Master's thesis

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

Lara Raffel

Risk Communication: Sexual Predators in Chat Environments

Master's thesis in Interaction Design
Supervisor: Professor Patrick Bours and Associate Professor Sashidharan Komandur
June 2020

NTNU
Kunnskap for en bedre verden

Lara Raffel

Risk Communication: Sexual Predators in Chat Environments

Master's thesis in Interaction Design
Supervisor: Professor Patrick Bours and Associate Professor Sashidharan Komandur
June 2020

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

NTNU
Norwegian University of Science and Technology

Preface

This Master's thesis constitutes the final assessment in the Master programme Interaction Design at NTNU i Gjøvik. It was mainly conducted during the spring semester 2020 and is accredited with a total of 30 ECTs. Preceeding the main work, the thesis was planned in the fall semester 2019, including the conduction of a literature review, which was accredited with 7,5 ECTs. It was realised as part of the AiBA project by the Norwegian Biometry Laboratory. The opportunity to join this project was initiated by my professor Sashidharan Komandur after I turned down a thesis idea that he proposed to me. He then introduced me to Patrick Bours who is leading the AiBA project and soon convinced me to join the team.

This thesis has been written predominantly as a contribution to the AiBA project with the intent to raise awareness about online grooming and protect children from sexual predators on the web. If it helps to save just one child from the darkness, my work has already been a success. In addition, the thesis has been written for people working with or interested in design methods for user research as this constitutes the main effort. Although I possessed little knowledge of the subject when starting to work on the thesis, it also presents the fundamentals of risk communication. This field particularly caught my interest as it can be practically applied in a vast amount of contexts and had proven to be a practice that could hardly be more topical during the COVID-19 pandemic. The interdisciplinary nature of the thesis is meant to encourage people working in design, communication and computer security to cooperate. It shows that the skills and methods taught in the Master programme Interaction Design at NTNU can be applied to a variety of fields outside the traditional design context.

The thesis consists of six sections. The first five sections follow 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. The last section presents a related paper that has been written about the ongoing research work and was submitted for publishing as a conference paper before this Master's thesis was completed.

NTNU i Gjøvik
01-06-2020
Lara Raffel

Acknowledgment

I would like to thank my supervisor Patrick Bours for letting me join AiBA and providing me with great support during the project. My thesis benefited greatly from his contacts to local schools and the seminar days that he organised. On this note, I also want to thank Blomhaug Barneskolen for participating in my study, the teachers who were open to integrate our workshops in their teaching and especially the amazing kids who could not have been more cooperative and helpful.

My thanks also go to my second supervisor Sashidharan Komandur who has given me valuable advice regarding my choice of methods and how to carry them out during the COVID-19 lockdown with its restrictions and challenges. Additionally, he was the driving force behind the submission of my first conference paper which was something I had never thought I would accomplish as a Master student.

I greatly appreciate the support and love I receive from my family, especially my mum and my aunts who had silenced all the doubts I had before coming to Gjøvik. Knowing that they are always there for me motivated me to excel and make them proud. I also want to thank my friends, new and old ones, for making my studies abroad a fantastic experience and for staying with me even though I was away. Special thanks go to Volker and Oleg who had the patience to read through this thesis and provided me with great feedback.

Last but not least, I would like to point out the importance that the international study environment has played for me. Meeting and working with so many different people has shown me the value of diversity. We can accomplish more if we work together, regardless of borders and nations. I would not be where and who I am today if I had not taken the decision to come to Norway during my bachelor studies in 2016, which has turned out to be the best decision of my life so far.

L.R.

Abstract

With the ever-increasing digitisation of our lives, online conversations through chats and messenger services have become an essential part of human communication habits. The global village that the world has become through the Internet enables friendships between people who have never met physically, however, it simultaneously poses new challenges and risks. When chatting with strangers, how can one be sure of their true identity? The relevance and importance of this question significantly increases when considering the safety and security of children who are accessing web-enabled devices at an increasingly younger age. Concurrently, the amount of reported cases of online sexual solicitation and so-called "grooming" of children is unfortunately rising steadily. Using an interdisciplinary approach, this thesis investigates preventive methods to protect children from sexual predators who use grooming strategies to bond with their victims. Following principles of risk communication and interaction design, the information needs of the different target groups - schoolchildren and their parents - are evaluated and translated into a communication strategy. The communication materials were developed following a user-centered design approach.

Results suggest that target group-appropriate education about the subject increases awareness of the risk and thus positively influences overall behavior and caution to improve online safety. The thesis is incorporated in the AiBA project which monitors chat conversations through behavioral biometrics and text analysis in order to warn users about fake identities and predatory behavior.

Sammendrag

Chat og meldingstjenester på nett er blitt en vesentlig del av menneskelig kommunikasjon som følge av den stadig økende digitaliseringen av våre liv. Den globale landsbyen som er oppstått gjennom internett lar oss knytte vennskap med mennesker vi aldri har møtt fysisk, men fører også med seg utfordringer og farer. Hvordan kan vi være trygge på identiteten til den vi snakker med? Dette spørsmålet blir desto viktigere når man tenker på tryggheten og sikkerheten til barn som bruker internett i stadig yngre alder. Dessverre øker antallet rapporterte tilfeller av online grooming og seksuelle tilnærminger mot barn jevnt parallelt med denne utviklingen. Denne tverrfaglige masteroppgaven undersøker metoder for å beskytte barn ved å forhindre seksuelle overgripere fra å bruke grooming til å knytte bånd til sine ofre. Med utgangspunkt i prinsipper om risikokommunikasjon og interaksjonsdesign må informationsbehovene til de forskjellige målgruppene - barn og deres foreldre - vurderes og omsettes i en kommunikasjonsstrategi. Kommunikasjonsmateriellet ble utviklet med en brukersentrert designtilnærming.

Resultatene antyder at informasjon tilpasset brukeren øker bevisstheten om temaet, og dermed påvirker oppførsel og varsomhet i positiv retning. Dette bedrer sikkerheten for brukerne. Masteroppgaven er del av AiBA-prosjektet, som overvåker chat-samtaler gjennom adferdsbiometri og tekstanalyse for å advare brukere om falske identiteter og mistenkelig adferd.

Contents

List of Figures

Acronyms

NTNU	Norges Teknisk- Naturvitenskapelige Universitet
AiBA	Author Input Behavioral Analysis
BPG	Before Presentation Group
APG	After Presentation Group
WHO	World Health Organization
GAAMM	Goals, Audiences, Appeals and barriers, Media and messengers, Message

1 Introduction

1.1 Keywords

Chat security, warning design, risk communication, human factors, user centered design, grooming.

1.2 Topics Covered

The thesis covers theories from the fields of IT security, risk communication, interaction design and human factors. It can therefore be described as an interdisciplinary thesis that contributes to each of these fields and promotes cooperation between them. Behavioral biometrics form the basis of the AiBA project, and the applied approaches will be explained briefly. Interaction design plays an important role as the thesis investigates the importance of user-centered design and its consequences for the communication of information. It makes extensive use of established design methods such as surveys and focus groups to conduct a thorough user research. The gathered data is in turn evaluated by additional design methods such as thematic analysis, affinity diagramming and gamestorming methods. The domain of human factors is covered by evaluating the effectiveness of the communication strategy and the audience's reaction to it, as well as by assessing ethical concerns related to the subject. Risk communication is the thread that leads through the thesis, from researching information needs to the creation of a communication strategy for educating children and parents about sexual predators on the web.

1.3 Problem Description

This thesis is part of the AiBA (Author Input Behavioral Analysis) project supervised by Patrick Bours. The project aims at identifying fake profiles in chat applications through biometry, text and media analysis in order to protect children from sexual predators, grooming and cyber bullying. Educating and informing parents and children about potential risks in that context is a central part of this project. Risk communication focuses on mediating information about risks before, during and after an incident and is therefore considered a valuable addition to the project's development. Firstly, making children and parents aware of sexual predators on the web will increase the likelihood of using the application and being overall more careful when conversing in chat environments. If both parents and children understand the risk, it is assumed that they are more likely to accept running the application on their devices, thus increasing the app's effectiveness. When the application is installed and a conversation follows the pattern of predatory behavior and detects an immediate risk, a warning is sent out. This marks the second stage of risk communication, the event of actual danger. However, the design of these warning messages has to be adapted to the recipient. The child will need different information about the immediate risk and how to react to it than the parents, or a chat administrator. Lastly, the third stage of risk communication describes

how one should behave after an incident when the immediate danger has been avoided. It aims at preventing further incidents and providing additional information.

The thesis will present a strategic plan for the AiBA project about communicating the risk of sexual predators on the web that is adapted to the target audiences. Conducting a risk assessment based on thorough user research in order to tailor information about risk factors to the target audience will be a central concern of this thesis. A strategy to communicate the risks of sexual predators on the web will be developed, incorporating all three stages from before, during and after the detection of predatory behavior. It will be investigated how a sensitive topic like sexual harassment can be addressed in an appropriate manner and how information should be communicated. Additionally, ethical and legal considerations will be evaluated and taken into account.

1.4 Significance, Motivation, and Benefits

Since children want to maintain a certain level of privacy and engage in chat conversations without the supervision of their parents, making them aware of the potential risks of sexual predators is key to a safer chat behavior. Enabling them to detect and avoid dangerous situations in the first place will contribute to their safety on the web. Using the AiBA application will add another layer of safety for the child, and will also help to reassure the parents that the child is not conversing with people who have dishonest intentions. This gains importance as technology and the internet have become a substantial part of children's lives at an increasingly younger age, while reports of negative experiences on the web are rising (Smahel et al. 2020). In case of detecting a predator with the AiBA application, the risk communication strategy will advise for appropriate actions that need to be taken, reducing the level of fear and stress faced by parents and children. Being involved in the AiBA project that is being funded by NTNU Discovery and the Norwegian Research Council offered great advantages for the development of this thesis as the project framework was used to make contact with relevant participants for focus groups and surveys as well as for evaluating the results.

Risk communication in general is an established and well-researched practice in the public health department, political institutions and environmental agencies that deal with natural disasters. It is believed that the approaches from these fields can be transferred to educating children and parents about grooming and sexual predators on the web. By raising awareness and knowledge about that topic, not only will the children and parents feel safer and more prepared, but it might also deter predators since they will face additional obstacles.

1.5 Research Questions

The thesis will work towards answering the following research question:

- Can a communication strategy be built for warning against sexual online predators and does it increase awareness of grooming strategies and caution when conversing in chats?

In order to answer this question, several issues need to be addressed:

- How can awareness of sexual predators be increased?
- How does awareness-building influence chat behavior?
- What information do the different audiences need at each stage of communication?
- What emotional responses can be triggered by such a sensitive topic?
- How can the risks be communicated without inducing irrational reactions?
- What ethical and legal issues arise from this topic?
- How can the findings be implemented in a project such as the AiBA project?

1.6 Contributions

The findings of the thesis contribute to the AiBA project by designing a strategy for risk communication about sexual predators on the web. To do so, the risk factors of the target groups will be evaluated and presented in a risk assessment and mental models, applying methods and approaches from the field of risk communication as well as established design methods. It results in applicable guidelines that will help the further development of the AiBA project.

The interdisciplinary nature of the thesis shows the advantages of including approaches and methodologies of different fields to create innovative and effective solutions. It therefore contributes to creating bridges between professions and research areas of different subjects. In addition to delivering a completed Master's thesis, the project resulted in a conference paper for the HCI International Conference 2020 in Copenhagen.

2 Background

2.1 The AiBA Project

The AiBA (Author Input Behavioral Analysis) 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 has received funding from NTNU Discovery in October 2019 and from NFR Forny in December 2019.

The project aims at identifying fake profiles in chat applications using a machine learning approach within the field of keystroke dynamics and stylometry, in particular for protecting children from sexual predators that find their victims online. For example, behavioral biometrics such as typing rhythm can reveal an adult pretending to be a teenager in order to get in contact with children, often with sexual intentions, a practice known as grooming. Writing style on a keyboard is unique for each individual which enables the system to make predictions about the identity of a user. Based on word usage, writing rhythm and media input, the algorithms are able to distinguish between adults and children as well as between males and females. For example, certain abbreviations or buzzwords are only common among certain age groups. Also, women tend to use more words, while men are usually very direct and use shorter sentences. The algorithm is capable of identifying patterns in the writing, thus being able to make highly accurate assumptions about the users. While abusers might be able to adapt their language to build a new identity, keystroke dynamics are hard to change, thus increasing the difficulty of deceiving the algorithm. Keystroke dynamics are therefore an effective way for profiling. In addition, the system distinguishes between normal conversations and grooming, as some abusers are not hiding their identity, but try to build relationships with children nonetheless, with the goal of building trust and committing sexual abuse. Data from convicted abuse cases is used to train the algorithms, in addition to chat data that has been acquired from children using a chat prototype. In particular, the system has been trained and tested on short messages with minimal information like they are typically used in chat applications. To mark suspicious conversations, the system is performing a continuous real-time analysis of the chat messages by applying natural language processing features and machine learning techniques. AiBA has been evaluated in terms of reliability and validity, showing that the system can correctly identify predators after less than 100 messages, while an average chat conversation consists of around 3000 messages.

It is envisioned that the algorithms will either be built into platforms and applications used by children, such as gaming platforms like MovieStarPlanet or social media like Snapchat and Instagram, or will act as a standalone application that retrieves data from the chats. Alerting the users that such a security measurement is in place will already contribute to deterring those with dishonest intentions, since there is a higher chance of being disclosed. Once the algorithm discovers

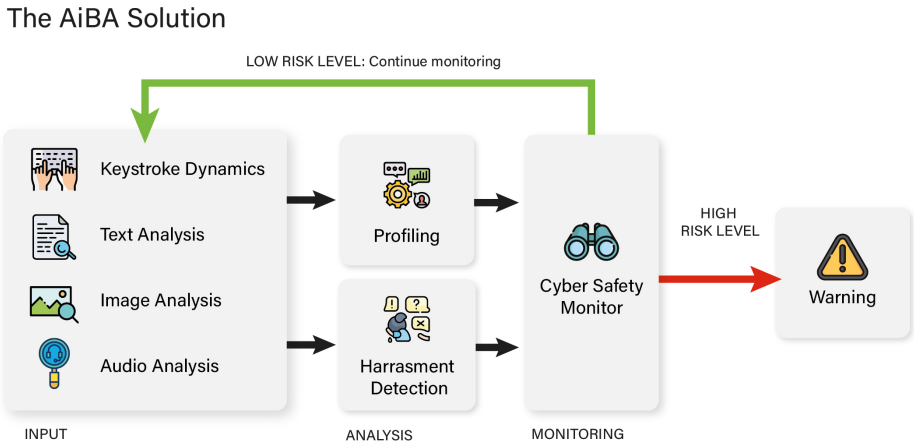


Figure 1: AIBA system structure

suspicious behavior, a warning is sent to the child conversing in the chat, as well as to the parents or the moderator of the platform. The nature of these warnings and how to design them to increase effectiveness will be the main point of interest of this thesis, building upon relevant literature and applying a user-centered design approach. Going one step further, the AiBA project can support the police with solving abuse cases where online conversations are involved. The algorithms analyse large amounts of text and retrieve sensitive data to help investigations.

2.1.1 Functionality

As outlined above, this thesis will focus on implementing advances in the theory of warning design and risk communication to describe guidelines for developing target group-oriented warning messages. However, it is important to understand the context and structure of the system in which the warnings will be incorporated. Figure 1 shows a visualisation of the process that is executed when the application is running. When a chat is started with the system enabled, the algorithms will analyse input during the conversation. In the first module, the system evaluates keystroke dynamics such as typing rhythm, speed and how long individual keys are pressed as well as text input, analysing buzzwords, amount of words, questions and topics of the conversations. Additionally, if media is sent, the algorithm scans for inappropriate contents. During the analysis, the system is profiling the users to detect age, gender and mood. In the second module, natural language processing is applied to available image or audio input to check for sexual harassment. It aims at minimising falsely labelling innocent conversations as grooming and maximising the detection of sexual predators. A cyber safety monitor oversees the safety of the conversation by assessing the level of risk. If the risk is below the threshold, the system continues to analyse the input. However, if the analysis

returns patterns that fit dishonest behavior and the risk is above the threshold, a warning needs to be issued immediately since the child could be in danger. At this point, two types of mistakes can happen. A type I error lets a predator go undetected (recall), meaning that the security threshold is too high. On the contrary, in the case of a type II error (precision), an innocent person gets accused of being a predator, thus the security threshold is too low. Since it is more desirable for the safety of the child to not let predators go undetected, avoiding type I errors should have higher priority. Precision and recall can be translated into an F-score based on the occurrence of type I and II errors. AiBA has achieved an average F-score of 0.88 which exceeds state-of-the-art research (0.87). The F-score for recall reached 0,87 and 0,89 for precision. The value should be as close to 1 as possible. To give an example, it can be assumed that a chat with 100.000 people consists of 1000 predators and 99.000 non-predators. A recall of 0.87 means that AiBA will detect 870 predators and miss 130. Precision of 0.89 means that it will suspect 107,5 innocents to be predators. It is believed that the F-score will be further improved with more training of the algorithms. Once the risk assessment is monitoring a high risk, a warning has to be sent out. It is part of this thesis to determine who is warned at what stage of the process. The warning is not meant to intrude the child's privacy in the chat, but to inform about the possibility of dishonest intentions and to advise on countermeasures. In cases with extremely high risk, a warning might also be sent to the platform administration.

2.2 Grooming

There is a wide and profound range of literature on the concept of grooming. Although it is not a new phenomenon, the last two decades have produced a vast amount of professional research. Numerous articles propose definitions to describe the term, although there is still disagreement about its precise meaning despite its common usage (Craven et al. 2006).

Grooming has been described as behavioral patterns that are employed by sexual predators to prepare a child for sexual abuse (McAlinden 2006). Colton et al. (2012) describe grooming as a multi-layered process that enables predators to gain access to chosen victims for initiating abuse and potentially maintaining control over time without being disclosed. However, there is no consensus over the explicit approaches and methods that are applied by offenders (Bennett & O'Donohue 2014) and literature suggests that grooming behavior can be hard to identify prior to abuse since it can resemble normal adult-child interactions (Winters & Jeglic 2017). Nonetheless, Winters & Jeglic (2017) have evaluated that there have been approaches that can be classified as grooming in nearly half of all persecuted cases of child abuse in the US. Lanning (2018) has proposed a detailed description of the process, emphasising the non-violent nature of grooming. He describes grooming as a tool for sexual victimization and control without using threats or physical force.

The term "grooming" was first used in the 1970s by US law enforcement and has gained popularity in the late 1980s when FBI agent and consultant Ken Lanning introduced it for educating the public and explaining its impact on the victims. Before that, professionals mainly used the terms sexual abuse, sexual assault, sexual misuse, and sexual molestation interchangeably. The special role of grooming behavior as a preparation for assault was not recognized since most emphasis was put on the assault itself and its after-effects (Burgess & Hartman 2018). However, a shift of

attention in order to help prevention of assaults has led to increasing interest in grooming. Now, the term supplants the more general word “seduction” for describing these behaviors in adult-child interaction. Lanning (2018) has found that the strategies that are employed are dependent on the relationship between the offender and the victim, for instance if they are strangers, acquainted or even family members. However, it is hard to distinguish grooming behavior within families, since engaging in these concepts is considered normal, for instance rewarding a child with gifts, money, privileges or affection. If this is used to commit sexual abuse, the term “coercion” is more fitting (Lanning 2018). Also, in relationships between two adults or two teenagers, most of the practices in grooming behavior can be considered normal parts of “dating” (Lanning 2010). Burgess & Hartman (2018) point out that the evolution of language around sexual assault influences the treatment of the victims and offenders alike, since it allows more specific and distinguishable descriptions of the offenses.

Legally speaking, grooming is in most cases considered as a lesser offense. According to Lanning (2005), the resulting cooperation of the child as a response to the grooming strategy is often falsely interpreted as consent or a lack of victimization. Instead, the child’s response should be viewed as an understandable human behavior, even more so when considering the young age of most victims. Lanning (2018) was clear to point out that a punishable crime has been committed no matter how the child reacts to it or what method of control has been employed.

2.2.1 The Grooming Process

By definition, grooming explicitly describes non-violent strategies to gain control over victims. Lanning (2010) has pointed out that non-violent techniques are more likely to result in cooperation from the victim’s side and secure constant access while at the same time decreases the probability of being disclosed. If at all, violence and threats are only used to avoid disclosure or if the victim wants to end the relationship. However, Lanning & Dietz (2014) point out that the grooming process and its precise steps are dependent on the characteristics of the picked victim, such as the child’s needs and vulnerabilities as well as its relationship to the molester.

Literature suggests that grooming is employed as a process that consists of a sequence of stages (Lanning (2010); McAlinden (2006)). As proposed by Lanning (2010), the incremental stages of the grooming process start with the identification of victims based on individual criteria. Once the victim is chosen, the predator gathers information about the child’s interests and vulnerabilities. The offender then tries to access the child through an available channel, for instance through clubs, sports or online. The offender gains the victim’s trust and controls the child with different strategies based on the child’s vulnerabilities, like filling emotional or physical needs, offering sympathy or applying peer pressure. Employing these strategies requires constant access to the victim, dedication of time and social skills as well as “the offender being, or at least perceived as, a nice guy” (Lanning 2018). Lanning also states that offenders who practice grooming do not always aim at engaging in physical abuse of their victims, but gain gratification from the grooming process itself.

In the first step, the offender selects a victim which can be influenced by several factors such as physical characteristics and attractiveness, perceived vulnerabilities and how easy the victim is

to access (McAlinden 2006). The latter two are often influenced by the child's family situation. Empirical research has found that children from dysfunctional families are more likely to be targeted by child molesters (Olson et al. 2007). Furthermore, situations that leave the child with less parent supervision such as single house-holds result in higher risk for the child (Elliott et al. 1995). Vulnerabilities that can be exploited by molesters are mostly psychological in nature, such as low self-esteem and confidence, insecurity, isolation and naivety (Olson et al. 2007). However, the initial targeting can be based on information that the child presents in his or her online profile, such as their profile picture or username. Winters et al. (2017) have found that profile pictures or usernames do not need to be sexual in nature in order to be targeted by predators. Regarding usernames, it has been found that children with young sounding usernames are more at risk of being targeted. It is recommended to not unveil one's name, age or location in a chat username, as well as avoid using nicknames that evoke sexual associations. The literature describes the selection process as highly strategic and planned.

In the second step, the offender tries to gain access to the selected victim. In the 1980s, there was increasing awareness of child offenders using youth organizations such as clubs, boy scouts or sport teams to gain access to victims (Lanning 2018). Without using physical force, the offender manipulated the victim by employing a combination of in-creased attention and affection, making (monetary) gifts, granting special privileges or providing drugs and alcohol. Nowadays, the internet and applications that are popular among children offer a new platform for offenders to engage with potential victims.

The central part of the grooming process involves developing trust and cooperation. This is realized through building an apparent friendship with the child by showing interest in hobbies, being understanding and helpful, sharing secrets and generally giving the child a lot of attention so that the children perceive the perpetrator as someone they can talk to (McAlinden 2006). The precise strategy in this step is highly dependent on the victim's age as this influences the child's interests (Lanning 2010). The developed trust can be used by the offender to manipulate and control the child, for example to pressure it into sending pictures or videos of increasingly sexual nature or to agree to a physical meeting (Winters & Jeglic 2017). If an offender fears disclosure, it is likely that he will adjust and change the grooming strategy, thus making identification even more difficult (Conte et al. 1989).

2.2.2 Online Sexual Grooming

With the Internet and its growing number of chat applications and social platforms, sexual predators have found a new channel to gain access to victims. Additionally, the internet provides anonymity and a wide reach to identify victims. Online predators use grooming as a means to engage in cyber-sexual activity, get access to child pornography or to arrange in-person meetings with their victims (Lanning 2005). Online chat rooms are a popular way for offenders to locate and engage with victims (Malesky 2007). However, it has been suggested that online sexual offenders are qualitatively different from offenders who practice in-person grooming. Babchishin et al. (2011) compared online and offline offenders through a meta-analysis and found that online offenders are significantly

younger, with an average age of 38.6 years. Also, while the grooming process is similar to in-person grooming, it has been found that the order and timing of the tactics might differ (Black et al. 2015). Online grooming strategies are even more dependent on the individual child than conventional grooming behaviors (Whittle et al. 2015). Staksrud (2013) adapted the grooming process model to the online environment and identified three stages. In the first stage, the offender solely observes the chat room without participation in communication until a victim is identified. Then, the offender engages in a conversation that is preferably personal and private. Finally, the main grooming tactics are employed to manipulate the child and push it towards sexual activities, either online or in-person. To further describe the main grooming tactics, O'Connell (2003) proposes five stages. The offender begins the process with friendship-forming and relationship-forming where information is gathered about the victim which is used to relate to the child. In the next stage, the offender assesses the risks of being disclosed and how secretive the child behaves about their conversations. If the offender feels secure enough, he attempts to bond further with the child by making the relationship seem exclusive and special. In the last stage, the conversation will start to include sexual content by pressing the child's boundaries, introducing explicit material or engaging in fantasies.

The public's awareness of online sexual grooming was raised significantly with the release of the TV show "To Catch a Predator" that aired in 2004 and showed encounters between the police who previously posed as children in online chats and predators who believed to meet the supposed child they conversed with. In a similar experiment by Winters et al. (2017), predators were made believe that they converse with a child in an online conversation. The offenders (which were all male) introduced sexual content mostly in a very early stage of the conversation which contradicts with O'Connell (2003) and Staksrud (2013) models. The duration of the contacts between the offenders and the supposed children varied greatly, ranging from one day to almost a year. Marcum (2007) suggests that the length of the conversation depends on the offender' intention of meeting the victim in-person or only engaging with it online. In this context, Briggs et al. (2011) argues that online offenders are driven by either of two goals. The first one is fantasy-driven and solely aims at sexually engaging with children online without personal meetings. The second type is contact-driven and uses the internet to set up personal meetings with children. The majority of offenders in the experiment conducted by Winters et al. (2017) suggested in-person meetings within a short period of time.

Marcum (2007) points out that online predators mostly state their gender, age, and location directly at the beginning of a conversation. At this point, it can be differentiated between "true-representation" of age and gender and "deceptive-representation" where the offender creates a fictional persona (Williams et al. 2013). Malesky (2007) found that up to one third of convicted online offenders pretended to be children themselves. It has been suggested that children who lack social support or feel isolated are more likely to engage in online conversations with strangers who show acceptance (Williams et al. 2013). Staksrud (2013) further points out that "the Internet does not make children more vulnerable, but might make already vulnerable children more accessible". Also, Malesky (2007) argues that children who explicitly state their age in their profile, use

young-sounding usernames or show neediness or submissiveness are more likely to be targeted by predators.

2.2.3 Identifying and Preventing Grooming

Unfortunately, the results of grooming are easier to identify than the process itself, since it can be hard to distinguish between early stages of grooming and mentoring, educating, parenting or other adult-child interactions (Winters & Jeglic (2017); Craven et al. (2006)). Nonetheless, empirical research employed by Canter et al. (1998) has found that almost half of all reported cases of sexual child abuse had been preceded by grooming behaviors. Winters & Jeglic (2016) have identified a hindsight bias phenomenon, showing that people overestimate their ability of identifying grooming behavior after an abuse has been committed. This results in parents and communities being blamed for not preventing the abuse. Winters & Jeglic (2017) point out that differentiating between normal interactions and sexually motivated grooming behavior is even more difficult when the involved people are not educated about grooming strategies. They emphasize the importance of spreading knowledge about child molesters and their grooming tactics, as well as how they might be identified prospectively, in order to protect children and prevent sexual abuse. They propose that parents can be educated on a community level through leaflets at frequented locations such as kindergartens and schools, public announcements and websites that aim at families. They emphasize the need to educate teachers, school staff and others that are in frequent contact with children. Coverage through the media, e.g. through TV shows such as “To Catch a Predator”, also capture public interest and mediate the danger of sexual online grooming. Initiatives such as CEOP (Child Exploitation and Online Protection Command) are raising further awareness of the subject and facilitate reporting of online grooming and abuse, to the extent that online solicitation of children is now one of the most reported inappropriate online behaviors and regarded as a serious social problem (Winters et al. 2017). Furthermore, children should be informed about the potential danger in a manner that is appropriate to their age, e.g. through their schools (Winters & Jeglic 2017). The literature suggests that a better understanding of grooming will be highly beneficial to preventing abuse.

2.3 Risk Communication

Risk communication describes communication measures that prepare an audience for informed decision making about a risk, including prevention methods, immediate reactions and recovery measures. It promotes positive behavior change and aims at building trust (Gamhewage 2014). Risk communication has its origins in the public health sector where it is practiced for communicating health risks and providing relevant education. The Oxford dictionary of public health describes risk communication as “The process of informing and educating all persons exposed or potentially exposed to a specified risk about the qualitative and quantitative dimensions of the specified risk.” (Last & Porta 2018). The practice has been adapted to risk management of natural disasters such as floods and fires, educating and preparing the population living in risk areas. Also, the underlying principles can be adapted to a smaller scale, for example in the design of warning messages and labels (Lundgren & McMakin 2009).

Risk communication can – like other forms of communication – be represented by communication models, such as the traditional model by Shannon (1948) that describes communication as a message that is sent through a channel from a source to a receiver. However, Gamhewage (2014) describes how risk communication has adapted to changes in society and advances in technology. It has evolved from a one-way communication of information about risks and how to mitigate them to a two-way and multi-directional communication strategy. Gamhewage (2014) finds three main reasons for this shift. Nowadays, less trust is put in experts and authorities, meanwhile people have developed a tendency to look for information online, often on social networks or other peer sources. Also, the media has shifted towards fast coverage and journalism that neglects using verified sources and focuses on opinions rather than good research. This has resulted in the need to actively engage the population and use a variety of channels to educate them about potential risks so that they can make informed decisions to protect themselves. Therefore, successful risk communication does not only require profound knowledge of the communicated subject, but also expertise in using mass media, social media, emergency communication and psychology.

Numerous practical approaches to risk communication have evolved from different disciplines so that one needs to investigate the context and the target audience for choosing a fitting approach Lundgren & McMakin (2009). Thus, at the start of the risk communication it is recommended to conduct a risk assessment for evaluating the risk groups among a population, expected effects of the risk and their duration. This information forms the basis to determine how a risk is communicated. Then, a strategy for how to achieve the communication goals and how to reach the audience is developed. Finally, clear and understandable information about recommended actions in case of imminent danger needs to be communicated. Boholm (2019) argues further that risk communication is always carried out within an institutional framework, so that the organizational context should be taken into account as well, thus making the process much more complex. Due to its user-centered perspective, the mental model approach (Lundgren & McMakin 2009) has been chosen for this project as will be explained in the methodology section.

2.3.1 Goals of Risk Communication

Literature (Lundgren & McMakin (2009); Gamhewage (2014)) describes that the goals of risk communication include education about a topic, starting with a rise of general awareness and knowledge about specific hazards and risks so that acceptance of risk management measures is increased. Also, risk communication promotes protective behavior and informs about how to behave during an incident, so that the audience can protect themselves and others against risks. Therefore, risk communication promotes a change of beliefs and a change in behavior. At the same time, it also reassures the audience, thus reducing anxiety and over-emotional behaviors. This can also be realized through an improved relationship and mutual dialogues between all involved actors. Boholm (2019) argues that communication goals are highly dependent on the involved parties and the reasons for communication. Therefore, the goal can vary greatly, from raising awareness to the empowerment of the audience to make well-informed decisions based on the provided information.

Gamhewage (2014) encourages that the reach of these goals should be measured in order to assess the success of the communication strategy and adjust it if necessary. The success or failure of risk communication can be determined by two main factors; how the same risk is perceived by experts compared to the public, and how trustworthy the communicated information is perceived. It can be counterproductive to disseminate information in a generic way without context. While experts assess risks methodically according to the level of hazard and how vulnerable an exposed population is to that hazard, the public judges a risk according to their emotional engagement with it (Sandman 1988). In his classic review that summarizes decades of research in risk perception theory, Slovic (1987) adds that people's perception of risks includes complex processes on a cognitive and psychological level and he shows the complexity with which risks are assessed by the general public. People make use of mental models or heuristics in order to make decisions in unclear or risky situations. Language has labeled this method with many terms such as 'common sense', 'rule of thumb' and 'intuition'. However, these heuristics also encourage biases such as stereotyping or avoidance behavior. Slovic (1987) gives an example:

> "[...] when eggs are recalled due to a salmonella outbreak, someone might apply this simple solution and decide to avoid eggs altogether to prevent sickness".

He also explains the concept of authority heuristics, that occurs when a figure of authority – such as a (religious) leader – is followed or believed only because of their authority position. This can pose additional challenges for risk communication and understanding the audience's perception of risk.

2.3.2 Effectiveness of Risk Communication

The effectiveness of risk communication can be described as the extent of achieving the intended aim of the communication strategy (Kasperson 2014). Effectiveness can be assessed based on the message's content, its sharing process and on the overall goals of the communication (Arvai & Rivers 2014). This includes the accuracy and relevance of the information about the risks, how it is received and understood by the target audience and to which degree the audience shows behavioral changes or collaboration. Kasperson (2014) emphasizes that risk communication should also point out uncertainties, especially if it is not clear when or how they can be resolved. Slovic (1987) proposes that risk communication should aim to be objective, honest, consistent and open for dialogue. He argues that psychological findings on risk perception should be considered and that ethical concerns should be taken into account. It is believed that people are more emotionally engaged and therefore more aware of risks that are unfamiliar to them and that they have not encountered before. People are also very sensitive towards risks that are hard to predict or seem unfair, because they affect a vulnerable group such as children. Of course, risks that can lead to severe consequences like death, severe physical or mental harm or major economic losses, are often perceived extremely emotionally (Gamhewage 2014).

Effective risk communication needs to take into account the context of the risk and those who might be affected (Gamhewage 2014). That includes cultural, political, religious, social and eco-

nomic factors. Communication and prevention strategies should include all involved persons, from the individual and its family to the community and institutions. Also, an effective risk communication strategy is distributed through channels that are frequented by the target audience (Lundgren & McMakin 2009). It makes little sense to expect teenagers to pick up a brochure when their main channel of information is social media. In addition, messages containing information should be designed and formulated in accordance with the audience's knowledge, interests and values (Boholm 2019). Lundgren & McMakin (2009) emphasise that understanding the perspective of the target audience(s) is essential for communicators to choose appropriate communication methods. This shows the importance of profound user research in risk communication and justifies the user-centered design approach that was employed in this thesis project. Lundgren & McMakin (2009) further explain that a pretesting of the communication material is essential and ensures its quality and effectiveness. Lastly, Kasperson (2014) pointed out that risk communication requires time and resources as it needs to be persistent.

Trust in the communicated information and in those providing it is essential. Literature suggests that the main factors for building and maintaining trust include accessibility and dependability of information, as well as clear and honest communication (Lundgren & McMakin 2009). Additionally, expertise is key (Boholm 2019). The provided information should be based on expert knowledge, and the provider should show responsibility, truthfulness and supportiveness. The audience should be able to relate to the information, thus it should include authentic experiences and address real concerns. Kasperson (2014) recommends that the process of disseminating information should be redesigned in case of high distrust.

Lundgren & McMakin (2009) identified issues that can lead to constraints in risk communication. They differentiate between constraints on the side of the communicator and of the audience. The communicator can be hindered by organizational issues like a lack of user research and resources or a lack of consistency throughout the communication strategy. The audience can face the communication with mistrust, disagreement, lack of interest or highly emotional responses that pose significant challenges to the effectiveness of the strategy. Such constraints need to be acknowledged by the communicator in order to prevent or overcome them.

2.4 Warning Design

A special role in risk communication is played by the design of warning messages. Taking the AiBA project as an example, a warning will be sent once the system detects behavioral patterns that indicate grooming tactics. In addition to the overall risk communication strategy, this warning makes the user aware of an immediate or potential danger that requires certain actions. The following chapter will have a look at existing literature on warning design in order to establish the groundwork for this design challenge.

2.4.1 Definition

Warning design and evaluation has been the subject of a vast amount of research in the field of Human Factors and Engineering. Laughery & Wogalter (1997) describe warnings as a subcategory

of a larger communication strategy that takes the needs of the end-users and the context of use into account. Wogalter (2006) later defines warnings as communication that is designed to protect people from harm. He categorizes warnings as the third-line defense against dangers in the "hazard control hierarchy". This hierarchy states that first of all, measures should be taken to eliminate the hazard if possible. Secondly, the exposure of people to the hazard should be limited as much as possible. And only as a last step, a warning for that hazard should be designed.

In computer systems, Cranor (2008) defines warnings as communication tools that make the users aware of a hazard and instruct them to react in certain ways to avoid negative consequences. Cranor further differentiates between warning dialogues that present different options to the user as several courses of action are available and warning notices that only provide information about a hazard to enable the user to make decisions in a dangerous situation. Again, it is recommended to use warnings only as a last resource when other communication or actions to reduce the risk have failed.

2.4.2 Design Guidelines

This thesis project will not be concerned with the visual design of warning messages, but will rather look at the conceptual strategy for warning design. Visual aspects of warning will therefore only be mentioned briefly for the sake of completeness.

Literature suggests that a user-centered approach that evaluates the perspectives of the end users is essential when designing effective warnings (Wogalter et al. 2002). Riley (2014) points out that understanding the user's risk perception is a central aspect of designing effective warning messages. She continues that a mental model methodology has been proven to build a good link between risk communication and warning design. Mental models help to evaluate the perceptions that underlie the audience's interaction with a warning and how this perception of risk is in turn influenced by the warning message. For example, a person's perception of a risk is influenced by how familiar that person is with the subject or product (Riley 2014). The more experience one has, the lower is the estimated risk which can lead to overconfidence and carelessness. In turn, studies have found that simply by looking at a warning, the awareness and hazard perception increases (Riley 2014). The following paragraphs present an overview of criteria for designing effective warning messages as suggested by relevant literature.

Noticeability

A warning needs to attract attention and compete with other stimuli in order to get attended to (Wogalter et al. 2002). Therefore, the message needs to stand out and be prominent to capture the users' attention who might be distracted by another task. Research suggests that prominent warnings are more likely to be read, are easier to understand and to remember and have a higher likelihood of influencing the user's behavior in the desired way (Wogalter et al. 2002). The noticeability of a warning is mainly determined by visual aspects such as colour, font and contrast, but can also be enhanced by auditory and tactile signals. Furthermore, the warning needs to be issued at a point of time when there is still time for the user to take countermeasures (Bauer et al. 2013).

Structure

Literature is in agreement that a warning should consist of four main components regarding its structure (i.e. Wogalter et al. (2002); Cranor & Egelman (2009); Bauer et al. (2013)). Firstly, a signal word that attracts the audience's attention, followed by an identification and description of the immediate risk. The warning should then explain the consequences that can arise from the risk, as well as give instructions for further actions to avoid the risk. The signal word aims at attracting attention to the message and give an indication of the severity of the hazard. Wogalter et al. (2002) proposes that the presence of a signal word increases the message's effectiveness and perceived urgency. The four most common signal words are 'danger', 'warning', 'caution' and 'notice', with 'danger' being the one perceived as most urgent and 'notice' as the least urgent. The second component should give a complete, but brief and understandable description of the hazard. This is followed by an outline of consequences that might result from the hazard if no measures are taken by the user. The user should be made aware of the importance to react. The more explicit the wording of the warning, the higher is the perceived hazard (Cranor & Egelman 2009). As an example, sending a message to a parent that says 'Your child is in danger of being sexually abused' paints a much more severe picture than 'There are indications that your child is having a chat conversation with a child offender'. The first version is much more likely to result in an emotional response or even panic, while the second offers a foundation for initiating a conversation with the child about its online acquaintances and chat behavior. Finally, the warning message should give instructions for recommended actions to take in order to respond to the hazard responsibly. These instructions should describe specific and clear instructions that are easy to follow. Bauer et al. (2013) further recommend to follow a consistent layout that goes in line with common established design guidelines such as the Human Interface Guidelines for most common operating systems. This is likely to increase recognizeability.

Understandability

Understandability is among the most important criteria for effective warnings (Bauer et al. 2013). Literature uses terms such as 'clear', 'concise', 'comprehensive' or 'understandable' to describe this aspect. A warning of which the content is not understood by the audience cannot effectively prevent a danger or encourage the recipient to take appropriate actions (Bauer et al. 2013). Both the cause as well as the consequences of the hazard should be made clear to the user (Cranor & Egelman 2009). To be understandable, the message should be written from the user's perspective and use terms that the audience is familiar with (Cranor & Egelman 2009). If a warning message is too long, contains too much professional jargon or inaccurate information, it is likely to be discarded and rendered useless by the audience (Bauer et al. 2013). An effective warning needs to find a balance between the amount and the quality of provided information, so that the user is presented with just enough content to make an informed decision. It should be avoided to have the warning text sound overly intimidating as this will lead to negative associations with the warning dialogues in general. Instead, Bauer et al. (2013) recommend using a supportive and encouraging tone.

Giving Options

A warning message should present clear choices for further actions and provide sufficient information to allow the user to make a well-informed decision between them (Nodder 2005). Furthermore, a recommendation should be made about what actions or choices are the most appropriate or safest. If there are no options available to the user, the warning is not considered a dialog, but a notification.

Context and Additional Information

During the design process, one should take the context into account in which the warning will be presented (Bauer et al. 2013). A warning message is in most cases interrupting a user that is working on a different task. A warning needs to grab attention despite the interrupted task and also compete with other stimuli that the user is facing. The user should be given all necessary information to make an informed decision about how to react to the warning. This includes contextual information as well as relevant auditory information if a warning reoccurs over time (Bauer et al. 2013).

2.4.3 Warning Effectiveness

A common approach to assessing the effectiveness of a warning is to evaluate or test the design. Evaluation describes the process of determining whether a warning has accomplished its intended goals, such as communicating a risk, advising for behavior change etc. (Wogalter 2006). Research has been conducted on different aspects of warning designs, such as graphic aspects like colours or the use of icons, and text related issues such as choice of words or overall understandability. Warnings can be evaluated formatively or summatively (Wogalter et al. 2002). Formative evaluation can be compared to usability testing where a prototype is tested before its release. It supports an iterative design cycle as the gained feedback can be used to improve the design and problems can be identified in an early stage of the design process. On the other hand, summative evaluation assesses the warning after it has been released and is put into its final context. This allows for an evaluation over a longer period of time in a real-world setting. However, identified problems are harder to fix since the product has already been released. Both types of evaluation can be applied to a project to increase the amount of insights.

Criteria that can be used to evaluate the effectiveness of a warning should be based on the goal of the warning message (Wogalter et al. 2002). A general criterion is behavioral compliance that can be measured by interviewing users during a formative evaluation about their intended actions after being presented with the warning. Furthermore, criteria like noticeability, understandability, perceived urgency and recall can be measured subjectively, i.e. through evaluation using Likert-scales. Also, quantitative measures like reaction time to a warning can be taken if appropriate.

Bauer et al. (2013) describe the consequences of ineffective warnings. An ineffective warning results in the user not being aware of or not understanding the hazard, so that the warning message

is dismissed without further thought as it is considered to be unimportant. If the messages point out the hazard, but fail to clearly state what actions to take, the user might be left with frustration as he does not know how to react to the danger. Lastly, if all information and instructions in the message are clear, but the consequences of not following the instructions are believed to be of little importance, the user might not take any actions, because he thinks that it is not worth the effort.

It has been suggested that warning messages quickly result in habituation which significantly decreases their effectiveness (Egelman et al. 2008). To counteract this effect, warnings should be used scarcely.

3 Methodology

With the goal of acquiring profound insights of the perception and knowledge about online sexual predators and grooming strategies, two main methods were chosen: Focus groups with schoolchildren and an online survey with parents of schoolchildren. These methods allow for a thorough understanding of the audiences in a relatively short period of time. They are common methods in a user-centered design approach, so that the perspective, needs and expectations of the end-users play a central role throughout the whole design process. The choice of methods was unfortunately influenced by the COVID-19 pandemic. Originally, it was planned to conduct in-depth one-on-one interviews with the parents instead of using an online survey. This plan had to be rejected due to health regulations that requested the reduction of social contacts. It was considered to hold the interviews digitally through video calls, however, it was pointed out that most parents would not feel comfortable with that situation, among other reasons because of language barriers. Therefore, surveys were chosen to gain insights from the parents and it was believed that the higher amount of feedback would make up for the lesser depth of the insights.

In order to find relevant participants for data collection, local schools were contacted and a cooperation with Blomhaug Barneskolen in Hunndalen, Gjøvik municipality, was established. This made it possible to conduct two project days about "Chat security" at the school and work with 35 pupils attending the seventh grade. During these days, the children were also given a presentation on online grooming, sexual predators and the AiBA project so that it was possible to identify the impact of education about these topics and how the children's behavior is affected. The cooperation with the school also provided participants for the survey among parents on Internet security and grooming, as well as for the evaluation phase.

After the collection, the data was analysed using established design methodologies such as affinity diagramming and thematic evaluation, as well as applying a set of gamestorming methods (Gray et al. 2010). This resulted in a tangible overview of the gained insights which forms the basis for risk assessment, as well as a mental model of the risk that is posed by online grooming. The insights can be used to tailor information to the audience's needs and provide them with constructive and understandable guidelines about safe chat behavior and grooming prevention. Based on this, a risk communication strategy was designed including the creation of illustrative examples of communication materials and a warning prototype. In an evaluation phase, participants were asked to reflect on the information and guidance that is given which in turn was the foundation of refining and adjusting the communication strategy. This chapter will present the employed methods for data collection, processing and evaluation in detail.

3.1 Focus Groups

3.1.1 Purpose

The focus groups aimed at gaining insights into children's perspective of chat behavior, to what extent they are aware of danger and how they react to certain messages. Focus groups gather information through group discussions, but also through observing the participants and their reactions to certain situations. As Tomitsch et al. (2018) explain, they are particularly useful for gaining insights into existing experiences, attitudes and practices in order to understand the audience and build empathy. Since focus groups include several participants at the same time, it is a fast and simple way of collecting a lot of data. Krueger & Casey (2009) describe focus groups as "a carefully planned discussion designed to obtain perceptions on a defined area of interest in a permissive, non-threatening environment".

The focus groups do not aim at asking the children about personal experiences with grooming in chat applications since this would breach their privacy. Instead, the children are encouraged to engage in role-playing to show how they would react to prepared chat messages. The workshop did not only educate the children, but also revealed their intuitive reactions to certain messages.

3.1.2 Identifying Participants

Participants were found through a cooperation with Blomhaug Barneskolen in Hunndalen. Two project days about "Chat Security" were held with 35 pupils who attend the seventh grade. The focus groups were incorporated in these project days so that six focus groups were conducted, each consisting of 5-6 children of twelve to thirteen years. Naturally, they only represent a certain age group and not the whole range of children or teenagers for whom the AiBA application is intended. However, taking the limited time and scope of the project into account, it is considered a convenient approach to include the perspective of at least one specific age group in detail. This approach can be described as convenience sampling, since the children are easily accessible through the local school. However, since they fulfill certain inclusion criteria such as a specific range of age and using chat applications, this aspect of the sampling can be described as purposive. The parents of the children were informed through the school's internal information system and gave their consent there. They were assured that the anonymity of their children is secured at all times since no personal data is gathered. Also, the collected data is stored securely and only those associated to the project have access. In short, the project follows the requirements of NSD (Norsk Senter for Forskningsdata).

3.1.3 Pilot Test

Before the project days at the school, a pilot test was conducted with a test group of four students from NTNU. The purpose of this pilot test was to practice the process of the focus group and to check if the estimated time of 30 to 40 minutes can be met. Although the participants of the pilot test were not part of the age group for the final focus groups, it was possible to identify some minor issues in wording and timing. In the original plan, the children were supposed to draw an avatar for a fictional chat application. However, it was found that this consumes too much time while merely serving the purpose of being an ice-breaker.

3.1.4 Focus Group Design and Conduction

During the preparation of the project days, it was acknowledged that working with children poses certain challenges that differ from conventional focus groups with adults. Therefore, a literature review on focus groups with children was carried out. Focus groups are an established method for gathering qualitative data in design practices (Tomitsch et al. 2018), but they also play an important role in social sciences and become increasingly popular in research with children (Adler et al. 2019). Focus groups can be applied to create a comfortable space for children where they can discuss with their peers and do not feel pressured by any perceived power imbalance between the researcher and the participants (Shaw et al. 2011).

Research agrees that there are significant differences in the way children communicate at different ages and that their knowledge levels also vary greatly (Clark 2011). In addition, it is important to consider that even when at the same age, children's development can differ and is heavily influenced by their culture and social environment (Adler et al. 2019). Literature therefore recommends conducting focus groups with children of approximately the same age. In this project, this is solved by recruiting pupils from the same class, so that the age difference is not greater than one year. Conducting the focus groups at their school also has the advantage that the place is accessible and familiar to the children, thus making them feel safe. A school-like setting has also be found to encourage the children to be more attentive and concentrated (Kennedy et al. 2001). Furthermore, it has been found that children feel safer and are more willing to talk honestly when they are within a group of participants that they know (e.g. McGarry (2016)). Again, the participants of this project all know each other well since they go to school together. Also, the teachers have been asked to form groups according to friendships among the children. Furthermore, gender can also have an influence on the dynamics within a focus group, especially when entering teenage years or discussing sensitive, gender-specific subjects (e.g. Kennedy et al. (2001)). It was planned to have the pupils separated into male and female groups, but unfortunately this was not possible due to organisational issues on the school's side.

Krueger & Casey (2009) point out that it is crucial to keep the goal of the study in mind when planning the content of the focus group and that open-ended questions should be preferred so that a discussion can take place. Furthermore, experts recommend to engage the children in participatory activities, such as role-playing, to reveal their opinions in a non-threatening way (Morgan, Gibbs, Maxwell & Britten 2002). For going deeper into details and for involving shy participants, prompts such as "What do the others think?", "Does someone have another opinion?" or "Tell me more about that" can be helpful (Lund et al. 2016). However, especially for shy children it is important to offer different ways of expressing their opinions that do not involve speaking in front of the group (Coyne et al. 2009). Therefore, the focus groups at the school also include writing notes that are handed in to the moderator. Clark (2011) also recommends activities that include ratings, listings, sorting items, brainstorming or using their imagination. Having such a mix of approaches counteracts some of the challenges that can arise when conducting focus groups with children. For example, the children can become inattentive or distracted from the topic, they might be slow in

their responses or feel intimidated by a dominant moderator (Prior & Van Herwegen 2016). Wong (2008) also emphasizes that a moderator has to make the participants feel welcome and secure at all times. Clark (2011) adds that the moderator should use child-friendly language and vocabulary. In order to be able to connect with the children and enable meaningful exchange, the moderator should be patient, flexible and humorous.

The literature review was the basis for designing the content and the set-up of the focus groups at Blomhaug Barneskolen. The focus groups were designed to gain insights into children's chat behavior, how they react to certain messages in chats and to what extent they are aware of dangers. It was also investigated how they determine if they can trust someone they have met online and where they set the border between appropriate and inappropriate messages. At the end of the focus groups, the children were asked to assess the concept behind the AiBA project.

Each focus group consisted of five to six children. During the planning, it was decided that the groups should be homogeneous in gender since gender is expected to have a significant influence on the risk of being targeted by offenders and also influences online behavior. However, since the teachers were responsible for creating the groups, it was not possible to separate boys and girls in the end, so that the focus groups were conducted in mixed groups. Nonetheless, the teachers were able to divide the groups so that friends could be part of the same group, thus increasing the feeling of safety for the kids.

To investigate the impact of education on the subject, two focus groups were conducted before a presentation on chat security and grooming strategies was given, and four groups after, resulting in a total number of six focus groups. Due to the school's schedule, it was not possible to have three groups before and three groups after the presentation. However, it is still believed that this separation already gives significant indications.

The children were seated in a half circle, so that everyone was able to see and hear the others, allowing for an open and comfortable discussion, as Wong (2008) suggests. Before the actual focus group activities started, a set of ground rules for communication was established with the children, as it is also recommended by Wong (2008). These rules mainly included social manners and basic politeness (take time to think before you speak, let everyone speak without interrupting, no teasing or making fun). Additionally, the children were made aware that they cannot give wrong answers, since the focus group was about understanding their perspective and opinions. However, they could also pass on a question if they did not like to share their views. They were encouraged to ask question if they did not understand something. At this point, it is important to mention that the focus groups were not carried out in their native language Norwegian, but in English. Even though this was worrisome in the planning stage, it did not result in any communication difficulties due to the children's excellent knowledge of the English language. Then, for the sake of the next groups, the children were asked not to tell their classmates what was discussed in the focus group, so that the following groups were not biased. Lastly, the children were offered to speak with the moderator in private after the focus group if there was something that they did not want to share in front of the group. The focus group was accompanied by presentation slides which were filled with content together with the children, so that they could directly see their impact.

The focus groups consisted of three sections. The opening part started with the moderator presenting herself and asking the participants for their names, so that everyone felt welcome (no names were recorded though, to ensure anonymity). Starting with something easy to encourage the children to talk, a brainstorming session was conducted. It was discussed what the children use the Internet for, leading to a more detailed discussion about different applications they use for chatting. Knowing which applications are popular among that age group helps to identify the most effective platforms for educating children about online predators, and also presents potential customers for AiBA. To engage the children and challenge their creativity, they were asked to create usernames for a fictional chat. The moderator started with presenting hers and explaining how she came up with it, which was then done by the participants as well. Usernames constitute a targeting criteria of online predators (Winters et al. 2017), thus it will be useful to investigate on what basis children are choosing them. After presenting the usernames to the group, the moderator exchanged her own username with one of the children, challenging the participants to discuss ideas how to find out the real identity of a person they meet online and how determine if someone can be trusted.

During the second part of the focus group, the children were presented with a made-up chat conversation that included simplified grooming messages. The children's task was to react and reply to the messages which got increasingly inappropriate. After each message, it was discussed if the sender was someone of their age, an adult or if the message could be sent by both. The goal is to gain insights on the children's behavior in chats and how they differentiate between appropriate and inappropriate conversations.

At the end of the focus groups, the AiBA project was explained in a simple and understandable manner. By assigning a number between 1 (worst) and 10 (best), the children were asked to rate how much they liked the idea behind AiBA, and also adding a short reason for their opinion if they liked. The rating was written on a sheet of paper. The opportunity to write the rating on a paper was believed to decrease the risk that the children are influenced by each other's opinions as well as feeling the need to be nice to the moderator and giving a high rating. This way, one of the disadvantages of focus groups was being avoided, social desirability, where participants adapt their statements to the peer opinion, because they are unwilling to disagree with other participants (Daley 2013). When the work was done, the children received a sweet reward so that they leave the focus group in high spirits. Meanwhile, the moderator took notes on the children's behavior during the focus groups, their body language or other extraordinary remarks.

3.1.5 Data Analysis

Since the data showed the children's opinions, experiences and behavior, it was mainly of qualitative nature. To analyse the data, a set of established design methods was applied, mainly based on thematic evaluation and affinity diagramming. A thematic analysis is a data evaluation method that helps to find patterns in order to make sense of what has been said and collected during interviews or focus groups. Tomitsch et al. (2018) call it a "*structured method for analysing, interpreting and managing qualitative data*" so that the content is processed from raw data to usable information for the following design process. The core of this method is the creation of themes and categories

that describe the collected data. In this case, a bottom-up approach was applied. This means that the themes emerged from exploring and working with the data. The notes from the focus groups were summarised by specific terms which were written down on post-it notes. The notes were then grouped in terms of content which led to the creation of overarching categories for each grouping, a process called Affinity Diagramming. By applying this approach to the focus group data, a tangible overview of the discussed topics and the children's behavior could be created. This method is very suited for organising qualitative data, while simultaneously allowing the researcher to empathise with the participants of the focus groups, so that a user-centered design approach can be assured.

In addition, to extract the core findings, a couple of "game-storming" methods was applied as well. Special attention was given to elicit differences between the groups who have not received education about the subject and those who have. As with all qualitative data analyses, it is important to pay attention to minority opinions as well, even if they do not fit into the preliminary theory of the study (Kitzinger 1995). This is particularly the case when discussing sensitive topics, therefore deviant case analysis ensures that each individual's perspective is heeded.

Furthermore, some quantitative data was acquired as well. Approaches of exploratory data analysis were used to investigate tendencies of the children's online behavior, such as determining percentages of the most used chat applications and the most common basis for usernames. This innovative data-driven methodology aims at maximizing the insights into a specific data set without requiring predefined hypotheses (Tattar et al. 2016). Instead, the goal is to discover the structure of the data and point out important variables in order to test assumptions. The use of graphical displays makes the data more accessible and provides understandable summaries at one glance.

3.2 Surveys

3.2.1 Purpose

Surveys are a low-cost way for collecting insights into self-reported behaviors and perspectives (Tomitsch et al. 2018). In order to get an understanding of the parents' knowledge and attitudes on chat security and grooming, a questionnaire was designed in addition to the focus groups. The combination of these two methods and the conducted literature review results in a holistic picture of the risk, presenting the children's perspective, the parents' experience and the experts' opinions. Furthermore, the survey investigated the needs and expectations of the parents towards the AiBA application. The aim was to gather an assessment of the parents perspective on online grooming, in order to create a mental model of their views that forms the basis of an effective risk communication strategy for this target audience.

3.2.2 Identifying Participants

Since there has been a successful cooperation with Blomhaug Barneskolen in Hunndalen for conducting the two chat security project days, the school kindly agreed to establish contact with parents through their online communication channel. The same tool was used to reach out to parents from two other schools in the vicinity. Since the main focus of the thesis lies on children in 7th grade, the invitation to participate was only sent to parents of children in that grade. This also ensures better

comparability of the focus groups and the survey. Since it can be assumed that the majority of the parents uses Norwegian as their main language, the survey has been translated to Norwegian. This simplifies the process for the parents and avoids language barriers. In case that some parents prefer filling out the survey in English, this option was provided as well, however, it has not been used in the end.

3.2.3 Pilot Test

In order to identify potential problems before sending the survey out, a pilot test was conducted with one native Norwegian speaker. The questionnaire was checked for wording and potential misunderstandings or biases, since the pilot participant was not involved in the project before. Minor clarifications had to be implemented after the test and the required time for completing the survey could be identified more accurately.

3.2.4 Survey Design

Tomitsch et al. (2018) point out that the survey design should closely follow the goal and research questions that were established in advance. It has to be considered what type of data can contribute to answering these questions and how it will be analysed before the survey is distributed. They further recommend to keep surveys as short as possible, since long questionnaires are less likely to be filled out and often return less valuable data. Therefore, every question was assessed regarding its contribution to the objective and the data it reveals. Ambiguous questions were taken out and the wording was carefully altered so it would not lead to biased answers. The final survey for this project is divided into five sections. The first section gives an introduction to the study, what the survey will include and explains the participants' rights. As the survey does not collect any data that is considered personal data, there was no need to request a NSD approval. The second section is comprised of questions regarding the parents' knowledge of grooming and their children's general internet behavior. The section aims at investigating the existing knowledge and availability of information about grooming in order to identify basic information needs. The next section starts with a short definition of the term *Grooming*. The following questions ask about the parents' conceptions of the grooming process and their personal appraisal of the risk. This part is essential for understanding the parents' mental model of grooming. The fourth part looks into ways to prevent grooming and asks for personal opinions and assessment. The long answer texts generate qualitative data that lead to a better understanding of the parents' information needs to increase their children's online security. The last part of the survey presents a short description of the AiBA project. It aims at understanding user expectations and information needs, especially when the system has detected grooming behavior and sends a warning.

The guidelines for creating understandable and satisfactory surveys by Baxter et al. (2015) are taken into account for designing the questionnaire itself. Firstly, the title is kept short and provides clear keywords for introducing the topic of the study. The first section clearly lays out instructions for completing the survey and the time that it requires, as well as contact details of the responsible people and an explicit statement of the participants' anonymity and confidential data processing.

The order of the questions is logical and builds up from general questions to more specific ones. Grouping the questions into sections increases clarity and breaks the questionnaire into manageable chunks. Displaying a progress bar throughout the completion of the survey allows the participant to keep an overview of the remaining sections. Also, the survey can be filled out comfortably on any device or screen size thanks to its responsiveness. The questionnaire is included in the appendix (8.1) for further examination.

3.2.5 Data Analysis

The survey collected a mix of quantitative and qualitative data. An exploratory data analysis approach was chosen since the amount of replies (20) would not yield significant statistical results. Choosing an exploratory analysis is the best way to reveal patterns and trends of this specific data set. The qualitative data was analysed with an affinity diagram to work out categories and relations within the data. Tomitsch et al. (2018) call affinity diagramming an excellent tool for translating data into user needs. It is a systematic method that starts by breaking the data down in parts for analysis and then synthesises groups of data to form categories. These categories can be connected with each other to form a coherent picture and generate ideas to solve the underlying (design) problem. It is important to keep in mind that the data cannot be regarded as representative for the whole population of the target group. It can, however, show tendencies and provide a basis for further development of the risk communication strategy.

3.3 Risk Assessment and Mental Model Approach

A risk assessment constitutes the starting point of creating a risk communication strategy and provides an overview of the context, such as affected population, known and unknown variables, stakeholders and potential risk consequences (Lundgren & McMakin 2009). It forms the basis of risk communication and informed decision making since it sets priorities and decides the scope of the communication strategy. A risk assessment starts by identifying a problem and the resulting hazard. The potential consequences of actions need to be considered as well as the user's perception of both the problem and any proposed solutions. The employed risk assessment identifies the underlying reasons why communication of the risk is necessary by applying the gamestorming method "The 5 Whys" (Gray et al. 2010). Another one of these methods, "The 4 C's", is used to describe the risk in detail by looking at its components, characteristics, challenges and consequences. Furthermore, the target audiences and their characteristics are determined based on the conducted data collection. Lastly, the desired outcomes of the communication strategy are assessed by compiling an "Elevator pitch". An elevator pitch is a popular exercise in product development for communicating the benefits of a new idea or product in a short and compelling manner.

The mental model approach (Morgan, Fischhoff, Bostrom & Atman 2002) aims at revealing knowledge gaps and incorrect beliefs of the audience by comparing their mental picture of a risk with an expert view. The differences in perception form the basis of establishing the information needs of the audience. The theory of mental models is grounded in cognitive psychology, but is also applied in Human Factors Engineering and Interaction Design. To systematically establish the

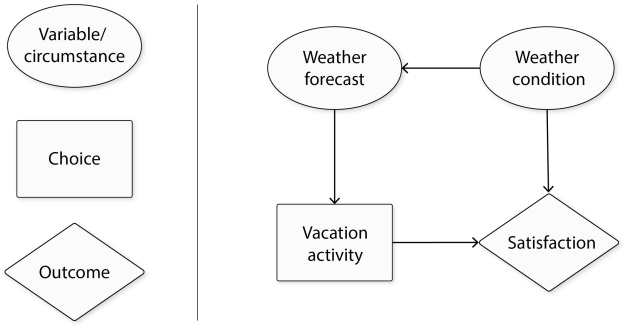


Figure 2: Example influence diagram showing influences on vacation satisfaction

audience's information needs, Morgan recommends following their strategic approach. They start by creating an expert mental model based on scientific literature or expert interviews. The mental model can be visualized by an *influence diagram*, a technique originating in decision theory, that summarises the experts' views on the risk level, risk consequences and prevention measures as well as an assessment of the relevance of different facts. It consists of *influences* that connect related *nodes*. Nodes can either represent circumstances (oval form), choices made by a decision maker (rectangular form) or outcomes (diamond). An arrow shows the direction of how the variables influence each other. A simple example is given in figure 2. An influence diagram should not be confused with a flowchart that illustrates a process following certain steps. Instead, an influence diagram can be seen as a snapshot of all aspects that influence the risk, regardless of any chronological order. The goal of the influence diagram is to extract knowledge and facts that experts deem relevant for the audience to make informed decisions regarding the risk. Much of the knowledge provided by experts is far too detailed or specialised to be of relevance for the general public, therefore, another goal of the influence diagram is to set priorities and define the level of detail. The influences, nodes and direction arrows were identified using the *assembly method* as described by Morgan, Fischhoff, Bostrom & Atman (2002). While reviewing the expert literature, post-it notes were created to list relevant information. Once the listing was completed, the notes were moved, grouped and connected to form the influence diagram.

Morgan, Fischhoff, Bostrom & Atman (2002) continue by identifying knowledge gaps and incorrect beliefs of the audience based on open-ended interviews with relevant representatives of the target audience. This step has been adapted to the health situation following the COVID-19 outbreak so that the investigation has been employed by online surveys as described in the previous chapter. The risk communication strategy then focuses on filling the gaps and inconsistencies between the two models so that the audience receives relevant information for informed decision making. It is not uncommon that there are more misconceptions than can be addressed in a risk communication effort of moderate length. Therefore, part of the assessment is to prioritise the most critical knowledge gaps. Morgan, Fischhoff, Bostrom & Atman (2002) recommend to "focus on the

facts that will have the greatest impact on the greatest portion of the audience". When the key aspects have been determined, the information needs to be logically organised so that it is easier for the audience to make sense of it and correct or expand their mental models. It is most effective to order the information hierarchically, with the most essential information placed highest, as this increases memorability (Kintsch & van Dijk 1978). The mental model approach fits well into the overall user-centered design approach of this project. It is central to seek a dialogue with the audience rather than just asking experts what the public needs to know. Failed communication can lead to confusion, mistrust or disinterest on the public's side and experts blaming the public to be stupid, hysterical or irrational; which highly restricts the success of future communication efforts as well.

3.4 Communication Strategy and Warning Design

A communication strategy forms the bridge between the insights gained through the literature review and the user research to the implementation of a strategic plan for educating the audience about the risk of online grooming. Effective communication strategies follow a systematic approach based on the conducted research and behavioral theories in order to tailor communication activities and materials to the target audience. It therefore acts as a planning stage before the production and implementation phase is taking place (Bingham et al. 2009). In risk communication, one further distinguishes between three risk-event phases. The *Preparedness stage* takes preventive actions before an incident happens, mainly with the goal of raising the public's awareness and educating them about the risk. The *Response stage* is taking place during an incident or crisis and needs to clearly instruct the audience on how to react to an immediate risk while avoiding irrational reactions. Lastly, the *Recovery stage* addresses needs after an incident, such as providing (emotional) support and directing to sources for additional help (Janoske et al. 2012). Lundgren & McMakin (2009) emphasise that the audience should always be provided with contact details where they can seek help, especially - but not exclusively - during the Recovery phase. The contact details need to stay consistent throughout the materials so that the audience will feel comfortable about the reliability of the information.

When it comes to the creation of risk communication materials, it is essential in all three stages to consider what information is included, how messages are organised and how they are formulated. As in user-centered design approaches, this stipulates profound knowledge of the target audience(s). The audience's ability to process the information and how they react to it are highly dependent on their previous experiences and feelings towards the risk, but also on variables such as education and reading level (Lundgren & McMakin 2009). Therefore, scientific and technical jargon needs to be avoided and the overall language has to be adapted to the audience. Language and writing style are a central part of the processing of information and special attention needs to be given to the effects of the used language. For example, calling the affected population "victims" will make the audience feel out of control, resulting in anxiety, hostility or denial. Using a narrative style for presenting information, either in addition to conventional data presentation or as a stand-alone approach, can heighten emotional involvement. Narrative style uses a personal story to present the

risk, thus making it more relatable and understandable. Golding et al. (1992) have assessed the effects of narrative style in comparison to "technical" style and found that a narrative encourages the audience more to keep reading while enhancing their knowledge equally well as the technical style. It is therefore an effective method to keep the audience engaged when conveying a lot of information. A good narrative shows three essential characteristics: involvement (Is the audience interested in the message?), relevance (Does the story apply to the audience?) and understandability (Does the audience understand the message and act accordingly?). The materials should be tested for these criteria in an evaluation phase. In addition, Kim & Choi (2017) have compared the influence of emotional and logical messages on risk perception and coping style. They have found that emotional messages lead to a higher risk perception and estimated probability of risk occurrence, as well as a better recognition memory. They suggest that emotional messages should be used in risk communication to achieve higher engagement of the audience. Lundgren & McMakin (2009) recommend to put the risk in context so that the audience can relate to it more easily. One way to achieve this is to compare the risk to other risks that the audience is familiar with. Before going into details or presenting data extensively, the risk and its assessment process should be shortly described to further clarify the context and provide an overview of the important aspects. They recommend to use leaflets and brochures for simple short-term communication efforts. These short materials are a good way to quickly and clearly communicate aspects of a complex risk. They have to be focused on specific information needs and be self-contained so that the audience can understand them without any previous or additional information. Several pieces of information material should follow a clear corporate design to achieve visual consistency and make the audience familiar and comfortable with their look. Print materials should be distributed in places that are frequented by the target audience so that they have easy access to it. Direct mail approach can also be a solution depending on the context and budget of the project. A communication channel that has exponentially gained importance in the last years is social media. Their interconnectedness makes it simple to publish and spread information to a wide audience. Social media blurs the line between sender and recipient as described in the classic communication model by Shannon (1948), since any user can become a sender and share the content with more people. Furthermore, social media allows for direct feedback from the audience in the form of reactions and discussions in the comment section. While they often require close monitoring to ensure the appropriateness of the comments, these discussions have the potential to start a valuable discourse on the topic. Furthermore, social media allows institutions with similar goals to connect with each other and spread their messages. Lastly, the practice of microtargeting offers the possibility to effectively target audience segments. Although microtargeting raises ethical concerns and it controversially discussed, it has the potential to directly provide specific groups of people with information that fits their needs (Bartlett 2018).

Sandman (2007*b*) has listed twenty guidelines for creating well-designed, on-point messages for the Preparedness phase. With the goal of raising awareness and pointing the public's attention towards the risk, his guidelines follow five main characteristics: be on point, raise interest, appeal to emotions, offer choice and monitor the reactions. Firstly, he emphasises that messages should be short, concise and understandable by the audience which is backed up by the previously conducted

literature review. However, he goes beyond that and further recommends that messages should be interesting and appealing to the previously established audience needs. In combination with his argument to appeal to emotions (especially fear in proportion to the risk), chances are higher that the communication strategy is successful and that people are paying attention. In accordance with the previously researched warning design principles, Sandman advises to offer people choices of actions to take, preferably in easy and small steps. Lastly, he points out that messages need to be tested, adapted and prepared for unforeseen reactions.

3.5 Evaluations

3.5.1 Purpose

Experts highly recommend to evaluate a risk communication strategy to monitor whether the objectives have been achieved. Ideally, evaluations should be conducted before making the communication public as well as after a project has been finished, to fully evaluate if the purpose has been reached and what changes need to be employed in future projects (Lundgren & McMakin 2009). Since this Master's thesis only covers the strategic design of a risk communication and not its practical application, just the first evaluation cycle will be applied. The importance of evaluation in risk communication goes in line with a user-centered design approach where usability testing or other kinds of evaluation play a significant role. Direct feedback from the audience provides valuable insights about the strengths and weaknesses of a design and how it can be improved. Morgan, Fischhoff, Bostrom & Atman (2002) compare the evaluation process to trustworthy engineering:

> "You'd never design a new product on the basis of an engineer's best guess. You'd insist on careful empirical design and testing. The same standard should apply to risk communication."

As evaluation methods for this project, an online expert review of the materials aimed at parents and feedback discussions in small focus groups with the children have been chosen.

3.5.2 Pilot Test

A pilot test was conducted with a Master student of Interaction Design who was familiar with design and usability concepts and guidelines. The main objective was to determine the required time for filling out the evaluation questionnaire and going through the discussion with the children. However, feedback on the wording and order of the questions was gathered as well so that the survey could be optimised before sending it out to the group of experts and the questions for the discussions with the children were easy to understand.

3.5.3 Evaluation Design

The evaluation design is closely related to the communication plan and objectives (Lundgren & McMakin 2009). It needs to be assessed to what degree the communication strategy works towards achieving the objectives. First, it needs to be evaluated whether the audience understands the message correctly and interprets its intention in the right way. Furthermore, following recommendations by Dozier et al. (1995), the evaluation should also include the audience's awareness,

knowledge, behavior and opinions of the risk after viewing the communication strategy materials. Weinstein & Sandman (1993) created a set of guiding questions that should be answered in the evaluation. They include an assessment of the audience's understanding of the presented content, their agreement with recommended actions, whether responses are consistent among people from the same risk group and whether they find the messages helpful, accurate and clear. Lundgren & McMakin (2009) add guidelines for evaluating social media efforts which has significantly gained importance over the past years. They advise to evaluate education (Is the information relevant?), engagement (Are people engaged in a positive and meaningful manner?), entertainment (Is the message offering entertaining value?), empowerment (Do people feel empowered to take actions?) and "Evangelism" (Do people feel inspired to share the messages with others?).

Lundgren & McMakin (2009) point out that surveys and interviews are highly suited for conducting the evaluation. The original plan of this thesis included the conduction of user tests following the Thinking Aloud approach with parents from local schools. However, the long lasting effects of the COVID-19 pandemic obstructed this plan due to health regulations. Furthermore, the parents were facing additional challenges during this time so that they were not available to take part in any user tests. It was shortly considered to adjust the user test to an online survey (as it was done with the interviews for user research), but it was assumed that none of the parents had participated in a user test before and therefore required instructions and guidance that would not be fully conveyable in an online form. It was therefore decided that the designs are evaluated by an expert team consisting of professionals working in the field of Interaction Design by conducting a heuristic evaluation. It is assumed that they are able to evaluate most parts of the communication efforts such as understandability and clarity and are able to identify usability issues. Luckily, by the time the second part of the evaluations was conducted, the local schools had opened again so that the children who participated in the Internet security workshops could be asked to participate in a short assessment of the communication materials aimed at them.

Taking the different information needs and expectations of the target audiences into account, the evaluation looks separately at the materials for the children and parents. The children were accessed through the established contacts with the local school, and the evaluation was conducted on location under consideration of health guidelines. The children were divided into groups of three who then discussed the communication materials, while the researcher acted as a moderator. The interaction design experts were contacted through the platform LinkedIn or through personal contacts of the research team. The requirement was to have relevant working experience in the field of Interaction Design or Communication of at least one year. In both evaluation set-ups, the participants received a short summary of the project and why their feedback is contributing to its success. Then, they were informed about their rights and it was emphasised that they cannot give wrong answers since it is not them who is being tested, but the designs. Each evaluation set consists of the materials for the three stages of risk communication. For the experts, this is an exemplary leaflet for the Preparedness phase, a warning about potential grooming approaches towards the child for the Response phase and a message with additional information for the Recovery phase. The children are presented with social media posts, a prototype of a warning that is sent by AiBA and a follow-up

message after the incident. In each phase, the participants are asked to read or look at the material and afterwards answer questions about their experience and opinion. Following literature recommendations, the questions are investigating issues such as relevance, understandability, agreement and usefulness of the information. It has been taken into account that the language used during the evaluation with the children has to be adapted so that they can easily follow. Exemplary questions for evaluating the success of the communication effort include:

1. How relevant is the content for you?
2. How much does it grab your attention?
3. How helpful was the given information?
4. What would you do after this warning?
5. How likely is it that you would share this post with friends or parents?

The experts were also asked to evaluate the warning design by answering additional questions based on the heuristics by Nielsen (1994). These heuristics serve as a solid set of guidelines that form the basis of good usability and user experience. The set of ten heuristics was condensed to 8 questions, since the heuristics "flexibility and efficiency of use" and "recognition, diagnosis and recovery from errors" were not applicable in the context of the prototype. This resulted in a heuristic evaluation investigating the following issues:

1. Visibility of system status: To what degree did you feel in control of the system? Did you get appropriate feedback to 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 minimalistic 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 require help from the system?

At the end of the evaluation, the experts are asked how high they rate the risk of online predators grooming children in order to investigate how the communication efforts influence risk perception. They are also asked for an assessment of the usefulness of a warning system such as AiBA so that their views can be compared to those of the parents who filled out the online survey in the research phase.

The full evaluation guides are attached in the appendix (8.2).

3.5.4 Data Analysis

The collected feedback from the experts was reviewed and analysed using an exploratory data analysis approach for the quantitative data and affinity diagramming for qualitative data. The goal was

to identify strengths and weaknesses of the designs and to collect feedback for potential improvements. Evaluating the data from the feedback rounds with the children also aimed at assessing how well the information needs of the target audience were met. It has to be taken into account that the setting for the evaluation did not match the context in which the communication materials will be presented in a real-life implementation. Although reactions and interactions are influenced by the test's context and setting, the chosen evaluation method is believed to reveal weaknesses of the designs that need to be refined. A list of recommended adjustments concludes the evaluation.

3.6 Ethical Considerations

Ethics can be a complicated topic since they are highly subjective and especially when treating a sensitive subject like child abuse, it is extremely important to discuss them in detail. Institutions have worked out ethical codes that practitioners are encouraged to follow. One example are the "Ethical Principles for Technical Communicators" (STC 1998) published by The Society for Technical Communication. Risk communication can face a number of ethical challenges, from which and how much information to make available, to choosing the target audience. Guidelines such as the Ethical Principles for Technical Communication aim at ensuring honesty, confidentiality, fairness and following regulations. According to Lundgren & McMakin (2009), ethics in risk communication can be subdivided into three categories; social ethics, organizational ethics, and personal ethics.

Social ethics describe the reaction and judgement of risk communication by the public. These ethics highly depend on the country and its culture, and they can change as society evolves. Even though the thesis project and the AiBA project aim at protecting children from harm, the topic of sexual online offenders is still very sensitive and needs to be handled with care. Even though Norway is a very progressive country, sexual offenses might still be considered a taboo in conversations, especially when including children, and make the audience feel uncomfortable. Lundgren & McMakin (2009) recommend identifying the target audience's concerns and perceptions of the subject early on in the process so that they can be taken into account during every stage of the process. Simultaneously, these concerns and perceptions might lead to additional insights that would not have been considered otherwise. They can thereby increase the quality of the risk communication and increase the credibility of the communication strategy. Lundgren & McMakin (2009) further continue that there is always the possibility that a message is misunderstood by the audience even if there has been profound user research. Naturally, the communicators should put all efforts into creating clear messages that are easy to understand and do not raise unnecessary concern. The information about online child offenders should therefore be backed with expert views, but should be presented in an objective and understandable way for both parents and children. Those who are at risk should understand the potential danger and be empowered to take appropriate actions, but the communication should not result in exaggerated, over-emotional responses since they hinder rational thinking. Again, the need for collecting information about the recipients is emphasized, although Lundgren & McMakin (2009) point out that this process is usually limited by resources such as time, money and available staff. To ensure understandability, they highly recommend pretesting of the information materials before they are spread to a wide audience. Another relevant social

ethical issue is the creation of (perceived) stigma. Risk communication should never make an audience feel like they are stigmatized as this increases discomfort and hostility towards the topic. As an example, even though a very high percentage of convicted child offenders is male, the risk communication strategy should not generally stigmatize men as child abusers. At the same time, even though girls are more likely to be targeted by online grooming than boys, girls should not be made to believe that they will encounter this event just because they are girls.

The second category of ethics that Lundgren & McMakin (2009) describe are organizational ethics. These ethics are mainly concerned with the issues of who is representing the stakeholders and the audience. This is relevant to the thesis project as it will invite parents and children from local schools in Gjøvik for data collection. As mentioned above, the children are in seventh grade, meaning that they cannot represent the whole range of intended users for the AiBA application. Also, their behavior might differ from peers living in other places, either big cities like Oslo or small villages on the country-side. The same can be said about their parents. However, if this concern is kept in mind throughout the process, it can be addressed in the final strategy. The results could be used for a specific strategy in this area and be adapted to other environments and cultures in follow-up projects. Lundgren & McMakin (2009) further emphasize that it is crucial to meet the needs and requirements of all audiences. They divide audiences into "Primary Audience" and "Secondary Audience", with the primary audience being the segment that is at most risk, has the least information to make decisions and will be most involved in decision making regarding the risk. In this project, the children who are intended to use the AiBA application can be considered the primary audience. The communication should therefore be tailored to them, using their language and be overall appropriate for this audience. However, it is equally important to educate parents about the risks since they have legal guardianship over the children and are highly concerned about their safety. It can also be argued that schools, clubs and other institutions that work with children can be considered a tertiary audience since they are in close contact with children as well. The communication strategy needs to take all these audiences and their information need into account. This approach goes hand in hand with the question of when, what and how much information should be released. Lundgren & McMakin (2009) suggest that the amount and timing of released information is crucial for the audience's reaction to it, although literature recommends making as much information available as possible, and as soon as possible.

The last category to describe ethics are personal ethics (Lundgren & McMakin 2009). These are concerned with the beliefs and behaviors of the communicators and responsible persons. One behavior that will be avoided in this project is using risk communication for persuasion, which intentionally presents information to force an opinion on the recipient. The thesis project aims at educating the audience and empower them to take well-informed decisions, not to force a behavior on them. The strategy will not aim at restricting the children's access to the internet or breach their privacy through a surveillance application. All decisions will be made independently by the audience based on the information that they receive. Lastly, as pointed out in the chapter about risk analysis, including children in the data collection poses some ethical concerns as they can be seen as the most vulnerable part of our society and their well-being and privacy should be ensured at all

times. As a matter of course, all collected data will be treated with confidentiality and the children's anonymity will be ensured at all times. The collected data will in turn contribute to a project that has set children's well-being as its overarching goal.

4 Results

4.1 Focus Groups

The focus groups took place at Blomhaug Barneskolen in Hunndalen with a total number of 35 children. The groups were very diverse, consisting of native Norwegians and children with migration background. The groups were mixed regarding gender so that there was an approximately even number of boys and girls in each focus group. Interestingly, it was possible to observe immediate results already during the project days. Filling out the Power Point presentations together with the children assured that their opinions were documented correctly. One could notice huge individual differences in the children's reactions to the fictional chat messages, ranging from answering honestly to using "protective" lies and from being extremely careful to evading the questions through humour and irony. The filled out paper slips with usernames, favorite chat application and the rating for the AiBA system were collected at the end of the focus group phase. After each focus group, some notes were taken on the children's overall behavior and reactions, as well as their body language and other surprising or extraordinary remarks. On the second day, after the children attended the presentation on chat security and grooming, it was particularly interesting to see that the children had become much more careful and suspicious when discussing the subject and they were stricter when differentiating between appropriate and inappropriate messages. Their vocabulary was also influenced, mentioning the terms "sexual predator", "kidnapper" and "pedophile", which had not occurred on the first seminar day.

Before conducting an in-depth analysis of the data, a quick read-through gave an overview of what had been collected. The papers with usernames, favorite chat applications and the AiBA ratings were transferred into a Microsoft Excel spreadsheet for further investigation. One rating card was taken out of the analysis since that child seemed to have misunderstood the instructions and wrote down its age instead of a rating onto the card. The collective notes from the Power Point presentations were transferred on post-it notes to prepare them for a thematic analysis. It was made sure that the data from before and after the presentation on chat security was handled separately, so that the influence of the education can be assessed. The two groups who had not attended the presentation before the focus group will be referred to as BPG (Before-Presentation-Group) and the four groups who saw the presentation before the focus groups will be called APG (After-Presentation-Group).

4.1.1 Thematic Analysis

In the following paragraphs, the data from the focus groups is evaluated chronologically according to the focus group guideline that was presented in the Methodology chapter. In order to encourage the children to talk and share their views, the focus group started by brainstorming activities that the

children do on the Internet (see figure 3). Although it mainly served as an ice-breaker, it also shows the range of things that children of the age of 12 to 13 perform on the Internet. As this task had nothing to do with grooming or security issues, it is not surprising that there were no differences between the groups before and after the presentation on chat security. Therefore, the results of each group have been combined. Among the first things that were mentioned in each group was "watching videos", "Youtube" or "movies/TV-series", which has been summarised in the category "Media". Although this mainly serves for entertainment, these platforms can be used to reach out to children and educate them about grooming and online predators, e.g. through advertisement before videos. The children also quickly mentioned a variety of online games such as "Fortnite", "Roblox" and "MoviestarPlanet" which have been assigned to the category "Games". As most online games revolve around a chat function, these are important stakeholders that represent potential clients for the AiBA system. This is particularly relevant since these kinds of online games have been criticised for being unsafe for children by several internet safety guides for parents. For example, Roblox offers many opportunities for predators to contact children, either through sexualized actions in the game itself or through the chat function, a problem that is very common for these kinds of "social games" (Dittman (2019); Ivins (2018)). The children were also quick to mention activities that can be summarised as "Chat"; e.g. "texting with friends", "sending messages", "Snapchat", "Messenger" etc.. Some chat applications connect the children to a community, like "Discord" which is associated with gaming or "Twitch" which enables live streaming and commenting for gamers. While texting with friends and family is a relatively secure matter, safety issues arise once the child does not know the chat partner personally. "Social Media" was another popular activity that describes the vast amount of social platforms that the children use, from popular ones like "Instagram", "Facebook" and "TikTok", to less known ones like "Jodl" and "House Party". "Social Media" is seen separately from chats where conversing with others is the main purpose, since social media is also about "posting videos" and "posting pictures" as well as "liking other's pictures". After some thinking, a few children mentioned activities that can be categorised as "Information"; e.g. "checking the weather", "doing homework", "translate" or "checking news". Lastly, one girl mentioned "shopping" which has been assigned to the category "other", since no similar activities were reported by the other children. This evaluation has shown that consuming media content is among the most popular activities on the Internet, as well as communicating with others through chats, either while playing games or in social media applications. The popularity of these activities justifies the need of a safety guard that protects the children from harassment and grooming.

When being asked who they mostly chat with, the very first answer in all groups was "Friends" and "People they know", such as friends of friends, children from other schools or friends who moved away. Soon after, the children mentioned "Family". As mentioned before, texting with people they know does not pose an immediate threat of becoming a victim to grooming by an online predator in most cases. However, after some consideration some children mentioned that they also text with "Strangers" and the more it was discussed, the more places were identified where these strangers can be met. Firstly, the children mentioned games again, where they chat with other players. They might play games together, but do not know each other otherwise. It was

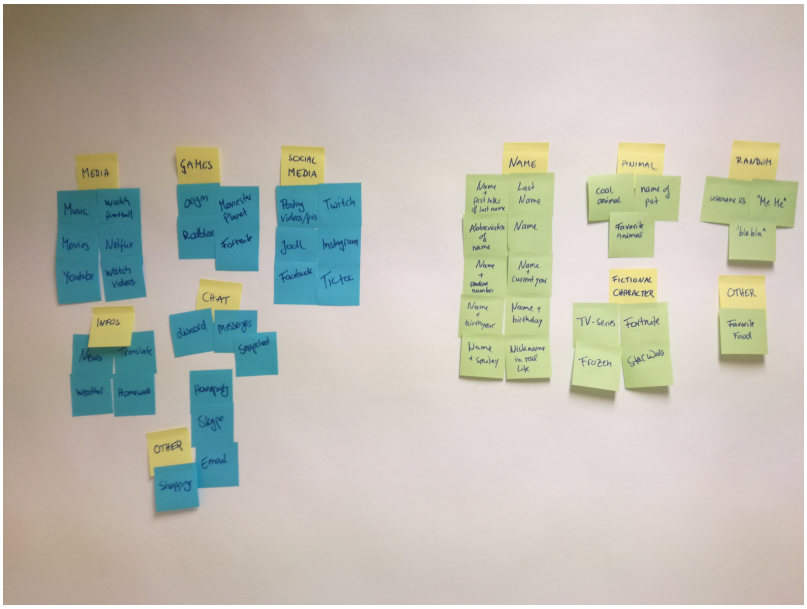


Figure 3: Thematic Analysis of online activities and usernames

also mentioned that some children exchange messages with influencers on social media which are people that they only know from what they post on their channels. Additionally, it was said that from time to time, they chat with people they do not know, but who share a common hobby or interest, again mostly in terms of gaming. While a handful of children said that they sometimes chat with strangers intentionally to get to know new people, only a few claimed that they have been contacted by absolute strangers without any particular reason. When being asked about how they feel when chatting with someone they do not know, a first difference between the BPG and the APG could be noticed. The children in the BPG also had some concerns and especially the girls pointed out that one has to "be careful" and one "cannot know who that is". However, a list of advantages was found as well, including "you can chat with people from other countries", "you meet people who like the same things", "you can make new friends" and "you find people to play with". When asking the same question to the APG, the main subject was that texting with strangers can be dangerous, because one cannot be sure of their true identity. The children mentioned the cases of sexual and emotional abuse that were shown during the presentation. "Kidnappers", "predators" and "pedophiles" were part of the discussion as well, showing that these groups were much more aware of the potential risks when chatting with strangers.

When being asked about how they would identify a person they are chatting with and how they can tell if someone is really the person they pretend to be, the children came up with a variety of ideas. The BPG would mainly rely on photo or video. They would ask the chat partner to send a picture or start a video call in order to confirm their identity. This approach was also mentioned

in the APG, but it was not as popular. In the discussion, it was mentioned that the chat partner could send a fake picture or pretend that he or she had some technical issues that made video calls impossible. The most popular strategy in the APG was to pay attention to the way the chat partner is writing, what words are being used and what topics are discussed. One mentioned that children of their age have a very specific way of using emojis and that it is hard for adults to imitate that. The children felt confident that they would identify an adult who pretends to be a teenager. They also proposed to ask questions that only children of their age could answer satisfactory (e.g. related to pop-culture) or that only specific people can answer (e.g. if the chat partner pretends to be from the same school, they would ask specific questions about the school). Some children would just directly ask about the other's identity ("Who are you?", "How old are you?" etc.). In the discussion this was quickly neglected since the other person can simply lie about that.

The main part of the focus group consisted of a fictional chat that investigated how the children react to certain messages and at what point they draw the line between appropriate and inappropriate conversation. The five questions got increasingly specific and followed a very simplified and shortened grooming process. It was striking to see how much more careful and suspicious the children had become after the presentation on chat security. Not only their replies to the messages, but also their initial reactions, body language and commenting within the group changed.

The first message asked the children about their age ("Hi, cool nickname! How old are you?"). In the BPG, it was very common to evade this question with another question, e.g. "Do I know you?", "Why are you asking?" or to ask the same question back before telling one's own age. Those who did not evade the question would simply answer by honestly telling their age. There were still children who told their age in the APG or who evaded by asking a question back, however, the most common answer was to deny the question ("I can't tell you", "I don't tell my age to people I don't know") or to lie about their age and make themselves older. It is not surprising that there were children who answered the question honestly in both groups, since some children are more careless, open or honest than others by nature, however, it was clear to see that the educated groups were much more careful even when being asked a rather common question. When the children were asked to discuss whether this chat message was written by someone of their age or by an adult, there was no agreement in any of the groups. There was too little information in the message itself to determine this. One group who attended the presentation before discussed about checking the other person's profile or to ask question to find out more about them.

The second question was pointing at the children's private interests ("Awesome. What are you doing after school?"). The same pattern as with the first message repeated; in the first two groups the children either evaded the question, asked the same question back or honestly answered and listed a lot of activities. If they were chatting with a predator, this would open up opportunities to find ways to bond with the child. However, there was one girl who pointed out that she would block that person and not chat any more if she did not know who it was. This suspicion was more common in the APG with several children pointing out that they would block the person or simply not answer the question. Some children even became offensive, saying for example "That's none of your business" or "I don't talk to pedophiles". On the other hand, it was just as popular to answer

honestly and tell about hobbies after school. This shows that the children are quite different, but the fact that there was already talk of "pedophiles" in one group shows that the presentation about grooming raised their awareness of the risk. It has to be kept in mind though that the setting of the focus group does not represent a real chat conversation and that the children might react differently in a real life situation. There was no agreement whether the message was sent by a child or an adult, but the majority suspected that it was an adult since other children usually do not ask such specific questions. In the APG, some children already became suspicious or uncomfortable, talking about the abuse cases from the presentation.

Nonetheless, at the third message it was clear to see that a line was reached for the APG, as it was asking whether they are alone ("Are your parents home right now?"). Many of them raised their eyebrows or looked at each other with wide eyes, making comments or jokes. When asked how they would react to that message, most would say that their parents are home, even if they were not, for safety reasons. The children were not very willing to give away that information and some would not answer at all or block the other person. In four out of six groups, there was one child who would say that the parents are not home in order to find out more about the other person's intention. While the children in the APG were very defensive at this point, those in the BPG kept being evasive. Even though they were not eager to give this information away either, they were less clear in their answers and did not draw a line. They either asked questions back ("Why are you asking?"), said nothing or evaded in other ways ("Maybe", "I am not home myself"). Just very few children would admit that they are alone at that moment. While some children still believed that this message could come from a teenager of their age, others started to be very suspicious, because this is not a usual question that children ask each other. The APG was very sure that the message came from an adult, since it is a very strategic and planned question. A group of girls mentioned that they would get scared if they got this message in real life.

The second to last question suggested interest in the children's clothing and physical appearance ("What are you wearing?"). At this point, also most children in the BPG thought that something suspicious was going on. The majority answered sarcastically, although some put themselves at risk by introducing sexual content ("Are you my mum?", "I never wear clothes", "I am naked"). Others kept avoiding the question by asking questions themselves ("Why are you asking?"), while some would describe a "normal" set of clothes or just answer honestly. The attitude towards the sender of the messages was much more offensive in the APG. Almost all children would block a person who sends them a message like this, some would insult the person first, call them a pedophile, sex predator or pervert, take a screenshot to show the police or tell their parents about it. Only very few would answer to that question. They mainly agreed in all groups that this messages comes from an adult with dishonest intentions. The message would make them feel uncomfortable and they would be very careful. Just one girl was still considering if this could come from someone of her age who wants to get to know her and might need advice on clothing styles.

The last message was asking for a picture ("Can you send me a picture?"). None of the children said that they would agree to this. The same pattern as in the message before was showing. In the BPG, the children reacted mostly with humour, saying they would send funny pictures they found

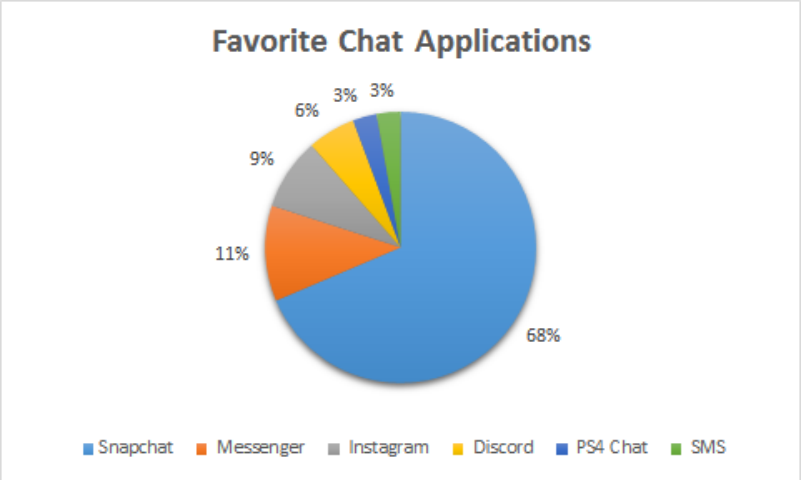


Figure 4: Favorite chat applications of the participants of the focus groups

on the internet. Only one child consequently said "No" to sending a picture, the rest would again try to evade the question. This was quite different in the APG. The most common reaction was to block the person, or say no to sending a picture, although some children would insult the sender first. They agreed now that the sender is an adult, because of the content and language used in the messages. They were also sure that this person has dishonest intentions. Interestingly, in almost all cases, the children were talking about a male person when talking about the sender. Just in one group it was mentioned that the other person could be female as well. Recalling the children's methods of how they themselves would identify an unknown person - by asking for pictures or video call - it is interesting to see that they deny sending pictures themselves.

4.1.2 Data Analysis

A quantitative data analysis was conducted on some insights of the focus groups by applying a set of basic statistical analyses such as percentages and mean values. In the opening phase, the children were asked about their favorite chat platform as this will give an insight into where children are chatting and thus which platforms would be promising partners for installing the AiBA system. Also, in terms of raising awareness, these platforms should pay additional attention to educating their users about online grooming and sexual predators. If they had to decide for one platform, a striking amount of 68% would choose Snapchat (Figure 4). The popularity of this application among this age group makes it a very promising place to reach out to children and educate them about online grooming and chat security. The second and third most popular applications are the social media chats Facebook Messenger (11%) and Instagram (9%). The official age limit of both Facebook and Instagram is 13 years which might indicate that these applications will become more popular when the children get older, since the majority was only 12 years old. This goes in line with the findings of a recent European study on youth online behavior (Smahel et al. 2020) that shows that the

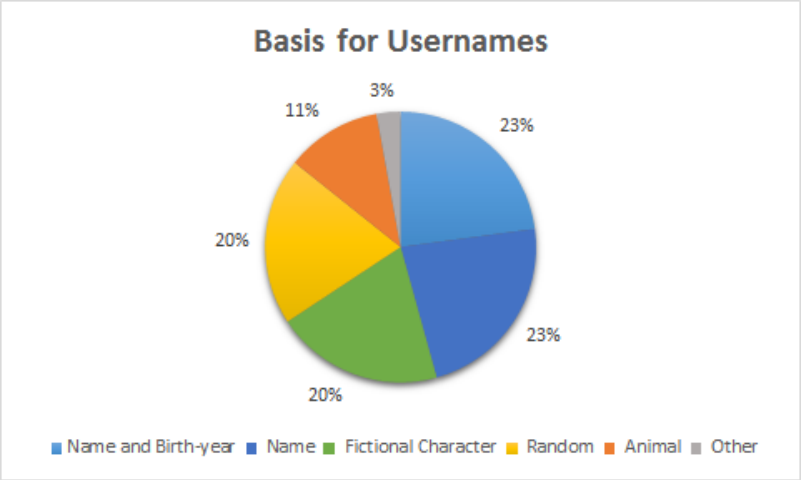


Figure 5: Basis for choosing usernames

European average of daily social media usage increases from 63% of 12-14 year-olds to 77% of 15-16 year-olds. In Norway, the percentages are even higher, with 75% of 12-14 year-olds and 90% of 15-16 year-olds. Therefore, social media advertisement will be most efficient for reaching older teenagers.

The creativity of the children was challenged in order to keep them engaged in the focus group. They were asked to come up with a username for a fictional chat. Since usernames are one of the most decisive factors for predators to target their victims (Winters et al. 2017), the goal of this game was to identify what the children base their usernames on and what information they reveal with it. There had been no indicators that the children who received education about online grooming chose usernames differently than those who were not educated. Reviewing the usernames, five categories were identified that served as a basis (see figure 5). The majority of children in both BPG and APG based their username on their real name or some variation of it (46%), like their first name and the year they were born in, their first name and a combination of smileys or their first name and an abbreviation of their last name. 23% of children were giving away their age in their username by stating their birthday. The second most common basis for usernames were fictional characters from movies, TV-series and games (20%). Some children modified the character's names with random numbers, additional words or smileys. 20% of the children reported that their username was chosen randomly by picking words that came to their mind, "something that sounds cool" or made-up words with no meaning. Examples are "username123", "Me Me" and "Yeah". Some children based their username on animals they like or using the name of their pets (11%). Lastly, one child chose to use its favorite food as a username, which has been assigned to the category "Other". Although these usernames were only chosen for a fictional chatroom, it is striking to see how many of the children used their names and even their age as a basis, thus revealing a lot of information about

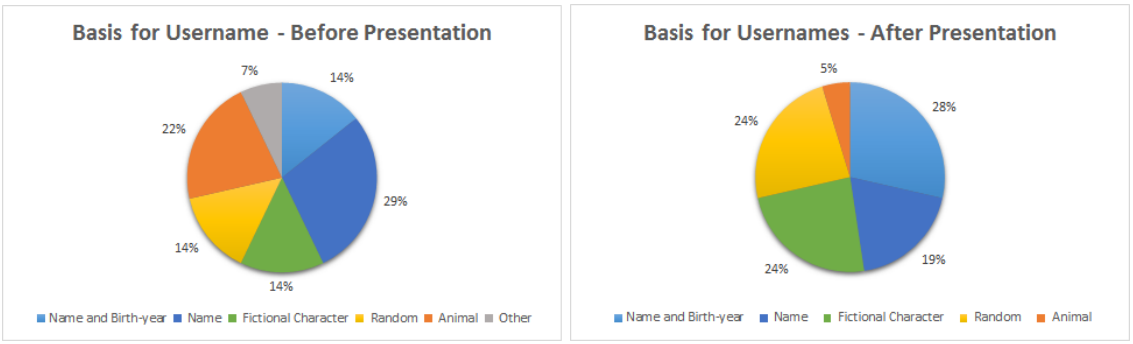


Figure 6: Basis for choosing usernames - before and after presentation

themselves. Also, the presentation did not influence the choice of usernames, as Figure 6 shows by comparing the two groups. Using names was the most popular basis in both BPG and APG, followed by fictional characters and random words with approximately the same popularity. This indicates that the children get more aware of online sexual predators in general and inappropriate messages that are directed at them personally, but are unaware of indirect factors that influence being targeted of online grooming. Choosing a username did not seem to be in direct relation to the subject of chat security which might be a reason why the children were acting more careless than during the direct messaging.

To conclude the focus groups, the children were asked to rate the AiBA system on a scale of 1 ("I don't like this idea at all") to 10 ("I would definitely use this application"). This shows a tendency of the children's overall opinion of the AiBA system. At this point it is particularly interesting to compare the rating from before and after the presentation about online grooming. It can be seen that the children rate the system as more important after the presentation, with a weighted average score of 8,7 points, compared to an average of 7,4 points before the presentation (see figure 7). This might be caused by an increased awareness of the risks regarding online chatting and a clearer understanding of the advantages of a system such as AiBA since this had been discussed in the presentation as well. It shows that education on chat security and online grooming has at least a short term effect on the children's awareness and caution. The overall high rating can be caused by the children's desire to "be nice", however, since the analysis shows a clear rise in the ratings by more than one point average, the results can still be seen as meaningful. The reasons that the children stated who gave high ratings after the presentation (8 and above) included "It can save a lot of children", "It is good to know who you are talking with and if they are dangerous" and "Like we saw in those stories, it can save lives". This emphasises the finding that the children are more aware of the dangers and that they see the urgency of being safe in chat environments. In opposition to that, low and average ratings (5 to 7) before the presentation were explained with statements like "I know already how to be safe in chats", "I am already careful and don't need it" and "Sounds ok". One child rated AiBA with a 1, saying "I would not use it". Comparing these statements from the

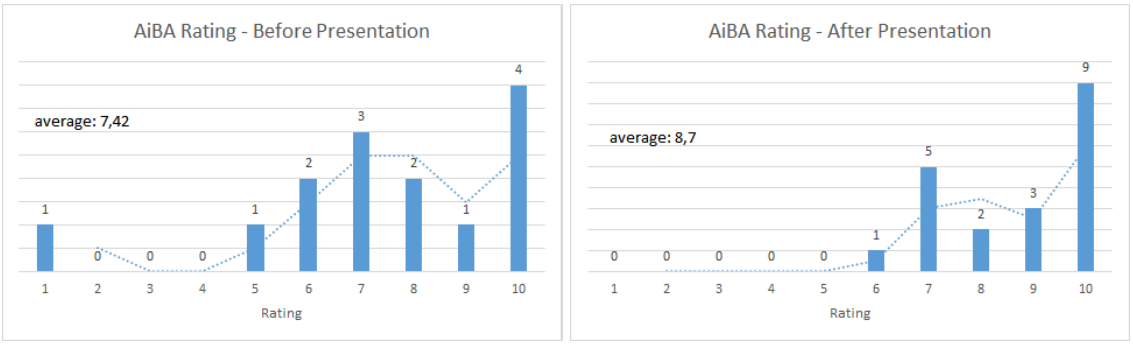


Figure 7: Rating of AiBA before and after presentation

low and high extremes shows how the children's views changed with the education. Although one has to keep in mind that the sample size of 34 ratings is rather low, it is still meaningful enough to show an overall tendency.

4.1.3 Summary of Results

Raffel et al. (2020) give a summary of the focus groups' results:

> "The focus groups showed that educating children about chat security and grooming can show some immediate, short-term results. The children became more aware of the risk and were discussing about sexual predators several times during the focus groups if they had been educated before. The focus groups showed the popularity of using Snapchat among children of 12 and 13 years as well as their strong interest in playing online games and consuming media content. These platforms can be important partners to spread education on online grooming and could also be potential customers for the finished AiBA system. The children mostly chat with friends, but it is not uncommon to chat with strangers when it is about a common interest, such as gaming. The children felt confident that they could detect an adult who tries to pretend to be a teenager through the language that is used and also the content of the conversation. They rated pictures or video calls as the most reliable option to find out who someone really is, however, they would not send pictures of themselves when being asked by a stranger. When creating usernames, the children unintentionally gave away a lot of personal information such as their name and age, regardless whether they had attended the presentation on chat security or not. In a fictional chat environment, those children who received education on grooming before were more self-assured to say "no", acted more confident and suspected dishonest behavior sooner than children without previous education on the topic. The overall rating of the AiBA system was more positive after the presentation, showing that the children saw more value in it than before."

4.2 Surveys

The surveys were sent out to parents of children in the seventh grade living in the area of Gjøvik. A total of 20 responses has been recorded. Although this amount does not yield reliable statistical results, the insights can still be used to identify information needs of the parents and reveal knowledge gaps. The low amount of responses can be explained by the strain that was put on the parents due to the COVID-19 outbreak.

4.2.1 Data Analysis

The first section to be analysed covers background information and the parents' general knowledge about grooming. Figure 8 shows a breakdown of the children's gender, the parents' knowledge of the term *grooming* and their familiarity with information materials about the subject. The distribution of the gender of the children was relatively even, with 55% of parents having daughters, 40% having sons and 5% having both a daughter and a son of 12-14 years. This information will be useful to identify differences between the opinions of parents with daughters and those with sons. Alarmingly, 25% of the parents have not heard the term *grooming* before. Although this does not imply that they are not aware of sexual harassment of children online, it shows that there is a general lack of information about the topic. This is backed up by the following question that asked if the parents have come across information material about online grooming. Only half of the parents have seen such materials. Of those, the most common source of information has been the internet, either through Facebook, online newspapers or by independent searches on the web. Two parents stated that they work with children themselves and have therefore received extensive education about grooming. In one answer, it was mentioned that information has been received from *Barnevakten*, a Norwegian foundation that advocates safe and responsible media use for children. These answers show that there is an imbalance in the parents' knowledge about grooming. While some have never heard the term before, others have received information or even extensive education. For the risk communication strategy, this means that the information has to accommodate a wide range of previous experience. It has to provide basic knowledge as well as helpful messages for those who are already familiar with the risk.

Looking at the next question, it is (positively) surprising that no parent has stated that their child has reported negative experiences on the internet to them. While it would be comforting to assume that this means that none of the children had made upsetting experiences, it can also indicate that they do not confide in their parents with these issues, in particular when looking at the data collected in the EU-kids-online report (Smahel et al. 2020) which shows that 25% of Norwegian children aged 12-14 years had made negative experiences on the web. However, since the sample size was very small and regional factors (such as Gjøvik being a small town in a rural area) might play a role, no clear deductions about this issue can be made. The last question in this section asked the parents whether they knew which websites and apps their children use. All parents answered that they knew at least some, but not all (45%) and more than half claimed to be fully aware of their children's internet usage (55%). This shows that there is some degree of communication about internet usage between the parents and the children which forms a good basis for educating them

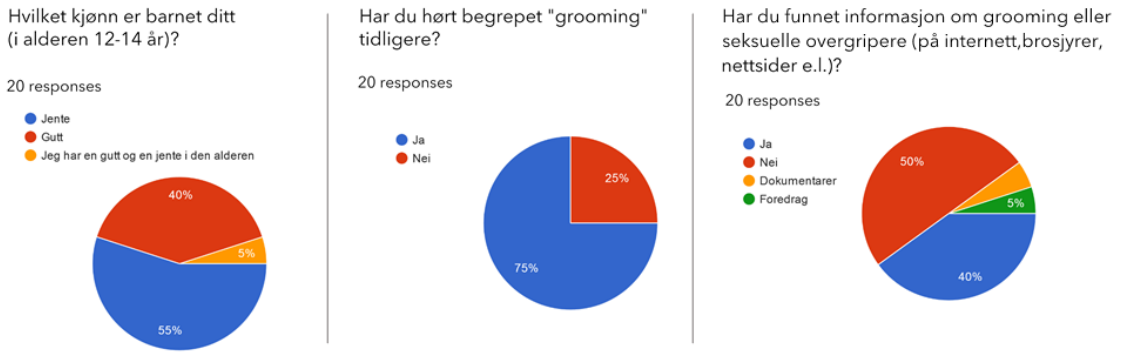


Figure 8: Children's gender, knowledge of the term "grooming" and familiarity with information materials

about grooming and online safety. Interestingly, 2/3 of parents who have a daughter claim to know all the websites and apps their children use, while only 1/3 of parents who have a son claim the same.

The second section investigated the parents' conception about grooming in further detail. The parents were asked to share their opinions and views in long answer texts, therefore a thematic analysis was chosen as evaluation method. The answers were written down on post-it notes and grouped and categorised with regards to their content. When being asked how predators are choosing their victims online, the parents jointly collected a vast amount of factors. They identified various websites and apps that are used by children as initial access points. Social media and chatrooms were mentioned several times. One parent assumed that grooming predominantly takes places "late at night". Potential victims were described as "lonely", "isolated", "vulnerable" and "with few friends". It was also pointed out that predators select their victims based on information in the child's public profile, such as gender, age, location and pictures. Four parents noted that predators select victims randomly and that they contact a lot of children in the hope to receive an answer. Therefore, they pointed out that any child can be targeted. One parent suggested that children can also be groomed by someone they know in real life. Regarding grooming strategies, it was often assumed that predators pretend to be children or teenagers themselves. They "lie and deceive" and exploit the children's interests in order to build trust and manipulate the victims. One parent said that they did not know how predators engage in grooming approaches.

The views on how one can distinguish a conversation where a child is being groomed from a normal conversation differ greatly among the parents. While some parents believed that the focus is immediately on sexual content, others assumed that the conversation gradually moves towards increasingly private topics. Some pointed out that the conversations can seem innocent at first, like a "friendly chat" or an "ordinary conversation". The predator asks the child many questions to find out more about interests and vulnerabilities while pretending to be the same age as the child. Compliments, encouragement and praise build confidence in the children and make them trust the

predator. A clear indicator for some was asking for private pictures or trying to set up a meeting in real life. Two pointed out that they do not know how to recognise grooming at all. The varying opinions and knowledge levels are confirmed in the next question that asked if the parents think that they themselves would be able to differentiate between a normal conversation and grooming strategies. While 30% said that they would be able to, 25% said that they do not think they could distinguish between the two. The remaining 45% was not sure about it. Again, this reflects the varying level of experience with the topic, but it can also indicate the accuracy of the hindsight bias that was investigated by Winters & Jeglic (2016). Considering that 25% of the parents said that they had not heard the term grooming before and only 50% has received information material about it, 30% saying that they can recognise grooming in a chat seems to be a relatively high number. However, due to the small sample size, this cannot be considered a significant statistical result, but should rather be treated as a tendency.

When asked about their main concerns regarding online grooming, many parents stated that they fear that their own child might be targeted (40%). Another concern shared by several parents was that children might not talk about negative experiences on the web or conceal new acquaintances (20%). Also, it was pointed out that they worry about children who are more vulnerable or gullible to become victims of sexual harassment. One parent said that it was worrisome that any child can be affected, regardless of external factors. Also, it is concerning that grooming is hard to detect and might therefore be discovered too late. All these concerns need to be taken into account when creating the communication strategy so that the parents feel understood and supported in their worries. Corresponding to their concerns, 80% of the parents said that there is a chance that their child can be selected by an online predator (70% saying that their child is *maybe* at risk and 10% saying *yes*, their child is at risk). This shows that there is general awareness that every child can become a victim of online grooming. Thus, it can be assumed that the parents are willing to receive information about the subject and are open for education. Interestingly, three of the four parents who said that their child is not in danger of becoming a victim, are parents who have a son. Simultaneously, those who said *yes* to their child being at risk all have a daughter. This accommodates the belief that girls are more at risk of being sexually harassed than boys. The section concluded with asking the parents if they have talked to their children about online security. 70% reported that they have talked *a lot* about it with their children, while the remaining 30% have talked *a little* about it. While it is hard to say what the parents perceive as *a lot* and *a little*, it shows that online security is a relevant topic in most families. Figure 9 shows a breakdown of the presented quantitative data.

The next section asked the parents about their opinions on grooming prevention. Again, it was evaluated with a thematic analysis. First, it was asked what kind of measures they think could help to prevent grooming. Two categories could be identified in this regard: communication with the child and restrictions/monitoring of online behavior. Those who were in favor of an open communication with their children proposed measures such as making them aware of the dangerous aspects of the internet, especially of the risk that is involved when chatting with strangers. Online grooming should be addressed openly, including real cases, to convince the children of the need to

Figure 9: Ability to recognise grooming, perceived risk that own child is targeted and communication about online safety with child

be cautious. It was advocated to be interested in the children's "web life" and get familiar with the platforms they use. The children should be reassured that they will not be punished in case they do something "wrong" on the web and it should be ensured that they are confident enough to talk about and report incidents. Additionally, it was advised to directly ask about negative experiences and not to be afraid to talk about unpleasant things. Those parents who were in favor of monitoring their children's online activities or to restrict internet use suggested to have clear guidelines and agreements about internet usage. They would not allow children to use specific websites or functions (e.g. a public profile) until they are older and prohibit contact with people they do not know in reality. One parent even suggested checking regularly with whom the child is chatting, while another admitted that fully monitoring the child's online behavior is neither possible nor the best solution. It can be assumed that the two categories represent different styles of parenting, one based on openness and trust, the other based on guidelines and control.

Then, the parents were asked about their personal information needs; in particular what information about grooming they as parents would rate as the most important. The answers could be divided into four categories. First, parents wanted more general information about grooming; what it is, where and how much it is happening, as well as how it is developing. Secondly, they expressed interest in getting more information about prevention measures and how to protect their children. Furthermore, they wanted to know more about recognising signs of grooming and uncovering it before it is too late. The main interest, however, was expressed regarding ways to communicate the topic to children and maintaining an open relationship. Information about real cases and experiences was requested, so that one is not perceived as "the desperate mum who thinks everything is dangerous". Additionally, parents were interested in advice and insights from professionals working with the subject. One parent summarised that he/she needs to know "actually everything". These interests show that the parents need information on the whole grooming process, but that special attention should be paid on how to communicate it in a child-friendly way.

Lastly, a short assessment of the AiBA project was conducted. A brief introduction to the idea and functionality of the system was given, and the parents were then asked about their expectations towards it. Three types of answers could be identified. Half of the parents expected the system to provide better online security for their children. Some remained quite general (*increase security, keep children safe online, prevent grooming*), while others were more specific. For example, one parent answered that AiBA should be used on social media platforms that are frequented by children and that it should be flexible enough to adapt to the quick changes in that industry. The second type of expectations consisted of the need to raise awareness of the topic. 25% of the parents hoped that AiBA could draw appropriate attention to the subject and enable a dialogue about it. This included discussions in the general public as well as communication between parents and children. Lastly, the remaining answers were quite vague, either stating that the parent had *great expectations* or that they simply *do not know*. The reason for the latter was sometimes explained to be a lack of information about the AiBA project.

Regarding information needs that the warnings have to fulfill, the parents mentioned a variety of information they would like to receive in case that AiBA detects a predator conversing with their child. Again, three main categories evolved from the answers. To start with, the parents want general information about the dialogue that triggered the warning. Such information includes the platform on which it took place, specific parts of the conversation that indicate grooming or harassment and what the alleged predator already knows about the child. Then, the parents were concerned about how to react to the warning and what should be done next, both from the parent's and the child's side. Some were wondering when they should contact the police and what information the police needs in that case, while others were explicitly asking for advice that did not include the police. Lastly, the parents were wondering how to talk to the child about the incident and how to communicate the danger without scaring or intimidating the child. One parent was suggesting that AiBA automatically blocks alleged predators so that the child cannot converse with them anymore.

The parents see some challenges in the implementation of the AiBA system, especially regarding privacy and data protection (30%). They are concerned that AiBA monitors the content of a conversation and can thereby be misused. For the communication strategy, this means that it needs to be clarified what information AiBA uses for its risk assessment and how that data is processed. Also, it was mentioned that having an application like AiBA in place can seem like monitoring to the children and imply that the parents are not trusting them. Furthermore, children might assume that they are completely safe from harm once they have installed the application as a safety measure. Again, these issues are dependent on the way that parents and children communicate about the subject. Therefore, advice on how to introduce AiBA to children should be given and it needs to be clarified what can be expected of the system. However, 25% of the parents said that they see no problems or challenges with the concept of AiBA, or that they cannot think of any at that particular moment.

A simple assessment of the perceived usefulness of the system shows that the parents have a neutral (20%), positive (35%) or very positive (45%) impression of AiBA (figure 10). The neutral

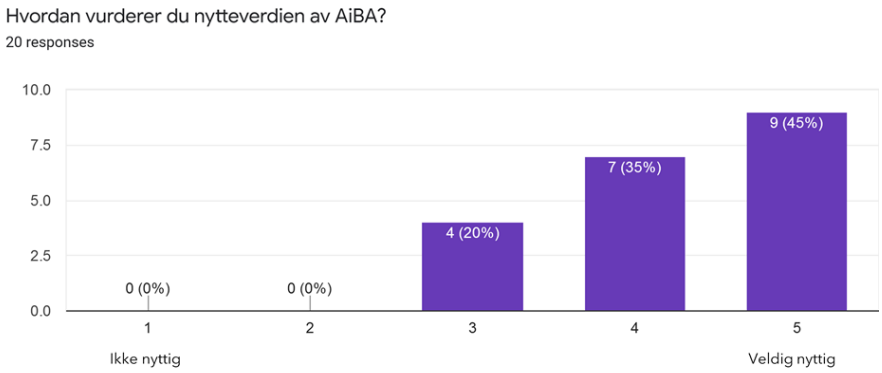


Figure 10: Rating of the perceived usefulness of AiBA

ratings were explained by perceived privacy issues and the surveillance character of the application, as well as the fear that it can be exploited. The positive and very positive ratings were explained by the need to protect children from abuse and that it is good to have additional safety measures. AiBA could be a great help for parents, and several parents pointed out that it is better to have it than not to have it. However, it became clear that many parents needed more information about the project before they could give an assessment of it, since 15% stated that they could not say much about it without further information. Nonetheless, this also shows the importance of marketing AiBA in an understandable way that presents its main functions and advantages in a short and compelling manner.

4.2.2 Summary of Results

The survey shows that there are huge differences in the general knowledge about grooming among parents. This means that the communication strategy has to deliver relevant information for both inexperienced and experienced recipients, covering basics as well as expert recommendations. The most common source of information about grooming is the internet, in particular online newspapers and Facebook. Offering a channel where material is bundled in one place will make it easier for parents to access information. It has been shown that internet security is a relevant topic in most families and that the parents address the subject (to varying degrees). Collectively, the parents were able to identify many aspects of grooming such as targeting methods and approaches. However, most answers only contained fractions of the whole picture or conceptions that are not fully accurate (such as victims being mostly isolated children). The parents have expressed great interest in advice on how to talk to their children about this sensitive subject. Communication has also been determined as one of the main prevention methods, along with guidelines and restrictions on internet use. The concept of AiBA has received a predominantly positive evaluation. However, the parents were torn between the surveillance character of the system and its safety benefits.

4.3 Risk Assessment

To identify underlying problems, set priorities and decide the scope of the risk communication strategy, a strategic risk assessment was conducted. Lundgren & McMakin (2009) propose to start by stating the reasons why a risk must be communicated. To do so, the gamestorming method "The 5 Whys" (Gray et al. 2010) was employed based on the insights gathered in the focus groups and surveys. The objective of this method is to reveal the underlying reasons by repeatedly asking "Why?". Each statement presents one reason for developing a risk communication strategy, meanwhile discovering related issues that are part of the problem. The results looked like this:

Why should the risk of online predators be communicated to children?

1. Because children have a high level of Internet access at an increasingly younger age that can expose them to danger.
   Why?
2. Because children are at risk of falling victim to grooming in chat applications.
   Why?
3. Because they converse with strangers, trust them, give away private information and have trouble saying 'no'.
   Why?
4. Because they are not aware of the risk of sexual predators and the consequences.
   Why?
5. Because they want to play online games, chat or talk without worry.

Why should the risk of online predators be communicated to parents?

1. To enhance the parent's knowledge of how predators groom children online.
   Why?
2. To enable parents to recognise the signs of grooming and to enable conversations with their children about this subject.
   Why?
3. Because parents need to be sure that their child can be safe on the Internet.
   Why?
4. Because parents cannot supervise all of their children's online activities.
   Why?
5. Because they respect their children's privacy and autonomy.

The next step when assessing a risk consists of determining the affected population segments and their characteristics (Lundgren & McMakin 2009). This can be realised by reviewing the discussed literature as well as drawing conclusions from the focus groups and surveys. The main target audience consists of children and teenagers, in particular aged 12-13 years as this age group provided the data for this study. As estimated by Smahel et al. (2020), the average of children in the EU of this age spends around 192 minutes online each day, in Norway the average time spent online

is even higher with 237 minutes. Among the main activities are online games and chatting, where they are potentially at risk of falling victim to online grooming. Webster et al. (2012) describe risk factors for grooming in two categories: vulnerability and risk-taking. Predators are more likely to target children who show vulnerabilities such as perceived neediness and attention-seeking, low self-esteem, difficulties with parents and lack of social interaction with peers. Risk-taking children feel like they are in control and are looking for an adventure, they are outgoing and confident online - behavior that could also be observed during the focus groups when questions were avoided with humour and irony or by becoming offensive. However, it is important not to stigmatise children who are at risk, or to summarise them as a homogeneous group. Targeting tactics of online predators can vary immensely and any child is at risk of becoming a victim. Therefore, it did not seem appropriate to create personas of the target audience when discussing such a sensitive subject. The surveys with the parents have shown that the level of knowledge about grooming varies greatly. However, they are all concerned about their children's online safety and address the risk with different parenting methods. While some rely on open communication and trust, others restrict access to specific online services.

In order to describe the risk as precisely as possible, the insights of the literature review and the data collection were evaluated with "The 4C's" method (Gray et al. 2010). This method is helpful for gathering and organising information about a subject with a structured and intentional approach. The topic is broken down into four categories; Components (what parts constitute the risk), Characteristics (how does the risk manifest), Challenges (obstacles associated with the risk) and Consequences (outcome if the risk is not addressed). The following assessment was done using a flipchart and sticky notes:

The risk of children being contacted and groomed by predators in chat environments consists of:

1. Components: Predators using the Internet to find victims, Internet access at a young age, security measures in chats, grooming strategies, conversing with strangers, trusting strangers
2. Characteristics: victim being targeted by predator, children "befriending" predators, predators requesting sexual content or activities from children,
3. Challenges: unawareness, lack of knowledge about topic, taboo, shame, victim-blaming, naivety, risk-seeking behavior, lack of security measures in chats, lack of parental supervision vs. wish for autonomy and privacy, hindsight-bias, ignorance ("This cannot happen to me")
4. Consequences: children falling victim to sexual abuse, children meeting with predators in real life, being exposed to sexual content, children sharing private pictures online, children sharing private information online, children being bullied, threatened or blackmailed, psychological damage, stress, dependency on the relationship with predator, problems with parents, social insecurity, self harm.

Reviewing the 4C's, the risk originates from predators that have discovered the Internet as a means to contact children who have access to web-enabled devices at an increasingly younger age. In

many chats, there are no sufficient security measures to protect children from grooming. A global information security survey has revealed that 77% of organisations are in need of ways to improve their cyber security (IBM 2019), since most existing solutions rely on single information sources that only allow for limited analyis. Additionally, predators have developed grooming strategies that encourage children to converse with them and build a trusting relationship. The risk manifests itself when a child is being targeted and "befriended" by a predator, often with a quick introduction of sexual content or the request of sexual activities. Raffel et al. (2020) further summarise that

> "Challenges that are faced when tackling the topic are the general unawareness of the children who are active in chats and also the parent's lack of knowledge about the subject. It is sometimes treated as a taboo topic that evokes feelings of shame, it can result in victim-blaming and is seen with hindsight-bias, meaning that people claim to have "seen it coming" only after an incident, or the risk is being ignored as it seems unlikely to happen to oneself. Since children want to maintain a certain level of autonomy and privacy, a lack of parental supervision can increase the risk, as well as a lack of security measures in many chat applications. However, if the risk is not addressed, it means that ultimately more children will fall victim to sexual abuse, either through physical meetings with the predators or through online activities. Children will be exposed to sexual content and might share private pictures and information. This can result in the children being bullied, threatened or blackmailed which in turn results in psychological damage and a dependency on the relationship with the predator. In real life, consequences can be seen in a problematic relationship with the parents and peers, since the online relationship gains importance."

Lastly, it is important to describe what the desired outcome of the risk communication will be, in as much detail as possible (Lundgren & McMakin 2009). For this, the "Elevator Pitch" method (Gray et al. 2010) was employed. It has to deliver the key issues and how the audiences will benefit from it. The pitch is compiled by the following sentence structure:

> "FOR (target audience), WHO HAVE (audience need), (product name) IS A (market category) THAT (one key benefit)."

In an ideation phase, the components of the elevator pitch were identified based on the previously conducted methods:

1. Target audience: children (age 12-13) who engage in chat environments, parents of schoolchildren
2. Audience needs: Safety, security, privacy, autonomy, trust, reassurance
3. Key benefits: raising awareness and caution, encouraging children to draw boundaries, discouraging children of risk-seeking behavior, recognising grooming behavior, conversation about subject with others, preventing abuse (psychological and physical), increasing safety,

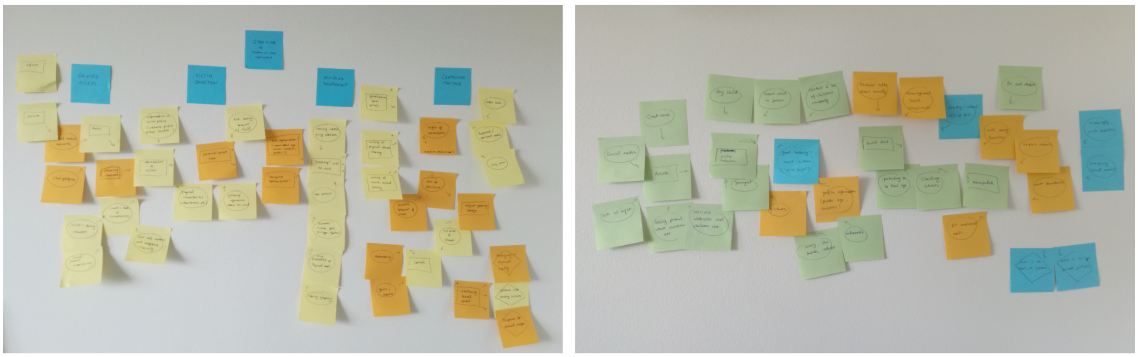


Figure 11: Creation process of mental models

reducing the perceived taboo around the topic to make people feel more comfortable to share experiences

Based on this ideation phase, the desired outcome of the risk communication can be described with the following elevator pitches for the different audiences (sentence structure has been adapted):

> "For children who engage in chat environments, who have a need for safety and security, as well as privacy and autonomy, educating them about predators on the web will make them more cautious and enable them to draw boundaries so that they can protect themselves from abuse and give them the courage to report incidents."

> "For parents of schoolchildren who want to trust their children to be safe online, educating them about predators on the web enables them to recognise signs of grooming and to talk about the subject with their children so that they can contribute to their children's safety on the web."

More specifically tailored to the AiBA system itself, the elevator pitch looks as follows:

> "For parents and children, who want reassurance that the child is not contacted by predators, AiBA is a software based on behavioural analysis that can contribute to detecting dishonest behavior and sexualized content in chat conversations."

4.3.1 Mental Model

The mental modal approach aims at revealing knowledge gaps of the audience by comparing their mental picture of a risk with an expert view. The differences in perception form the basis of establishing the information needs of the audience. Following the approach described by Morgan, Fischhoff, Bostrom & Atman (2002), an expert mental model was created based on the literature

review. The model was assembled by writing key terms of expert insights on post-it notes which were then grouped and connected (the process can be seen in figure 11). It illustrates the stages of grooming and how they are influenced by various factors (figure 12). The model does not claim to be complete, it rather shows a review of the insights that are most relevant for developing information material for parents. The model is built around the choices that a predators makes as described in the literature, such as selecting a victim and introducing sexual content in the conversation, and how these choices are influenced by circumstances and behaviors. The diagram concludes with consequences of grooming such as anxiety and self-harm. However, it is important to note that these effects can already occur at an earlier stage of the process.

In order to identify misconceptions and knowledge gaps, a second mental model was created based on the online questionnaire with the parents (figure 13). Not surprisingly, the mental model of the parents is more limited than the expert model. However, the identified aspects predominantly overlap with the expert model, such as the key concepts *access to and identification of victims, building trust, manipulation* and *moving boundaries*. The parents' model is lacking mostly in terms of the conception of risk factors. Although it was mentioned that any child can become a victim, the majority believed that mostly lonely children that are naive will be targeted. While this is not wrong and most likely implies other factors such as low self-esteem, it leaves out a number of additional risk factors, e.g. physical characteristics, limited awareness of online risks or risk-seeking behavior of the child. Also, the parents were not aware that not all predators deceive their victims regarding their age. Literature suggested that the majority of convicted predators employed a true representation of their age and gender (Malesky 2007). The parents accurately described the main grooming process as a seemingly friendly chat at first which aims at building trust. The predator then exploits and manipulates the child. The parents did not mention the possibility that the child might receive gifts from the predator, however, this is only the case in some grooming strategies. Furthermore, they missed that some children are exploring sexuality and identity online and that it is thus easier for predators to introduce sexual content. While the parents saw arranging physical meetings or the reception of private pictures as the main goals of grooming, experts point out that some predators gain gratification from the process itself or from exposing children to sexual content. Although grooming is predominantly a non-violent process, parents were not aware that threats or blackmailing can be employed if the child shows signs of revealing or ending the relationship. The parents saw abuse as the main consequence of grooming, which is accurate, but left out the accompanying consequences of anxiety, stress, shame and potentially self-harm. However, the parents showed good understanding of prevention approaches which mainly included open communication and partly restrictions of internet use. The experts merely added one aspect, public awareness of the risk, which is one of the overarching goals of the communication strategy.

The parents' model contained three misconceptions. Firstly, it was mentioned that online grooming takes place mainly *late at night*. No expert view on this could be found, but it is unlikely that this is the case since it can be assumed that most young children are not online at that time. Secondly, it was pointed out that predators *talk a lot about themselves*. It has been found that the opposite is true; that they are secretive about themselves but ask the child a lot of questions in order to gather

information (this aspect has been recorded in the parents' model). Lastly, it was already mentioned that most parents believed that mainly isolated and naive children were at risk, when actually any child can be targeted. Although the parents collectively cover the most important concepts, it has to be considered that there were great differences in their individual knowledge level, with some parents who were not informed about the subject at all and others having received professional training. Condensing the insights gained from the mental models, the key issues that need to be covered in the communication strategy are a clarification of the grooming process itself and how to identify it, a list of risk factors in combination with prevention methods and - also remembering the surveys - advice on how to talk to children about the topic.

4.3.2 Summary of Results

Based on the risk assessment and the mental model approach, the key messages for the communication strategy can be extracted. These messages should represent the audiences information needs and should be clear and concise (Lundgren & McMakin 2009). The key messages can be divided into four categories: description of the risk, risk consequences, level of control and awareness, and communication goals.

1. Description: Child predators are targeting victims in online gaming and chat applications based on certain criteria. They apply grooming strategies that can be hard to identify in order to gain the trust of children. The children are manipulated and pushed into online sexual activity or arranging a physical meeting.
2. Consequences: The children can suffer from a variety of psychological damages, social isolation, self-harm and sexual abuse (physically or online).
3. Level of control and awareness: It is generally known that predators use the Internet to contact children, however, the knowledge about risk factors, signs of grooming and prevention methods varies greatly. Also, the risk can seem "far away" in the sense that people are not aware that it can happen to any child.
4. Communication goals: The communication strategy aims at increasing awareness and knowledge about the grooming process to enable an open communication about the subject between parents and children. Children will be made aware of online risks and how to navigate safely on the web. Parents will be given education on how to prevent and recognise grooming. The overall goal is to increase children's online safety while also considering their privacy and autonomy.

Conveying and explaining these key messages will be the goal of the communication strategy and the warnings that are sent by the AiBA application. Regarding the AiBA application itself, it has been found that the judgement of the concept is predominantly positive both among parents and children. It is perceived as an extra layer of security that increases the chance to discover grooming before the child is harmed. However, concerns about privacy, information security and the feeling of being monitored need to be addressed.

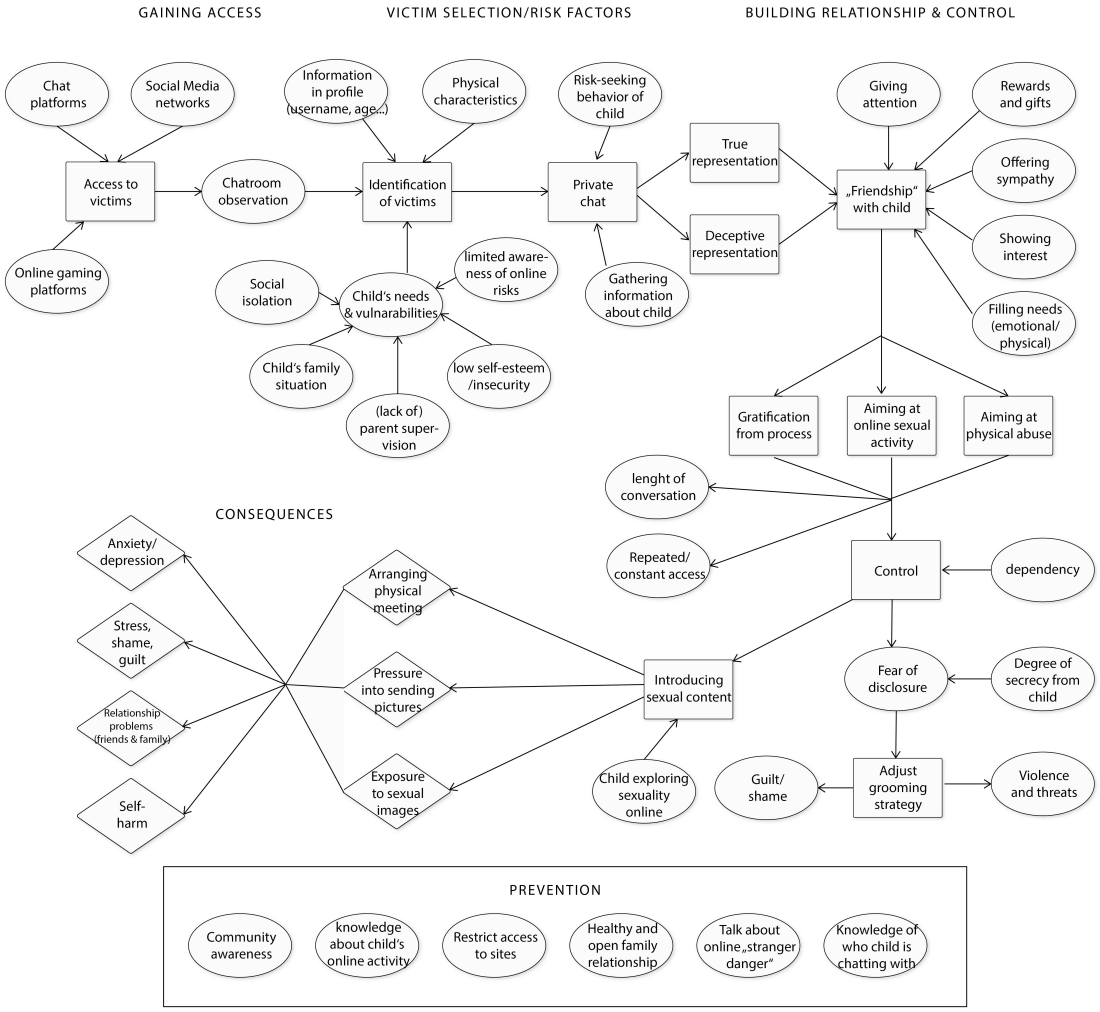


Figure 12: Expert mental model of the online grooming process

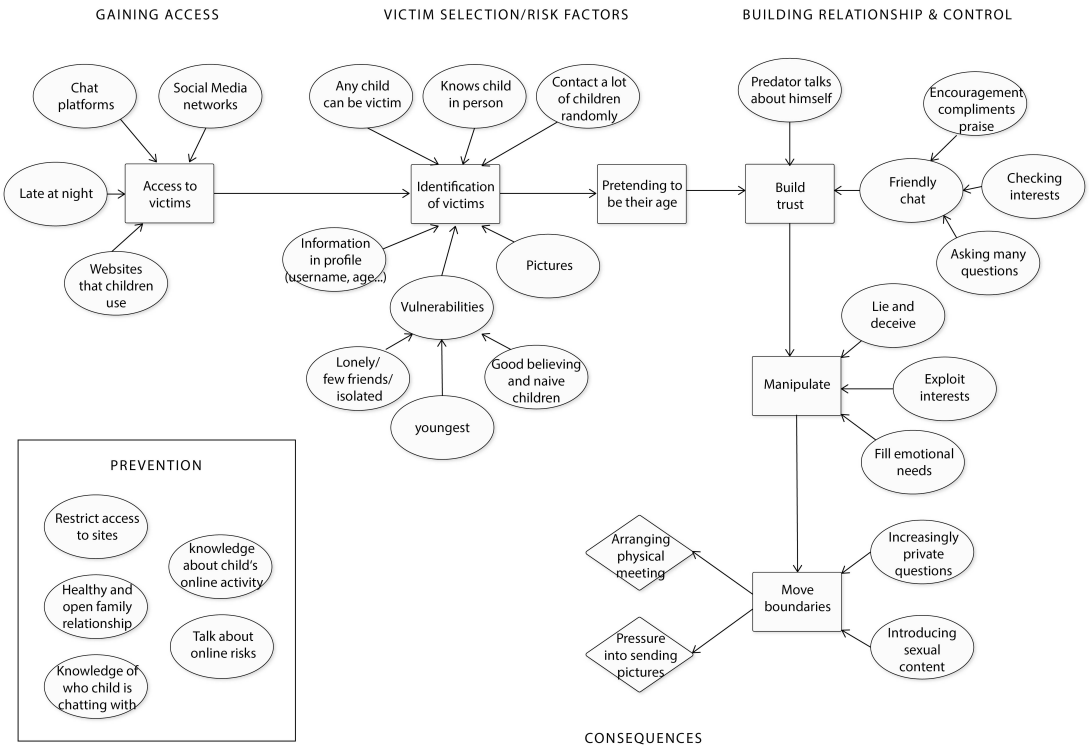


Figure 13: Parents' mental model of the online grooming process

4.4 Communication Strategy and Warning Design

The communication strategy systematically tailors the previously gained insights into a tangible plan for educating the audience about online grooming and how to react to the risk. The strategy is divided into three stages; Preparedness, Response and Recovery phase as described by Janoske et al. (2012).

4.4.1 Preparedness Phase

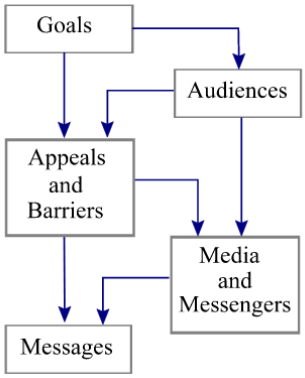


Figure 14: The GAAMM Model by Sandman (2007*a*)

Raising awareness among children and parents in order to sensitise them towards the danger of online grooming and enable them to recognize grooming patterns is the main goal of the preparedness phase. The WHO and Sandman (2014) propose four communication strategies according to the hazard level as assessed by experts and the public outrage related to the risk. High hazard and high outrage require *Crisis Communication* as could be observed during the COVID-19 pandemic in 2020, low hazard and high outrage should be addressed with *Outrage Management* in order to calm the audience down. High hazard and low outrage require *Precaution Advocacy* in order to raise awareness of an underestimated risk. If both hazard and outrage are low, *Education* can enable a dialogue with an interested audience. Recalling the expert's mental model, the literature and the potential consequences of grooming while being aware of the relatively low knowledge about the topic, the Precaution Advocacy strategy is an appropriate choice for designing a communication strategy. To craft this kind of strategy, Sandman (2007*a*) recommends to follow the GAAMM (Goals, Audiences, Appeals and barriers, Media and messengers, Message) Model as shown in figure 14. Goals and Audiences have been discussed in detail in the previous chapter. Appeals and barriers have also been discussed, but have not been labeled as such. Appeals describe needs, attitudes and emotions that make the audience inclined to follow the communication strategy's recommendations while barriers are opposing the audience to follow. The most important appeals that have been identified in the user research phase are the desire to protect children from harm, the need for children to be safe in chat environments and the children's wish for autonomy to speak for them-

selves. Main barriers or challenges are general lack of knowledge about the topic (both parents and children), ignorance and denial ("This cannot happen to me") as well as being ashamed to address the topic. Very important for the success of a communication strategy is the choice of appropriate media and messengers to spread the information. Here it is important to point out the differences between the target groups. The children spent a vast amount of time on the Internet, so it makes sense to target them there. Advertisement and information material can be posted directly in the chat environments that have children as their main users. To illustrate this approach, a Snapchat advertisement has been developed as an example. Furthermore, postings on other social media can extend the reach of the campaign and can be used to precisely target user groups that are at higher risk (e.g. users of a certain age group who "like" or "follow" specific applications). Since watching videos was among the main activities of the children on the web, creating video content is also highly recommended. The children need to be able to relate to the messengers that present the content, therefore the messenger should be close to the peer group, either being of approximately the same age or being liked by the audience, e.g. a popular celebrity. It is believed that this approach increases the children's interest in the content and reduces barriers such as ignorance and shame. Generally, the medium should support short messages that grab the children's attention. Raffel et al. (2020) further point out that

> "another effective way to reach the children is to conduct seminar days at schools similar to those conducted during the user research. This can provide the children with valuable background knowledge of Internet security and online behavior that can encourage them to rethink and adjust their own behavior."

The survey has shown that those parents who have received information about grooming before have found that information on the Internet. In fact, a couple of helpful and professional websites that educate about grooming have been identified, e.g. NSPCC (2020) and Childline (n.d.). Since this source is already available and offers in-depth information (depending on the website), an alternative medium should be considered to initially raise awareness among parents. For example, they can be reached through more conventional media such as leaflets and brochures that are available in school meetings or similar places. These materials can cover the essential aspects that have been identified with the mental model approach so that the parents gain a basic understanding of the subject. To create an illustrative example, a leaflet has been chosen for this project. Additional sources of information can be stated for parents who are in need of more in-depth resources. Furthermore, teachers can be appropriate messengers to convey the initial information to raise awareness, for instance during school meetings. Newspaper articles can also make parents aware of the risk. However, in-depth information should be presented by trusted experts or authorities so that credibility and integrity are ensured. Such experts can be people involved in the AiBA project, other IT security experts or police officials. Information can also be integrated in the chat or game applications themselves, as many provide information sites for parents, such as MovieStarPlanet, that already offers advice and on healthy media usage for children. In order to heighten emotional involvement in the issue, the communication effort can be written in narrative style as described

by Golding et al. (1992). Having a narrator that the parents can relate to is expected to increase interest and understandability.

In the following, the design guidelines by Sandman (2007*b*) are applied to craft the content of messages aimed at children and parents. Recalling the core values of his guidelines, the messages need to be on point, raise interest, appeal to emotions, offer choice and monitor the reactions. The leading questions that lie behind the messages are: How does grooming happen? What can it do to me/my child? How can I protect myself/my child?

Messages for the Preparedness stage aimed at children, applied in a Snapchat advertisement campaign:

1. Mia2008 was actually Peter1970.
   Anyone can be behind a username. #DontTrustStrangers
2. Do I know you?
   Be careful when chatting with strangers. #DontTrustStrangers
3. I like you, wanna know a secret?
   A predator can seem like a friend, don't fall for it. #DontTrustStrangers
4. Can you send me a picture?
   Predators find victims for grooming and abuse on the Internet. #DontTrustStrangers
5. Wanna hang out together?
   Never meet with someone you don't know personally. #DontTrustStrangers
6. Say no. Block. Report.
   Fight against sexual harassment and bullying. #DontTrustStrangers

The key message that leads the campaign is #DontTrustStrangers. Using a hashtag not only appeals to the young audience, but also helps spreading information and increases memorability of the campaign. The visual design of the Snapchat advertisement follows a clear structure. The overall colour scheme is held dark and simple in order to reflect the seriousness of the subject. First, a picture catches the viewer's attention which is then directed to the short message. The average length of a Snapchat ad is 4-7 seconds, so the message needs to be understood quickly. The hashtag and the AiBA logo are prominently displayed so that the viewer can connect the campaign with the brand. The user can interact with advertisement on Snapchat by clicking on the button at the bottom of the page or swiping upwards. This interaction leads the user to a website with additional information or to a store for downloading the AiBA application. Therefore, after raising awareness about the topic and increasing the viewer's caution when chatting with strangers, a sub-goal of the ad is to lead users to these additional sources of information. Two examples are given in figure 15, the full set of Snapchat advertisements can be found in the appendix (8.3). Apart from Snapchat, the design can be used on other social media platforms as well.

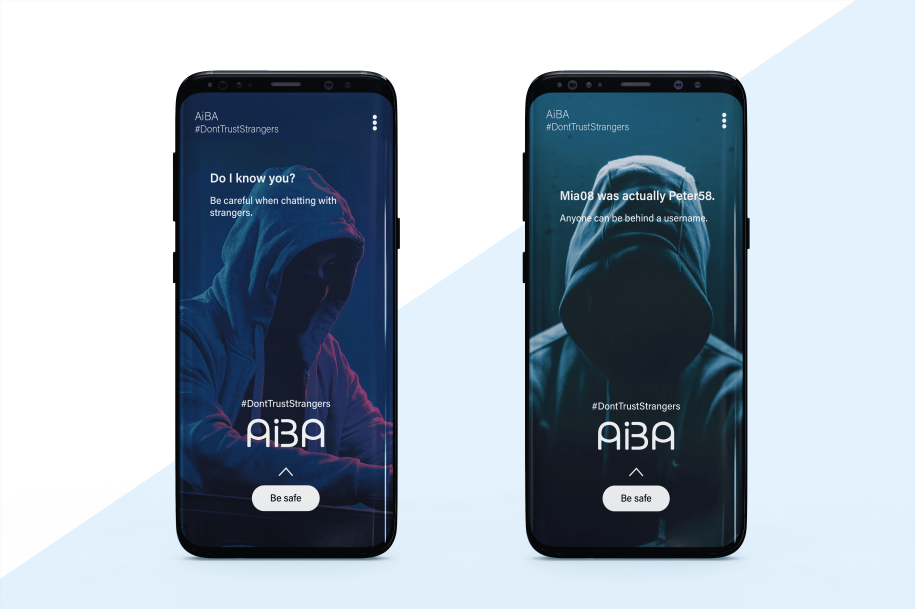


Figure 15: Two examples of the Snapchat advertising campaign

Content of the Preparedness stage aimed at parents, applied in a folded information paper:

1. **What is online grooming?**
   Online grooming describes the process of building a relationship or emotional connection with a child through web applications such as chats. Child predators can use grooming to manipulate children and push them to online sexual activity, sending private pictures or arranging a physical meeting for sexual abuse.
   Goal: Information about the basic definition of online grooming.
2. **How does online grooming happen?**
   Grooming is a highly strategical process that involves a number of steps. The predator identifies and accesses children through popular sites (chats, gaming platforms, social media etc.). In a seemingly friendly conversation, the predator learns about the child's interests and vulnerabilities. Over time, the predator gains the child's trust and makes the relationship seem special and exclusive. Based on the child's interests and vulnerabilities, the predator can exploit and manipulate the child by filling emotional or social needs. The predator introduces sexual content to the conversation, pushing the child into online sexual activity, sending private pictures or meeting in person. *Goal: An illustration of the process to increase the parents' understanding.*
3. **What makes children vulnerable to grooming?**
   Any child is at risk of grooming, girls and boys alike. However, predators will search for a child's vulnerabilities that can be exploited. For example, predators look for insecure children

with low self-esteem, or isolated children with few friends or a difficult family situation. Contrary, also very open children are more at risk, particularly when they explore sexuality online or show risk-seeking behavior. Little knowledge of online safety and naivety or openess towards strangers can also put children in danger. Children with disabilities are particularly at risk.

Goal: An explanation of risk factors that increase vulnerability, but also emphasising that any child can be targeted.

4. **How can I detect that my child is groomed?**
   Warning signs can be subtle, but you should pay attention if your child spends significantly more time online or is suddenly becoming secretive about online activities and chat partners. Some children neglect real life friendships while others might become stressed or depressed. Groomers sometimes give gifts to children. Also, sexualised behavior or language that is not appropriate for the child's age can be an indicator.
   Goal: A list of signs that indicate grooming so that the parents have a guideline to refer to.
5. **What can I do to lower the risk?**
   Education about online safety is key to the prevention of grooming. You should show interest in your children's online activities and get familiar with the platforms they use, but also trust them enough that you do not need to monitor all their chats. Clear guidelines on internet usage and online presence should be established. At the same time, a trusting environment will make your child feel safe to share experiences and worries. Teach your child about healthy relationships and that they always have the right to say no.
   Goal: Information on prevention methods and how to keep children safe online.
6. **How do I talk to my child about online safety and grooming?**
   Always listen carefully to your child and show them that they do not need to be afraid to share experiences with you. Stress that it is never the child's fault. Make sure your child understands that people are not always honest on the Internet and that they need to be just as careful as in real life when meeting a stranger. Establish guidelines, for example what information or pictures can be put online, but leave the child enough autonomy so that it does not feel monitored.
   Goal: Practical advice about how to address the topic and establish a healthy communication with clear guidelines.
7. **What do I do when I find out that my child is being groomed?**
   If the child explains that it has experienced grooming or harassment, always take the matter seriously and let your child know that it is not at fault. Let your child explain what has happened and report the incident to child care authorities and the police. Do not confront the alleged predator, because this can influence further investigations.
   Goal: Advice on how to react when the child reveals that it is experiencing grooming.
8. **Where can I get help?**
   For reporting grooming, getting additional advice or information, please contact: www.barnevakten.no (Information and advice on safe media use for children), www.overgrep.no (Personal advice

and possibility to report grooming) or www.nspcc.org.uk (detailed information about grooming in English)
Goal: Offering additional sources to learn more about the topic or receive help.

The content follows a logical order and covers all aspects of the identified information needs. The visual presentation supports understandability and presents the content in a structured way. The headline of each section is formulated as a question in order to represent the parents' information needs which is answered by the following texts. A narrative is added by introducing (fictional) messengers who tell their experiences with the subject. One narrative tells a story from the perspective of a 13 year old girl:

> "I was chatting with a girl who said she was my age and I felt really close to her. But then, the conversation turned and she asked me for naked pictures. I wasn't very confident and I wanted her to like me, so I just sent one. When she wanted more, she used that picture to threaten me. I was desperate and didn't know what to do, even thinking about hurting myself. When I told my mum and she involved the police, they found that I was actually chatting with a 45 year old man."

Although this story is fictional, it is based on reports of real grooming cases. The goal is to illustrate how children feel when they are groomed so that parents can understand them more easily. The second story is told from the perspective of a mother who's son was groomed online. It explains some if the signs that indicate grooming and a possible way to react:

> "When Lucas spent more time on the Internet, I first thought it was normal for his age. But then he pulled away, saying he was chatting with a friend he met online. He wouldn't let me see the chat. Lucas seemed stressed and nervous about it. Eventually, we had a long talk about online safety and he told me about his "friend" asking for private pictures and a meeting. I contacted Barnevakten and reported the grooming case to the chat administration. The predator was identified and is now facing serious charges. Lucas is now much more careful on the web."

At the end, a reference to AiBA is given where the main functionalities are shortly explained. This shows the parents who is responsible for the information material and directs them to AiBA's website with additional information. An exemplary mock-up is given in figure 16, more illustrations can be found in the appendix (8.4).

4.4.2 Response Phase

Raffel et al. (2020) write that

> "the immediate response phase to a risk is triggered when the AiBA system detects indicators of predatory behavior. A warning has to be sent so that the child and the parents can decide how to respond to the threat. For creating these warnings, design principles can be applied regarding the structure, understandability, noticeability and context of the messages.

Raffel et al. (2020) continue by describing that the warning message needs to make the user aware that a current chat conversation is showing indicators of predatory behavior or grooming. To do so effectively, it has to attract the user's attention so that the content will be read and the situation understood. Therefore, it needs to be displayed prominently so that the users are interrupted

Figure 16: Information brochure, unfolded.

in the current task and shift their attention. The design needs to be clear so that the message is understood immediately. Short, clear sentences are essential. Timing plays an important role since sending the warning too late leaves a child at risk and might result in harm to the child. On the other hand, sending the warning too early can produce unnecessary fear and false accusations. Therefore, it is crucial to train the system and set an appropriate threshold for sending warnings. In the same context, it is important to inform the user how the system arrived at this conclusion in order to justify the warning and ensure understandability. For example, this can be done by listing the detected characteristics that indicate grooming behavior. In addition, the urgency of the situation needs to be made clear by explaining the risk and its consequences so that the user sees the need to act. To support the user to take action, choices and recommendations for appropriate reactions should be given. One way to implement this would be a checklist for identifying grooming behavior and recommendations on blocking or reporting chat partners. Ultimately, the warning can only provide advice and suggestions, as the final decision to act or change behavior has to be taken by the user.

For a more detailed analysis of the information needs and design challenges at this stage, the target audiences are looked at separately. As described previously, the children are in need of an alert that they might be chatting with a person who is attempting to groom them. They need to be encouraged to draw boundaries for increasing their own safety when chatting with strangers. The used language should be simple and understandable for children. That also means that technical terms should not be used and that the information has to be reduced to the essential. Using a visual approach such as information graphics or charts to present the warning is believed to both

increase attention and understandability. The biggest challenge will be to make the children aware of the urgency of the warning, so it is important to directly address the risk of online predators. The focus groups have shown that addressing this topic made the children act more carefully, at least as a short term result. However, the reasons why AiBA is suspecting grooming should be given objectively as to not induce unnecessary fear. After explaining why the message is shown, the children need to receive advice regarding recommended actions. They need to be urged to reflect on the conversation and pause or end it if necessary. However, since a central wish of children is autonomy, they need to be given the option to continue the conversation as well. If a child chooses this option, they need to be urged to pay increased attention to signs of grooming. Finally, ways of seeking additional help need to be presented, as well as emphasising the importance of real life relationships with friends and family.

Making parents aware of the situation that their children are in, and encouraging them to approach them in the right way is the main goal of the warning to the parents. The warning is sent as a counteractive measure so that there is still time to act and enter a dialogue with the child. First, they need to be informed on what platform the alleged grooming is happening and which users are involved. Also, the indicators of predatory behavior that the system has detected need to be listed. Jargon and technical terms should be avoided to increase understandability, however, it should be offered to receive more in-depth information about the underlying process to increase trust in the system. Building trust is essential as it constitutes one of the key elements of risk communication and several parents have uttered concerns about privacy and potential exploitation of the system. Parents need to be instructed how to proceed after receiving the warning, as overly emotional and irrational reactions can have negative effects on the child's behavior (e.g. triggering defiance). The instructions need to be given in clear, simple steps so that they are easy to follow. The message needs to clarify that it is important to address the topic carefully and listen to the child's perspective. Judgemental reactions could deter the child from telling the truth, because of fear of the consequences. In addition to the indicators of grooming that have been identified in the child's chat conversation, the parents need to be encouraged to look for other signs of grooming. Such signs can include the child pulling back from real life relationships or spending more time than usual on their devices. If evidence of grooming is lining up, a more serious conversation about the child's online activities is necessary. Finally, the parents need to be provided with contacts where they can report online grooming.

In order to visualise these insights and ideas to design the warning, an iterative design process has been employed. The ideas were first sketched as simple paper wireframes which were evaluated according to the warning design guidelines by Wogalter et al. (2002). The wireframes have been adapted and elaborated into a clickable prototype using the design tool Figma. Exemplary screens can be seen in figure 17 and 18. This process has been employed for both target groups. The prototype of the warning that is sent to the children's device starts with a short exemplary chat conversation between the user and "Noah" who is applying grooming strategies. When "Noah" asks for a private picture, the threshold is reached and AiBA sends a warning, saying that it has detected grooming behavior. The warning is displayed on the bottom part of the screen as an overlay, so that

it covers the field for entering messages. Aditionally, it is displayed in bright red to attract attention. Thereby, the message cannot be missed if the user wants to continue the chat. The user has the option the close the warning in order to be in line with usability heuristics that stipulate that the user should always be in control and have choices of action (Nielsen 1994). However, the design of the warning encourages the user to click on "What now?" to learn more. The warning expands and it is explained why the user received the message. In particular, it is stated that there is a risk that the chat partner is a sexual predator. The user research had shown that naming the risk straight forward increases awareness and attention. Then, the indicators that were identified by AiBA are listed, e.g. messages that contain sexual content or insights from biometric assessments. If desired, the user can access the questionable messages or get more information about the biometric approaches. Presenting the "proof" in this manner is believed to increase transparency and trust in the system. It is emphasised that predators are using the Internet to access victims and that one should not thoughtlessly trust strangers. On the next screen, the user is given advice on how to handle the situation. The user can swipe through three recommendations. The texts are kept short so that they are easy to read and understand. Additionally, illustrations are added to make the message less text-heavy and make the design more child-friendly. The order of the advice was chosen according to the insights from the user research. The child can first try to handle the situation independently by asking the chat partner to stop sending inappropriate messages. It is also emphasised that the child should talk to a trusted adult and seek for help. Lastly, the grooming (attempt) should be reported. The last page wraps up the warning by remembering the child that it is not at fault and that it always has the right to say no. The importance of communication with family and friends is emphasised, as well as a reminder to be careful when chatting with strangers. The colour scheme of the warning is simple, but uses a bright red to emphasise interface elements and attract attention. The use of simple icons gives additional structure and adds to a clear hierarchy. A progress indicator at the bottom of the page gives the user an idea of the scope. When the warning is closed, a notification that a report of the incident has been added to the AiBA application appears. Although this application would go beyond the scope of this thesis, it is imagined to serve as a central hub to review warnings. This will make communication between children, parents and authorities easier, especially when grooming is reported and evidence is needed.

The warning that is sent simultaneously to the parent's device resembles the warning for the children in order to maintain a consistent design and increase recognition of the brand. After opening the warning, the parent is made aware that their child might be chatting with a predator. Immediately stating the risk is believed to increase attention. First, the warning gives an overview of the facts related to the risk (in what application is the chat happening, what is the username of the chat partner and what indicators for grooming have been found?). More detailed information on the found indicators can be accessed by clicking on them. This screen explains the basis of the suspicion that the child is conversing with a predator. On the next screen, the user gets advice on how to react to the situation at hand: remaining calm, talking to the child about the incident and potentially reporting grooming. The texts are kept short so that they are easy to read in a stressful situation. On the next page, the user receives additional advice for addressing the topic. These

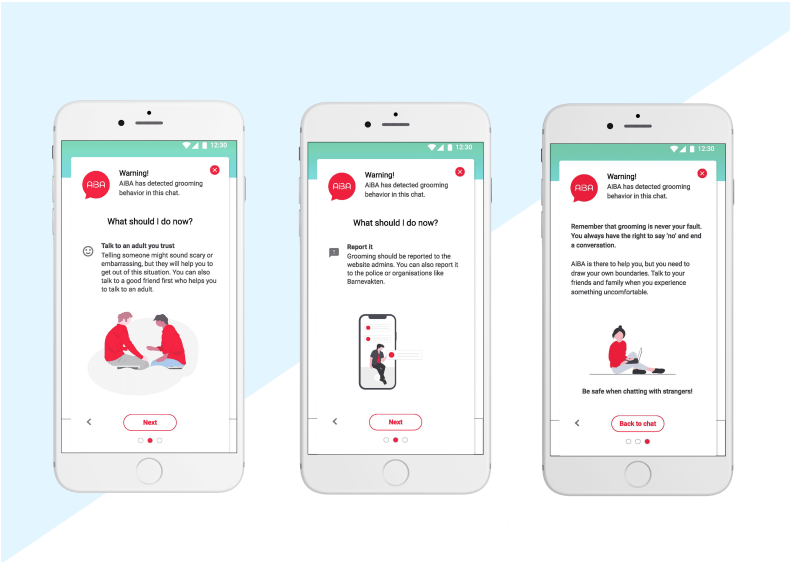


Figure 17: Three exemplary screens of the clickable prototype for children

recommendations are intended to encourage teaching the child responsible online behavior. Signs of grooming are repeated so that the parent feels in control and knows how to spot long-lasting grooming attempts. The last page directs the parent to online resources for additional information or organisations for reporting grooming. After closing the warning, the parent also gets a notification that a report of the warning has been saved for future review. The visual design is kept simple and clear. Red colour is used to highlight interface elements. There are less illustrations than in the children's design, because the parents are in need of trustworthy information rather than an artistic screen design. All exemplary designs and links to the clickable prototypes can be found in the appendix (8.5 and 8.6).

4.4.3 Recovery Phase

After the immediate risk has been averted, the goal of the Recovery phase is to provide additional support and to encourage the audience to take further actions, as well as counteracting apathy (Janoske et al. 2012). The information should be directly available to the users so that they can access it after receiving the warning about predatory behavior from the AiBA system. The most effective way to reach the users is to send the information directly on their devices after a warning has been sent by AiBA. This can be realised in the application itself and via email to a connected account. The exemplary designs show how the recovery messages can be integrated in the application. It is believed that sending the message one day after the warning is an appropriate time, since it allows the situation to cool down and gives children and parents time to talk. However, information where to get additional help should also be available unrelated to the warning message so that it is

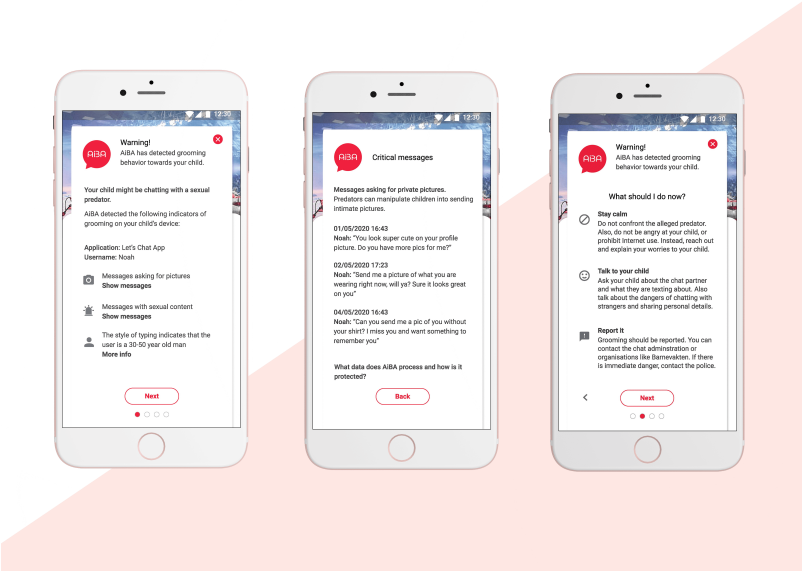


Figure 18: Three exemplary screens of the prototype for parents

accessible whenever the audience needs it. Therefore, it is also included in the previously discussed material. Important aspects in the recovery phase are providing emotional support, indicating institutions for additional help and making an appeal that grooming should be reported, even if no sexual harassment has happened. The same rules regarding the structure, wording and design of these messages apply as described in the Preparedness stage. They are kept as short as possible and are written in a friendly, caring tone. Bright colours and an illustration help to structure the text into easily readable chunks, so that the children's motivation to read it is increased. It is essential to make them understand that no form of sexual solicitation directed at them is acceptable and that it is never their fault. If they intend to continue the conversation after the warning, they have to pay additional attention and end the chat as soon as they feel uncomfortable and report the chat partner to the chat administration. Furthermore, the importance of real-life relationships needs to be emphasised. Parents, teachers, friends and classmates can be trusted adults to speak to and process experiences. Institutions that offer (anonymous) help in Norway are the project "Kors på Halsen" by the Red Cross, "Barnevakten", "Alarmtelefonen for barn og unge" and the police. The complete message to the children reads as follows, and the design can be seen in figure 19 or found in the appendix as a link to a prototype (8.7):

> Hei! How are you doing?
> AiBA sent you a warning about grooming not long ago. We just want to check in that you are ok and let you know that you can get help if you need.
> Grooming is not ok and you should always report if someone approaches you inappropriately. That can mean sending you sexual messages, asking you for private pictures, video chat or a

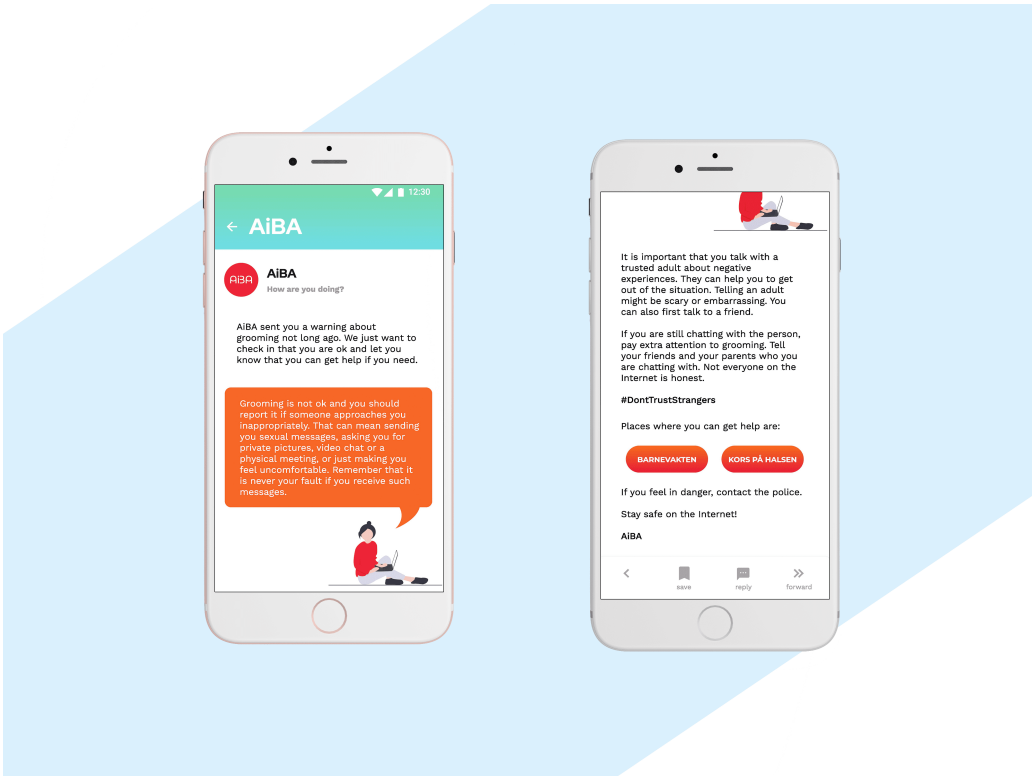


Figure 19: Recovery message sent to children

physical meeting, or just making you feel uncomfortable. Remember that it is never your fault if you receive such messages. Unfortunately, it happens to many kids - on average, 1 out of 4 teenagers receives unwanted sexual messages on the Internet. So remember, you are not alone and we are here to help you.
It is important that you talk with a trusted adult about negative experiences. They can help you to get out of the situation. Telling an adult might be scary or embarrassing. You can also first talk to a friend.
If you are still chatting with the person, pay extra attention to grooming. Tell your friends and your parents who you are chatting with. Not everyone on the Internet is honest. #DontTrustStrangers
Places where you can get help are: Barnevakten (link) and Kors på Halsen (link). If you feel in danger, contact the police. Stay safe on the Internet!

In the Recovery phase, parents need to be reminded to pay extra attention to their child and receive information on how to recognise if a child is groomed by a predator. In long term grooming cases, it can be hard for the child to let go of the "relationship". Strengthening family relations should be a priority, as well as open communication about online behavior and security. Parents can establish guidelines together with the child about information that can be shared online and platforms that can be used. It is important to conduct this in a dialogue with the child so that

the child does not take the guidelines as a punishment for its behavior. The parents are given an example of a real case where grooming resulted in the murder of a 15-year old girl so that they can discuss a worst case scenario with their children if deemed appropriate. A link to the Youtube video by the police department of Leicestershire (Leicestershire 2017) will open when clicking on the corresponding button. The video is very powerful and is likely to appeal to the parents' emotions. If parents want to seek additional help, they can be directed to relevant institutions to receive advice on how to address topics such as sexual harassment and Internet safety. The Recovery phase can also act as a reminder to continuously pay attention to signs of grooming and the children's online behavior. Therefore, indicators to detect that a child is groomed are repeated once more. Overall, it needs to be ensured that both children and parents are not left alone. The message directed at the parents is more detailed and text-heavy to convey all relevant information. The text has been broken down into logical chunks, and illustrations and colours are used to make the text more readable and the overall experience more enjoyable. The complete message to the parents reads as follows, and the design can be seen in figure 20 or found in the appendix as a link to a prototype (8.8):

> AiBA - Grooming and online safety
> You receive this message because AiBA has recently detected potential grooming attempts on your child. We want to check in that you and your child are ok and let you know that you can get help if you need.
> We recommend that you talk to your child about the chat and discuss online safety together. You should give your child clear guidelines as to which platforms it is allowed to use, what information it can share and who it can chat with. Seek an open discussion with your child and explain your reasons so that it does not feel monitored or punished. You can tell them about the dangers of sharing personal details with people they don't know and the dangers of meeting up in real life with people they only know online. Discuss real stories like 'Kayleigh's Love story' - which resulted in the murder of a 15-year old - where appropriate (link).
> You should also watch out for signs of grooming. Ask your child about its online activities and chat partners if:
>
> - Your child is suddenly very secretive about chat partners or spends significantly more time online
> - Your child neglects real life friendships
> - Your child seems stressed or depressed
> - Your child receives inexplicable gifts and is secretive about their origin
> - Your child suddenly develops sexualised language or behavior that is inappropriate for its age
>
> If your child is reluctant to speak to you or you still feel worried, discuss the topic with their friends, teachers or someone that might be able to tell you.
> If your child was groomed or sexually harassed, it is important that you report the incident. First, you should contact the chat administration and report the user. It is important that you do not confront the alleged groomer yourself as this might influence further investigations. You can also report grooming at childcare institutions. You will be contacted by a child protection advisor regarding the details of the incident. If a crime has been committed, safety professionals will

investigate who was involved and bring them to justice.
Places where you can get help and additional information are: Barnevakt, Kors på Halsen and NSPCC. If your child (or any other child) is in immediate danger, you should call the police.
We hope that you and your child are safe. We cannot emphasise enough the importance of an open and trusting relationship. Encourage your child to share negative experiences with you and always listen carefully.

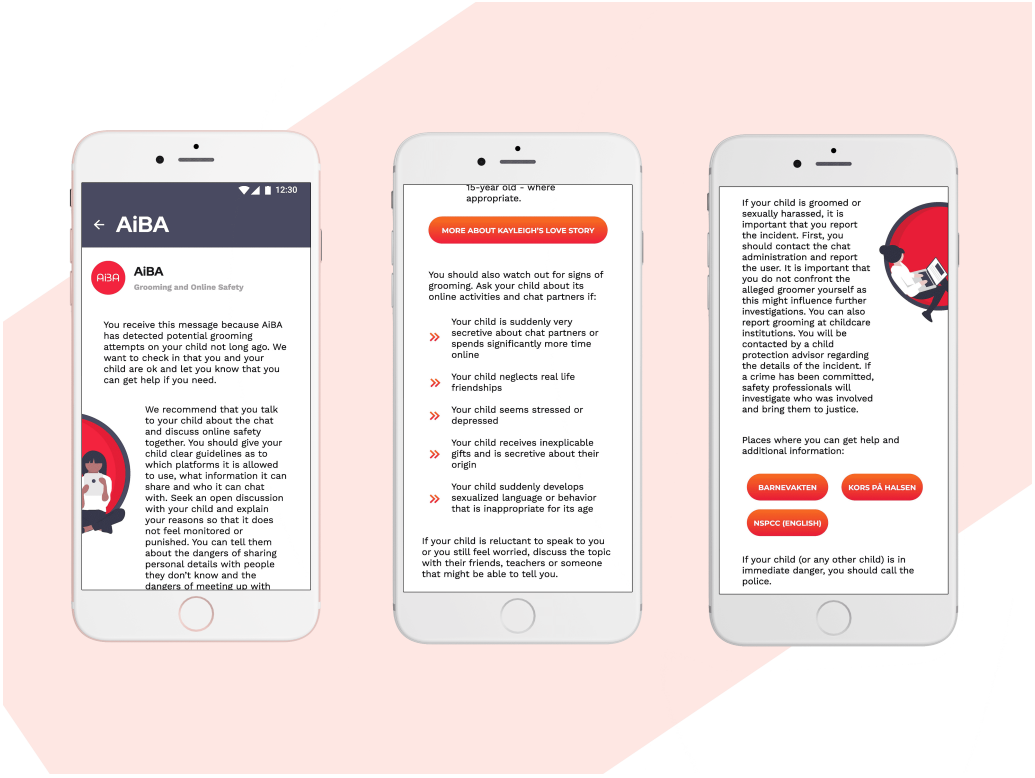


Figure 20: Recovery message sent to parents

4.4.4 Summary of Results

To summarize the communication strategy, figure 21 has been created to illustrate the elements of each communication stage. In the Preparedness stage, the goal is to raise awareness and caution, with the ultimate goal to ensure autonomy and safety of children in chat environments. Target-group oriented messages are used to reach that goal, including the choice of appropriate communication channels and messengers. Acknowledging barriers and challenges such as risk-seeking behavior and lack of knowledge contributes to the creation of a flexible strategy. The Response phase consists of a warning that is sent by AiBA to the child and the parents. The content and design is adapted to the audience so that they receive the information they need to make an informed

decision about how to react to the risk. Lastly, the Recovery stage provides additional support and information to children and parents. This stage is essential in order to ensure continuous attention to the risk. The communication materials have been created in English for this project, however, taking into account that the target audience's native language is Norwegian, the communication efforts should be published in that language as well.

4.5 Evaluations

4.5.1 Children

The evaluations were conducted at Blomhaug Barneskolen and included five groups consisting of three students each, so feedback was gathered from 15 pupils in total. Conducting the evaluations in small groups aimed at making the children feel more comfortable and to encourage them to discuss the questions with each other. It was decided to limit the number of groups to 5 since the answers and insights given by the children were repeating at that point. This issue is also addressed by usability expert Jakob Nielsen who therefore recommends user tests with 5 participants (or groups) for the greatest benefit-cost ratio (Nielsen 2012). He argues that more participants do not reveal more weaknesses of a design since the number of new insights significantly drops after the fifth participant, while the main issues are constantly repeated. The children were given a short introduction to what the evaluation will include, stressing that they cannot give any wrong answers and that their opinions are highly appreciated.

Starting with the social media advertisements, the children were shown each of the designs for 7 seconds, the average time of an advertisement on Snapchat. Following the evaluation guide, they were then asked to share their opinions and feelings regarding the designs. When being asked if they would pay attention to the ad if it appeared on their Snapchat, the majority said that they would read it. The reasons for this were diverse, some saying that it "looks cool" or "interesting", others saying that it is an "important" or "serious" topic. Some children, however, said that they would only pay attention to it if they had nothing else to do or if they were "just browsing" through social media. One child made an interesting point by saying that he would probably click the ad away on Snapchat, but pay more attention to it on Instagram. The reason for this is that advertisement on Instagram is less intrusive than on Snapchat. To increase the chances that the advertisement is perceived, one could consider to use animated content instead of a static image, since motion attracts more attention. When asked how the ad makes the children feel, a common answer was that it evokes a "sightly worried" or "bad" feeling. It also reminded the children of the dangers and that one "should follow the rules" and not chat with strangers. They said that the information is helpful to avoid dangerous situations and to remind them "not to do something dumb". It was also pointed out that the ads give courage to block strangers or talk to someone about bad experiences. Therefore, it can be assumed that the advertisements have achieved the desired effect; making the children aware of the risk of online predators and keeping them on their toes to watch out for themselves. None of the children said that they would share the advertisement online, for example on their personal account, because they do not like sharing such serious things, or simply think it would be

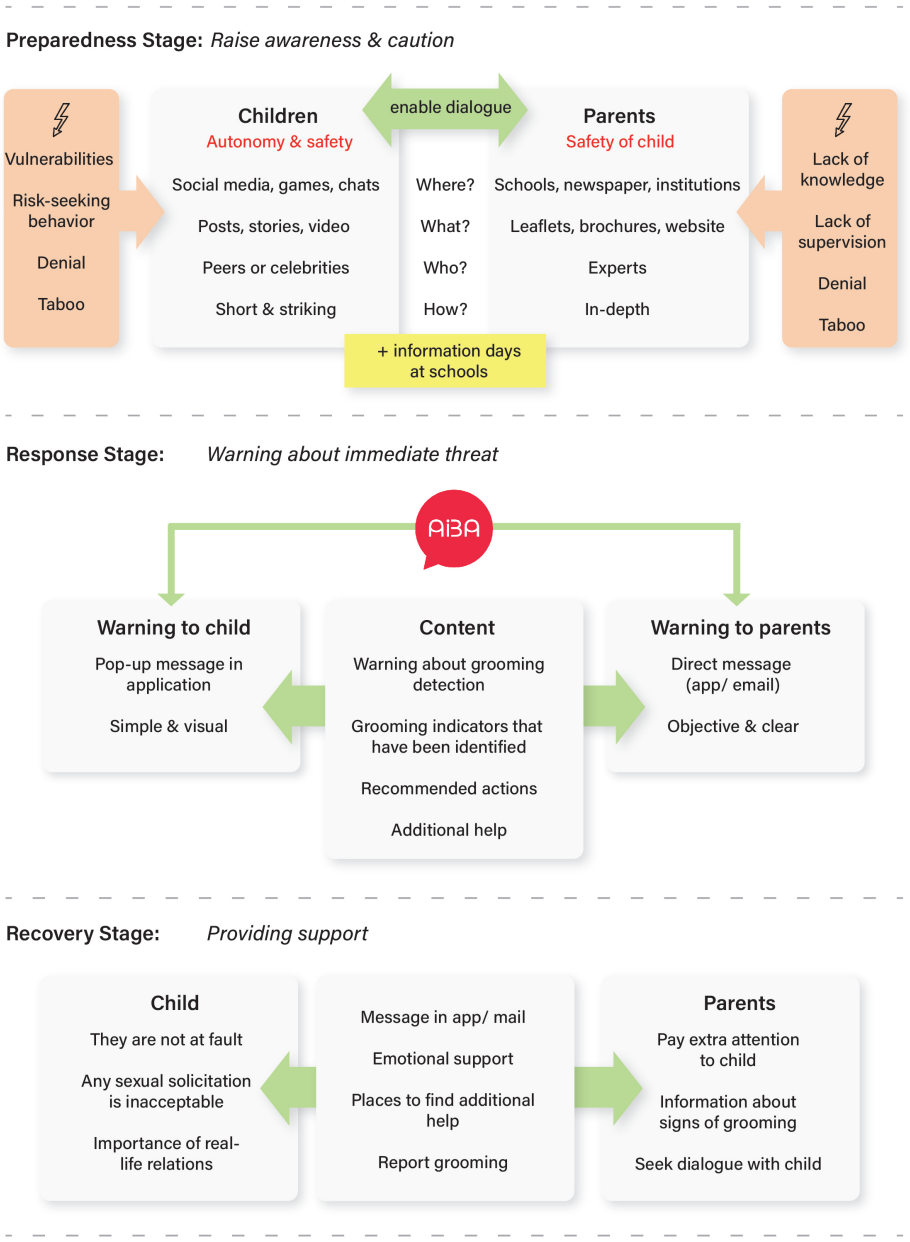


Figure 21: Overview of the risk communication strategy

"weird". This shows that in order to gain reach or (in the best case) to go viral, the advertisement needs to appeal more to the target audience. However, the children said that they would talk to their friends and parents about the ads, especially if they see it several times. That shows that the children do grasp the importance of the topic and that they are interested in discussing it. Asking them to summarise the message of the advertisement in their own words was a challenge for some pupils. Those who shared their view on it said that it "Tells you to stay away from strangers", "Block bad people", "Helps you to stay safe in chats" and that it "protects children". It is understandable that some children were struggling with that task since they have only seen the ads once and for a very short time. However, it is important that the message of an advertisement is understood within a few seconds. Therefore, the messages could be improved by making them even shorter and on point, or simultaneously increasing the text size so that they can be read faster.

The children then went through the clickable warning prototype together with the researcher. Afterwards, they said that the warning made them feel insecure or even scared at first, because it made them aware that they could be in a dangerous situation. However, following the advice, they said that it made them feel safe and protected, because they knew what to do next. Some children said that they gained confidence to tell the other person to stop texting or block them. Several times, it was pointed out that they feel like "someone cares about me and is there to protect me". However, one of the pupils mentioned that it is also a bit "creepy" that AiBA knows what they write and tells them what to do based on that. It is important to heed these critical thoughts and make the process of how AiBA assesses the risk level transparent so that it is comprehensible how one's data is used. The children understood the content of the warning very well and they were able to comprehend that it will be send in a situation when the systems detects danger ("someone is being bad", "you are contacted by a predator") and that it is there to protect them ("It keeps you safe", "It reminds you not to send pictures to someone"). However, it was noticed that the children were not familiar with the term "grooming". Since the very first interaction with the warning says "Grooming behavior has been detected", it should be considered to use a different term. Using specialised vocabulary decreases understandability and makes it less likely that the warning will be read with full attention. Alternative options could be: "AiBA has detected harmful behavior" or, more directly, "AiBA suspects that you are chatting with a sexual predator". Imagining being in such a situation, the children predominantly rate the warning as very helpful. They were most convinced by the possibility to indicate the age of the chat partner (based on stylometry and keystroke dynamics), because it is easy to lie about that in a chat. At this point, one of the children told about a friend being in a similar situation when a stranger was texting increasingly inappropriate messages. The pupil said that receiving such advice would have been helpful in that situation, however, it is much harder to follow the advice in real life than in a fictional scenario. This shows the importance of encouraging the children to stand up for themselves and seeking help, and that the current prototype succeeds in providing helpful information. The children also said that they trusted the warning, even though some said that they are a bit sceptical about the accuracy of the risk assessment. However, there was a consensus that they trust AiBA more than they would trust a stranger. Discussing what they would do after receiving that warning, many of the children would block the chat partner and report the

incident if they felt seriously bothered. Many pointed out that they would talk to their parents about it, which constitutes another success considering that another goal of AiBA is to increase communication about online security in families. In one group, there was a discussion if telling their parents would make them overprotective and result in limited Internet access for the children. This shows that the communication materials for the parents need to stress that the children need to maintain a certain level of autonomy and that monitoring them is not an appropriate reaction to the risk. The children agreed that the warning makes them think about the subject and they would reflect on the messages they received from the chat partner. They also pointed out that it reminded them to be more careful on the web, and that they should not send pictures of themselves. One child summarised it as a reminder of "not doing something dumb". While there were quite many children showing risk-seeking behavior during the focus groups, there was only one child who would still "troll" the alleged predator after reading the warning and advice. This can be an indicator that giving clear instructions decreases the chances that children engage in risky behavior.

Lastly, the children looked at the recovery message. They all agreed that it made them feel safer and protected. They appreciated that AiBA is catching up on them and gives them additional information. Again, they said that it feels like someone cares about them and protects them, and that they are "not alone". This message gives another push to report inappropriate messages and provides the courage to talk about the subject. Since the message felt important and serious, most children said that they would read the whole message also if they would receive it in real life, although it can be assumed that not all would actually do that. This is even more relevant in the event of multiple warnings being sent, since it can be assumed that the perceived urgency and therefore the children's attention decreases with each incident. To counteract this issue, dynamic messages can be developed that are tailored to the kind of incident or grooming behavior that the child experienced. Some children pointed out that the message could also use a few more pictures to make it more interesting. Nevertheless, the children felt that the information is very helpful and easy to understand. The advice is easy to follow and the children knew what to do next. They said that it made them feel more suspicious towards strangers on the Internet and that it is important to talk about the risks with someone they trust.

The evaluation concluded with asking the children how they rate the risk of chatting with someone they do not know. The predominant opinion was that chatting with strangers is dangerous and that they would not feel safe when a stranger contacted them. They understood that it is easy to pretend to be someone else on the Internet and that predators can be manipulative. Nonetheless, the children who regularly spend time playing online games said that it can also be a good way to get to know people, but they admitted that one needs to be very careful and not share private information. One child said that she once texted with a stranger and told a lot about herself, including where she lived and what school she visited. She now regrets having shared so much, but also admits that she learnt from it.

4.5.2 Experts

The expert evaluations were conducted through an online form that was sent to professionals working in Interaction Design or related fields for at least one year. Eight experts evaluated the communication efforts aimed at parents in accordance to design principles and heuristics. The professional experience ranged from one year to 25 years in the industry, and the professions included UX designers, interaction designers, digital product designers, an art director and a communication designer. This mixture of creative professions ensures a profound evaluation of the communication materials, since it includes the expertise of each creative field. To quickly gain an overview of the experts previous knowledge of grooming, they were asked if they had heard the term before in the context of sexual harassment. Only one out of the eight experts was familiar with the term, the rest did not possess any previous knowledge of the subject. This is an important factor for evaluating the understandability of the materials. Furthermore, only one of the experts stated to have children. Therefore, it has to be remembered that the majority of the experts is not part of the actual target group. While this might influence the level of identification with the subject and its relevance, the designs can still be evaluated according to design standards and guidelines.

The first communication material that was evaluated was the information leaflet. It was assessed regarding to how well it grabs the viewers attention, its understandability, relevance and helpfulness, on a scale from 1 to 5. All four characteristics received high ratings between 4 and 5, showing that the leaflet succeeds in these categories. However, two experts were neutral regarding how well it grabs the viewers attention and assigned a 3. This indicates that the leaflet needs to stand out more. Some experts added a comment to this issue, pointing out that the visual design should be pushed even further, using more emotional pictures and illustrations that emphasise the severity of the situation. Also, it was suggested to include some sorts of numbers or statistics (e.g. about number of cases or reports) beside the content as they draw in people's attention. The high rating of understandability is backed up by asking the experts to summarise the content in their own words. All answers were very good representations of the subject, for example: "*That parents should talk to their children about the dangers of chatting with strangers and to be aware of grooming signs*", "*Be aware of your child's internet usage, and maintain a trusting and safe environment*" and "*Grooming is a hidden danger to your children. You can protect them by contacting the trustworthy sources and using AiBA to prevent grooming from happening*". All experts agree that this message is highly relevant and should be communicated to the parents. It was further mentioned that the leaflet gives a good overview and initial information about the subject, but that is could go a bit more into detail at some points (e.g. what happens after an incident has been reported). While the brochure is well structured, it was argued that "*it could be a bit more "scary". The information is very objective, which is good, but it does not feel like a real threat.*". Also, it was mentioned that the brochure could present the perspective and dangers for both genders more directly, as well as going further into differences for different age groups. Comments regarding the visual language included that the brochure is clearly designed and looks very professional, but that the visual language mainly has a "*dark, threatening or unknown*" feeling to it. To work out the security and safety character even

more, it was suggested to include visuals like digital devices, human hands or cuddly toys. Also, to increase the identification with the personal stories it was suggested to use pictures instead of illustrations. Lastly, the offers for additional help should be presented more dominantly since they are a valuable source of information for the parents.

The next part of the evaluation concentrated on the warning that AiBA sends to the parents once it detects predatory behavior in a chat. The experts assessed the clickable prototype regarding the level of safety that it evokes,its urgency, understandability, helpfulness and trustworthiness. Interestingly, there was no consensus over the feeling of safety that is evoked by the warning. While three of the experts stated that they feel "rather safe" or neutral when viewing the warning, the majority stated a "rather insecure" or even "very insecure" feeling. Although it is understandable that receiving a warning about a sexual predator contacting one's child is very upsetting, the recipient should only feel insecure to the extent that the urgency of the situation is understood so that preventive measures are taken. It should therefore be considered to increase the feeling of safety even more, e.g. by more sympathetic wording or soothing visual design. Simultaneously, the experts collectively rated the perceived urgency as "high" or "very high", showing that the warning succeeds in conveying the seriousness of the situation. It therefore needs to be balanced carefully between evoking a feeling of safety and maintaining a sense of urgency. Understandability, helpfulness and trustworthiness of the warning have all been rated as "high" or "very high", indicating that the warning succeeds in these aspects. This can also be seen when evaluating how the experts would react after receiving such a warning. All of them said that they would talk to their child after receiving the warning, which is highly recommended. For example, the experts say:

> "I would probably give myself a few minutes to digest the information and consider how to start talking to my child. Then I would ask my child to have a private conversation in a familiar place."
>
> "I would follow the advice of the app. Talk to my child about chatting, but not in the sense that I monitor the behavior."
>
> "Talking to my child about the chat and who she is chatting with. Explaining that texting with strangers can be dangerous."

Additional comments to the warning included suggestions to improve the visual language. While it was mentioned several times that the design is very focused and well structured, it was pointed out that some interactions could be designed more clearly, like changing the generic "Next" button to a more specific "What should I do?". Also, several experts pointed out to make the close button less obvious since the warning is very important and should not be closed light-heartedly. One critical remark included that such a warning might create "helicopter parents" and can lead to feelings that exacerbate the issue and reduce a trusting environment. This emphasises the importance of clearly communicating that AiBA is not a tool for monitoring children's behavior, but rather an extra layer of security.

After this general assessment of the warning, the experts were provided with guiding questions to perform a heuristic evaluation. They all agreed that the used language and terms are very understandable, even though most experts were not native English speakers. On that note it was pointed

out that the main target group is Norwegian parents and that the warning should therefore be in Norwegian or offer a way to select a language. The experts also rated the experience while navigating as very pleasant: "Clear step by step instructions. Going back and forth was easy. All in all very self-contained.". The experts were taking into account that it is likely that panic occurs when a parent receives such a warning and that it is therefore very appropriate that the information is kept short and on point. It was positively remarked that the structure accompanies the information needs by first stating the alleged problem, then offering insights in the data that led to the assumptions so that the viewer can make up his own mind. The viewer is then led through different steps, describing recommended actions and receiving additional information to get a hold of the situation. Most criticism was pointed towards the "Next" buttons that are used to navigate from one screen to the next. As described earlier, the label should be changed to "What should I do?" so that it is clear that more crucial information is following. Also, it was suggested to offer more ways to navigate, for example arrows or supporting swipe gestures. The level of control while viewing the warning was also rated as very high since all instructions were very clear and straightforward. Also, all actions worked as expected. However, it was mentioned several times that the warning cannot give a guarantee that the child is protected and that the actual threat is therefore not completely under control. Two experts remarked that they would have liked additional help from the system regarding approaches to have a conversation with the child about that subject. While this information need is filled in the next communication effort (the recovery message), it can be considered to include it in the warning message as well, since parents will be eager to speak to their children and require all relevant information in one place. The consistency in the visual language was rated as very high, uniform and pleasant. However, it was pointed out that the colour scheme does not go completely in line with the leaflet which uses more purple than red colours. To achieve a consistent corporate design, this needs to be improved by deciding on one colour scheme. Regarding the clarity of interaction elements such as buttons and links, the general opinion was that they predominantly are clear, except for the buttons leading to more information about the data that the warning is based on. Instead of just using bold text, the experts recommended to add red colour to it as a first step or using a conventional button shape. Also, the close buttons could be coloured grey instead of red so that they draw less attention. The user feedback to performed actions is satisfying for a prototype, but it was suggested to improve it in a later stage of the project, e.g. by adding hover and pressed states, animations, or auditory and tactile feedback. The experts agree that the warning concentrates on relevant information and is very focused. However, it was also remarked that a parent in such a situation will be quite stressed and might find the amount of information still overwhelming. Therefore, it could be considered to reduce the density of information and spread it over several pages. The experts had a variety of additional comments at the end of this section. It was pointed out that the choice of the colour red could be revised since it might be too alarming in a situation where a parent needs to be calm and focused. For this decision, it has to be evaluated how the feeling of safety can be balanced with an appropriate feeling of urgency. Another expert suggested to add contact details to the institutions that offer additional help so that the user can access them directly without having to search for their websites. Furthermore, includ-

ing tips and age-appropriate approaches to having a conversation with the child about this subject was requested by two of the experts.

Lastly, the experts were asked to evaluate the recovery message that is sent after the warning. Again, they were asked to assess the feeling of safety, the understandability and helpfulness of the message. This time, they agreed that the message makes them feel "safe" or even "very safe". This might be due to the less alarming character of the message and the overall lower risk perception at that point. Simultaneously, the experts rate understandability and helpfulness as "high" or "very high", again proving that the communication materials are strong in that aspect and manage to convey important information in an easy way. The proposed reactions to the message show that the key points were understood and that the recommended actions are applied:

> "If I haven't already, I would talk to my child about grooming. Maybe watch the video together (depends on the child). If I have the feeling that something is wrong I would have a more serious conversation."
>
> "If I had not talked to my child yet, I would plan when I would do so, and even if I had talked to them already, I would sit down with them and ask them how they feel about the situation and ask if they want to hear about how others have been in a similar situation."

However, one expert pointed out that the information in the recovery mail should be sent immediately after the warning has been received ("*Why need to wait for one day to send this email to the user? If grooming happens to my child, I expect guidelines, sharing stories, advice to come at once.*"). At the same time, another expert saw the purpose of the message as "*a reminder and as a signal of interest for the well-being of my child.*". For the latter, sending the message one day after the warning seems to be an appropriate time, while the first would need the information earlier. This indicates that the purpose of the message has to be worked out more clearly. While the intended purpose was indeed more of a reminder, it is equally important to provide advice on how to talk to children about the subject at an earlier time since communication is the key aspect for establishing a trusting environment. It could therefore be considered to include more information in the warning itself and clearly mark the recovery message as a reminder. Also, two experts commented that the message is rather long and that it might be difficult to encourage the recipients to read all the way to the end. Although, it was pointed out that the text is easy to read and that the illustrations make the design lighter which in turn increases the chances that the text is read completely. Also, the short movie "Kayleigh's Love Story" was described as very powerful and touching so that the parental worry and protectiveness is more legitimate. The experts further commented that the information that was provided in the leaflet can be helpful in all three situations and that it should be made accessible through a link to the PDF in the warning and the recovery message. The insights regarding the design gained from the expert's feedback are also applicable to the prototype for the children's design since it follows the same structure and visual design.

To conclude the evaluation, the experts were asked to rate the severity of the risk of online grooming. Seven out of eight experts perceived the risk as "high" or "very high". This clearly shows the relevance of the subject and the need to educate people about it. The experts reason that the

anonymity of the Internet in combination with less social contacts abets online grooming. Also, children can be naive and vulnerable since they might not know how to interpret certain signs of dishonesty and trickery. One expert pointed out that education is particularly important for parents who did not grow up with the Internet since they might not be as aware of the dangers and possibilities for predators. There was one expert who rated the risk of online grooming as "low", arguing that while it might happen more often than one might think, it comes down to only "a few perpetrators who do it a lot". To convince people of the severity of the problem, one could include statistics in the information materials that show the reach of the problem and the disturbing amount of cases. Another expert wrote:

> "I do not know any statistics (maybe that would be something to include?), but I guess that it happens more often than you would think, but often goes undetected or unreported."

Also, they were asked to share their opinion about AiBA and its usefulness. Here, they agreed that AiBA is "very useful" (seven ratings) or "useful" (one rating). The experts appreciated the extra security measures that this technology offers, especially for children who are not familiar with the dangers that come with the Internet. However, the experts also see the issues that might come with a system like AiBA, mainly "*panic or extreme surveillance of the child which can lead to the child blocking himself or looking for risks out of defiance*". The critical opinions justify the need to design a risk communication strategy that teaches children and parents how to treat the risk correctly.

4.5.3 Summary of Results

The two evaluation methods show that the communication materials provide relevant and understandable information. The materials for the Preparedness stage successfully increased awareness about the risk of online grooming. Both the children and the expert group stated that the instructions and advice given in the Response stage are helpful in an immediate situation of need. Furthermore, the materials build trust and provide a feeling of safety which is particularly important in an upsetting situation like this. The advice and the reminders given in the Recovery stage were appreciated, creating a feeling of not being alone with the situation.

For the children's designs, it was found that the term "grooming" is too specific and is not recognised by most children. Therefore, it should be replaced with easier language. Also, the importance of providing transparency regarding how AiBA is operating was highlighted as it directly contributes to how much the system is trusted. The main feedback from the experts suggested an improvement of some interaction elements to make the user experience more intuitive. Furthermore, the visual language should be revised to better balance the feeling of safety and perceived urgency. While it is important that parents understand the severity of the situation, they should feel safe for their child and in control to avoid panic. Overall, AiBA was assessed as a valuable addition to children's safety on the Internet and all participants acknowledged the relevance of education on grooming and online safety.

5 Discussion

The literature review in Chapter 2, the practical application of research methods and the design of communication efforts in Chapter 4 have contributed to answering the research questions of this thesis. The first part of the overarching question, "Can a communication strategy be built for warning against sexual online predators?", has been answered with the delivery of the practical part of this thesis. It shows that target audience-oriented communication efforts can be used to warn against sexual predators. However, the second part, "Does it increase awareness of grooming strategies and caution when conversing in chats?", cannot be answered with certainty because no long term results could be recorded within the scope of this thesis. Although, it became clear during the user research phase that addressing the topic in a school environment and discussing online safety with children increases their (short term) awareness of the risk of sexual predators on the web. Also, even though the children did not recall the term "grooming", they were eager to discuss online safety during the evaluation phase and remembered the key aspects of the seminar days. Thus, it can carefully be assumed that some long term awareness can be achieved.

It has been found that parents also see the relevance of the topic, but that there are huge differences in the knowledge level and assessment of the risk level, resulting in differing information needs. Therefore, the sub-question "How can awareness of sexual predators be increased?" was answered extensively, combining insights of the literature review about grooming and risk communication with practical experiences working with the target audiences. Short term results regarding the question "How does awareness-building influence chat behavior?" could be seen during the focus groups with the children when comparing the BPG with the APG. Having discussed online safety and sexual predators, the children behaved more careful and suspected dishonest intentions earlier. Even though the thesis cannot provide long term results for this issue, it can be assumed that a good understanding of online safety and regularly being exposed to information about it will also increase awareness and cautious chat behavior in the long term. From the data that was obtained during the research phase, it was possible to extract detailed information needs of the audiences for each communication stage, thus answering the sub-question "What information do the different audiences need at each stage of the communication?". The question "What emotional responses can be triggered by such a sensitive topic?" was answered as a byproduct of the user research phase. During the focus groups, some children - especially girls - pointed out that they would be scared if they received such messages in real life, or at least feel uncomfortable. On the other hand, some children also reacted with humour to the topic, bringing a laugh to their classmates with funny comments, although this could also be due to peer pressure or an indicator of risk-seeking behavior. The emotional responses of the parents were much clearer; the topic made them worry about the safety of their own children and resulted in the wish to protect them. There-

fore, it was important to investigate ways to communicate the topic without inducing irrational responses ("How can the risks be communicated without inducing irrational reactions?"). The basis for this was extracted from the literature about grooming and risk communication and applied in the communication efforts by presenting objective facts, giving clear instructions and advice, as well as providing emotional support and additional sources of information. The question "What ethical and legal issues arise from this topic?" has been answered in the literature review about grooming and more detailed in Chapter 3.6, particularly emphasising the importance of ensuring the physical and mental well-being of all participants of the study. Lastly, the designed communication strategy answers the question "How can the findings be implemented in a project such as the AiBA project?". Although the proposed design is just one of several potential implementations, it shows the benefits of thorough user research and an interdisciplinary approach to solving such a complex challenge. However, the design needs to be checked for technical feasibility that takes privacy and data protection issues into account.

5.1 Focus Groups and Surveys

The observations made during the focus groups with schoolchildren and the results of the data analysis imply that education about online security and grooming has an influence on the children's chat behavior (Raffel et al. 2020). It was observed that they became more aware of the risks related to texting with strangers and thus acted more careful after participating in a presentation about online safety. This goes in line with the recommendations by Winters & Jeglic (2017) who propose to raise awareness through education by schools. It was striking to see how extensively the children are using the web and some applications in particular, justifying the relevance of this project. The children mentioned a large variety of applications that they use, some of which have been unknown to the researcher before. That emphasises the fast-paced nature of the communication environment that the children are exposed to which also constantly offers new channels for predators to access victims. Furthermore, reviewing the amount of reported negative experiences and exposure to sexual content by Smahel et al. (2020), the need for education becomes indisputable. Also, the children have shown high interest in the seminar days which suggests that they would eagerly receive additional education measures. Although it was not among the most popular online activities, the majority of the children said that they have indeed chatted with people they have never met in real life. Even though none of the children mentioned any negative experiences in this context, it shows that they are regularly exposed to the risk. The differences in their reactions to the prompted chat messages highlights the children's individuality and confirms the suitability of education about grooming at school, since the teachers are familiar with the children and their characters. The discussions that emerged in all groups (BPG and APG) about whether a message is written by a child or an adult illustrate the difficulty to identify the early stages of grooming, although most children immediately marked more explicit messages as inappropriate. The chosen usernames often gave away some personal information, even though the children were not aware of it. This suggests that education about safe online behavior should also include advice on choosing a safe username for a profile. In accordance with increased caution and scepticism, the education

also resulted in a higher appreciation of the concept behind AiBA. One possible way to explain this is the increased awareness of the risk and a resulting need for security which can be addressed by AiBA. The focus groups have shown popular sites and platforms that can be contacted as potential partners for implementing AiBA.

Including parents in the communication strategy increases the reach and consistency of the education effort. The surveys have shown that there are immense differences in the parents knowledge about the topic. As the children's main role models and close confidants, it is essential that parents are well aware of grooming, including how to prevent and detect it. Again, this is supported by Winters & Jeglic (2017) who recommend educating parents on a community level, for example by handing out leaflets in frequented places. It became apparent that an information source is needed that bundles all relevant information in one place, since most parents were aware of parts of the risk, but were lacking a holistic picture. Those parents who had a very good understanding of the risk pointed out that they had received relevant training related to their professions. Generally speaking, the importance of the subject has been acknowledged by all parents which suggests a willingness to receive education. Online safety is already addressed in most families, even though to a varying degree. The parents' interest in learning how to talk to their children about such sensitive subjects indicates that they are open to discuss the subject more extensively with their children as well. This forms a solid basis for a communication strategy and ensures the parents' initial interest in the content. The confidence of some parents about being able to identify grooming behavior in chats goes in line with the findings by Winters & Jeglic (2016) who found that people generally overestimate their ability of identifying grooming. The concept of the AiBA application was positively received as it forms an additional layer of security. However, it has been viewed with scepticism regarding its perceived surveillance character and potential data protection issues. This offers valuable insights for the marketing of AiBA, since these concerns need to be addressed for the parents to trust the system. However, it has to be said that the insights of this survey cannot be generalised as only a limited number of responses has been recorded that is not representative for the whole target group.

5.2 Risk Assessment and Mental Model

By formulating information needs and extracting the key messages for the three phases of risk communication, it was possible to differentiate the information distribution so that the audience is provided with relevant information when it is needed. Starting with a strategic risk assessment, applying a selected set of gamestorming methods allowed for a creative take on the subject. The gamestorming techniques by Gray et al. (2010) are well suited to explore different alternatives and facets of a problem and lead to its solution(s) through serious games. For example, conducting the "5 Whys" revealed underlying reasons and motivations for the communication effort and the "4 Cs" resulted in a detailed description of the risk. This approach also suits a user-centered design process very well. For example, the reason for communicating the risk of grooming to children - that they just "want to play online games, chat or talk without worry" - could also be described as naivety or carelessness, however, it would be a less emphatic description that does not enable the researcher

to fully identify with the target audience. Furthermore, the gamestorming techniques are also an interdisciplinary approach. For instance, the "Elevator Pitch" has its origins in economics and product development, but it is an excellent method to structure user needs and resulting benefits that the communication strategy and AiBA can offer. While the results of these methods are not absolute and can vary depending on the questions asked, they offer a flexible tool to think independently and explore possibilities. It can be argued that they are non-scientific methods as different researchers will arrive at different results when repeating the methods, although this also constitutes their greatest advantage since their goal is to find a variety of approaches to a problem that do not necessarily need to follow conventions. The results of the applied gamestorming methods condensed the relevant information about the risk, its underlying reasons, risk factors and affected population so that they can be directly translated into requirements for the communication strategy.

Similarly, the mental model approach evaluated the knowledge about grooming of the parents who took part in the survey, and compared it to an expert model. It is for good reason that this is a standard method in risk communication as it has two main advantages. First, it summarises the expert knowledge on the subject and puts the information bits into relation. Secondly, it is very effective for identifying knowledge gaps and misconceptions. When reviewing the results, one can see that the parents' model largely overlaps with the expert model. However, one has to remember that the parents' model is the cumulative result of all input given by the parents, meaning that the knowledge of each individual is not as complete as the model suggests. At the same time, the number of participants was relatively low so that no generalisation is possible. The mental model approach would therefore benefit from further investigations with more participants. Nonetheless, it served the purpose of this thesis well by establishing the basic information needs of the selected population. The data from the surveys was put into context so that the communication strategy can be tailored to the target audience, again following a user-centered design approach.

5.3 Communication Strategy and Warning Design

Based on the insights of the user research phase and the resulting implications, a communication strategy was developed that addresses schoolchildren in the 7th grade and their parents. According to common practice in risk communication, the strategy was divided in three stages. This has the advantage that the different information needs during each phase can be addressed more efficiently. Also, the phases differ in emotional involvement and thus require different forms of interaction. While emotional involvement of a parent during the Preparedness stage is probably relatively low and the main goal is to raise awareness, receiving a warning in the Response stage is likely to result in high emotional involvement since one's own child might be in danger. Then, during the Recovery stage, the immediate danger has been averted, but the parents might still be grateful for additional information and emotional support. Designing for these different contexts and information needs was the main challenge. The communication effort during the Preparedness stage includes advertisements on social media aimed at schoolchildren. This medium is believed to have the highest reach among that target audience and its efficiency is increased by integrating the messages directly in the platforms where grooming is happening. Keeping the messages short and using strong

visuals was the main focus in this phase, since the content needs to quickly grab the audience's attention and be easily understood. Although it can be argued that advertisement or sponsored content can be perceived as annoying spam, it is believed that repeated exposure to its content will result in increased awareness. Also, using a hashtag makes it more likely that the message is spread widely and referred to in other postings. As a reference, the campaign "Listen to your selfie" by the British organisation Childline was launched in 2016 (NSPCC 2016). It consists of two short videos which tell the stories of two teenagers getting caught in unhealthy relationships with people they met online, and a number of related posts on social media. The teenagers, a girl and a boy, both seem relatable and do not follow the clichee of lonely, insecure victims, showing that any child can be targeted by groomers. The goal was to raise awareness about online abuse and grooming in the UK. The campaign was relaunched in 2018 to tackle the rise of peer-on-peer sexual abuse and to educate teenagers about consent. It resulted in a huge amount of reactions and was viewed over 320k times on YouTube. Accordingly, the campaign "Careful Parents" is an awareness campaign by the Polish Safer Internet Centre that was launched in 2018 and highlights the importance of parental guidance and presence for preventing grooming and abuse (PSIC 2018). The campaign is made of an emotional video about an isolated child that finds acceptance and appreciation when chatting with a stranger on the Internet who later grooms and blackmails her. It powerfully shows how easily vulnerable children can be lured by predators. The video is complemented by a brochure, a website, several articles and classroom lessons. The two examples show how the target audiences can be reached and addressed appropriately which has been continued in this thesis' project. The brochure which is the communication effort aimed at parents during the Preparedness phase is much more in-depth than the fast-paced advertisements aimed at the children. The parents need a detailed and trustworthy information source that provides them with relevant information to keep their children safe. The content is presented objectively, however, the two short stories aim at heightening emotional involvement and increased sympathy. This is believed to hold the parents' attention as well as fulfilling their information need.

The context of the warning that is sent in the Response phase differs greatly from the Preparedness stage. The detection of grooming behavior by AiBA implies immediate danger for the child which requires the parents' attention and call to action. While extreme emotional responses such as panic should be avoided, the warning needs to create a certain level of urgency. Additionally, the information and recommendations given by the warning have to be trustworthy which is why it needs to be transparent how the system operates. The warning avoids jargon and technical terminology since the parents and children need to understand the content in a stressful and emotional situation. For the children, it is particularly important that the used language is on an age-appropriate level. The warnings concentrate on essential information and avoid clutter so that it is easy for the recipient to follow the recommendations. The applied design principles resulted in a structured design that leads the audience through the content, using colour to highlight interaction elements. Although the designs might look simple and reduced, it is argued that simplicity is an essential characteristic of a warning. By giving clear instructions, it is believed that the warnings give the audience a sense of control that is needed in such a stirring situation that can easily be emotionally

overwhelming. Feeling in control and knowing what to do next is crucial for handling the situation correctly, both for children and parents. The parents need to remain calm and enter a dialogue with the child since overly emotional responses, monitoring or punishment of the child will have negative influences on the child's behavior. The child, however, might be surprised or shocked by the presumption that the seemingly friendly chat partner is a sexual predator. It is also not unlikely that it will react with ignorance and denial, depending on how far the grooming has proceeded. Here the goal is to convince the child of the urgency and providing understandable reason why AiBA is assuming predatory behavior. Of course, it is desirable that AiBA detects the grooming attempts before a deeper bonding can happen. Sending warnings to children and parents simultaneously increases the chances that they talk about the subject, making it more likely that the children share their experiences. To conclude, one aspect that needs to be considered is the feasibility of the proposed designs. In order to justify the warning, critical messages that contain hints of grooming are displayed in the warning. However, that requires that messages are stored which goes against data protection regulations. Also, AiBA continuously monitors and adjusts the risk level until a threshold is reached that triggers the warning. The adjustments can be very detailed and based on minimal deviations that are evaluated by the algorithms so that compiling all indicators is likely to result in a long and for the user incomprehensible list. This issue needs to be investigated and addressed in cooperation with the developer team, for example by using the test data that has been collected during the seminar days at the school to develop a prototype that focuses on that problem.

Even when the immediate danger has been overcome, the Recovery phase still plays an important role. Its main goal is to sympathise with the audience and provide additional support - emotionally and professionally. The information provided in the messages is not completely new, it can be found in the information materials of the previous stages as well. However, it stresses particular topics more intensely and gives additional examples. It is believed that the advice that is given, the more sympathetic style of writing and the repeated offer to get further help encourages parents and children to discuss the matter and take it seriously. The challenge is to keep the audience's attention even though they are already familiar with the subject. The mail might be perceived as repetitive or even spam. However, it has to be considered that not all recipients have obtained the information materials from the previous communication stages and that their level of knowledge might be lower than anticipated. The messages sent in the Recovery stage are therefore another layer of educational efforts. The initial idea was to send the recovery messages one day after the warning in order to give the family time to discuss the incident and let the situation cool down. However, during the evaluation it was mentioned that sending the message right after the warning would have a greater benefit, especially for parents who are in need of more information than the warning provided. Both approaches are justifiable and have their advantages. For making an informed decision on this subject, the target audience who receives the message should be involved. It is also imaginable to solve this through a user setting so that the users can choose themselves when to receive such notifications.

5.4 Evaluations

Evaluating and refining results is an essential part of iterative and user-centered design. Likewise, in risk communication, experts highly recommend to test communication efforts before launching a campaign and monitor its performance over time (Lundgren & McMakin 2009). The chosen methods for conducting the evaluations worked very well given the circumstances. Evaluating the designs with the children in groups of three was a comfortable set-up for small discussions that revealed interesting insights in the children's perspective. The children were very open and interested in the work that has been done in the project. Therefore, a side effect of the development of this thesis has been that the pupils at Blomhaug Barneskolen have received education on online security and grooming, making them more aware of dangers and teaching them how to behave safely. Seeing the success of the seminar days on Internet security and also the discussions during the evaluation, one can assume that developing cooperations with schools appears to be an effective method for raising awareness among schoolchildren. Reviewing the results of the group discussions with the children, one can say that the evaluation phase indeed yielded meaningful insights and that the children expressed some helpful and critical thoughts. The most eye-opening finding was the realisation that the children were not as familiar with the term "grooming" as expected. It shows how easily one can falsely assume to speak the user's language when actually using jargon or expert terms. These assumptions can only be tested when directly speaking to the target audience, again highlighting the importance of evaluating the communication materials. Since it can be challenging to keep up with the fast-changing trends on social media, it was helpful to hear the children's views on the advertisements that have been developed for the Preparedness stage. While the children commented that they look "cool" and "interesting", it was found that they need to draw more attention in order to increase their reach. One possible way to realise this could be by using animations or more striking colours. It was also remarkable to observe that risk-seeking behavior decreased after the children had read the advice given in the warning. Answering inappropriate messages with humour or by being offensive was quite common during the initial focus groups in the research phase, while only one child suggested such behavior in the evaluation phase. This can be an indicator that education and precise advice on recommended reactions to such messages increases the children's confidence to draw clear boundaries, not making it necessary to evade advances through risk-seeking behavior. Generally speaking, it can be said that the communication efforts succeeded in providing understandable and helpful information. Also, they managed to convey a feeling of safety and confidence to reasonably handle the situation.

Even though the expert review has been an alternative method due to COVID-19, it provided valuable feedback on a professional level. Combining the knowledge of experts of different creative professions subjected the communication materials to a holistic and thorough examination. The UX and interaction designers provided feedback regarding the user-friendliness, the use flow and the overall experience when interacting with the materials; while the graphic designer was specialised in the visual language and the communication designer evaluated the overall communication effort. This evaluation method has shown the advantage of working in a design team with different

specialities. The only drawback was that just one of the experts had children and could therefore identify with the subject on a different level. However, the feedback often showed that the other experts were able to sympathise as well and understood a parents' needs and feelings in such a situation.

Two main findings emerged from the expert evaluation that require further discussion. Firstly, there were differing opinions among the experts regarding the density of information in the communication materials. While some appreciated that the information is focused and reduced to the essentials, other wished for more in-depth information to better equip the parents with relevant knowledge, for example including advice how to approach the subject in a child-friendly way. The underlying discussion concerns whether parents rather require an overview of the subject or detailed information. Recalling the insights from the user research phase, it is argued that the warning should be as reduced and focused as possible so that the parent is not overwhelmed by information. However, it can be argued that the information materials before and after the immediate Response stage could go further into detail. This can be realised in a way that the recipient can choose independently whether to consume more information. In the Preparedness stage, several leaflets can be produced that concentrate on different aspects of the risk. Thereby, the parents can choose to go further into detail after reading the general introductory leaflet. The same approach can be realised in the Recovery phase. While the information email should be kept short to ensure the parents' attention, information material can be linked (similar to the video "Kayleigh's Love Story") so that more in-depth information can be easily accessed if necessary.

Secondly, there was no consensus over the feeling of safety that is evoked by the warning. While "safety" is of course a very personal impression that is highly dependent on the context and individual experiences, visual design and stylistics can be used to support and increase the perceived level of safety. For example, the signal colour red has a highly alarming character while colder colours such as blue are generally perceived as more soothing. It can therefore be argued to reduce the use of red in the warning so that the recipients feel less alarmed and therefore safer. However, this is likely to also reduce the perceived urgency of the warning, and might lead to the parents not taking the warning seriously enough. It should be worked towards finding a balance between urgency and perceived safety, although the researcher argues that being overly alarmed and feeling insecure is the better alternative to not taking the risk of online predators seriously.

5.5 Limitations

As with every study, it has to be taken into account that there are limitations to the results and their implications. The most prominent limitation that has been mentioned several times before is the outbreak of the COVID-19 pandemic and its related restrictions. Although the responsible researcher has adapted the methodology so that it was still possible to gather data, the quantity - and to a certain degree also the quality - has been lower than anticipated. In addition to the seminar days conducted at Blomhaug Barneskolen, it was planned to visit two more local schools which would have resulted in almost twice as many focus groups with children. It would have been interesting to investigate differences between the schools, particularly because they represent different

social environments. The largest adaption that was made due to the pandemic was the redesign of the data collection with the parents. All existing plans for in-depth semi-structured interviews were cancelled and replaced by an online survey. This inevitably influenced the nature of the collected data. While the lack of depth was partly compensated by a higher number of participants, it would have been desirable to be able to ask follow-up questions to some answers. Although it is understandable that the parents were facing great challenges, it would have been helpful to receive a higher amount of replies to the survey. As it is now, the data cannot be generalised since it is not fully representative of the whole target group. While assumptions about that particular target group (parents living in a small Norwegian town in a rural area) can be made, more research has to be done for generalising the results to a wider degree. The same limitations apply to the evaluation of the communication strategy.

It was very unfortunate that the materials aimed at parents could not be evaluated with the target audience. While the experts were able to identify a number of relevant design and usability issues, conducting tests with parents was expected to reveal issues that are unique to the target audience (for example how well the information needs are met). However, this extraordinary situation shows the importance of being fluent in a wide variety of design methods so that one is flexible and confident enough to adjust the data collection to unexpected challenges. Despite the spontaneous adjustments, it was still possible to extract the key insights that led to a well founded communication strategy.

Furthermore, it has to be considered that the scope of a Master's thesis does not allow for the collection of long term results. The assumptions about the effectiveness and success of the communication efforts are based on the initial reactions of the target audience and the expert group. In order to draw more sophisticated conclusions, one needs to investigate how exposure to the communication materials influences chat behavior and risk awareness in the long term. For this purpose, it is essential to observe the communication materials put to action instead of making assumptions based on prototypes. Many of these limitations can be addressed and resolved in future work.

6 Conclusion and Future Work

6.1 Conclusion

While the Internet enables us to connect with people all over the world and thus created a global village, it simultaneously presents us with new challenges and dangers. Raising awareness about the risk of sexual predators that approach children online should be a central concern in today's digitised society, especially when reviewing the alarming findings of the European Grooming Report (Webster et al. 2012) and the corresponding findings of the EU Kids Online Report (Smahel et al. 2020). This thesis suggests that target group-appropriate education about the subject increases awareness and thus positively influences overall behavior and caution online. It is apparent that all involved participants see the need to protect children from sexual predators, and this thesis has proposed one possible approach. Acknowledging that a risk consists of three subsequent stages allowed for a detailed analysis of the information needs during each stage, and the design of appropriate communication efforts to provide this information. The information materials in the first stage, Preparedness, broadly educate the recipients about grooming to raise awareness and ensure a good knowledge level. As the name suggests, it prepares the audience for a situation of risk. In that case, when AiBA detects grooming behavior and sends a warning, only the most essential and relevant information is presented in precise and short instructions. The aim is to enable the recipient to take informed and conscious decisions in a stressful situation to protect them from an immediate threat. Lastly, a recovery message provides emotional and informative support so that the recipients are not left alone in such a challenging situation. This holistic approach is believed to provide children and parents with the knowledge and confidence to protect themselves and others from online grooming and sexual solicitation.

Joining the AiBA project has been a huge advantage for this thesis as it provided a tangible example for innovative prevention methods. It is hoped that establishing the information needs of parents and children in the context of grooming detection and prevention can contribute to the success of the project. Working closely with the target groups has shown that they have great interest in learning about the subject and see the importance of raising awareness about it in the general public. However, still more work needs to be put into the creation of awareness campaigns and grooming prevention technologies so that the most vulnerable members of our society can be protected from grooming and sexual solicitation.

On a methodological level, the thesis has shown that design approaches can successfully be applied to a variety of disciplines. The interdisciplinary approach combined insights from risk communication, design and IT security to gain a holistic picture of the research problem and how to solve it. In today's fast paced society and working environment, being able to adapt the methodology to different contexts is a crucial skill for every designer.

6.2 Future Work

Future work in regards to this topic should be focused on gaining long term insights about the influence of education on online safety and grooming on the behavior of children and parents. This work will help to reduce the limitations that have been mentioned in the previous chapter. It is advisable to refine the communication efforts and do additional testing with the target audience before implementing the communication strategy. Additionally, more content can be created to complement the strategy, such as a video campaign or more detailed brochures on selected topics related to the risk. The project should be monitored over a longer period so that its effectiveness can be evaluated more accurately. Feedback on the materials can be used to adapt the strategy and determine the effectiveness of each individual communication effort. Regarding the AiBA application, the designed prototype can be used as a basis for the development of an interface for the finished system. The challenge will be to implement it in different applications such as chat rooms or online games. However, since the content stays relevant regardless of the platform, it is believed that this thesis provides a solid groundwork for the design of effective warning messages within the AiBA application.

Bibliography

Adler, K., Salanterä, S. & Zumstein-Shaha, M. (2019), 'Focus group interviews in child, youth, and parent research: An integrative literature review', *International Journal of Qualitative Methods* **18**.

Arvai, J. & Rivers, L. (2014), *Effective Risk Communication*, Routledge.

Babchishin, K. M., Hanson, R. K. & Hermann, C. A. (2011), 'The characteristics of online sex offenders: A meta-analysis', *Sexual Abuse* **23**(1), 92–123.

Bartlett, J. (2018), *The People Vs Tech. How the internet is killing democracy (and how we save it)*, Ebury Publishing.

Bauer, L., Bravo-Lillo, C., Cranor, L. & Fragkaki, E. (2013), 'Warning design guidelines'. Accessed: 2019-11-07.

Baxter, K., Courage, C. & Caine, K. (2015), *Understanding Your Users: A Practical Guide to User Research Methods*, 2 edn, Morgan Kaufmann.

Bennett, N. & O'Donohue, W. (2014), 'The construct of grooming in child sexual abuse: Conceptual and measurement issues', *Journal of Child Sexual Abuse* **23**(8), 957–976.

Bingham, A., Brawley, M. & Gopinath, C. (2009), 'Designing communication strategies that work: Implementing the sim process'.

Black, P. J., Wollis, M., Woodworth, M. & Hancock, J. T. (2015), 'A linguistic analysis of grooming strategies of online child sex offenders: Implications for our understanding of predatory sexual behavior in an increasingly computer-mediated world"', *Child Abuse and Neglect* **44**, 140–149.

Boholm, A. (2019), 'Lessons of success and failure: Practicing risk communication at government agencies', *Safety Science* **118**, 158 – 167.

Briggs, P., Simon, W. T. & Simonsen, S. (2011), 'An exploratory study of internet-initiated sexual offenses and the chat room sex offender: Has the internet enabled a new typology of sex offender?', *Sexual Abuse* **23**(1), 72–91.

Burgess, A. W. & Hartman, C. R. (2018), 'On the origin of grooming', *Journal of Interpersonal Violence* **33**(1), 17–23.

Canter, D., Hughes, D. & Kirby, S. (1998), 'Paedophilia: Pathology, criminality, or both? the development of a multivariate model of offence behaviour in child sexual abuse', *The Journal of Forensic Psychiatry* **9**(3), 532–555.

Childline (n.d.), 'Online grooming', https://www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/online-grooming/. Accessed: 2020-04-12.

Clark, C. (2011), *In A Younger Voice: Doing Child-Centered Qualitative Research*, Oxford University Press.

Colton, M., Roberts, S. & Vanstone, M. (2012), 'Learning lessons from men who have sexually abused children', *Howard Journal of Criminal Justice* **55**(1), 79–93.

Conte, J. R., Wolf, S. & Smith, T. (1989), 'What sexual offenders tell us about prevention strategies', *Child Abuse and Neglect* **13**(2), 293 – 301.

Coyne, I., Hayes, E. & Gallagher, P. (2009), 'Research with hospitalized children: Ethical, methodological and organizational challenges', *Childhood* **16**(3), 413–429.

Cranor, L. F. (2008), A framework for reasoning about the human in the loop, *in* 'UPSEC'08 Proceedings of the 1st Conference on Usability, Psychology, and Security', USENIX Association, pp. 1–15.

Cranor, L. F. & Egelman, S. (2009), 'Trust me: design patterns for constructing trustworthy trust indicators'.

Craven, S., Brown, S. & Gilchrist, E. (2006), 'Sexual grooming of children: Review of literature and theoretical considerations', *Journal of Sexual Aggression* **12**, 287–299.

Daley, A. M. (2013), 'Adolescent-friendly remedies for the challenges of focus group research', *Western Journal of Nursing Research* **35**(8), 1043–1059.

Dittman, S. (2019), 'Parent alert: Is roblox safe for kids? watch out for these 4 dangers', https://www.protectyoungminds.org/2019/07/23/is-roblox-safe-for-kids-4-dangers/. Accessed: 2020-02-16.

Dozier, D., Grunig, L. & Grunig, J. (1995), *Manager's Guide to Excellence in Public Relations and Communication Management*, Lawrence Erlbaum Associates.

Egelman, S., Cranor, L. F. & Hong, J. (2008), You've been warned: An empirical study of the effectiveness of web browser phishing warnings, *in* 'Proceedings of the SIGCHI Conference on Human Factors in Computing Systems', Association for Computing Machinery, p. 1065–1074.

Elliott, M., Browne, K. & Kilcoyne, J. (1995), 'Child sexual abuse prevention: What offenders tell us', *Child Abuse and Neglect* **19**(5), 579 – 594.

Gamhewage, G. (2014), 'An introduction to risk communication', https://www.who.int/risk-communication/introduction-to-risk-communication.pdf?ua=1. Accessed: 2019-11-11.

Golding, D., Krimsky, S. & Plough, A. (1992), 'The narrative versus technical style in risk communication', *Risk Analysis* **12**(2).

Gray, D., Brown, S. & Macanufo, J. (2010), *Gamestorming: A Playbook for Innovators, Rulebreakers, and Changemakers*, O'Reilly.

IBM (2019), 'Ibm study: More than half of organizations with cybersecurity incident response plans fail to test them'. https://newsroom.ibm.com/2019-04-11-IBM-Study-More-Than-Half-of-Organizations-with-Cybersecurity-Incident-Response-Plans-Fail-to-Test-Them. Accessed: 2020-03-26.

Ivins, J. (2018), 'The hidden dangers of 'roblox' every parent should know about', https://www.websafety.com/2018/07/the-hidden-dangers-of-roblox-every-parent-should-know-about/. Accessed: 2020-02-16.

Janoske, M., Brooke, L. & Sheppard, B. (2012), 'Understanding risk communication best practices: A guide for emergency managers and communicators'.

Kasperson, R. (2014), 'Four questions for risk communication', *Journal of Risk Research* **17**(10), 1233–1239.

Kennedy, C., Kools, S. & Krueger, R. (2001), 'Methodological considerations in children's focus groups', *Nursing Research* **50**, 184–187.

Kim, M. & Choi, Y. (2017), 'Risk communication: The roles of message appeal and coping style', *Social Behavior and Personality: An international journal* **45**, 773–784.

Kintsch, W. & van Dijk, T. A. (1978), 'Toward a model of text comprehension and production', *Psychological Review* **85**(5), 363–393.

Kitzinger, J. (1995), 'Qualitative research: Introducing focus groups', *BMJ* **311**(7000), 299–302.

Krueger, R. & Casey, M. (2009), *Focus groups: A practical guide for applied research*, 4 edn, Thousand Oaks.

Lanning, K. (2005), Compliant child victim: Confronting an uncomfortable reality, *in* E. Quayle & M. Taylor, eds, 'Viewing child pornography on the Internet', Russell House, pp. 49–60.

Lanning, K. (2010), *Child molesters: A behavioral analysis*, 5 edn, National Center for Missing and Exploited Children.

Lanning, K. (2018), 'The evolution of grooming: Concept and term', *Journal of Interpersonal Violence* **33**(1), 5–16.

Lanning, K. & Dietz, P. E. (2014), 'Acquaintance child molesters and youth-serving organizations', *Journal of Interpersonal Violence* pp. 1–24.

Last, J. & Porta, M. (2018), 'A dictionary of public health', https://doi.org/10.1093/acref/9780191844386.001.0001. Accessed: 2019-11-11.

Laughery, K. & Wogalter, M. (1997), *Handbook of Human Factors and Ergonomics*, 2 edn, Wiley.

Leicestershire (2017), 'Kayleigh's love story - full version', https://www.youtube.com/watch?v=WsbYHI-rZOE. Accessed: 2020-05-10.

Lund, I., Helgeland, A. & Kovac, V. B. (2016), 'Empirically based analysis of methodological and ethical challenges in research with children as participants: the case of bullying in kindergarten', *Early Child Development and Care* **186**(10), 1531–1543.

Lundgren, R. & McMakin, A. (2009), *Risk communication: A Handbook for Communicating Environmental, Safety, and Health Risks*, Wiley-IEEE.

Malesky, L. (2007), 'Predatory online behavior: Modus operandi of convicted sex offenders in identifying potential victims and contacting minors over the internet', *Journal of child sexual abuse* **16**, 23–32.

Marcum, C. D. (2007), 'Interpreting the intentions of internet predators: An examination of online predatory behavior', *Journal of Child Sexual Abuse* **16**(4), 99–114.

McAlinden, A.-M. (2006), "setting 'em up': Personal, familial and institutional grooming in the sexual abuse of children', *Social and Legal Studies* **15**(3), 339–362.

McGarry, O. (2016), 'Repositioning the research encounter: exploring power dynamics and positionality in youth research', *International Journal of Social Research Methodology* **19**(3), 339–354.

Morgan, M., Fischhoff, B., Bostrom, A. & Atman, C. (2002), *Risk Communication: A Mental Models Approach*, Cambridge University Press.

Morgan, M., Gibbs, S., Maxwell, K. & Britten, N. (2002), 'Hearing children's voices: methodological issues in conducting focus groups with children aged 7-11 years', *Qualitative Research* **2**(1), 5–20.

Nielsen, J. (1994), '10 usability heuristics for user interface design', https://www.nngroup.com/articles/ten-usability-heuristics/. Accessed: 2020-04-12.

Nielsen, J. (2012), 'How many test users in a usability study?', https://www.nngroup.com/articles/how-many-test-users/. Accessed: 2020-05-26.

Nodder, C. (2005), Users and trust: a microsoft case study, *in* L. C. Simson Garfinkel, ed., 'Security and Usability: designing secure systems that people can use', O'Reilly Media.

NSPCC (2016), 'Unhealthy relationships highlighted in new childline campaign', https://www.nspcc.org.uk/what-we-do/news-opinion/unhealthy-relationships-highlighted-new-childline-campaign/. Accessed: 2020-05-20.

NSPCC (2020), 'Grooming', https://www.nspcc.org.uk/what-is-child-abuse/types-of-abuse/grooming/. Accessed: 2020-04-12.

O'Connell, R. (2003), 'A typology of child cybersexploitation and online grooming practices'.

Olson, L. N., Daggs, J. L., Ellevold, B. L. & Rogers, T. K. K. (2007), 'Entrapping the innocent: Toward a theory of child sexual predators' luring communication', *Communication Theory* **17**(3), 231–251.

Prior, J. & Van Herwegen, J. (2016), *Practical Research with Children*, Taylor and Francis.

PSIC (2018), 'Careful parents – new campaign of the empowering children foundation', https://www.betterinternetforkids.eu/web/portal/practice/awareness/detail?articleId=3111402. Accessed: 2020-05-20.

Raffel, L., Bours, P. & Komandur, S. (2020), 'Attention! designing a target group-oriented risk communication strategy', *HCI International 2020 Conference Proceedings: Communications in Computer and Information Science* . As of the date of submission, no further details of this publication were known to the authors, but the paper can be found in the appendix.

Riley, D. (2014), 'Mental models in warnings message design: A review and two case studies', *Safety Science* **61**, 11–20.

Sandman, P. (1988), 'Risk communication: Facing public outrage', *Management Communication Quarterly* **2**(2), 235–238.

Sandman, P. (2007*a*), 'Precaution advocacy messaging strategy: The gaamm model', https://www.psandman.com/handouts/sand38a.pdf. Accessed: 2020-03-12.

Sandman, P. (2007*b*), 'Watch out! precaution advocacy fundamentals', http://www.psandman.com/handouts/sand59a.pdf. Accessed: 2020-03-12.

Sandman, P. (2014), 'Introduction to risk communication and orientation to this website', http://www.psandman.com/index-intro.htm. Accessed: 2020-03-12.

Shannon, C. E. (1948), 'A mathematical theory of communication', *Bell System Technical Journal* **27**(4), 623–656.

Shaw, C., Brady, L.-M. & Davey, C. (2011), *Guidelines for research with children and young people*, National Children's Bureau (NCB) Research Centre.

Slovic, P. (1987), 'Perception of risk', *Science* **236**(4799), 280–285.

Smahel, D., Machackova, H., Mascheroni, G., Dedkova, L., Staksrud, E., Ólafsson, K., Livingstone, S. & Hasebrink, U. (2020), 'Eu kids online 2020: Survey results from 19 countries'.

Staksrud, E. (2013), 'Online grooming legislation: Knee-jerk regulation?', *European Journal of Communication* **28**(2), 152–167.

STC (1998), 'Ethical principles for technical communicators', https://www.stc.org/about-stc/ethical-principles/. Accessed: 2019-11-11.

Tattar, P., Ramaiah, S. & Manjunath, B. (2016), *A Course in Statistics with R*, Wiley.

Tomitsch, M., Wrigley, C., Borthwick, M., Ahmadpour, N., Frawley, J., Kocaballi, A., Nunez-Pacheo, C., Straker, K. & Loke, L. (2018), *Design. Think. Make. Break. Repeat. A Handbook of Methods*, BIS Publishers.

Webster, S., Davidson, J., Bifulco, A., Gottschalk, P., Caretti, V., Pham, T., Grove-Hills, J., Turley, C., Tompkins, C., Ciulla, S., Milazzo, V., Schimmenti, A. & Craparo, G. (2012), 'European online grooming project - final report'.

Weinstein, N. & Sandman, P. (1993), 'Some criteria for evaluating risk messages', *Risk Analysis* **13**(1), 103–114.

Whittle, H. C., Hamilton-Giachritsis, C. E. & Beech, A. R. (2015), 'A comparison of victim and offender perspectives of grooming and sexual abuse', *Deviant Behavior* **36**(7), 539–564.

Williams, R., Elliott, I. A. & Beech, A. R. (2013), 'Identifying sexual grooming themes used by internet sex offenders', *Deviant Behavior* **34**(2), 135–152.

Winters, G. M. & Jeglic, E. L. (2016), 'I knew it all along: The sexual grooming behaviors of child molesters and the hindsight bias', *Journal of child sexual abuse* **25**, 1–17.

Winters, G. M. & Jeglic, E. L. (2017), 'Stages of sexual grooming: Recognizing potentially predatory behaviors of child molesters', *Deviant Behavior* **38**(6), 724–733.

Winters, G. M., Kaylor, L. E. & Jeglic, E. L. (2017), 'Sexual offenders contacting children online: an examination of transcripts of sexual grooming', *Journal of Sexual Aggression* **23**(1), 62–76.

Wogalter, M. (2006), *Handbook of warnings*, Lawrence Erlbaum Associates.

Wogalter, M., Conzola, V. C. & Smith-Jackson, T. L. (2002), 'Research-based guidelines for warning design and evaluation.', *Applied ergonomics* **33**(3), 219–30.

Wong, L. P. (2008), 'Focus group discussion: A tool for health and medical research', *Singapore medical journal* **49**, 256–60.

7 Conference Paper for HCI INTERNATIONAL 2020

On the following pages you can find the paper "Attention! Designing a target group-oriented risk communication strategy" which was accepted as a contribution to the 22nd International Conference on Human-Computer Interaction. It presents and discusses the focus groups that have been conducted with the children at Blomhaug Barneskolen. It will be published as part of the conference proceedings, but is not yet available at the time of submission of this thesis.

Attention! Designing a target group-oriented risk communication strategy

Lara Raffel[1], Patrick Bours[1], and Sashidharan Komandur[1]

Norges Teknisk Naturvitenskapelig Universitet (NTNU) Gjøvik, Teknologiveien 22. 2815 Gjøvik, Norway

Abstract. Online conversations through chat applications have become a universal part of human communication. But how can we be sure that the person we are chatting with is in fact the person they claim to be? This question significantly gains importance from the standpoint of safety and security when considering the chat behavior of children who are allowed access to web-enabled devices at an increasingly younger age. At the same time, the number of reported experiences with online sexual harassment and so-called grooming is unfortunately growing steadily. This paper presents insights from focus groups with school children and a resulting approach to communicating the risk of cyber grooming. The paper explores communication strategies for different stages of risk – before, during and after an incident. The way people interpret information affects the way they interact with it, which is why a user-centered design approach is employed in addition to standard guidelines of design to structure and design a communication strategy. Protecting children from sexual predators who use grooming strategies to bond with their victims is the main goal of this project.

Keywords: Chat security · Warning Design · Risk Communication · Grooming · Human Factors · User-centered Design.

1 Background

1.1 AiBA

This project is conducted as part of the AiBA (Author Input Behavioral Analysis) project by the Norwegian Biometry Lab at NTNU Gjøvik. AiBA aims at identifying fake profiles in chat applications using behavioral biometrics, in particular for protecting children from sexual predators that find their victims online. For example, behavioral biometrics can reveal an adult pretending to be a teenager in order to groom children online. The algorithms analyse word usage, writing rhythm, linguistics and media input to differentiate between adults and children as well as between males and females. The system is trained with data from convicted abuse cases and chat data acquired from children using a chat prototype. It is envisioned that the algorithms will either be built into platforms and applications used by children, such as Roblox, Snapchat and Instagram, or will act as a standalone application that retrieves data from the chats. Alerting

the users that such a security measurement is in place will contribute to deterring those with dishonest intentions, since there is a higher chance of being disclosed.

1.2 Online Grooming

Grooming describes behavioral patterns that are applied by sexual predators in preparation to sexually abuse a child. Colton et al. [4] describe grooming as a complex process in which the predator gains access to the chosen victim so that abuse can be initiated and maintained without being disclosed over time. However, literature shows no consensus over the specific methods that are employed by offenders [2] and empirical research has found that it is hard to recognize grooming behavior prior to abuse since it is not always clearly distinguishable from normal adult-child interactions [16]. Nevertheless, Winters et al. [16] describe that almost half of all convicted child abuse cases in the US have been preceded by what was identified as grooming behavior. Lanning [10] developed an accurate description of the process and emphasizes that grooming is a non-violent practice that aims at sexual victimization and control without using threats or physical force, as these techniques are more likely to result in cooperation from the victim's side. Lanning [9] describes the process of grooming as incremental stages, starting with identification of targets based on certain factors, followed by gathering information about the child's interests and vulnerabilities. The offender then gains access to the victim through a variety of channels, for example through clubs, sports or online. The victim is controlled by the offender by a combination of strategies such as filling emotional or physical needs, bonding, sympathy or peer pressure. The internet and its infinite number of chat platforms has opened up a new channel for child offenders to gain access to victims and provides the offenders with anonymity and a wide reach to locate victims. Goals of online sexual grooming include cyber-sexual activity, access to child pornography or arranging in-person meetings [8].

1.3 Risk Communication

Risk communication describes a set of communication measures that prepares the audience for informed decision making before, during and after an event [5]. Risk communication originates from the public health sector where it is used to communicate and educate about health risks and epidemics. The approach has also been adapted to communicate risks of natural disasters such as floods and fires, but it can also be practiced on a smaller scale, for example in the practice of warning messages and labels [11]. Lundgren et al. [11] point out that there are a vast number of approaches to risk communication that have evolved from various disciplines and that the approach should be chosen according to the context and the audience. The risk communication process usually starts with a risk assessment that evaluates who will be harmed by the hazard and what effects can be expected, as well as how long these effects last. A strategy is developed how awareness can be raised about the subject and how the audience

can be educated. Information about how to take action in case of an event needs to be communicated in a clear and understandable manner. Also, a risk communication strategy should be disseminated through channels that are frequented by the target audience [11]. In addition, it is recommended to design messages according to the audiences' knowledge, interests and values [3]. Lundgren et al. [11] emphasize that the more the communicators understand the perspective of the target audience(s), the better they can choose appropriate communication methods and thus implement successful risk communication. This shows the prominent role that user research should play in risk communication and justifies the user-centred approach taken in this project.

2 Methodology

2.1 Focus Groups with children in 7th grade

With the goal of acquiring profound insights into the perception and knowledge about online sexual predators and grooming strategies, focus groups were designed to investigate children's chat behavior, how they react to certain messages in chats and to what extent they are aware of dangers. Two seventh grade classes with a total number of 35 pupils participated in two project days about "Chat Security". To investigate the impact of education on the subject, two focus groups were conducted before a presentation on chat security and grooming strategies was given, and four groups after, resulting in six focus groups being conducted at the school, each consisting of 5-6 children of 12 to 13 years. During preparation, it was taken into consideration that working with children results in certain challenges such as differences in children's development due to their culture and social environment [1], ensuring the children's engagement and attention [7] as well as their safety and comfort [12]. It was investigated how they think they can trust someone online and where they draw the line between appropriate and inappropriate messages. The focus groups concluded with an assessment of the concept behind the AiBA project.

The focus groups were divided into three sections. In the opening part, a brainstorming session was conducted, first on what the participants use the Internet for, and then more specifically what applications they use for chatting with other people. This data can be used to establish the most effective locations for placing information about online predators and also potential customers for the AiBA application. To challenge the children's creativity, they were then asked to come up with a username for a fictional chat. Since usernames are one of the targeting criteria of sexual predators [17], the data will be helpful to determine how children choose them. After presenting the usernames, the moderator challenged the participants by exchanging her username with one of the children's. They were asked to come up with ideas how to find out who really is behind a nickname and how to trust someone online. The second part of the focus group consisted of a made-up chat conversation that followed a simplified grooming process. The children were challenged to come up with replies or reactions to the messages which got increasingly inappropriate. After each message,

the children were asked if they thought this message was written by someone of their age, an adult or if it could be both. This data will give insights about how children behave in chats and where they draw the line between appropriate and inappropriate conversations. As the last part, the AiBA project was summarised in a simple and understandable way. The children were then asked to rate how much they liked the idea of such a system by assigning a number (1 being worst and 10 being best) on a sheet of paper. They were also asked to write down a reason for their decision. After each focus group, some notes were taken on the children's overall behavior and reactions, as well as their body language and other remarks.

3 Results

The collected data was mainly of qualitative nature, showing opinions, experiences and reactions of the children. This data was analysed by applying a mix of design methods such as thematic evaluation and affinity diagramming . Exploratory statistical analyses was also used. Special attention was given to understand differences between the groups who have not received education about the subject and those who have. Already on location during the project days, it was possible to notice some immediate results. It was clear to see that there are immense individual differences in how the pupils reacted to the prompted chat messages, some being very honest, others extremely careful or evading through humour and irony. On the second day - after the presentation on chat security and online grooming - it was very striking to observe how much more careful and suspicious the children were acting. Their behavior changed and they were more direct in differentiating between appropriate and inappropriate messages. Also, the terms "sexual predator", "kidnapper" and "pedophile" were mentioned regularly, while this had not occurred on the previous day.

After an in-depth analysis, one could see that educating children about chat security and grooming can show immediate, short-term results. The children became more aware of the risk and were discussing about sexual predators several times during the focus groups if they had been educated before. The focus groups showed the popularity of using Snapchat among children of 12 and 13 years as well as their strong interest in playing online games and consuming media content. These platforms can be important partners to spread education on online grooming and could also be potential customers for the AiBA system. The children mostly chat with friends, but it is not uncommon to chat with strangers when it is about a common interest, such as gaming. The children felt confident that they could detect an adult who tries to pretend to be a teenager through the language that is used and also the content of the conversation. They rated pictures or video calls as the most reliable option to find out about someone's real identity. When creating usernames, the children unintentionally gave away personal information such as their name and age, regardless whether they had attended the presentation on chat security or not. In a fictional chat environment, those children who received education on grooming before were more self-assured

to say "no", acted more confident and suspected dishonest behavior sooner than children without previous education on the topic. The overall rating of the AiBA system was more positive after the presentation, showing that the children saw more value in it than before.

The insights were further evaluated with a set of gamestorming methods as described by Gray [6], resulting in a risk assessment. The reason for a need of education are the high level of Internet access and chat usage at an increasingly younger age, meanwhile predators are using chats as a means for easy access to victims. As estimated by a recent EU study [14], children aged 12-14 years in the EU spend around 192 minutes online each day. Children are particularly at risk once they start conversing with strangers and give away private information, either unknowingly (i.e. through usernames), due to risk-seeking behavior (doing something "forbidden") or simply because they are not aware of the danger and engage in seemingly harmless conversations. The European Online Grooming Report [15] describes that children that are perceived by predators as particularly vulnerable are more likely to be targeted, as well as risk-taking children who are outgoing and confident online - similar to the children in the focus groups who reacted to the chat messages with humour or by being offensive. However, while it is important to take these risk factors into account, children at risk should not be stigmatised or reduced to a homogeneous group as both individual behavior and targeting tactics of online predators vary greatly. Challenges that are faced when tackling the topic are the general unawareness of the children who are active in chats and also the parent's lack of knowledge about the subject. It is sometimes treated as a taboo topic that evokes feelings of shame, it can result in victim-blaming and is seen with hindsight-bias, meaning that people claim to have "seen it coming" only after an incident, or the risk is being ignored as it seems unlikely to happen to oneself. Since children want to maintain a certain level of autonomy and privacy, a lack of parental supervision can increase the risk, as well as a lack of security measures in many chat applications. However, if the risk is not addressed, it means that ultimately more children will fall victim to sexual abuse, either through physical meetings with the predators or through online activities. Children will be exposed to sexual content and might share private pictures and information. This can result in the children being bullied, threatened or blackmailed which in turn results in psychological damage and a dependency on the relationship with the predator. In real life, consequences can be seen in a problematic relationship with the parents and peers, since the online relationship gains importance. Therefore, the goal of the risk communication is mainly preventive, aiming at children who engage in chat environments, whose safety and security as well as privacy and autonomy should be secured. Educating them about grooming will increase their caution on the web, enable them to protect themselves and give them the courage to report incidents.

As children spent a vast amount of time on the Internet, spreading information directly in the chat environments, on social media or gaming platforms is believed to be an appropriate choice of media. Furthermore, postings on social media can be used to target specific user groups that are at a higher risk. The

children should be able to relate to the messengers that convey the content, therefore it is important that the messenger is close to the peer group and that the wording appeals to them. This is believed to increase the children's interest in the content and work against barriers such as ignorance and shame. Another effective way to reach the children is to conduct seminar days at schools similar to those conducted during the user research. This can provide the children with valuable background knowledge of Internet security and online behavior that can encourage them to rethink and adjust their own behavior. Building on this, the messages for precautionary advocacy can be designed, taking into account the guidelines for warning design by Sandman [13]. Thus, the messages need to be on point, raise interest, appeal to emotions and offer choice. Short, concise and understandable messages ensure that the information is interpreted in the intended way. Additionally, messages need to be interesting and appealing to the audience so that they are heeded in the first place. In combination with appealing to emotions (especially fear in proportion to the risk), chances are high that people will pay attention. Offering choices of actions to take, preferably in easy and small steps, encourages necessary changes in behavior. The main questions that need to be answered at this stage are: How does online grooming happen? What are the consequences? How can I protect myself?

The immediate response phase to a risk is triggered when the AiBA system detects suspicious behavior that indicates predatory behavior. A warning has to be sent so that the child and the parents can decide how to respond to the threat. For creating these warnings, design principles can be applied regarding the structure, understandability, noticeability and context of the messages [18]. The goal of the warning message is to make the user aware that the chat partner is showing signs of predatory behavior or grooming. The message needs to attract the users attention, so it needs to be prominently displayed and designed. Timing is crucial as sending a warning too late can result in harm to the child, while sending it too early can result in unfounded fear and false accusations. In order to justify the message and to ensure understandability, it needs to be explained how the system arrived at this conclusion, for instance by listing the suspicious characteristics of the conversation. The risk and its consequences should be explained briefly to mark the urgency of the situation and the need to take action. The warning needs to present choices and recommendations for subsequent actions in easy steps. For instance, a checklist can help the user to identify grooming behavior and if the chat partner should be blocked and reported. Since AiBA will not be infallible, the final decision to take action lies with the user.

After the immediate risk has been averted, the audience should be given options to recover and react to the incident. The focus of the recovery phase lies on providing support and counteracting apathy. The information should be sent directly to the audience so that they immediately have access to it after AiBA warned them about predatory behavior. Additionally, the information should be available on demand so that it can be reviewed at all times. Crucial points to consider are providing emotional support, indicating institutions where one

can receive additional help and encouraging that grooming should be reported. Again, the information should encourage young people to draw lines and stand up for their own well-being.

4 Discussion

The short term results of the focus groups show that education about online security and grooming does seem to influence behavior and makes children more aware of risks on the web and thus more careful. The extensive use of the web and particularly chat environments by young children shows the importance of this project. Also, the high interest that the children have shown towards the topic gives hope that education measures will be received eagerly and the seriousness of this is understood very well. However, further assessment is needed to establish long term results. The importance of education on online grooming for raising awareness and preventing abuse is backed up by previous research [15]. Establishing information needs and extracting the key messages for each stage of risk communication allows for differentiated information distribution that provides the audience with relevant information when it is needed.

Work in Progress: Additional focus groups with children are planned to strengthen the results and gain additional insights. Furthermore, the communication strategy will be supplemented by a similar approach that provides information for parents, since they serve as role models and close confidants of the children. Future work will consist of refining the strategy and creating a set of tangible messages and information materials that will be evaluated and adapted based on user tests. The completed strategy will be presented in a master's thesis at NTNU and is hoped to be implemented with the completion of the AiBA system, providing children and parents with both education and practical means to protect themselves and their loved ones on the web. The interdisciplinary nature of this project is meant to encourage people working in design, risk communication and computer security to cooperate. It shows that user-centered design approach can be applied to a variety of fields outside the traditional design context. A multi-faceted risk such as online grooming needs to be managed as a collaborative approach in order to promote prevention and minimise the degree of harm.

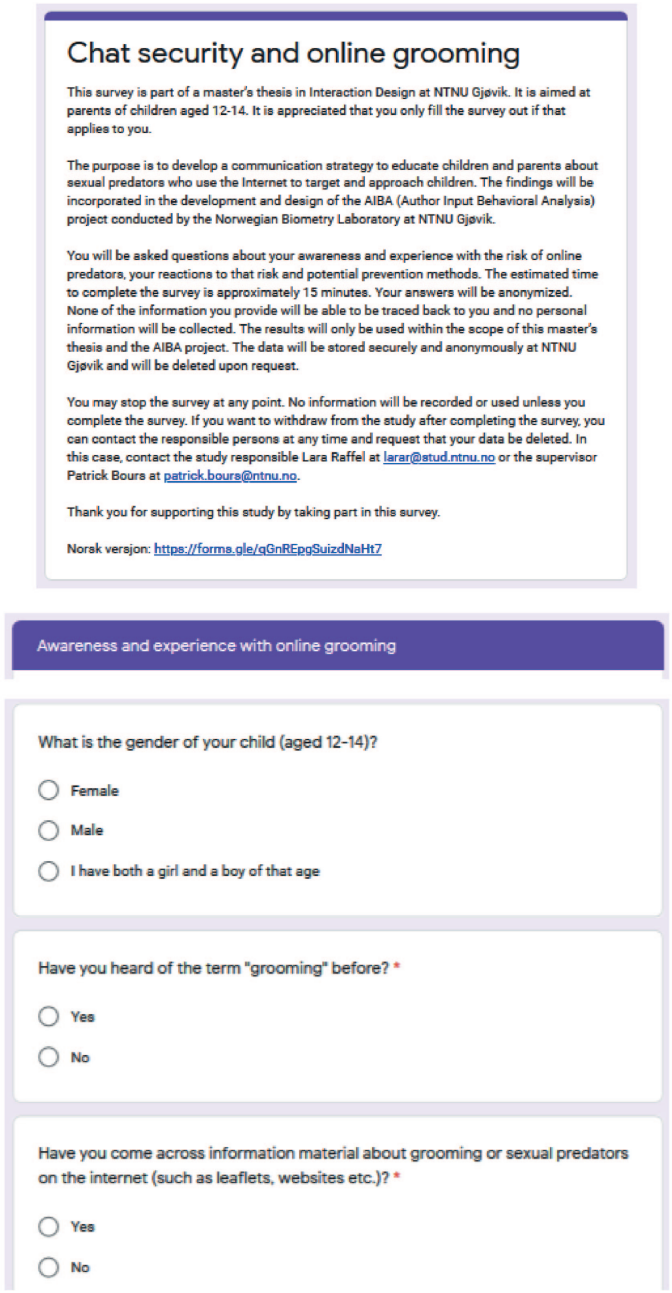
References

1. Adler, K., Salanterä, S., Zumstein-Shaha, M.: Focus group interviews in child, youth, and parent research: An integrative literature review. International Journal of Qualitative Methods **18** (2019)
2. Bennett, N., O'Donohue, W.: The construct of grooming in child sexual abuse: Conceptual and measurement issues. Journal of Child Sexual Abuse **23**(8), 957–976 (2014)
3. Boholm, A.: Lessons of success and failure: Practicing risk communication at government agencies. Safety Science **118**, 158 – 167 (2019)

4. Colton, M., Roberts, S., Vanstone, M.: Learning lessons from men who have sexually abused children. Howard Journal of Criminal Justice **55**(1), 79–93 (2012)
5. Gamhewage, G.: An introduction to risk communication. http://www.who.int/risk-com-munication/introduction-to-risk-communication.pdf?ua=1 (2014), accessed: 2019-11-11
6. Gray, D., Brown, S., Macanufo, J.: Gamestorming: A Playbook for Innovators, Rulebreakers, and Changemakers. O'Reilly (2010)
7. Kennedy, C., Kools, S., Krueger, R.: Methodological considerations in children's focus groups. Nursing Research **50**, 184–187 (05 2001)
8. Lanning, K.: Compliant child victim: Confronting an uncomfortable reality. In: Quayle, E., Taylor, M. (eds.) Viewing child pornography on the Internet. pp. 49–60. Russell House (2005)
9. Lanning, K.: Child molesters: A behavioral analysis, 5th edition. National Center for Missing & Exploited Children (2010)
10. Lanning, K.: The evolution of grooming: Concept and term. Journal of Interpersonal Violence **33**(1), 5–16 (2018)
11. Lundgren, R., McMakin, A.: Risk communication: A Handbook for Communicating Environmental, Safety, and Health Risks. Wiley-IEEE (2009)
12. McGarry, O.: Repositioning the research encounter: exploring power dynamics and positionality in youth research. International Journal of Social Research Methodology **19**(3), 339–354 (2016)
13. Sandman, P.: "watch out!" precaution advocacy fundamentals. http://www.psandman.com/handouts/sand59a.pdf (2007), accessed: 2020-03-12
14. Smahel, D., Machackova, H., Mascheroni, G., Dedkova, L., Staksrud, E., Ólafsson, K., Livingstone, S., Hasebrink, U.: Eu kids online 2020: Survey results from 19 countries (2020)
15. Webster, S., Davidson, J., Bifulco, A., Gottschalk, P., Caretti, V., Pham, T., Grove-Hills, J., Turley, C., Tompkins, C., Ciulla, S., Milazzo, V., Schimmenti, A., Craparo, G.: European online grooming project - final report (2012)
16. Winters, G.M., Jeglic, E.L.: Stages of sexual grooming: Recognizing potentially predatory behaviors of child molesters. Deviant Behavior **38**(6), 724–733 (2017)
17. Winters, G.M., Kaylor, L.E., Jeglic, E.L.: Sexual offenders contacting children online: an examination of transcripts of sexual grooming. Journal of Sexual Aggression **23**(1), 62–76 (2017)
18. Wogalter, M.S., Conzola, V.C., Smith-Jackson, T.L.: Research-based guidelines for warning design and evaluation. Applied ergonomics **33 3**, 219–30 (2002)

8 Appendix

8.1 Survey Questionnaire (English)



Chat security and online grooming

This survey is part of a master's thesis in Interaction Design at NTNU Gjøvik. It is aimed at parents of children aged 12-14. It is appreciated that you only fill the survey out if that applies to you.

The purpose is to develop a communication strategy to educate children and parents about sexual predators who use the Internet to target and approach children. The findings will be incorporated in the development and design of the AIBA (Author Input Behavioral Analysis) project conducted by the Norwegian Biometry Laboratory at NTNU Gjøvik.

You will be asked questions about your awareness and experience with the risk of online predators, your reactions to that risk and potential prevention methods. The estimated time to complete the survey is approximately 15 minutes. Your answers will be anonymized. None of the information you provide will be able to be traced back to you and no personal information will be collected. The results will only be used within the scope of this master's thesis and the AIBA project. The data will be stored securely and anonymously at NTNU Gjøvik and will be deleted upon request.

You may stop the survey at any point. No information will be recorded or used unless you complete the survey. If you want to withdraw from the study after completing the survey, you can contact the responsible persons at any time and request that your data be deleted. In this case, contact the study responsible Lara Raffel at larar@stud.ntnu.no or the supervisor Patrick Bours at patrick.bours@ntnu.no.

Thank you for supporting this study by taking part in this survey.

Norsk versjon: https://forms.gle/qGnREpqSuizdNaHt7

Awareness and experience with online grooming

What is the gender of your child (aged 12-14)?

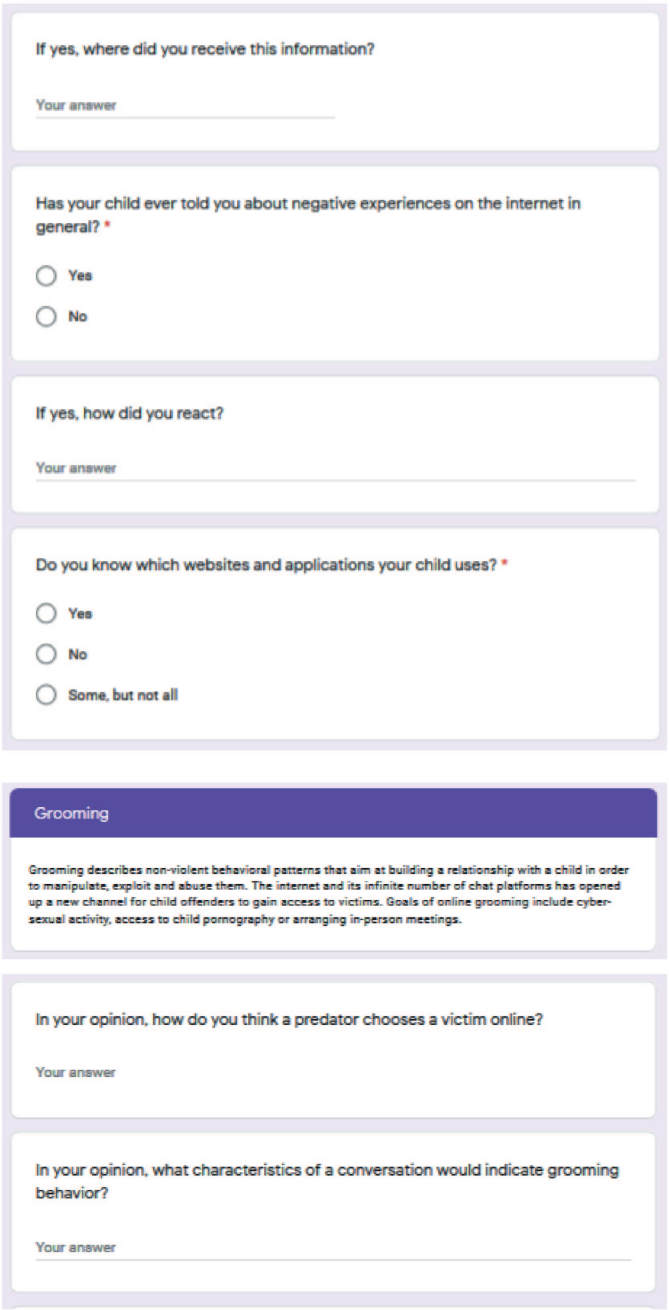
- Female
- Male
- I have both a girl and a boy of that age

Have you heard of the term "grooming" before? *

- Yes
- No

Have you come across information material about grooming or sexual predators on the internet (such as leaflets, websites etc.)? *

- Yes
- No



If yes, where did you receive this information?

Your answer

Has your child ever told you about negative experiences on the internet in general? *

- Yes
- No

If yes, how did you react?

Your answer

Do you know which websites and applications your child uses? *

- Yes
- No
- Some, but not all

Grooming

Grooming describes non-violent behavioral patterns that aim at building a relationship with a child in order to manipulate, exploit and abuse them. The internet and its infinite number of chat platforms has opened up a new channel for child offenders to gain access to victims. Goals of online grooming include cyber-sexual activity, access to child pornography or arranging in-person meetings.

In your opinion, how do you think a predator chooses a victim online?

Your answer

In your opinion, what characteristics of a conversation would indicate grooming behavior?

Your answer

Do you think you would be able to distinguish a normal chat conversation from one that applies grooming? *

- ◯ Yes
- ◯ No
- ◯ Maybe

What are your main personal concerns regarding grooming?

Your answer

Do you think your child is at risk of being targeted by an online predator? *

- ◯ Yes
- ◯ No
- ◯ Maybe

Have you talked to your child about online security? *

- ◯ Yes, extensively
- ◯ Yes, a bit
- ◯ No

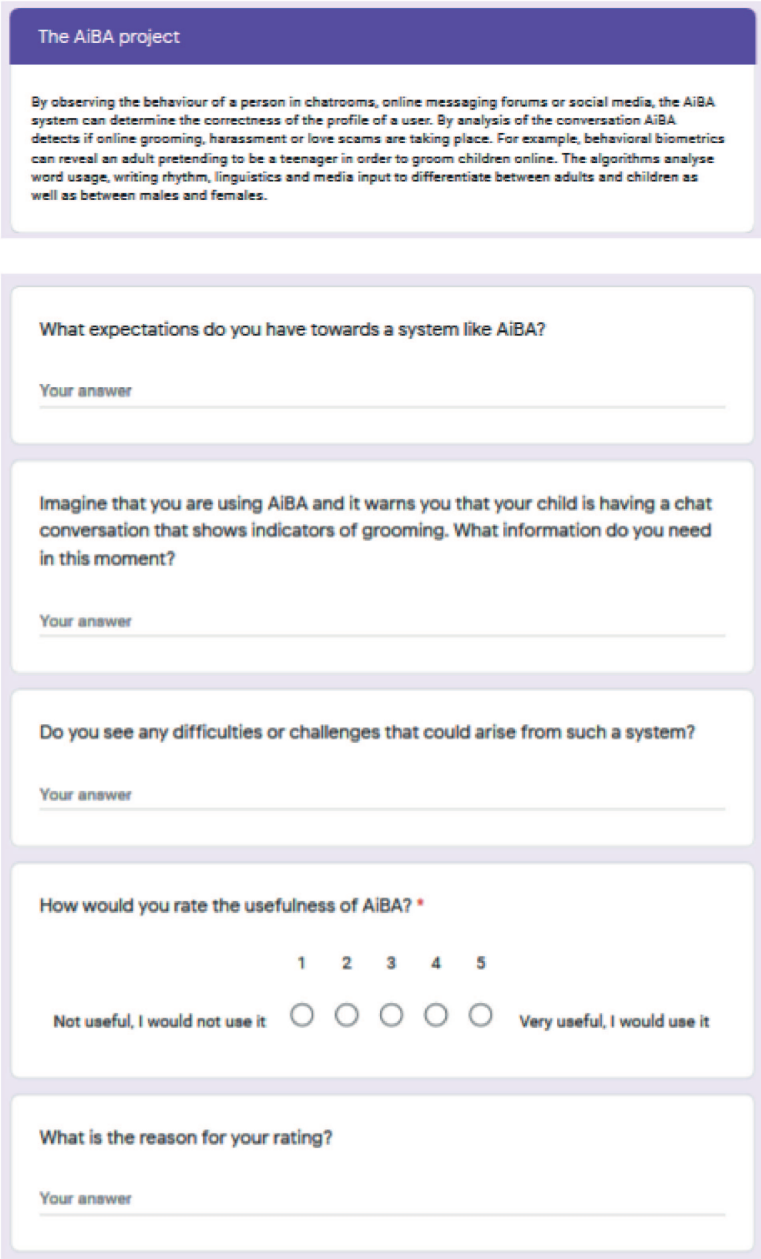
Prevention of grooming

In your opinion, what is the best way to protect children from online predators?

Your answer

As a parent, what is the most important information that you would like to receive about online grooming?

Your answer



The AiBA project

By observing the behaviour of a person in chatrooms, online messaging forums or social media, the AiBA system can determine the correctness of the profile of a user. By analysis of the conversation AiBA detects if online grooming, harassment or love scams are taking place. For example, behavioral biometrics can reveal an adult pretending to be a teenager in order to groom children online. The algorithms analyse word usage, writing rhythm, linguistics and media input to differentiate between adults and children as well as between males and females.

What expectations do you have towards a system like AiBA?

Your answer

Imagine that you are using AiBA and it warns you that your child is having a chat conversation that shows indicators of grooming. What information do you need in this moment?

Your answer

Do you see any difficulties or challenges that could arise from such a system?

Your answer

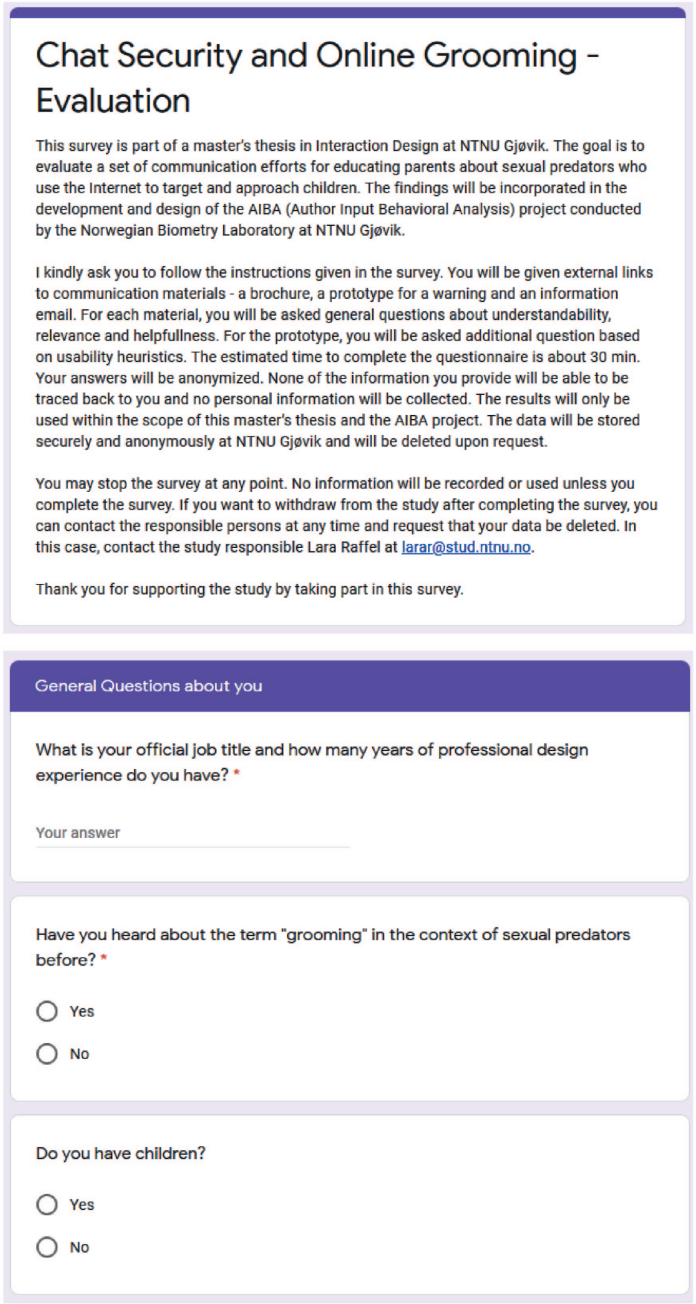
How would you rate the usefulness of AiBA? *

	1	2	3	4	5	
Not useful, I would not use it	○	○	○	○	○	Very useful, I would use it

What is the reason for your rating?

Your answer

8.2 Evaluation Guide for Experts



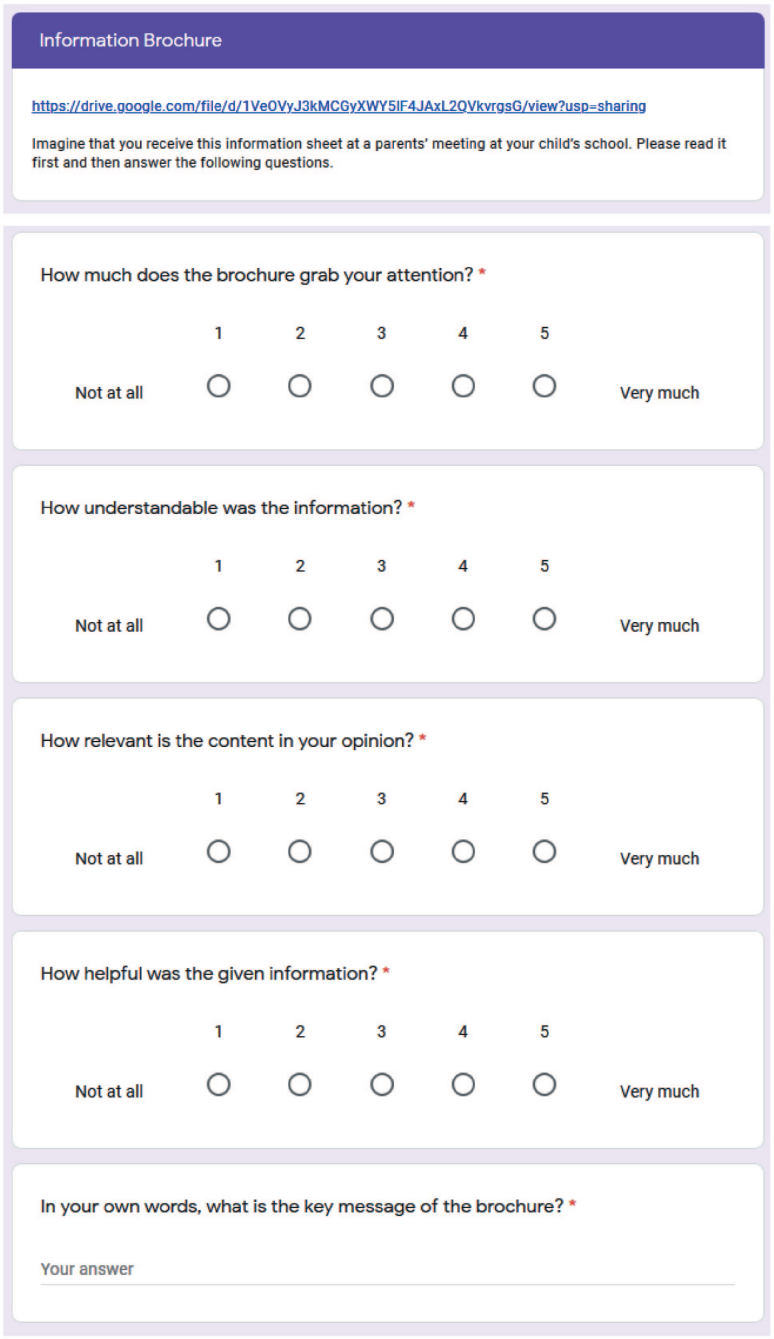
Chat Security and Online Grooming - Evaluation

This survey is part of a master's thesis in Interaction Design at NTNU Gjøvik. The goal is to evaluate a set of communication efforts for educating parents about sexual predators who use the Internet to target and approach children. The findings will be incorporated in the development and design of the AIBA (Author Input Behavioral Analysis) project conducted by the Norwegian Biometry Laboratory at NTNU Gjøvik.

I kindly ask you to follow the instructions given in the survey. You will be given external links to communication materials - a brochure, a prototype for a warning and an information email. For each material, you will be asked general questions about understandability, relevance and helpfullness. For the prototype, you will be asked additional question based on usability heuristics. The estimated time to complete the questionnaire is about 30 min. Your answers will be anonymized. None of the information you provide will be able to be traced back to you and no personal information will be collected. The results will only be used within the scope of this master's thesis and the AIBA project. The data will be stored securely and anonymously at NTNU Gjøvik and will be deleted upon request.

You may stop the survey at any point. No information will be recorded or used unless you complete the survey. If you want to withdraw from the study after completing the survey, you can contact the responsible persons at any time and request that your data be deleted. In this case, contact the study responsible Lara Raffel at larar@stud.ntnu.no.

Thank you for supporting the study by taking part in this survey.



Information Brochure

https://drive.google.com/file/d/1Ve0VyJ3kMCGyXWY5lF4JAxL2QVkvrgsG/view?usp=sharing

Imagine that you receive this information sheet at a parents' meeting at your child's school. Please read it first and then answer the following questions.

How much does the brochure grab your attention? *

	1	2	3	4	5	
Not at all	○	○	○	○	○	Very much

How understandable was the information? *

	1	2	3	4	5	
Not at all	○	○	○	○	○	Very much

How relevant is the content in your opinion? *

	1	2	3	4	5	
Not at all	○	○	○	○	○	Very much

How helpful was the given information? *

	1	2	3	4	5	
Not at all	○	○	○	○	○	Very much

In your own words, what is the key message of the brochure? *

Your answer

How much do you agree with the message? *

	1	2	3	4	5	
Not at all	○	○	○	○	○	Very much

Do you have any other comments (e.g. about the concept, the content or the design)?

Your answer

Warning Message - General Questions

By observing the behaviour of a person in chatrooms, online messaging forums or social media, the AiBA system can determine the correctness of the profile of a user. By analysis of the conversation AiBA detects if online grooming, harassment or love scams are taking place. For example, behavioral biometrics can reveal an adult pretending to be a teenager in order to groom children online. The algorithms analyse word usage, writing rhythm, linguistics and media input to differentiate between adults and children as well as between males and females.

https://www.figma.com/proto/uAxXcu7ZwLIke16m1qvmvd/AiBA-parent?node-id=37%3A0&scaling=contain

Imagine the following scenario:
While you are listening to music, you receive a message from the AiBA application, telling you that your child might be groomed by an online predator. Please open the prototype and afterwards answer the following questions.

How did the warning make you feel? *

	1	2	3	4	5	
Safe	○	○	○	○	○	Insecure

How urgent did the warning feel? *

	1	2	3	4	5	
Not at all	○	○	○	○	○	Very much

How understandable was the information? *

	1	2	3	4	5	
Not at all	○	○	○	○	○	Very much

How helpful was the given information? *

	1	2	3	4	5	
Not at all	○	○	○	○	○	Very much

How much do you trust the warning? *

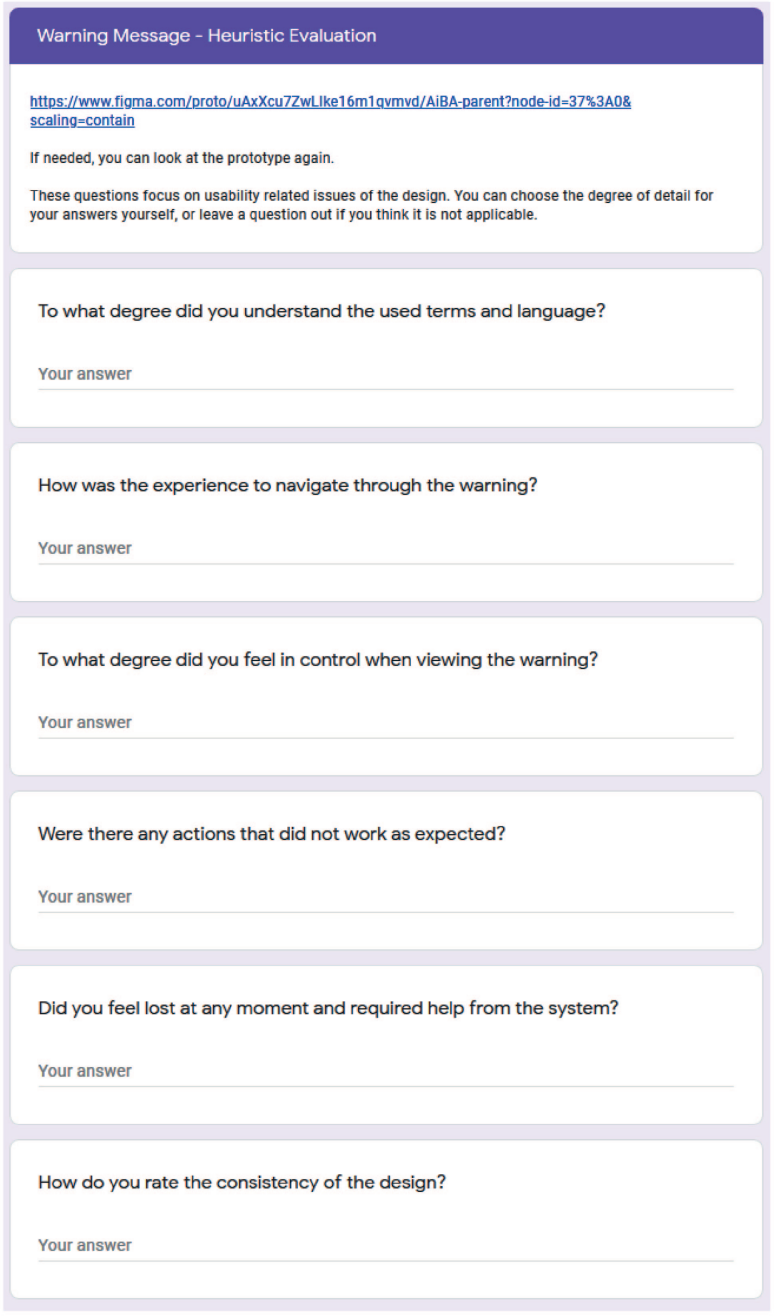
	1	2	3	4	5	
Not at all	○	○	○	○	○	Very much

What would you do after receiving this warning? *

Your answer

Do you have any other comments (e.g. about the concept, the content or the design)?

Your answer



Warning Message - Heuristic Evaluation

https://www.figma.com/proto/uAxXcu7ZwLIke16m1qvmvd/AiBA-parent?node-id=37%3A0&scaling=contain

If needed, you can look at the prototype again.

These questions focus on usability related issues of the design. You can choose the degree of detail for your answers yourself, or leave a question out if you think it is not applicable.

To what degree did you understand the used terms and language?

Your answer

How was the experience to navigate through the warning?

Your answer

To what degree did you feel in control when viewing the warning?

Your answer

Were there any actions that did not work as expected?

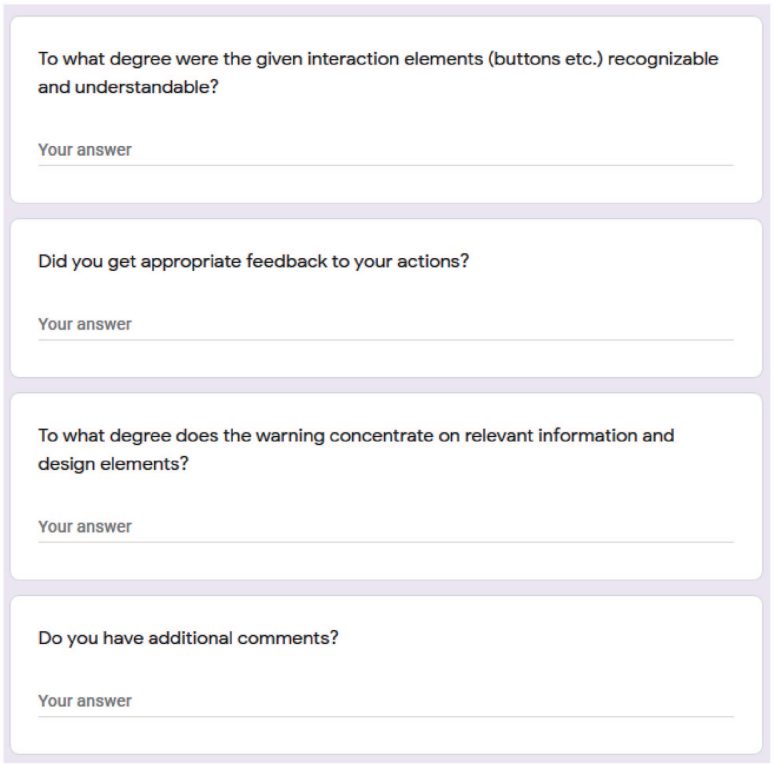
Your answer

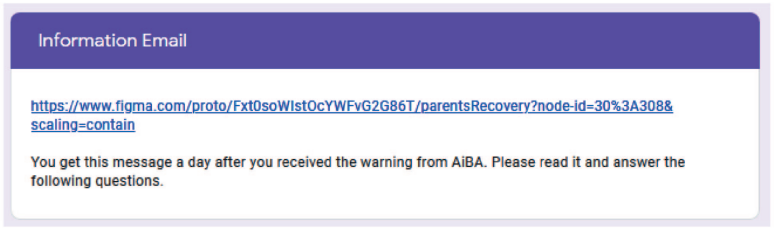
Did you feel lost at any moment and required help from the system?

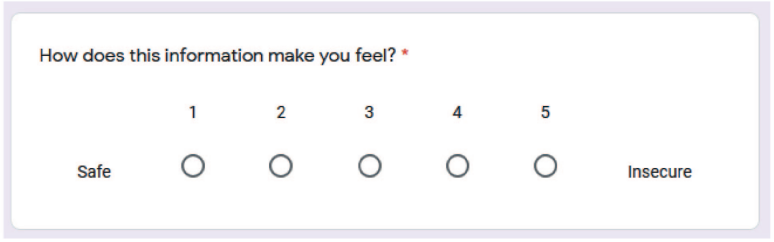
Your answer

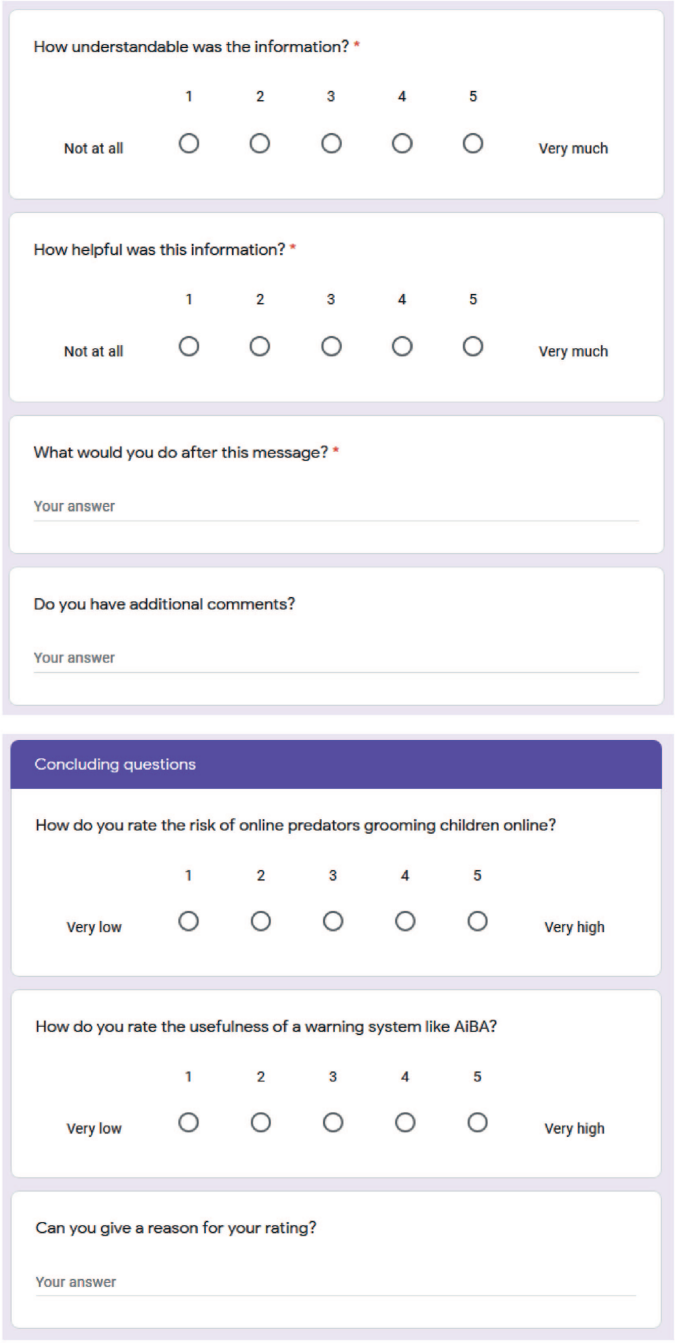
How do you rate the consistency of the design?

Your answer


To what degree were the given interaction elements (buttons etc.) recognizable and understandable?
Your answer
Did you get appropriate feedback to your actions?
Your answer
To what degree does the warning concentrate on relevant information and design elements?
Your answer
Do you have additional comments?
Your answer

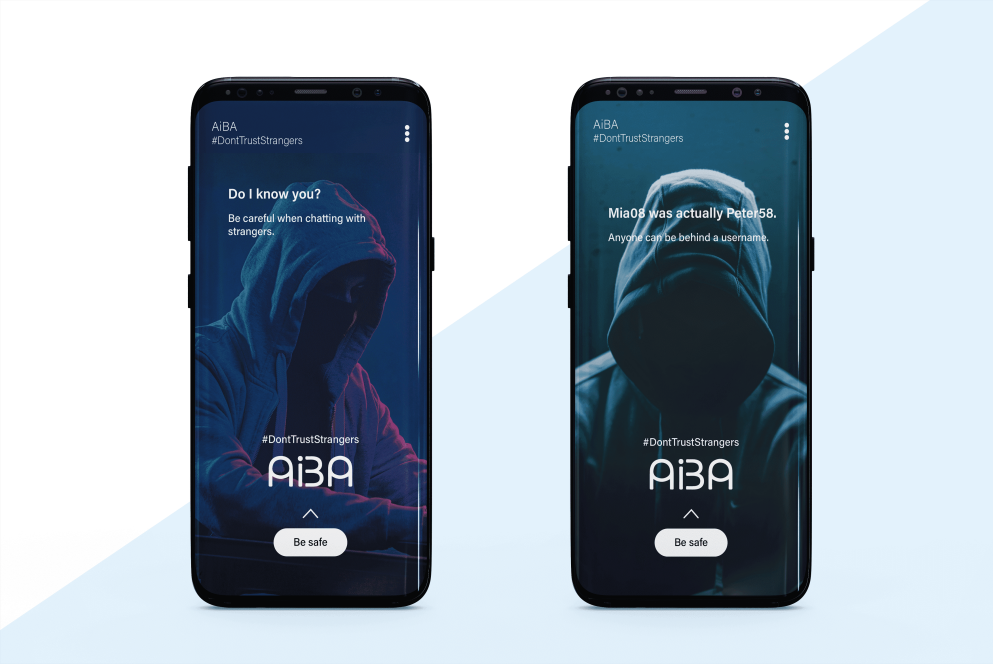

Information Email
https://www.figma.com/proto/Fxt0soWIstOcYWFvG2G86T/parentsRecovery?node-id=30%3A308&scaling=contain
You get this message a day after you received the warning from AiBA. Please read it and answer the following questions.

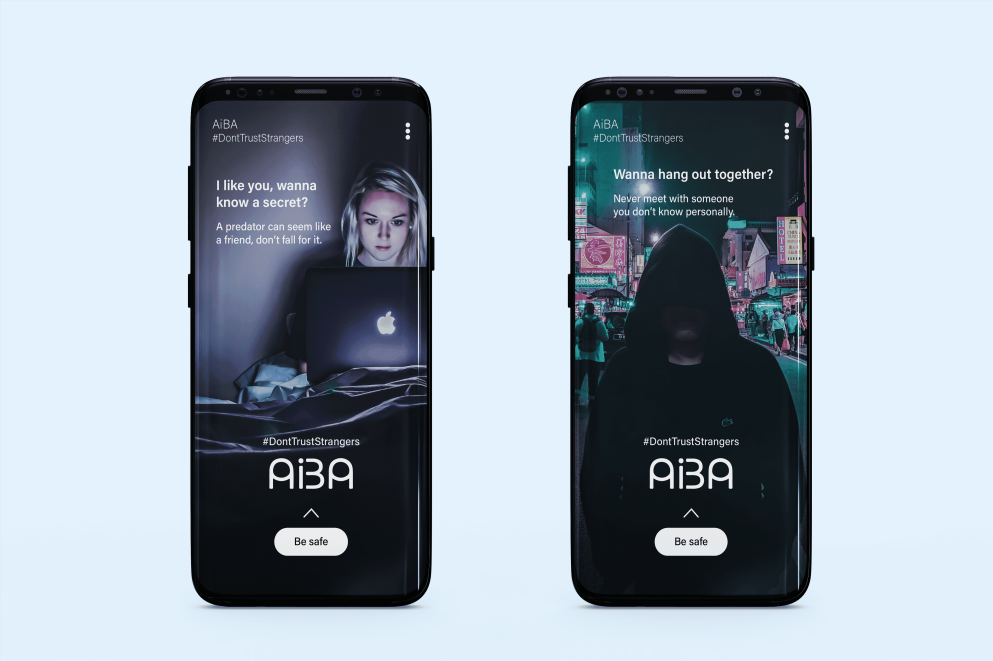

How does this information make you feel? *
1
2
3
4
5
Safe
Insecure

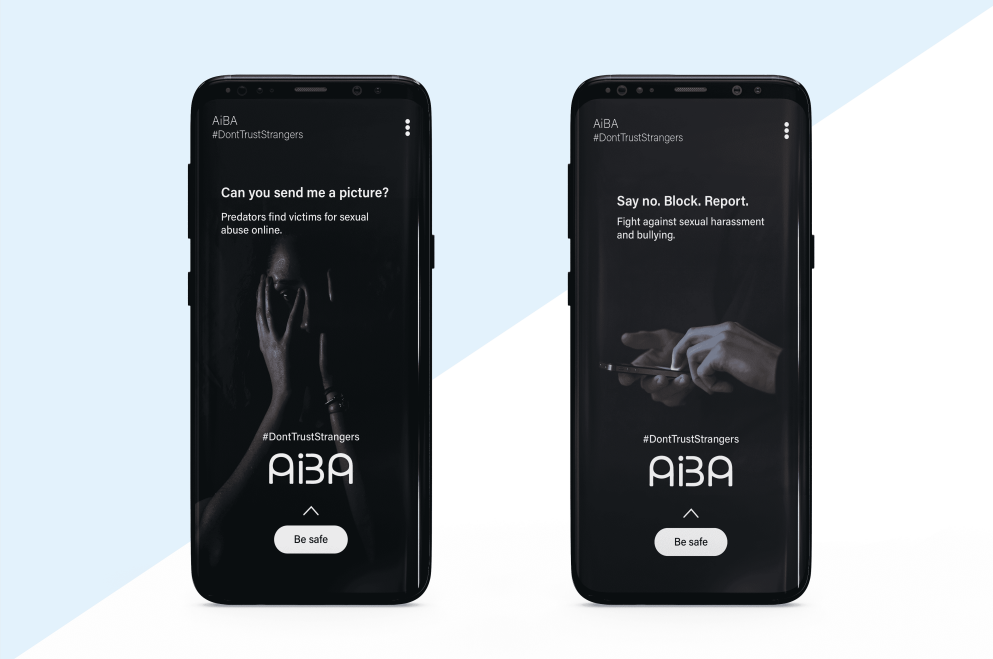

How understandable was the information? *
1 2 3 4 5
Not at all
Very much
How helpful was this information? *
1 2 3 4 5
Not at all
Very much
What would you do after this message? *
Your answer
Do you have additional comments?
Your answer
Concluding questions
How do you rate the risk of online predators grooming children online?
1 2 3 4 5
Very low
Very high
How do you rate the usefulness of a warning system like AiBA?
1 2 3 4 5
Very low
Very high
Can you give a reason for your rating?
Your answer

8.3 Snapchat Advertisement Campaign

The advertisements can be found in full screen following this link.




AiBA
#DontTrustStrangers
I like you, wanna know a secret?
A predator can seem like a friend, don't fall for it.
#DontTrustStrangers
AiBA
Be safe
AiBA
#DontTrustStrangers
Wanna hang out together?
Never meet with someone you don't know personally.
#DontTrustStrangers
AiBA
Be safe


AiBA
#DontTrustStrangers
Can you send me a picture?
Predators find victims for sexual abuse online.
#DontTrustStrangers
AiBA
Be safe
AiBA
#DontTrustStrangers
Say no. Block. Report.
Fight against sexual harassment and bullying.
#DontTrustStrangers
AiBA
Be safe

8.4 Information Brochure for Parents

A PDF version of the brochure can be found following this link.

What makes children vulnerable to grooming?

Any child is at risk of grooming, girls and boys alike. However, predators will search for a children's vulnerabilities that can be exploited.

Such risk factors can be:

- Insecurity and low self-esteem
- Loneliness, few friends
- Difficult family situations
- Low knowledge of online safety
- Risk-seeking behavior
- Naivety and openess to strangers
- Exploring sexuality online
- Children with disabilities

I was chatting with that girl who said she was my age and I felt really close to her. But then, the conversation turned and she asked me for naked pictures. I wasn't very confident and I wanted her to like me, so I just sent one. When she wanted more, she used that picture to threaten me. I was desperate and didn't know what to do, even thinking about hurting myself. When I told my mum and she involved the police, they found that I was actually chatting with a 45 year old man.
- Alice (13)

How does online grooming happen?

Grooming is a highly strategical process that involves a number of stages.

The predator identifies and accesses children through popular sites (chats, gaming platforms, social media etc.)

In a seemingly friendly conversation, the predator learns about the child's interests and vulnerabilities

Over time, the predator gains the child's trust and makes the relationship seem special and exclusive

Based on the child's interests and vulnerabilities, the predator can exploit and manipulate the child by filling emotional or social needs

The predator introduces sexual content to the conversation, pushing the child into online sexual activity, sending private pictures or meeting in person

What can I do to lower the risk?

Education about online safety is key to the prevention of grooming. You should show interest in your children's online activities and get familiar with the platforms they use. Clear guidelines on internet usage and online presence should be established. At the same time, a trusting environment will make your child feel safe to share experiences and worries. Teach your child about healthy relationships and they always have the right to say no.

How can I detect that my child is groomed?

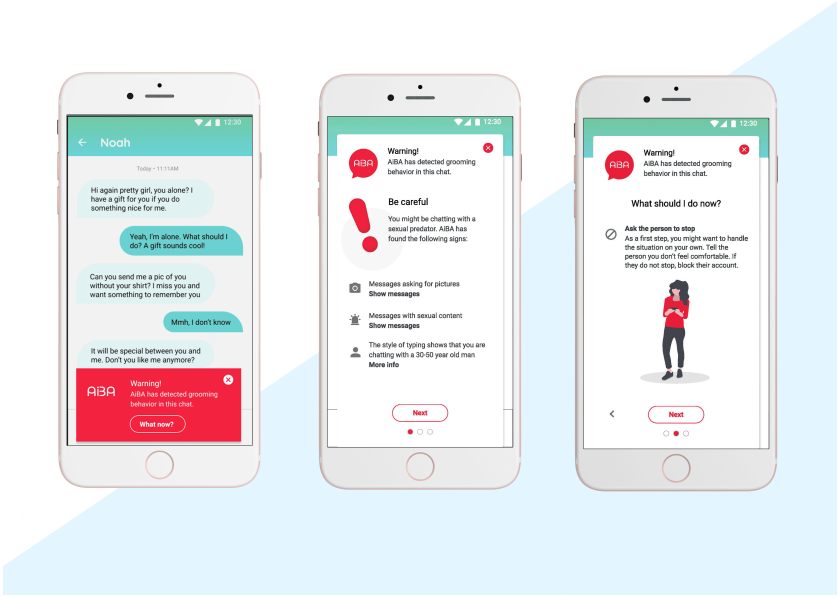
Warning signs can be subtle, but you should pay attention if your child shows the following behaviors.

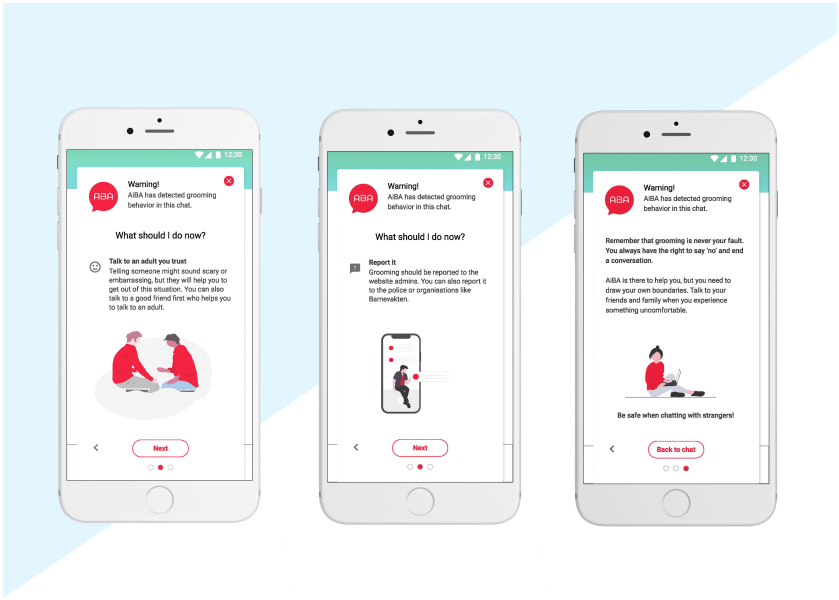
- Spending significantly more time online
- Suddenly becoming secretive about online activities and chat partners
- Neglecting real life friendships
- Seeming stressed or depressed
- Receiving unexpected gifts
- Sexualised behavior or language that is not age-approriate

When Lucas spent more time on the internet, I first thought it was normal for his age. But then he pulled away, saying he was chatting with a friend he met online. He wouldn't let me see the chat. Lucas seemed stressed and nervous about it. Eventually, we had a long talk about online safety and he told me about his „friend" asking for private pictures and a meeting. I contacted Barnevakten and reported the grooming. Lucas is now much more careful on the web.
- Ingrid, mother of Lucas, (12)

8.5 Clickable Prototype: Warning to Children

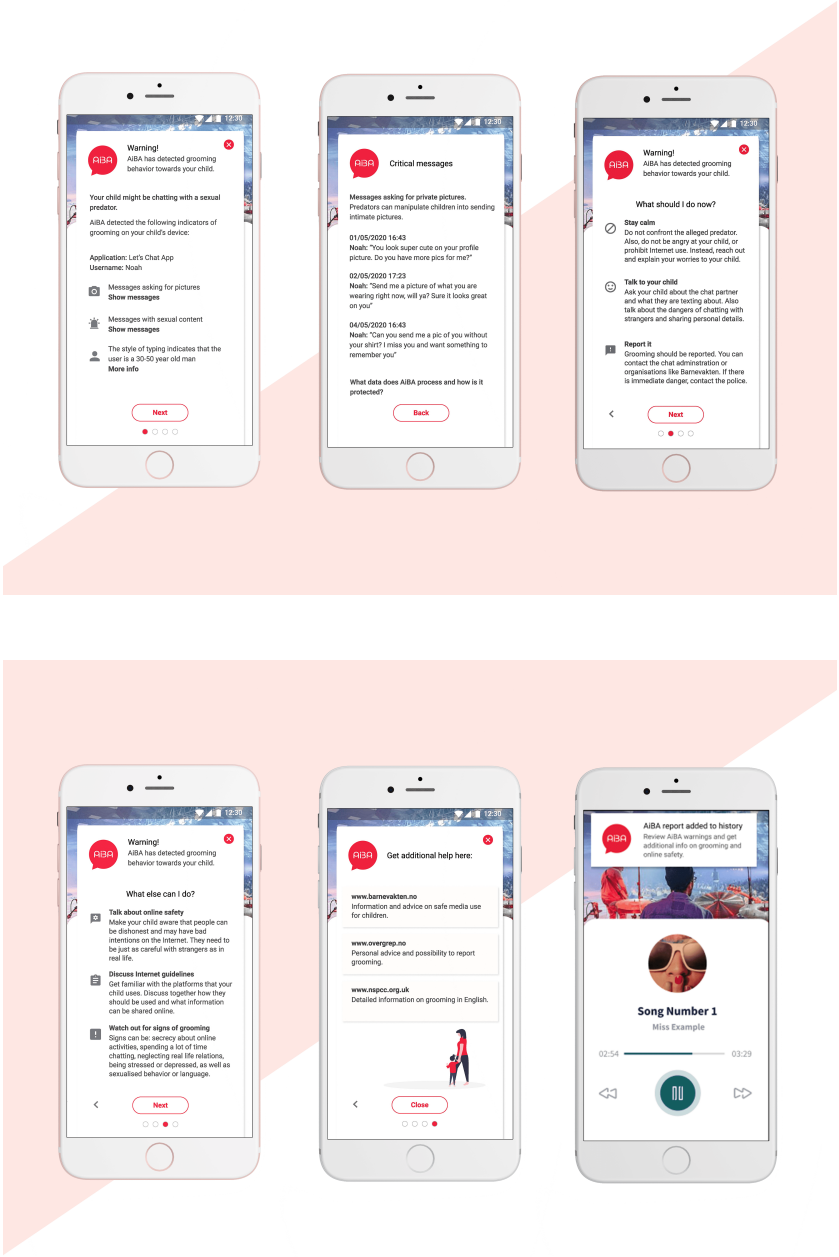
The interactive prototype can be found following this link.





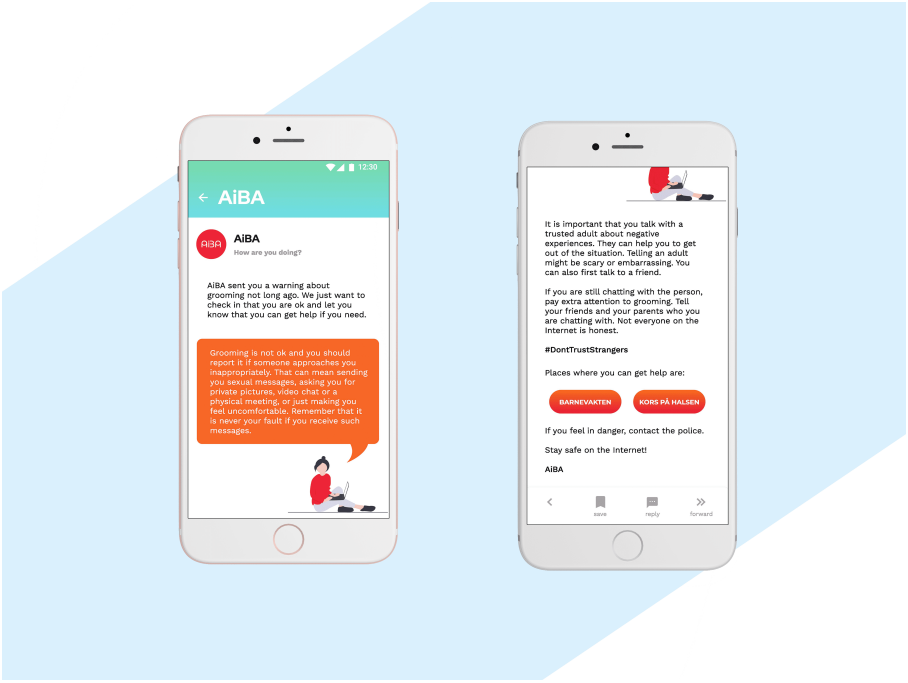
8.6 Clickable Prototype: Warning to Parents

The interactive prototype can be found following this link.



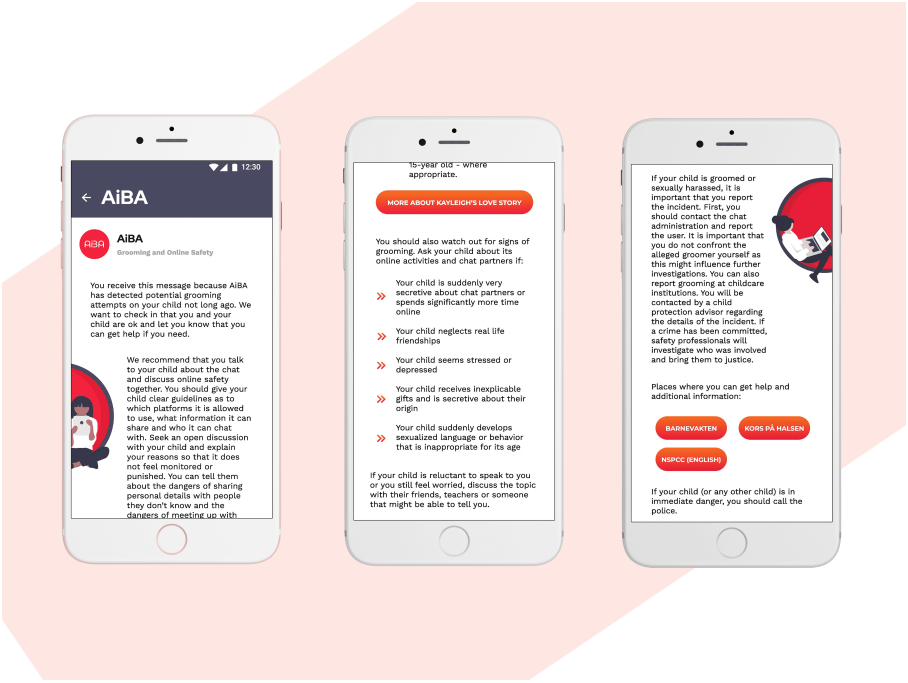
8.7 Clickable Prototype: Recovery Message to Children

The message can be viewed here.



8.8 Clickable Prototype: Recovery Message to Parents

The message can be viewed here.



Lara Raffel

Risk Communication: Sexual Predators in Chat Environments

NTNU
Norwegian University of
Science and Technology