions to describe the term, and there is no lack of professional literature on the concept of grooming. Over the years, numerous articles and descriptions have been proposed (Craven, Brown and Gilchrist, 2006).

The Oxford dictionary defines grooming as “the action by a paedophile of preparing a child for a meeting, especially via an internet chat room, intending to commit a sexual offence” (*GROOMING*, no date).

The concept and use of the term grooming gradually emerged during the 1980s with the growing recognition of cases perpetrated by extrafamilial acquaintance offenders (i.e., sexual exploitation of children) (Lanning, 2018). Supervisory Special Agent Ken Lanning from the Federal Bureau of Investigation (FBI) used the terms grooming and seduction interchangeably. However, he might not want to take credit for originating the term grooming (Burgess and Hartman, 2018) credit the term to him. Lanning defines

grooming/seduction as using nonviolent techniques by one person to gain sexual access to and control over potential and actual child victims. The grooming or seduction process usually consists of identifying preferred or acceptable child targets, gathering information about interests and vulnerabilities, gaining access (i.e., sports, religion, education, online computer), filling emotional and physical needs, lowering inhibitions, and gaining and maintaining control (i.e., bonding, competition, challenges, peer pressure, sympathy) (Lanning, 2010).

Following a review of the literature, (Craven, Brown and Gilchrist, 2006) proposed the following definition: *grooming is a process where an individual prepares the child and their environment for abuse to take place, including gaining access to the child, creating compliance and trust, and ensuring secrecy to avoid disclosure.*

Grooming can be difficult to identify and define, especially Internet sexual grooming, as it incorporates various behaviours and processes and can differ significantly in duration (Williams, Elliott and Beech, 2013). However, there has yet to be a universally accepted model for this process, and, as a consequence, there is no clear understanding of which behaviours constitute sexual grooming (Winters, Jeglic and Kaylor, 2020). Their research proposed a comprehensive model of the in-person sexual grooming process that is outlined in these five stages:

1. Victim selection
2. Gaining access and isolating a child
3. Trust development
4. Desensitisation to sexual content and physical contact
5. Maintenance following the abuse

2.4 Online sexual grooming

Online abuse, or digital violence, is threats, harassment, bullying, financial exploitation, and sexual abuse on the internet. These can be criminal acts. Online abuse is not a separate form of abuse but an arena where abuse can take place. Offensive behaviour online can take place in several different ways. It can, for example, start with a conversation on a social network or via SMS and go from linguistic harassment to sexual abuse (Bufdir, 2019). The purpose of this thesis is to describe and examine the grooming process that happens online.

An online predator will want to create a world where the child experiences that it is safe, you are friends; you can be in a relationship. Kripos states that they have often seen perpetrators operate with several identities that reinforce each other. For the child, this is experienced as different people. It can be difficult for the child to identify who is

dangerous when everyone seemingly appears to be children (Kripos, 2019a). The police in Norway are experiencing an increase in the number of online sexual abuse of children cases. The content of the cases is getting rougher. Seemingly unobtrusive Norwegians, without any other criminal behaviour, engage in online sexual abuse (Aanerød, L. and Mossige, S, 2018). Research shows a large increase in the number of tips reported to the NCIS about criminal online-related sexual activity in Norway. Sexual chat between children and adults and between adults makes up 1/3 of the tips. It is mainly men who commit online abuse, regardless of age (Aanerød, L. and Mossige, S, 2018). Adults with a sexual interest in children will always seek out the places where children are. However, these may be services made for children (Kripos, 2019a).

In 2016 Operation "Darkroom" was launched. Many people have since been charged and convicted in this large abuse case, including rape, human trafficking, production, and sharing of images of abuse of children. The procedure for getting in touch with the children, and eventually getting pictures and videos and perhaps finally also committing physical abuse often start with seemingly innocent inquiries. - "*They initiate dialogue with the children, give them many compliments, and manipulate and entice the children to send pictures and videos of themselves naked or where they masturbate*", says police attorney Janne Ringset Heltne (Otterlei, 2016). It also emerged that some of the perpetrators have also had their online accounts where they pretend to be children. Heltne tells NRK a "*frighteningly high*" number of people who participate in the hidden abuse forums. - "*It has scared us when we see how widespread this is*", she says (Otterlei, 2016).

Children rarely report online sexual abuse because they feel ashamed and partly to blame for what has happened. This is confirmed in a case written by NRK, where they reviewed 15 online abuse convictions that have been reported in the media over the past five years. The victims, all of whom are children under the age of 16, have all been pressured into taking nude photos and threatened to perform sexual acts on themselves. They never met their abuser physically, and there are hundreds of victims in the verdicts. Some of them recur in several cases. One of them is "Thea". Her story starts with the mobile app Kik. The app can be used to chat and send pictures to friends and strangers. In 2015, Thea, then 13 years old, talked to a person who used a girl's name. Over several days they developed a relationship, and one day Thea was asked to send a naked photo of herself, which she did. Thea was subsequently pressured to send more and more. The images would later end up on a Russian website with abusive material. The girl Thea thought she was chatting with turned out to be a 40-year-old man in a different part of the country. He was convicted of online abuse against several underage girls. The girls he was interested in were all girls who have not yet reached puberty. For a long

time, Thea felt ashamed and that what had happened was only her fault (Engebretsen, 2020). Younger children may believe they did something "wrong" or "bad" for getting into a grooming situation and are afraid of getting into trouble. Older children may be more ashamed and embarrassed. Some victims not only do not disclose what happened, but they also often vehemently deny it happened when confronted (Lanning, 2010). Many children carry an extra shame when they think they are to blame for what has happened, says Psychologist Svein Øverland. For many years he has worked with young people who have been sexually abused (Engebretsen, 2020). Research indicates that the knowledge that the abuse material has been shared involves a sizable additional burden, and many say that they feel that the abuse never ends (Kripos, 2019). Many of the victims do not even know that they have been offended in a case and think they have talked to someone their age. Children and adolescents explore their sexuality and sometimes do so with an adult who lies to them (Kripos, 2019a).

When cases like these are not reported to the police it allows the abuser to continue for long periods and get many victims. This is a challenge for the police today and has previously been identified as a challenge (Mossige and Stefansen, 2007). So how can there be hundreds of victims in a case? Superintendent of Police Bjørn-Erik Ludvigsen believes that many children do not say anything because they are afraid of losing privileges, that their parents will take away their mobile phones. Then they will be cut off from their whole lives. Then many feel that it is better not to say anything (Kripos, 2019a).

We do not know how many Norwegian children and young people are exposed to sexual abuse over the internet, and there is little Norwegian updated research on the topic. According to Redd Barna's report "Internett er et stort mørkt rom...» from 2020, there is reason to believe that children and adolescents living in child welfare institutions are particularly vulnerable to such offences (ReddBarna, 2020a). In the NKVTS report, being a child in a low-income family or where the parents had psychosocial difficulties constituted a significantly increased chance of online abuse. In addition, girls were 3.5 times more likely to be sexually abused online than boys (Hafstad and Augusti, 2020). Both research and Kripos' experiences indicate that it is often the extra vulnerable children who are abused. At the same time, experienced investigators emphasise that there are also many resourceful children among the victims and that "anyone" can be exposed (Kripos, 2019b).

In recent years, the police in Norway have investigated several cases in which the perpetrator has succeeded in establishing such contact, in some cases with several hundred children. Meet "Stian", he is serving time in prison for the third time because he has sexually abused children. Under a false name, Stian has contacted children on

Snapchat and made them perform sexual acts with themselves. He has had them send him pictures and videos of it. He has invited some of them, children down to the age of 13, to his home to exploit them sexually. Short prison stays did not stop him. The data from NRK's investigations show that Stian is one of 1798 people who have been convicted in Norwegian district courts and courts of appeal during 2015 through 2019. Over 2,300 named children have been involved as victims in these criminal cases. The number of unidentified children from photos and videos is far higher. Of 1798 convicted, NRK found that 195 of the men had been convicted once or several times before for similar offences (Kringstad, 2020).

The internet provides anonymity and a broad reach to identify victims (Kripos, 2019b). Today, young people are more accessible to sexual predators through technology (Whittle *et al.*, 2013). As shown in Stian's case mentioned earlier, people with a sexual interest in children want to make friends with and manipulate children online to win the children's trust, isolate them and get them to do things that satisfy their desires. The person gives the child positive attention or promises other benefits. The goal is to become friends with the child, which the adult can later sexually exploit. The perpetrators often make contact in public chat rooms. Then they try to get the kids over to online services where they can communicate one-on-one. Services such as Snapchat, Skype, and Instagram are repeated in many online abuse cases. Some sexual predators use a fake profile to initiate contact with children by pretending to be a child themselves. Grooming techniques vary and may involve manipulation, flattery, and sexualisation (Whittle et al. 2013). There is no doubt that some of the people who establish sexual contact with children on the internet also desire to commit physical abuse. In many child sexual abuse cases, the abuse is preceded by sexual grooming (Pollack and MacIver, 2015). In recent years, many have been convicted not only of seducing or forcing children to produce sexual material of their own but also of initiating and then conducting physical encounters with them to commit abuse (Kripos, 2019b).

An example of this is a case from the UK which has received a lot of publicity, and it is the case of Breck Bednar, a 14-year-old schoolboy who was lured to his death after being groomed online by Lewis Daynes. Lewis targeted Breck after befriending him while gaming. The predator's lies and false identity allowed him to build a close controlling relationship with Breck, who admired him and regarded him as a friend he could trust. Despite the efforts of Breck's friends and family, the predator, Lewis, continued to manipulate Breck and eventually persuaded him to meet him in private. Breck ended up being killed in his groomer's apartment. Lewis Daynes was later convicted of murder with sexual and sadistic intent. Leicestershire police have made an informative video about this case called "Breck's Last Game" (*Breck's Last Game*, 2019). The film was made to

raise awareness of online grooming and carries an important message – do you really know who your online friends are?

2.5 Children's awareness and perceptions of online risks

The cognitive maturity of young children poses a significant challenge for coping with online risks (Livingstone and Haddon, 2009). While the internet offers excellent opportunities for learning, communication, creativity, and entertainment, it also opens up certain risks to vulnerable users such as children. A study that explored relationships among adolescents' perceptions of chat-site safety and risky online behaviours found that teens with more social discomfort and those who thought it was safe to reveal personal information and trust chat-site "friends" were more likely to take risks. As time spent in chat sites increased, so did risk-taking behaviours (McCarty *et al.*, 2011).

According to the report "Digital Natives or Naïve Experts? Exploring how Norwegian children (aged 9-15) understand the Internet ", children lack a holistic understanding of the risks and opportunities that may be associated with their actions. For instance, they understand that they should not send photos of themselves to strangers on request. In some instances, they do not consider it problematic to upload videos of themselves to social networks or interact with strangers in gaming communities (Ni Bhroin and Rehder, 2018). These results are also consistent with previous research by (Ey and Glenn Cupit, 2011), who examined five to eight-year-old children's understanding of dangers associated with the Internet. The study showed that although the children identified several risk categories when presented with potentially dangerous Internet interactions, almost half could not identify the associated risks. For instance, a considerable number of children did not consider it dangerous to meet with people they only know from the Internet, and a few children were unsure, supporting claims that children are unable to recognize such dangers (Ey and Glenn Cupit, 2011).

It may seem as if the internet gives a false sense of belonging to a private sphere. Those who communicate with each other online therefore tend to include each other in this private sphere and thus have fewer inhibitions against disclosing intimate material (Schouten, Valkenburg and Peter, 2007). Many children and young people have different boundaries for what they do online than what they would do in the real world. They feel more anonymous online, and the setting makes it easier to talk about good and bad feelings. As early as 2007, Schouten?, Valkenburg & Peter found that one in three young people prefers online communication over face-to-face communication when thematising intimate matters such as infatuation, sexuality, shame, and embarrassment. In addition, many want to be recognised and get attention from others. This makes children and young people vulnerable to people who want to exploit them (Kripos, no date). Data from

the European study "EU Kids Online 2020" showed that the majority of the children in most countries agreed that they at least sometimes or more often find it easier to be themselves online than when they are with people face-to-face. This seemed to be an increasing trend already in 2010. At that time half of European 11-16-year-olds stated that they found it easier to be themselves online than offline (Livingstone and Ólafsson, 2011). The preference for online communication might be positive and negative and can become an opportunity or a risk. Furthermore, according to EU Kids Online 2020, "*Most Norwegian children experience the internet as a positive social environment and feel safe online*". In addition, Norwegian children are understood to have a high risk of encountering sexual messages – 32% of those aged 11 to 17 have received such messages. Between 8% (Italy) and 39% (Flanders) of the children aged 12-16 have received sexual messages in the past year. In all of the countries, more girls than boys are upset by seeing sexual images. Evidence suggests most children are unable to determine the age and gender of the people they are talking to online, so they tend to be more easily deceived (Badillo-Urquiola *et al.*, 2019). Having contact on the internet with someone you do not know from the outside world is considered risky behaviour. Many children do this, and being in contact with someone unknown on the internet is a common experience among children, and 57% of children in Norway have done this. There is also a clear age pattern as more older children had contact with unknown people online than younger ones, and more of the older children also met them face-to-face (Smahel *et al.*, 2020).

Teaching children how to use the internet safely and how to make informed decisions is an integral part of digital education that children should receive. It is crucial to ensure that those who experience risk get the help and guidance they need without drawing away from the internet's positive experiences. In most countries, over 80% of children receive advice on safe internet use from parents, friends, or teachers (Smahel *et al.*, 2020). It does not say anything about the quality of the advice or what type of topics are covered.

2.6 Parental mediation

Caring about children's safety is at the cornerstone of parenting. Children's lives are increasingly interwoven with digital friends, settings and phenomena. The continuous evolution of technology creates ever-changing online and digital scenarios. Parents, guardians and others responsible for

supervising children play an essential role in shaping children's media use, keeping certain possibilities open for children to play, learn and socialise, while limiting others (Zaman and Nouwen, 2016).

Overall, parental concern regarding their children's safety online is high, stimulating a fair range of practices designed to make internet use safer for their children (Livingstone and Haddon, 2009). Parental mediation of media involves parents' interactions with their children about media use (Coyne *et al.*, 2017). In literature, two broad mediation approaches are described. Enabling mediation encompasses parental practices that aim at enabling children's positive use of the internet. Restrictive mediation then aims to limit children's use of the internet (Smahel *et al.*, 2020).

According to the EU Kids Online report of 2009 (Livingstone and Haddon, 2009), parental mediation is lower in countries where children's internet use is high. Many teens express resentment around their parents' rules, restrictions, and, in many cases, surveillance practices, feeling that they reflect parents' misunderstanding of how and why they use technology (Davis, Dinhopl and Hiniker, 2019).

Research by (Wisniewski *et al.*, 2017) showed that most teens had little or no communication with their parents regarding their online risk experiences. Parents and teens shared very different perceptions and reactions when risks were reported. This different point of view indicated why communication was so poor. On a positive note, parents were more likely to know about higher-risk events, especially ones related to online harassment and sexual solicitation. During instances where parents actively mediated the teen's online experiences, they were often pivotal in helping their teens fix the situation.

Recently digital tools have emerged where parents or guardians can monitor or track children and teen's digital media use through "parental controls software". The common denominator is ways to restrict time, content, and activity of what the child can do or see online. Mobile applications developed to promote online safety for children are underutilised and rely heavily on parental control features that monitor and restrict their child's mobile activities. To compromise on a solution that may meet both parents' desire to keep their children safe and teens' desire to uphold personal privacy, (Ghosh *et al.*, 2018) recommend that app designers create online safety apps that give parents helpful meta-level information regarding teens' mobile activities instead of full disclosure. Too much monitoring has the potential to undermine trust with the result that the child will not disclose negative experiences for fear of increased restrictions and loss of access to digital devices. Recent research by (McNally *et al.*, 2018) that included children in the design process found that the children preferred and designed controls that emphasised restriction over monitoring, taught risk coping, promoted parent-child communication, and automated interactions. Design research by (Badillo-Urquiola *et al.*, 2019) uncovered that children are aware of risks they may face online. They want to balance having control over situations they may encounter with guidance and assistance in choosing a

course of action. It also found that children want to learn about the potential dangers and how to mitigate their risk or address situations they encounter (Badillo-Urquiola *et al.*, 2019). The children in this study felt that an automated intelligent assistance feature should recommend specific actions the child should take, like blocking or telling a parent, in addition to identifying the potential risk.

Used wisely, technical mediation tools such as parental control apps can be great tools to assist parents in keeping their children safe online. It should not replace positive interaction and good conversation between parents and child. It is essential that the parents show an interest in their child's online activities and also make themselves familiar with the various platforms and arenas that their child is involved in. There is evidence that parental support and the creation of clear expectations are more likely to result in less problematic behaviour in adolescents than over-controlling or overprotective parenting, which negatively affects the child's development (Janssens *et al.*, 2015). Most Norwegian children speak to a friend (50%) (rather than a parent (34%) if they experience something negative online (Medietilsynet, 2020). This shows that the parents must be interested in their children's online activities or be left in the dark. This is also supported by a documentary from 2018, The Paedophile Next Door. Here Jonathan Taylor, a renowned Online Safety & Social media Awareness Consultant, states that "*Start with online safety at home. Letting parents know that whatever happens, wherever the child goes online, whatever device they use, however they are connected; be there with them. Spend time with your child to understand their world. Their real-world now is an online world"* (RealStories, 2018). When parents and children communicate well

with each other, they can come to a better understanding of online risky behaviour. Through education parents and teachers can help children build more resilience to cope with the harm and risks they may encounter online (Zaman and Nouwen, 2016).

2.7 Risk communication

Risk means that events can occur that have consequences for something that is of value to us humans. The consequences can be related to, for example, life and health, the environment, or economic values. There is always at least one outcome that is perceived as negative or undesirable (Aven, 2019a). Risks are not perceived the same way by everybody; it depends on age, education, and experience. Depending on how we communicate risk, we may prevent crises and help people lead good lives in a world full of potential dangers.

There are several definitions of risk communication. What many of them have in common is that risk communication is an interactive process between experts and the public. In

other words, it is about two-way communication. It is about risk assessments and perception of risk. An early definition is that risk communication includes all messages and interactions that bear on risk decisions (National Research Council (US), 1989). The society for risk analysis describes risk communication as the exchange and sharing of risk-related data, information, and knowledge between and among different groups, such as professionals, authorities, consumers, the media, and the general public (Aven, 2019b) (Society for Risk Analysis, 2018). WHO's description also says something about the purpose; Risk communication refers to the exchange of real-time information, advice, and opinions between experts and people facing threats to their health, economic or social well-being. The ultimate purpose of risk communication is to enable people at risk to make informed decisions to protect themselves and their loved ones (WHO, 2015).

To succeed in risk communication, it is essential to have a strategic approach and know your audience well. The complexities of communicating risk may increase when working with children and teenagers. Their understanding, preferences, and attitudes to risk may frequently change as they grow, develop, and mature. Their wishes, needs, and feelings may also need to be balanced with their parents' (Koussa, no date). For the parents, there are difficult trade-offs between giving children and young people freedom and the opportunity to participate and communicate and restricting that freedom to give them protection against dangers such as online sexual abuse. The goal must be to implement adequate safety measures without hindering a child's use of the internet. It is essential to alert children to risks they may encounter and help them develop safe and responsible behaviours when using technologies. The findings from a study from 2016 identified that children were aware that there are risks online; however, they were not wholly educated in identifying these risks and, as a result, did not take the required precautionary measures when entering the online world (Annansingh and Veli, 2016).

The literature in risk communication discusses several principles on how best to communicate risk, according to (Lundgren and McMakin, 2018). Two overarching principles are repeated for risk communication to work well:

1. The public must view the communicating organisation as credible and trustworthy
2. The public must be allowed to participate in risk management decisions
3. A third overriding principle is that actions, guidelines, and language must be congruent for risk communication to work.

Risk communication goals are to share information vital for saving a life, protecting the health, minimising harm to self and others, changing beliefs, and/or changing behaviour (Fischhoff, 2012).

This thesis will not be concerned with designing a strategy for risk communication about sexual predators on the web. This has already been designed and described in the thesis ”Risk Communication: Sexual Predators in Chat Environments” incorporated in the AiBA project (Raffel, 2020). The concept of risk communication has therefore only been mentioned briefly for the sake of completeness.

2.8 Warning design

In computer systems, we understand a warning as communication that alerts users to take immediate action to avoid a hazard (Bauer *et al.*, 2013). A warning message represents communication designed to prevent users from hurting themselves or others. Warning and design are closely connected because they are alternative mechanisms for controlling hazards and promoting safety (Green, 2013). In a mobile device alerts convey important information related to the state of your app or the device, and often request feedback. An alert consists of a title, an optional message, one or more buttons, and optional text fields for gathering input (Apple Inc, no date). In addition to colour and text a warning also often contains graphics or symbols. Graphical symbols are means of communication: they are used to convey complex concepts within a lesser space than a complete written sentence does (Womack, 2005). Safety symbols have been developed as an alternative means of communicating safety messages to both literate and illiterate populations (Lehto, 2000). Well-designed symbols can improve the usability of a system by increasing its intuitiveness, i.e., learnability; (Reddy *et al.*, 2020), memorability, and efficiency (Nielsen, 2010).

In the AIBA project, a warning will be sent once the system detects behavioural patterns that indicate grooming tactics. Warnings are part of people's daily lives. However, and similar to real-life situations, digital warnings are often ignored in the computer context. Today's web security warnings often rely on visual cues such as colour, e.g., red URL highlighting indicates a security risk. However, such cues often go unnoticed by users and, even when noticed, are ignored (Wilson, Maxwell and Just, 2017). In addition, security warnings that repeatedly convey the same message tend to be ignored, and this repetition eventually leads to habituation. The higher the number of stimuli present, the faster the habituation will occur. Changing the intensity or duration of the stimulation may result in a reoccurrence of the original response (Amran, Zaaba and Singh, 2018). Every warning should be designed to protect the user from a risk. This risk should be stated clearly, along with instructions for avoiding it and the consequences of not avoiding it. The warning should be displayed when the user can still take preventive action (Bauer, Bravo-Lillo and Cranor, 2013). Alerts disrupt the user experience and should only be used in important situations like confirming purchases and destructive actions (such as deletions), or notifying people about problems (Apple Inc, no date).

A well-designed warning message should communicate risk effectively and attract attention at the right time. For example, (Petelka, Zou and Schaub, 2019) showed that warning placement and forcing interaction with the warning improves warning adherence. This is more important for warning effectiveness than the method of activation. Also, people are more likely to behave consistently with a warning sign or label if they believe the danger is considerable (Lehto, 2000).

According to (ISMP, 2019) to be effective, a warnings must:

1. Reach their target audience
2. Capture the attention of recipients at the right time
3. Cause recipients to understand the risk, believe that the warning relates to them, and understand the actions they need to take
4. Lead the recipients to respond appropriately

Based on an overview of the empirical literature on warning guidelines and evaluation approaches (Wogalter, Conzola and Smith-Jackson, 2002) described a set of guidelines for warning design:

1. **Salience**. Getting noticed and attended to are the first requirements of an effective warning. The salience of a visual warning can be enhanced using:
    a. large bold print
    b. high contrast
    c. colour
    d. borders
    e. pictorial symbols
    f. Special effects like flashing lights
2. **Wording**. An effective warning consists of four message components:
    a. signal word to attract attention
    b. identification of the hazard,
    c. explanation of consequences if exposed to hazard,
    d. directives for avoiding the hazard.
3. **Layout and placement.** Presenting warning text as bullets in outline form is preferred to continuous flowing text.
4. **Pictorial symbols.** Including pictorial symbols in warnings increases their salience and likelihood of being noticed.
5. **Personal factors**. Personal factors include age, gender, cultural background, product or task familiarity and training, and individual differences.

(Bauer et al., 2013) further recommend guidelines that may help designers and developers create more effective cyber warnings. These guidelines were derived from

current literature on usable security and warnings research from Human Interface Guidelines (HIG) for Windows, macOS, and Linux operating systems. The researchers recommended the following six guidelines:

1. **Describe the risk comprehensively**: Warnings are meant to alert the user of impending risk to her information or her identity. Whenever a warning is used, the risk that motivates the usage of a warning should be identified and presented clearly.
2. **Be concise and accurate**: Warnings always interrupt the user. If too long, overly technical, inaccurate, or ambiguous, a warning will simply be discarded, and its purpose will be lost.
3. **Offer meaningful options**: Warnings should present understandable choices and enough information to decide between them.
4. **Present relevant contextual information**: In most contexts that require a warning to be shown, a computer or software system cannot decide on behalf of the user. Warnings should present relevant contextual information that allows the user to make an informed decision.
5. **Present relevant auditing informatio**n: In some contexts, actions have been performed in the past that may help a user understand the risks associated with the choice she needs to make. In such cases, relevant auditing information should be presented.
6. **Follow a consistent layou**t: Warnings should follow a commonly suggested layout based on the Human Interface Guidelines (HIG).

An investigation done by Wogalter et al., on the influence of warnings, signal words, and a signal icon on the perceived hazard of consumer products showed that the presence of a signal word increased perceived product hazard compared with its absence. Significant differences were noted between extreme terms (e.g., NOTE and DANGER) but not between terms usually recommended in warning design guidelines (e.g., CAUTION and WARNING) (Wogalter, Jarrard and Noel Simpson, 1994). The four most common signal words recommended for use by the American National Standards Institutes Z535 Standards on Safety Signs and Colors are DANGER, WARNING, CAUTION, and NOTICE (Wogalter, Conzola and Smith-Jackson, 2002). It corresponds to the international ISO 3864 standard (ISO (the International Organization for Standardization), 2016).

Studies have been conducted to examine warning design for adults, but there is little data to establish recommendations for children. A study involving the design and evaluation of a set of safety signs for younger children (i.e., aged between 5-10) showed that children could not understand the meanings of words such as “caution”. In addition, the children said that they often ignored signs that had a lot of written text, particularly

small text size. Large font sizes increased the salience of some of the text messages. Pictograms proved to be a highly effective method for communicating safety information to the children in the study. The children were more responsive to the images where children were depicted as having round faces, with big eyes and smiles (Waterson *et al.*, 2012). (Waterson and Monk, 2014) later evaluated the guidelines developed from this study. Their findings offered broad support for the guidelines and they developed some revisions. In addition to the original guidelines, they recommended avoiding the use of text in signs where possible. Where this is not possible, keep the language used in signage as simple as possible. Use examples of pictograms that primarily demonstrate 'good' (i.e., safe and correct) behaviour. Also, consider the use of characters that may be topical and popular with children (e.g., TV characters). Use bright colours to reinforce the safety message and take into account that some children suffer from colour vision deficiencies.

2.9 Design guidelines

Design guidelines are sets of recommendations on how to apply design principles to provide a positive user experience. Designers use such guidelines to judge how to adopt principles such as intuitiveness, learnability, efficiency, and consistency to create compelling designs and meet and exceed user needs (Interaction Design Foundation, no date). Design principles should help designers find ways to improve usability, influence perception, increase appeal, teach users and make effective design decisions in projects. To apply design principles effectively, you need a firm grasp of users' problems and a good eye for how users will accept your solutions (Lidwell, Holden and Butler, 2010). In user experience (UX) design and especially warning design, it is vital to minimise users' cognitive loads and decision-making time. Literature suggests that a user-centred approach that evaluates the end-user' perspectives is essential when designing effective warnings (Riley, 2014). Understanding the user's risk perception is a central aspect of designing effective warning messages. The design of the warning message should be:

- Consistent, keep words and actions consistent
- It should be displayed in proximity of the incident
- There should be a visual hierarchy
- Sufficient colour contrast and emphasis
- Have intuitive icons
- Make the main task apparent

2.9.1 Usability Heuristics

Known principles, usability heuristics, for what makes interfaces easy to use such as Jakob Nielsen's 10 general principles for interaction design. They are called "heuristics"

because they are broad rules of thumb and not specific usability guidelines (Nielsen, 2020). In a warning design it is important to inform the users when an error has occurred with an error message, red text or warning signs. In ideal composition would be a mix between the error message and visual treatments. The users should be informed using plain language what is wrong. The next step is to offer the users a solution, something they can click or tab right now to fix the problem. Furthermore it is important to help users recover from errors; such as providing an undo function. There should be a match between the system and the real world. This means that it should "speak the user's language". It is vital to avoid marketing jargon and complex language. If people don't understand the terms used, not only will they feel unsure and ignored, but many will be forced to go elsewhere to find explanations (Kaley, 2018). This is especially important to keep in mind when your users are children. It is essential that they understand the information that is presented and that the language is adapted to meet their needs. Another key element is that the solution should follow real-world conventions. This means that the information should appear in a natural and logical order. Users are often distracted from the task at hand, so preventing unconscious errors by offering suggestions, utilizing constraints, and being flexible can stop errors before they happen (Sherwin, no date). The interface should promote recognition by making objects, actions, and options available. The user should not have to remember information from one part of the dialogue to another. Instructions should be visible. This minimises the user work which is essential for a good user experience.

2.9.2 Universal and accessible design

To succeed with good solutions that everyone can use, universal design must be an obvious part of all development processes, whether it is about redesign or a new solution. Universal Design is the design and composition of an environment so that it can be accessed, understood, and used to the greatest extent possible by all people regardless of their age, size, ability or disability. It is designing for all users, rather than the typical or average user. Universal Design is inclusive of Accessibility, and not solely focused on Accessibility. Rather, Universal Design expands Accessibility's definition by including all persons, not only persons with disabilities (KUMC, 2021). Universal design of ICT is a legal requirement for both the public and private sector in Norway (*Intro til universell utforming*, no date). For digital solutions, the international standard WCAG 2.0 applies.

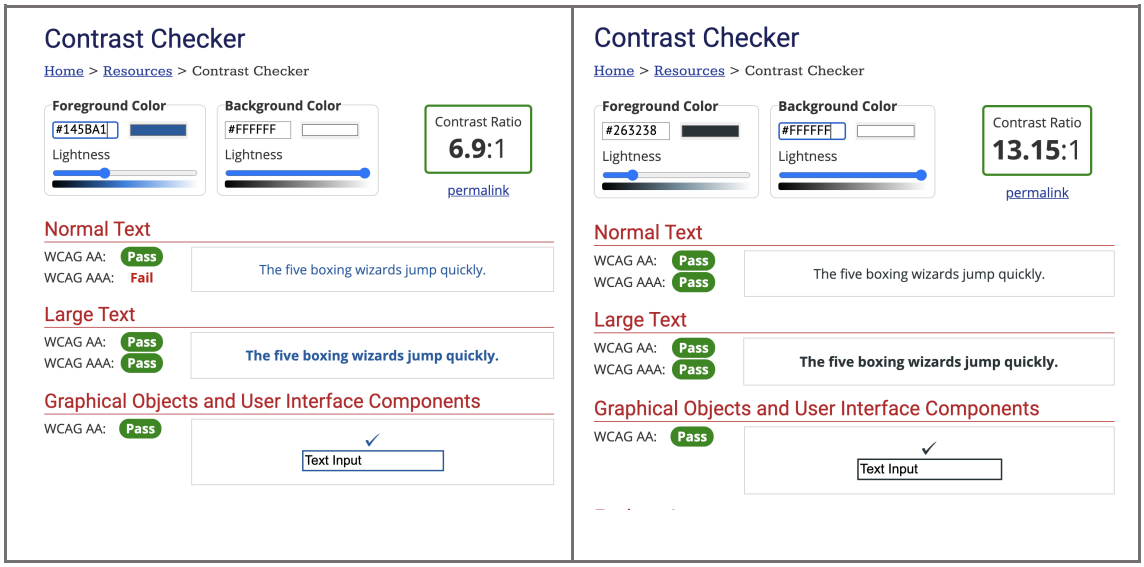
One example of this is; to ensure good readability, all text must have sufficient contrast to the background. This is important for all users, especially under demanding lighting conditions. WCAG 2.0 guidelines are categorized into three levels of conformance in order to meet the needs of different groups and different situations: A (lowest), AA (mid

range), and AAA (highest). To get an AAA rating you have to make sure all text has a contrast ratio of at least 7: 1 for normal text and 4.5:1 for large text. Large text is defined as 14 point (typically 18.66px) and bold or larger, or 18 point (typically 24px) or larger (W3C Web Accessibility Initiative (WAI), no date).

The industry standard guidelines for web content accessibility are organized around four principles: Perceivable, Operable, Understandable, and Robust (or POUR).

1. **Perceivable**; the users must be able to perceive the information being presented
2. **Operable**; users must be able to operate the interface
3. **Understandable**; users must be able to understand the information as well as the operation of the user interface
4. **Robust**; users must be able to access the content as technologies advance (as technologies and user agents evolve, the content should remain accessible) (*Introduction to Understanding WCAG 2.0*, no date)

To ensure sufficient contrast a contrast check was performed on the designs primary design colour and on the primary text colour.



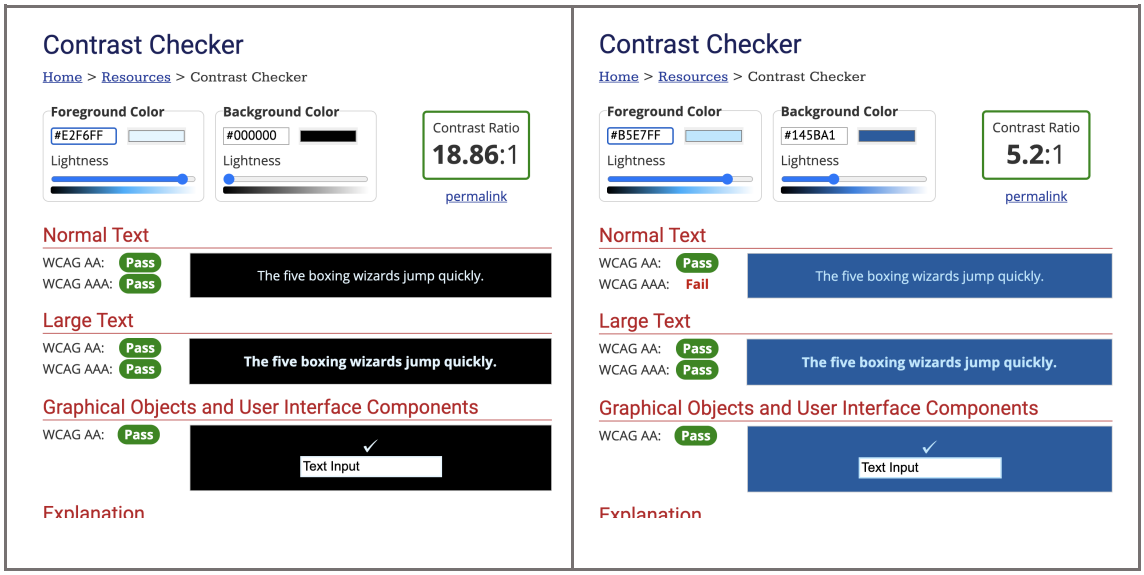


Figure 2 Colour contrast check on primary design and text colours.

2.9.3 Use of colour

Colour, it plays a vital role in design and in our everyday lives. Colour is a widespread communication tool, used for conveying information in design, architecture, traffic and education. It also represents an important design element and a tool to drive the user's decisions. The use of appropriate colour coding can help determine the intended conceptual meaning of warning signs and labels (Chapanis, 1994; Braun and Silver, 1995),(McDougald and Wogalter, 2014). The colour-in-context theory suggests a strong link between colour and psychological reasoning (Elliot and Maier, 2012). The decision-making process is a result of trust and different risk factors, which will ultimately help or hinder the entire process where the colour inputs play an essential role. Drivers will stop at red traffic lights as red suggests that there is danger ahead. In security, red is often used for alarms and warnings. When (Braun and Silver, 1995) examined the interaction of signal words and colours, they found that red conveyed the highest level of perceived hazard, followed by orange, black, green, and blue. A study that examined colour-concept associations among designers and non-designers with commonly used warning and operation concepts showed that both groups had the same colour associations for several of the concepts tested. Red-fire, red-hot, and red-danger were the strong stereotypical colour-concept associations for both groups (Ng and Chan, 2018). Colour coding methods consistently associate colours with particular levels of hazard. For example, red is used in all of the standards to represent the highest level of danger. Orange is often used to identify hazards, Yellow caution, Green first aid, and Blue sources of safety information (Lehto, 2000).

However, only a few studies have tried to understand whether red is the most efficient colour for computer warning messages when it comes to drawing the user’s attention. Research conducted by Silic and Cyr (2016) aimed at understanding how colour affects

users’ decision-making processes in warning banner messages suggests a strong association between arousal preference and colour preference. Meaning that users will be excited and aroused by certain colours and relaxed by others (Silic and Cyr, 2016). This study also found that the colour red has a high arousal effect. They also found that yellow and green are as powerful as red to prevent users from committing a potentially harmful action. Giving evidence that other colours, such as yellow and green, can have a high arousal effect on a user's attention.

Warning message designers should take into account the colour application and which colour best communicates to users. More precisely, colour seems to be an important design element that can be more or less efficient across different cultures (Silic *et al.*, 2017) This report also suggests that users are willing to pay more attention to warning messages if they are more informed about the hazards that are communicated through the warning message. (Egelman and Schechter, 2013) showed that distinguishing severe risks from other less-severe risks may aid in capturing the user's attention. (Wilson, Maxwell and Just, 2017) investigated the potential for using thermal feedback to improve comprehension of and adherence to security warnings. Their results indicate that people generally associate a cold temperature with a secure page and warm with an insecure page.

If colour is used to convey functionality or importance, it is a must to supplement with other methods to ensure that all users understand what you are conveying.Colours cannot be used as the only information carrier, because everyone perceives colours differently. By looking at previously done work on methods developed to change colours to make them more discriminable a colour palette for the warning levels was developed (Okabe and Ito, 2008). This will make the design more accessible for people with Colour Vision Deficiencies (CVD). Colours help us in guiding attention to different elements in a design. Many daily tasks can be problematic for people with CVDs. The tool “Adobe color” (Figure 3) was used to confirm that the colour scheme conforms to accessibility guidelines (Adobe, no date).

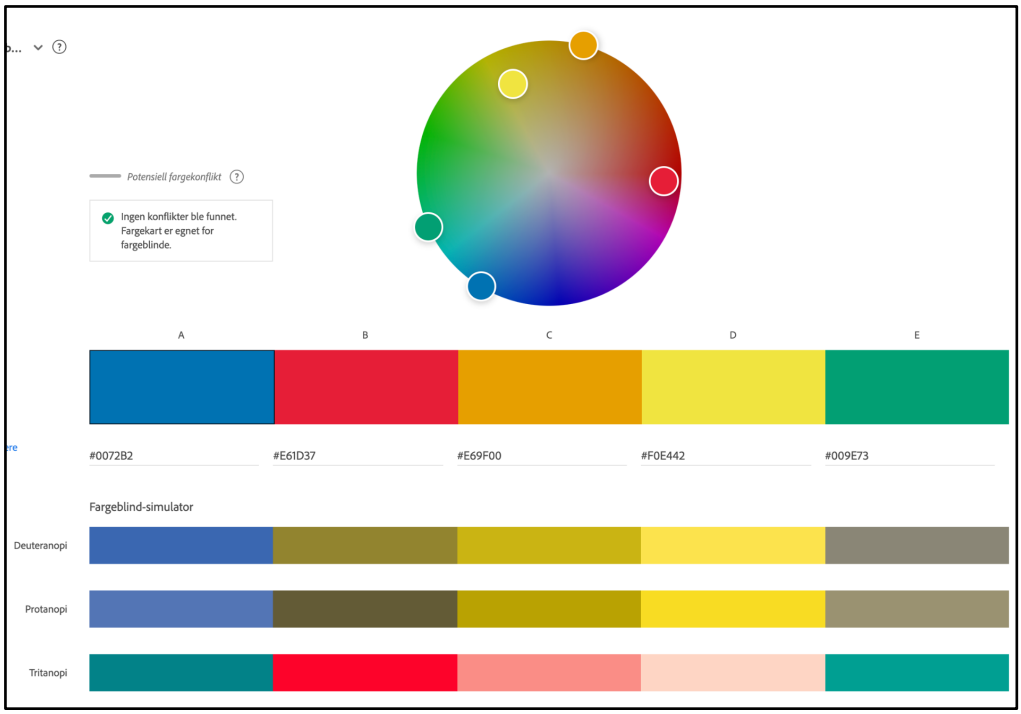


Figure 3 Adobe colour tool used to evaluate the colour scheme of the warning levels

2.9.4 Visualisation

When it comes to information visualisation, studies have shown that contrasting colours attract viewers' attention. If the contrasting colours are not related to a viewer's task, then their use creates a distraction (Few, 2013).

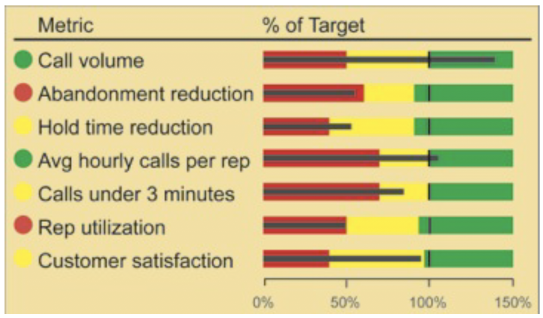


Figure 4

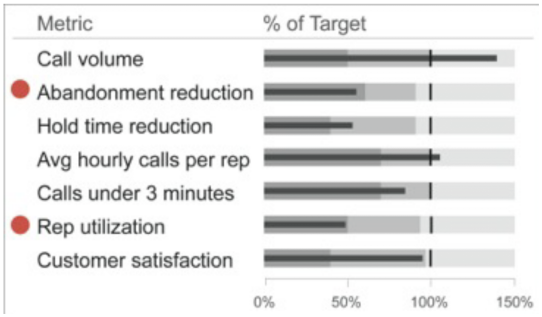


Figure 5

Too much colour is visually overwhelming; it tires our eyes. Also, if you use colour gratuitously, you undermine its ability to make things stand out. Notice how the red alerts stand out Figure 5 in contrast to the neutral greys and blacks that have been used elsewhere, rather than being lost in the meaninglessly colourful display to the left in Figure 4 (Few, 2013). Supporting the statement made by Stephen Few that "Colour should be used sparingly" and that "Too much colour undermines its potential" (Few, 2013).

2.10 Government prevention efforts

In 2006, Minister of Justice Knut Storberget appointed a task force to look more closely at preventing internet-related child abuse. This task force proposed several measures to combat Internet-related child abuse among them;

- More research should be initiated on internet-related abuse against children
- Competence development in the area of support, school, and health care
- Norwegian authorities must take the initiative for prevention and awareness campaigns aimed specifically at parents, children, and teachers, as well as other relevant audiences (Justisdepartementet, 2007)

More recently in connection with the celebration of Safer Internet Day in March 2021, the government announces coordination and strengthening of the public efforts to secure the digital lives of children and young people through a national strategy for safe digital upbringing. The Norwegian Media Authority will prepare the strategy in collaboration with other companies and actors who do essential work in the field. The Norwegian Media Authority will also be responsible for coordinating practical, user-oriented work in the field (Kulturdepartementet, 2021). A national strategy for safe digital upbringing will lead to good knowledge-based advice and measures to keep children and young people safe online. The government has allocated NOK 1 million for this work in 2021 (Medietilsynet, 2021).

3 9. Methodologies

This thesis is intended to acquire insight into the knowledge of grooming and online sexual predators. The target audience for this research was children in 5th to 9th grade and their parents. The aim is to develop a way to warn children in live conversations. They will then be able to make informed decisions regarding whether to continue the online chat conversation or not. The data collection for this thesis that encompassed the semi-structured interviews, the survey and focus groups were conducted with fellow master student Nakul Pathak. The remaining methods, design work and analysis was conducted singularly.

3.1 The research process

User-cantered design (UCD) is an iterative design process in which designers focus on the users and their needs in each phase of the design process. UCD calls for involving users throughout the design process via a variety of research and design techniques so as to create highly usable and accessible products for them. UCD is an iterative process where designers employ a mixture of investigative (e.g., surveys and interviews) and generative (e.g., brainstorming) methods and tools to develop an understanding of user needs This design process is about gaining a deep understanding of the users, who should be involved in the design process from the very beginning. The goal is to understand, rather than simply assume, what the problem is, discover key directions, requirements, and design opportunities, and understand the subject matter. It involves speaking to and spending time with people affected by the issues (Design Council, 2015).

For the past 15 years, the Double Diamond model of the design process has been the most used model to structure design projects. Recently the Design Council published a new model. What used to be called the Double Diamond is now a Framework For Innovation (see figure 3). Divided into four distinct phases: Discover, Define, Develop and Deliver, it maps how the design process passes from points where thinking and possibilities are as broad as possible to situations where they are deliberately narrowed down and focused on distinct objectives.

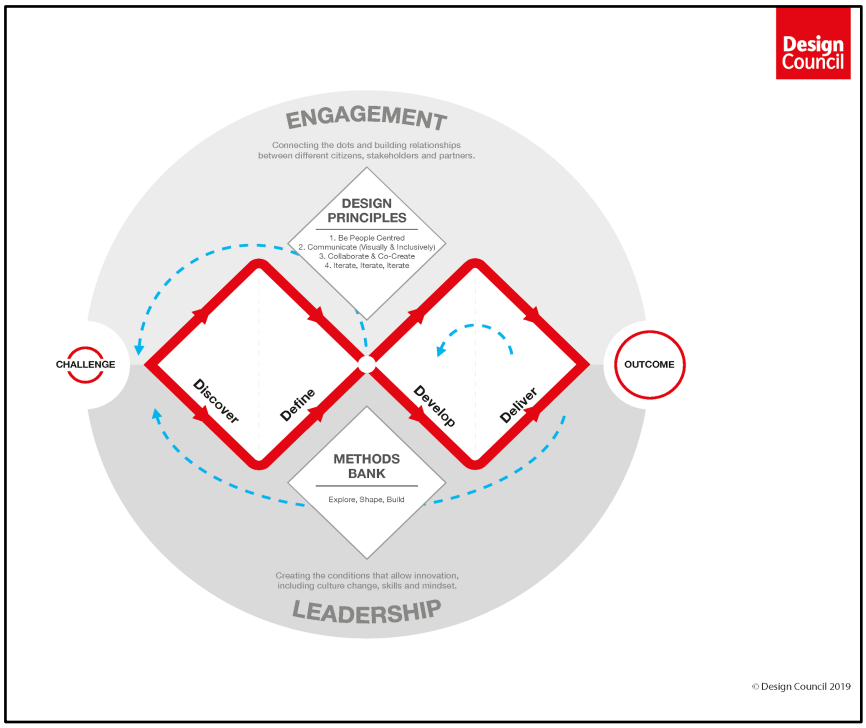


Figure 6 Design Council's Double Diamond conveys a design process. The two diamonds represent a process of exploring an issue more widely or deeply (divergent thinking) and then taking focused action (convergent thinking)(Design Council, 2015).

3.2 Research participants

To do this thesis and find relevant participants for data collection, local schools in the area were contacted, and collaboration with primary and lower secondary schools was established through the principals and NTNU. The target audience is the children in 5th to 9th grade and their parents. In this thesis, a collaboration was established with Kopperud School and Vestre Toten Ungdomsskole (VTU). The parents of the children were asked to participate and informed about the project through the school's internal information system. They also gave their consent for their children's participation in the survey and focus groups. All of the children's parents or guardians provided informed consent to participate in this thesis project. The children were further informed that they could choose whether or not they wanted to participate before responding to the survey, and that they could withdraw their consent at any stage. The project and methodological approach were approved by the Norwegian Centre for Research Data (NSD).

The parents were assured that the anonymity of their children is secured at all times since no personal data is gathered. The children participated in the survey during school hours. A total of 265 children from the two schools participated in our student survey. 14 parents volunteered to participate in the semi-structured interviews, 8 of them were actually interviewed and 8 teenagers from Kopperud School participated in the focus groups.

3.3 Semi-structured Interviews with parents

The most commonly used method of understanding users is interviewing. In a broad sense, an interview is simply something as mundane as a guided conversation in which one person seeks information from another (Baxter, Courage, and Caine, 2015). Interviews are a great way to empathise with users. It will be a valuable method to gain insight into the children and their parent's perceptions and experiences with online chat rooms and help us gain insight into their perspective (Stickdorn et al. 2018). Parents from local schools in Gjøvik were asked to take part in semi-structured interviews. These interviews aimed to investigate their views and knowledge about children's chat behaviours and how they assess the risks of online grooming.

The initial recruitment of parents for the interviews was conducted by designated contact persons at Kopperud School and Vestre Toten Ungdomsskole (VTU). The contact person at each school was responsible for sharing the information about this thesis study with the parents. Our liaisons at the schools also received instructions on practical implementation through an information letter with background information about the AiBA project and our thesis implementation and purpose. The schools shared relevant information with the parents, including details regarding how we protect their information and privacy. A digital registration form was generated using Nettskjema. Nettskjema is a universally designed self-service form solution hosted by the University of Oslo. It is a secure solution for data collection via the web through questionnaire, registrations and multiple-choice assignments. Parents who were willing to participate could fill out the form and register their participation. The form also included detailed information about the thesis project, such as:

- What it means to participate
- Who is responsible for the research project
- Why they were asked to participate
- Information about voluntary participation
- Contact information
- Practical information
- The opportunity to read more about the AiBA project through news articles

To organise the different time slots for the interviews a tool called Calendly was used. This was a very useful tool as the participants were able to pick their own time slots and it eliminated the hassle of back-and-forth emails. The interviews were designed to take between 45 to 60 minutes. Audio recordings were made of the interviews. They were used in the analysis work after the interviews. The audio recordings are stored on a

secure server at NTNU and will be deleted after this thesis is completed. Due to corona restrictions, the interviews were conducted digitally through Microsoft Teams.

Interviews are especially suitable for creating insights in design projects that aim to find solutions to specific problems or challenges. For this thesis, the goal was to investigate whether the parents:

- Use any form of **active mediation** - do they talk with their children about particular media activities or sharing these activities with them?
- Use any form of **restrictive mediation** - do the parents have rules for what children can or cannot do online?
- Use any form of **monitoring** - do the parents control or check up on what the children have been doing? For instance, do they check the computer log or chat messages to see what children have been doing or who they have been talking with?
- Use any form of **technical mediation**. Do the parents use any form of technical tools or specific software to filter and restrict unwanted use or content?
- What **information** they would like regarding online risks and grooming
- Do the children or teens, according to their parents, communicate with their parents regarding their online risk experiences?
- **Children's privacy**. With age, children have an increasing right to privacy. What views do the parents have on this issue?

Our goal for all our interviews was to ask open-ended questions to encourage users to speak. We asked questions like "tell me about" ... and followed up with "tell me more about it". Questions with open inputs sometimes lead to long answers. To ensure that we understood the participant correctly, we often summarised and reformulated the answers to check if our opinion was correct. This also helped us summarise the essential findings after each interview.

As this is a potentially sensitive topic, it was essential to let the participants know that they did not have to answer any questions that they felt were uncomfortable or too intrusive. Based on the initial research, an interview guide was created with the option to elaborate on topics that arose during the interview, including spontaneous follow-up questions that could be asked along the way. There were a set of predetermined topics, with the ability to change the order of questions or explore different topics during the interviews. We were surprised by the honesty and self-reflection among those we interviewed. There was a clear, strong commitment, and it was evident that the parents we talked to felt strongly about this topic.

User interviews can be very informative and valuable, and they can be an excellent method to gain insight into who the users are. These conversations became our most important method of mapping and understanding the parents. We asked questions to enable the parents to share their reflections, divulge what they experienced as challenging, what positive opportunities they saw, what they were motivated by, what values they based their parenting on, etc. We also looked for moments that could come from the sidelines and surprise us and create "revelations". The most challenging part of this method was to wait while the user pondered their answer and not rush to ask further questions. We always interviewed with both master students present, where one of us asked the questions, and the other took notes.

3.4 Survey for children 5th to 9th grade

Surveys are great, affordable, and practical ways of collecting data where the goal is to learn about a large population, such as pupils at a school. We conducted an online survey to gain insight into the children's experiences and attitudes towards online communication, social media, and the dangers they might face online. The survey was digital, and the school children could answer the questions by phone, PC, or tablet. The digital questionnaire in the survey is flexible and provides the opportunity for customised follow-up questions. The aim was that the survey should be as brief as possible and solicit only relevant information to the research. We conducted one pilot test to determine the validity of the questions in the survey before publishing the final version that was distributed to local schools in the Gjøvik region. During the pilot, we discovered that some of the questions and wording were confusing to the target audience, so they were rephrased.

The survey was conducted by NTNU recruiting pupils from Kopperud School and Vestre Toten Ungdomsskole (VTU) to participate though our designated contact persons at each school. The schools could choose when they wanted to carry out the survey within the set data collection period. At each school, a contact person was set up who was responsible for the survey and who received instructions on practical implementation. Each school received an information letter with background information about the survey's implementation and purpose. The schools also received a letter to the children's parents about the survey and how we protect their children’s information and privacy. It was possible to reserve against participating. It was also informed at the start of the survey that it was voluntary to fill out the online form. This was stated in the questionnaire itself and by the teacher. This also applied to individual questions as students were able to answer “don’t know” or “don’t want to answer” if there is a question they did not want to answer. To the children we also stressed that we would not

collect information that can identify them individually as a person. Also that their individual answers would not be shared with their school, parents or friends.

We used a tool recommended by NTNU called Nettskjema for the online survey. The University of Oslo hosts it, and it is a tool for designing and conducting online surveys and data collection for the university and college sector (*Hva er Nettskjema*, 2020). For surveys that use Nettskjema.uio.no for data collection and have made available measures for anonymisation, it should not be possible to track who answered. In this case, the data processor is USIT. The IP address is stored in the system log, but these will not be linked to single responses. This means that an online form as an IT solution can be used for anonymous surveys according to current NSD guidelines (*Er det meldeplikt til NSD for anonyme spørreundersøkelser i Nettskjema?*, 2020). The webform is subject to UiO's management system for information security (LSIS) (Gulbrandsen, 2020). Qualitative research conducted after the survey, in particular, could provide more insight into the situations and context of the children's experiences online.

3.5 Focus group and co-creation with 9th-grade children

Conducting research involving children can be a challenging task. Children are not miniature adults, and the way we develop and design research will play a big part in whether we get the information we need (Interaction Design Foundation, 2020). Most children have relatively short attention spans, which indicates that conducting research that lasts for hours is not advised. According to (Kirk, 2007) there are differences and similarities between conducting qualitative research with children and adults. Often, the similarities have been overlooked, and the differences overstated. Even so, there are inherent differences between children and adults. Children have limited vocabulary and understanding of words; they usually have less experience of the world and may have a shorter attention span. With this in mind, we wanted to conduct focus groups with children within the relevant age groups to learn more about their views on online risks and grooming. In addition, the goal was to see what solutions the children would come up with when given specific design-related tasks.

Focus groups have become a popular and widely used method in qualitative research. A focus group is an interview where five to ten people are brought together to discuss their experiences or opinions around a topic introduced by a moderator. Observing the participants and their reactions to certain situations is also a part of the method. The session typically lasts one to two hours and is suitable for quickly understanding users' perceptions about a particular topic (Baxter, Courage and Caine, 2015). Few empirical studies exist to guide researchers in determining the number of focus groups necessary for a research study. Analyses by (Guest, Namey and McKenna, 2017) revealed that

more than 80% of all themes were discoverable within two to three focus groups. Unfortunately, in this study, we were only able to conduct two focus groups as one of the schools we were in contact with had a coronavirus outbreak in April 2021. Therefore, the school principal was reluctant for their students to participate as the students were behind on their schoolwork and wanted to limit the risk of further infection.

To succeed with conducting focus groups with children, there are some key things to keep in mind such as early planning and preparation. This will increase success and go some way to ensure a positive experience for participants. Group composition factors such as age, sex, and personality must be considered. It is also essential to create the right environment where the children will feel safe. Also, the skills and personality of the moderator will influence the success of the discussion and the quality of the outcome (Gibson, 2007). Key benefits are that the group can bring up topics you never thought to ask about. Also, as it includes several participants simultaneously, it is a fast and straightforward way of collecting a lot of data. The downside is that the participants may be more susceptible to social influence.

When working with children above eleven years of age, co-creation activities benefit greatly from the discussion between researchers and children and their peers. Sessions with groups of up to six children are manageable. Professor Thomas M. Archer, of The Ohio State University, (Archer, 1993) recommends doing the following:

- Define age-appropriate questions that use casual language.
- If possible, recruit participants who know each other.
- Keep sessions' duration under one hour.
- Gather children in groups of five or six in the same age range.

3.5.1 Practical implementation

We held two focus groups and co-creation sessions with children in 9th grade from Kopperud skole in Gjøvik. There were a total of eight children present that contributed to this research. The school contact organised a space and time that fitted with the childrens' schedules. She also picked out the group of children that was to participate and decided on the composition of the group. There were four girls and four boys that participated in the focus groups. The children were divided into two groups after the initial warm-up session with two boys and two girls in each of the two groups.

Figure 7 Kopperud school

3.5.2 Purpose of exercise

The goal of this exercise was to gain insight into the children's understanding of online risks and their perceptions of their online interactions. To what extent they are aware of the danger and how they respond to various messages. The aim was not to discuss these sensitive and possibly uncomfortable topics as this would not be appropriate in a group session, but merely introduce the topics and then see what design suggestions the teenagers might come up with. Co-creation activities were a core part of the session and the goal was to see what solutions the children would propose. To sum up the goal of the different exercises was to:

- Understanding their app usage
- Understanding their perspectives on online chatting/ risks benefits
- Co-creation activities and design exercises

Key takeaways from that we wanted to be answered was

1. How do teenagers understand the dangers online?
2. What design solutions do children come up with when asked to design online chat features that can help them cope with potential online grooming situations?
3. How can an AiBA app help them cope with the situations they may face online?
4. Can we get help to design a solutions that is desirable to children

3.5.3 Focus group design and conduction

The presentation for this session can be found in the Appendices along with the design results made by the students.

The session was consisted of:

- An introduction to the master students
- An introduction to the topic, including a video from Kripos
- An introduction to the AiBA project
- Some ice-breaker questions to get the children to relax and talk
- Generic questions about online risks
- Brainstorming sessions in groups
- 4 design activities
- Wrap up

3.5.4 Child persona

In preparation for this session a child persona "Amalie" (Figure 8) was developed based on the survey result, literature research data and conversation with a child acquaintance. A persona is simply a fictional character created to describe a typical user, a model that can represent them (Baxter, Courage, and Caine, 2015).

This was to give the teenagers a typical user to focus on and have in the back of their mind when conducting the brainstorming activities. Also the purpose was to distance the teenagers from their own daily lives whilst feeling connected to the topic at hand.

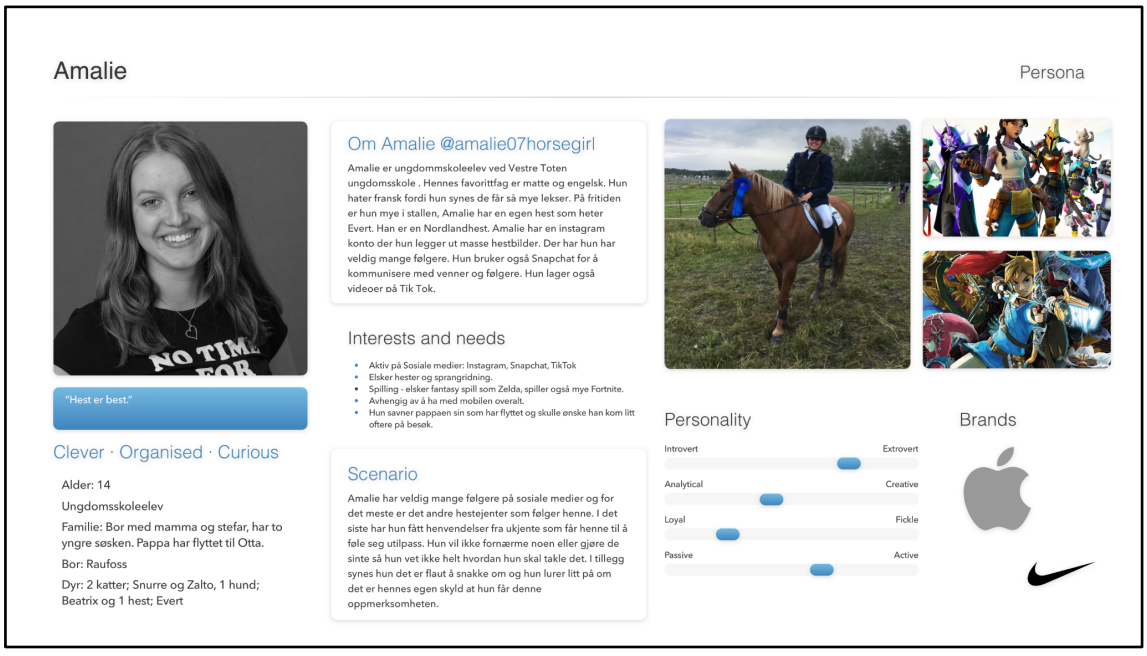


Figure 8 Child personas

3.5.5 Design methods used

3.5.5.1 Brainstorming in Activity 1, 2 and 3

A wants and needs analysis is a special kind of focus group exercise in which participants brainstorm about product features and services they would like to see. The goal is to gain an understanding of what the users want and need in a potential AiBA app.

We asked the teenagers questions like:

- What do you think it should have/do?
- What do you think it should not have/do
- What do you think it should say?
- What do you think it should not say?

3.5.5.2 Crazy 8's in Activity 4

Crazy 8's is a core Design Sprint method. It is a fast sketching exercise that challenges people to sketch eight distinct ideas in eight minutes. The goal is to push beyond your first idea, frequently the least innovative, and to generate a wide variety of solutions to your challenge (Google, no date).

3.5.5.3 Dot Voting In activity 3 & 4

This is a simple decision-making and prioritising technique used to democratically prioritize items or make decisions in a group setting. The group is asked to cast their vote by placing a dot next to the items they like the most or feel the most strongly about (Gray, Brown and Macanufo, 2010). In this exercise we used stickers to complete this task.

3.6 Expert and Heuristic Evaluation

Nearly 30 years ago, Jakob Nielsen described the 10 general principles for interaction design. These principles were developed based on years of experience in the field of usability engineering and they became rules of thumb for human-computer interaction. A heuristic evaluation is a usability engineering method for finding usability flaws in a user interface design, thereby making them addressable and solvable as part of an iterative design process. The method involves having a small set of evaluators examine the interface and judge its compliance with recognised usability principles (Nielsen, 1994). Nielsen suggests that between three and five evaluators is sufficient because when the number of evaluators used increases, the number of problems identified increases in turn. The purpose of the evaluation is to get insight into how we can improve the usability of the warning design and notifications designed for the parents and the children in an AiBA application. The best practice is to use established heuristics like Nielsen and

Molich's 10 rules of thumb and Ben Shneiderman's 8 golden rules as a stepping stone and inspiration while making sure to combine them with other relevant design guidelines and market research (Wong, 2020).

The benefits of conducting a heuristic evaluation is that it can be performed at any stage during the design process. Also there are no end users involved and it is a quick and inexpensive approach to track obvious usability issues.

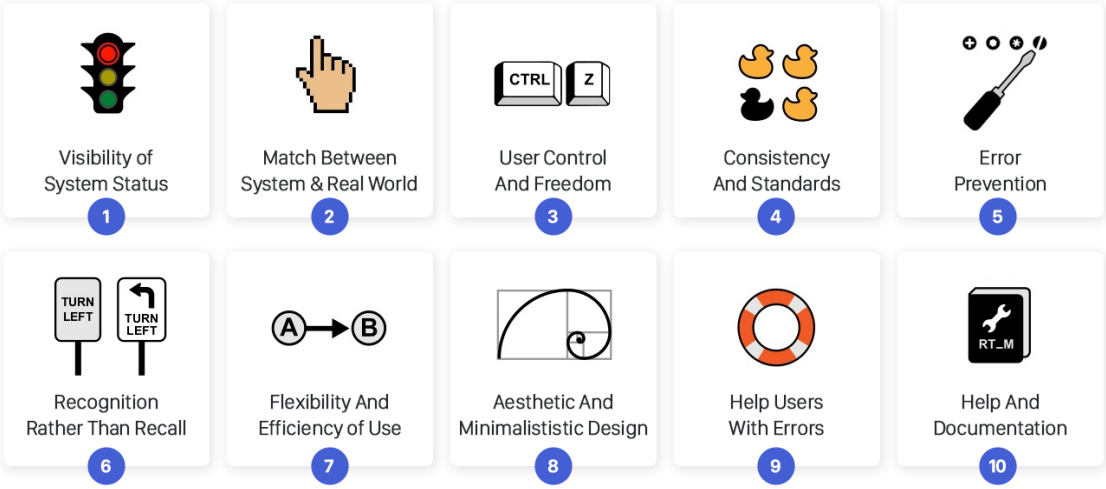


Figure 9 Jakob Nielsen's ten usability heuristics that can help the designers to make applications intuitive. Source: (Langmajer, 2019).

Some of the core heuristics are too general for evaluating newer products that have come onto the market since Nielsen and Mohlich first developed the method (Preece, Rogers and Sharp, 2015). Human-computer interaction (HCI) researchers argue that traditional heuristics sets are not completely relevant for current smartphone and applications mainly due to mobile specific features (Bashir and Farooq, 2019). For this thesis design-specific heuristics were established to evaluate and combined with other relevant design guidelines.

1. Visibility of system status: To what degree did you feel in control of the system? Did you get appropriate feedback on your actions?
2. Match between system and the real world: To what degree did you understand the used terms and language?
3. User control and freedom: How was the experience to navigate through the warning?
4. Consistency and Standards: How do you rate the consistency of the design?
5. Error prevention: Did you try to take any actions that did not work as expected?
6. Recognition rather than recall: To what degree were the given interaction elements (buttons etc.) recognizable and understandable?

7. Aesthetic and minimalist design: To what degree does the warning concentrate on relevant information and design elements?
8. Help and documentation: Did you feel lost at any moment and required help from the system?

In addition the experts were to evaluate the design according to the six recommended guidelines for effective cyber warnings to ensure usable security and warnings in the design as mentioned in chapter 8.8. Warning design.

The expert evaluations were conducted through an online form that was sent to professionals working in Interaction Design or related fields. Four experts, three UX designers and one Service designer, evaluated usability of the warning design and notifications designed for the parents and the children in an AiBA application in accordance with the design principles and heuristics.

3.7 Prototyping

Prototypes are one of the most important steps in the design process. At its most basic a prototype is a simulation or sample version of a product. The prototype can be used for testing as a part of the design process towards a finished product. The purpose for making a prototype is to test products or product ideas. Prototyping is essential for discovering and resolving usability issues, it can also reveal areas that need improving (Cao, 2016).

3.7.1 Paper Prototyping

At early stages of the design process, paper prototyping is a fast and inexpensive way to test your ideas.

3.7.2 Digital Prototyping

Digital prototypes are the most common form of prototyping, and are realistic enough to accurately test most interface elements. The goal is to test early and test often by starting with lo-fi prototypes that become progressively more advanced as the design process moves forward. The key benefit of this method is that realistic interactions can be tested and improved for the next iteration.

3.7.3 Warning message and safety words

Inspired by the international ISO 3864 standard these signal words will be used in the design as the detection of grooming behavior by AiBA implies immediate danger for the child In addition, there is the need to differentiate between the various levels of danger.

DANGER = Signal word used to indicate an imminently hazardous situation which if not avoided will result in serious injury

WARNING = Signal word used to indicate a potentially hazardous situation which, if not avoided, could result in serious injury.

CAUTION = Signal word used to indicate a potentially hazardous situation which, if not avoided could result in minor or moderate injury

INFORMATION = Signal word used to indicate important information not related to immediate risk.

3.8 Ethical Considerations

It is essential to be aware of the ethical implications of what we aim for when conducting research involving people. Most ethical issues in research fall into one of four categories; protection against injury, voluntary and informed participation, the right to privacy, and honesty with professional colleagues. Researchers must be susceptible to and thoughtful about the potential harm they may cause participants, especially vulnerable populations. This is especially true when treating a sensitive subject like online child abuse or grooming. It is essential to take special care with participants who cannot easily advocate for their own needs and desires - such as children (Leedy and Ormrod, 2015). Research must be undertaken in ethically sound ways. Therefore, it is a goal for this research to conform to the general guidelines and principles for research ethics prepared by the Norwegian National Committees for Research Ethics. Where the general principles are stated to be; respect, sound consequences, fairness, and integrity. (Norwegian National Committees for Research Ethics, 2014).

In addition, The Norwegian National Committee for Research Ethics in Science and Technology states that "When research involves humans as research subjects, researchers must, as a general rule, obtain freely given, informed consent".

This ensures that the person(s) taking part in the research:

1. Understand the purpose of the project and the part concerning their participation in the project
2. Can evaluate their situation
3. Can make an independent decision as to whether they wish to participate, without external pressure, based on the information and their preferences and values
4. Can freely communicate their decision

When dealing with people, especially those considered vulnerable research subjects such as children, a key aspect for researchers is to protect and safeguard the privacy of their

research subjects. The vulnerability occurs when a person's ability to protect himself is absent or diminished. Vulnerable populations are more susceptible to both intentional and inadvertent harm. Children are considered vulnerable because they have undeveloped decision-making skills (Schwenzer, 2008). Generally, in Norway, the law considers any person under 18 years old a child. Their ability to give informed consent is less than that of adults. Therefore informed consent from the legal representatives and written or oral consent from the child needed to be obtained before any interview or survey started. The children were guaranteed anonymity and allowed to choose the option "I do not know" or "Prefer not to say" for each of the questions. During the data collection, special efforts were made to provide comfortable conditions for the participants. This included maximising the anonymity of the participants and limiting interference.

The data collection for this thesis was reviewed and approved by the Norwegian centre for research data (NSD) in advance of implementation (Appendices). This shows that the project satisfies the high ethical requirements set by NSD, including an assurance that data about people and society is collected, stored, and shared safely and legally. In its implementation, we have emphasised following established norms for ethically sound research. Participation in research must be voluntary and informed, i.e. the decision to participate must be based on information about the topics and purpose of the research. We informed the participants about the project's purpose and how the research would be carried out through our contacts at each school, who distributed and shared the relevant information through the schools' internal communication system. In addition, the participants received the relevant information and option to consent or opt out through our online registration form.

Their task was to ensure that the students received the necessary information before they eventually chose to participate in the survey. In the same written document, we emphasised that it was voluntary to participate. It would not have any consequences for the individual if they chose not to participate and that all answers were anonymous.

4 10. Results

4.1 Semi-structured interviews

This chapter presents the findings of the semi-structured interviews of parents, who have children in primary and secondary school at Kopperud School and Vestre Toten Ungdomsskole. They were asked to reflect upon their children's use of chat apps, their concerns about online risks, their attitude towards parental mediation, how they communicate with their children, and their views on children's right to privacy.

The interview guide and interview schedule can be found in the Appendices. Eight parents participated in the semi-structured interviews. During the initial recruitment period, 15 parents filled out the online registration form and volunteered to participate. There were 6 parents that did not respond to our meeting invitation after initially filling out the registration form. One parent forgot to leave any contact information so we were unable to set up a meeting with that parent.

4.1.1 Thematic Analysis

The first step in quantitative analysis is to gain an overall impression of the data and to start looking for patterns. A thematic analysis strives to identify patterns of themes in the interview data and it is useful for summarizing key features of a large data set, as it forces the researcher to take a well-structured approach to handling data (Nowell *et al.*, 2017)

After the interviews all the data and audio recordings were transcribed and analysed. As a way of familiarising with the data, preliminary tags or keywords were assigned to the data in Figure 10 order to describe the content. This made it easier to sift through the data later. Coloured coded markers were used to indicate which code each piece of data refers to. A digital spreadsheet was used to keep track of the data, codes, and themes.

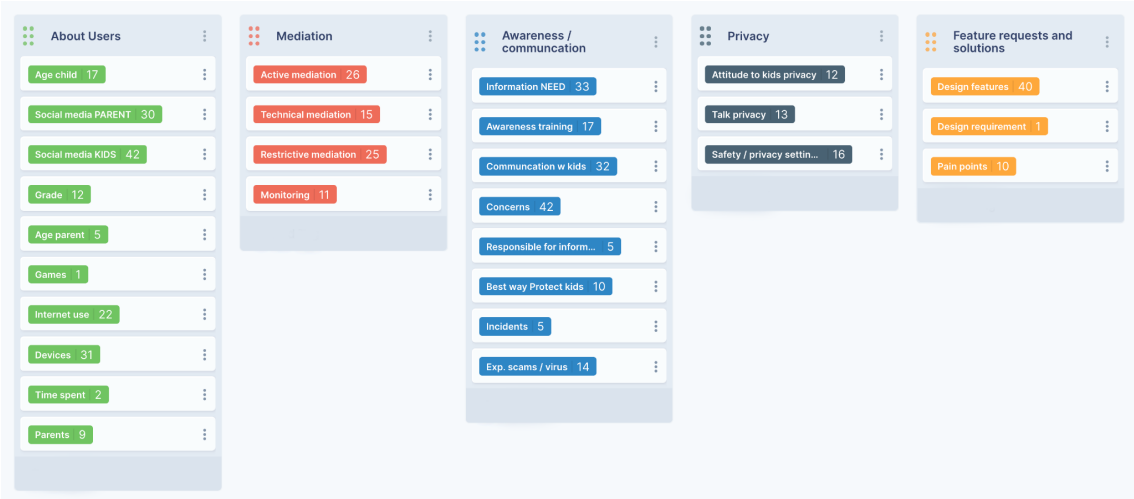


Figure 10 An overview of the colour coded tags assigned to the data.

After the preliminary tags were generated the data was sorted according to similarity and divided into five categories by creating affinity diagrams.

- About the users
- Mediation
- Awareness and communication
- Privacy
- Future requests and solutions

4.1.2 The users

Seven women and one man, their ages ranged between 36 to 55 participated in the interviews. A detailed overview of the participants age, and position can be found in the interview schedule in the Appendices along with the interview dates. The parents had children in 4th grade up to 10th grade, with the mean age being 14 years. There is a clear difference between the preferred social media for the children; Snapchat, Tiktok and Instagram Figure 11 to the parents Figure 12 who mostly use Facebook.

Figure 11 Word cloud of social media used by children

Figure 12 Word cloud of social media used by parents

Several of the parents state that their children view Facebook as being for their parents' generation Figure 13.

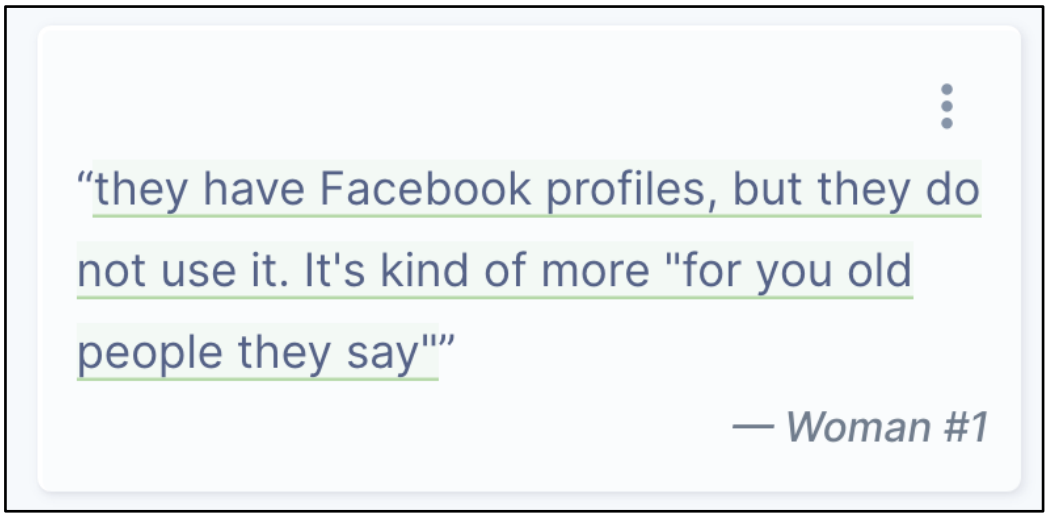


Figure 13 Quote from a parent regarding their kids' view on Facebook

The corona pandemic hit Norway, and on March 12 2020, society locked down. In response to the pandemic the Norwegian government advised that if possible, people should be working out of their homes as a tool to limit the spread of infection. Home office is an important measure to reduce contact between people both in the workplace and on the journey to and from using public transport (Folkehelseinstituttet, 2020). As a result of this all the parents who participated in the interviews have spent more time in front of the computer and using digital tools Figure 14 at home in the past year than they normally do.

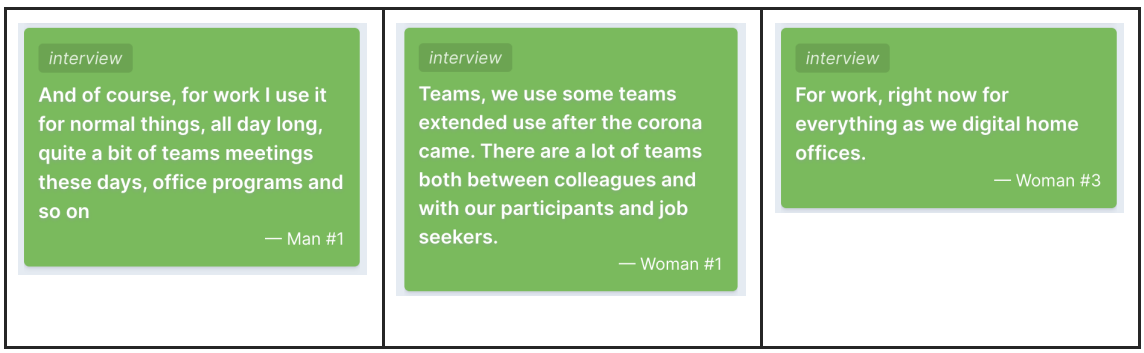


Figure 14 Quotes regarding parents’ internet use

4.1.3 Mediation

The most popular form of mediation is active mediation Figure 15, which means that the parents talk with their children about particular media activities or share these activities with them. Parental mediation has been a suggested approach for promoting media literacy skills within the home. This mechanism relies on parents to mediate their children's media use by talking with them about media, and/or watching or using content with them (Uhls and Robb, 2017).

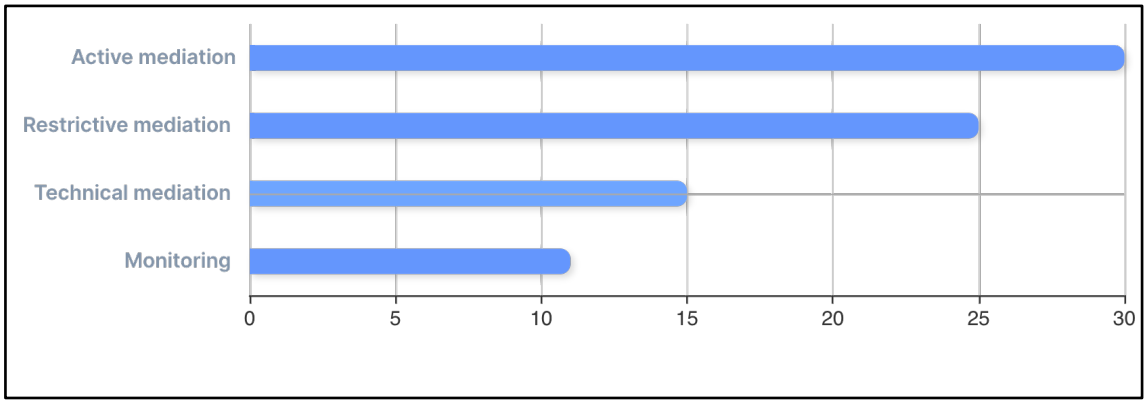


Figure 15 Mediation

Mediation	Number Parents	Highlight count
Active	8	30
Restrictive	6	25
Technical	6	15
Monitoring	5	11

Table 2 Overview mediation techniques

Active Mediation

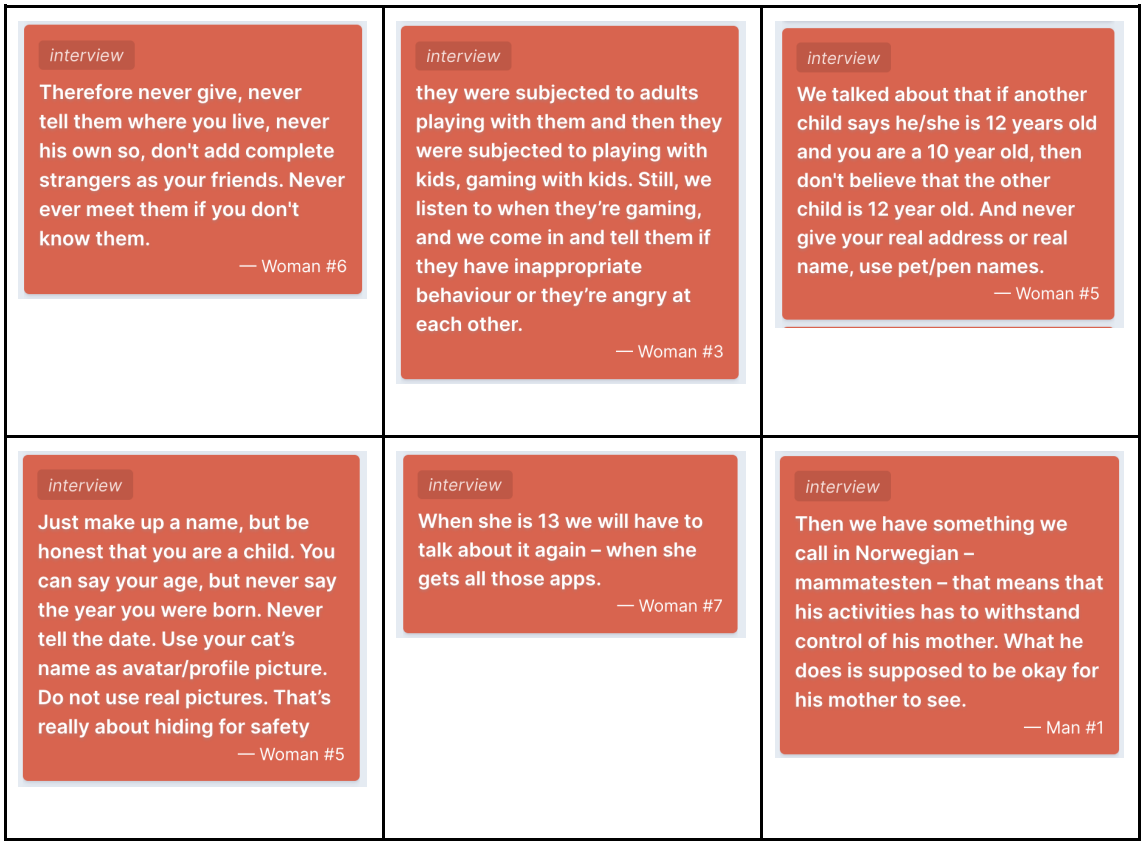
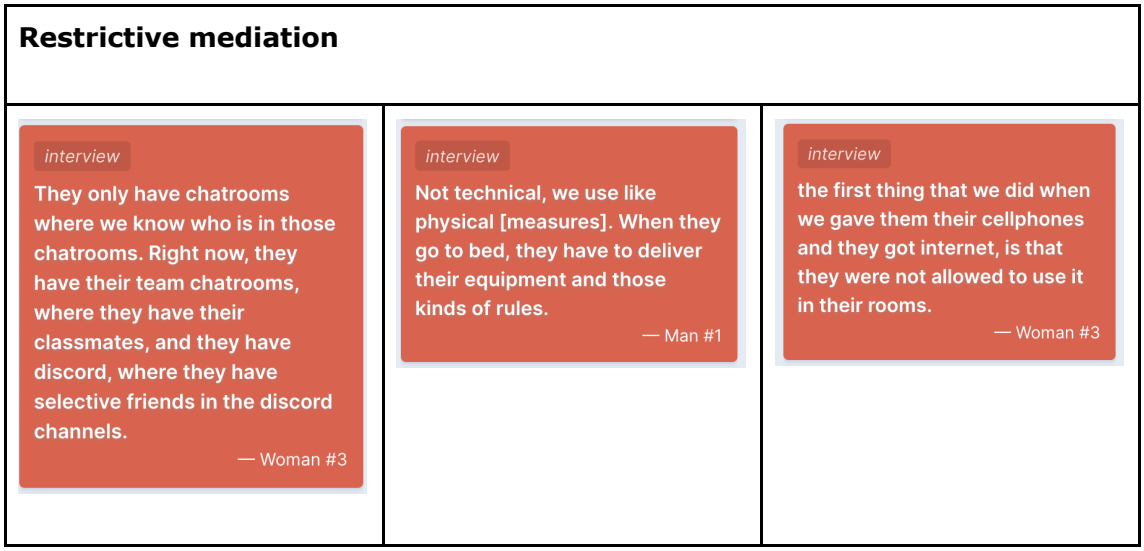


Figure 16 Quotes regarding active mediation

All the parents seem genuinely interested and involved in their children's digital life. They also think it is important to get involved with and use social media or games with the children as a way of teaching them about being safe online.

Secondly, the parents talk alot about using some form of restrictive mediation, which means that the parents have rules for what children can or cannot do online.



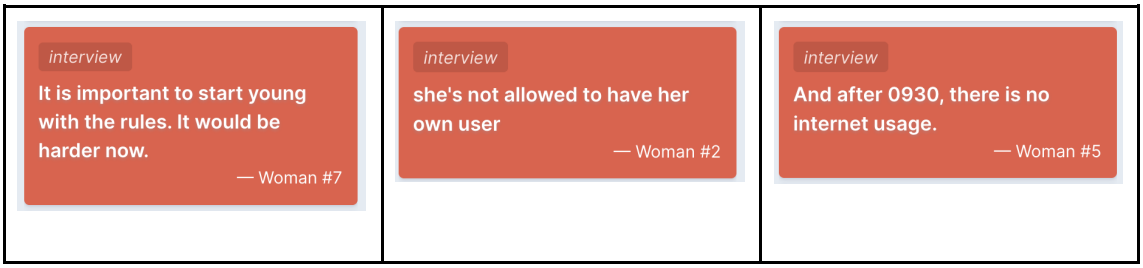


Figure 17 Quotes from parents about restrictive mediation

The most common forms of restrictive mediation are rules about who the kids can communicate with, where the kids can use their digital devices or time restrictions.

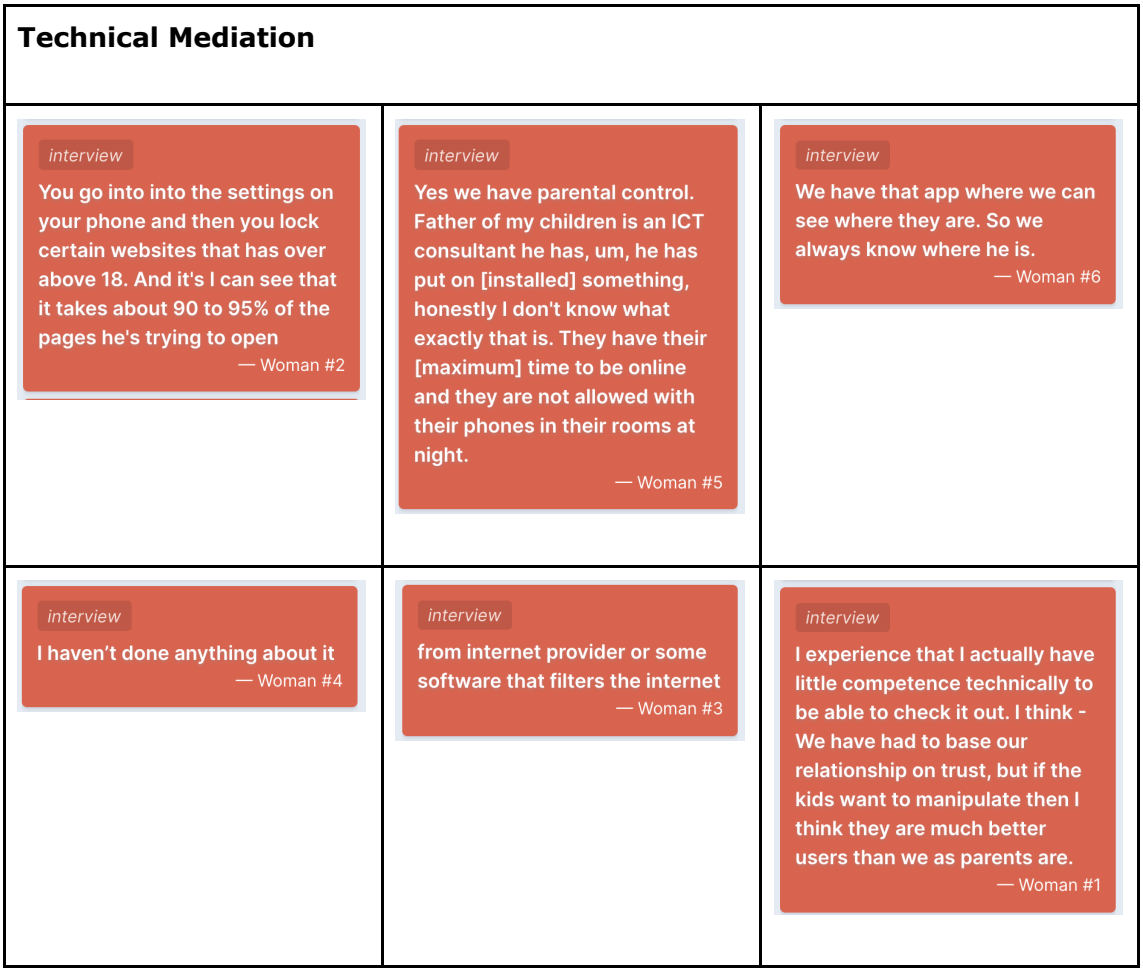


Figure 18 Quotes from parents about technical mediation

Most of the parents would like to implement some form of technical mediation Figure 18, but not all feel they are competent to do so. The technical restrictions that the parents use are tools or software that block adult content, limit screen time, position services and/or restrict which apps can be installed.

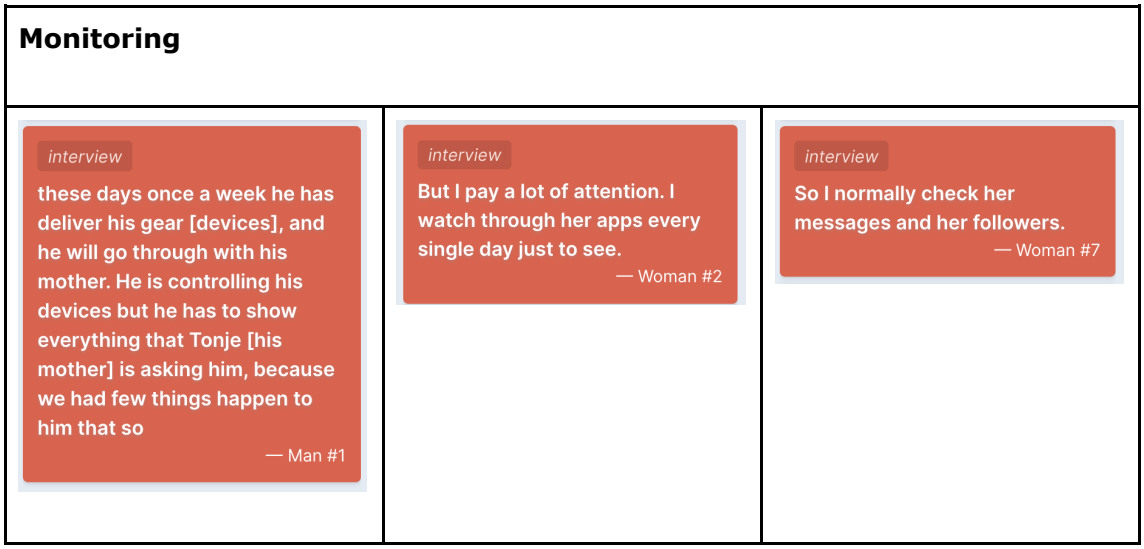
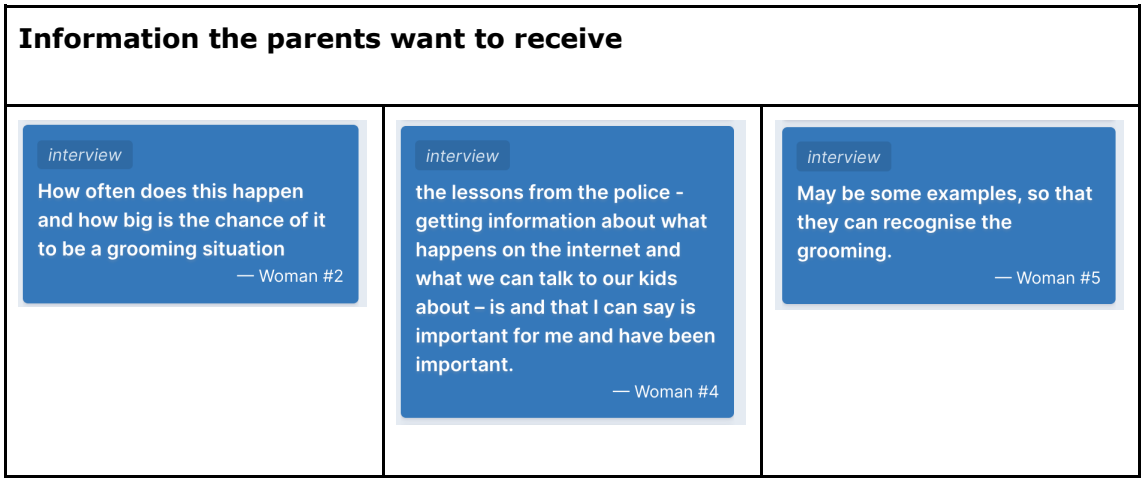


Figure 19 Quotes from parents about monitoring

Parental monitoring Figure 19 refers to when parents check up on their kids by going through phone logs or messages on their children's device (s). Five of the parents that were interviewed monitored their children's internet use by going through phone logs and/or messages on their children's devices. A couple of the parents started doing this after there had been incidents where the children had done something they shouldn't have done, like sharing inappropriate content or sending nasty messages to other children. The parents that did not use this form of mediation all felt that to do so would be an invasion of their children's privacy.

4.1.4 Communication and awareness

In this section of the interview we wanted to find out what kind of information the parents have and would like to receive about the risks of online grooming and sexual predators. Also we looked into how the parents communicate this topic with their children, their concerns and what they thought would be the best way to protect their children from harm.



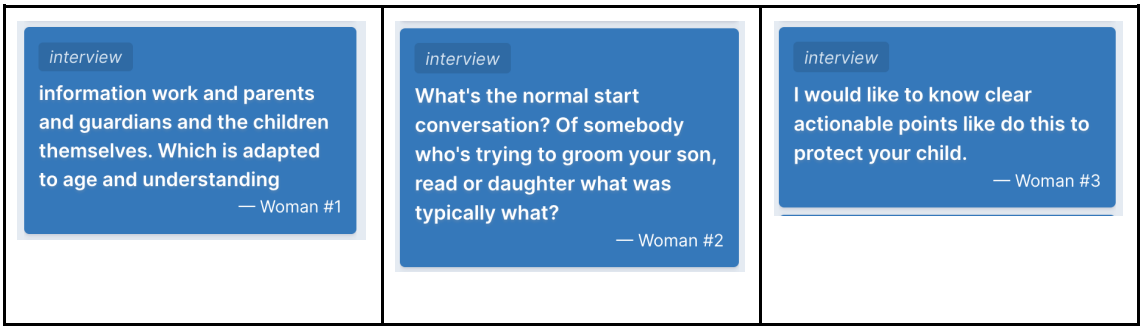


Figure 20 Information the parents want to receive

All the parents wanted to receive Figure 20 practical information such as:

- Information about grooming; how does it happen
- How to talk to their children
- Age appropriate guidance
- Statistics; how often does it happen
- How do the groomers come in contact with and get the kids to answer

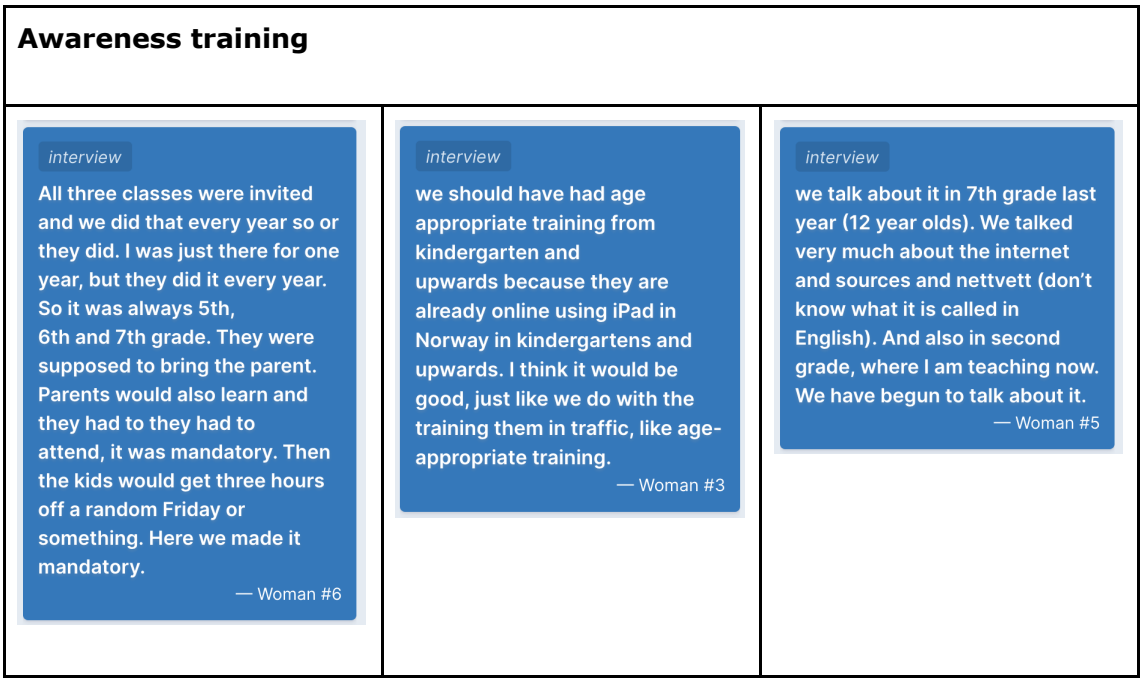


Figure 21 Awareness training comments from parents

Six of the eight parents have received some form of awareness training Figure 21 either through the school or through parents meetings in connection with the school. One parent had initiated the "Nettvett" evening while being a part of the parents' council's working committee (FAU) at her children's school. It seems to vary greatly how much and how regular these sessions are. Most of the parents seem to think this is a school responsibility as this is, in their opinion, the best way to reach all the children and also this would mean that all the schoolmates would have the same or similar rules.

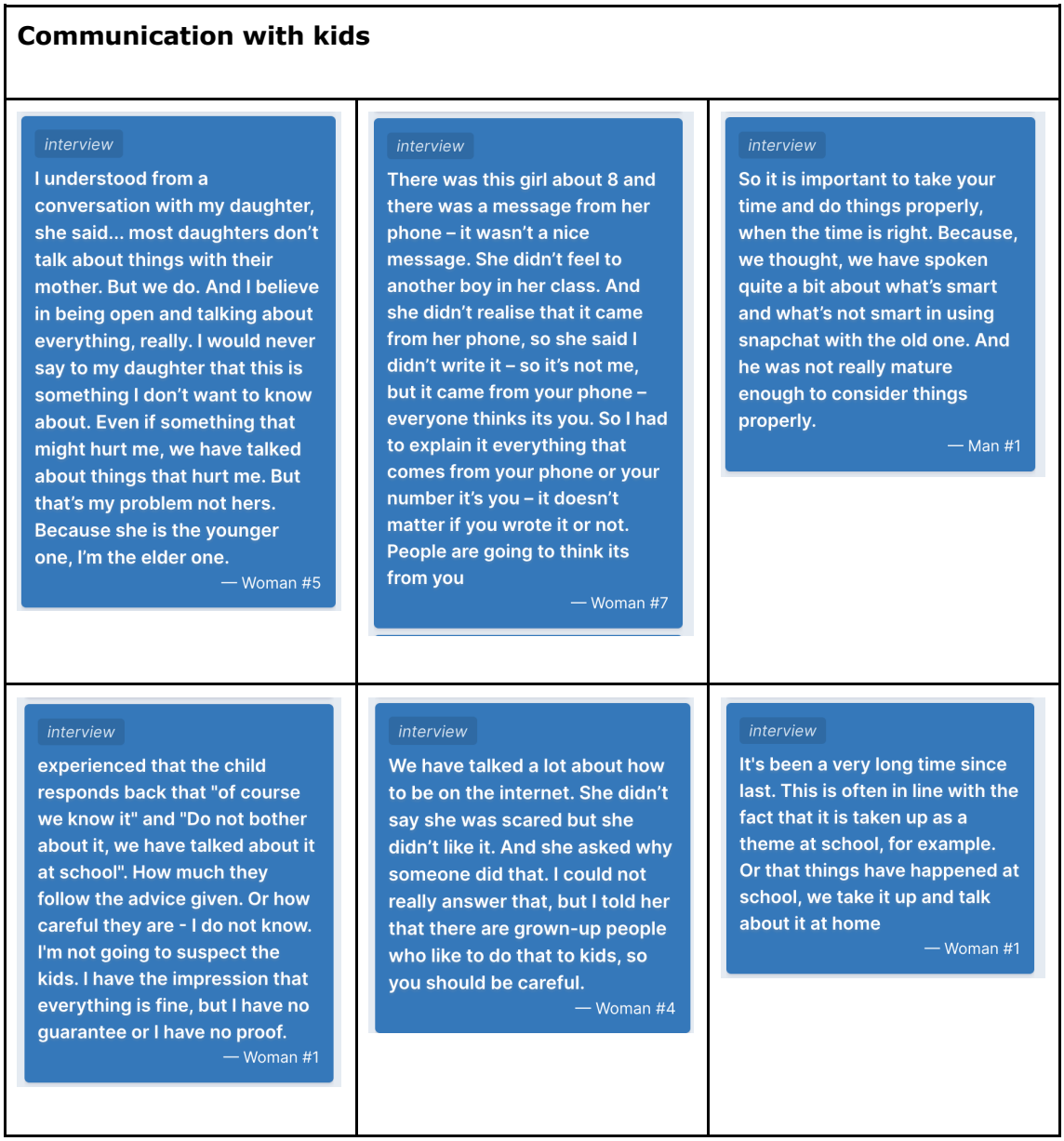


Figure 22 Quotes regarding how parents communicate with their kids

When the parents communicate with their children Figure 22, the children often get the impression that everything is fine. Often they discover that even though they have talked about risks and how to behave online, it is sometimes difficult for the kids to translate that into what goes on in their real lives. Often it is not until something happens and they talk about it with their parents that there is real learning.

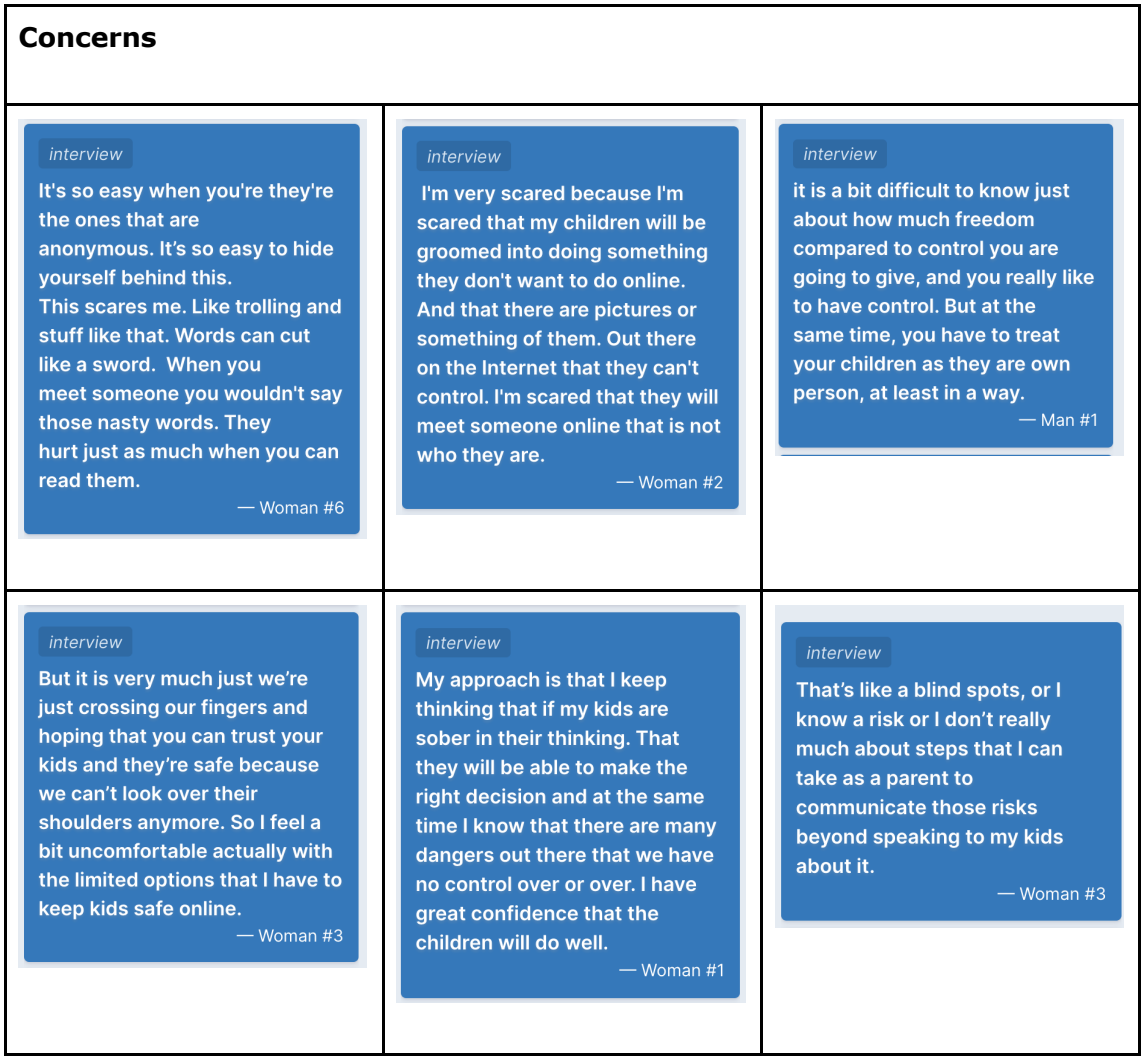


Figure 23 Quotes regarding the parents main concerns

Parents' main concerns Figure 23 is how to protect their children from online grooming and bullying. In addition they struggle with how much freedom they should give their children and also how to communicate the risks to their children. Furthermore, parents generally hope they can trust their children to make sound choices.

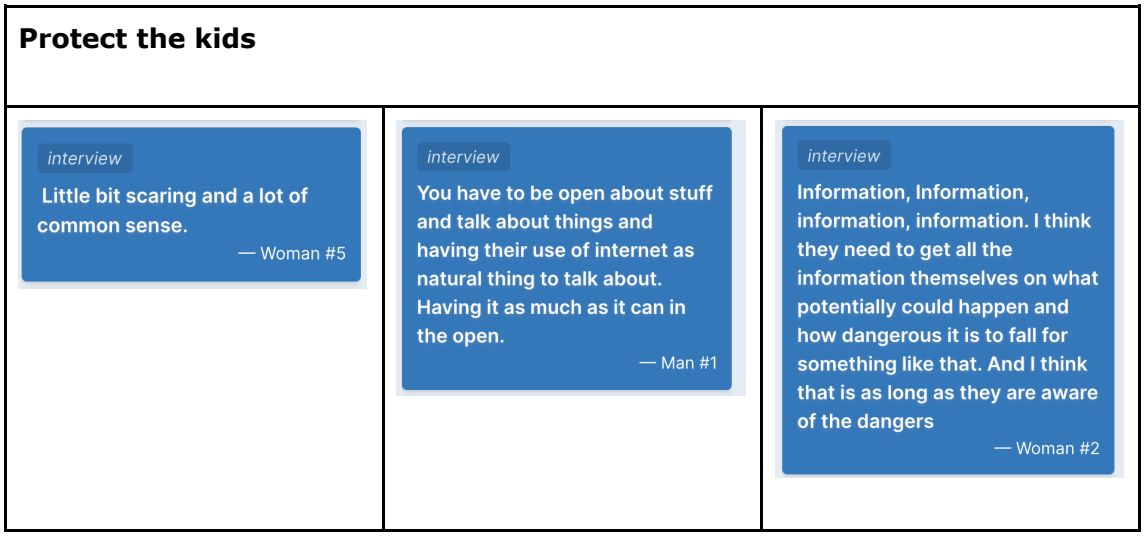
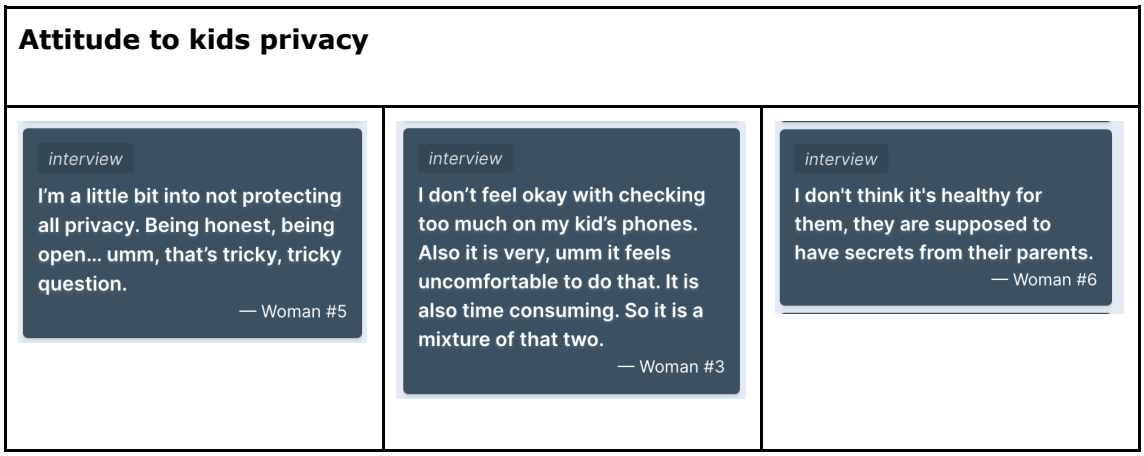


Figure 24 Quotes from parents regarding how to protect the kids online

The best way to protect children, according to the parents we talked to, is awareness Figure 24. Talking to them about the subject and being open, watching programs or videos together and talking about it afterwards are important steps towards keeping the children safe. In addition, scaring them a little with realistic stories can also help. It is important to let the children know that you are there for them and that they can come to you without fear of judgement.

4.1.5 Privacy

The parents we talked to thought that the questions about privacy was one of the more difficult issues to talk about. For some of the parents, keeping their children safe outweighs their children's right to privacy. On the other hand some of the parents think that in today's society we know too much about our children and that they should be given the opportunity to have "good secrets" without their parents interference and constant monitoring Figure 25.



interview That's difficult. Because, I want children to be protected. — Woman #5		

Figure 25 Attitude to kids privacy

When parents talk about privacy with their children they discuss issues like sharing of photos on different platforms and how information that is published online is difficult to control once it is out there. Furthermore they talk alot about how images and information are hard to remove once it is shared online.

Talk about privacy		
interview I've talked to him a lot about pictures online that the pictures that you share on Facebook and Instagram are pictures that you put online that might never go away, so you should make sure that this is OK for you, that these pictures are there. Never take pictures of others we've had sort of those conversations. Yeah. But no more than that. — Woman #2	interview we have talked a bit about what information he should show, what information he should keep in the open [visible], what he should keep to himself and done that using a apps and programs with him and looking at how others do it. — Man #1	interview I've talked to him a lot about pictures online that the pictures that you share on Facebook and Instagram are pictures that you put online that might never go away, so you should make sure that this is OK for you, that these pictures are there. Never take pictures of others we've had sort of those conversations. Yeah. But no more than that. — Woman #2

Figure 26 Parents' quotes about privacy

4.1.6 Feature requests and possibilities

After talking to the parents regarding what a possible AiBA app could be, we asked them to give their opinion on what features the parents would like to see in such a solution.

Design features

Figure 27 Design improvements and suggestions from the parents

Some of the features (Figure 27) that the parents came up with were:

- A feature where the kids could ask for help
- See suspicious activity on my children's phone "I would buy it for thousands of kroner"- woman #2
- Family security as a service
- Notifications about grooming in real time
- An app that could help the child stay safe
- A way of "blacklisting" or tagging bad users, or warning against bad IP-addresses
- A tool to help me with the difficult conversations
- Filter contacts and content

- A rule book, short and simple or videos you could watch with your child
- Really simple set up, super easy like putting on an alarm
- Age appropriate settings, more freedom as the kids get older

4.2 Survey

The purpose of conducting the survey was to understand how children in 5th to 9th-grade use chat apps and to contribute to an up-to-date knowledge base about how children and young people relate to others on the internet. Two hundred sixty-five pupils between the age of 10 to 15-year-olds from Kopperud School and Vestre Toten Ungdomsskole (VTU) participated in the survey. The respondents answered questions about their media use and experiences related to the web and mobile, computer games and social media, primarily focused on online chatting and chat apps. The survey collected a mix of quantitative and qualitative data.

In the following, the sample is described in more detail with a view to the distribution of gender and age groups. Statistically significant and otherwise interesting differences between boys and girls and different age groups will be commented on throughout the report.

4.2.1 About the population

Out of the 265 students, 262 completed the survey. There were 133 girls and 123 boys; six students did not want to divulge their gender (Figure 28). The sample contains relatively equal numbers of people from these two segments, thus having a representative sample where the segmentation criterion is gender.

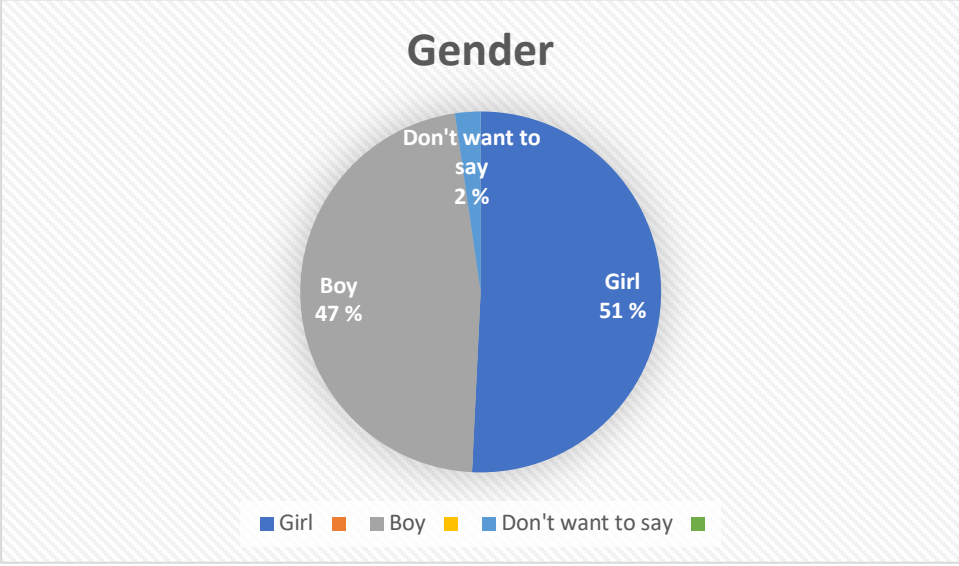


Figure 28 Gender of the respondents

The most significant majority of respondents were from secondary school in 8th grade and 9th grade, respectively, 98 and 126 respondents (Figure 29). In addition, 32 students from 7th grade responded. This is a representative sample when the segmentation criterion is secondary school students in the Gjøvik and Toten area. Four students were from primary school students in 5th and 6th grade. Two respondents did not want to say which grade they were in. We were not able to get a representative sample of children from primary school.

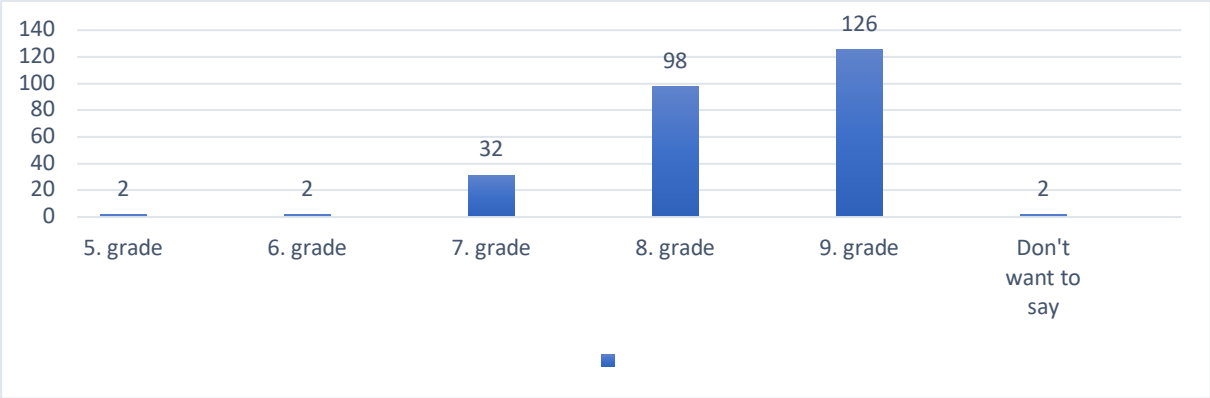


Figure 29 Which grade the kids are in

4.2.2 Access to equipment and technology

In total, 95 % of the children have or have access to a smartphone. A large proportion also have a laptop or computer (74,3%), either on their own or on sharing with others in the family. Furthermore, more than half have their own tablet and their own game console (61 and 60 per cent, respectively). It is not as common to have a smartwatch; 21 percent of the children have this at home. (Figure 30)

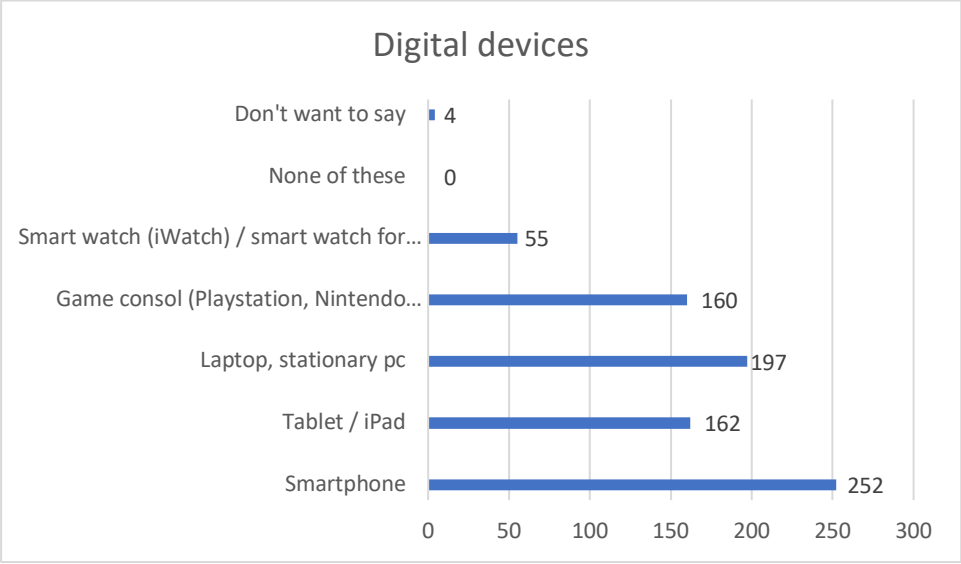


Figure 30 Kids' access to digital devices

4.2.3 What social media and chat apps do children use?

Among boys, a larger proportion use Discord (Table 3) than among girls. The proportion who use Tiktok, on the other hand, is greater among girls than among boys. For other social media and apps, there are relatively small gender differences at the overall level. A total of 94 percent of the children use Snapchat.

Group Statistics

	1. Er du	N	Mean	Std. Deviation	Std. Error Mean
a. Facebook	Jente	133	2.44	.667	.058
	Gutt	121	2.64	.645	.059
b. Snapchat	Jente	133	4.03	.921	.080
	Gutt	123	3.83	1.014	.091
c. Instagram	Jente	133	3.38	.911	.079
	Gutt	123	3.15	.897	.081
d. TikTok	Jente	132	4.31	.966	.084
	Gutt	123	3.91	1.008	.091
e. Discord	Jente	133	2.38	.858	.074
	Gutt	121	3.12	1.279	.116
f. Messenger	Jente	133	2.51	.572	.050
	Gutt	120	2.68	.724	.066
g. Messenger kids	Jente	133	2.02	.213	.018
	Gutt	120	2.01	.242	.022
h. Telegram	Jente	133	2.02	.288	.025
	Gutt	120	1.99	.159	.014
i. YouTube	Jente	132	3.52	.961	.084
	Gutt	123	4.37	.727	.066

Table 3 a larger proportion of boys use Discord

The most popular apps that the children use are by far Tiktok and Snapchat, with 76 (Tiktok) and 62 (Snapchat) percent of the children using these apps 1 to 2 hours a day or more than 2 hours a day. (Table 4)

d. TikTok

		N	%
Jeg får ikke lov å bruke denne appen		3	1.1%
Jeg bruker ikke denne appen		24	9.1%
Mindre enn 1 time om dagen		32	12.1%
1 til 2 timer om dagen		84	31.7%
Mer enn 2 timer om dagen		117	44.2%
Missing	Ã nsker ikke Ã¥ si det	2	0.8%
	System	3	1.1%

b. Snapchat

		N	%
Jeg får ikke lov å bruke denne appen		4	1.5%
Jeg bruker ikke denne appen		11	4.2%
Mindre enn 1 time om dagen		81	30.6%
1 til 2 timer om dagen		73	27.5%
Mer enn 2 timer om dagen		92	34.7%
Missing	Ã nsker ikke Ã¥ si det	1	0.4%
	System	3	1.1%

Table 4 The most popular apps that the children use are by far Tiktok and Snapchat

4.2.4 Experience with chat apps

When asked "what do you usually do when someone asks you to become "friends" (Figure 31) follow you on social media" 22 percent (57) of the children responded "I accept everyone" and 19 percent answered "I accept if we are the same age".

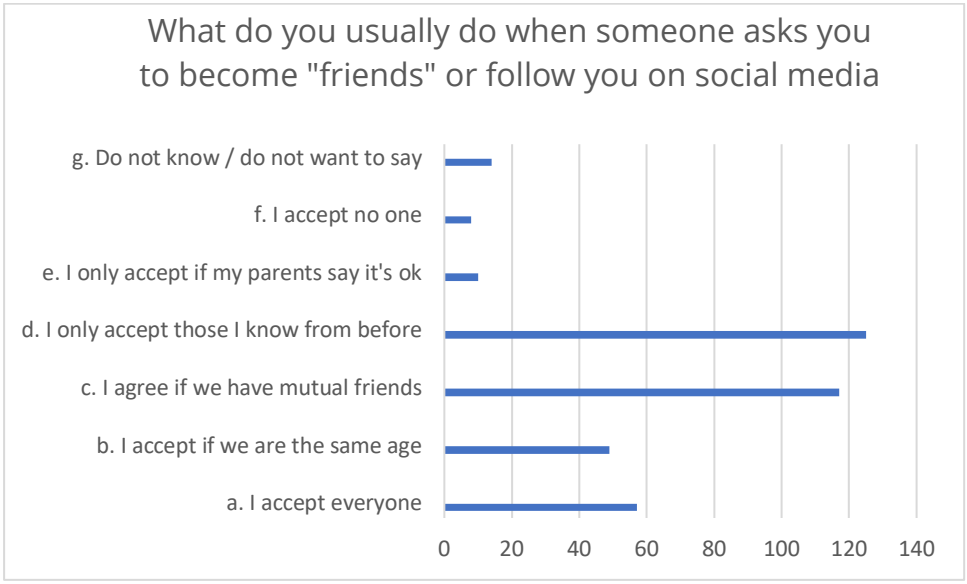


Figure 31 When someone asks you to become "friends"

79 percent agree that they have a lot of contact with their friends on social media (Figure 32). 26 percent feel more "myself " online than in reality, that is 69 children. A total of 93 children are not sure, as 36 percent answer "neither agree nor disagree". 21 percent have regretted sharing something on social media or in a chat.

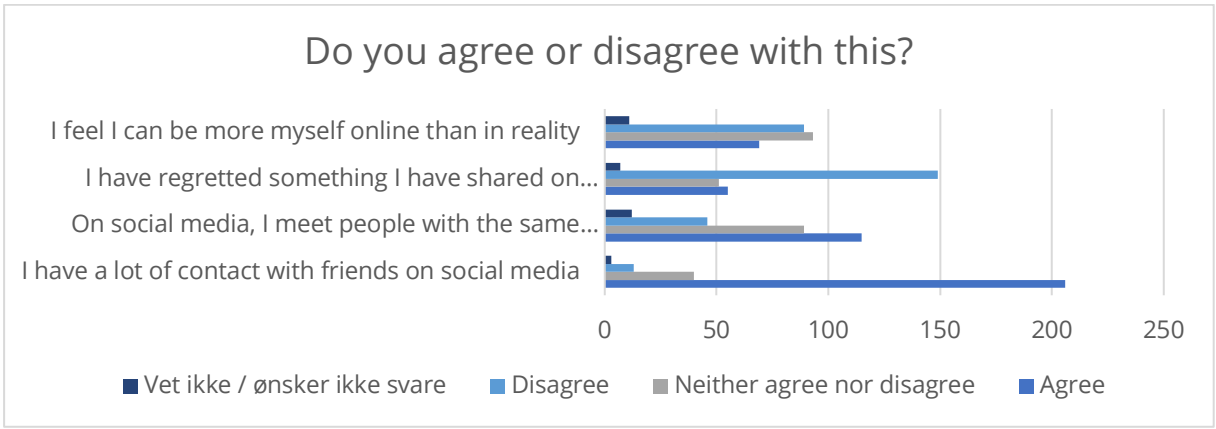


Figure 32 79 percent agree that they have a lot of contact with their friends on social media

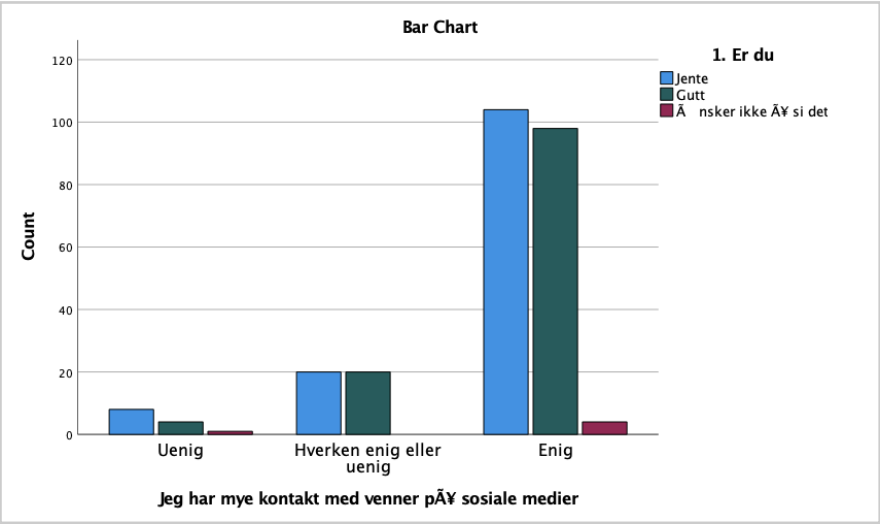


Figure 33 I have a lot of contact with my friends on social media

As seen in Figure 33 there is not a lot of difference between girls and boys when it comes to contact with friend online.

4.2.5 Communicating with strangers online

16 percent (41) of the children have never had contact on the internet with someone they have not met in real life. This means that 84 percent of the children have had contact with strangers online (Figure 34).

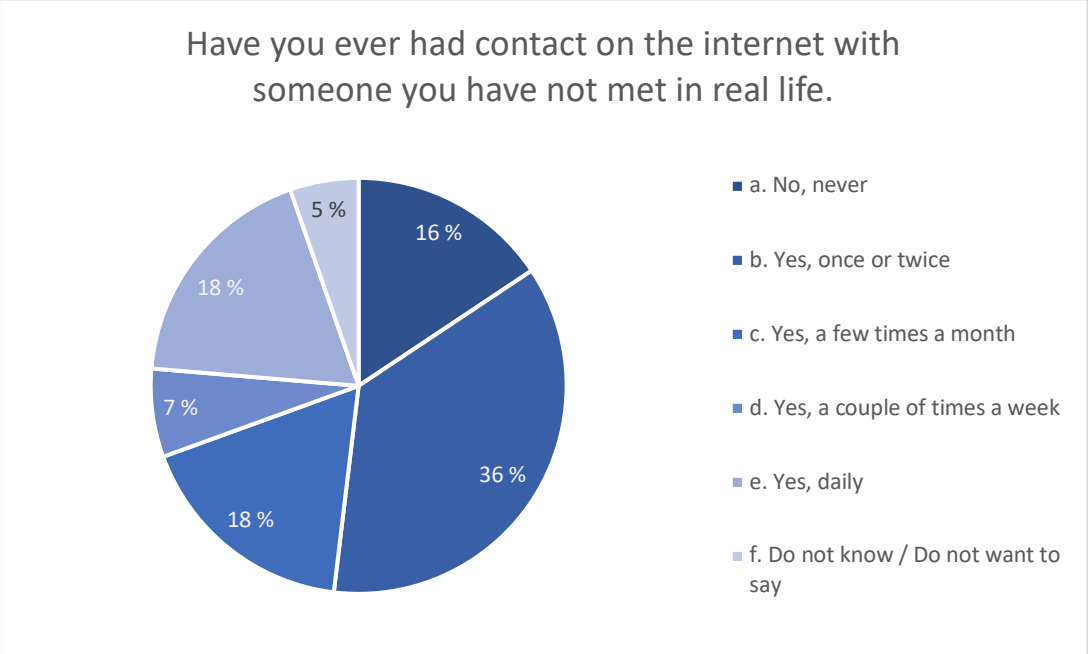


Figure 34 84 percent of the children have had contact with strangers online

Crosstab

Count

		1. Er du			
		Jente	Gutt	Ã nsker ikke Ã¥ si det	Total
8. Har du chattet eller snakket med fremmede pÃ¥ nett?	a. Nei, aldri	23	18	0	41
	b. Ja, en eller to ganger	50	44	1	95
	c. Ja, et par ganger i mÃ¥neden	23	22	1	46
	d. Ja, et par ganger i uka	4	14	0	18
	e. Ja, daglig	26	19	3	48
Total		126	117	5	248

Figure 35 Crosstab: have you chatted with strangers online

There does not seem to be a large difference between how many girls and how many boys have communicated with strangers online (Figure 35).

Out of the 84 percent, 36 percent (94) children have met someone in real life that they first got to know online. Most, 70 percent, met someone their own age and had a positive experience (69 percent). 22 percent were neither happy nor upset about the experience, one person was a little upset.

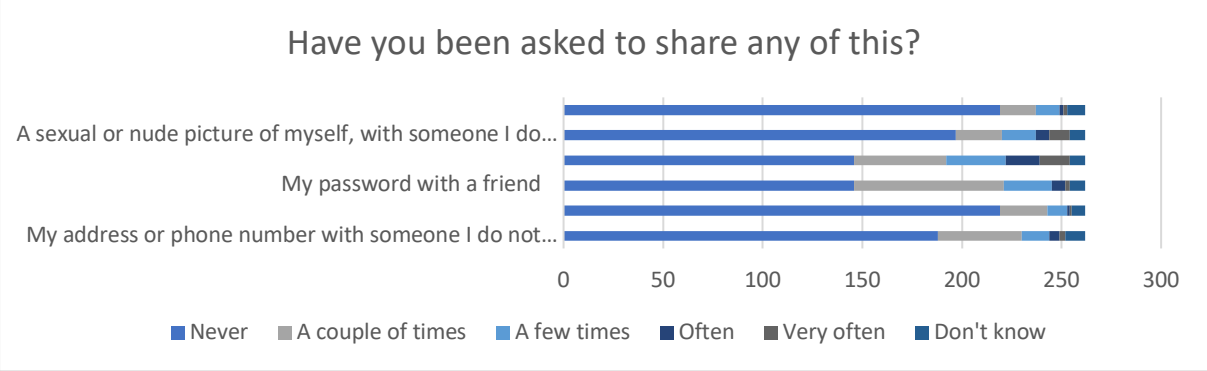


Figure 36 Have you been asked to share

Then we asked the children whether they had ever been asked to share any private information in a chat conversation or on social media (Figure 36). 24 percent had been asked by a stranger for their address or phone number, 41 percent have had a friend ask them to share their password. 41 percent had also been asked to share a photo with a stranger online. 22 percent had been asked to share a sexual or nude photo of themselves, with someone they did not know. This has happened to a larger proportion

of the girls compared to the boys (Figure 37).

Crosstab

Count

		1. Er du			
		Jente	Gutt	Ã nsker ikke Ã¥ si det	Total
d. Et seksuelt eller nakenbilde av meg selv, med noen jeg IKKE kjenner	1. Aldri	88	107	2	197
	2. Et par ganger	12	10	1	23
	3. Noen ganger	15	1	1	17
	4. Ofte	7	0	0	7
	5. Veldig ofte	9	1	0	10
Total		131	119	4	254

Figure 37 22 percent had been asked to share a sexual or nude photo

Figure 38 What did you do the last time you were asked for private information

Last time they were asked for private or sexual information online 41 percent of the children blocked the person who had asked them (Figure 38), 21 percent did nothing in particular and only 2 percent told their parents or an adult they trust. 21 percent don't know or don't remember what they did.

4.2.6 Security and privacy

We asked the children one open ended question, "What do you need to feel safe while chatting on the internet or using a chat app"?(Figure 39). The number one answer here was "I need to know who I am talking to". This statistic includes 74 of the responses to this question. In total there were 101 relevant responses.

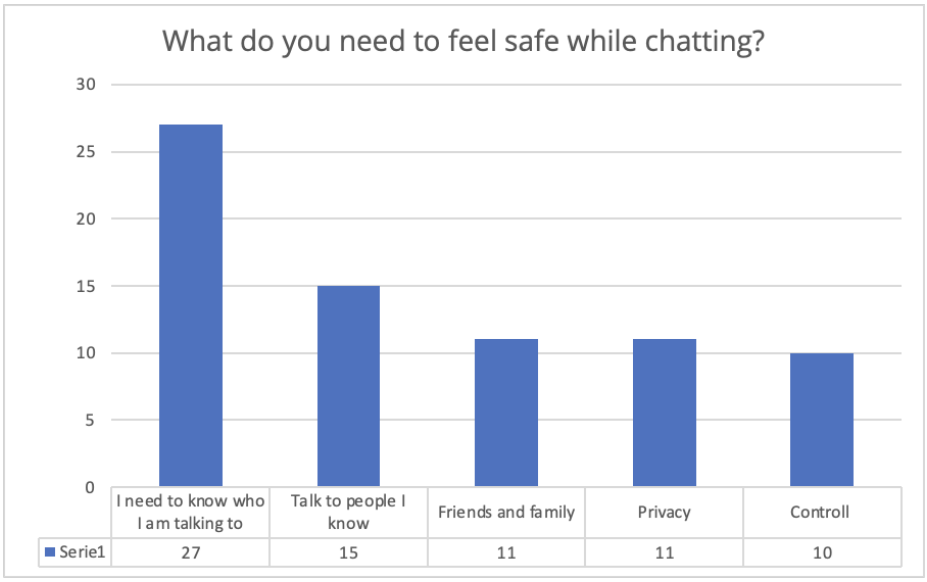


Figure 39 "What do you need to feel safe while chatting on the internet or using a chat app"

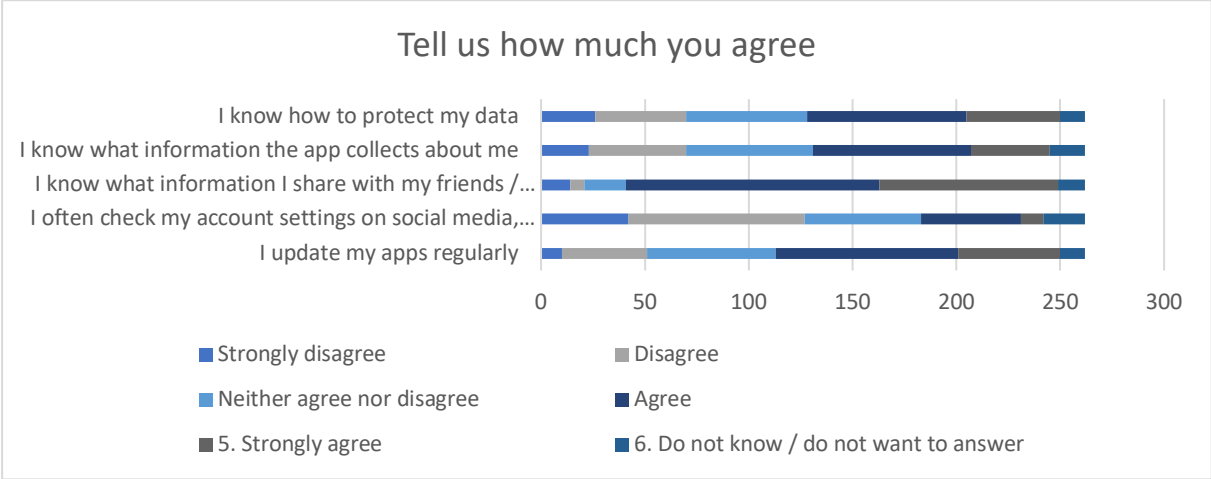


Figure 40 The participants strongly believe that they have control over the information they share with their friends and followers

The participants strongly believe that they have control over the information they share with their friends and followers (Figure 40) as 80 percent agree or strongly agree with the statement. Around half of the students state that they update their apps regularly, know how to protect their data and know what information the app collects about them. In contrast 48 percent state that they disagree or strongly disagree with the statement " I often check my account settings…".

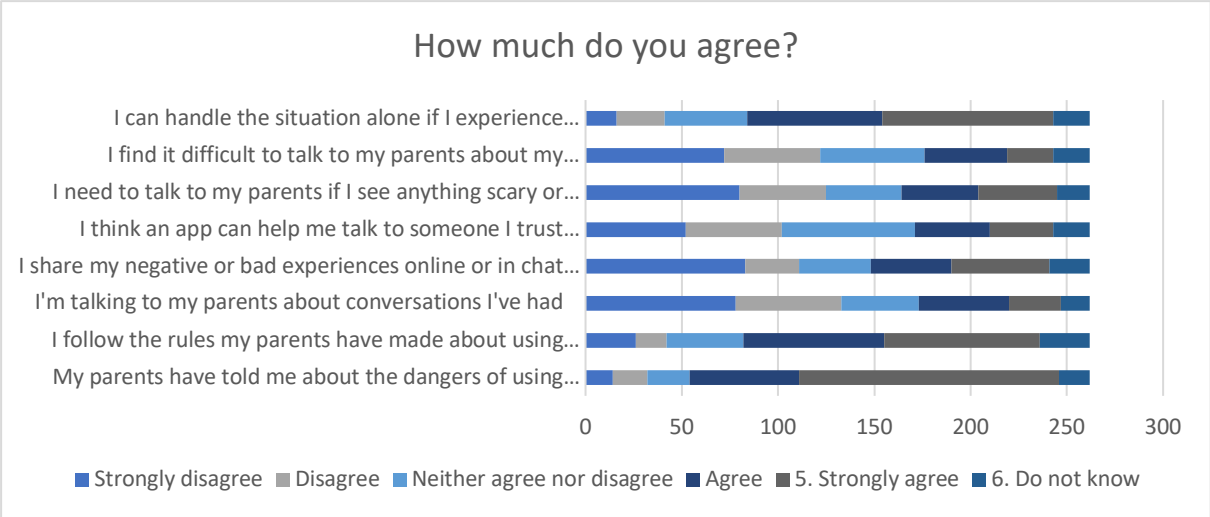


Figure 41 73 percent of the children state that they have been informed by their parents about the dangers of using chat apps

Quite encouragingly, 73 percent of the children state that they have been informed by their parents about the dangers of using chat apps (Figure 41). Moreover 59 percent abide by the rules made by their parents. More than half the children state that they disagree or strongly disagree with the statement " I'm talking to my parents about using chat apps". Only 25 percent find it difficult to talk to their parents about negative experiences, whilst 35 percent share their negative experiences with their parents. Furthermore, 61 percent respond that they can handle the situation alone if they experience something painful or negative.

From the literature, it was apparent that the internet posed risks to any user, especially children. Therefore, it was essential to identify whether participants were aware of these risks. The responses in this survey largely correspond to the data found in the literary study from the background chapter. Quite surprising was the discovery that even though the children mostly don't find it difficult to talk about this topic with their parents, a majority are able to handle difficult situations themselves.

4.3 Focus groups

The data collected included observational notes from the facilitators, photographs from the sessions, and the children's design suggestions. The online collaborative tool Miro was used to structure and analyse the data.

4.3.1 Questions about online risks

The overall impression from speaking with the teenagers is that they generally feel safe online Figure 42. This is especially true for when they are using their mobile phones as they feel this is safer than being on their laptop or computer. Most of the children were pretty adamant about what they would do if a sexual predator was to contact them "I

block them”. All the teenagers stated that they would not tell their parents about their negative experiences as this would cause a lot of extra hassle and that the parents and school would turn it into “a big thing”.

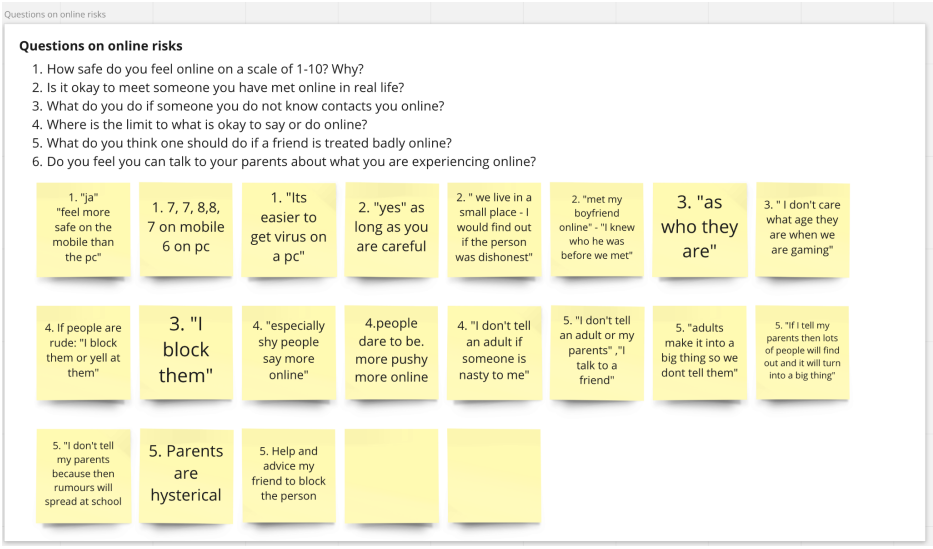


Figure 42. The teenagers generally feel safe online

4.3.2 Activity 1

AiBA is planned to be an app in the future. The app can be installed on children’s and parents’ phones. It will notify and provide information if there is any grooming behaviour in a conversation. This activity discovered that the teenagers themselves want to decide what should be shared with their parents, they also specified that this would be age specific and that younger children should be more closely monitored by their parents.

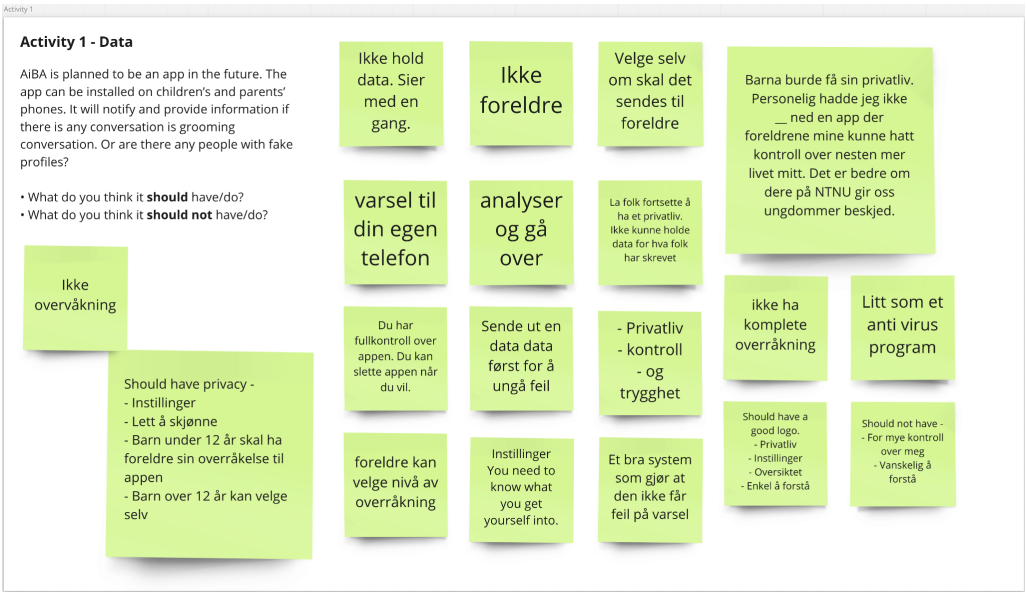


Figure 43. teenagers themselves want to decide what should be shared with their parents

4.3.3 Activity 2

AiBA app will send out notifications in case there is a risk or grooming situation. These notifications and details will be sent out to parents', children's phones and moderators. The children were told to reflect on what these notifications should say. Some of the responses can be seen in the Miro board below Figure 44.

Figure 44. children reflect on what AiBA notifications should say

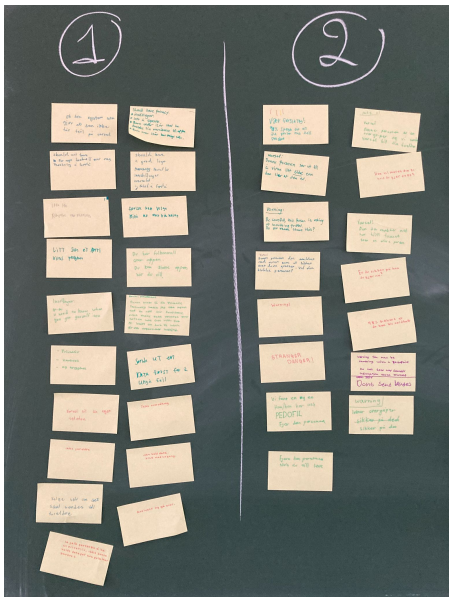
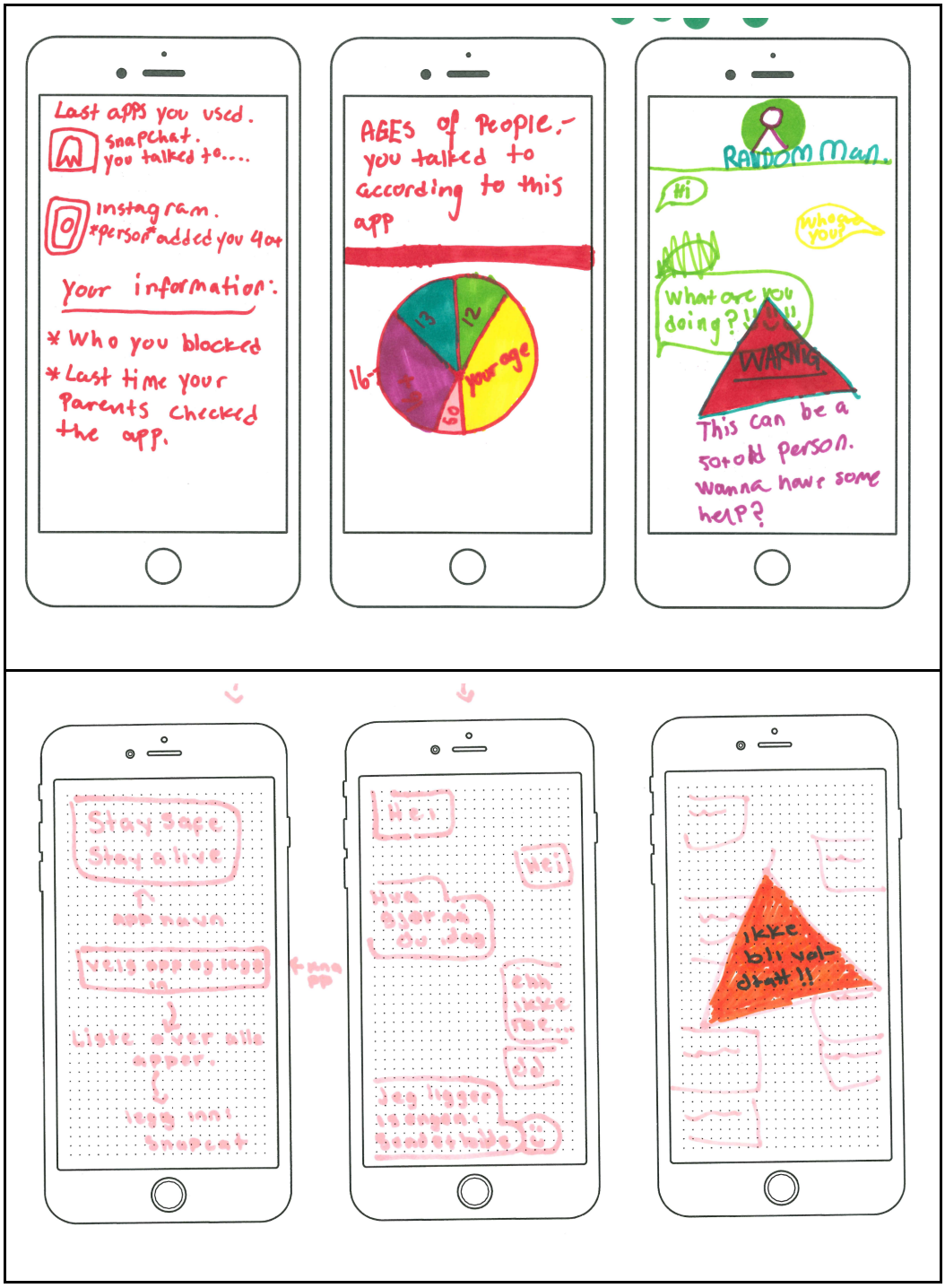


Figure 45. Post-its from activity 1 and activity 2

4.3.4 Activity 3

All the mock-ups for this exercise can be found in the Appendices.

If someone faces difficulties or problems, how can the app help? Which features do you think it should have? What would you like to do with it? Can the app help to talk to someone they trust?



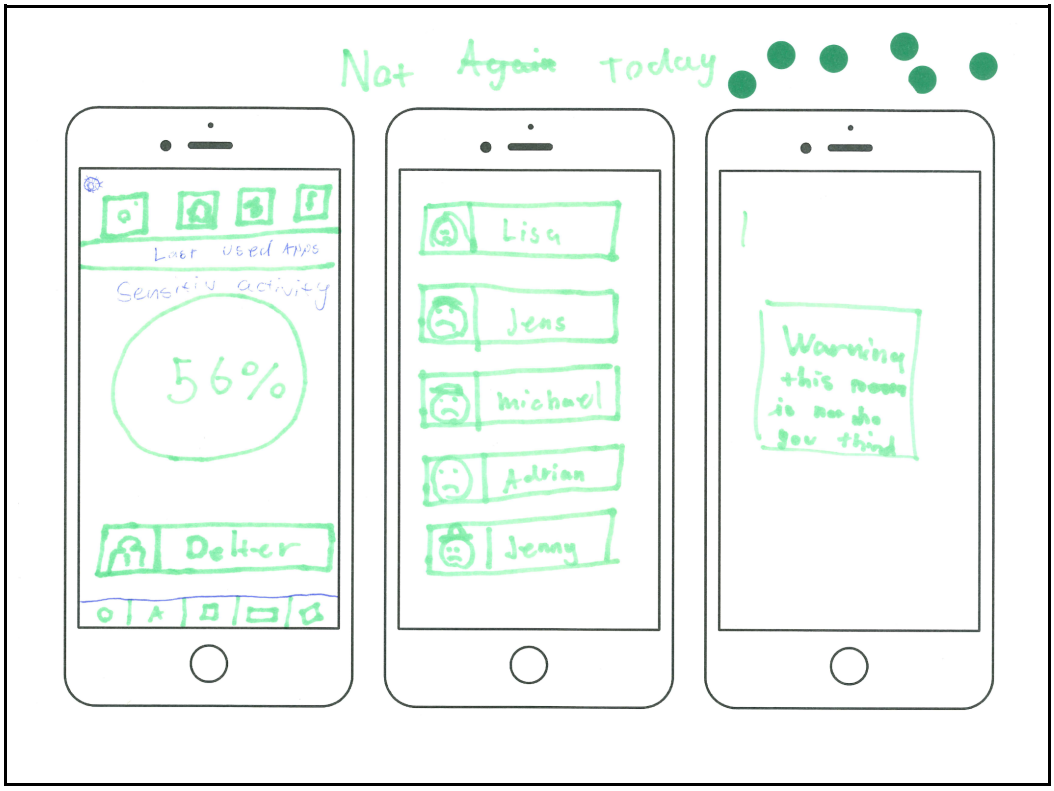


Figure 46. Possible features

4.3.5 Activity 4

In this exercise the children were to design an online feature that can help Amalie cope with an online grooming situation.

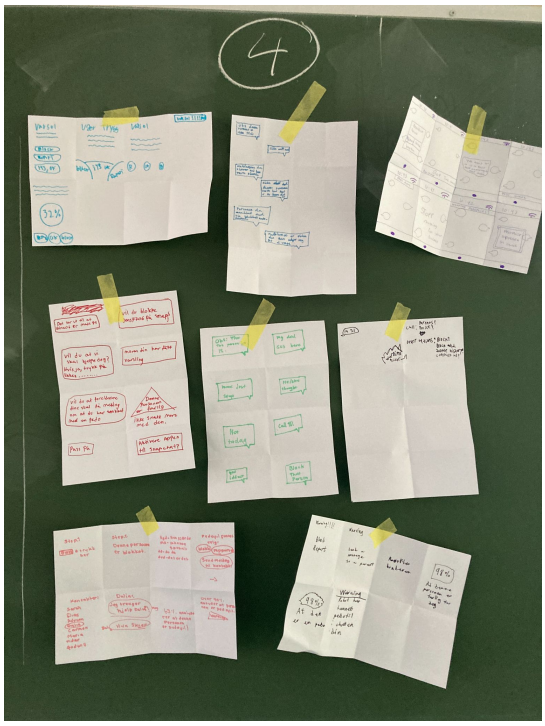


Figure 47. Crazy 8s results

Instead of parental control features, most of the children in our study preferred self-regulatory features that would assist them in dealing with a potential grooming situation such as a “help button”, a way to block the person or an easy way to contact the police. Furthermore, the children often wanted the app itself (instead of adults) to provide assistance that kept them safe from online risks and detect potential sexual predators. The teenagers were greatly opposed to features that would impede on their privacy, leave the control up to their parents or restrict their behaviour. Although they did agree that this would have to be age appropriate and that younger children should have more restrictions placed upon them. The teenagers wanted the app to guide them and help them perform the necessary actions needed, as opposed to a general warning. Furthermore they clearly opposed constant parental monitoring and especially feared that the AiBA solution would misclassify a conversation as risky and notify their parents.

4.4 Initial prototypes

Based on the literary review and initial results from the parents' interviews, children’s survey and focus groups several prototypes were made. Starting with the lo-fi paper prototypes and then moving to higher fidelity prototypes. For the digital design and prototyping the tool Figma was used.

4.4.1 Paper prototypes

In Figure 48 Paper prototypes and ideation

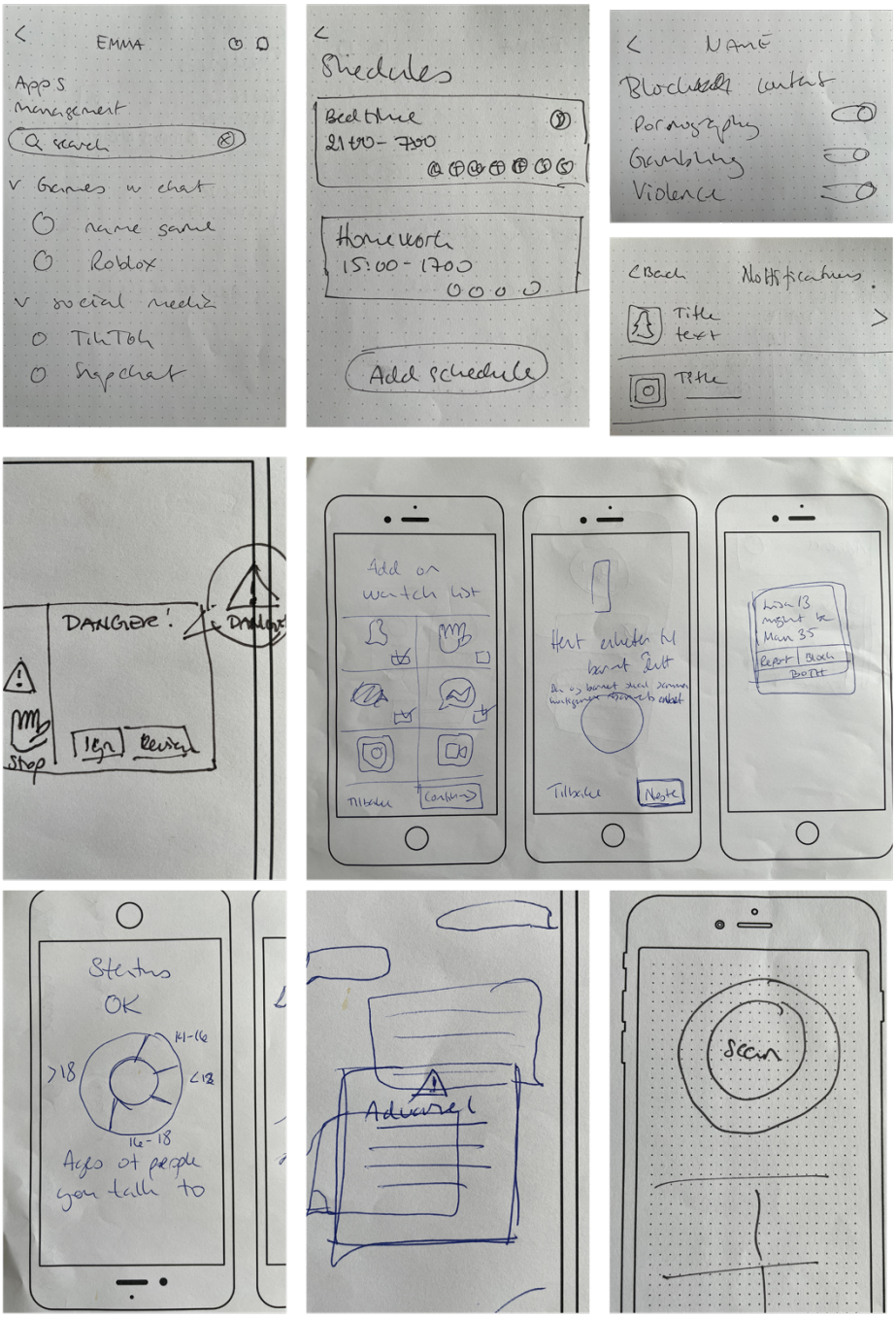


Figure 48 Paper prototypes and ideation

4.4.2 Initial digital prototypes

Three prototypes were designed

- Figure 49 AiBA app prototype with basic features
- Figure 50 AiBA child warning prototype
- Figure 51 AiBA parents notification.

4.4.2.1 AiBA app prototype

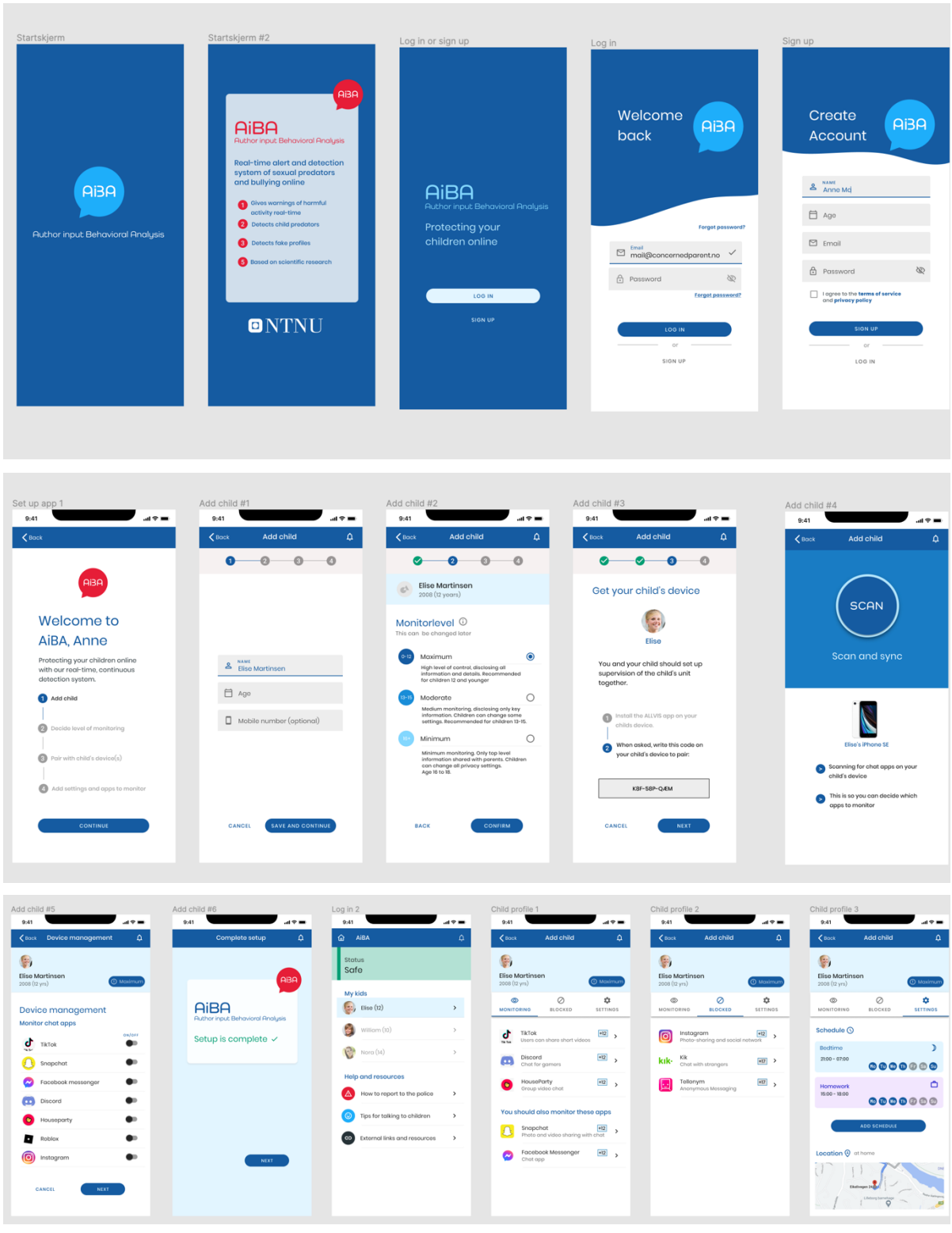


Figure 49 AiBA app prototype with basic features

4.4.2.2 AiBA child warning prototype

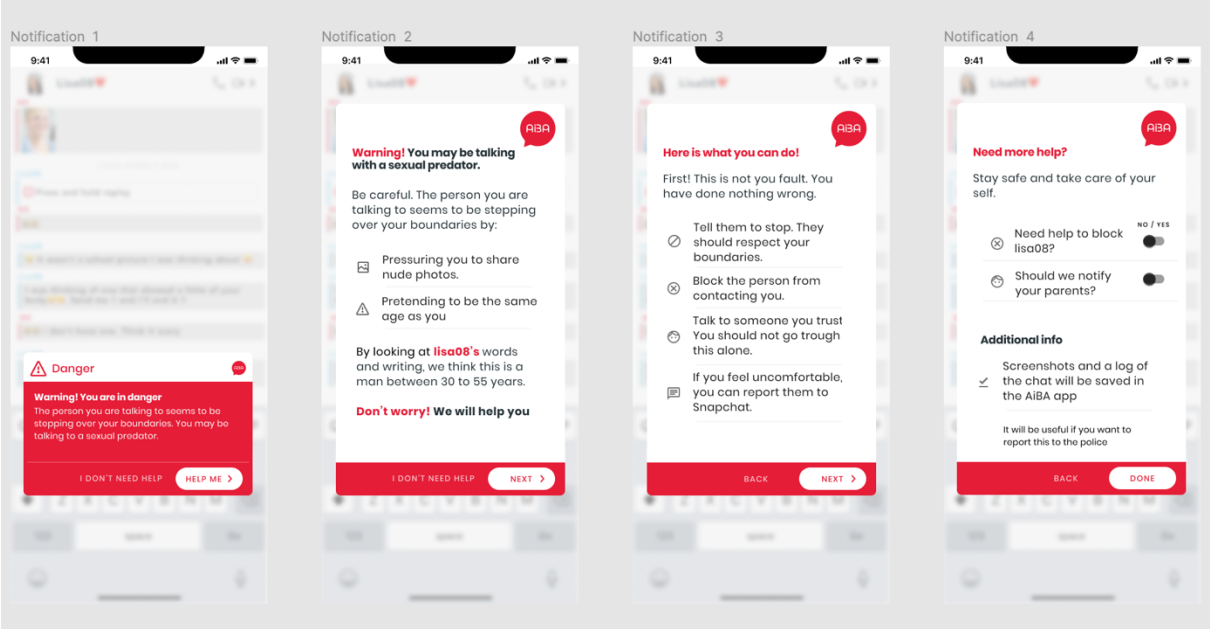


Figure 50 AiBA child warning prototype

4.4.2.3 AiBA parents notification

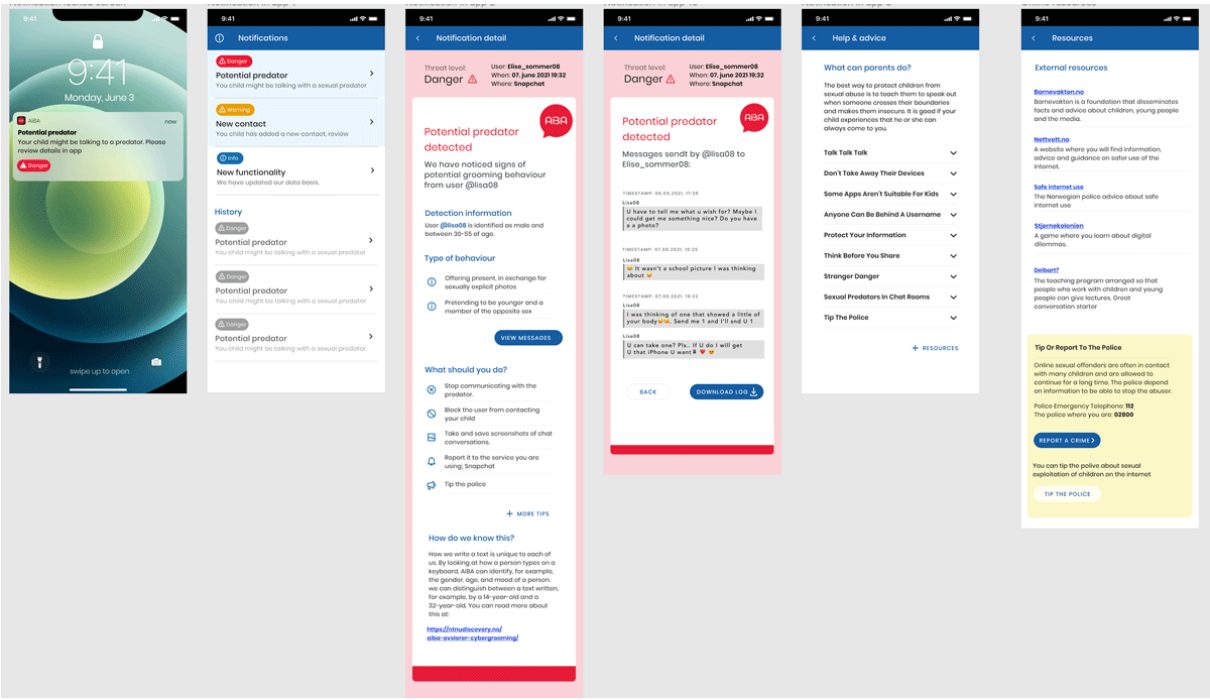


Figure 51 AiBA parents notification

4.5 Expert evaluation

Evaluating and refining results is an essential part of iterative and user-centered design. The purpose of the expert evaluation was to evaluate the usability of the warning design and notifications designed for the parents and the children in an AiBA application in accordance with the design principles and heuristics. To further improve the usability of the warning design and notifications designed for the AiBA child warning and AiBA parents notification.

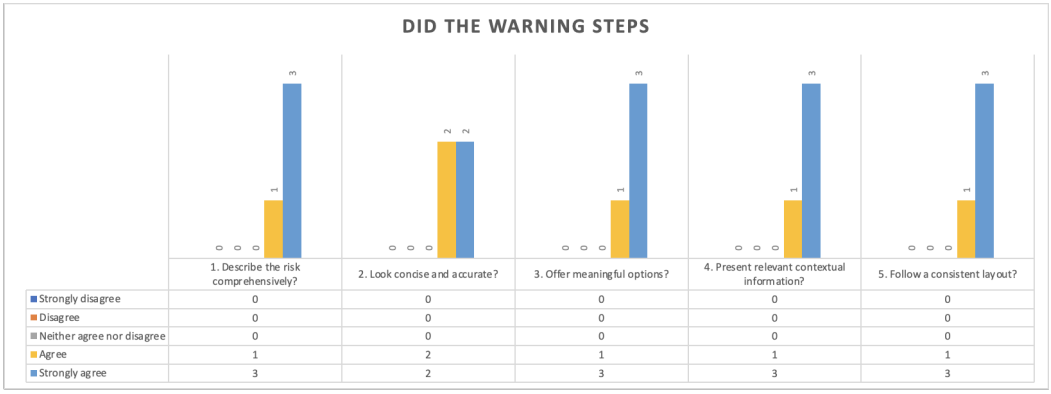
All of the experts that conducted the evaluation of the two prototypes are familiar with the term grooming. Out of the four experts three of them have kids.

4.5.1 Prototype: AiBA warning to children in chat

Imagine a system that gives you a warning about potential "grooming" in a chat. The system's goal is to protect the child and keep the parents informed of potential dangers. The experts were told to evaluate the following scenario: Your child is on Snapchat and is asked to share nude photos. The child then receives a warning about a potential grooming. The experts were told to evaluate the warning steps that the child received based on the criteria's below.

Did the warning steps:

1. Describe the risk comprehensively
2. Look concise and accurate
3. Offer meaningful options
4. Present relevant contextual information
5. Follow a consistent layout?



	1. Describe the risk comprehensively?	2. Look concise and accurate?	3. Offer meaningful options?	4. Present relevant contextual information?	5. Follow a consistent layout?
Strongly disagree	0	0	0	0	0
Disagree	0	0	0	0	0
Neither agree nor disagree	0	0	0	0	0
Agree	1	2	1	1	1
Strongly agree	3	2	3	3	3

Figure 52 experts were told to evaluate the warning steps

As seen in Figure 52 all the experts either agreed or strongly agreed to the five statements.

The second task for the experts was to evaluate the design-specific heuristics which were established to evaluate and combined with other relevant design guidelines.

To what degree (on a scale from 1-5 where 1 is Not at all and 5 Very much) did youFigure 53:

- Understand the used terms and language?
- Understand the navigation?
- Feel in control when viewing the warning?
- Feel lost or in need of help?
- Rate the consistency of the design?
- Think the buttons and interaction elements were recognisable?
- Get appropriate feedback on your actions?
- Think the warnings concentrated on relevant information and design elements?

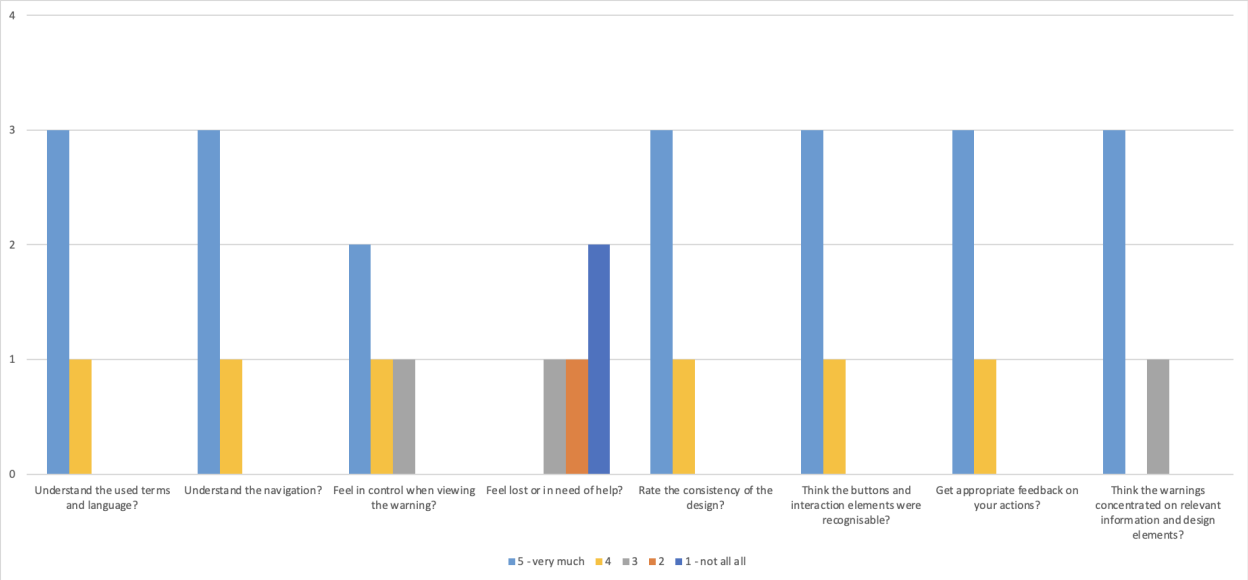


Figure 53 results from the heuristic evaluation AiBA warning to children

4.5.1.1 Were there any actions that did not work as expected?

- I didn't realise that screenshots were being taken - not necessarily bad, but I was unaware. Back button is not interactive in some places, but that is the prototype build and not the design I guess. I wonder about what the default positions of some of the later switches should be - should some actions be "suggested" by having the default position set to "on"?
- It was unclear how to get back to Snapchat and close the dialogue. On the “stay safe” final screen, there should be a button closing the Aida dialogue that returns

you to the app. I'm not sure what it should say, but maybe something more encouraging than "I'm ready to return to Snapchat"?

4.5.1.2 Other comments

- When it says "It would be useful if you would like to report this to the police" – I find this unclear. You should have a button that they can just push and the police will get the information in the app including the screenshots of the messages the child has received. This I think would increase the chance of them notifying the police. And the child could also choose to be anonymous when contacting the police. The main issue is to report Lisa08 to the police so this 30-55 year-old male can be identified and stopped in his attempts to groom children..
- High impact and easily understood graphical elements. Only thought is that when you use red to this extent, there is nowhere left to go (nothing looks high impact after 2 screens, you adjust to the colour scheme).
- The design appears friendly and unthreatening, while also communicating professionalism and trust. I really liked the visual design.

4.5.2 Prototype: AiBA warning to parents

Scenario: You as a parent receive a notification on your mobile that your child may be exposed to grooming from an online sexual abuser. Look at the prototype and evaluate the warning steps. The evaluation criteria is the same as for the children's prototype.

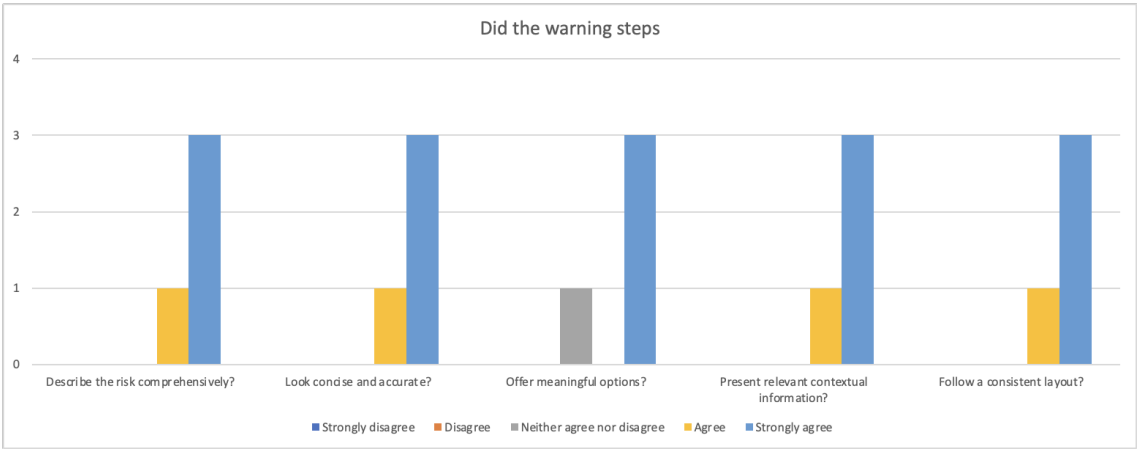


Figure 54 Evaluation of the warning steps

As seen in Figure 54, all the experts either agreed or strongly agreed to the five statements, except on the statement "offer meaningful options" - here one expert neither agrees nor disagrees.

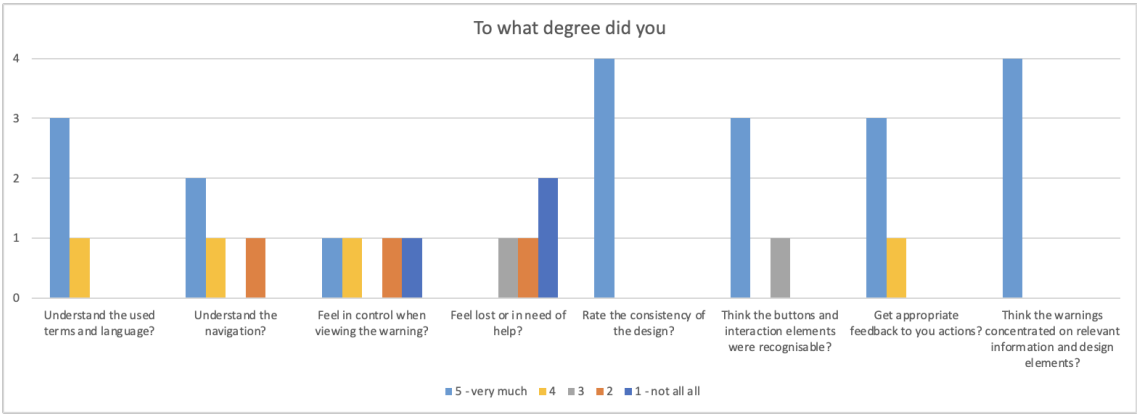


Figure 55 Heuristic evaluation AiBA warning to parents

4.5.2.1 Do you have any other comments?

- I would love to have my soon to be 12 year-old son use this app. He recently got a Snapchat. I would like to get warnings from Aiba if some predator could potentially trick and eventually hurt him.
- Remember to allow users to close or exit windows whenever they want - or even save for later. This is distressing information to learn and so users might want to hold it off until an appropriate moment when they can leave a meeting or pull the car over. There is a primary interaction button missing at the bottom of the initial parent information page, I don't know what it is, but to have a dead-end is a bit strange.
- Some of the language is culturally Norwegian (such as "moral index finger") and needs a cultural translation. Some text sections lack line space (enter) between sections. I would consider using bold font on single words to aid the parent in understanding main information points (f.ex in the section What can parents do?). I did not feel in control of the situation as I felt Aida very accurately communicated to me the seriousness of the situation. I am glad it felt uncomfortable even in a user test. Parents should feel really upset and take action in this case, and the prototype really conveys this and appropriate actions to take. I really liked the "don't take their device" section. Was a version of this Help and advice section in the child's UI?

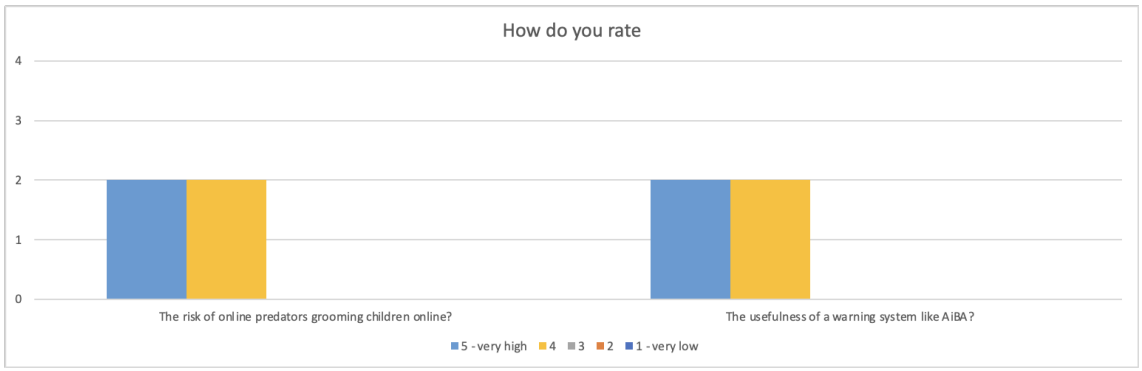


Figure 56 All the expert rate the risk of online grooming as very high or high, they also rate the usefulness of the AiBA app as high or very high

4.6 Final prototypes

Through our iterative process from paper ideation and paper prototyping to final prototypes the aim was to map out all the possible objectives and compare them to the base objectives; design user friendly warnings for children and their parents.

After reviewing the expert evaluations several changes were made to the prototypes.

4.6.1 The AiBA app prototype

Link to the

The AiBA app

4.6.2 Notification from AiBA to parents prototype

Link to the

AiBA parent notification prototype

4.6.3 Notification from AiBA to child prototype

Link to the

AiBA child warning prototype

5 Discussion and conclusion

The literature review in Chapter 2, the practical application of research methods and the design of suggestions visualised in the prototypes in Chapter 4 have contributed to answering the research questions of this thesis. The main research question "*Can we design a way to warn children in live chat room conversations that they are/might be talking to a sexual predator*?" has been answered positively through the practical design visualised in the AiBA child warning prototype. In addition, the prototype also suggests a way to inform the child about the risk profile and the sexual predator's suspicious behaviour in a chat situation. It also points to particular parts of the conversation that are suspicious. Supporting the hypothesis that if we alert and advise the children in a chat that they might be talking to a sexual predator, it will enable them to, depending on their age, either notify a trusted adult or take the necessary steps to stop, block and/or report the incident.
Furthermore, the subquestion " How do we communicate risk in a chat conversation and influence kids' behaviour in real-time" is featured in the AiBA child warning prototype through clear warnings and suggested actions for the child in real-time. Supporting this is the WHO definition that the "ultimate purpose of risk communication is the exchange of real-time information that enables people to make informed decisions to protect themselves and their loved ones" (WHO, 2015). In addition a well-designed warning message should attract attention at the right time, which in this case is in "real-time" as the child is in the process of being groomed. Previous research by (Petelka, Zou and Schaub, 2019) showed that warning placement and forcing interaction with the warning improves warning adherence.
Utilising a future development of an AiBA automated tool or app can "help the parents (or guardians) monitor and keep their children safe from online predators" by flagging potentially dangerous situations and providing guidance to parents. This is partly visualised in the AiBA app prototype. As a result of feedback from the children and parents, monitoring levels differentiated by age and applicable rules and regulations such as GDPR including age restrictions imposed by vendors, were introduced in the AiBA app prototype. The subquestion "how can design notifications that inform the parents (or guardians) about a potential grooming situation?" has been answered positively through the practical design visualised in the AiBA parents notification prototype.

Previous studies by (Ey and Glenn Cupit, 2011) have shown that although the children identified several risk categories when presented with potentially dangerous Internet interactions, almost half could not identify the associated risks.
This adheres to the importance of the future implementation of an AiBA application as such a solution, as shown in the AiBA warning for children, could assist the children in this task. Another important issue that this solution could support the children with, is to help them determine the age and gender of the people they are talking to online, this is

especially important since we know that some sexual predators use a fake profile to initiate contact with children by pretending to be a child themselves.

In the AIBA project, a warning will be sent once the system detects behavioural patterns that indicate grooming tactics. Pairing a notification with a confidence rating and brief description of why the automated system has flagged a message could serve to avoid the escalation of less critical types of behaviour. The participants in our research raised concerns regarding how reliable these detections are. Some of the children in our focus groups felt it was very important to know how much they could trust such a system. As people are more likely to behave consistently with a warning sign or label if they believe the danger is considerable (Lehto, 2000), iconography and text should clearly signal the gravity of potentially serious situations. The children requested that the solution should incorporate clear, unambiguous, visual indication of when and why they are being actively monitored or blocked from communicating with someone. A key goal of a warning design is to reach their target audience – in this case children and parents. Further testing of the warning design from this thesis is therefore needed.

Based on an overview of the empirical literature on warning guidelines and evaluation approaches (Wogalter, Conzola and Smith-Jackson, 2002), personal factors include age, gender, cultural background, product or task familiarity and training, and individual differences must be carefully considered when designing a warning.

After comparing the findings with the existing literature, there was a clear history of child protection on the internet. However, the need to raise awareness and protection is as dominant today as they have been since the number of children falling victim to online grooming and sexual abuse is only increasing. In recent years, awareness of child grooming has increased due to high profile cases being discussed in the media such as “project darkroom” that was mentioned in this thesis’ background chapter.

The research for this thesis discovered some concerning trends regarding family communication indicating that a lot of teenagers (48 percent) don’t want to talk to their parents about negative experiences online. It seems that even though the children mostly don’t find it difficult to talk about this topic with their parents, a majority state that they are able to handle difficult situations themselves. The survey found that 84 percent of the children have had contact with strangers online which is considered risky behaviour. This confirms the need for a monitoring tool such as a potential AiBA app as the children themselves do not always have the cognitive maturity or a holistic understanding of the risks involved in their behaviour.

Previous research has shown that parents often underestimate teenagers’ exposure to sexual content. In general there is also a mismatch between what parents and children perceive as harmful. Parents and teens shared very different perceptions as parents tend to underestimate the frequency with which their teens experience online risks. This is also supported in our research as most of the parents feel they have an open and trusting relationship with their child at the same time as the teenagers state that parents are normally the last to know. This shows the importance of adopting a proactive process where parents actively engage in their children’s digital lives. Both children and

parents should also receive regular awareness training including updated information on technological trends, as it is often difficult for parents to keep up with these. Parents often deal with a sense of losing control, as they feel they lack the skills to deal with their child's media use. There are also huge differences in parents' knowledge level and assessment of the risk level.

Research also shows that parental concern regarding their children's safety online is high, stimulating a fair range of practices designed to make internet use safer for their children (Livingstone and Haddon, 2009). Teaching children how to use the internet safely and how to make informed decisions is an integral part of digital education, as children are aware of risks they may face online but they need to learn how to handle them. Our research discovered that the most popular form of mediation used by the parents is active mediation, which means that the parents talk with their children about particular media activities or share these activities with them, which in turn will improve the children's ability to handle these risks. Furthermore, our research has shown that parental support and the creation of clear expectations is desired by both parents and children. Social media apps should provide parents and children with opportunities for dialogue - such as videos, that a parent and child can watch together and discuss prompting active discussion between parents and child. This is also a need expressed by the parents in our research. It is vital to educate parents and teens on digital online safety that includes how to help teens resolve negative online experiences.

The parents in our research would like to implement some form of technical mediation, but not all felt they had the competence to do so. So the need for a user friendly solution demanding a minimum effort from the parents to set up and maintain is great. Mobile applications developed to promote online safety for children are underutilised and rely heavily on parental control. Most parental controls today focus on the protection of children by limiting time spent online, filter web content, block apps and block internet access. These restrictive measures have some drawbacks and advocate one-sided focus on protection. Punishments do not teach children values or norms, and increase the likelihood of secret misbehaviour. Joint engagement and involvement is key, this is supported in the results from the focus groups and the survey as children are willing to be monitored as long as they are given the opportunity to voice their opinion and some freedom to influence the level of monitoring. It is important to limit the child's fear of increased restrictions and loss of access to digital devices.

The questions about privacy was one of the more difficult issues to talk about. For some of the parents, keeping their children safe outweighs their children's right to privacy. There seems to be a mismatch between the parent's need to keep their children safe and teens' desire to uphold personal privacy. On the other hand some of the parents think that in today's society we know too much about our children and that they should be given the opportunity to have "good secrets" without their parents interference and constant monitoring. This topic would need to be thoroughly investigated before implementing a solution as there are many rules, regulations and ethical considerations that would need to be addressed.

The AiBA project is in a unique situation as there is great need for this kind of service, as stated by one of the parents in our interviews " *if I had an app like that where I could actually follow and see what they're doing and see if there's any suspicious activity going on in one of their apps, I would buy it for thousands of kroner. Because I really can't emphasize enough how important I think it is.*" The automated risk detection and machine learning provide the potential for real-time filtering and intervention.

5.1 Limitations

The scope of a Master's thesis does not allow for the collection of long term results as this is a very time consuming process. It was very unfortunate a useability test of the prototypes with the target audience parents and children, could not be completed as this would have given valuable insight and enabled further development of the digital prototypes. While the experts were able to identify a number of relevant design and usability issues, conducting usability tests with real users would have been able to reveal if the proposed design would appeal to the users and reveal further usability issues.
The digital barrier of having to conduct online interviews may have limited the amount of parents that volunteered to participate. Had we been able to conduct face to face interviews we might have been able to interview more parents, but this is just speculation.

5.2 Further research

Online abuse is a societal problem in Norway. Being sexually abused can be traumatic. There is a need for more knowledge about the dynamics of online sexual exploitation of children. There is a need for knowledge about people who commit criminal internet-related sexual exploitation of children to put in place appropriate preventive measures. There is a need to understand more about the importance of the internet for abusive behaviour and the consequences of online abuse for victims.
Studies have previously been conducted to examine warning design for adults, but there is little data to establish recommendations for children. The data gathered in our research for this thesis mainly covers middle school children, the warning design for younger children, primary school, should be further investigated.

Regarding the AiBA application, the designed prototypes can be used as a basis for the development of an interface for the finished system. Some of the groundwork for the design of effective warning messages within the AiBA application has been laid through this thesis and can be further amended. In addition, the design of warning messages from this thesis should be combined by the previous work
described in the thesis "Risk Communication: Sexual Predators in Chat Environments" incorporated in the AiBA project (Raffel, 2020). In addition, it would be useful to test the suggested solution on children to see if they understand the language and would act on the warning displayed. It would also be interesting to find out what the child's preferred action would be; block, notify parent, or report to police or possibly a combination of these.

6 References

Aanerød, L. and Mossige, S (2018) *Nettovergrep mot barn i Norge 2015–2017*. 10/18. OsloMet. Available at: https://fagarkivet.oslomet.no/handle/20.500.12199/5127 (Accessed: 4 October 2020).

Adobe (no date) *Color Accessibility*, *Adobe Color*. Available at: https://color.adobe.com/nb/create/color-accessibility (Accessed: 4 June 2021).

Amran, A., Zaaba, Z. F. and Singh, M. K. M. (2018) 'Habituation effects in computer security warning', *Information Security Journal: A Global Perspective*, pp. 192–204. doi: 10.1080/19393555.2018.1505008.

Annansingh, F. and Veli, T. (2016) 'An investigation into risks awareness and e-safety needs of children on the internet', *Interactive Technology and Smart Education*, pp. 147–165. doi: 10.1108/itse-09-2015-0029.

Apple Inc (no date) *Alerts - Views - iOS - Human Interface Guidelines - Apple Developer*. Available at: https://developer.apple.com/design/human-interface-guidelines/ios/views/alerts/ (Accessed: 5 June 2021).

Archer, T. (1993) 'Focus Groups for Kids', *Journal of Extension*, 31(1). Available at: https://www.joe.org/joe/1993spring/tt2.php (Accessed: 31 October 2020).

Aven, T. (2019a) *Risiko*, *Store norske leksikon*. Available at: https://snl.no/risiko (Accessed: 13 May 2021).

Aven, T. (2019b) *Risikokommunikasjon*, *Store norske leksikon*. Available at: https://snl.no/risikokommunikasjon (Accessed: 13 May 2021).

Badillo-Urquiola, K. A. *et al.* (2019) 'Stranger Danger!: Social Media App Features Co-designed with Children to Keep Them Safe Online', in *IDC '19: Proceedings of the 18th ACM International Conference on Interaction Design and ChildrenJune 2019*. *18th ACM International Conference on Interaction Design and Children*, Association for Computing Machinery New York NY United States, p. Pages 394–406. doi: 10.1145/3311927.3323133.

Bakken, A. (2019) *Ungdata 2019. Nasjonale resultater*. NOVA, Oslomet. Available at: http://hdl.handle.net/20.500.12199/2252 (Accessed: 21 October 2020).

Bashir, M. S. and Farooq, A. (2019) 'EUHSA: Extending Usability Heuristics for Smartphone Application', *IEEE Access*, pp. 100838–100859. doi: 10.1109/access.2019.2923720.

Bauer, L. *et al.* (2013) *Warning Design Guidelines*, *Cylab*. Available at: http://www.cylab.cmu.edu/research/techreports/2013/tr_cylab13002.html (Accessed: 3 January 2021).

Bauer, L., Bravo-Lillo, C. and Cranor, L. (2013) 'Warning design guidelines', *'^'eds.'): Book Warning*. researchgate.net. Available at: https://www.researchgate.net/profile/Cristian-Bravo-Lillo/publication/258499093_Warning_Design_Guidelines/links/5b912dcb92851c6b7ecb6721/Warning-Design-Guidelines.pdf.

Baxter, K., Courage, C. and Caine, K. (2015) *Understanding Your Users: A Practical Guide to User Research Methods*. Morgan Kaufmann. Available at: https://play.google.com/store/books/details?id=l9-cBAAAQBAJ.

Braun, C. C. and Silver, N. C. (1995) 'Interaction of signal word and colour on warning labels: differences in perceived hazard and behavioural compliance', *Ergonomics*, 38(11), pp. 2207–2220. doi: 10.1080/00140139508925263.

Breck's Last Game (2019). Available at: https://www.youtube.com/watch?v=hZIYSCE-ZjY (Accessed: 9 May 2021).

Bufdir (2019) *Nettovergrep*, *https://www.bufdir.no/*. Available at: https://bufdir.no/vold/TryggEst/Overgrep/Nettovergrep/ (Accessed: 23 May 2021).

Burgess, A. W. and Hartman, C. R. (2018) 'On the Origin of Grooming', *Journal of Interpersonal Violence*, pp. 17–23. doi: 10.1177/0886260517742048.

Cao, J. (2016) *What Is a Prototype: A Guide to Functional UX*. Available at: https://www.uxpin.com/studio/blog/what-is-a-prototype-a-guide-to-functional-ux/ (Accessed: 7 June 2021).

Chapanis, A. (1994) 'Hazards associated with three signal words and four colours on warning signs', *Ergonomics*, pp. 265–275. doi: 10.1080/00140139408963644.

Coyne, S. M. *et al.* (2017) 'Parenting and Digital Media', *Pediatrics*, 140(Suppl 2), pp. S112–S116. doi: 10.1542/peds.2016-1758N.

Craven, S., Brown, S. and Gilchrist, E. (2006) 'Sexual grooming of children: Review of literature and theoretical considerations', *Journal of Sexual Aggression*, pp. 287–299. doi: 10.1080/13552600601069414.

Davis, K., Dinhopl, A. and Hiniker, A. (2019) '"Everything's the Phone"', *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. doi: 10.1145/3290605.3300457.

Design Council (2015) *What is the framework for innovation? Design Council's evolved Double Diamond*, *Design Council*. Available at: https://www.designcouncil.org.uk/news-opinion/what-framework-innovation-design-councils-evolved-double-diamond (Accessed: 2 November 2020).

Egelman, S. and Schechter, S. (2013) 'The Importance of Being Earnest [In Security Warnings]', *Financial Cryptography and Data Security*, pp. 52–59. doi: 10.1007/978-3-642-39884-1_5.

Elliot, A. J. and Maier, M. A. (2012) 'Color-in-Context Theory', in *Advances in Experimental Social Psychology*. Academic Press, pp. 61–125. doi: 10.1016/B978-0-12-394286-9.00002-0.

Engebretsen, L. N. (2020) *Unge blir utsatt for nettovergrep flere ganger – av ulike gjerningsmenn*. NRK. Available at: https://www.nrk.no/osloogviken/xl/unge-blir-utsatt-for-nettovergrep-flere-ganger-_-av-ulike-gjerningsmenn-1.15001757 (Accessed: 8 May 2021).

Er det meldeplikt til NSD for anonyme spørreundersøkelser i Nettskjema? (2020) *uio.no*. Available at: https://www.uio.no/tjenester/it/adm-app/nettskjema/mer-om/personvern/meldeplikt.html (Accessed: 12 December 2020).

EU Kids Online (no date) *London School of Economics and Political Science*. Available at: http://www.eukidsonline.net/ (Accessed: 13 May 2021).

Europol (no date) *COVID-19: Child sexual exploitation*, *https://www.europol.europa.eu/*. Available at: https://www.europol.europa.eu/covid-19/covid-19-child-sexual-exploitation (Accessed: 10 May 2021).

Ey, L.-A. and Glenn Cupit, C. (2011) 'Exploring young children's understanding of risks associated with Internet usage and their concepts of management strategies', *Journal of Early Childhood Research*, pp. 53–65. doi: 10.1177/1476718x10367471.

Few, S. (2013) *Information Dashboard Design: Displaying Data for At-a-glance Monitoring*. Available at: https://books.google.com/books/about/Information_Dashboard_Design.html?hl=&id=7k0EnAEACAAJ.

Fischhoff, B. (2012) *Communicating Risks and Benefits: An Evidence Based User's Guide*. Government Printing Office. Available at:

https://books.google.com/books/about/Communicating_Risks_and_Benefits.html?hl=&id=lLA2vrcQN_AC.

Fleming, M. J. *et al.* (2006) 'Safety in Cyberspace', *Youth & Society*, pp. 135–154. doi: 10.1177/0044118x06287858.

Folkehelseinstituttet (2020) *Covid-19-epidemien: Veileder for hjemmekontor og arbeidsplasser*, *www.fhi.no*. Available at: https://www.fhi.no/publ/2020/covid-19-epidemien-veileder-for-hjemmekontor-og-arbeidsplasser/ (Accessed: 2 January 2021).

Ghosh, A. K. et al. (2018) 'Safety vs. Surveillance', Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems. doi: 10.1145/3173574.3173698.

Gibson, F. (2007) 'Conducting focus groups with children and young people: strategies for success', *Journal of Research in Nursing*, 12(5), pp. 473–483. doi: 10.1177/1744987107079791.

Google (no date) *Share and engage with the Design Sprint Community*. Available at: https://designsprintkit.withgoogle.com/methodology/phase3-sketch/crazy-8s (Accessed: 7 June 2021).

Gray, D., Brown, S. and Macanufo, J. (2010) *Gamestorming: A Playbook for Innovators, Rulebreakers, and Changemakers*. O'Reilly Media. Available at: https://books.google.com/books/about/Gamestorming.html?hl=&id=E2C6wAEACAAJ.

Green, M. (2013) *Safety Hierarchy: Design Vs. Warnings*, *http://www.visualexpert.com*. Available at: https://www.visualexpert.com/Resources/safetyhierarchy.html (Accessed: 3 January 2021).

GROOMING (no date). Lexico Dictionaries. Available at: https://www.lexico.com/definition/grooming (Accessed: 9 May 2021).

Guest, G., Namey, E. and McKenna, K. (2017) 'How Many Focus Groups Are Enough? Building an Evidence Base for Nonprobability Sample Sizes', *Field Methods*, pp. 3–22. doi: 10.1177/1525822x16639015.

Gulbrandsen, A. (2020) *Informasjonssikkerhet og risikovurdering for Nettskjema*, *uio.no*. Available at: https://www.uio.no/tjenester/it/adm-app/nettskjema/mer-om/informasjonssikkerhet/index.html (Accessed: 12 December 2020).

Hafstad, G. S. and Augusti, E. M. (2020) Barn, ungdom og koronakrisen. En landsomfattende undersøkelse av vold, overgrep og psykisk helse blant ungdom i Norge våren 2020: Delrapport 1 av 3. 2. Nasjonalt kunnskapssenter om vold og traumatisk

stress. Available at: https://www.nkvts.no/content/uploads/2020/12/Rapport_2-20.pdf (Accessed: 8 May 2021).

Hagen, T. A. (2020) *Politiet forteller hvordan du kan avsløre en nettovergriper*. NRK. Available at: https://www.nrk.no/trondelag/seksuelle-overgrep-mot-barn-pa-internett_-slik-gar-barneovergriperne_frem-pa-nett-1.15249347 (Accessed: 9 December 2020).

Hva er Nettskjema (2020) *uio.no*. Available at: https://www.uio.no/tjenester/it/adm-app/nettskjema/mer-om/index.html (Accessed: 12 December 2020).

Interaction Design Foundation (2020) *Ideas for Conducting UX Research with Children*, *Interaction Design Foundation*. Available at: https://www.interaction-design.org/literature/article/ideas-for-conducting-ux-research-with-children (Accessed: 30 October 2020).

Interaction Design Foundation (no date) *What are Design Guidelines?*, *Interaction Design Foundation*. Available at: https://www.interaction-design.org/literature/topics/design-guidelines (Accessed: 15 May 2021).

Internet Watch Foundation (2021) *Child Sexual Abuse Online Trends & Data in 2020 - IWF Annual Report 2020*. IWF. Available at: https://annualreport2020.iwf.org.uk/ (Accessed: 26 April 2021).

Intro til universell utforming (no date). Available at: https://www.uutilsynet.no/veiledning/intro-til-universell-utforming/238 (Accessed: 5 June 2021).

Introduction to Understanding WCAG 2.0 (no date). Available at: https://www.w3.org/TR/UNDERSTANDING-WCAG20/intro.html (Accessed: 5 June 2021).

ISMP (2019) *Your attention please… Designing effective warnings*, *Institute for Safe Medication Practices*. Available at: https://www.ismp.org/resources/your-attention-please-designing-effective-warnings-0 (Accessed: 18 May 2021).

ISO (the International Organization for Standardization) (2016) *ISO 3864 Graphical symbols — Safety colours and safety signs — Part 2: Design principles for product safety labels*. ISO 3864. Available at: https://www.iso.org/obp/ui/#iso:std:iso:3864:-2:ed-2:v1:en (Accessed: 15 May 2021).

IWF (2021) *Campaign launches as new report finds girls at worsening risk of grooming from sexual predators online*, *Internet Watch Foundation*. Available at: https://www.iwf.org.uk/news/campaign-launches-new-report-finds-girls-worsening-risk-grooming-sexual-predators-online (Accessed: 26 April 2021).

Janssens, A. *et al.* (2015) 'Parents' and Adolescents' Perspectives on Parenting: Evaluating Conceptual Structure, Measurement Invariance, and Criterion Validity', *Assessment*, 22(4), pp. 473–489. doi: 10.1177/1073191114550477.

Justisdepartementet (2007) *Forebygging av internettrelaterte overgrep mot barn*. Justisdepartementet. Available at: https://www.regjeringen.no/globalassets/upload/kilde/jd/nyh/2007/0012/ddd/pdfv/305458-faremo-rapport_30.1.2007.pdf (Accessed: 4 October 2020).

Kaley, A. (2018) *Match Between System and Real World: 2nd Usability Heuristic Explained*. Available at: https://www.nngroup.com/articles/match-system-real-world/ (Accessed: 7 June 2021).

Koussa, N. (no date) *Not 'mini adults': Communicating risk with children and young people*, *Me first*. Available at: https://www.mefirst.org.uk/not-mini-adults-communicating-risk-with-children-and-young-people/ (Accessed: 13 May 2021).

Kringstad, K. (2020) *Gjengangerne: Hvorfor har ikke Stian stoppet å begå seksuelle overgrep mot barn?* NRK. Available at: https://www.nrk.no/trondelag/xl/gjengangerne_-hvorfor-har-ikke-stian-stoppet-a-bega-seksuelle-overgrep-mot-barn_-1.15205833 (Accessed: 21 December 2020).

Kripos (2019a) *Det heter ikke barneporno og saken som fortsatt gir ham frysninger*. Spotify. Available at: https://open.spotify.com/episode/1FP50XYevHlrnBWET53HZP (Accessed: 25 May 2021).

Kripos (2019b) *Online sexual exploitation of children and young people*. Kripos. Available at: https://www.politiet.no/globalassets/04-aktuelt-tall-og-fakta/seksuelle-overgrep-mot-barn/online-sexual-exploitation-of-children-and-young-people.pdf (Accessed: 3 October 2020).

Kripos (no date) *Barn og unges nettbruk*. Available at: https://www.politiet.no/rad/trygg-nettbruk/barn-og-unges-nettbruk/ (Accessed: 21 December 2020).

Kulturdepartementet (2021) 'Varsler nasjonal strategi for trygg digital oppvekst'. regjeringen.no. Available at: https://www.regjeringen.no/no/aktuelt/varsler-nasjonal-strategi-for-trygg-digital-oppvekst/id2832509/ (Accessed: 21 March 2021).

KUMC (2021) *Universal Design and Accessibility*, *The University of Kansas*. Available at: https://www.kumc.edu/information-technology/teaching-and-learning-technologies/universal-design-and-accessibility.html (Accessed: 5 June 2021).

Langmajer, M. (2019) *10 Usability Heuristics Every Designer Should Know - UX Collective*, *UX Collective*. Available at: https://uxdesign.cc/10-usability-heuristics-every-designer-should-know-129b9779ac53 (Accessed: 6 June 2021).

Lanning, K. (2018) 'The Evolution of Grooming: Concept and Term', *Journal of interpersonal violence*. SAGE Publications Inc, 33(1), pp. 5–16. doi: 10.1177/0886260517742046.

Lanning, K. V. (2010) *Child Molesters: A Behavioral Analysis for Professionals Investigating the Sexual Exploitation of Children*. Available at: https://books.google.com/books/about/Child_Molesters.html?hl=&id=QFOOAQAACAAJ.

Leedy, P. D. and Ormrod, J. E. (2015) *Practical Research: Planning and Design, Global Edition*. Pearson Higher Ed. Available at: https://books.google.com/books/about/Practical_Research_Planning_and_Design_G.html?hl=&id=2v0wCwAAQBAJ.

Lehto, M. R. (2000) 'Designing warning signs and warning labels: Part II – Scientific basis for initial guidelines', *Ergonomics Guidelines and Problem Solving*, pp. 257–280. doi: 10.1016/s1572-347x(00)80021-x.

Lidwell, W., Holden, K. and Butler, J. (2010) The Pocket Universal Principles of Design: 125 Ways to Enhance Usability, Influence Perception, Increase Appeal, Make Better Design Decisions, and Teach through Design. Rockport Publishers. Available at: https://play.google.com/store/books/details?id=l0QPECGQySYC.

Livingstone, S. and Haddon, L. (2009) 'EU Kids Online: final report 2009'. unknown. Available at: http://dx.doi.org/ (Accessed: 24 March 2021).

Livingstone, S. and Ólafsson, K. (2011) 'Risky communication online'. London, UK: LSE London, EU Kids Online (EU Kids Online), p. 3. Available at: http://eprints.lse.ac.uk/33732/1/Risky%20communication%20online%20%28lsero%29.pdf (Accessed: 5 January 2021).

Lundgren, R. E. and McMakin, A. H. (2018) *Risk Communication: A Handbook for Communicating Environmental, Safety, and Health Risks*. John Wiley & Sons. Available at: https://books.google.com/books/about/Risk_Communication.html?hl=&id=V9djDwAAQBAJ.

McCarty, C. *et al.* (2011) 'Perceived Safety and Teen Risk Taking in Online Chat Sites', *Cyberpsychology, Behavior, and Social Networking*, 14(3). doi: 10.1089/cyber.2010.0050.

McDougald, B. R. and Wogalter, M. S. (2014) 'Facilitating pictorial comprehension with color highlighting', *Applied ergonomics*, 45(5), pp. 1285–1290. doi: 10.1016/j.apergo.2013.05.008.

McNally, B. *et al.* (2018) 'Co-designing Mobile Online Safety Applications with Children', *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. doi: 10.1145/3173574.3174097.

Medietilsynet (2020) *Barn og medier-undersøkelsen*. Available at: https://www.medietilsynet.no/barn-og-medier/barn-og-medier-undersokelsen/ (Accessed: 3 October 2020).

Medietilsynet (2021) *Medietilsynet starter arbeidet med nasjonal strategi for trygg digital oppvekst*. Available at: https://www.medietilsynet.no/om/aktuelt/medietilsynet-starter-arbeidet-med-nasjonal-strategi-for-trygg-digital-oppvekst/ (Accessed: 21 March 2021).

Medietilsynet (no date) *Barn og sosiale medier: Dette bør du vite*, *Medietilsynet*. Available at: https://www.medietilsynet.no/barn-og-medier/sosiale-medier/ (Accessed: 1 November 2020).

Mossige, S. and Stefansen, K. (2007) *Vold og overgrep mot barn og unge*. doi: 10.7577/nova/rapporter/2007/20.

National Research Council (US) (1989) 'Purposes of Risk Communication and Risk Messages', in Committee on Risk Perception and Communication (ed.) *Improving Risk Communication*. National Academies Press (US). Available at: https://www.ncbi.nlm.nih.gov/books/NBK218575/ (Accessed: 14 May 2021).

Ness, K. K. (2018) *Vil avsløre overgripere på nett*. NRK. Available at: https://www.nrk.no/viten/vil-avslore-overgripere-pa-nett-1.14002040 (Accessed: 15 May 2021).

Ng, A. W. Y. and Chan, A. H. S. (2018) 'Color associations among designers and non-designers for common warning and operation concepts', *Applied ergonomics*, 70, pp. 18–25. doi: 10.1016/j.apergo.2018.02.004.

Ni Bhroin, N. and Rehder, M. (2018) Digital Natives or Naïve Experts? Exploring how Norwegian children (aged 9-15) understand the Internet. EU Kids Online. doi: 10.1080/136911808026354.

Nielsen, J. (1994) *Heuristic Evaluation: How-To: Article by Jakob Nielsen*. Available at: https://www.nngroup.com/articles/how-to-conduct-a-heuristic-evaluation/ (Accessed: 26 April 2021).

Nielsen, J. (2010) *Mental Models and User Experience Design*, *Nielsen Norman Group*. Available at: https://www.nngroup.com/articles/mental-models/ (Accessed: 5 May 2021).

Nielsen, J. (2020) *10 Usability Heuristics for User Interface Design*. Available at: https://www.nngroup.com/articles/ten-usability-heuristics/ (Accessed: 4 June 2021).

Norwegian National Committees for Research Ethics (2014) *General guidelines for research ethics*, *https://www.forskningsetikk.no/*. Available at: https://www.forskningsetikk.no/en/guidelines/general-guidelines/ (Accessed: 15 November 2020).

Nowell, L. S. *et al.* (2017) 'Thematic Analysis', *International Journal of Qualitative Methods*, p. 160940691773384. doi: 10.1177/1609406917733847.

NTNU (no date) *The AiBA solution*, *AiBA*. Available at: https://aiba.ai/ (Accessed: 15 December 2020).

Okabe, M. and Ito, K. (2008) *Color Universal Design (CUD) / How to make figures and presentations that are friendly to Colorblind people*. Available at: https://jfly.uni-koeln.de/color/#convert (Accessed: 5 June 2021).

Oppenheim, M. (2021) 'Girls aged 11-13 "more at risk of online grooming than ever before"', *The Independent*, 21 April. Available at: https://www.independent.co.uk/news/uk/home-news/stalkerware-spyware-apps-coronavirus-domestic-abuse-b1835237.html (Accessed: 7 May 2021).

Otterlei, S. S. (2016) *«Dark Room»-ledelsens råd: Slik kan seksuelle overgrep mot barn forebygges*. NRK. Available at: https://www.nrk.no/vestland/_dark-room_-ledelsens-rad_-slik-kan-seksuelle-overgrep-mot-barn-forebygges-1.13237526 (Accessed: 18 May 2021).

Petelka, J., Zou, Y. and Schaub, F. (2019) 'Put Your Warning Where Your Link Is: Improving and Evaluating Email Phishing Warnings', in *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. *CHI '19: CHI Conference on Human Factors in Computing Systems Glasgow Scotland Uk May, 2019*, Association for Computing MachineryNew YorkNYUnited States, pp. 1–15. doi: 10.1145/3290605.3300748.

Pollack, D. and MacIver, A. (2015) 'Understanding Sexual Grooming in Child Abuse Cases'. American Bar Association. Available at: http://repository.yu.edu/handle/20.500.12202/4649 (Accessed: 15 November 2020).

Preece, J., Rogers, Y. and Sharp, H. (2015) *Interaction Design: Beyond Human-Computer Interaction*. John Wiley & Sons. Available at: https://books.google.com/books/about/Interaction_Design.html?hl=&id=n0h9CAAAQBAJ.

Raffel, L. (2020) *Risk Communication: Sexual Predators in Chat Environments*. Edited by Patrick Bours and Associate Professor Sashidharan Komandur. Master in Interaction Design. Norwegian University of Science and Technology (NTNU). Available at: https://paperpile.com/app/p/674414ee-9daf-054c-9580-4f735f00650c (Accessed: 13 May 2021).

RealStories (2018) *The Paedophile Next Door*. United Kingdom: Little Dot Studios Network. Available at: https://youtu.be/ClRxuu-Pd4Y (Accessed: 11 May 2021).

ReddBarna (2020a) - *Internett er et stort mørkt rom*. Available at: https://www.reddbarna.no/nyheter/-internett-er-et-moerkt-rom (Accessed: 4 January 2021).

ReddBarna (2020b) *Nettvett for barn og unge*. Available at: https://www.reddbarna.no/vart-arbeid/barn-i-norge/nettvett/ (Accessed: 31 May 2021).

Reddy, G. R. *et al.* (2020) 'The effects of redundancy in user-interface design on older users', *International Journal of Human-Computer Studies*, p. 102385. doi: 10.1016/j.ijhcs.2019.102385.

Riley, D. (2014) 'Mental models in warnings message design: A review and two case studies', *Safety Science*, pp. 11–20. doi: 10.1016/j.ssci.2013.07.009.

Schouten, A. P., Valkenburg, P. M. and Peter, J. (2007) 'Precursors and Underlying Processes of Adolescents' Online Self-Disclosure: Developing and Testing an "Internet-Attribute-Perception" Model', *Media Psychology*, pp. 292–315. doi: 10.1080/15213260701375686.

Schwenzer, K. J. (2008) 'Protecting vulnerable subjects in clinical research: children, pregnant women, prisoners, and employees', *Respiratory care*, 53(10), pp. 1342–1349. Available at: https://www.ncbi.nlm.nih.gov/pubmed/18811998.

Sherwin, K. (no date) *Usability Heuristic 5: Error Prevention (Video)*. Nielsen Norman Group. Available at: https://www.nngroup.com/videos/usability-heuristic-error-prevention/ (Accessed: 7 June 2021).

Silic, M. *et al.* (2017) 'Effects of Color Appeal, Perceived Risk and Culture on User□s Decision in Presence of Warning Banner Message', *Proceedings of the 50th Hawaii International Conference on System Sciences (2017)*. doi: 10.24251/hicss.2017.065.

Silic, M. and Cyr, D. (2016) 'Colour Arousal Effect on Users' Decision-Making Processes in the Warning Message Context', *HCI in Business, Government, and Organizations: Information Systems*, pp. 99–109. doi: 10.1007/978-3-319-39399-5_10.

Smahel, D. *et al.* (2020) 'EU Kids Online 2020: survey results from 19 countries'. London, UK: London School of Economics and Political Science. doi: 10.21953/lse.47fdeqj01ofo.

Society for Risk Analysis (2018) *The Risk Analysis Glossary*, *Society for Risk Analysis*. Available at: https://www.sra.org/wp-content/uploads/2020/04/SRA-Glossary-FINAL.pdf (Accessed: 13 May 2021).

Sylwander, K. R., Vervik, A.-K. and Greijer, S. (2021) *Online child sexual exploitation and abuse: A review of Norwegian case law*. ECPAT Norway. Available at: https://kommunikasjon.ntb.no/data/attachments/00868/4144151d-1ffc-40d9-874d-c86d75cf125c.pdf (Accessed: 10 May 2021).

Uhls, Y. T. and Robb, M. B. (2017) 'How Parents Mediate Children's Media Consumption', *Cognitive Development in Digital Contexts*, pp. 325–343. doi: 10.1016/b978-0-12-809481-5.00016-x.

W3C Web Accessibility Initiative (WAI) (no date) *Web Content Accessibility Guidelines (WCAG) Overview*. Available at: https://www.w3.org/WAI/standards-guidelines/wcag/ (Accessed: 5 June 2021).

Waterson, P. *et al.* (2012) 'Developing safety signs for children on board trains', *Applied ergonomics*, 43(1), pp. 254–265. doi: 10.1016/j.apergo.2011.05.012.

Waterson, P. and Monk, A. (2014) 'The development of guidelines for the design and evaluation of warning signs for young children', *Applied ergonomics*, 45(5), pp. 1353–1361. doi: 10.1016/j.apergo.2013.03.015.

Whittle, H. *et al.* (2013) 'A review of online grooming: Characteristics and concerns', *Aggression and Violent Behavior*, pp. 62–70. doi: 10.1016/j.avb.2012.09.003.

WHO (2015) 'General information on risk communication'. World Health Organization. Available at: https://www.who.int/risk-communication/background/en/ (Accessed: 14 May 2021).

'WHO | Responding to children and adolescents who have been sexually abused' (2019). World Health Organization. Available at: http://www.who.int/reproductivehealth/topics/violence/clinical-response-csa/en/ (Accessed: 30 November 2020).

Williams, R., Elliott, I. A. and Beech, A. R. (2013) 'Identifying Sexual Grooming Themes Used by Internet Sex Offenders', *Deviant behavior*, 34(2), pp. 135–152. doi: 10.1080/01639625.2012.707550.

Wilson, G., Maxwell, H. and Just, M. (2017) 'Everything's Cool: Extending Security Warnings with Thermal Feedback', in *Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems*. New York, NY, USA: Association for Computing Machinery (CHI EA '17), pp. 2232–2239. doi: 10.1145/3027063.3053127.

Winters, G. M., Jeglic, E. L. and Kaylor, L. E. (2020) 'Validation of the Sexual Grooming Model of Child Sexual Abusers', *Journal of child sexual abuse*, 29(7), pp. 855–875. doi: 10.1080/10538712.2020.1801935.

Wisniewski, P. et al. (2017) 'Parents Just Don't Understand', Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing. doi: 10.1145/2998181.2998236.

Wogalter, M. S., Conzola, V. C. and Smith-Jackson, T. L. (2002) 'Research-based guidelines for warning design and evaluation', *Applied ergonomics*, 33(3), pp. 219–230. doi: 10.1016/s0003-6870(02)00009-1.

Wogalter, M. S., Jarrard, S. W. and Noel Simpson, S. (1994) 'Influence of Warning Label Signal Words on Perceived Hazard Level', *Human Factors: The Journal of the Human Factors and Ergonomics Society*, pp. 547–556. doi: 10.1177/001872089403600310.

Womack, M. (2005) *Symbols and Meaning: A Concise Introduction*. Rowman Altamira. Available at: https://books.google.com/books/about/Symbols_and_Meaning.html?hl=&id=MQi5x7_-eksC.

Wong, E. (2020) *Heuristic Evaluation: How to Conduct a Heuristic Evaluation*. Available at: https://www.interaction-design.org/literature/article/heuristic-evaluation-how-to-conduct-a-heuristic-evaluation (Accessed: 6 June 2021).

Zaman, B. and Nouwen, M. (2016) *Parental controls: advice for parents, researchers and industry*. EU Kids Online. Available at: https://www.researchgate.net/publication/301775592_Parental_controls_advice_for_parents_researchers_and_industry (Accessed: 31 May 2021).

7 Appendices

7.1 NSD application

NSD NORSK SENTER FOR FORSKNINGSDATA

Meldeskjema 780520

Sist oppdatert

30.01.2021

Hvilke personopplysninger skal du behandle?

- Navn (også ved signatur/samtykke)
- E-postadresse, IP-adresse eller annen nettidentifikator
- Lydopptak av personer

Type opplysninger

Skal du behandle særlige kategorier personopplysninger eller personopplysninger om straffedommer eller lovovertredelser?

Nei

Prosjektinformasjon

Prosjekttittel

AiBA – Trygghet for barn i chatterom

Prosjektbeskrivelse

Denne studien er ment å skaffe seg innsikt i kunnskapen om grooming i online chatterom hos foreldre og barn på barneskolen. Formålet er å forstå hvordan barn bruker chat-apper og hvordan vi kan designe en løsning som beskytter barn i chatterom mot overgripere på nett.

Denne masteroppgaven vil bli innlemmet i AiBA (Author Input Behavioral Analysis) prosjektet veiledet av Patrick Bours. AiBA-prosjektets overordnede mål er å beskytte barn på nettet mot seksuelle overgripere, grooming og nettmobbing gjennom å identifisere og forhindre grooming i online chatterom. Det tar sikte på å identifisere falske profiler i chatte-applikasjoner. Denne studien er ment å skaffe innsikt i kunnskapen om grooming og seksuelle overgripere på nettet. Gjennom dette er målet å utvikle en måte å advare barn i live chatte-samtaler om potensiell fare. Bevissthetskampanjer og å se på hvordan foreldre og barn kan informeres om potensielle risikoer på nett er en viktig del av dette prosjektet.

Begrunn behovet for å behandle personopplysningene

Formålsrike intervjuer, undersøkelser og fokusgrupper. Design av relevant advarsel.

Ekstern finansiering

Type prosjekt

Studentprosjekt, masterstudium

Kontaktinformasjon, student

Marit Sylstad, maritsyl@stud.ntnu.no, tlf: 92042532

Behandlingsansvar

Behandlingsansvarlig institusjon

Norges teknisk-naturvitenskapelige universitet / Fakultet for informasjonsteknologi og elektroteknikk (IE) / Institutt for datateknologi og informatikk

Prosjektansvarlig (vitenskapelig ansatt/veileder eller stipendiat)

Patrick Bours, patrick.bours@ntnu.no, tlf: 41265872

Skal behandlingsansvaret deles med andre institusjoner (felles behandlingsansvarlige)?

Nei

Utvalg 1

Beskriv utvalget

Foreldre til skolebarn

Rekruttering eller trekking av utvalget

Rekruttering gjennom skoleledelse i kommunen. Foreldre til barn i 5. til 9. klasse vil først bli kontaktet via skoler. AiBA-prosjektet har samarbeidet med skoler rundt Gjøvik og Hamar. Foreldre som er interessert i å delta frivillig, blir deretter kontaktet for intervjuer.

Alder

19 - 70

Inngår det voksne (18 år +) i utvalget som ikke kan samtykke selv?

Nei

Personopplysninger for utvalg 1

- Navn (også ved signatur/samtykke)
- E-postadresse, IP-adresse eller annen nettidentifikator
- Lydopptak av personer

Hvordan samler du inn data fra utvalg 1?

Personlig intervju

Grunnlag for å behandle alminnelige kategorier av personopplysninger

Samtykke (art. 6 nr. 1 bokstav a)

Informasjon for utvalg 1

Informerer du utvalget om behandlingen av opplysningene?

Ja

Hvordan?

Skriftlig informasjon (papir eller elektronisk)

Utvalg 2

Beskriv utvalget

Skolebarn

Rekruttering eller trekking av utvalget

Rekruttering gjennom skoleledelse i kommunen, med tillatelse fra foreldre. Barnas deltakelse er frivillig.

Alder

9 - 15

Inngår det voksne (18 år +) i utvalget som ikke kan samtykke selv?

Nei

Personopplysninger for utvalg 2

Hvordan samler du inn data fra utvalg 2?

Elektronisk spørreskjema

Grunnlag for å behandle alminnelige kategorier av personopplysninger

Samtykke (art. 6 nr. 1 bokstav a)

Hvem samtykker for barn under 16 år?

Foreldre/foresatte

Gruppeintervju

Grunnlag for å behandle alminnelige kategorier av personopplysninger

Samtykke (art. 6 nr. 1 bokstav a)

Hvem samtykker for barn under 16 år?

Foreldre/foresatte

Informasjon for utvalg 2

Informerer du utvalget om behandlingen av opplysningene?

Ja

Hvordan?

Skriftlig informasjon (papir eller elektronisk)

Tredjepersoner

Skal du behandle personopplysninger om tredjepersoner?

Nei

Dokumentasjon

Hvordan dokumenteres samtykkene?

- Manuelt (papir)
- Elektronisk (e-post, e-skjema, digital signatur)

Hvordan kan samtykket trekkes tilbake?

Melding via e-post / telefon til studieansvarlig. Hver deltaker får en identifiserende nøkkel slik at det anonymiserte datasettet kan identifiseres

Hvordan kan de registrerte få innsyn, rettet eller slettet opplysninger om seg selv?

Notification via email/ phone of study responsible

Totalt antall registrerte i prosjektet

100-999

Tillatelser

Skal du innhente følgende godkjenninger eller tillatelser for prosjektet?

Behandling

Hvor behandles opplysningene?

- Maskinvare tilhørende behandlingsansvarlig institusjon
- Ekstern tjeneste eller nettverk (databehandler)

Hvem behandler/har tilgang til opplysningene?

- Student (studentprosjekt)
- Prosjektansvarlig
- Databehandler

Hvilken databehandler har tilgang til opplysningene?

Nettskjema (https://nettskjema.no/) for spørreundersøkelse og Nettskjema-diktafon-appen til lydopptak av intervju.

Tilgjengeliggjøres opplysningene utenfor EU/EØS til en tredjestat eller internasjonal organisasjon?

Nei

Sikkerhet

Oppbevares personopplysningene atskilt fra øvrige data (koblingsnøkkel)?

Ja

Hvilke tekniske og fysiske tiltak sikrer personopplysningene?

- Opplysningene anonymiseres fortløpende
- Adgangsbegrensning

Varighet

Prosjektperiode

04.01.2021 - 31.05.2022

Skal data med personopplysninger oppbevares utover prosjektperioden?

Nei, data vil bli oppbevart uten personopplysninger (anonymisering)

Hvilke anonymiseringstiltak vil bli foretatt?

- Koblingsnøkkelen slettes
- Personidentifiserbare opplysninger fjernes, omskrives eller grovkategoriseres
- Lyd- eller bildeopptak slettes

Vil de registrerte kunne identifiseres (direkte eller indirekte) i oppgave/avhandling/øvrige publikasjoner fra prosjektet?

Nei

Tilleggsopplysninger

Denne forskningen er en del av AiBA-prosjektet ved NTNU på Gjøvik. Vi er to forskere med samme veileder som samarbeider om datainnsamlingen, men skriver to separate masteroppgaver. Den andre NSD-søknaden

har referansenummer 754575.
Informasjonsbrevet vil først bli sendt til foreldrene for å få tillatelse til at barna kan delta i forskningen. Barn kan også se en liten beskrivelse i begynnelsen av spørreundersøkelsen.

7.2 Information letter about the project and consent form

Vil du delta i forskningsprosjektet

"AiBA – Trygghet for barn i chatterom"

Vil du delta i et forskningsprosjekt om trygghet for barn i chatterom? Formålet er å forstå hvordan barn bruker chat-apper og hvordan vi kan designe en løsning som beskytter barn i chatterom mot overgripere på nett. I dette skrivet gir vi deg informasjon om målene for prosjektet og hva deltakelse vil innebære for deg.

Formål

Dette prosjektet er en del av masteroppgave i interaksjonsdesign på Norges teknisk-naturvitenskapelige universitet (NTNU). Denne masteroppgaven vil bli innlemmet i AiBA (Author Input Behavioral Analysis) prosjektet veiledet av Patrick Bours. AiBA-prosjektets overordnede mål er å beskytte barn på nettet mot seksuelle overgripere, grooming og nettmobbing gjennom å identifisere og forhindre grooming i online chatterom. Det tar sikte på å identifisere falske profiler i chatte-applikasjoner. Denne studien er ment å skaffe innsikt i kunnskapen om grooming og seksuelle overgripere på nettet. Gjennom dette er målet å utvikle en måte å advare barn i live chatte-samtaler om potensiell fare. Bevissthetskampanjer og å se på hvordan foreldre og barn kan informeres om potensielle risikoer på nett er en viktig del av dette prosjektet.

Hvem er ansvarlig for forskningsprosjektet?

Norges teknisk-naturvitenskapelige universitet (NTNU) i Gjøvik er ansvarlig for prosjektet.

Hvorfor får du spørsmål om å delta?

For å kunne gjøre denne studien og finne relevante deltakere for datainnsamling, har lokale skoler i området blitt kontaktet og et samarbeid med barneskolene er etablert gjennom rektorene og NTNU. Målgruppen her er barna i 5. til 7. klasse og deres foreldre. Det er blant annet etablert kontakt med Kopperud (Gjøvik) og Vestre Toten Ungdomsskole (VTU i Raufoss) Målgruppen her er barna i 8. til 9. klasse og deres foreldre.

Hva innebærer det for deg å delta?

Utvalg 1-Foreldre til barn i 5. til 9. klasse - intervju

Hvis du velger å delta i prosjektet, innebærer det at du vil delta i et dybdeintervju. Det vil ta mellom 45 til 60 minutter. Intervjuet inneholder spørsmål om barns chattevaner og dine erfaringer rundt tema. Dine svar fra i intervjuet blir registrert som notater og det vil

bli tatt opp lyd av samtalen. Lydopptakene brukes i analysearbeidet i etterkant av intervjuene og vil deretter slettes. På grunn av koronarestriksjoner så vil intervjuene mest sannsynlig bli gjennomført digitalt via Zoom eller Microsoft Teams.

Utvalg 2- Barn i 5. til 9. klasse - spørreundersøkelse og fokusgrupper

Hvis du velger å delta i prosjektet, innebærer det at ditt barn/ dine barn i relevant aldersgruppe fyller ut et spørreskjema. Det vil ta dem ca. 20 minutter. Spørreskjemaet inneholder spørsmål om barns erfaringer med sosiale medier og spesielt chattefunksjonen i disse. Målet er å få innsikt i hvordan barn bruker chat-apper, barnas erfaringer og holdninger til online kommunikasjon, sosiale medier og farene de kan møte i chatteapplikasjoner.

Selv om du som forelder sier ja til at ditt barn kan delta, er det fortsatt frivillig for barnet om det velger å delta eller ikke.

Vi vil bruke funnene fra denne spørreundersøkelsen i vår forskning for å komme med bedre løsninger som beskytter barns privatliv og øker barn og foreldres bevissthet. Svar fra spørreskjemaet blir registrert elektronisk via en sikker løsning for datainnsamling via nett.

Som forelder har du rett på å få se spørreskjema på forhånd. Ta kontakt med studieveileder om du ønsker denne informasjonen.

I tillegg til spørreundersøkelse ønsker vi at noen av barna deltar i fokusgrupper der de skal løse en designutfordring i samarbeid med masterstudent fra NTNU. Formålet er å designe funksjoner i chatteapper som kan hjelpe dem med å takle situasjoner der de møter potensielle overgripere.

Det vil IKKE gjøres lydopptak av utvalg 2.

Det er frivillig å delta

Det er frivillig å delta i prosjektet. Hvis du velger å delta, kan du når som helst trekke samtykket ditt uten å oppgi noen grunn. Alle dine personopplysninger vil da bli slettet. Det vil ikke ha noen negative konsekvenser for deg hvis du ikke vil delta eller velger å trekke deg ved en senere anledning.

Ditt personvern – hvordan vi oppbevarer og bruker dine opplysninger

Vi vil bare bruke opplysningene om deg til formålet vi har fortalt om i dette skrivet. Vi behandler alle opplysninger konfidensielt og i samsvar med personvernregelverket.

Det er kun prosjektansvarlig Patrick Bours og studenter Marit Sylstad og Nakul Pathak ved NTNU som vil ha tilgang til dataene i prosjektet.

Utvalg 1

Det er kun prosjektansvarlig Patrick Bours og student Marit Sylstad og Nakul Pathak ved NTNU som vil ha tilgang til dataene utvalg 1 før de anonymiseres. Navnet til utvalg 1 og kontaktopplysningene dine vil erstattes med en kode som lagres på egen navneliste adskilt fra øvrige data. Dette lagres på trygg forskningsserver med passord. I publikasjoner vil dataene være anonymisert. Det er likevel en mulighet for at du gjenkjenner egne uttalelser fra intervjuet.

Utvalg 2

I utvalg 2 vil det ikke samles inn noe personidentifiserende informasjon.

Du som testperson vil ikke, kunne identifiseres (direkte eller indirekte) i oppgaven eller øvrige publikasjoner fra prosjektet.

Hva skjer med opplysningene dine når vi avslutter forskningsprosjektet?

Opplysningene anonymiseres når prosjektet avsluttes, noe som etter planen er ved utgangen av juli 2021. Personopplysninger, koblingsnøkkelen og opptak vil da slettes, og kun det anonymiserte datamaterialet beholdes.

Dine rettigheter

Så lenge du kan identifiseres i datamaterialet, har du rett til:

- innsyn i hvilke personopplysninger som er registrert om deg, og å få utlevert en kopi av opplysningene
- å få rettet personopplysninger om deg,
- å få slettet personopplysninger om deg, og
- å sende klage til Datatilsynet om behandlingen av dine personopplysninger.

Hva gir oss rett til å behandle personopplysninger om deg?

Vi behandler opplysninger om deg basert på ditt samtykke.

På oppdrag fra Norges teknisk-naturvitenskapelige universitet (NTNU) har NSD – Norsk senter for forskningsdata AS vurdert at behandlingen av personopplysninger i dette prosjektet er i samsvar med personvernregelverket.

Hvor kan jeg finne ut mer?

Hvis du har spørsmål til studien, eller ønsker å benytte deg av dine rettigheter, ta kontakt med:

Norges teknisk-naturvitenskapelige universitet (NTNU) ved Patrick Bours.

Forskningsveilederen kan kontaktes på patrick.bours@ntnu.no. Hvis du har andre praktiske spørsmål, kan du kontakte student Marit Sylstad og Nakul Pathak

Vårt personvernombud er Thomas Helgesen, thomas.helgesen@ntnu.no.

Hvis du har spørsmål knyttet til NSD sin vurdering av prosjektet, kan du ta kontakt med:

NSD – Norsk senter for forskningsdata AS på epost (personverntjenester@nsd.no) eller på telefon: 55 58 21 17.

Med vennlig hilsen

Patrick Bours	Marit Sylstad	Nakul Pathak
Forsker/veileder	Student	Student

Samtykkeerklæring - intervju

Jeg har lest prosjektbeskrivelsen, og i tillegg fått informasjon vedrørende forskningen og er kjent med hva det innebærer å være deltaker i intervju. Dette er ikke en test av dine ferdigheter. Vi er kun interessert i dine opplevelser og meninger om tema.

Det er frivillig å delta og du kan avbryte intervjuet når som helst.

Jeg bekrefter å ha fått den informasjon som er angitt ovenfor og at jeg gir tillatelse til at opptak av lyd kan bli delt med studieveileder på NTNU. Jeg har mottatt og forstått informasjon om prosjektet AiBA – Trygghet for barn i chatterom, og har fått anledning til å stille spørsmål. Jeg samtykker til:

- å delta i intervju
- at det gjøres lydopptak av samtalen

Jeg samtykker til at mine opplysninger behandles frem til prosjektet er avsluttet

Dato og underskrift:

(Signert av prosjektdeltaker)

Samtykkeerklæring - digitalt spørreskjema

Jeg har lest prosjektbeskrivelsen, og i tillegg fått informasjon vedrørende forskningen og er kjent med hva det innebærer for barnet å være deltaker i spørreundersøkelsen.

Jeg samtykker til at mitt barn deltar i spørreundersøkelse om trygghet for barn i chatterom i forbindelse med masteroppgave på NTNU.

Jeg samtykker til at mitt barns opplysninger behandles frem til prosjektet er avsluttet

Dato og underskrift:

_____

Underskrift foresatte

Der foreldre bor sammen, er det tilstrekkelig at den ene skriver under. Der foreldre ikke bor sammen er det den som har daglig omsorg som skal skrive under. Ved delt omsorg skal begge foreldre skrive under.

Samtykkeerklæring - fokusgruppe

Jeg har lest prosjektbeskrivelsen, og i tillegg fått informasjon vedrørende forskningen og er kjent med hva det innebærer å være deltaker i fokusgruppen.

Jeg samtykker til at mitt barn deltar i fokusgruppe om trygghet for barn i chatterom i forbindelse med masteroppgave på NTNU.

Jeg samtykker til at mitt barns opplysninger behandles frem til prosjektet er avsluttet

Dato og underskrift:

_____

Underskrift foresatte

Der foreldre bor sammen, er det tilstrekkelig at den ene skriver under. Der foreldre ikke bor sammen er det den som har daglig omsorg som skal skrive under. Ved delt omsorg skal begge foreldre skrive under.

7.3 Interview Schedule – Semi-Structured Interviews

Nr	Date	Sex	Age	Position/type of employment
1	22 March	Female	47	Team leader
2	25 March	Female	36	Teacher
3	27 March	Female	40	Senior adviser
4	27 March	Female	55	Nurse
5	30 March	Female	40	Student
6	12 April	Female	50	Senior adviser
7	13 April	Female	41	Higher executive officer
8	18 April	Male	43	Head of the schools

7.4 Interview guide - interview with parents

Introduction

Hello __!

We are Marit and Nakul. We are studying for masters in interaction design here at NTNU in Gjøvik.

We are conducting this research to understand children's chat app usage and your thoughts on the topics.

We will use the findings from this discussion in our research to come up with better solutions that protect children's privacy and increase children and parent's awareness.

We have few questions for you, the questions are open-ended and there is no right or wrong answer. So feel free to say whatever comes to your mind that you feel is relevant. You can stop the discussion if you feel uncomfortable or don't wish to continue.

About privacy and confidentiality

We would like to share a few details about how we handle data.

All the data collected is in the form of notes, sound recording and will be only shared with the research supervisor from NTNU. The data is safely stored. We will anonymise all the raw data once the analysis is completed. The raw data will only be retained until this thesis is completed, tentatively by the end of July 2021.

If you would like to withdraw your data from the research, please send an email to the following email addresses. Your unique data key is – <Key here>. This key is unique and is associated with your data.

In case you have any other questions, you can reach us at nakulp@stud.ntnu.no or maritsyl@stud.ntnu.no. The thesis/research supervisor can be contacted at patrick.bours@ntnu.no.

The research is part of the AiBA (Author Input Behavioural Analysis) project, which monitors chat conversations through behavioural biometrics and text analysis to warn users about false identities and suspicious behaviour. The AiBA project is conducted by the Norwegian Biometry Laboratory which is part of the Department of Information Security and Communication Technology at NTNU Gjøvik.

- Shall we continue?
- Do you have any questions before we start?

Warm-up questions and Introduction (10 min)

1. Can you tell me about yourself?
2. What grade level are your children in?
3. What do you usually use the internet for? (Online banking? Online newspapers? Facebook?)
4. What type of devices do you use regularly?
    a. Smartphone/Mobile
    b. Laptop or PC
    c. Tablet/iPad
    d. Game console (PlayStation, Nintendo Switch, Xbox etc.)
    e. Smartwatch - Fitbit, Apple Watch, Garmin etc.
    f. None/prefer not to say
5. How much time do you spend online each day outside of work?
    a. Less than an hour
    b. 1-2 hours
    c. 2-3 hours
    d. More than 3 hours
6. What social media do you use? (Facebook, Snapchat, Instagram, TikTok, YouTube or any other)
7. Have you experienced attempts of internet scams/virus?
    a. If yes, how did you react to it?

The main question (20 – 25 min)

For an elaboration of topics that arise, spontaneous follow-up questions can be asked along the way.

Part 1 – Awareness of safe internet usage

8. Have you received any information on – how can you make a child's internet usage safe? For instance, Nettvett etc.
9. (Optional) Where would you like to get information and advice on how to help and support your child on the internet and keep him or her safe?
10. How do you talk to your kids about safe internet use and the dangers they can face online? (hints if asked: Namely - Safe use of passwords, sharing private information/photos, predators online etc.)
11. Do you think your child(ren) is aware of risks online?

Part 2 – How parents monitor a child's usage

12. Are your kids on social media?
    a. Do you follow them on all those platforms?
13. Can you describe your main concerns regarding your children and the dangers they may face online? Bullying, grooming etc.
14. Can you describe how if you use any digital apps/tools such as parental controls software to keep your children safe online?
    a. How do you keep track of what your kids are doing online/control time spent?
    b. What are its pros and cons? What could be done better?
    c. Have you faced any challenges?
    d. Is it anything you think is difficult or too complex to talk to your child about

Part 3 – Parents' preferences of receiving information

15. Do you know the meaning of the term grooming/predators?

ENG: Grooming is when someone builds a relationship, trust and emotional connection with a child or young person so they can manipulate, exploit and abuse them.

NO: Grooming er prosessen hvor en voksen blir venner med, og oppretter en emosjonell kontakt med et barn, for så å avtale et møte med det slik at det vil bli mulig for den voksne å ha seksuell omgang med barnet.

16. As a parent what kind of information would you like to receive about the risks of online grooming/ predators?
17. In your opinion what is the best way to protect children from online predators?

Part 4 – Privacy and thoughts on privacy solution - Personvern

18. Do you talk about privacy with your child? If yes, how often?
    a. How would you approach this topic?
19. What do you think about children's privacy?
    a. In case if he/she would like to share an online experience, what do they like sharing/talking about? What do they prefer to keep secret?
20. (Optional) What do you think he/she thinks about privacy concerning these topics?
21. What do you think of the – safety review system that is built into their chat apps?

Description – Imagine a system that gives you a warning about potential sexual grooming in chats. The system protects the child and keeps parents informed about potential dangers. With help of some features, a child can have a conversation with parent(s) about his/her experiences online. The system can also protect a child's privacy in cases where there is potential grooming. A child can select what parents can see and know.

22. If you as a parent are to choose what you would like to see, what would you prefer from the following?

Wrap up (Summary and clarification 5-10 mins)

23. Summarize the main findings
24. Do you want to elaborate on some of what we have said?
25. Would you like to add something to the discussion so far?

Thank you for taking the time to talk to us. We have gotten very valuable information from this discussion. It was nice talking to you. Have a nice day!

7.5 Survey questions

Introduction

Hello __!

We are Marit and Nakul. We are studying for masters in interaction design here at NTNU in Gjøvik. The purpose is to understand how children use chat apps.

We will use the data to create a better system that –

1. Protects children's privacy
2. Keep children safe online
3. Increase parent's and children's awareness

About privacy and confidentiality

We would like to share a few details about how we handle data.

We are not gathering any personal information that identifies you individually. The data is anonymized and safely stored. Your participation is completely voluntary, and you can stop the survey at any time if you feel uncomfortable or don't wish to continue.

In case you have any other questions, you can reach us at xxx@stud.ntnu.no or xxxl@stud.ntnu.no. The thesis/research supervisor can be contacted at xxx@ntnu.no. Thank you for helping us.

Part 1 – About you

We would like to know a little bit about you and how you use the internet and devices.

1. Are you a
    a. Girl
    b. Boy
    c. Other
    d. Prefer not to say.
2. What grade are you in?
    a. 5th grade
    b. 6th grade
    c. 7th grade
    d. 8th grade
    e. 9th grade
3. Do you use any of these digital devices? (Select that applies) / Har du noe av dette hjemme?
    a. Smartphone/mobile

b. Tablet /Nettbrett (IPad el.)
c. PC/Laptop/Gaming PC
d. Spill konsoll (Playstation, Nintendo Switch, Xbox etc.)
e. Smart Kids watch /Klokke du kan ringe med

4. How much do you use each of the following apps? For each app, options are - More than 2 hours a day, 1-2 hours a day, less than an hour, I don't use this app, I'm not allowed to use this app, don't want to say
    a. Facebook
    b. Snapchat
    c. Instagram
    d. TikTok
    e. Discord
    f. Messenger
    g. Messenger kids
    h. Telegram
    i. Others (please specify -)
5. How much do you play any of these online games: (For each app, options are - More than 2 hours a day, 1-2 hours a day, less than an hour, I don't use this app, I'm not allowed to use this app, don't want to say)
    a. Fortnite
    b. Minecraft
    c. Roblox
    d. Movie Star Planet
    e. MarioKart Tour
    f. Other: _____

Part 2 – Your experiences on chat apps

A chat conversation can happen in various apps such as Snapchat, Facebook Messenger, Discord, online chatrooms such as www.Chatroulette.com, during online games such as Fortnite, MovieStarPlanet FIFA, Roblox, Minecraft and so on.

Remember that other people will not know that these answers are yours, so please answer as best you can. If you don't know or don't want to answer any of the questions, just answer "don't remember, I don't know or rather not say.

Rate the following statements (1 – Least agree, 5 - Highly Agree)

g. I have a lot of contact with my friends on social media
h. In social media, I meet people with the same interest as me
i. I have regretted sharing something on social media or in the chat

j. I feel like I am more myself online than in real life

6. What do you usually do when someone asks you to become "friends" or follow you on social media? Tick all that is right for you
    a. I accept everyone
    b. I accept if we are the same age
    c. I accept if we have mutual friends
    d. I only accept if I know them
    e. I only accept if my parents say it's ok
    f. I do not accept anyone
    g. I don't know
7. Have you ever had contact on the internet with someone you have not met in real life/face-to-face before?
    a. Yes, often
    b. Yes, once or twice
    c. No, never
    d. Don't know/ don't remember
8. In the past have you ever met anyone face-to-face that you first got to know online?
    a. Yes, often
    b. Yes, once or twice
    c. No, never
    d. Don't know/ don't remember

Routing if yes;

9. The LAST time you met someone face-to-face that you first got to know online or on a phone, how did you feel about it?
    a. I was happy
    b. I was not happy or upset
    c. I was a little upset
    d. I was fairly upset
    e. I was very upset
    f. Prefer not to say
11. The LAST time you met someone face-to-face that you first got to know online or on a phone, how old was the person you met? (Choose one answer)
    a. I met with someone about my age
    b. I met with someone younger than me
    c. I met with a teenager older than me
    d. I met with an adult

12. Rate following statements based on your experiences (1-Never 5- Many times)
    a. I have been asked for an address, phone number or password during a chat conversation with someone I don't know
    b. I have been asked to share a photo of myself during a chat conversation with someone I don't know
    c. I have been asked to share a sexual or naked photo of myself (picture or video) with someone I don't know
    d. I have been asked to share a sexual or naked photo of myself (picture or video) during a chat with someone I know

Routing if not never

13. Last time you were asked for private or sexual information online -What did you do?
    a. Nothing in particular
    b. I blocked the person
    c. I talked to a friend about it
    d. I am still in contact with the person
    e. I reported the person
    f. I didn't tell anyone
    g. I told my parents/a trusted adult
    h. I reported the person using the applications reporting function
    i. don't know/ don't remember

Part 3 – Privacy towards the outside world

14. What is the best way to protect children online? What do you think is most important to be safe in chat apps? What will make you feel safe while chatting? What is needed to be safe in chatting?
15. What do you need to feel safe, while chatting online or using chat apps?
16. Rate statements from 1 to 5 (1- least applicable, 5-most applicable and not sure/don't know)
    a. I like keeping my apps/software up-to-date.
    b. I often check my social media account settings (including privacy settings) regularly.
    c. I know what information I am sharing with my friends/followers/everyone.
    d. I know what information the app is gathering about me.
    e. I know how to keep my data safe.

Part 4 – privacy and keeping parents informed about daily usage

17. Rate following statements based on your understanding and experiences (1-Least applicable 5- most applicable)
    a. My parents have told me about the risks of using chat apps.
    b. I follow the rules my parents have made about using chat apps
    c. I talk to my parents about conversations I have had over chat apps.
    d. I like to discuss my negative/strange experiences online (or on chat apps) with my parents.
    e. I think a chat app can help me discuss dangers/negative experiences on chat apps with my parents.
    f. I feel the need to talk to my parents if I come across something strange/negative/unusual.
    g. I find it difficult to talk to my parents about my experiences in chat apps.
    h. I can handle the situation by myself after experiencing something unusual/concerning on chat apps.

Part 5 – Questions around privacy check solution and questions around it

17. Imagine a system that is built into your chat apps. The system is designed to ensure you are safe and protected against any risk such as grooming, sexual predators etc. The system can detect if the other person is fake (sharing wrong details like age) and/or if trying to get private information for the wrong purposes.

It can also help to increase awareness about safety. It will send you a reminder with a notification to help you go through your chat app's settings and make sure it is safe. Below is a brief description of some of the features -

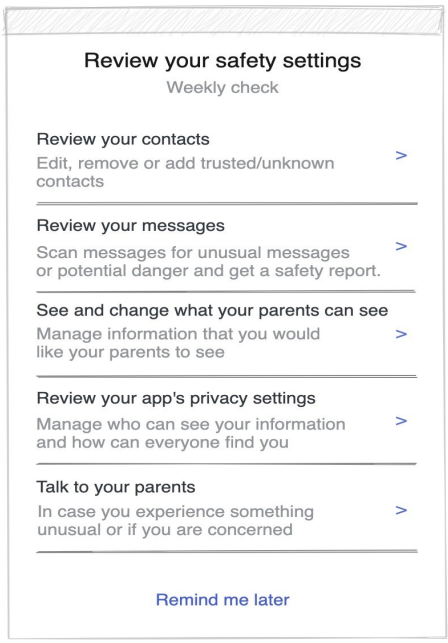
18. Review messages - You can get a safety report on your chats. The system will notify you if there are any risks (such as someone asking for private/sexual information or a fake profile). The system can highlight chats that contain risk and help you take action on it.
19. Review your app's privacy – Reviewing your app's privacy setting is important to control who can find you and contact you. It also includes who can see posts or data that you share.
20. Review newly added contacts or pending requests - Here you can go through your contact/follower list to see if there is someone you don't know or don't trust.
21. Edit what your parents can see – This system will work with parental control software if your parents use any. In case of any risk is detected, parents will also get a notification. However, what they can see can be edited by you. The system helps you maintain privacy in all scenarios.

22. Talk to your parents – If you experience something negative or strange, talking to your parents can help a lot. The system can support you by helping you to have a conversation with your parents, whenever you think you need it.

Imagine your chat apps (or social media apps) with additional features. These features will keep children safe and detect risks. For example, the system can identify if a child is talking to someone who is having a fake profile or someone trying to get private information for the wrong purposes.

The app will send a reminder every 15 days to remind you to go through some things –

1. Review messages – You can scan messages and see if there are any risks. The system can highlight chats with risk, and you can take action on it.
2. Review your app's privacy – You can control and change who can find you, contact you and see your profile information.
3. Review your contacts – With this, you can go through your contacts/follower list. You can edit/remove unknown contacts or add trusted contacts.
4. Edit what your parents can see – In case there is a risk that requires action, your parents might be notified. However, you can decide what information they can see along with the warning.
5. Talk to your parents – If you experience something negative or strange, you can talk to your parents about it through chat.



18. The app will remind you to go through these steps every 15 days. This can be changed through settings.
19. Please rate the following statements on a scale of 1 to 5 -

a. I find this solution useful.
b. I think this will help me to talk about my experiences with my parents.
c. I feel this can protect and make me aware of dangers.

Thank you note

If you experience something negative, it is important to talk to someone you trust.

You can also call "Alarmtelefonen for barn og unge" on 116 111

- Alarmtelefonen er en gratis telefon for barn og unge som er utsatt for vold, overgrep og omsorgssvikt. Alarmtelefonen er døgnåpen. https://www.116111.no/

You have given us valuable information and inputs. This will help make children's lives safer and better. Thank you for your time. Have a great day ahead!

Useful Scale

1. (Not useful)
2. (Somewhat useful)
3. (Useful)
4. (Very useful)
5. (Extremely useful)
6. Don't know/don't want to answer

Agree on scale

How much do you agree with the questions below?

1 – Strongly disagree, 5 – Strongly agree and Don't know/Don't want to answer

1. (Strongly disagree)
2. (Disagree)
3. (Somewhat agree)
4. (Agree)
5. (Strongly agree)
6. Don't know/Don't want to answer

Frequency scale

1. (Never)
2. (Couple of times)
3. (Sometimes)
4. (Often)
5. (Very often)
6. Don't know/Don't want to answer

Frequency scale-2

1. (Never)
2. (Couple of times)
3. (A couple of times a month)
4. (Couple of times a week)
5. (Daily)
6. Don’t know/Don’t want to answer

7.6 Focus group

7.6.1 Plan

After survey and interview with parents

- Create a safe setting - Children need to feel safe to tell.
- Listen to the child - the child knows best and is an expert on his reality.
- Ask open-ended questions, help and motivate the child to tell.
- Children need time.

Structure

- Understanding their app usage
- Understanding their perspectives on online chatting/ risks benefits
- Design solutions
- Wrap up /solution.

Introduction - 15 minutes

- Tell me a bit about yourself? Siblings? Pets? Hobbies (Make them relax)
- How old were you when you had your first smartphone or digital device ie? IPad or similar?
- Can you describe how you talk to your friends online? What apps do you use the most?
- Do you have a favourite game?

Main question/ Co-creation tasks 60-120 minutes

- Where is the limit for what is okay to say or do online? / What do you think one should do if a friend is treated badly online?
- Do you think you can talk to your parents about what you experience online?
- What do you do if someone you do not know contacts you online?
- What design solutions do children come up with when asked to design online chat features that can help them cope with potential online grooming situations?
    - Asking for Help
    - Parental Notification
    - Automated Assistance
- Wrap up

7.6.2 Presentation for focus groups

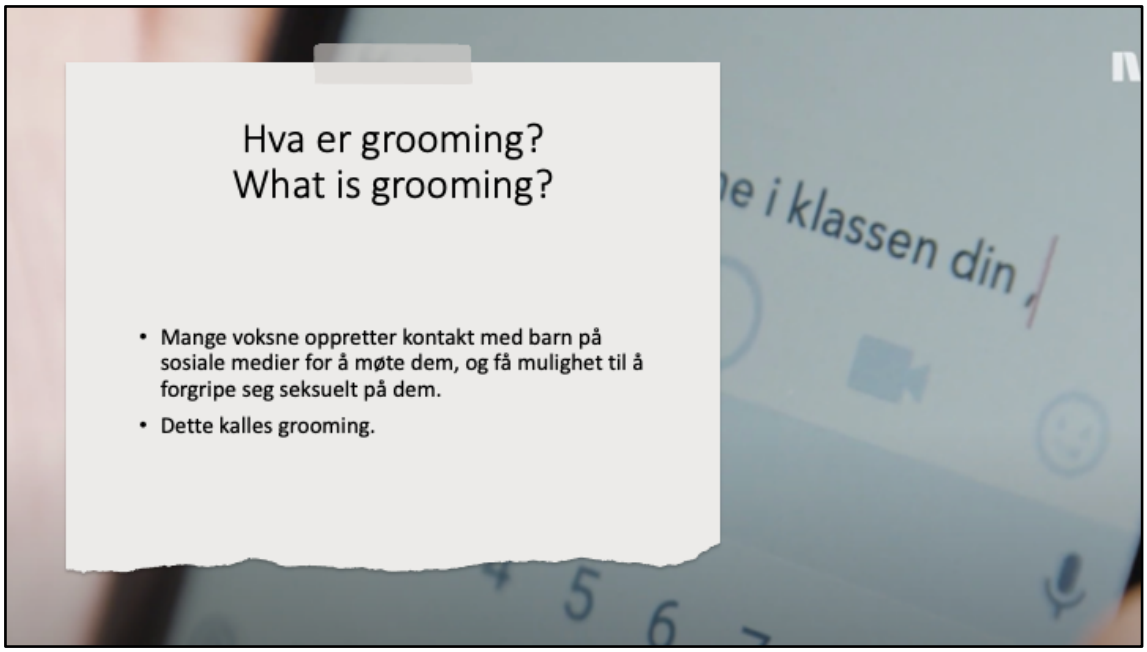
Who are we?

Hello! I am Nakul -

- I am from India.
- I like biking, motorcycle riding and trucks.
- Like books and writing

Marit

- From Nittedal
- Have 3 kids; 8, 10 and 16
- Also have 2 cats, 1 dog and a horse
- Moviebuff and gamer
- Love reading fantasy books


Hva er grooming?
What is grooming?
• Mange voksne oppretter kontakt med barn på sosiale medier for å møte dem, og få mulighet til å forgripe seg seksuelt på dem.
• Dette kalles grooming.


karlerik31
Blir skuffet hvis jeg ikke får se mer :(
Og hvis jeg blir skuffet, blir jeg nødt til å dele bildet ditt med flere.
Kanskje foreldrene dine?
Du får 10 sekunder på deg
10
9
Det er viktig å si i fra
https://youtu.be/x9MOhsd86Xc

What is AiBA

- AiBA is a system that detects grooming, predators by analysing typing rhythm behaviour, chat conversation content -
  - Currently for moderators
  - Sends a warning to children and predators, if a risk is detected
  - In future, it is likely to be an app that can be installed on parents' and children's devices

Ice-breakers

- Tell me a bit about yourself? Siblings? Pets? Hobbies
- How do you communicate with your friends?
- If you could only be on one social network for a week, which would you choose and why?
- What would it be like to be without the internet for a whole week?

Questions about online risks

1. How safe do you feel online on a scale of 1-10? Why?
2. Is it okay to meet someone you have met online in real life?
3. What do you do if someone you do not know contacts you online?
4. Where is the limit to what is okay to say or do online?
5. What do you think one should do if a friend is treated badly online?
6. Do you feel you can talk to your parents about what you are experiencing online?

Work in groups

- Get divided in groups of 3.
- Draw a sketch of a person to your left in 45 seconds.
- Decide your group's superpower and draw a mascot in 2 mins.

Time for ideation and sketching

- Anyone can draw!
- You can draw almost anything with circles and squares
- All drawing is done individually.
- Topics

Activity 1

Problem

AiBA is planned to be an app in the future. The app can be installed on children's and parents' phones. It will notify and provide information if there is any conversation is grooming conversation. Or are there any people with fake profiles?

- What do you think it **should** have/do?
- What do you think it **should not** have/do?

- Time – 5 mins
- Write your thoughts on post-its
- As many things as you want
- Discuss within your groups

Activity 2

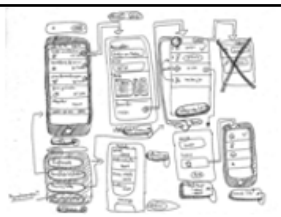
Problem

AiBA app will send out notifications in case there is a risk or grooming situation. These notifications and details will be sent out to parents', children's phone and moderators.

- What do you think it **should** say?
- What do you think it **should not** say?

- Time – 5 mins
- Write your thoughts on post-its
- As many things as you want
- Discuss within your groups

Activity 3



Problem

If someone faces difficulties or problems, how can the app help?

- What features do you think it should have?
- What would you like to do with it?
- Can the app help to talk to someone they trust?
  - If yes, how?

- Time – 6 mins
- Write your thoughts on post-its
- Sketch your ideas on phone mockups
- As many things as you want
- Discuss within your groups

Amalie

Persona

"Hest er best."

Clever · Organised · Curious

Alder: 14

Ungdomsskoleelev

Familie: Bor med mamma og stefar, har to yngre søsken. Pappa har flyttet til Otta.

Bor: Raufoss

Dyr: 2 katter; Snurre og Zalto, 1 hund; Beatrix og 1 hest; Evert

Om Amalie @amalie07horsegirl

Amalie er ungdommskoleelev ved Vestre Toten ungdomsskole . Hennes favorittfag er matte og engelsk. Hun hater fransk fordi hun synes de får så mye lekser. På fritiden er hun mye i stallen, Amalie har en egen hest som heter Evert. Han er en Nordlandhest. Amalie har en instagram konto der hun legger ut masse hestbilder. Der har hun har veldig mange følgere. Hun bruker også Snapchat for å kommunisere med venner og følgere. Hun lager også videoer på Tik Tok.

Interests and needs

- Aktiv på Sosiale medier: Instagram, Snapchat, TikTok
- Elsker hester og sprangridning.
- Spilling - elsker fantasy spill som Zelda, spiller også mye Fortnite.
- Avhengig av å ha med mobilen overalt.
- Hun savner pappaen sin som har flyttet og skulle ønske han kom litt oftere på besøk.

Scenario

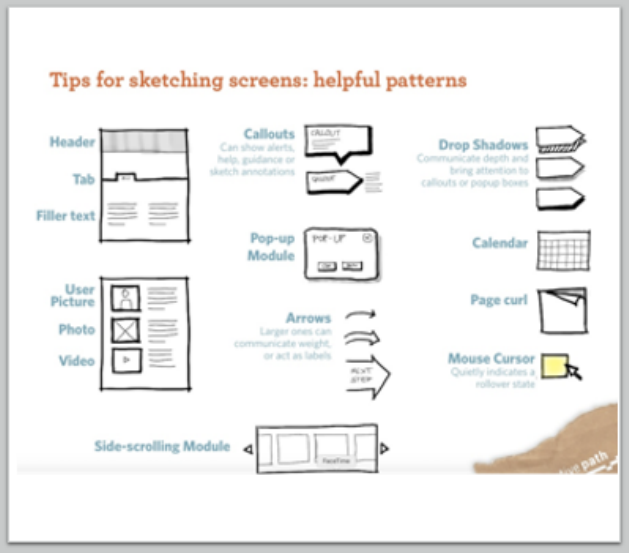
Amalie har veldig mange følgere på sosiale medier og for det meste er det andre hestejenter som følger henne. I det siste har hun fått henvendelser fra ukjente som får henne til å føle seg utilpass. Hun vil ikke fornærme noen eller gjøre de sinte så hun vet ikke helt hvordan hun skal takle det. I tillegg synes hun det er flaut å snakke om og hun lurer litt på om det er hennes egen skyld at hun får denne oppmerksomheten.

Personality

Brands

Tips

- Write an explanation
- Use simple elements; square, rounding, line, arrow, etc.
- Use realistic text
- Use a pen - it should be fast and does not have to be perfect
- If you make a mistake; just keep going
- If it goes completely wrong - curl up, throw away and take a new sheet



Activity 4

Problem

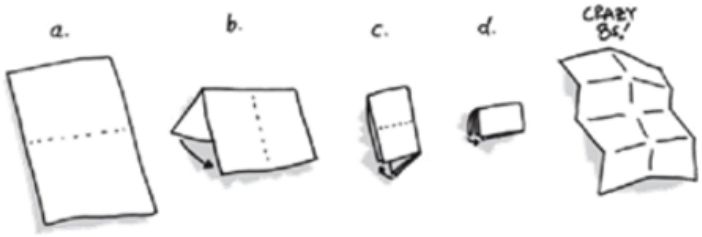
- Design an online feature that can help Amalie cope with this online grooming situation?
  - Group 1: Asking for Help (block, alert button, report to police..)
  - Group 2: Parental Notification
  - Group 3: Automated Assistance (identify fake profiles, flag suspicious behaviour)

- Crazy 8's – 10 minutes
- Pick 1 – spend 5 minutes on making it better
- Discuss within your groups

Crazy 8's

1. Brett et A4-ark i 8 (brett det på midten 3 ganger).
2. Tegn i ca **1 minutt** per rute (følg timer).

Tegn gjerne flere variasjoner av samme idé – bytt idé når du vil.



Velg 1 –

- Alle tegner sin beste idé på et ark.
- Løsningen skal være selvforklarende med tekst og piler.
- Ikke sett navn på.
- Stygt er bra (detaljert og fullstendig er viktig).

Activity 5

Problem

Can we discuss your ideas and thoughts?

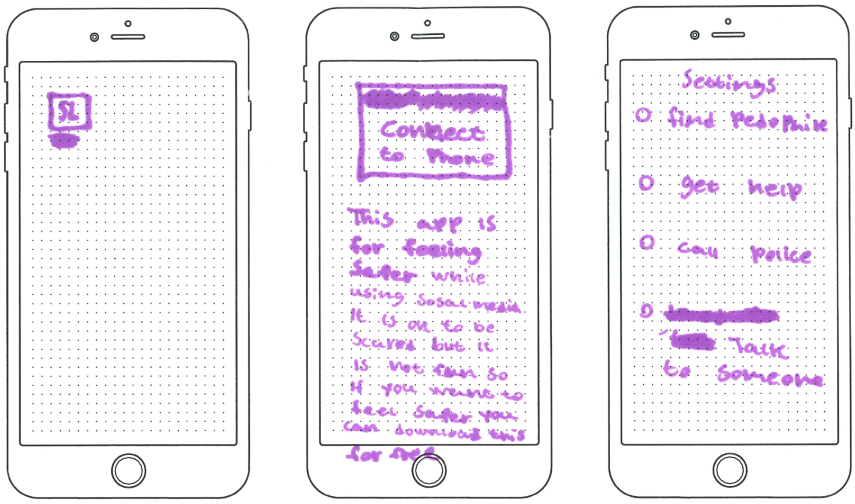
We will go around the group and one of you can quickly tell what you all have come up with.

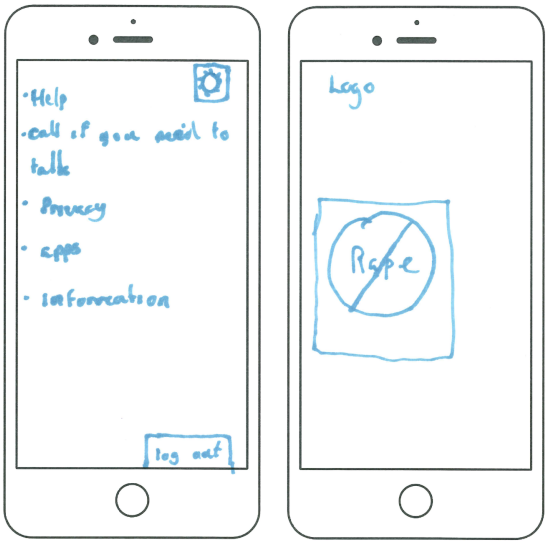
- Time – 10 mins
- Discuss within your groups

Takk for hjelpen og husk..

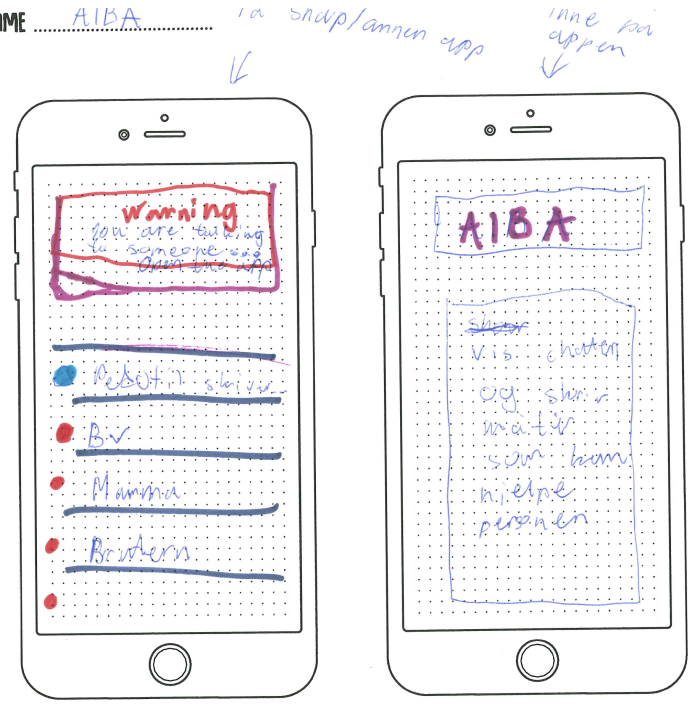
- **Be om hjelp** hvis du opplever noe ubehagelig
- **Tips politiet** hvis du tror du kan ha vært utsatt for noe straffbart eller ta kontakt med politiets nettpatrulje.
- Rapporter det til tjenesten du bruker, for eksempel Snapchat, Instragram osv., dersom noen oppfører seg ubehagelig.
- Snakk med en voksen du stoler på, for eksempel en forelder, nabo, lærer eller trener.
- Du kan også spørre, snakke eller chatte med en trygg voksen på en hjelpelinje, for eksempel 116111.no, ung.no eller korspaahalsen.no.
- En liten video (6 min) https://youtu.be/lhUF4RoUb7o

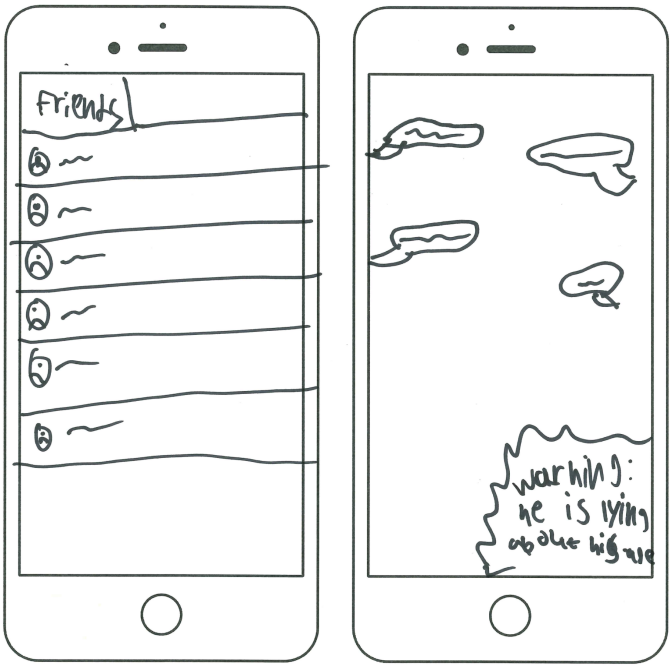
7.6.3 Mock-ups by the teenagers





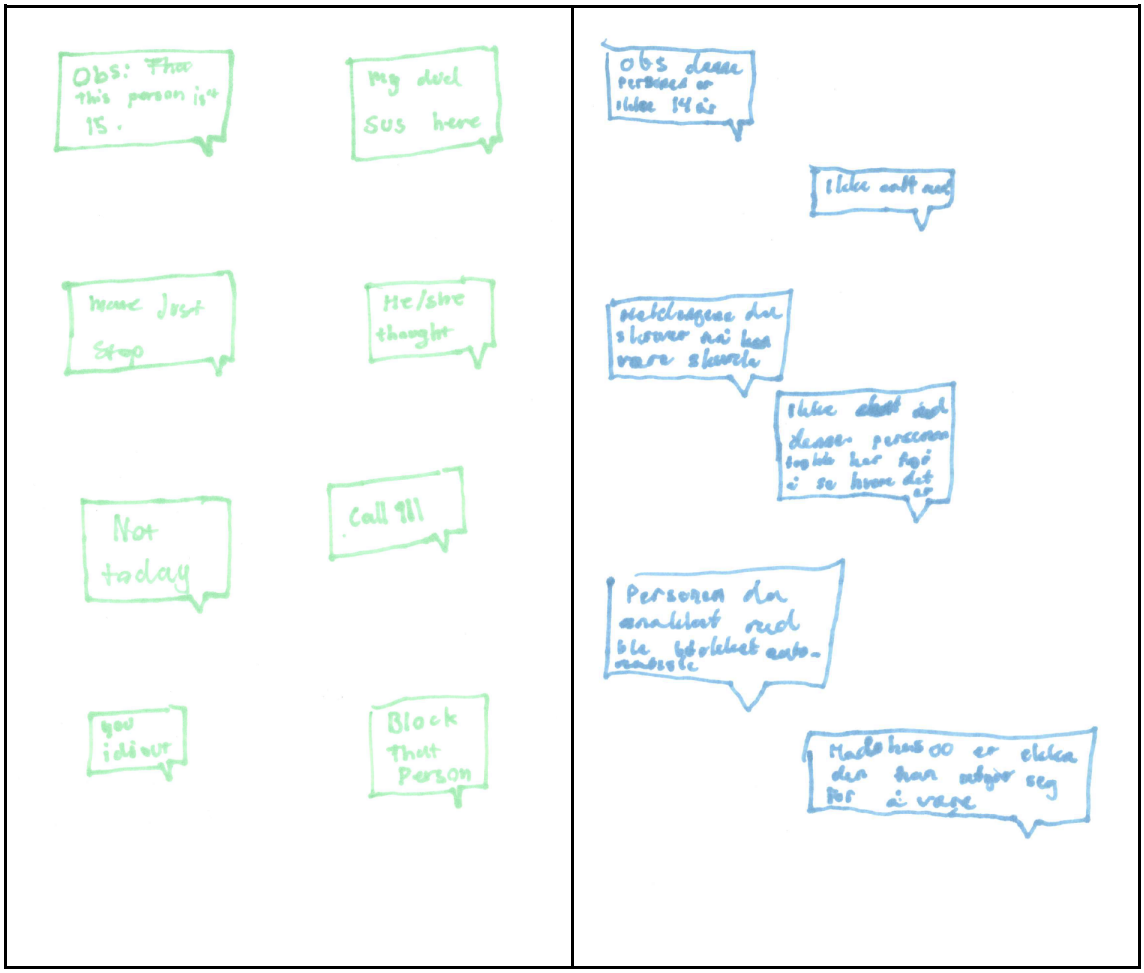
CT NAME ..... AIBA .....






Friends/groups
AIBA
APPer: av/ på
Snap
insta
Messenger
Meldinger
Discord
← SWIPE →
Stay safe
Stay alive!
Status - ok
Danger: 30%
Potential predato
blokk
blokk
blokk
Varsligner:
Friends/groups
Status: OK
Danger:
30%
potential predators

7.6.4 Crazy-8s


Obs: Fhor this person is 15.
My dwel sus here
Meme Just Stop
He/she thought
Not today
Call 911
Block That Person

Warning!!!!

Block
Report

Warning

send a
message
to a parent

Rapporter
brukeren

98%

At denne
personen er
farlig for
deg

98%

At det
er en pedo

Warning
Robot har
tunnet
pedofil
i chatten
din

Varsel

Block
Report
ITS, OK

Vær Trygg

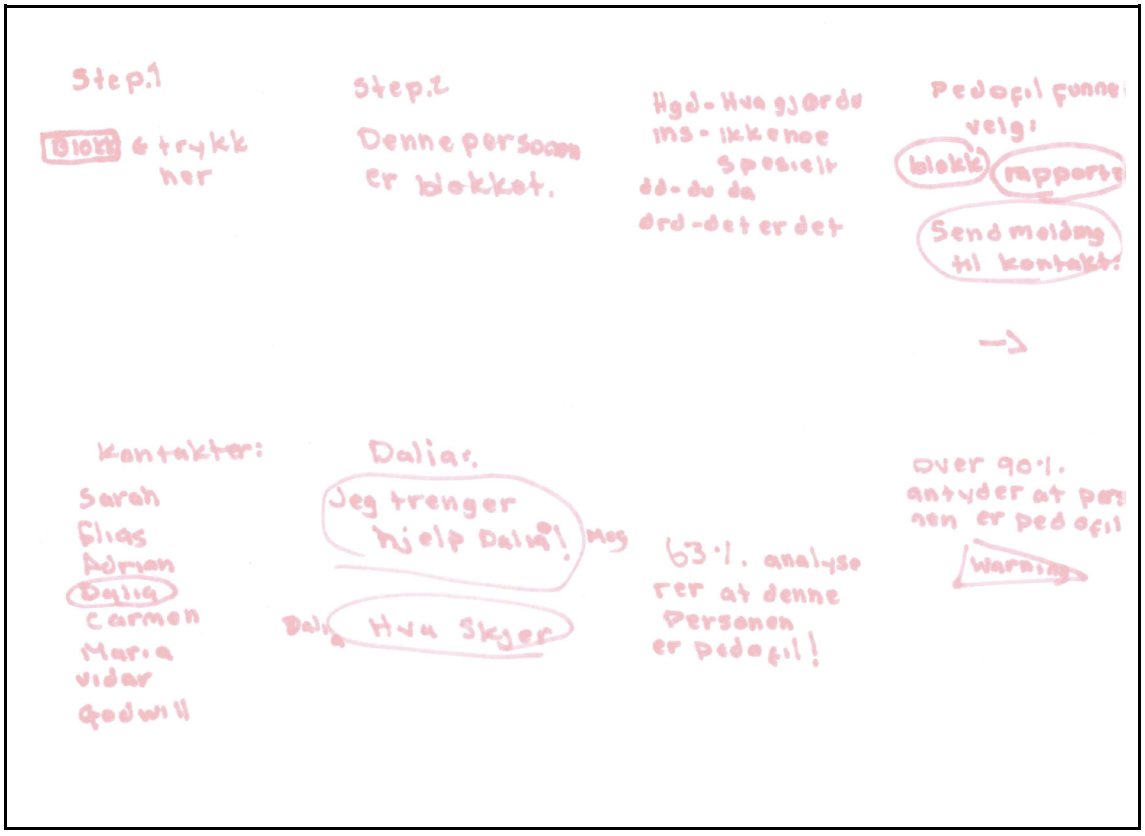
blocr iTS ok
Report

Varsel

Varsel !!!!

32%

Report Ok block


Step.1
Block
Step.2
Denne personen er blokket.
Hgd. Hva gjorde ins. ikke noe spesielt dd. du da drd. det er det
Pedofil funne
velg:
blokk
rapporte
Send melding til kontakt
Kontakter:
Sarah
Elias
Adrian
Dalia
Carmen
Maria
vidar
Godwill
Dalia.
Jeg trenger hjelp Dalia!
Dalia Hva skjer
63%. analyser at denne personen er pedofil!
over 90%. antyder at per nen er pedofil
Warning

7.7 Expert evaluation - questionnaire

Forskningsprosjekt AiBA

Dette prosjektet er en del av masteroppgave i interaksjonsdesign på Norges teknisk-naturvitenskapelige universitet (NTNU). Denne masteroppgaven vil bli innlemmet i AiBA (Author Input Behavioral Analysis) prosjektet veiledet av Patrick Bours. AiBA-prosjektets overordnede mål er å beskytte barn på nettet mot seksuelle overgripere, grooming og nettmobbing gjennom å identifisere og forhindre grooming i online chatterom. Det tar sikte på å identifisere falske profiler i chatte-applikasjoner. Denne studien er ment å skaffe innsikt i kunnskapen om grooming og seksuelle overgripere på nettet. Gjennom dette er målet å utvikle en måte å advare barn i live chatte-samtaler om potensiell fare.

Generelle spørsmål om deg

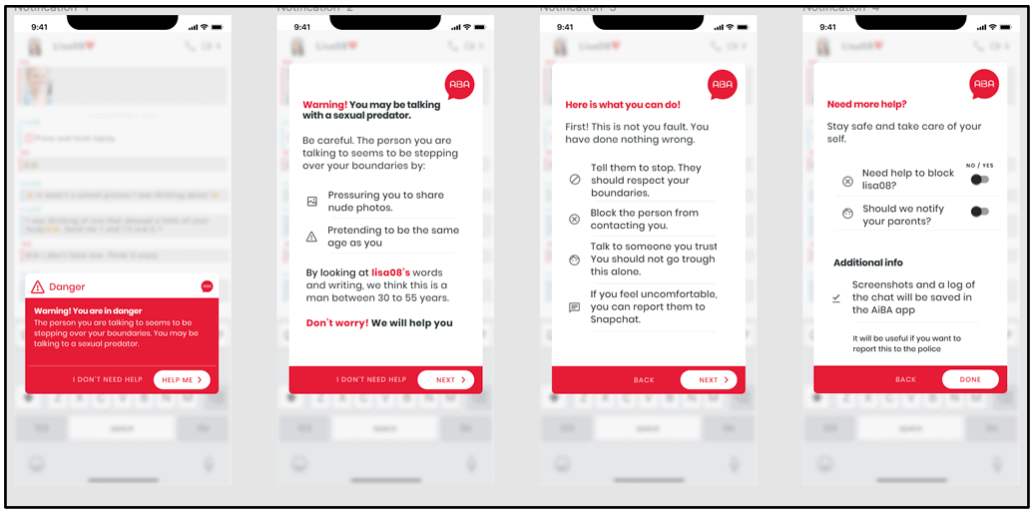
Have you heard about the term "grooming" in the context of sexual predators before? *

Har du hørt om begrepet "grooming" i sammenheng med seksuelle overgripere før?

- ○ Yes
- ○ No

Do you have kids?

- ☐ Yes
- ☐ No



AiBA warning to children in chat

Tenk deg et system som gir deg en advarsel om potensiell "grooming" i chatter. Systemet beskytter barnet og holder foreldrene informert om potensielle farer.

Prototype: AiBA varsler til barn i chatterom

Scenario: Barnet ditt er på Snapchat og blir spurt om å dele nakenbilder. Åpne prototypen og svar på følgende spørsmål: *(Trykk Restart (R) dersom prototypen ikke starter fra begynnelsen av.)*

Did the warning steps..

	Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
1. Describe the risk comprehensively?	○	○	○	○	○
2. Look concise and accurate?	○	○	○	○	○
3. Offer meaningful options?	○	○	○	○	○
4. Present relevant contextual information?	○	○	○	○	○
5. Follow a consistent layout?	○	○	○	○	○

AiBA warning to children in chat - Heuristic Evaluation

Hvid du trenger det kan du se på prototypen igjen:

Prototype: AiBA varsler til barn i chatterom

Scenario: Barnet ditt er på Snapchat og blir spurt om å dele nakenbilder. Åpne prototypen og svar på følgende spørsmål: *(Trykk Restart (R) dersom prototypen ikke starter fra begynnelsen av.)*

To what degree did you..

On a scale from 1-5 where 1 is **Not at all** and 5 **Very much**

	1 - Not at all	2	3	4	5 - Very much
Understand the used terms and language?	○	○	○	○	○
Understand the navigation?	○	○	○	○	○
Feel in control when viewing the warning?	○	○	○	○	○
Feel lost or in need of help?	○	○	○	○	○
Rate the consistency of the design?	○	○	○	○	○
Think the buttons and interaction elements were recognisable?	○	○	○	○	○
Get appropriate feedback to you actions?	○	○	○	○	○
Think the warnings concentrated on relevant information and design elements?	○	○	○	○	○

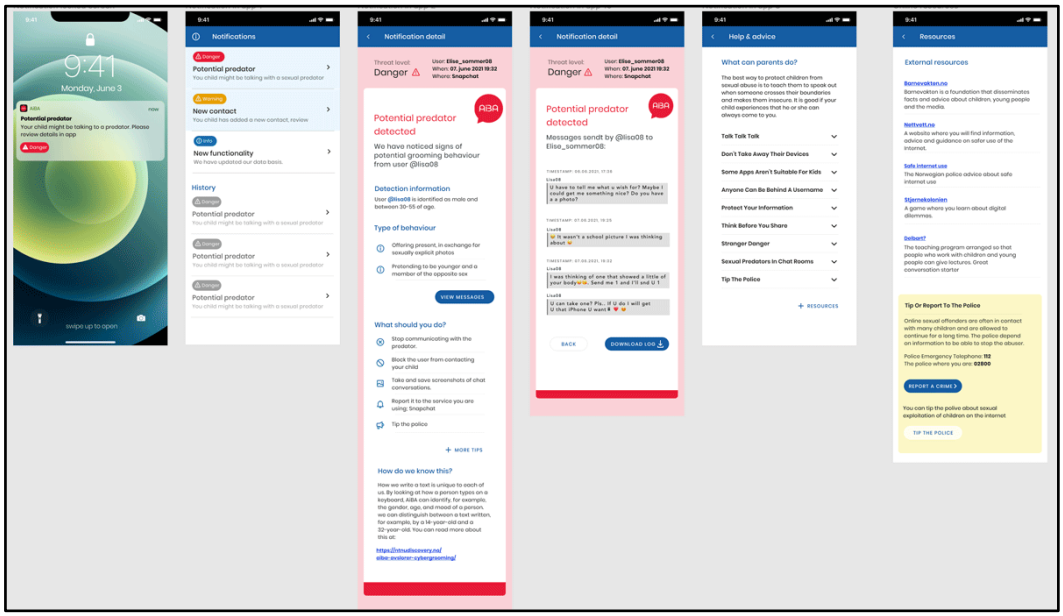
Where there any actions that did not work as expected?

Do you have any other comments?

Notifications from AiBA app to parents

Prototype : AiBA notification to parents

Scenario: Du som forelder mottar et varsel på din mobil om at ditt barn muligens er utsatt for grooming fra en seksuel overgriper på nett. Se på prototypen og svar på følgende spørsmål: *(Trykk Restart (R) dersom prototypen ikke starter fra begynnelsen av.)*



Did the warning steps

	Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
1. Describe the risk comprehensively?	○	○	○	○	○
2. Look concise and accurate?	○	○	○	○	○
3. Offer meaningful options?	○	○	○	○	○
4. Present relevant contextual information?	○	○	○	○	○
5. Follow a consistent layout?	○	○	○	○	○

AiBA notification and warning to Parents in app - Heuristic Evaluation

Prototype : AiBA notification to parents

Scenario: Du som forelder mottar et varsel på din mobil om at ditt barn muligens er utsatt for grooming fra en seksuel overgriper på nett. Se på prototypen og svar på følgende spørsmål: *(Trykk Restart (R) dersom prototypen ikke starter fra begynnelsen av.)*

To what degree did you..

On a scale from 1-5 where 1 is **Not at all** and 5 **Very much**

	1 - Not at all	2	3	4	5 - Very much
Understand the used terms and language?	○	○	○	○	○
Understand the navigation?	○	○	○	○	○
Feel in control when viewing the warning?	○	○	○	○	○
Feel lost or in need of help?	○	○	○	○	○
Rate the consistency of the design?	○	○	○	○	○
Think the buttons and interaction elements were recognisable?	○	○	○	○	○
Get appropriate feedback to you actions?	○	○	○	○	○
Think the warnings concentrated on relevant information and design elements?	○	○	○	○	○

How do you rate

	1 Very low	2	3	4	5 Very high
The risk of online predators grooming children online?	○	○	○	○	○
The usefulness of a warning system like AiBA?	○	○	○	○	○

Do you have any other comments?

Marit Sylstad

Chat Room safety. Keeping children safe in online environments

NTNU
Norwegian University of
Science and Technology