Threats Targeting Children on Online Social Networks

ALEKSANDAR KARADIMCE
Faculty of Information and Communication Sciences
University of Information Science and Technology “St. Paul the Apostle”
Partizanska bb, 6000 Ohrid
REPUBLIC OF NORTH MACEDONIA

MARIJA BUKALEVSKA
Faculty of Applied IT, Machine Intelligence, and Robotics
University of Information Science and Technology “St. Paul the Apostle”
Partizanska bb, 6000 Ohrid
REPUBLIC OF NORTH MACEDONIA

Abstract: Today, practically everyone has access to the internet and owns some type of digital gadgets, such as a smartphone, laptop, tablet, etc. We live in a digital world where internet use is widespread. Nowadays, a growing number of children have access to the internet via portable electronic devices such as tablets, laptops, and gaming consoles. Online social networks (OSN) have become increasingly popular and are now widely used along with the rise of the internet. A large percentage of children worldwide have profiles on at least one online social networking site. Children register on these platforms so they can communicate with their peers, make new friends, share their interests and hobbies in the hopes of meeting someone who has similar ones, play games, and more. But in addition to the benefits and enjoyment that kids derive from social networks, there are also risks and dangers that specifically target children on OSN platforms. Online harassment, online predators, sexual solicitation, cyberbullying, and cyber grooming are all threats that target children on OSNs. This paper aims to bring awareness to parents and children about the potential dangers present on online social networking platforms and offers guidelines on how to better protect children in the social networking environment.

Key-Words: Online Social Networks, Threats, Risks, Children, Cyber grooming, Cyberstalking, Cyberbullying, Protecting children online.

Received: June 3, 2022. Revised: December 19, 2022. Accepted: January 22, 2023. Published: February 22, 2023.

1 Introduction

The development of the internet and its widespread use provides a wide range of possibilities for communication, interaction, entertainment, education, information gathering, and many other activities, thus becoming a necessary component in today's modern and digital era. Today's youth spends a significant amount of time online, whether for learning, communicating with peers through various OSNs (online social networks), or for amusement. In addition to the many benefits that the internet and OSNs offer, because of their widespread use, there are also certain threats to online safety and privacy. Children’s usage of social networks can also have a negative effect on them by interfering with their ability to focus, hindering them from sleeping, and making them subject to bullying, rumours, online harassment, and unrealistic expectations of other people's lives. There are also risks and dangers related to privacy and security with children having profiles on OSNs. Children are particularly prone to be deceived or groomed by adults they meet online. Online predators target children online and engage with them by sending them a direct private message or commenting on a post about the children. Predators can easily hide their identity online and usually deceive children about who they really are and their age, and adopt a false identity so that they may establish a stronger connection with the child and gain trust. Once a relationship is established and trust is gained, predators manipulate, abuse, and exploit their victims. The children may not recognize the risks or dangers present on OSNs until it’s too late. Security guidelines and awareness about the potential dangers of OSNs can assist parents and children in safeguarding children's privacy and security and keeping them safe online. The paper is organized as follows: Section 2 presents the related work, Section 3 discusses the usage of the internet and OSNs by children and the benefits of using them, and Section 4 talks about the various threats and risks that are present in OSNs that target children, Section 5 gives guidelines on how to better protect children and teenagers on OSNs and Section 6 concludes the paper and proposes future work.

2 Related Work

Fire, Goldschmidt, and Elovici [3] presented a taxonomy of numerous security threats that put the safety of users and children on OSNs in danger. They categorized threats targeting children into three categories: online predators, risky behaviors, and cyberbullying. The authors as well gave an overview of the solutions offered by OSN platform owners, commercial manufacturers, and academic solutions that have been implemented to improve OSN user privacy, security, and protection.

The author [4] discusses the dangers and effects of social media on children, focusing on preteens and young teenagers while also including information from older teenagers, particularly in Canada and the US. He discusses the dangers that the youths face as a result of the inappropriate and harmful content that is available on social media, as well as the consequences that lack of online privacy and cyberbullying may have on them. Additionally, the author makes suggestions on how to protect youngsters online.

In their review article on cybersecurity awareness for children [5], the authors analyzed other studies that report on various cybersecurity risks and awareness approaches. As a result, they included a list of risks for children, a list of commonly used approaches to raise awareness among children, and a list of the factors the researchers took into account while analyzing cybersecurity awareness strategies and solutions.

In the study [2] the risks and threats that children who use the internet and online social networks are exposed to are identified through a review of the literature on internet use by minors and the motivations behind it. Additionally, a methodical approach is offered for creating cutting-edge methods to shield young people from these dangers and threats.

3 Children's Online Social Networks usage, Benefits from using the internet and OSNs

First, let's define what is understood under the term "children". According to the Convention on the Rights of the Child, "a child means every human being below the age of eighteen years unless under the law applicable to the child, the majority is attained earlier" [20]. Another commonly used term for "children" is the term "minors". Even though all individuals under the age of 18 are referred to as children, it is common to divide them into several categories, as children between the ages of 9 and 12 are called preteens, whereas children between the ages of 13 and 19 are considered teenagers. The ITU (International Telecommunication Union) has divided children into five age-related groups, roughly matching the important developmental stages of a child's growth to adulthood [2].

3.1 Children's Online Social Networks Usage

Statistics show that the average daily screen time for children between the ages of 8 and 12 was 5 hours and 33 minutes in 2021, while it was 8 hours and 39 minutes for kids between the ages of 13 and 18—an increase of 2 hours daily from 2015 when the latter group's average daily screen time was 6 hours and 40 minutes [21]. Below are more statistics about children's media usage [22]:

- Reports show that in 2021, 99% of children went online by using a mobile phone or tablet;
- Using video-sharing platforms (VSPs) like YouTube or TikTok was the most common online activity among children (3–17) (95%);
- Most youngsters under 13 have their profile on at least one social networking app or website;
- 33% of parents of children in the age range of 5-7 stated their child had a profile, while 60% of children in the age range of 8–11 claimed they had a profile;
- More than six out of ten children (ages 8 to 17) reported using several profiles on various online apps and websites (62%);
- The majority of 12 to 17-year-olds felt confident in their ability to distinguish between real and false content online, but only 11% of them correctly identified the elements of a social media post that showed genuineness in an interactive survey question;

- Children between the ages of 8 and 17 (36%) reported seeing something "worrying or unpleasant" online and 6 out of 10 claimed they would always inform someone about it (59%);
- Technology-based bullying was more common than face-to-face bullying for children: 84% of 8–17-year-olds reported having experienced it.

3.2 Benefits of using the Internet and OSNs for Children

We experience both positive and negative effects from living in a world of internet communication and online social networks. Children and teenagers that use social networks in large numbers are also impacted by positive and negative factors. Children use the internet for many different things, including learning, researching, taking online classes, helping with doing their homework, and reading books. Children also use the internet for amusement by playing games and watching videos, movies, and shows, among other things. As previously mentioned, a large number of kids have profiles on one or more social networking sites. The benefits and positive factors of children using social networking platforms include [18]:

- improve social skills;
- feeling less lonely and isolated;
- entertainment;
- connect with peers;
- be creative and share their ideas online;
- learn about global events, and understand current world issues and topics.

Furthermore, the use of social media in daily life means that kids and teenagers must learn how to communicate online to be ready for opportunities in their professional careers and to maintain their relationships with friends and family [19].

Social platforms can assist kids in gaining digital literacy across a range of topics. The barriers to connecting with people, keeping in touch, and developing ties across borders are removed by social media [19]. The barriers to connecting with people, keeping in touch, and developing ties across borders are removed by social networking. It can be a terrific opportunity for kids who might have a disability or who don't feel like they can interact with others in their community to meet others who share their interests and opinions [19].

4 Threats Targeting Children and Teenagers on Online Social Networks

The European Children Online: Research and Evidence (CO: RE) project and OECD (Organization for Economic Cooperation and Development) have classified online risks to children into four categories: content risks, conduct risks, contact risks, and consumer risks [6].

Different authors have classified risks and threats targeting children into different categories [1][2][3][5].

For our study we decided to focus on the following risks and threats:

- Online predators
- Cyber grooming
- Online harassment which includes cyberbullying and cyberstalking
- Sexting

Online Predators - Online predators, often known as internet pedophiles, are the main cause for concern when it comes to the privacy of children's information and their safety online [3].

Online child predators often visit social media platforms that are popular among youngsters and pretend to be their age. By using deceptive profile pictures, pretending to have similar interests, giving the youngster gifts, or complementing them, the adult may attempt to gain the child's trust [9]. Through a web of fake Facebook, Instagram, and Snapchat accounts, a 36-year-old man tried to befriend children and gain their trust by using stolen pictures of young girls and posing as such [15]. The adult man would send sexually explicit pictures of young girls and demand that his underage victims send him pictures and videos of themselves in exchange. He then used these pictures as blackmail to force his victims into sending more extreme content. More than 5,000 children were approached by Wilson between 2016 and 2020, mostly via Facebook. It's estimated that 500 of them sent him pictures or videos. The police were able to trace him and arrest him. He was sentenced to 25 years in jail [15].

Cyber Grooming - Cyber grooming is when online predators (often adults) befriend a child or adolescent (teenager) with the intention of developing a close, trustful and emotional bond with the victim, in order to coerce sexual abuse [1]. Gaining a child's trust is the main goal of cyber grooming, which is also a means of getting the child to provide personal information [1][2]. The behavior, called "cyber grooming," is illegal in almost all countries [2]. A common form of the material includes sexually explicit discussions, images, and videos, which provides the perpetrator with the advantage when threatening and extorting the youngster [1].

According to the NSPCC (National Society for the Prevention of Cruelty to Children), police in England and Wales recorded 1,944 instances of sexual communication with minors in the six months leading up to September 2018 [16]. Of the 1,317 incidents where a method was recorded, 32% of them involved Instagram, 23% Facebook, and 14% Snapchat. While Snapchat called grooming "unacceptable," Instagram and Facebook said they "aggressively" opposed it. In April 2017, after demands from activists, sexual communication with a kid became an offence. According to information acquired by the NSPCC, almost 5,000 internet grooming offences were reported by police in the 18 months that followed [16].

Online harassment - There are risks associated with harassment that arise from many types of unwanted internet contact. According to research, the two most prevalent types of online harassment are cyberbullying and cyberstalking [5].

Cyberbullying - Cyberbullying is the repeated and intentional harming of someone through online technological communication platforms such as OSNs, chats, emails, and more [3][4]. This behavior is made easier by the amount of personal information available online and the potential for user interaction, which is partly the result of kids and teenagers not properly protecting their internet privacy [4]. Due to the nature of the internet, cyberbullying can occur at any time and can spread simply and fast to a large online audience [4]. It can be challenging to identify the offender or offender(s), and it has been discovered that the victim does not know them in roughly one-third of cases [4]. Cyberbullying differs from traditional bullying in that the offender can remain anonymous by using a fake account, making it practically impossible for the victim to track them down or confront them in person [4]. There are several forms of cyberbullying such as: receiving a mean comment, online gossip, publishing a private message without permission, being excluded from an online forum, and more [4]. Cyber threats and sextortion are also types of cyberbullying.

A case of cyberbullying, cyber threats, and sexual extortion that ended tragically is the case of Amanda Todd [17]. Amanda was a 15-year-old Canadian teenager who had been the target of cyberbullying and committed suicide by hanging herself in her home. Before she passed away, Todd recorded a video on YouTube in which she used a set of flashcards to describe how she had been physically assaulted, bullied, and forced to expose her breasts on camera. After she passed away, the video became viral, attracting the attention of global media [17]. A Dutchman was found guilty of sexually extorting Amanda and was given a 13-year prison sentence. Using 22 different fake social media profiles, Coban harassed the girl online for almost three years. In some of the messages he sent her, he threatened to distribute graphic photos of her to her friends, family, and teachers if she didn't consent to give him a webcam "performance". He was charged with making and distributing child pornographic material as well as child luring, extortion, and harassment [17].

Cyberstalking - Cyberstalking is the practice of harassing someone through unwelcome communication using technology such as computers, global positioning systems (GPS), cell phones, cameras, communication platforms, and the like option. Cyberstalking was one of the most common threats identified in a study where teenagers were surveyed to learn about and understand the various cybersecurity threats they face [5]. It can be seen as a continuity from both online stalking and cyberbullying. It often comes in the form of continuous, planned, and methodical text messages, emails, social media posts, and other forms of communication. A cyberstalker may harass a target by sending messages from various accounts multiple times per day. Some stalkers even contact the victims' friends and continue harassing the victim offline [12]. Cyberstalkers belittle, torment, manipulate, and intimidate their victims using a range of strategies and methods. Many cyberstalkers are both technologically adept and creative in their tactics. Here are some cases of possible cyberstalking [12]:

- sending the victim obscene, rude, or threatening emails or texts;
- joining the same forums and groups, the victim is a member of;
- making fake social networking profiles to stalk the victim;
- sending the victim a lot of explicit photos of oneself;
- texting the victim constantly.

A California man was arrested because he committed a "sextortion" campaign by cyberstalking several young women in California [23]. He set up and used several different online identities to continually stalk, harass, and threaten women who did not comply with his requests that they send him pornographic, sexually explicit, or otherwise indecent images and videos of themselves. Sextortion is the term used frequently to describe this type of behavior. His cyberstalking, threats, and sextortion demand reportedly persisted for more than a year in some cases, according to the lawsuit [23].

Sexting - Sexting is a combination of the words "sex" and "texting." Although this etymology ties sexting to the practice of exchanging sexually explicit text messages using mobile phones, the term has now been expanded to encompass visual content [7]. Sexting can be defined as the act of sending or exchanging one's own sexually explicit text messages, photos, or videos via a computer, mobile device, and/or the internet [7][8]. Sexting has repeatedly been connected to harmful and risky behaviors. Unauthorized sext distribution to a larger audience that was not intended to be the target audience for such content poses one potentially major concern. Sharing content can take place in a variety of ways, including sending it via email, and posting it online. This might cause reputational harm and subsequent bullying and cyberbullying victimization, particularly in the case of sexually explicit photographs. To boast to friends about receiving sexting content is one reason someone could share sexting texts. In fact, according to qualitative studies, disclosing received sexting content makes male teenagers feel more popular in their peer group. Contrarily, involvement in sexting behavior is often linked with humiliation and reputational damage [7].

5 Guidelines to better protect children on social media

5.1 Guideline for Parents on How to Protect Children on OSNs

Being their children's guardians and supervisors, parents also play a significant role in teaching children about the possible dangers associated with social networks and educating them on how to safeguard their privacy and security online.

- Parents should educate themselves more about the social networking platforms their children are interested in using and explore the privacy and safety features of those platforms. The default settings on most platforms should be checked, changed, and customized when an account is created to better safeguard the account of the child, and should regularly check the privacy settings. They should also instruct their kids to do the same when creating profiles on other platforms [10].
- Parents should decide at what age their child may begin using social media.
- Parents should be open and discuss with their children the potential dangers of social networks. Furthermore, parents can instruct them on how to create strong passwords and the importance of not posting personal information such as phone numbers, location, and other details [10].
- On your child's device, think about installing a reliable security program with parental controls. Enable all safety measures to shield kids from unintended online exposure [10].

Parents should also consider using tools and software to keep children safe online, such as Pocket Guardian, Net Nanny, Qustodio, Teensafe, and others. These tools offer the ability to track and monitor email, and social networks, give information about browsing history, filter inappropriate content, and offer other features. Some of these tools can also track if the child is going through cyberbullying or sexting [11].

5.2 Guideline for Teenagers on How to Protect themselves on OSNs

Following are some guidelines and recommendations for teenagers to safeguard their privacy and security online [13] [14].

- Never disclose your password to anyone;
- Do not accept friend requests from strangers;
- Learn about privacy settings, and check them frequently;
- Avoid posting information that could be used to locate you offline; even unintentionally, you could provide details that could be used to locate you. Posting images with identifying objects, such as license plates or landmarks, should be done with caution;
- Don’t feel pressured to reply to messages that harass you or make you uncomfortable. Despite how much you might want to do

this; it is exactly what online bullies want. They are interested in learning that they have reached you and that you are concerned and upset;

- By being able to get a response from you, they want to feel important;
- Do not post or share cruel or embarrassing stories or pictures or spread rumours. What could appear to be a harmless joke to one person may cause great pain to another.

6 Conclusion and Future Work

Given the rise of technology, digital gadgets, and the growth of social networks, children in today's world grow up with these modern technologies and use them from their earliest age. Although children can benefit from using the internet and social networks, there are also risks and dangers on these sites, as well as potentially dangerous circumstances where kids might find themselves. These threats and risks may include, but are not limited to: sexting, cyberbullying, online harassment, cyber grooming, online predators, sexual solicitation, extortion, and many other issues. To help children be cautious about who they friend, communicate with, and share information with online, it is important to educate children about the possible risks of online social networking sites. This paper provides a short review of the threats that target children on OSNs, gives brief descriptions of threats by including cases and offers guidelines on how to safeguard children's privacy and security in the context of networking platforms. This topic will be explored further in the future and include other types of risks and threats children face on OSN platforms, such as children’s exposure to inappropriate content, dangerous risks that derive from unsafe trends present on some OSN platforms, and more.

References:

[1] Jain, A.K., Sahoo, S.R. & Kaubiyal, J. “Online social networks security and privacy: comprehensive review and analysis”. *Complex Intell. Syst.* 7, 2021, pp. 2157–2177. https://doi.org/10.1007/s40747-021-00409-7

[2] Tsirtsis A., Tsapatsoulis N., Stamatelatos M., Papadamou K., and Sirivianos M. "Cyber security risks for minors: A taxonomy and a software architecture," *11th International Workshop on Semantic and Social Media Adaptation and Personalization (SMAP)*, 2016, pp. 93-99, doi: 10.1109/SMAP.2016.7753391.

[3] Fire M., Goldschmidt R., and Elovici Y. "Online Social Networks: Threats and Solutions," in *IEEE Communications Surveys & Tutorials*, vol. 16, no. 4, 2014, pp. 2019-2036. doi: 10.1109/COMST.2014.2321628.

[4] Dyer, T. “The Effects of Social Media on Children”, *Dalhousie Journal of Interdisciplinary Management*. 14. 2018, pp. 1-16. doi: 10.5931/djim.v14i0.7855.

[5] Quayyum F., Cruzes D.S., Jaccheri L. “Cybersecurity awareness for children: A systematic literature review”, *International Journal of Child-Computer Interaction*, Volume 30, 2021, pp. 1-25, 100343, ISSN 2212-8689, https://doi.org/10.1016/j.ijcci.2021.100343.

[6] OECD "Children in the digital environment: Revised typology of risks", *OECD Digital Economy Papers*, No. 302, 2021, pp. 1-28, OECD Publishing, Paris, https://doi.org/10.1787/9b8f222e-en.

[7] Van Ouytsel, J., Walrave, M., Ponnet, K. and Temple, J.R. “Sexting”. In *The International Encyclopedia of Media Literacy* (eds R. Hobbs and P. Mihailidis), 2018, pp.1-6. https://doi.org/10.1002/9781118978238.ieml0219

[8] Ringrose J., and Gill R., and Livingstone S., and Harvey L. “A qualitative study of children, young people and 'sexting': a report prepared for the *NSPCC” (National Society for the Prevention of Cruelty to Children, London, UK.)*, 2012, pp. 1-75.

[9] “Children and Grooming / Online Predators.” *Child Crime Prevention & Safety Center*, (no date), [online] Available at: childsafety.losangelescriminallawyer.pro/children-and-grooming-online-predators.html. [accessed: 10.2.2023]

[10] NortonOnline. *Kids and social media: Online safety tips every parent should know*. Norton. (no date), [online] Available at: https://us.norton.com/blog/kids-safety/parents-best-practices-to-social-media-security. [accessed: 10.2.2023]

[11] MyBangla24. *7 best tools to keep kids safe online*. MyBangla24, (no date), [online] Available at: https://mybangla24.com/best-kids-safe-online-tools. [accessed: 10.2.2023]

[12] Aziz Ahmed. “What Is Cyberstalking? - Differences, Types, Examples, Laws.” *Intellipaat Blog*, 2022, [online] Available at:

https://intellipaat.com/blog/what-is-cyberstalking/. [accessed: 10.2.2023]

[13] Webster. *Social networking advice for teenagers: Protect your privacy*. Webwise.ie. 2018, August 17. https://www.webwise.ie/parents/social-networking-advice-for-teenagers-2/

[14] *10 tips Teens can stay safe online*. UNICEF. 2020, April 8. [online] Available at: https://www.unicef.org/armenia/en/stories/10-tips-teens-can-stay-safe-online. [accessed: 10.2.2023]

[15] Burgess, Matt. "Police Caught One of the Web's Most Dangerous Paedophiles. Then Everything Went Dark." *WIRED UK*, May 2021, [online] Available at: www.wired.co.uk/article/whatsapp-encryption-child-abuse. [accessed: 10.2.2023]

[16] BBC. *Instagram biggest for child grooming online - NSPCC finds*. BBC News. 2019, March. [online] Available at: https://www.bbc.com/news/uk-47410520. [accessed: 10.2.2023]

[17] BBC. *Amanda Todd: Dutch man convicted of sexually extorting teenager*. BBC News. 2022, August. [online] Available at: https://www.bbc.com/news/world-us-canada-62326780. [accessed: 10.2.2023]

[18] "Social Media and Teenagers." *ReachOut Parents*. (no date). [online] Available at: https://parents.au.reachout.com/skills-to-build/wellbeing/social-media-and-teenagers. [accessed: 10.2.2023]

[19] "Social Media Platforms Benefits for Young People." *Internet Matters*. (no date). [online] Available at: https://www.internetmatters.org/resources/social-media-advice-hub/social-media-benefits/. [accessed: 10.2.2023]

[20] *Convention on the rights of the child OHCHR*. (no date). [online] Available at: https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child. [accessed: 10.2.2023]

[21] Written By Ben Pilkington . "All the Statistics You Need about How Kids Use the Internet in 2022." *WizCase*. [online] Available at: https://www.wizcase.com/blog/stats-how-kids-use-the-internet/. [accessed: 10.2.2023]

[22] Ofcom, Children, and parents: media use and attitudes report, 2022. [online] Available at: Children and parents: media use and attitudes report 2022 [accessed: 10.2.2023]

[23] "California Man Arrested for Cyberstalking Young Women in Sextortion Campaign." *The United States Department of Justice*. 9 Feb. 2022. [online] Available at: www.justice.gov/opa/pr/california-man-arrested-cyberstalking-young-women-sextortion-campaign. [accessed: 10.2.2023]

Contribution of Individual Authors to the Creation of a Scientific Article (Ghostwriting Policy)

Marija Bukalevska has provided the conceptualization and completed the formal analysis in this research study.

Aleksandar Karadimce has provided mentoring, supervision and guidance for the complete manuscript writing - review & editing.

Sources of Funding for Research Presented in a Scientific Article or Scientific Article Itself

No funding was received for conducting this study.

Conflict of Interest

The authors have no conflicts of interest to declare that are relevant to the content of this article.

Creative Commons Attribution License 4.0 (Attribution 4.0 International, CC BY 4.0)