ST. PÖLTEN UNIVERSITY
OF APPLIED SCIENCES

Informatik & Security

fh st.pölten

A Cyber Security teaching concept for children and parents

Master thesis

for attainment of the academic degree of

Diplom-Ingenieur/in

submitted by

Marko Kozlica, BSc

2010619801

in the

University Course Information Security at St. Pölten University of Applied Sciences

Supervision

Advisor: FH-Prof. Mag. Dr. Simon Tjoa

Assistance: -

Declaration

Title: A Cyber Security teaching concept for children and parents

Type of thesis: Master thesis

Author: Marko Kozlica, BSc

Student number: 2010619801

I hereby affirm that

- I have written this thesis independently, have not used any sources or aids other than those indicated, and have not made use of any unauthorized assistance.
- I have not previously submitted this thesis topic to an assessor for evaluation or in any form as an examination paper, either in Austria or abroad.
- this thesis corresponds with the thesis assessed by the assessor.

I hereby declare that

☒ I have used a Large Language Model (LLM) to proofread the thesis.

☐ I have used a Large Language Model (LLM) to generate portions of the content of the thesis. I affirm that I have cited each generated sentence/paragraph with the original source. The LLM used is indicated by a footnote at the appropriate place.

☐ no Large Language Model (LLM) has been used for this work.

Date *Signature*

Kurzfassung

Heutzutage nutzen immer mehr Menschen die Technologie im Zuge der Digitalisierung für verschiedene Bereiche ihres Lebens. Die neue Generation junger Menschen hat die Technologie, insbesondere Smartphones in Kombination mit sozialen Medien, zu einem großen Teil in ihren Alltag integriert. Das macht die Kommunikation zwar einfacher und weniger zeitaufwändig, eröffnet aber auch viele Angriffspunkte für Täter. Es gibt viele verschiedene Arten von Bedrohungen mit unterschiedlichen Auswirkungen auf die Opfer, aber es gibt auch viele verschiedene, meist einfach durchzuführende Vorsichtsmaßnahmen, die einen Angreifer abschrecken und es so schwer wie möglich machen können, Opfer zu werden.

Diese Arbeit konzentriert sich auf die Analyse der Gründe für verschiedene Bedrohungen im Cyberspace, die Kinder betreffen, und versucht, ein geeignetes Unterrichtskonzept zu finden, das bei Kindern eingesetzt werden kann, um ihnen ein Gefühl der Sicherheit zu vermitteln, wenn sie sich im Cyberspace bewegen. Es zeigt auch, dass ein sehr wichtiger Teil dieses Plans die Eltern der Kinder sind, weshalb das entworfene Konzept auch ein Modul speziell für die Eltern enthält, in dem sie über die Bedrohungen und die Möglichkeiten, ihnen entgegenzuwirken, informiert werden, aber auch Ratschläge erhalten, wie sie mit möglichen Bedrohungssituationen für ihre Kinder umgehen können.

Ziel ist es, eine Generation zu schaffen, die möglichst wenig anfällig für Cyber-Bedrohungen ist und somit alle Möglichkeiten der Technologie zur Verfügung hat, ohne dass sie mit Risiken konfrontiert wird, die sie nicht bewältigen kann.

Abstract

Nowadays, more and more people are using technology in the course of digitalization for different parts of their life. The new generation of young people have to a great part integrated technology, especially smartphones combined with social media, into their everyday life. While making communication easier and less time consuming, it also opens up a lot of possible points of attack for perpetrators. There are many different types of threats with varying impacts on the victims, but there are also a lot of different, mostly easily done, precautions which can deter an attacker and make it as hard as possible to become a victim.

This work concentrates on analyzing the reasons for different threats in the cyber space concerning children and tries to find a suitable teaching concept which can be used on children to give them a sense of security when maneuvering through the cyber space. It also shows, that a very important part of this plan, are the parents of the children, which is why the designed concept also has a module specifically for parents where they will learn about the threats and how to counteract them, but will also be advised on how to handle possible threatening situations concerning their children.

The goal is, to ultimately create a generation that is a little susceptible to cyber threats as possible, and therefore have all the possibilities that technology has to offer at their handy, with little to none risks that they cannot overcome.

Contents

1 Introduction

Digital media and the corresponding devices have been an integral part of everyday life for years. Digitalization is processing steadily in all areas of society and with the current rapid developments in the field of artificial intelligence, further upheavals in working life, but also in private life, are already on the horizon. Smartphones have made it possible to transport digital content in mobile form into every area of live and work. The proportion of smartphone Users in Germany is currently 81.1%, with almost everyone under the age of 50 owning one. [1] Almost complete saturation can be observed with people between the ages of 14-49, where 95% of people use smartphones daily. [1]

As smartphones are essentially characterized by the fact that they can be used not only for phone calls, but also for a variety of different everyday activities, they have penetrated everyday life extensively. For example, they can be used to navigate while driving, to keep detailed shopping lists and have also largely replaced handheld cameras due to their built-in powerful lenses. However, communication is still one of the most important aspects of smartphone use, and as mentioned, not only phone calls but using a variety of applications, each offering different multimedia options.

Even though this appears to be a fantastic way of communication, it also has its downsides. Criminals exploit the technical vulnerabilities of devices to misuse sensitive information from private users for their own purpose. However, cyber security is also an important issue in the business world, as such attacks can cause millions in damage. In the police crime statistics for 2021, more than 140,000 cases of Cyber crime were registered nationwide in Germany, and the number is increasing. [2]

At an economic level, the amount of losses due to Cyber crime in Germany was about 203 billion euros in 2022 [3]

The figures in Austria are similar. Here, too, a sharp rise in Cyber crime can be observed over the last five years. While there were initially 19,627 reported Cyber crimes in 2018, the Federal Criminal Police Office reports more than 60,000 Cyber crimes in 2022. [3] It should be noted, that the actual solving rate in this period fell from 37.4% in 2018 to just 33.9% in 2022. It can therefore be assumed that not only more offenders are committing more crimes, but that they are also becoming more skillful in doing so, as the falling

solving rate suggests.

In addition to economically significant offenses such as malware attacks and phishing, there are numerous other offenses that relate directly to the personal level of the victim. These include cyberbullying, cyberstalking and sexual harassment via digital channels [2] These acts also have a significant impact on the victims in the digital space, such as anger, helplessness, sleep problems an inner turmoil. Children and teenagers who are active in the digital space are particularly vulnerable, as they are initially unable to recognize that they are at risk, for example by contacting a perpetrator, even though they are often referred to as “digital natives”.

1.1 Relevance and research question

The topic of this paper is cyber security with regard to the use of digital content by young people between the ages of 11 and 15. Although children and young people often cannot imagine a world without the internet and are adept at using devices and applications, they need guidance on how to navigate the digital space safely.

Simply banning devices and digital content is not the preferred way. In addition, from a developmental psychological perspective, it must be taken into account that the peer group is the main socialization instance at the age relevant here and that digital media also has a socializing function as the most important communication channel for this age group.

However, as aspects of self-expression and self-presentation already play an important role at this age from a psychological perspective, it is even more difficult to categorically prohibit children and young people from using digital content, especially social media.

Parents find themselves in the situation of wanting to allow their children to socialize with their peers, but at the same time having to protect them from any possible danger. As children and young adults are often ahead of their parents in terms of digital affinity, it is all the more complicated to implement effective protective measures. Against this background, the targeted sensitization of children and young adults must have a particularly high priority.

Numerous training programs from a wide range of institutions and initiatives already exist for this purpose and this content is also specifically addressed in schools.

This study will focus on the following question: “What would an effective cyber security training concept for 11 to 15-year-olds look like?”

To get the most effective training, more questions need to be asked:

- What are the current and possible future threats in terms of cyber security?
- What is currently being done to ensure the safety of children on the internet?
- Considering what is currently taught to children, which of the methods used are having the best effect overall?

The aim of this training concept is to teach children and young adults how to use digital media safely and responsibly and keep their private data private. In addition, the target group should be made aware of possible dangers in the digital space. For parents, the aim is to obtain the necessary knowledge to be able to support their children in the best possible way when interacting in the digital space.

1.2 Structure of the work

Chapter 3 of this paper will first lay the conceptual foundations with which we will work. This includes a central definition of the term cyber security and a description of its relevance. In addition, the concept of cyber security will be differentiated according to age groups, with a distinction being made between young people and adults.

The use of the internet and smartphones makes it necessary to think about cyber security in the first place. Chapter 4 therefore deals with this aspect in detail. First of all, the specific conditions of use of digital media by children and young adults will be considered, but in particular the resulting potential risks. In addition, the motivators for Internet and smartphone use, which have already been briefly outlined in the introduction, will be examined in greater depth in this chapter. Directly related to this topic is the question of the extent to which it is possible to influence the usage behavior of young people and how this can be implemented. With regard to usage behavior, a distinction will again be made between young people and parents in order to identify the most important aspects for each age group.

Following the theoretical foundation, Chapter 5 will focus on the cyber training concepts to be examined. First, their benefits will be considered, followed by an examination of international training concepts and their parameters. In a further step, cyber security training concepts in Austria are considered and examined. Chapter 5 concludes with a summary of the common elements of international and Austrian training concepts on this topic.

Based on the results obtained, a cyber security training course for 11 to 15-year-olds will be developed in Chapter 6. This will begin with a comprehensive didactic analysis of the topic, on the basis of which training modules will be created for both children and their parents. It will also attempt to answer the research question posed at the beginning. Chapter 8 concludes with further suggestions for additional research and offers an outlook on the possible future of cyber security training for young adults and parents.

2 State of research

With the rapid spread of the internet, which began in the last 25 years before the turn of the millennium and accelerated thereafter, the need arose to research internet security and cyber security issues [4]. This situation led to the founding of the Institute for Internet Security at the Westphalian University of Applied Sciences in Gelsenkirchen in 2005 with the aim of developing solution-oriented methods to increase Internet security for all target groups [5].
Theoretical consideration and research into the topic had already begun before this and produced the first manuals on the subject, such as "Internet Security" by Fuhrberg et al. [6] which appeared in its third edition in 2001. This book was primarily aimed at a specialist audience of system administrators and network operators, but also at advanced private users.
Early educational materials, such as the BPB's Internet security topic sheets published in 2004, also focused on comprehensible explanations of technical dangers for users, such as computer viruses [7].
In less than two decades after the turn of the millennium, the field of cybersecurity had grown in complexity to such an extent that reductionist approaches had to be used to explain it to laypeople [8].

Social platforms and communication services linked to the mobile device also increasingly became the focus of research. The market launch of the first iPhone in 2007 marked the beginning of a rapid development in the mobile device industry, which embedded media multifuncionality into everyday life and increasingly became a comprehensive communication medium [9]. The development of media use by children and young people is traced, among other things, by the JIM study conducted by the Media Education Research Association Southwest, which has been investigating the media use of 12 to 19-year-olds for 25 years. [10] The study is conducted annually and collects data on, for example, device equipment, media use, duration of use and other aspects, including demographic aspects [10]. Current studies, such as those by Grabensteiner [11], therefore look at the dynamics of instant messaging in lower secondary school in the context of media education and media action.
The complex of topics surrounding digitalization and schools is another focus of research on this topic, as

security and media education can also start there as part of projects or teaching units. On this topic, Elsenau et al. [12] provide a comprehensive overview of digital transformation processes in schools and the conditions for success, also with regard to the accompanying pedagogical discourse.
There was also a differentiation into numerous different areas relating to internet security, such as cryptography. Data protection is an aspect of the topic that was only discovered comparatively late, but is now a factor that became highly significant for the international economy at the latest with the General Data Protection Regulation (GDPR), which was only adopted in 2018 [13].

Ever-advancing technologies, the use of artificial intelligence and encryption techniques can provide more security in the digital space, but at the same time also pose security risks themselves. This is still an ongoing development that can by no means be considered complete at the present time. Current drafts that deal with pedagogy in the age of increasing digitization should also be seen against this backdrop. One example of this is the volume "Umrisse einer Pädagogik des 21. Jahrhunderts im Kontext der Digitalisierung" by Schorb et al. [14], which is intended not only to relate to childhood and adolescence, but to encompass the entire human lifespan.

3 Prerequisites and related work

Cyber security is a topic that originated in the technical field but is now also an important aspect of the social and societal use of digital media.
This chapter will lay the foundations for children and young adults to use the internet safely, starting with a definition of cyber security and the relevance of the topic. It will also look at which security measures play an important role for children and adults.

3.1 What is cyber security?

If you take an initial look at the topic of cyber security, the wide range of terms used in this context is particularly striking. There is talk of cyber security [15], but also of descriptive terms such as internet safety of internet rules for children and young adults. [16] While these terms are primarily concerned with the safe use of the internet and smartphones by children and young adults, the term cyber security has a much broader meaning and refers to the security of information processing in general, which also includes the planning, implementation and organizational security of digital communication [17].
Cyber security is a particularly important topic from an economic perspective, as it is responsible for protecting corporate and organizational networks and preventing unauthorized access, unauthorized data changes or the theft of confidential data [18]. For example, the company Cisco, which offers security solutions in the digital space, defines cyber security as multi-layered protection that extends to individual computers as well as entire networks, programs and data that has been classified as worthy of protection [18]. In this context, cyber security also means that employees, processes and technologies must complement each other to protect data in order to ward off cyber attacks [18]. Companies therefore rely on standardized threat protection management that can identify, investigate and eliminate potential threats [18]
With regards to the topic to be examined in this thesis, we must therefore always speak of cyber security for children and young adults in order to precisely define the field to be examined.

The term cyber crime is also often used in connection with cyber security, In its Cyber Crime Report from 2023, the Austrian Federal Criminal Police Office distinguishes between cyber crime in the narrower sense and cyber crime in the broader sense. The narrow use of the Term cyber crime is always used when criminal acts involving attacks on data or computer systems are committed using information and communication technology [3]. The crimes are directed against the networks themselves or associated devices, services or data [3]. The aim of cyber crime in the narrower sense can also be to damage data or carry out so-called DDOS attacks [3].

In cyber crime in the broader sense, ICT systems are primarily used as a means of committing crimes, but they can also serve as an important infrastructure in the planning, preparation and execution of conventional criminal offenses [3]. Cyber crime in the broader sense therefore concerns a particularly wide range of possible offenses, ranging from fraud to drug trafficking on the darknet and pornographic depictions of minors to cybergrooming or cyberbullying [3]. Cyber crime in the broader sense represents the largest share of cyber crime and is on the rise, as traditional fraud crimes are also increasingly shifting to the internet or digital space as digitalization progresses [3]. For example, text messages were used for data phishing, but alleged delivery notifications from parcel services were also reported, which contained further links to data theft. [3]

3.2 Relevance of cyber security

For companies, the damage caused by cyber-attacks, such as data loss or blackmail through ransomware, can be extremely high. However, cyber security is also highly relevant to society, particularly with regard to the protection of critical infrastructure, which also includes power plants, hospitals and financial service providers [18]

The shift of numerous areas of life and work to the internet, as was observed during the Covid-19 pandemic, led to an increase in cybercrime, which also increased the relevance of combating and investigating it [19]

With regard to the purely economic relevance of cybercrime, ransomware attacks make up a particularly challenging part [19]. The affected companies have to rely on IT experts to reactivate their systems, often with the support of the criminal investigation department and, for example, receiving tips on perpetrator communication on the darknet [19]

In Austria, the cybercrime Reporting Center has been established for over ten years and can be contacted around the clock by victims [19]. It was initially intended as a point of contact for the authorities' own re-

ports, but was increasingly used by citizens, companies, as well as national and international police forces. In 2022, a considerable overall increase in cybercrime in the narrower sense was recorded, which amounted to 44.5% compared to the previous year.

Technical possibilities, such as the anonymization and concealment of financial flows, make fraudulent activities even easier. As more and more people are gaining access to the internet and digital spaces, the number of potential victims is also increasing.

Phishing, ransomware, malware and social engineering are among the most common cyber security issues that can play a role in business, but also for private individuals. Phishing is the sending of emails with fraudulent intent. It should be noted that the emails are often deceptively genuine imitations of trustworthy sources and senders [18]

The aim of phishing emails is to obtain data from the recipient, such as credit card information or login information. It should be noted that phishing is highly geared towards current socially relevant topics and is the main entry point for malware [3]

The term ransomware refers to a type of software that is used to extort money from companies. This malware locks out the rightful owner of the data and only releases access again after a ransom has been paid [18]. It must be considered that the ransom payment is still no guarantee that the data will be recovered. Ransomware attacks are the primary threat to companies and public institutions in the digital space [19].

The term malware is used to describe all malicious software that enables unauthorized people to gain access to a computer or data [18]. Social engineering is a tactic in which criminals attempt to obtain confidential data by simulating communication with trusted individuals. Attackers may attempt to solicit payments or obtain confidential login information. It should also be noted that it is not uncommon for several of these cyber security threats to be used together [18]

In Austria extortion offenses on the internet play an important role in relation to cybercrime. They are punishable under §144, 145 StGB and are often transregional or transnational [19]

Despite the statistics on cybercrime aggregated by the Federal Criminal Police Office, it must be noted that a particularly high number of unreported cases must be expected in this area [19]. It is not uncommon for perpetrators to exploit human weakness such as greed or a desire for recognition or relationships in order to find victims [19].

However, the fear that the case will not or cannot be pursued further also inhibits the reporting behavior of those affected. The effort required by the police to prosecute cybercrime is enormous. Scalable, highly redundant storage solutions are required to cope with the enormous volumes of data [19].

Efficient anonymization services also make it difficult and sometimes impossible to find the perpetrators,

and the prosecution of those often requires international cooperation between the units concerned.

3.2.1 Cyber security for young people

Children and young adults mainly use messaging services on their mobile devices, but also use them to consume music and videos [11]. They also use social networks for communications purposes, as well as learning activities.

In general, it can be stated that the smartphone accompanies the majority of young people in their everyday lives and is used for numerous different communication tasks. Communication on various channels therefore is the basic function of smartphone and media use in adolescence. Against this background, the media activities of children and young people are closely related to a social development that is closely linked to technological progress, but also to processes of change in the media and in society [11].

Knowledge about safety measures on the internet and in digital spaces can be seen as part of media education. This is due not least to the fact that the media landscape has changed significantly as a result of widespread and mobile use of the media [20]. This was accompanied by an expansion of the digital infrastructure, which means that children and young adults today find a completely different media landscape to that of their parents' generation. Today, media and media technologies are generally accessible to children from birth die to the equipment in private households. However, the question of media safety is much older than smartphones and the internet and is based on the modern idea that childhood should be understood as a protected space in which the child must be protected from negative influences. In addition, the image of the child in the modern age is associated with the conviction that it must be pedagogically influenced. However, it is precisely through their omnipresence that digital media manage to largely eliminate this separation between the worlds of children and adults [20].

Historically established child and youth protection restrictions are therefore difficult or often impossible to enforce, as they can be easily circumvented. Digital media use therefore becomes an individual risk/opportunity management for children and young adults, but also for parents.

Parents in particular are often seen as having a duty to provide educational support for their children's media use and to take appropriate measures that take into account the child's needs and stage of development.

However, this claim falls short precisely because the living environment of children and young people is permeated by digital media. Digital media should therefore be seen as part of the socialization process in which the individual deals with social and ecological conditions based on their personal foundations and develops an individual and social personality in the process [20]. The process of socialization does not

only mean the mere adaptation of the individual to the given circumstances, but also the reproduction of society and its renewal. In the context of cyber security in childhood and adolescence, it should be noted that socialization typically develops between family, peers and school. The family is considered the first place of socialization, but with the onset of adolescence and the growing importance of peers, they replace the family as the central socialization instance. As a result, digital communication is becoming increasingly friendship- and interest-driven. [20]. Media use is part of everyday communication and therefore requires pedagogical reflection.

With regard to cybersecurity, however, it is usually almost impossible to ensure that children and young adults are able to use digital media responsibly, which makes preventive measures essential. Children and young adults are exposed to very similar risks in the digital space as adults, but they can still be considered particularly at risk, as attackers can exploit their inexperience to a particular extent [21]. According to the A-SIT, the measures generally recommended as preventive include, above all, making children aware of possible dangers in the digital space, but also protecting their identity.

To this end, children should be told that they must not share sensitive data in order to avoid risks or identity theft. Efforts should be made to make children aware of what data they are allowed to share in the digital space and what consequences phenomena such as cyberbullying can have. Children should also be made aware that, in the anonymity of the internet, not everything that can be seen is necessarily real. Goods purchased online can also turn out to be counterfeit, but digital content can furthermore contain deliberate false statements or forgeries.

When it comes to cyber security for children and young people, many options for action initially lie in the handy of the parents. This includes not only raising awareness of dangers and risks in cyberspace, but also setting up Internet-enabled devices safely. This includes, for example, creating child-safe accounts, but also setting further restrictions such as content filters or screen time. Safeguarding the online activities of children and young people also includes randomly checking their content to determine its suitability and, if necessary, talking to the child about it.

3.2.2 Cyber security for adults

As already indicated, technological advances are creating a media landscape that is not only new for children and young people, but also for their parents' generation. When it comes to their children's media education, they cannot draw on cross-generational experience, but have to moderate and negotiate the appropriation of

new digital media [20]. In general, children and adults can be affected by the same threats in the digital space, especially when adults themselves are new or inexperienced in dealing with online media [21]. Nevertheless, a number of cyber security issues can be identified below that are particularly aimed at adults.
For example, the Federal Criminal Police Office recommends not providing your own payment details for online sales [3]. In addition, any costs for insurance and similar should be strictly checked for accuracy when selling online.
[3]. Even if authorization messages are received via push function on an end device, recipients should check them critically and never confirm them prematurely [3]. For money transactions, the payment service providers offered by the platforms should always be used for online sales [3]. This assumes that you have familiarized yourself with them in detail. Unknown links that purport to come from payment service providers should be checked and, if in doubt, should never be clicked on [3].

Caution should also always be exercised if primary family members contact you on a new telephone number with demands for money [3]. In this case, the Bundeskriminalamt, Federal Criminal Police Office advises checking the old telephone number or other contacts [3]. If damage has been caused by unauthorized transactions, the Federal Criminal Police Office advises informing the bank or credit card provider immediately, who should arrange for a chargeback [3]. In addition, a report should be made to the nearest police station [3].

The Federal Criminal Police Office sees concrete possibilities for damage primarily through fraud, which according to §146 to 148 of the Criminal Code includes obtaining a financial advantage by, for example, misrepresenting facts [19].
Further cyber security advice from the BKA proves to be primarily centered around online payment and goods transactions. The BKA also warns against investment fraud through fraudulent investment sites on the internet [19]. Potential victims are enticed to make payments for supposed investment transactions via fraudulent websites [19]. The recruitment process is usually professionally designed and includes advertisements in the digital space, postings on social platforms, but also mass emails and call center calls [19]. Once payments have been made, they are not invested but disappear into the criminal network, which usually consists of a complex conglomerate of various front and front companies [19].
Other types of fraud that the BKA warns against include various types of advance payment fraud and order fraud [19]. In particular, it warns against the spying out of sensitive data, which can be obtained digitally via phishing, for example, but also through telephone enquiries, personal conversations or even by rummaging

through waste [19].
The BKA also explains the police trick, in which fraudsters pretend to be police officers and demand the surrender of money or valuables for processing [19].
Cyber security can also be seen as a question of digital competence for adults. This is why its promotion has also been recognized by private civic initiatives such as the "fit4internet.at" association, which has set itself the goal of improving the digital skills of the Austrian population as a non-partisan and independent initiative [22]. The purpose of the association initially includes the rapid and standardized development and deepening of skills in relation to the successful management of digitization in business and society [22]. The focus of the association's activities is also on young people, but in particular also on people returning to work and the 60+ generation [22].

The German association "Deutschland sicher im Netz e.V." also focuses on private individuals and aims to support them in using the digital world safely and confidently, cooperating with international IT companies such as Avast, Avira, Telekom and others [23]. The tips that DsiN (2024) offers adults on digital protection mainly include information on securing devices [24]. This primarily concerns securing IT devices with up-to-date antivirus software and strong passwords [24]. However, regularly updating antivirus software is also described as a security measure [24].

According to DsiN, it is important that mobile devices should also be protected with an antivirus program, but the operating system and important apps should also always be kept up to date with updates [24].
Encryption technologies are also described as effective, in particular the encryption of data and hard disks on several data carriers [24]. Email communication should also be protected with suitable encryption technology as part of end-to-end encryption [24]. Avoiding unnecessary data traces on the internet also increases security. For example, search histories in search engines and browser histories in cookies in particular should be deleted regularly [24]. When dealing with social networks, DsiN (2024) recommends making very conscious decisions about the images and information published and also specifying exactly who is allowed to view them [24].

4 Use of the Internet and smartphones by young people and its risks

As we have already seen, the use of smartphones and other mobile digital devices has long since become part of the everyday lives of children and young people. However, the potential dangers that await young users in the digital space are enormous. In this chapter, the potential dangers will be elaborated in more detail, as will the motivators for Internet and smartphone use among children and young people that nevertheless exist. This chapter then deals with the possibilities of influencing the usage behavior of young people, differentiating between the possibilities of peers and those of parents.

4.1 How are children and young adults using the new media such as smartphones?

A study from D. Smahel *et al.* which was conducted between 2017 and 2019 has analyzed how children are accessing the internet today and whether there are specific risks that come with it. According to this study, children in general have access to the internet anytime and anywhere if they have a smartphone, and a majority of children are using it daily or almost all the time[25]. This study was conducted in 19 European countries, which means there are some differences throughout the countries, and even gender makes for a slight difference in the usage of smartphones and the internet in general[25]. The most prominent difference between boys and girls, was that boys overall spent a bit more time online than girls, however, there are some countries where girls are more likely to access the internet daily than boys[25].
In a world where it seems like every single person is using some or all social media platforms at least daily, it is quite interesting to see, that a little over 40% of children between 9 and 16 in France, Germany and Malta never or hardly ever visit those sites[25]. In most of the other countries, more than half of this specific age group is using those platforms at least on a weekly basis[25].

4.2 Potential threats in the digital space

Everyday life and society are permeated with digital technology not only for adults but also for children and young people, resulting in both synchronous and asynchronous communication options [26]. The importance of digital technologies is also reflected in their high significance for young people's leisure activities, with the daily duration of internet use having increased significantly over the last ten years [26].
Social networking platforms and video streaming are considered particularly interesting for children and young people [26].
However, Grabensteiner [11] also emphasizes the great importance of instant messaging among young people, who have been identified as the target group that uses such applications the most [11]. The smartphone is always the carrier of the messaging app and is therefore available everywhere in a mobile way [11]. However, user-generated content is largely without professional regulation in the digital space, as there is no professional pre-selection and discursive examination of the content before it is published [20]. Children and young people have almost unfiltered access to opinions and content shared via social media platforms [20]. This in turn opens the door for criminals to exploit and directly endanger children and young people.

In the study by D. Smahel *et al.* some more risks were identified. They have asked children of different ages a few questions about harm in general and then went on with more specific scenarios. The results to the question "In the PAST YEAR, has anything EVER happened online that bothered or upset you in some way (e.g., made you feel upset, uncomfortable, scared or that you shouldn't have seen it)?"[25] varied throughout different countries, ranging from 7% of children answering "yes" in Slovakia, and 45% in Malta. Another interesting finding was, that most of the countries, the number of children who answered "yes" to the previous question was less than the number of children who reported the more well known risks such as sexting or meeting strangers on the internet. This may suggest, that not all risks that we know of, are self-reported by children as harmful[25]. According to the study, most kids that did report such negative online experiences said it happened more than once, but not on a regular basis[25]. The children that did have such experiences, most often told a friend or a parent about it, but not a teacher or another person who should be expected to help in such situations[25]. Looking at this behaviour, it could be possible that these children are not aware of the potential help they could get from a teacher, which would make it necessary to enhance the trust between the two parties. Another possible point of view would be, that while these children are confiding their problems and possibly fears into their parents, the grown-ups are potentially unable to help in the right way, which would mean, that parents need to be trained as well if not even more so than the children.

4.2.1 Cyberbullying and cyberstalking

Cyberbullying is defined as ongoing, prolonged psychological violence in online spaces [26]. Around 11% of 12 to 13-year-olds in Germany have already experienced cyberbullying, and 13% of this age group have already been victims of cyberstalking [27]. In contrast to cyberbullying, cyberstalking is defined as the stalking of children and young people in online spaces [26].
Cyberbullying is expressed through verbal and psychological bullying, insults and lies and the dissemination of intimate, embarrassing or manipulated photos and videos [28]. Thanks to new technologies, these images can be made available to hundreds of thousands of people in a very short period of time [28]. A distinction is made between verbal cyberbullying, in which teasing, insults, but also blackmail and threats are spread via digital channels such as text messages, emails, chats, social networks and websites [28]. Psychological cyberbullying always occurs when rumors and lies are deliberately spread online, individuals are isolated or blocked in chats or friend requests are rejected [28]. Cyberbullying also occurs when the identity of the victim is assumed by the perpetrators [28].

Typically, cyberbullying is carried out over a longer period of time on digital media and repeatedly conveys hostile or aggressive messages that are published with the aim of harming the victim [28]. Due to the nature of digital media, it is almost impossible to permanently delete this content, which is why the consequences for the victim can be serious and long-lasting [28]. The psychological consequences of such prolonged victimization are manifold and range from trauma to extreme feelings of anger and resignation in the face of the high level of suffering, which can lead to suicide [28]

According to Waasdorp *et al.* there is evidence, that those who are involved in bullying offline, are often also involved in cyberbullying. A very important aspect of cyberbullying compared to offline bullying is, that those specific attacks can occur at any time and even at home, where the victims would usually feel more safe when it comes to bullying in general[30][25]. Another important aspect from a psychological point of view, is that caber bullying has a potentially wider audience and is a lot harder to contain because it is not just between two people but invites a lot of other parties to join[31]. Cyberbullying also has a tendency to be more destructive, as all the parties concerned, especially the perpetrators have no immediate feedback on their actions and therefore can tend to be more disinhibited in their actions, therefore causing even more harm to the victim[32]. The fact that it occurs online, means that the published material is stored there ba-

sically forever, which opens up the possibility of reusing and sharing the content trough different channels such as social media and therefore causing even more harm to the victims[32].

According to Olweus, not all kinds of aggression should be labeled as bullying, because there are defined criteria on what constitutes bullying[33]: "The victimisation is repeated and happens over time; the harm is conducted intentionally; there is an asymmetric power relationship between the aggressor(s) and victim(s)"[32][25]. In the study of D. Smahel *et al.* the kids were presented with the following definition of bullying: *"Sometimes children or teenagers say or do hurtful or nasty things to someone and this can often be quite a few times on different days over a period of time, for example. This can include:*

- *teasing someone in a way, that this person does not like*
- *hitting, kicking or pushing someone around*
- *leaving someone out of things*

When people are hurtful or nasty to someone in this way, it can happen:

- *face-to-face (in person)*
- *by mobile phone (text, calls, video clips)*
- *on the internet (email, instant messaging, social networking, chatrooms)"[25]*

The fact that this definition was necessary for the kids to be able to answer the questions in a meaningful way, may suggest that the first thing to do in a training concept is to make sure, that children and possibly their parents actually know what bullying is and firstly how to detect it and differentiate between the so-called "kids being kids" and actual harmful actions.

Cyberbullying in Austria

In Austria, cyberbullying has been a criminal offense in the Criminal Code since January of 2016 and is referred to as "continued harassment by means of telecommunications or a computer system" [34]. It is essential for the offense that the harassment affects the person's lifestyle in an unreasonable manner and continues over a longer period of time [34]. In addition, the victim's honor must be violated perceptibly for a larger number of people and facts or images of the person's most personal sphere of life must be made perceptible to a larger number of people without their consent [34]. Cyberbullying is punishable by up to one year's imprisonment or a fine of up to 720 daily rates [34]. If the cyberbullying results in suicide or attempted suicide, the perpetrator may be sentenced to up to three years' imprisonment [34].

Contradicting studies on cyberbullying

The European Journal of Developmental Psychology has published a paper by Dan Olweus called "Cyberbullying: An overrated phenomenon?"[35] in which he describes a very different angle on cyberbullying than what might be expected nowadays[35]. The study that was published in 2012 describes an experiment done in the USA and Norway, where they wanted to find out whether cyberbullying is really something to be concerned about, or if the traditional face-to-face bullying is still more popular[35]. The paper goes on to describe, that the media and some researchers that present cyberbullying as a problem that has been more and more present in the last few years, may be wrong in doing so[35]. The author has done studies in which he confronted a large group of students from different schools and different ages with a set of questions about bullying in general and also cyberbullying and their experiences with it[35]. According to these questionnaires that were done over a period of five years, the conclusion was, that cyberbullying, while definitely being existent, is nowhere near as present as the so-called traditional bullying[35].
While these claims may suggest that cyberbullying is nothing to be worried about, there are some things to be considered before coming to that conclusion. For once, the researcher himself writes in his paper, that there could be some factors that may have biased this specific outcome, for example that the children who have been bullied could not exactly differentiate between the two kinds of bullying and therefore may have answered in a different manner as they should have[35].
Another important Aspect to consider is that this was published in 2012, and the studies were conducted even earlier. This could mean, that perhaps in these times, cyberbullying actually was not as popular as it perhaps became later on.

There is however another study, published in the same year of 2012 by Slonje *et al.*, which contradicts the previous study as it assumes that cyberbullying is a very important topic amongst children and young people[36]. This paper explains that there are some difficulties with definitions of cyberbullying in general, because some aspects overlap with the traditional bullying and some other aspects are more difficult to define. For example, if a picture is uploaded on the internet, as an act of (cyber-)bullying, and then later on is distributed by different people, causing even more harm then it is difficult to say who the actual perpetrator is[36].

When it comes to bullying in general and also cyberbullying, the question that may rise at first would probably be about the motives. Varjas *et al.* have found, that there are of course many different motives that can be categorized into two main categories - internal and external[37]. For internal motives they found

revenge, boredom, jealousy, trying out a new persona or redirecting feelings. The external motives are no consequences, non-confrontational or that the target was different in some way e.g., appearance[37].

4.2.2 Summary of the most relevant risks when it comes to the usage of the digital space

- Health Risks
  - There are many Health Risks associated with excessive smartphone usage, such as Eye damage, Headaches and migraine headaches, Back pain, Pain and injuries to the wrists and arms in general due to wrong sitting positions and long rests of the body in static positions [38]
- Psychological and psychical threats
  - There are potential negative psychological impacts that come with excessive usage of computers and internet in general, such as distortion of the reality, becoming resistant to brutality that is presented on the internet, being exposed to sexual, pornographic and pedophile content or being exposed to various sects and even satanists or terrorists[38]
  - These things can cause disruption of social contact and sometimes an increase in aggressive behaviour[38]
- Disorders of sexual behaviour
  - According to Kopczewski *et al.* there are three factors that affect sexuality on the internet:
    - anonymity
    - accessibility
    - unlimited possibilities
  - The anonymity is giving the users a (false) sense of security, which can lead to children exposing themselves to strangers because they think that there are no consequences[38]
- Social risks
  - Hackers: Hackers can steal data, delete critical information and important files, and blackmail people for money[38]
  - E-Commerce: Disclosing secret personal data to a website that is potentially unsafe[38]
  - Cyberbullying: The anonymity of the internet makes it easier for bullies to attack their victims, and also lowers the threshold which can turn more people into bullies[33]
  - Cyberstalking: Cyberstalking is especially dangerous for children, as they often can be manipulated by strangers on the internet and trust them[26]

- Cyber Terrorism: It is more of a global problem than a personal, but still not to be underestimated. Cyber Terrorism can disable or destroy a whole nation in order to change political decisions and gain benefits

5 Overview of cyber security training concepts

Having previously clarified the definition of cyber security and its significance for children, young people and adults, the following chapter examines international and Austrian training concepts that aim to teach cyber security to children and young people in particular.
The benefits of training concepts will first be considered in order to classify their relevance. Next, we will look at some international training concepts, followed by cyber security training concepts that are used in Austria. Finally, at the end of this chapter, the common elements of the training concepts examined here will be described.

5.1 Benefits of training concepts

Awareness is one of the elementary security measures for the secure handling of IT systems. This term describes the awareness of cyber security issues that leads to a change in behaviour towards the secure handling of digital content [15]. Awareness of this topic mus be created at eye level with the recipients, because cyber security is only as strong as the awareness of the people who use these systems [15].
From this perspective, however, people themselves should be seen less as a potential security vulnerability and more as a defensive shield that needs to be developed as a security factor in its own right [15]. For the BSI, the focus of awareness building is on factors such as recognizing fraudulent emails, protection against SPAM and password theft through phishing [15] . Protecting passwords, using a screen lock and recognizing malicious emails are seen as basic components of information-secure behavior [39]. However, the use of unknown USB sticks can also be considered a major entry point for malware [39].

Training concepts for adults primarily emphasize the economic loss potential and, accordingly, training concepts for raising awareness are also geared towards this topic area. Exploiting human vulnerabilities through social engineering is a particularly important factor that plays a major role in spying on internal access data [40]. Cyber security training concepts are particularly successful if they manage to improve the

engagement of those being trained [40].
Methods such as gamification should be used to facilitate learning and create a stronger connection to the learning content among participants [40]. The nudging method can also be used to improve participant engagement. They are repeatedly reminded of the topic of information security by automated emails and motivated to remember the information [40]. Both methods can also be combined to further increase engagement and create a dynamic learning experience [40].
Long-lasting workshops for the pure transfer of information are no longer considered up-to-date and should be replaced by so-called spaced learning [40]. With this method, the knowledge to be imparted is conveyed continuously and in manageable sections as part of a multichannel concept and thus remains interactive, which also has a positive effect on motivation [40].
Training concepts should ultimately lead to employees correctly recognizing attacks and reacting safely [40]. To do this, they must not only practice safe behaviour, but also receive the appropriate tools to protect the organization [40].
Training concepts are intended to achieve a long-term change in behavior among participants that leads to safe usage habits and allows them to reliably identify suspicious activities [40].
Successful awareness-building does not only extend to the professional field, but also continues in the participants' private lives [39]. This is because it is also possible to be exposed to company-related social engineering attacks in private life [39].

5.1.1 International training concepts

In the following, four international training concepts on cyber security will be examined and analyzed with regard to their essential components. The two studies by Ondruskova et al. (2023) [41] and Tosun et al. [42] were obtained via the ERIC database using the search term "cyber security". Given the high number of hits generated, only a sample of suitable training concepts could be drawn, with a focus on raising awareness among children and young people.

In order to be able to compare these concepts and approaches, it is necessary to define criteria by which the comparison will be done. For that, we will need to look at some important factors that an approach should have defined, and therefore is suitable to take into account when comparing. For once, it is important to analyze what the key aspects of the approach are. This is to summarize, what the concept is about. This part can be used to determine, whether this concept is the right one for a specific use case, because it describes

the most important aspects of the concept.

Another important factor is the target group. The target group is defined as the demographic of people that the creator had in mind when designing the concept. It could be described as age, gender, occupation or nationality. In this case, it was chosen to use students, teachers and parents as these were the categories that would be the most interesting in this case.

In order to correctly differentiate between various approaches, it is furthermore necessary to extract the main topic of cyber security that the specific concept is trying to teach. Cyber security is a rather broad term and not specific enough, as there are a lot of categories that are included in this term, thus adding this category to our catalogue of criteria.

Another characteristic, that may not be as significant as others but nevertheless worthy of being included, is the nationality of the targeted audience. While some concepts only concentrate on a national level, others may be more adaptable to a broader, maybe even worldwide audience. This depends on how the concept is structured, whether specific information about the country of origin are necessary knowledge in order to complete the training, or if it is possible to just translate the information given into any language and teach people all around the world.

Apart from the actual content of the training concept, the teaching method is maybe the most important criteria which will be analyzed. There are countless different approaches when it comes to teaching people things in general, for this reason it will be outlined which presented concept uses which teaching method. However, in this part it will not be done in detail but more of a rough overview. The categories that will be available to choose from are: Classroom training, Workgroup, Workshops, Discussions, and some more, if necessary. Since gamification is another big part of teaching methods, this category will be analyzed in a different part of this work, with similar categories.

Tosun et al [42]

The paper refers to the great importance of awareness, which must be associated with the use of the Internet and social media in particular [42].
This study examines the effect of a workshop on cyber security and safe use of social media held in Istan-

bul. The workshop was carried out with the participation and support of numerous institutions, including the Turkish Ministry of Health and Ministry of Communications, but also several universities [42]. The workshop focused on the topics of cyber security and safe use of social media, which was discussed within groups that came together during the event. Each of these groups included 42 teachers from different types of schools and other academics who have specializations in the field of cyber security [42].

In addition, each of these groups included two moderators [42]. The groups were asked to either present current problems on this topic with regard to students, teachers and parents from the province of Istanbul, develop a SWOT analysis with proposed solutions or present proposals for solutions [42].

This was the first SWOT analysis conducted on this topic by the Turkish Ministry of Education [42]. The results were intended to support decision-makers and implementers at individual, institutional and national levels [42].

In the area of strengths, the possibility of reaching parents in the different schools and school levels was identified, using the support of decision-makers, but also parent representatives [42]. In addition, it should be measured and assessed how cyber awareness is positioned among the addressees [42]. Another strength identified was the availability of sufficient documentation and materials on the topic and the availability of sufficient staff to support the process [42].

A major advantage of the school setting was identified as the fact that parents are very easy to reach, on the one hand via parent representatives, but also via teachers and directly with parents [42]. Information can be exchanged at periodic events, but also via the schools' social media presences and websites, as well as via other channels [42]. The fact that schools can be in virtually constant contact with parents makes it very easy for them to pass on information about misbehavior, awareness and development with regard to cyber security [42].

Other strengths in this context include the fact that training materials are already available through the Ministry of Education and can be used to improve permanence among students through animations, drawings and images, but also through gamified content [42]. These are intended to supplement direct instruction by teachers [42].

However, the identified strengths are countered by significant weaknesses, which include in particular a low level of awareness of cyber security on the part of teachers, as well as a low level of awareness of ethical issues related to Internet use [42]. The preference for weak passwords and the use of unlicensed software as virus protection but also as an operating system was also detrimental [42].

The fact that telephones and Internet access were shared by several people was also identified as a disadvantage [42]. Another weakness was the lack of labeling during use and a lack of awareness or respect for the

privacy and personal information of others [42].

Other problem areas on the user side include the presence of email accounts that are not actively used and the short retention of information material on cyber awareness on the school notice board [42]. The lack of two-factor authentication, but also a lack of knowledge of social media in teaching programs were identified as further weaknesses [42]. The lack of awareness and knowledge of the topic was also identified as a weakness in the interaction between students and teachers, but also school administrators and parents [42].

It was also identified as a weakness that both teachers and students do not use social media for educational purposes and that the content disseminated via social media is not sufficiently checked [42]. A general deficiency was also noted that affects the professional activities that deal with social media and education, but it was also noted with regard to jurisdiction that offenses committed there are not yet sufficiently equated with crimes in real life and that many users do not know how to report such crimes [42].

On the other hand, the weaknesses are offset by numerous opportunities that can be seen as positive, including, above all, easy access to the internet and social media [42]. Another positive opportunity arises from the fact that individuals use social media intensively and can easily follow developments in the field of cyber security [42].

In addition, positive opportunities include the fact that threats on the Internet can be easily demonstrated and that there are students who show both interest and skills in the field of information technologies [42].

Occupational fields and business areas that deal with social media and cyber security are also counted as opportunities, as is the existing knowledge of users who need to effectively protect gaming accounts or YouTube channels [42].

Threats were also identified as part of this study. In addition to the existence of fake mobile accounts, these also include the unconscious uploading of mobile applications [42]. Malware is also a significant threat, as is the use of social media from a very young age [42]. It is also a threat if personal information is shared unconsciously on social media and is either misused or deliberately collected by companies [42]. Misuse of WhatsApp by parents is also a cyber security threat, as is using the internet late at night and the lack of a password security policy [42]. The easy accessibility of content on sexuality, violence and hatred for individuals is also highlighted as a threat, as is the concealment of negative experiences already suffered in connection with the internet and social media, for example in connection with cyberbullying [42].

The threat that experiences on social media can have the same meaning as those that have happened in real life is also particularly significant [42].

The authors of the study come to the conclusion that raising awareness of cyber security among students, teachers and school management plays a particularly important role [42].

In addition, the importance of possible cooperation with international companies, NGOs and universities is emphasized, as well as the option of including new courses and new content for existing cyber security courses for students in the curriculum [42].

Ondrušková, Dana& Pospíšil, Richard [41].

The study by Ondrušková *et al.* deals with the cyber security awareness of Czech primary school children. They were tested on their ability to react to risks and dangers in the online environment. The children first completed a pretest and then received training [41]. Finally, the children were asked to complete a questionnaire, which was administered after some time in order to find out to what extent the children were able to recall the information they had learned and apply it in the online environment [41].

The aim of the study was to test the children's cyber security awareness. To this end, the children's ability to recognize or identify risks or risky contexts was to be examined first [41]. In addition, the children's behavior in relation to such risks or risky content should also be examined [41]. The study was intended to determine the current level of cyber security awareness of primary school children, but also to investigate the influence of one-off cyber security training on children's risk awareness [41].

The study was conducted on pupils attending the second grade of Czech secondary schools in the west of the Czech Republic [41]. The study involved 770 children in 35 respective classes from 21 different secondary schools [41]. The test was carried out in the form of three online games with closed questions [41]. A total of 125 students had to be excluded, so the results were obtained by testing 645 students between the ages of 13 and 15. The online questionnaire was designed in a form similar to usual online communication, with questions formulated with an emphasis on the principles of cyber security rules [41]. When completing the questionnaire in Czech, students were asked to either select the correct answers or identify any forms of risky behavior in communication on social media [41]. They were also asked to identify misinformation, with the questionnaire focusing on blackmail and exploitation of trustworthiness [41].

The aim of the questionnaire was to find out the respondents' existing cyber security literacy and to test their awareness of security risks in online communication [41]. The study design was to have the questionnaire filled out by the students first, before they had received an intervention on cyber security in the classroom [41].

One week later, the students attended two lessons of cyber security training in class, which was given by an external person in cooperation with the researchers and teachers [41]. The content of this course included topics such as social media use, security for mobile devices, password security and authentication [41]. In

addition, the risk factors of public WiFi, the Internet and the use of e-mail were addressed [41].
The training was intended to make students aware of information, but also of information security and related areas [41].
The aim was to inform students about the risks of social interactions on the Internet, but also about risk prevention, especially with regard to data and information loss, theft prevention and prevention of misuse of personal data [41]. The teaching was mainly done by frontal teaching, which was combined with demonstrations and the performance of individual tasks on the students' personal devices [41].
In addition, short educational videos were also shown, which mainly concerned the dangers on social media [41].

They were also specifically educated about cyberbullying, cyberstalking and cybergrooming, with all risks illustrated using practical examples [41]. During this training, the students were also asked to create a secure password and edit faces in Photoshop to learn how easy it is to manipulate photographs [41]. With a duration of 90 minutes, the safety training took two school hours [41]. After six months, the participating students were asked to complete a similar questionnaire with modified questions, followed by a final questionnaire after another six months, which concluded the study [41]. Statistical methods were used for the evaluation.
The result showed that the students' level of cyber security remained in the medium range [41]. Although students have basic knowledge of cyber security risks, they tend to be guided by intuition when making decisions [41]. However, this is by no means a reliable, empirically sound method for detecting online risks.
The study has shown that even the intensive cyber security training of the intervention had only a small impact on creating risk awareness among the students [41]. However, five-day interventions have proven to be more promising in comparison with adults than the 90-minute intervention with pupils [41]. More structured training programs are therefore necessary, especially for school age [41]. These results underline the need for robust and complex cyber security education programs [41].
According to the authors of the study, a good cyber security training concept should copy reality and focus on events that can occur in real use [41]. In particular, the weaknesses and vulnerabilities of students of this age should be emphasized [41]. A training concept must have a strong attention-getting approach, as students do not wait for the training concept until they acquire new online skills [41].
A training strategy that is less oriented towards short-term interventions and extends over an entire school year and several subjects also appears promising [41]. With methods such as storytelling, digital comics or games, the transfer of knowledge could be geared towards the preferences of the pupils [41].

klicksafe.de (2023) [43]

Klicksafe is an EU initiative that aims to promote people's online skills [44]. The focus is on numerous and diverse services that support users in dealing critically and competently with the Internet, provide relevant information on many relevant topics and promote self-determined use [44].
The main target group of klicksafe includes people who want to support children and young people in developing their Internet skills, in particular parents and teachers, but also everyone interested [44]. In order to make this support as accessible as possible, the klicksafe website offers a wide range of up-to-date information on the relevant topics as well as tips and materials on the subject areas [44].
In addition, klicksafe offers training courses for children and young people, as well as parents, teachers and professionals who want to communicate the opportunities and risks of the internet [44].

A closer look at the klicksafe.de website shows that it actually provides highly relevant and target group-oriented information on each of the topics already identified as relevant to the cyber security of children and young people. For this reason, a single topic area had to be selected for this report. Cyberbullying was chosen because, as has already been shown, it is a particularly widespread phenomenon among children and young people. On the general information page, klicksafe.de initially offers general information on cyberbullying, but also tips that are primarily aimed at adults such as parents or teachers.

For example, klicksafe.de emphasizes that, regardless of the issue at hand, close parental supervision of children's online activities is necessary [43]. Parents should also keep up to date with the latest technical developments and current trends [43].
When dealing with cyberbullying, klicksafe.de starts with prevention and recommends that parents inform themselves about possible warning signs and prevention options [43]. It is also the parents' task to pass this knowledge on to their children and to encourage a regular exchange about media experiences both within the family and with the school or in discussions with other parents [43].

Parents should also agree clear rules on smartphone and internet use with their children to show them what is allowed and what to watch out for when using the internet [43]. Younger internet users should also be informed about the legal aspects by their parents and know, for example, that they are not allowed to distribute photos of people without their consent [43]. Personal information or videos of people should also never be distributed on the internet [43].

If cyberbullying has already occurred, klicksafe.de believes that parents have a duty to support their child. Offering the person concerned help should be the first step; under no circumstances should they be blamed for cyberbullying in any way [43]. Research into the causes of one's own part in avoiding cyberbullying should only be carried out once the person concerned has gained some distance from the experience [43].

Both victims of cyberbullying and their relatives should not defend themselves directly against cyberbullying with offensive content, but should first try to remain calm and plan the next steps [43]. In a second step, the attacks should be documented, for example by taking screenshots or saving cyberbullying messages that have been sent [43]. This is an important step in proving cyberbullying [43].

Subsequently, cyberbullying should be stopped immediately, for example by blocking or blocking the relevant phone number or contacts [43]. If the cyberbullying occurs on a social platform, in a messenger app or an email program, the incident can also be reported directly to the service [43]. klicksafe.de recommends that parents do not contact the parents of the perpetrators too quickly, as they are likely to protect their children [43].
Involving a less emotionally involved person as a mediator, on the other hand, is more promising in order to start a conversation [43]. However, serious cases of cyberbullying may also require involving the police and reporting the perpetrators [43].

Datz, Margret [45]

The teaching unit "Safe surfing on the Internet" available on the lehrer-online.de website was written by Margret Datz and was found using the search function of the German education server for the search term "Internet safety for children". The lehrer-online.de platform is a material and service portal where teachers from all types of schools can obtain professionally designed and tried-and-tested teaching material. The platform was set up with funding from the BMBF and is managed by a specialist editorial team. The quality-assured materials can be used in the respective lessons without any major preparation and thus contribute to more varied teaching.

The teaching material examined here is aimed at pupils in the third and fourth grades of elementary school [45]. It is a teaching unit that should cover a period of about one week and only requires basic knowledge of computer use from the teachers [45]. The content touches on both general studies and the main subjects of

German and mathematics [45]. The lesson plan includes an initial introductory round, which starts with a brainstorming session on the topic of safety and a discussion of terms [45].
This is followed by a brief presentation of the project, the worksheets and the distribution of the cover sheet [45]. In addition, a PC expert from the class should be chosen and it is explained which Internet address should be called up with an accompanying offer via the browser [45]. At the end of each working day of the teaching unit, the results are summarized in a circle discussion, while a presentation at the end of the project reports on the work results and the progress of the development [45].

With a total of 12 worksheets, a cover sheet and a certificate, which is used at the end of the teaching unit, this concept can be described as quite extensive. It begins with a reflection on the concept of security and refers to both online and offline content [45].
The second worksheet includes a description of how students can access the website with the accompanying offer. The direct comparison between the online and offline world is made in worksheet three, where the students have to recognize and correctly assign terms.
Worksheet four already deals with situations and content that children can encounter on the internet that can scare them. Here, too, a distinction is made between the real city and the virtual Internet, and children are also given behavioral tips on how to deal with frightening situations [45]. Worksheet five looks at legal aspects that deal with freedom of expression, but also with checking content and the behavior of criminals on the Internet [45].
Worksheet six deals with the handling of personal data on the internet and develops six internet rules as well as rules for your own website [45].
Worksheet seven deals with how students should behave towards strangers on the internet and their potential contact requests. Three behavioral tips are developed for this purpose, which should relate to meeting acquaintances from the Internet [45].
Worksheet eight, on the other hand, deals with behavior in chat rooms or forums and the associated risk of being threatened or insulted. Here, too, students are asked to reflect on and assess possible behaviors [45]. They also learn about the email address for youth protection, which is presented as a possible point of contact for experiences [45].
Worksheets nine to eleven are dedicated to the topic of safety from the perspective of the subject German and examine word families such as word building blocks and idioms in this field.
Worksheet 12, on the other hand, uses the perspective of mathematics to calculate the costs of security software [45].

5.1.2 Cyber security training in Austria

Austria also has a number of cyber security training concepts specifically tailored to children and young people. The concepts considered in this section were found during the research for this paper.

Firstly, reference should be made to the safety guidelines for children and young people formulated by the Federal Ministry of the Interior, which also see parents as having a duty to make their children aware of the potential dangers that can lurk in the digital world. According to the Ministry of the Interior, this includes ensuring that children and young people know that nicknames and avatars have nothing to do with the actual person behind them [46]. Parents should also take an interest in the new media and explain to their children as much as possible what social networks, chat rooms and other media are and what dangers may be present there [46]. Parents who show interest and competence are also ideal contact persons for their children, with whom they are also willing to talk about stressful experiences online [46]. According to the Home Office, another topic that parents should discuss with their children is the dissemination of personal information, for example via photos [46]. The distribution of erotic photos in particular can give rise to cybergrooming, cyberbullying or blackmail [46]. Parents should also make it clear to their child that they should end verbal sexual harassment with a clear "no" and practice this together [46].

According to the Home Office, a key role in the prevention of abuse is for parents to inform their children about how they can reduce their risk in the digital space. This includes, for example, not giving any information about their own identity, not publishing erotic photos and never meeting up with chat friends they do not know personally without adult supervision [46].

Setting up and maintaining effective virus protection by parents also plays a role in preventing infection with malware [46].

BKA [47]

Click&Check is a violence prevention program of the Austrian Federal Criminal Police Office that deals with the promotion of responsible use of digital media by children and young people [47]. The focus of this program is on preventive legal information, with a particular focus on youth protection regulations [47].

"Click&Check" is designed for implementation in a school setting, but also strongly involves teachers and legal guardians. The prevention program is aimed at young people between the ages of 10 and 12, but can also be carried out for 13 to 17-year-olds [47]. The aims of "Click&Check" include promoting legal awareness and developing strategies for positive coexistence [47]. It also provides factual information about the dangers of the internet and introduces children to the responsible use of digital media [47]. Action strategies for behaviour in social networks are also practised, expanded and internalized [47]. In addition, "Click&Check" aims to improve communication skills in interactions between students, teachers and parents [47].
The prevention program itself is divided among the various target groups and initially comprises program information for teachers in the form of a teaching unit [47]. This is followed by an information evening for parents/guardians comprising a further teaching unit [47]. The prevention program itself is implemented together with the students within ten lessons [47]. It should be noted that implementation is planned on at least three dates spread over the school year [47].

In terms of content, the focus is strongly on the legal situation in Austria. Already in the initial basic information, a personal examination of the Austrian legal system takes place, whereby the focus is on understanding the necessary terms in connection with the legal provisions [47]. This also includes working through the youth protection provisions, recognizing the differences between the various legal matters and transferring the legal provisions to the young people's world [47]. In particular, the Youth Protection Act is at the forefront of the discussion [47]. The competent use of digital media is also addressed, especially one's own behavior in social networks [47]. Awareness is also to be raised about the importance of privacy on the internet [47].
Learning how to assess opportunities and dangers in the digital space is also one of the topics of "Click&Check". New possibilities and perspectives are discussed and assessed, but in particular the topic of civil courage is also discussed and used to expand one's own options for action [47]. In the topic area of sensitization and internalization, strategies for action when using digital media are trained, which should lead to an expansion of communication skills [47].
In general, it can be stated that the majority of the planned teaching units for "Click&Check" have a strong practical focus and deal with behavior in chats, social media and communicating via smartphone, computer and online games [48]. In particular, the unit on raising awareness and preventing acts deals with the topics of cyberbullying, sexting, grooming, data protection and copyright law [48]. These topics account for a total of six out of ten teaching units [48].

For teachers and legal guardians in particular, the focus is on conveying relevant factual and legal information, with the aim of raising awareness of their role model function [47].

Saferinternet.at [49]. Examples of workshops for children and young people

Saferinternet.at is an initiative that was founded together with the EU to enable children and young people to use digital media safely. In addition to a wide range of online information, saferinternet.at also offers on-site workshops and networking meetings as well as specialist conferences for teachers, educators, parents, interested parties and, of course, children and young people. The spectrum of specialized topics ranges from cyberbullying and digital games to safe cell phone use and safe behavior on social networks [50].
Awareness of information literacy, self-presentation in the digital space and problematic content is also highlighted [50]. Information on copyright, malware, online shopping and internet fraud are also among the topics covered [50]. saferinternet.at [50] also offers specially tailored privacy guides for popular social media platforms. The saferinternet.at [50] service selects strongly according to the respective target group and divides the information into suitability for teachers, parents, young people and youth workers [50].
With saferinternet.at, workshops on cyber security for children and young people can be planned individually but should each comprise at least two teaching units [49]. In addition, the desired workshops can be implemented both online and offline in the classroom [49].
Example workshops include the topic of responsible use. This basic module covers all important topics for children from the age of six, such as the use of social media, digital games, privacy settings in social networks, but also aspects of copyright [49]The evaluation of online content, excessive use, nude photos, blind dates and pornography are also discussed [49]. The focus can be set depending on the interest and use of the students.
In two lessons, another module deals with interaction in the online space, whereby general rules of interaction are assumed and common rules are developed [49]. Other content areas such as copyright, dealing with illegal content such as child pornography and prohibited symbols are also available here [49].
From the age of ten, it is interesting to address the topic of self-presentation on the Internet, whereby it is discussed that some children have been on the Internet since the beginning of their lives via photos of family and relatives and leave their own traces on the Internet with increasing independent use [49]. The handling of self-published content is discussed in the context of possible misuse of the content [49]. The topics of body image, health, job applications and career choices are also discussed in this context [49].
From the age of eleven, dealing with problematic behavior can also be addressed, with possible topics fo-

cusing on prohibited symbolism, child pornography and inadvertent violations of the law [49]. Insulting other participants in a WhatsApp group, sending nude images or adding other people without first agreeing this with the group are also covered [49]. Self-harming behavior and its possible manifestations are also addressed, as are tips on how to deal with it [49].

The workshop on fake news and information evaluation can be held for pupils as young as ten years old. This involves learning and practising how to deal with sources from the internet, with a focus on everyday life and health topics rather than classic fake news [49]. As part of this workshop, pupils learn to recognize false information [49]. Building on this, the topic can be deepened from the age of 14 by specifically analyzing false reports and instructing young people to produce fake news themselves [49]. The typical characteristics of false reports are then analyzed in greater depth and finally used for their own false reports or conspiracy narratives [49]. As part of this three-hour workshop, pupils also learn how to check sources and recognize fake news even better [49].

The workshop on online hate, cyberbullying and moral courage is suitable for young children from the age of six, as it first shows why such situations cannot be tolerated and what consequences online harassment can have for those affected [49]. How those affected can be supported and how action can be taken against hate speech and cyberbullying [49]. The legal aspects of the topic are also addressed [49].

The workshop on dealing with prohibited symbols in the digital space is again suitable for children aged 14 and over. Within two teaching units, knowledge about extremist ideologies is imparted and symbol and prohibition laws in Austria are discussed [49]. Pupils learn to recognize extremist ideologies and world views and to identify the associated symbols [49]. They also learn why sharing such content is problematic and what the consequences can be [49]. It also explains how prohibited content can be reported online [49].

5.2 Common elements of the training concepts

After looking at the training concepts shown here, it can be seen that they are very different in terms of their implementation and target group, although the subject areas are essentially the same.

As far as the age of the target group is concerned, this varies from 6 to 17 years and is therefore aimed at children and young people who have already acquired reading skills and an understanding of the basic rules of social interaction. However, offers such as klicksafe.at [43], the information provided by the Federal Ministry of the Interior and the Federal Criminal Police Office are also aimed at adults, primarily parents, but also teachers who carry out corresponding offers with their pupils at school.

With regard to the duration of the offers, further key distinguishing features can be identified. For example, Ondrušková and Pospíšil [41] work with an intervention that extends over an entire school year, whereas klicksafe.at works with a one-off training course. Datz [45], on the other hand, sets a complete week for the training project and the Federal Ministry of the Interior recommends dealing with the topic on an ongoing basis. The BKA [3] also has a long term approach to its training program and recommends spreading the ten minimum teaching units over three different dates. In contrast, saferinternet.at [50] has designed its workshop to be much smaller, with at least two lessons per topic.
In terms of methodology, the training concepts range from traditional frontal teaching and working on worksheets to working on online tasks and dealing with practical examples. In this context, Tosun et al. [42] clearly recommend aligning the methods to the preference of the students and working with animations, comics and elements of gamification.

In terms of content, the offers are very similar, with cyberbullying in particular standing out as an important topic, followed by cybergrooming and the handling of personal information. Ondrušková and Pospíšil also highlight security guidelines for end devices and risk factors such as the use of public WiFi.

Datz sees the cross-curricular communication of information as another opportunity to use training content with the practise of skills in the main primary school subjects. Both the Federal Ministry, the BKA and saferinternet.at see cyberbullying and cybergrooming as key topics, but also address how to deal with prohibited images and symbols.

With the exception of the klicksafe.at training concepts and the information provided by the Federal Ministry of the Interior, all of the studies and materials examined placed the highest value on creating cyber security awareness, i.e. raising awareness among pupils themselves, but also among parents. In addition, the concepts are aimed at developing skills in cyber security and developing strategies that lead to children and young people moving safely in the digital space. Klicksafe.at and the information provided by the Federal Ministry of the Interior stand out in that they strongly emphasize the role of parents in information and prevention.

5.3 Overview of the chosen concepts with regards to the chosen criteria

Name	Tosun et al.
Key aspects of the approach	Raise awareness, create solutions with SWOT analysis
Target group / suitable age group	Parents, Teachers
Main topic that is being taught	Awareness, potential threats, Managing threats
National or international audience	National in Turkey, but applicable internationally with potential small changes due to different cultures
Teaching method	Workgroup/discussion

Table 5.1: Description of the concepts with defined criteria: Tosun et al.

Name	Ondrušková et al.
Key aspects of the approach	Awareness, ability to recognize and identify risks
Target group / suitable age group	Children
Main topic that is being taught	How to identify risks and how to handle potentially dangerous situations online
National or international audience	internationally applicable
Teaching method	Classroom training

Table 5.2: Description of the concepts with defined criteria: Ondrušková et al.

Name	klicksafe.de
Key aspects of the approach	Promote online skills
Target group / suitable age group	Children, Teachers, Parents
Main topic that is being taught	How to navigate trhough the internet safely, what threats are there, Cyberbullying
National or international audience	Mainly Germany because of the language, but generally applicable internationally
Teaching method	Website, Reading material

Table 5.3: Description of the concepts with defined criteria: klicksafe.de

Name	Datz, Margret
Key aspects of the approach	Information for teachers
Target group / suitable age group	Teachers
Main topic that is being taught	Teaches teachers how and what to communicate towards children regarding safety on the internet
National or international audience	Mainly Germany/Austria
Teaching method	Website, Reading material

Table 5.4: Description of the concepts with defined criteria: Datz, Margret

Name	Click&Check (BKA)
Key aspects of the approach	Made by the Federal Police, specifically designed for children
Target group / suitable age group	Children
Main topic that is being taught	Teaches responsible use of digital media, information about threats on the internet, Focus on legal issues
National or international audience	Mainly Austria, due to legal information that could be different in other countries
Teaching method	Classroom training

Table 5.5: Description of the concepts with defined criteria: Click&Check (BKA)

Name	Saferinternet.at
Key aspects of the approach	Initiative by EU, Safe use of digital media and smartphones
Target group / suitable age group	Children, Teachers, Parents
Main topic that is being taught	Teaches safe and responsible use of Smartphones, digital media in general, awareness on cyberbullying
National or international audience	National in Austria, but also applicable to all german speaking countries/people
Teaching method	Workshops, meetings, conferences

Table 5.6: Description of the concepts with defined criteria: Saferinternet.at

5.4 Overview of Cyber Security awareness games

Additional to the traditional teaching concepts, there are also Cyber Security Awareness games. The following are some of the most suitable games, that can be used in the final concept of this work.
According to a paper by Scott Nicholson, the term gamification is a word that has become symbolic of gratification. The most systems focus on rewarding the players by adding some sort of points, levels or rankings to a real world scenario in order to entice people to engage with the real world to earn these rewards.[51] When we think about it, it may seem unlikely that just by rewarding someone with points, we can change their behaviour in a specific way, but this technique has been known for centuries. A very good example is the thing that most of us do on a daily basis: getting paid to work somewhere, especially if you do not like the job that you are doing. Of course, most of us see it more like a necessity than a rewarding game, but there are still plenty of examples in our modern day world: slot machines in casinos and lottery tickets for instance are designed to give you little to no rewards most of the time, but you still keep playing in hope of getting the big reward the next time. Nicholson also points out, that this reward structure is expected and also accepted in many different life situations. In his paper [51] (The RECIPE for meaningful Gamification) Nicholson explores six elements inspired by game design, and explains the meaning of each one of them:

1) Play - facilitating the freedom to explore and fail within boundaries
2) Exposition - creating stories for participants that are integrated with the real-world setting and allowing them to create their own

3) Choice - developing systems that put the power in the hands of the participants
4) Information - using game design and game display concepts to allow participants to learn more about the real-world context
5) Engagement - encouraging participants to discover and learn from others interested in the real-world setting
6) Reflection - assisting participants in finding other interests and past experiences that can deepen engagement and learning

5.4.1 d0x3d!

Type of game:

Tabletop game

Target audience:

School Workshop

Gameplay:

The game is made for informal computer security education. Some of the main goals as stated by the authors are to engage a new audience, be accessible to everyone, inspire "adversarial-thinking" and improve security literacy [52]. Their goal was to design a simple, challenging and rewarding game that people may play outside the classroom. The name comes from 'd0x3d' which is slang for the practice of intentionally releasing Personal Identifiable Information on the internet for the purpose of embarrassment" [53] a topic which is part of the game.

In this game, the players are white hat hackers such as in Control-Alt-Hack [54]. Different digital assets have been stolen and are held in an adversarial network. The goal of the game is to retrieve these assets. In order to do so, the players have to infiltrate the aforementioned Network, recover the stolen assets and escape without being noticed by the enemy. The enemy is directly encoded in its mechanics, as the network may change its state and the players may have to start over again. Time is, as in reality, also a crucial aspect of the game, because when time runs out, the stolen information gets published to the internet.

5.4.2 GAP

Type of game:

Computer Simulation/Video game

Target audience:

School Workshop, Students, IT-Professionals

Gameplay:

This game is a bit more specific than the previous ones, it is made to improve the awareness about insecure passwords. The development team states in their paper about it, that they had read studies which show a big number of users choosing very weak passwords [55], [56]. They wanted to change this, and since there are many studies, proving that serious (video-)games can help solve such problems [57]–[60], they decided to design a game where the player learns everything about strong and weak passwords, and how to improve the security of a given weak password [61].

The gameplay is pretty easy and self-explanatory. You operate a tank in a 2D maze, where you have obstacles consisting of weaknesses in passwords. To eliminate these, you have to choose the right type of ammunition to defeat the weak password and proceed with the game. If you choose the wrong ammunition you suffer deductions of your own health, and the obstacle is left untouched. As the inventors summarize: The player sees the obstacle, identifies the problem, solves the problem and proceeds with the game [61].

5.4.3 PHISHY

Type of game:

Computer Simulation/Video game

Target audience:

School Workshop

Gameplay:

As it is written in their paper [62], this game was developed mainly as an experiment to see whether or not it is possible to teach enterprise users about the potential risks of phishing emails through a game. The three main goals of this game are to teach how to identify possible phishing URLs, to get familiar with shortened URLs and to search online for different brand names to find legitimate URLs of these companies.

The main character (Sam) gets stuck in a boat on the sea with a tiger in it because he received a phishing mail and fell for it. The objective of the player is, to feed the tiger with fish in order not to get eaten, but to get the fish you first must answer a question correctly.

5.4.4 Budd:e

Type of game:

Computer Simulation/Video game

Target audience:

School Workshop

Gameplay:

Budd:e [63] has been developed primarily for Australian primary schools, and educates children about the risks of going online and the consequences of those risks. It contains several online learning activities and also one offline activity. It has a special section for teachers so that they can see what it is all about and how to teach using Budd:e. It has also a reward system, which is important to make it more appealing for the kids and easier to learn. The objective for the player is to create their own "Buddy (Budd:e)", and in order to reach this they have to master a series of levels which all address different topics that are relevant. Each level unlocks a part of the body which then is used to create the Budd:e.

5.4.5 Enter - IT Security Game

Type of game:

Smartphone app

Target audience:

School Workshop, Students, Just for Fun/Gamers

Gameplay:

This app [64], [65] is made for people that like to sneak into a network or building without being noticed, in order to steal sensitive data. False identities, distraction and open WiFi-Networks are what you will need to win this game. Your target is to infiltrate a company and steal something very important. You will get help from the app on how to navigate through the missions, where you have to solve different tasks in order to succeed. You have a map with all your targets, and you have to steal different things from each target.

5.4.6 NSteens

Type of game:

Computer Simulation/Video game

Target audience:

School Workshop, Just for Fun/Gamers

Gameplay:

NSteens [66] is a website created by NetSmartz Workshop, a part of the National Center for Missing & Exploited Children [67].

It offers a variety of Videos, Games, Comics and Quizzes which help children and teenagers to make safer choices online. There are eight different games on this Website, which are described below:

- Website Warrior
  - In this game there is a website that has been hacked, and it is your task to help the owner defeat the viruses, phishers, and Trojan horse before they ruin everything. There are three levels that you can choose from: normal, hard, and expert. It is designed as a Jump & Run game, where you have to navigate your character through different worlds and fulfill the given tasks in order so save your website.
- Password Plunder
  - In order to be safe, you have to choose a strong password. This game teaches the importance of this by making you build your own password to protect yourself from vikings. You do not have to choose a password, but just be quick enough to collect the letters, but still especially for kids, this seems suitable.
- Rescue Run
  - Rescue Run raises awareness to a very serious matter. You are playing a hero that has to save his friends that are about to meet someone from the internet that they do not know. It is also a Jump & Run game, where you have to evade different obstacles in order to save your friends.
- Stop That Post
  - In this game your job is to stop your friends and family from posting something embarrassing. Of course, it is not a security issue if you post something embarrassing, but the fact that you post something without thinking about it enough, makes it possible to post sensitive Data unintentionally.
- Stop That Post...Again!
  - This is just a new version of Stop That Post.
- Tad's Profile Panic
  - The mission is to keep your friends from sharing personal information, especially on social

networks. You have to solve different puzzles and mazes in order to clean the profiles of your friends from too much personal information.

- Cyberbully Zombies Attack!
  - Here you fight against Zombies, that are trying to steal your identity, post embarrassing pictures of you, send private messages to everyone in school, and eat your brain.
- Gem Jam!
  - This game has nothing to do with Cyber Security and is only there for fun.

6 Cyber security training concept

As has been shown, cyber security training concepts rely to a large extent on creating awareness of the problem among students, but also among parents and sometimes teachers, as the concepts are intended for implementation in the school setting.
This chapter aims to develop a cyber security training program that brings together the best features of existing ones. It will start with a clear analysis to understand how to teach these important topics effectively, followed by creating specific training sections for both young people and their parents.

The first step in this process involves analyzing teaching methods to make sure we can reach every type of learner effectively. We want to make sure that the training is not only informative, but also engaging and easy to understand for everyone respectively.

After the analysis, the training modules will be outlined. These modules will cover everything needed for a basic knowledge in online safety. The idea is to tailor the information so that both young users and also their parents can understand and use in their daily digital lives.

6.1 Didactic analysis

The training concept to be described here on the topic of cyber security is intended to address both the students themselves and their parents in order to achieve the highest possible level of awareness of risks and dangers in the online space on both sides. To this end, the topic can be subjected to a didactic analysis in order to uncover important aspects for implementation.

It is important to note that the didactic analysis is never complete, but must be reassessed for each class or group [68]. The didactic analysis is centered around the five basic questions of present meaning, future meaning, content structure, exemplary meaning and accessibility [68]. They are used as a structuring aid for

lessons and are intended as a reflection and problematization aid for teachers [68]. Even though the work of Oelke & Meyer is intended for teachers in nursing and healthcare professions, the same general principals can be applied in teaching of cyber security.

What are the five basic questions?

- The present significance of a topic should shed light on the importance that the content in question already has in the lives of the learners [68]. In addition, the pedagogical significance of the topic should be recognized.
- The dimension of the future significance of the topic asks what significance the topic will have for learners in the future. [68]
- The question about the structure of the content primarily concerns the specific pedagogical view of the content to be taught or its desired pedagogical significance in the lives of the learners. [68]
- The exemplary significance of the topic, which also needs to be analyzed, asks what general facts or general problem the content in question opens up for the learners [68]
- The question about the accessibility of the topic is also of particular importance. This perspective examines which particular cases or phenomena in the structure of the content could be considered particularly interesting and illustrative for learners [68]

The question of how lessons are conducted is also important for lesson planning. Despite massive criticism, frontal teaching, in which the teacher gives the lecture in front of the class, is still the most widespread form of teaching. [68] In frontal teaching, the teacher takes on the main control, monitoring and assessment tasks. The focus is on communication between teachers and learners, communication between learners is only possible if explicitly requested by the teacher. Teachers questions and student responses are considered the most important staging techniques in frontal teaching, while guided discussions and teacher presentations are the most important patterns of action. It is therefore also characteristic of frontal teaching that it is predominantly received by learners in a seated position, with the blackboard, textbook, worksheets, projector or demonstration objects being added as typical media. [68] Situation-based ad-hoc learning is the exception in frontal teaching, but the knowledge learned is regularly tested in exams or other forms of testing. [68] Repetition, practice and application phases help to ensure learning success [68].

Present meaning	Knowledge about cyber security is very important for young people, as it helps to protect them from dangers in the digital space. Knowledge about cyber security can also help young people to avoid unintentionally violating legal regulations or unintentionally harming others through careless behavior. Cyber security knowledge helps young people to take advantage of the opportunities offered by digital content without exposing themselves to the associated dangers.
Significance for the future	Cyber security will not become less relevant as technical development continues to accelerate and the importance of digitality is expected to increase. This makes it all the more important to lay the foundations of cyber security for young people.
Educational significance	The aim of the training units for young people is to create awareness of cyber security, but also to achieve competence in taking action. Once awareness has been achieved, it can be assumed that young people will engage critically with digital content and are more likely to recognize dangers
Exemplary meaning	The training units are designed to teach young people how to recognize dangers in the digital space. Practical examples are particularly suitable for this.
Accessibility of the topic	Pupils use digital media as an instance of socialization, which underlines the great importance, but also the everyday access to the corresponding media.

Table 6.1: Didactic analysis: Training modules for children

Present meaning	It is very important for parents to enable their children to use digital media safely and positively. In doing so, it is of the utmost importance for them to avert danger from their children.
Significance for the future	As children and young people inevitably engage with digital media in the course of their socialization, it is essential for parents to address cyber security. Parents should see cyber security as a building block of children's education that enables their children to use digital media safely.
Educational significance	The aim of the training sessions for parents is not only to create awareness of cyber security, but also to provide information and skills to support their children on their way into the digital world.
Exemplary meaning	Parents should learn how they can protect their children from dangers in the digital space and which early signals they should look out for in their children.
Accessibility of the topic	Due to the high level of penetration, parents have their own digital practices, but do not always have insight into their children's practices. The training series is intended to give them access to the typical use of digital content by children in order to build on this and achieve awareness.

Table 6.2: Didactic analysis: Training modules for parents

6.2 Insight on different opinions and techniques when teaching children

When it comes to teaching children in general, there are a lot of different opinions on what works best. Different opinions will be discussed in the course of this section, and based on that the most suitable approaches

will be chosen.

In his paper, Ayeyemi is stating that when it comes to teaching children, starting from kindergarten where teachers say that using cartoons to deliver information is has the greatest effect, primary school teachers claim to have the most success with animations and students need stories in order to get their attention in the most efficient way. This goes to show, that, with small adjustments due to age, in general, children need some form of creative input in order for them to get the best learning result possible[69]. The younger the children, the simple and more graphical this input needs to be, but as a rule we can extract that there needs to be some sort of attention grabbing material in order to get the best effect possible. Ayeyemi goes on to say, that many schools are already using a variety of methods, such as hands-on activities, project-based learning and also a blend of traditional lectures [69]. The work also shows, that using games as a teaching method has shown some great results with this specific age group[69]. In general, it is presented that the best results in creating awareness and teaching children the basics of cyber security can be achieved through active learning, because the children have the opportunity to engage with the topic and learn about the possible consequences in a safe space without fearing any actual repercussions in the real life[69].

A more general overview in talking to children is given by Greenberg. In her article she lists a few different ways on how to successfully deliver information to a child and make sure, that they actually receive it. The first and probably most important thing is, that people and especially children can only keep up to about 30 seconds of speaking in their short term memory, which would be about 1-2 sentences[70]. This means, that in order to successfully deliver any information to children, it is necessary to put the information into small chunks, and deliver them accordingly[70]. Another important aspect that is mentioned, is listening to children and validate what they are saying, described as effective listening in this article[70]. This helps the kids in general develop empathy and feelings[70], which helps them in life but is also beneficial when the goal is to create a generation where things like cyberbullying are not as present as they are today.

Another advocate of active listening is found in the Australian parenting website raisingchildren.net.au[71]. This Website is supported by the Department of Social Services and is reviewed by different psychologist on a regular basis[71]. The most significant statement of this website, is that it is essential for building trust, that active listening is used when communicating[71]. According to what was already discussed in this paper, it seems that this type of communication can possibly prevent a lot of causes of cyberbullying and other threats, just by giving the child the attention that it need from the right peers, which are primarily parents but also friends.

What key points can be concluded from this?

- Children are able to learn better, if there is interesting material in form of a story or graphical aids
- The best results can be achieved through active learning
- It is most beneficial, if different teaching techniques are combined, e.g. games and discussions
- Communication with children is important, the kind of communication is essential for success
- When talking to children, a certain trust can be achieved with the use of active listening
- Creating trust lowers the risk of children seeking attention on the internet, potentially exposing themselves to threats

6.3 Important facts to consider for a cyber security training concept

There are a many perspectives to consider when designing a training concept which needs to be compatible for children and parents at the same time. One important step to take, is to differentiate between those two groups when teaching, because it would be very difficult to find a way of teaching that works with children and grown ups, since those two groups tend to have very different learning types. Children may need more visual content, whereas teachers may need more of a theoretical approach in order to develop their own strategy that is best suitable for their specific group of students. Therefore two modules will be created, each of them tailored to its specific target group.
Additionally to the two modules, this section will try and decide which of the previously listed teaching methods will be the most suitable for the training concept.

6.3.1 Target audience for the training concept

This work had already a defined target audience from the beginning, which are children from the ages of 11 to 15, and their parents. When planning a training concept for children, the teachers also can be included as part of the solution, but for this case we will consider the teachers in the same group as the parents, because they often have very similar roles in the life of a child. The concept will not be specialized for a specific nationality, although there may be some cultural differences which may require some adjustments. The gender of the trainees will also not be considered, as the content should address all children and all parents, regardless of their gender.

6.3.2 Most important learning contents that children need to learn

Lamond *et al.* have shown in their study, that there are several weak-points when it comes to children understanding cyber security. A great difficulty it the difference between children's perceived knowledge and their actual knowledge[72]. This not only makes the children more vulnerable to potential threats, but also suggests, that children may not be able to sufficiently self evaluate what they do and do not know, which would rule out any teaching methods that rely on self evaluation.

In general, looking at the previously described concepts and approaches, it looks obvious that the primary concern that needs to be addressed is the awareness, that bad things can happen but at the same time not to spread panic. The children need to be aware of the potential threats and be taught on how to recognize them. After that, they also need to learn, how to correctly react when they find themselves in a potentially dangerous situation. Taking cybermobbing as an example, the approach is a bit different, because there are more social factors included than in a typical attack from a hacker, but nevertheless, there are some things that can be done from the perspective of children in order to deescalate the situation. This specific part of the concept should teach both sides, the potential victim of cybermobbing but also any potential perpetrators, with the hope that it never comes to cybermobbing in the first place.

A very important fact that children need to understand, is that they are not alone in the world, and that they always should have a set of tools to rely on, e.g. knowing how to react in a specific situation can deter potential perpetrators before anything bad can even start do develop. One of the reasons why children are often victims of cyberstalking and cybergrooming, is the fact that they are trusting and vulnerable which is often used by the perpetrators. If we can bring the children to a level of confidence and knowledge, so that they can easily differentiate between a genuine request from someone trustworthy and someone with a hidden agenda, they will be less susceptible of becoming victims.

Another important issue is cybermobbing, which can occur at any time and affect anyone. It is necessary to differentiate between the psychological factors and the technical ones, as there are different guidelines for both of those. This work will concentrate more on the technical aspect, but also give general recommendations. From a technical point of view, it is crucial to teach the children a correct way of using their devices and how to correctly deal with other people online.

Knowledge about cyber security can also help young people to avoid unintentionally violating legal regula-

tions or unintentionally harming others through careless behavior. Cyber security knowledge helps young people to take advantage of the opportunities offered by digital content without exposing themselves to the associated dangers.

6.3.3 Most important learning contents that parents need to learn

When it comes to the role of parents in cyber security awareness, there are multiple things to consider. The most important part is again creating awareness of the possible threats. Regarding knowledge, they themselves need to be taught the basics of cyber security but also need to be able to act accordingly and help their children if a potentially dangerous situation arises.

Regarding the training concept for students, it has been concluded that a continuous approach, e.g. one lasting beyond a single session and ideally spanning the entire school year, is most beneficial. Similarly, such a duration allows for the comprehensive and thorough coverage of the topics on cyber security and should therefore be reflected in the parent training programs. The main purpose of the session is twofold: firstly, to notify parents about the topics of cyber security and, secondly, to provide them with the basic skills for identification of possible threats to their children and adequate responses.

Schools being able to directly communicate with parents using parent representatives and school heads is an essential advantage in ensuring an successful implementation of the training. To lay the necessary foundation for the topic and also gain the parents trust in that matter, an opening parent's evening should be organized, offering at once the basic yet vital information and outlining the planned thematic blocks for the year. These evenings should be organized every other month, and may include talks by expert speakers on important themes as cyberbullying, cybergrooming and protecting the personal data. Given the potential difficulty ensuring the attendance of all parents, these offline meetings should be supplemented with online resources, which may include the recorded talks. In some schools it may be beneficial if, except for the first evening, all these meetings were held online, making it easier for parents to attend.

Nevertheless, those talks from experts should be recorded and provided to the parents in order to ensure that everyone has the opportunity to listen to them again at their convenience. Furthermore, some informational materials should be sent proactively: Either in form of a newsletter, where an email would inform the parents about cyber security tips and practises, or through an online forum or web page, where the school

could post the same for the parents to stay informed and the topic to stay relevant with them. Parents should be provided with enough information on cyber security practises, including securing passwords, antivirus software and restrictions for device use.

If the parents are well informed, they should be capable of guiding their children in the world of the cyber space. As one final recommendation, parents' contact for further requests should be provided in some form, thus enabling them to receive expert advice and assistance when facing a serious or complex cyber-centered situation. Such a connection would ensure that parents remain informed and guided in the cyber-related manners, fostering a safe and informed community.

6.4 Training Modules for young people

According to the analysis above, the main learning outcomes should include increased awareness as to the cyber security field as a whole. Cyberviolence and personal online activity are crucial areas for prevention, which in turn means that understanding basic security measures is very important. A part of these security measures would be setting the privacy settings on the devices, as well as their social media accounts, to a certain level of security.

The training may additionally cover the ability to use limited public networks, sharing devices with others, depending on the age group and whether this content is appropriate and useful. The most important lesson, is to teach the importance and awareness of sharing personal data. Children need to understand the basics of data sharing and the implications of doing so with strangers, which might be risky and can create a lot of potential threats.

Cybergrooming should also be discussed, as it is the major course of inappropriate behaviour, both online and offline. Another important part of the training is creating point of contact where students can get the needed help and information when they need it. These points of contact can be in form of Databases with information, web pages and forums where they can discuss topics with teachers, parents and professionals.

To make the overall discussion of this concept more clear and easy to understand, there should be a number of interactive sessions throughout the training, such as scenario based role-playing exercises or games and

group discussions on the perceived difficulties and solutions, which should enable the children to share their experiences with their peers. It is important to prepare the topic in such a way, that the children are able to comprehend the lesson, which can be achieved with visual aids such as presentations, charts and videos. Another possible method to make complicated content more understandable for children are games that are made to raise awareness and train the players in certain parts of cyber security, such as those presented in this work.

Furthermore, creating an environment of general discussion within the classroom will lead to a situation where students will feel free to discuss the cyber security issues that affect them. This can be facilitated by teachers and trainers who can make their students know that they are available and willing to attend to any areas of concern. Moreover, such exercises can be used by teachers to create a bond with the students making them comfortable talking about their experiences to their peers. The program can include regular assessments and feedback exercises which can be used to check the level of progress along, to ensure that training is in line with the students' needs. Assessments can be in the form of a quiz, project work or it can be essays that require students to tell what they know about cyber security. However, depending on the specific group of children, it may be beneficial of these assessments did not have the characteristic of a work assignment, but more of an open discussion or a quiz that can be taken together as a class or in small groups. This would further enhance the trust between the students as they would work together in finding the correct answers.

At the end of the day, the target of the training is to equip the students with the theoretical and practical capacity to guard their beings in the cyber world and ultimately build a generation not only familiar with technology but also capable of being resilient in cyber space at all times.

Short listing of the training module for young people

- Raising awareness: Use examples from the real world to raise awareness
- Keep it simple: focus on the topics that children actually need
- Show them why keeping their personal data secure is important
- Show easy tips and tricks to increase security of their personal data
- Present ways how to identify potential threats in the cyber space
- Create discussions in order to further enhance the participation of children in the matter
- Build a solid network of information that children can turn to when they need help
- Ensure that the children are aware of different options of where to get help in case they need it

6.5 Training modules for parents

To make the parent training part of the program a more effective cycle, it is essential to include a variety of interactive and participatory elements. Apart from the first parents' evening and themed sessions, the program should also involve hands-on workshops where they can practise the measures themselves and thereby raise the awareness and skills. For instance, these activities could include identifying phishing emails, installing and managing antivirus solutions, or concluding a privacy check-up.

Furthermore, it is a good idea to include case studies into such training classes and show real-life examples. This way parents will understand the practical implications of cyber threats better and will be more aware of possible consequences, meaning they are more likely to take the necessary actions. New case studies based on recent cyber incidents could be interesting as they show this to be a very current topic, but also, combined with older ones, it can help to describe the most known vulnerabilities and the suggested response strategies.

With the aim to secure accessible and low-cost ongoing learning and support, the program should also establish and online portal, just as described for the children. This online portal should be featured in all the documentations and be presented as a reference for parents that they can use at all times. The portal should contain tutorial videos, a collection of information material, articles on new trends and what to look out for, FAQs and potentially also tests. A very important part of this portal should be a forum or chatroom where not only children but also parents can ask questions, or write about their own experiences for all other parents to see and learn from it or help in case of need. The crucial part is to create a community of parents, teachers and professionals, that functions as a holistic system, in which every member always can rely on getting help and information that they need.

It is also important to state, that in order to be able to help their children navigate through the dangers of the cyber space, the parents are not required to become technical experts on cyber security. Most often it is enough to understand the basics of what can happen and how to prevent it, and in any other case they only need to know, who to ask. In particular, they could ask their questions in such an online platform and they can rely on other parents, teachers or professionals to help them along the way and offer solutions.

It is important that regular feedback is given concerning the training and all parts of the system, in order to ensure the effectiveness of the program and address possible problems. This feedback will enable the

organizers to adapt the details of the training in such a way, that is most beneficial for all parties concerned. Such an educational solution consisting of comprehensive content, practical applications, community building and continuous improvement will help lead to a more safe digital space for parents and children.

Short listing of the training module for parents

- Raise awareness: Through examples of what is currently happening in the world of cyber attacks, especially concerning children
- Soften the potential initial shock: Explain that these are Situations that can happen, but can also be avoided just as easily
- Explain the process: What will they learn, what is expected of them?
- Show them how to recognize that something may be going on with their children
- Show them how to react if they find something or their child comes to them
- Open the topic up for discussion, give the parents a chance to ask questions throughout

7 Discussion

Digitization is one of those processes that with time becomes more important for both society as a whole but also at an individual level. Among the most impacted are children and young people due to the widespread use of the internet that nowadays, has an influence on almost every aspect of their lives. Children use social media and chatrooms to communicate with peers, but they also may face potential risks with using the same. Among those risks and potential threats are cybergrooming, cyberbullying and also the potential of excessive consumption of digital content which may alter their perception of reality in certain aspects of life. Thus, it should be understandable that the issue of cybercrime and how to protect yourself from possible threats should not be limited to corporations, but rather be extended to everybody, especially children as they hold the status of being potential victims who are not always capable of defending themselves in certain scenarios. Moreover, the easiest victims of perpetrators when it comes to cybergrooming, and more generally speaking, sex offenders for example, are in fact children as they are more easy to be manipulated into believing the lies that are told to them by the offenders.

Another important role is played by the parents, who oftentimes do not have the knowledge or capabilities to help their children, but also do not always succeed in monitoring the behaviour of their child appropriately which in some cases may even benefit the perpetrators. This goes to show, that only educating children will most likely not be enough, but also giving the parents their share of information end experience should be considered.

After conducting the analysis of currently existent teaching modules and concepts, combined with different statements and reports of the current usage and involvement of children and parents in the cyber space, it became apparent, that any new training concept should, as a primary part, involve raising awareness. It is necessary to bear in mind that one should not only explain to the children the facts and associated risks when using the internet and social media for instance, but also establish a certain norm of behaviour in order to mitigate some of the risks they could be faced with on a daily basis.

If we take cyberbullying into consideration, we can extract some of the reasons behind such actions. One of those reasons is the feigned feeling of anonymity in the digital space, which can lead to people, especially

children, getting carried away and sometimes even unconsciously participate in bullying others without ever thinking about possible consequences. This can be counteracted and prevented, if the children are taught that the cyberspace, while being digital and not something that can be physically perceived, can still have consequences in the real world and oftentimes those consequences show themselves at a later time, but in a substantially more impactful way regarding the victims. If we educate the children from a young age, by showing them real life examples, and also teaching them empathy, and correct ways of communicating with each other along the way, it could lead to a new generation of people, where such threats as cyberbullying no longer exist in the future, or at least are significantly less present.

As already described, while being the most obvious choice, it is not enough to only concentrate on the children themselves when trying to achieve such a goal. The parents and teachers also play a very important role in this scenario, as they are the ones that form the children throughout the most crucial time. It is essential, to get the parents' attention in a program like this, as they also need to learn certain technical aspects of cyber security, but more importantly, they need to be able to identify risks that their child is potentially exposed to and react in a manner that will help the child in the short run, but also deepen the trust and bond that they have, getting the benefit in the long run by developing the child into an individual that is able to navigate themselves safely through the cyber space, and use the internet and all the applications to their advantage, while minimizing the risks they are exposed to.

After thinking about all the goals that need to be achieved with this training concept, it becomes apparent that the suggested option of expanding the training throughout the whole school year is really necessary. This opens up options for parents to also participate in certain exercises together with their child, but also independently. It also creates the possibility, to track the progress and success without the stress of being forced to do it in a small time frame. Combined with the suggested collection of information material and other resources, it should be a teaching concept that provides the desired outcome.

8 Conclusion

Cyber security can be considered a key topic in a special way, as it is permeating everyday life together with advancing digitization and will become an important aspect of general knowledge. As the use of digital content has become more integrated in our social life, especially with children, it is not suitable for parents to simply ban or keep them away from the devices. It is necessary to find a way for children to experience the benefits of having the cyber space while minimizing the risks that come with it.

The creation of awareness of the risks of the digital space on the part of children and young people as well as on the part of parents should therefore be considered in the context of the most comprehensive media education possible, which leads to a high level of media literacy among the addressees, prevents dangers and allows them to take advantage of the opportunities offered by the new communication media. Furthermore, children should also learn to deal with social media platforms in a critical way in this context and recognize, that these are highly commercialized media offerings that are operated by companies with the aim of making a profit. This aspect should also be taught in order to achieve the highest possible level of responsible use of such services, and to prevent the children from being exploited through those channels.

Only by teaching children at a young age on the possibilities and possible threats when using the internet or, more specific, social media platforms, combined with educating them in countermeasures, will they be able to successfully use those new methods of communication to their advantage, while minimizing the risks that usually come with using the internet in any way.

By using the described training concept, an opportunity is created to not only teach the mentioned technical backgrounds to children and parents, but also create a community that has the potential to be strong enough as a whole to minimize risks to a level where every part of the community can feel safe. This is achieved not only by bringing people together, but also by building trust between them and showing the children especially, that they can trust their parents, their teachers and also their classmates when having a problem. In order for the program to be successful however, every member of this described community has to do their part to the fullest extent, be it children making an effort to learn about different threats and how to defuse a potentially dangerous situation, or parents learning how to trust their children and how to safely monitor

their activity in order to help them along the way.

8.1 Future Work

Future research should concentrate on expanding this work by taking into account more programs that are potentially already included in the curriculum in some schools. It would be beneficiary if, taking this work as a basis, a concrete training module would be developed and tested in schools. There were time limitations in place that unfortunately disallowed this work to go as far as that. Creating a training module would need some of the work that is presented in this paper, but also would require some experts on the matter in the region that are available and willing to be a part of it. It would be interesting to accompany the training concept outlined here with follow-up studies after successful implementation in order to identify further optimizations and to achieve the greatest possible long-term and sustainable awareness of cyber security among students.

Another possible path of future research could concentrate on including more cyber security games in such a program, and examine the different parameters needed in order to implement a successful program. If such a module were to be implemented, it would be interesting to compare the results of those two concepts and further investigate if a different combination of the parts of each module would work better.

This work concentrated on a specific age group of children and their parents, this was because there were only few concepts found that really combine teaching the both. Choosing children over the age of eleven was not a coincidence, as this is currently the age where they are mostly fixated on their digital devices and in the future this age threshold could sink to even younger children, making it necessary to start teaching children at even younger ages. In that case, the concept would need to be changed in order to appeal to a younger audience, possibly making the content easier to understand and changing certain parts that require capabilities that younger children do not have out for ones that they are able to comprehend.

List of Tables

Acronyms

BKA	Bundeskriminalamt, Federal Criminal Police Office
BMBF	Bundesministerium für Bildung, Wissenschaft und Forschung
BSI	Bundesamt für Sicherheit in der Informationstechnik
DDOS	Distributed Denial of Service
GDPR	General Data Protection Regulation
IT	Information Technology

Bibliography

[1] F Tenzer, "Anteil der smartphone-nutzer* in deutschland in den jahren 2012 bis 2021," *online] https://de. statista. com/statistik/daten/studie/585883/umfrage/anteil-der-smartphonenutzer-in-deutschland/*, 2022.

[2] Philipp Müller, Arne Dreißigacker, and Anna Isenhardt, "Cybercrime gegen privatpersonen," *Ergebnisse einer repräsentativen Bevölkerungsbefragung in Niedersachsen*, 2022.

[3] Bundeskriminalamt. "Cybercrime report 2022." Last accessed: 2024-03-10. (), [Online]. Available: `https://bundeskriminalamt.at/306/files/Cybecrime_2022_V20230517_webBF.pdf`.

[4] Albrecht Beutelspacher, Heike B Neumann, Thomas Schwarzpaul, Albrecht Beutelspacher, Heike B Neumann, and Thomas Schwarzpaul, "Internetsicherheit," *Kryptografie in Theorie und Praxis: Mathematische Grundlagen für elektronisches Geld, Internetsicherheit und Mobilfunk*, pp. 277–288, 2005.

[5] Institut für Internet-Sicherheit - if(is). (), [Online]. Available: `https://www.internet-sicherheit.de/ueber-uns/das-institut/` (visited on 03/17/2024).

[6] Kai Fuhrberg, Dirk Häger, and Stefan Wolf, *Internet-Sicherheit*. Hanser, 2001, ISBN: 3-446-21725-8.

[7] Ludwig Janssen. "Themenblätter im unterricht nr. 33 - internet-sicherheit." (), [Online]. Available: `https://www.bpb.de/shop/materialien/themenblaetter/36729/internet-sicherheit/` (visited on 03/17/2024).

[8] Hannfried Leisterer, *Internetsicherheit in Europa: Zur Gewährleistung der Netz-und Informationssicherheit durch Informationsverwaltungsrecht*. Mohr Siebeck, 2018.

[9] Mirjam Oertli, *" Wer auf dem Handy kein gratis Internet hat, ist tot!": zur Relevanz des Smartphones für Kinder an der Schwelle zum Jugendalter*. kopaed, 2019, ISBN: 9783867365628.

[10] Medienpädagogischer Forschungsverbund Südwest, "Jim-studie 2019: Jugend, information, medien," *Basisuntersuchung zum Medienumgang*, 2019.

[11] Caroline Grabensteiner, *Medienbildung im Medienhandeln: Rekonstruktionen am Beispiel von Instant-Messaging-Gruppen in Schulklassen*. Springer, 2023.

[12] Detlef von Elsenau, Hager Sarx, Wolfgang Strauß, and Alex Torka, *Digitalität in Schule und Unterricht: Ein Leitfaden für die Praxis*. Berlin: Cornelsen, 2021, ISBN: 3589168129.

[13] Europäische Kommision. "Eu-datenschutzvorschriften." (), [Online]. Available: https://commission.europa.eu/law/law-topic/data-protection/eu-data-protection-rules_de (visited on 03/17/2024).

[14] Bernd Schorb, Anja Bensinger-Stolze, Fred Schell, Birgita Dusse, and Wolfgang Antritter, *Umrisse einer Pädagogik des 21. Jahrhunderts im Kontext der Digitalisierung*. kopaed, 2022, ISBN: 978-3-96848-075-6.

[15] BSI. "Awareness." (), [Online]. Available: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Faktor-Mensch/Awareness/awareness_node.html (visited on 03/10/2024).

[16] Schau hin. "Tipps für ein sicheres internet für kinder." (), [Online]. Available: https://www.schau-hin.info/tipps-regeln/sicheres-internet-fuer-kinder (visited on 03/17/2024).

[17] Bundesnachrichtendienst. "Sichere die digitale zukunft." (), [Online]. Available: https://www.bnd.bund.de/DE/Karriere/Ausbildung_Studium/Master/Cyber-Security/master_node_cyber.html (visited on 03/17/2024).

[18] CISCO. "Was ist cybersicherheit?" (), [Online]. Available: https://www.cisco.com/c/de_de/products/security/what-is-cybersecurity.html (visited on 03/17/2024).

[19] Bundeskriminalamt. "Betrügereien verhindern." Last accessed: 2024-03-10. (), [Online]. Available: https://www.bundeskriminalamt.at/202/Betrug_verhindern/start.aspx.

[20] Rudolf Kammerl, Claudia Lampert, Jane Müller, Katrin Potzel, Andreas Dertinger, and Paul Petschner, "8. medienbezogene sozialisation in der familie: Einordnung und fazit," in *Sozialisation in einer sich wandelnden Medienumgebung*, Nomos Verlagsgesellschaft mbH & Co. KG, 2022.

[21] A-SIT Zentrum für sichere Informationstechnologie – Austria. "Top 10 it-sicherheitstipps zum schutz von kindern im netz." Last accessed: 2024-03-10. (), [Online]. Available: https://www.onlinesicherheit.

gv.at/Services/Technologie-Schwerpunkte/Kinder-und-IT-Sicherheit/Top-10-Kinderschutz-IT-Sicherheit.html.

[22] fit4internet - Verein zur Steigerung der digitalen Kompetenzen in Österreich. "Fit4internet." (), [Online]. Available: https://www.fit4internet.at/view/verein (visited on 03/10/2024).

[23] DsiN. "Sicher im netz." (), [Online]. Available: https://www.sicher-im-netz.de/ueber-uns (visited on 03/10/2024).

[24] DsiN. "Digitaler selbstschutz im ueberblick." (), [Online]. Available: https://www.sicher-im-netz.de/node/2225 (visited on 03/10/2024).

[25] H. Machackova D. Smahel and G. Mascheroni. "Eu kids online 2020: Survey results from 19 countries." (), [Online]. Available: https://www.lse.ac.uk/media-and-communications/research/research-projects/eu-kids-online/eu-kids-online-2020 (visited on 03/27/2024).

[26] Olivier Steiner, Paul Burkhard, Rahel Heeg, and Kay Biesel, "Risiken des aufwachsens in einer kultur der digitalität: Einführung," *Digitale Kindeswohlgefährdung: Herausforderungen und Antworten für die Soziale Arbeit*, p. 7, 2023.

[27] Martin Kern Steffen Zdun. "Aktuelle zahlen zur cyberkriminalität von jugendlichen." (), [Online]. Available: https://www.dji.de/veroeffentlichungen/aktuelles/news/article/aktuelle-zahlen-zur-cyberkriminalitaet-von-jugendlichen.html (visited on 03/10/2024).

[28] Kay Biesel, Paul Burkhard, Rahel Heeg, and Olivier Steiner, "Digitale kindeswohlgefährdung: Eine begriffliche annäherung," *Digitale Kindeswohlgefährdung: Herausforderungen und Antworten für die Soziale Arbeit*, p. 20, 2023.

[29] Tracy E. Waasdorp and Catherine P. Bradshaw, "The overlap between cyberbullying and traditional bullying," *Journal of Adolescent Health*, vol. 56, no. 5, pp. 483–488, 2015. DOI: 10.1016/j.jadohealth.2014.12.002.

[30] Robert S Tokunaga, "Following you home from school: A critical review and synthesis of research on cyberbullying victimization," *Computers in human behavior*, vol. 26, no. 3, pp. 277–287, 2010.

[31] Jan Pfetsch, "Who is who in cyberbullying? conceptual and empirical perspectives on bystanders in cyberbullying," *A social-ecological approach to cyberbullying*, pp. 121–149, 2016.

[32] Robin M Kowalski, Gary W Giumetti, Amber N Schroeder, and Micah R Lattanner, "Bullying in the digital age: A critical review and meta-analysis of cyberbullying research among youth.," *Psychological bulletin*, vol. 140, no. 4, p. 1073, 2014.

[33] Dan Olweus, "Bullying at school: Basic facts and effects of a school based intervention program," *Journal of child psychology and psychiatry*, vol. 35, no. 7, pp. 1171–1190, 1994.

[34] Österreichische Regierung. "Gesetzliche lage." (), [Online]. Available: https://www.oesterreich.gv.at/themen/bildung_und_neue_medien/internet_und_handy___sicher_durch_die_digitale_welt/3/1/Seite.1720720.html (visited on 03/10/2024).

[35] Dan Olweus, "Cyberbullying: An overrated phenomenon?" *European Journal of Developmental Psychology*, vol. 9, no. 5, pp. 520–538, 2012. DOI: 10.1080/17405629.2012.682358. eprint: https://doi.org/10.1080/17405629.2012.682358. [Online]. Available: https://doi.org/10.1080/17405629.2012.682358.

[36] Robert Slonje, Peter K. Smith, and Ann Frisén, "The nature of cyberbullying, and strategies for prevention," *Computers in Human Behavior*, vol. 29, no. 1, pp. 26–32, 2013, Including Special Section Youth, Internet, and Wellbeing, ISSN: 0747-5632. DOI: https://doi.org/10.1016/j.chb.2012.05.024. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0747563212002154.

[37] Kris Varjas, Jasmaine Talley, Joel Meyers, Leandra Parris, and Hayley Cutts, "High school students' perceptions of motivations for cyberbullying: An exploratory study," *Western Journal of Emergency Medicine*, vol. 11, no. 3, p. 269, 2010.

[38] Marian Kopczewski and Agnieszka Napieralska, "Cyber space–risks to children and young people–research results," *Scientific Journal of the Military University of Land Forces*, vol. 50, 2018.

[39] Kristin Weber, Andreas E Schütz, and Tobias Fertig, "Grundlagen und anwendung von information security awareness," 2019.

[40] sosafe. "Verhaltenspsychologie als erfolgsfaktor in security awareness trainings." (), [Online]. Available: https://sosafe-awareness.com/de/blog/verhaltenspsychologie-als-erfolgsfaktor-in-security-awareness-trainings-die-5-groessten-vorteile/ (visited on 03/10/2024).

[41] Dana Ondrušková and Richard Pospíšil, "The good practices for implementation of cyber security education for school children," *Contemporary Educational Technology*, vol. 15, no. 3, ep435, 2023.

[42] Nilgün Tosun, Murat Altinöz, Emil Çay, Turan Çinkiliç, Sevinç Gülseçen, Tülay Yildirim, Muhammed Ali Aydin, Bilgin Metin, Zerrin Ayvaz Reis, and Nafiz Ünlü, "A swot analysis to raise awareness about cyber security and proper use of social media: Istanbul sample," *International Journal of Curriculum and Instruction*, vol. 12, 2020.

[43] klicksafe. "Cybermobbing – rechtzeitig erkennen und handeln." (), [Online]. Available: https://www.klicksafe.de/news/cybermobbing-rechtzeitig-erkennen-und-handeln (visited on 03/10/2024).

[44] klicksafe. "Die initiative klicksafe." (), [Online]. Available: https://www.klicksafe.de/die-initiative (visited on 03/10/2024).

[45] Margret Datz. "Sicher surfen im internet." (), [Online]. Available: https://www.lehrer-online.de/unterricht/grundschule/sachunterricht/sache-und-technik/unterrichtseinheit/ue/sicher-surfen-im-internet/# (visited on 03/10/2024).

[46] Brunhofer Julia and Herbert Zwickl. "Pädokriminalität." (), [Online]. Available: https://bmi.gv.at/magazin/2022_01_02/Paedokriminalitaet.aspx (visited on 03/10/2024).

[47] BKA. "Jugendprogramme." (), [Online]. Available: https://www.bundeskriminalamt.at/205/start.aspx (visited on 03/10/2024).

[48] BKA. "Click&check, präventionsprogramm." (), [Online]. Available: https://www.bundeskriminalamt.at/205/files/FlyerClickundCheck.pdf (visited on 03/10/2024).

[49] Saferinternet. "Beispiele workshops für kinder und jugendliche." (), [Online]. Available: https://www.saferinternet.at/services/veranstaltungsservice/zielgruppen/beispiele-workshops-fuer-kinder-und-jugendliche (visited on 03/17/2024).

[50] Saferinternet. "Saferinternet - das internet sicher nutzen." (), [Online]. Available: https://www.saferinternet.at/ (visited on 03/17/2024).

[51] Scott Nicholson, "A recipe for meaningful gamification," in *Gamification in Education and Business*, Torsten Reiners and Lincoln C. Wood, Eds. Cham: Springer International Publishing, 2015, ISBN: 978-3-319-10208-5. DOI: 10.1007/978-3-319-10208-5_1. [Online]. Available: https://doi.org/10.1007/978-3-319-10208-5_1.

[52] "[d0x3d!]" Last accessed: 2019-05-04. (), [Online]. Available: http://d0x3d.com/d0x3d/welcome.html.

[53] David M. Douglas, "Doxing: A conceptual analysis," *Ethics and Information Technology*, vol. 18, no. 3, pp. 199–210, Sep. 2016, ISSN: 1572-8439. DOI: 10.1007/s10676-016-9406-0. [Online]. Available: https://doi.org/10.1007/s10676-016-9406-0.

[54] Tamara Denning, Adam Lerner, Adam Shostack, and Tadayoshi Kohno, "Control-alt-hack: The design and evaluation of a card game for computer security awareness and education," in *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, ACM, 2013, pp. 915–928. DOI: 10.1145/2508859.2516753. [Online]. Available: http://doi.acm.org/10.1145/2508859.2516753.

[55] Dinei Florencio and Cormac Herley, "A large-scale study of web password habits," in *Proceedings of the 16th international conference on World Wide Web*, ACM, 2007, pp. 657–666. DOI: 10.1145/1242572.1242661.

[56] Michelle L Mazurek, Saranga Komanduri, Timothy Vidas, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, Patrick Gage Kelley, Richard Shay, and Blase Ur, "Measuring password guessability for an entire university," in *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, ACM, 2013, pp. 173–186. DOI: 10.1145/2508859.2516726.

[57] Thomas M Connolly, Elizabeth A Boyle, Ewan MacArthur, Thomas Hainey, and James M Boyle, "A systematic literature review of empirical evidence on computer games and serious games," *Computers & education*, vol. 59, no. 2, pp. 661–686, 2012. DOI: https://doi.org/10.1016/j.compedu.2012.03.004. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0360131512000619.

[58] Michele D Dickey, "Engaging by design: How engagement strategies in popular computer and video games can inform instructional design," *Educational technology research and development*, vol. 53, no. 2, pp. 67–83, 2005. DOI: 10.1007/BF02504866. [Online]. Available: https://doi.org/10.1007/BF02504866.

[59] Kurt D Squire, "Video game–based learning: An emerging paradigm for instruction," *Performance Improvement Quarterly*, vol. 21, no. 2, pp. 7–36, 2008. DOI: 10.1002/piq.20020. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/piq.20020.

[60] Pieter Wouters, Christof Van Nimwegen, Herre Van Oostendorp, and Erik D Van Der Spek, "A meta-analysis of the cognitive and motivational effects of serious games," *Journal of educational psychology*, vol. 105, no. 2, p. 249, 2013. DOI: 10.1037/a0031311.

[61] Harshal Tupsamudre, Rahul Wasnik, Shubhankar Biswas, Sankalp Pandit, Sukanya Vaddepalli, Aishwarya Shinde, C. J. Gokul, Vijayanand Banahatti, and Sachin Lodha, "GAP: A Game for Improving Awareness About Passwords," in *Serious Games*, Stefan Göbel, Augusto Garcia-Agundez, Thomas Tregel, Minhua Ma, Jannicke Baalsrud Hauge, Manuel Oliveira, Tim Marsh, and Polona Caserman, Eds., 2018. DOI: 10.1007/978-3-030-02762-9_8.

[62] Gokul CJ, Sankalp Pandit, Sukanya Vaddepalli, Harshal Tupsamudre, Vijayanand Banahatti, and Sachin Lodha, "Phishy - a serious game to train enterprise users on phishing awareness," in *Proceedings of the 2018 Annual Symposium on Computer-Human Interaction in Play Companion Extended Abstracts*, ser. CHI PLAY '18 Extended Abstracts, Melbourne, VIC, Australia: ACM, 2018, ISBN: 978-1-4503-5968-9. DOI: 10.1145/3270316.3273042. [Online]. Available: http://doi.acm.org/10.1145/3270316.3273042.

[63] "Budd:e." Last accessed: 2020-08-03. (), [Online]. Available: http://portal.ccgs.nsw.edu.au/curriculum/budde/teachers/primary/budde.html.

[64] "Enter - it security awareness game." Last accessed: 2020-08-03. (), [Online]. Available: https://play.google.com/store/apps/details?id=com.blindflugstudios.enter.

[65] "Enter - it security awareness game." Last accessed: 2020-08-03. (), [Online]. Available: https://entergame.ch/en/.

[66] "Nsteens - making safer choices online." Last accessed: 2020-08-03. (), [Online]. Available: https://www.nsteens.org/.

[67] "National center for missing and exploited children." Last accessed: 2020-08-03. (), [Online]. Available: https://www.missingkids.org/.

[68] Uta Oelke and Hilbert Meyer, *Didaktik und Methodik für Lehrende in Pflege-und Gesundheitsberufen*. Cornelsen, 2021, ISBN: 3064500546.

[69] Mubarak Ayeyemi, "A systematic review of cybersecurity education in k-12 context," 2023.

[70] Melanie Greenberg. "Worst mistakes parents make when talking to kids." (), [Online]. Available: https://www.psychologytoday.com/intl/blog/the-mindful-self-express/201209/worst-mistakes-parents-make-when-talking-kids (visited on 04/02/2024).

[71] raisingchildren.net.au. "Active listening with pre-teens and teenagers." (), [Online]. Available: https://raisingchildren.net.au/teens/communicating-relationships/communicating/active-listening (visited on 04/02/2024).

[72] Maria Lamond, Karen Renaud, Lara Wood, and Suzanne Prior, "Sok: Young children's cybersecurity knowledge, skills & practice: A systematic literature review," in *Proceedings of the 2022 European Symposium on Usable Security*, ser. EuroUSEC '22, <conf-loc>, <city>Karlsruhe</city>, <country>Germany</country>, </conf-loc>: Association for Computing Machinery, 2022, pp. 14–27, ISBN: 9781450397001. DOI: 10.1145/3549015.3554207. [Online]. Available: https://doi.org/10.1145/3549015.3554207.