https://doi.org/10.36007/4966.2024.09

How safe are children during holidays? – Increased cyberthreats during summer vacation

László BOTTYÁN[1]

ABSTRACT
Over the past year, technological advancements have significantly impacted how young children interact with their surroundings. Nowadays, kids are spending more time online than ever before. This can be attributed to several factors, including the widespread availability of smartphones, tablets, and internet-connected devices and the integration of digital tools into our daily routines, such as education and entertainment. During the summer months, many children spend even more time online while their parents are at work, making it difficult for them to monitor their online activities. Unfortunately, the potential dangers of online activity are often not discussed with children, leaving them vulnerable to various risks. In this article, I will examine children's cybersecurity risks during summer break or while traveling and provide practical solutions to mitigate each.

KEYWORDS
cybersecurity, cyber_safety, security awareness, digital risks, social media, cyberbullying, phishing, social engineering, online harassment

Introduction

As technology advances, cybersecurity threats have become increasingly frequent and intricate. The definition of cybersecurity is very complex and beyond the scope of this article, but perhaps the most succinct definition is from the UK Cyber Security Centre: "*cybersecurity is how individuals and organizations reduce the risk of cyber attack*". [13] According to the European Union Agency for Cybersecurity (ENISA), these attacks continued to rise in the latter half of 2021 and 2022, not just in quantity but also in their impact. [8] As technology becomes increasingly intertwined with our everyday routines, kids are at a higher risk of falling prey to cybercrimes and online hazards. In 2022, a report by Boston Consulting Group titled 'Why Children Are Unsafe in Cyberspace' revealed that 93% of children from ages 8 to 17 are on the internet, and the survey results indicate that 72% of children worldwide had experienced at least one cyber threat online. [18]

During the summer vacation, children may be even more susceptible to cyber threats due to reduced adult supervision, more free time, a less structured routine, a desire for entertainment, and an increased likelihood of interacting with peers online. In order to successfully mitigate online risks, parents and guardians must be aware of the potential threat factors and take proactive steps to protect their kids from potential threats and dangers on the internet.

Research in the field of kids' cyber-safety

Mitra made a comprehensive literature review in 2020 over 150 documents since 2014 and analyzed 36 detailed documents regarding cyber-safety. Her analysis highlights the importance

[1] PhD student. University of Pécs, Hungary.

of developing the digital literacy and technical skills of parents, educators, and adopting a systems approach that involves policymakers, commercial stakeholders, and law enforcement. [12] One of the most well-known, cross-border research network about children's online safety, with more than 20 countries' participation, is the EU Kids Online, funded by the the European Commission. Their research aims to assess European children's opportunities, risks, and safety online. The first research's results in 2009 identified that giving out personal information, seeing violent or hateful content, and being bullied online is the most common risky behavior. The authors proposed a typology (3C) that classified online risks into content, contact, and conduct risks. [10] Hungary participated in the second EU Kids Online research between 2009-2011. Based on the summary prepared by the ITHAKA Consulting company on behalf of the Hungarian National Media and Infocommunications Authority (NMHH), it has been identified that 37% of Hungarian children aged 9-16 have encountered at least one of the risky activities examined in the research. In general, 10% of children reported terrible experiences while surfing the Internet. [14] As a result of the changed environment and the effect of the COVID-19 pandemic, a new, updated typology (4C) was released in 2021, in which the fourth C, the contract risk appeared. [11]

Digital competence and security in public education

The European Union has defined eight key competences with which it has set the goal of lifelong learning, one of which is digital competence. Although the concept of digital competence was already defined in 2006, the committee formulates it as follows in recommendation No. 2018/C 189/01: „*Digital competence involves the confident, critical and responsible use of, and engagement with, digital technologies for learning, at work, and for participation in society. It includes information and data literacy, communication and collaboration, media literacy, digital content creation (including programming), safety (including digital well-being and competences related to cybersecurity), intellectual property related questions, problem solving and critical thinking.*"; [3] it is therefore clearly visible that security appears in digital competences. In order to strengthen digital competencies in Hungary, in 2016, the government introduced Hungary's Digital Education Strategy (Digital Education Strategy, 2016), in which the need to develop digital competence is also clearly present. Furthermore, the digital culture subject of the National Core Curriculum (NAT) includes some aspects of information security. [9] For example, the curriculum proposal by the Educational Authority (Oktatási Hivatal - OH) mentions the attitudes of a conscious user in the 8th grade, the safe usage of smartphones and e-mail security in the 9th grade, the safety of online communication, netiquette, and access rights in the 10th grade, cryptography and certificates in the 11th grade. [17] Based on what has been learned, the student will know how to follow data protection and information security rules when using digital devices and communicating online.

Increased Online Activity

There are many studies discussing internet addiction and its effects. Romano et al. made a study with the primary objective to investigate whether internet exposure had varying effects on individuals categorized as 'internet addicts' compared to those with minimal problematic usage. The findings revealed a notable adverse influence of internet exposure on the positive mood of individuals classified as 'internet addicts.' [19]

Kids spending more time online has been on the rise in recent years. UNICEF's global research points out that one child in three is an internet user and that child under 18 years old. In 2017, half of the world's population used the Internet; among the 15–24 age group, the proportion rose to about two-thirds. [22] The result of the EU Kids Online research between 2017-2019

shows that, across the EU countries, more than half of the children in age 9-16 use their smartphones daily or several times a day accessing the Internet. [21]
During their summer vacation, children spend even more time online [25] with various digital activities such as social media interaction, gaming, streaming, and browsing. This increased online presence makes them vulnerable to cybersecurity threats, such as harassment, misinformation, cyberbullying, sexual exploitation, or other harms. [23]
As a responsible parent, it is crucial to establish boundaries between screen time and other leisure activities. In order to have a well-rounded summer vacation experience for children and minimize potential online risks, it is essential to encourage them to participate in outdoor activities, engage in social interactions, and pursue physical exercise and hobbies that do not involve being online.

Public WiFi

Public WiFi has become integral to our modern lifestyle, offering convenience, accessibility, and connectivity. From cafes and airports to libraries and shopping malls, these networks offer numerous undeniable advantages, but they also present specific challenges and security concerns that we must be aware of. According to research by cybersecurity company NordVPN, 25% of travelers have been hacked while using public WiFi abroad, 85% of travelers from the United States fear they will be hacked on vacation, and 63% didn't know if they used secure networks. [15]
Children use public WiFi networks for various reasons, often influenced by their need for connectivity or to stay connected conveniently. Hungarian security education portal Kiberpajzs by the Hungarian National Bank and the National Cybersecurity Center mentions that public WiFi connections could be hazardous among its summer security tips. It's relatively easy to find a public access point to the Internet, and it can be very tempting to be able to browse for free, but it has its threats. It is pervasive for cybercriminals to provide and share Internet access points with a name specific to the location, and if we connect to these networks, all our Internet traffic goes through the attacker's device. Sensitive data (e.g., usernames, passwords, IDs, etc.) could be revealed with this technique in case not encrypted. [4]
Another aspect is that the exposure of those with lower incomes is the greatest here. The cheapest mobile subscriptions that are available on the market usually contain a minimal amount of data traffic. Packages with unlimited Internet are usually 2,5-3 times more expensive. If parents share the data usage with kids, more is needed for their increased online activities, especially during traveling. Therefore kids seek public WiFi access points, e.g., at the hotel or airport, which is more risky, as mentioned above.
Considering the latter aspect, it is challenging to recommend not allowing our child to use public WiFi while traveling. In my opinion, a hybrid solution can be used in which we rely only on the mobile Internet, avoiding the use of public WiFi; at the same time, we prepare in advance for activities that require data traffic, e.g., we download videos and music in advance, so that they do not drain our limited data package.

Social media

As children become more digitally connected at an early age, the impact of their interactions and experiences on social media is becoming a topic of paramount importance. According to Children's Commissioner report, the reasons kids are on social media vary. However, they mainly play games with friends, maintain friendships, or get emotional support in the case of older children. [1] One of the significant concerns regarding social media is not just the possibility of addiction among kids but also the potential exposure to violent or harmful content

through photos and videos shared on these platforms. This can have a significant impact on the behavior of young people. [20]
Furthermore, posting vacation photos, location updates, and personal information during the holidays can inadvertently provide cybercriminals with valuable data that could be exploited for identity theft or other scams.
Parents and guardians are crucial in guiding kids' social media usage. First, it should be used in a limited way to avoid kids' addiction. Setting clear rules, time limits and communicating expectations are essential. Demonstrating responsible online behavior and maintaining honest communication by discussing the child's online experience and concerns is helpful. Moreover, education and guidance about online safety, for example, do not include home address, phone number, or birth data on social media profiles; or talking about the risks of interacting with strange persons, could help recognize potential dangers.

Phishing and Social Engineering
Based on ENISA 2022 Threat Landscape, social engineering is in the top three of all cybersecurity dangers nowadays. [8] The term itself refers to a range of malicious activities accomplished through human interactions. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information. [16] One of the most popular social engineering attack type is phishing scams that is usually email or text message aimed at creating a sense of urgency, curiosity or fear in victims. [7] Kids are more vulnerable to social engineering due to a number of reasons, for example their limited life experience, general trust and innocent, curiosity, limited understanding of potential consequences etc. Social engineering involves manipulating individuals to divulge sensitive information, perform actions, or make decisions that they wouldn't otherwise do, which sometimes also tricky for adults, let alone children.
During summer vacations, when kids might be less cautious due to relaxed routines, they could become more susceptible to falling victim to such scams. They are not always conscious of the risks associated with downloading files from unknown sources or react on fraudulent emails, messages, or links that appear legitimate but are designed to trick individuals into revealing personal information or login credentials. [2]
It is important to educate children on how to recognize social engineering attempts and verify the authenticity of any communication before sharing sensitive information. This can be achieved by explaining common techniques such as phishing (fake emails or messages), showing real and fake examples, highlighting signs such as misspellings, unfamiliar senders, and suspicious URLs, and teaching them how to identify legitimate websites, emails, and messages versus fake ones.

Cyberbullying
Cyberbullying is *"bullying with the use of digital technologies; it can take place on social media, messaging platforms, gaming platforms, and mobile phones; it is repeated behavior, aimed at scaring, angering or shaming those who are targeted."* [24] There are many ways of cyberbullying, such as sending threatening or abusive messages and sharing embarrassing photos or false information with the intent to harm the victim. The increase in cyberbullying can be attributed to a combination of factors, such as the Internet's anonymity, which can make people more likely to engage in hurtful behaviors. Online interactions might feel detached from the emotions of the people involved, leading to a lack of empathy.
Extended leisure time during summer vacation often leads kids to engage in more online interactions, which can also expose them to cyberbullying and online harassment. The EU Kids

Online survey asked 9- to 16-year-old children if anything that happened online bothered or upset them in the past year. The answers varied among countries, but an average of one-fourth said' yes.' Furthermore, one in ten children feels unsafe online. [21] Recent studies point out that social media is becoming an increasingly common platform for cyberbullying, as identified by Giumetti and Kowalski. [5]
Children must be aware of the potential for negative online interactions and be encouraged to talk about any suspicious activities or uncomfortable feelings triggered by these interactions. Teach children to recognize signs of cyberbullying, such as hurtful comments, threats, and exclusion. Explain the importance of reporting such incidents. Adults and guardians, on the other hand, have to be able to recognize red flags. It is also essential to help them understand that only some things they see online are true. They need to critically evaluate information, question sources, and verify facts before sharing or reacting.

Free charging stations

Recently, the FBI and FCC in the USA warned about the risks of using free USB charging stations in public places like airports, hotels, hospitals, and other locations. These charging stations can contain hidden devices that load up malware, steal data or spread other malicious activities through USB cables. This practice is commonly referred to as juice jacking. [6] The term "juice" refers to the electrical power provided by the charging station, while "jacking" refers to the unauthorized access or manipulation of data.
While traveling with kids, their smartphones' and tablets' batteries running low, charging them at public stations such as airports and hotel lobbies seems easy and comfortable. However, it may result in unwanted consequences. One example of a security threat is the potential for malware to be introduced through corrupted USB ports. Additionally, data could be tampered with to steal information from connected devices.
Although FCC does not know of any confirmed occurrences of this type of attack, it's still necessary to be prepared by providing children with the knowledge and tools (e.g., to charge devices only through electric plugs or to bring external batteries) to make informed decisions about their online and technology usage, parents and educators can help minimize their vulnerability to juice jacking.

Conclusion

As kids prepare for summer break, there may be an increase in online safety risks such as cyberbullying, social engineering, cyberbullying and juice jacking. It's crucial to educate them on how to protect themselves from these threats by promoting responsible online behavior, fostering open communication, and implementing effective protective measures. By doing so, we can create a safer digital environment for children to learn and thrive without being victimized by the dangers of the online world.

Bibliography

[1] Commissioner UK. (2017). *Life in "Likes": Children's Commissioner Report into Social Media Use Among* 8-12 Years Old. Retrieved from https://www.childrenscommissioner.gov.uk/wp-content/uploads/2018/01/Childrens-Commissioner-for-England-Life-in-Likes.pdf
[2] ESET Software UK Ltd. (2022, December 1). *Identifying common social engineering attacks to kids.* Retrieved August 18, 2023, from saferkidsonline.eset.com website:

https://saferkidsonline.eset.com/uk/article/identifying-common-social-engineering-attacks-to-kids

[3] EU. (2018). Council Recommendation of 22 May 2018 on key competences for lifelong learning. *Official Journal of the European Union*, *61*(C189). ISSN 1977-091X. Retrieved from https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=uriserv%3AOJ.C_.2018.189.01.0001.01.ENG

[4] FRANK Digital KFT. (2023, July 15). *Közlemények.* Retrieved August 11, 2023, from kiberpajzs.hu website: https://kiberpajzs.hu/kozlemenyek

[5] Giumetti, G. W., & Kowalski, R. M. (2022). *Cyberbullying via social media and wellbeing. Current Opinion* in Psychology, 45, 101314. https://doi.org/10.1016/j.copsyc.2022.101314

[6] Herold, R., & ISACA. (2023, June 30). Protecting Phones, Data, and Your Business from Juice Jacking Risks. Retrieved August 20, 2023, from ISACA website: https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2023/protecting-phones-data-and-your-business-from-juice-jacking-risks

[7] Imperva. (2019). *What is Social Engineering | Attack Techniques & Prevention Methods* | Imperva. Retrieved August 13, 2023, from Learning Center website: https://www.imperva.com/learn/application-security/social-engineering-attack/

[8] I., Tsekmezoglou, E., Svetozarov Naydenov, R., Ciobanu, C., Malatras, A., Theocharidou, M., & European Union Agency for Cybersecurity. (2022). *ENISA THREAT LANDSCAPE 2022* Retrieved from https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022/@@download/fullReport

[9] Igazságügyi Minisztérium. (2020, January 31). *Magyar Közlöny*. Retrieved September 21, 2023, from Magyarkozlony.hu website: https://magyarkozlony.hu/dokumentumok/3288b6548a740b9c8daf918a399a0bed1985db0f/megtekintes

[10] Livingstone, S., & Haddon, L. (2009). *EU kids online: final report 2009.*

[11] Livingstone, S., & Stoilova, M. (2021). *The 4Cs: Classifying Online Risk to Children. (CO:RE Short Report Series on Key Topics)*. Hamburg: Leibniz-Institut Für Medienforschung | Hans-Bredow-Institut (HBI); CO:RE - Children Online: Research and Evidence. https://doi.org/10.21241/ssoar.71817

[12] Mitra, D. (2020). *Keeping children safe online: A literature review.*

[13] National Cyber Security Centre. (2020). *What is cyber security?* Retrieved from ncsc.gov.uk website: https://www.ncsc.gov.uk/section/about-ncsc/what-is-cyber-security

[14] Nemzeti Média- és Hírközlési Hatóság, & ITHAKA. (2011). *EU Kids Online II – A magyarországi kutatás eredményei.* NMHH. Retrieved from NMHH website: https://nmhh.hu/dokumentum/3886/ITHAKA_EU_KIDS_Magyar_Jelentes_NMHH_Final_12.pdf

[15] NordVPN. (2022, June 6). *85% of holidaymakers are worried they'll get hacked* | NordVPN. Retrieved August 13, 2023, from nordvpn.com website: https://nordvpn.com/de/blog/85-of-holidaymakers-are-worried-theyll-get-hacked/

[16] Northern Ireland Cybersecurity Centre. (2020, February 5). *How Attacks Happen.* Retrieved August 20, 2023, from NI Cyber Security Centre website: https://www.nicybersecuritycentre.gov.uk/how-attacks-happen

[17] Oktatás Hivatal. (2020) *Kerettantervek.* Retrieved September 23, 2023, from www.oktatas.hu website: https://www.oktatas.hu/kozneveles/kerettantervek/2020_nat

[18] Panhans, D., Hoteit, L., Yousuf, S., Breward, T., AlFaadhel, A. M., & AlShaalan, B. (2022). *Why Children Are Unsafe in Cyberspace*. In BCG Global. Boston Consulting Group . Retrieved from Boston Consulting Group website: https://www.bcg.com/publications/2022/why-children-are-unsafe-in-cyberspace

[19] Romano, M., Osborne, L. A., Truzoli, R., & Reed, P. (2013). *Differential psychological impact of internet exposure on internet addicts*. PLOS ONE, 8, 1–4.
[20] Siddiqui, S., & Singh, T. (2016). *Social Media its Impact with Positive and Negative Aspects.* International Journal of Computer Applications Technology and Research, 5(2), 71–75. Retrieved from https://jogamayadevicollege.ac.in/uploads/1586197536.pdf
[21] Smahel, D., Machackova, H., Mascheroni, G., Dedkova, L., Staksrud, E., Ólafsson, K., Hasebrink, U. (2020). *EU Kids Online 2020: Survey results from 19 countries.* London, UK: London School of Economics and Political Science. https://doi.org/10.21953/lse.47fdeqj01ofo
[22] UNICEF. (2019). *Growing up in a connected world.* UNICEF. Retrieved from UNICEF website: https://www.unicef-irc.org/publications/pdf/GKO%20Summary%20Report.pdf
[23] UNICEF. (2021, February 9). *Growing concern for well-being of children and young people amid soaring screen time.* Retrieved August 15, 2023, from www.unicef.org website: https://www.unicef.org/turkiye/en/press-releases/growing-concern-well-being-children-and-young-people-amid-soaring-screen-time
[24] UNICEF. (2023, February). *Cyberbullying: What is it and how to stop it.* Retrieved August 20, 2023, from UNICEF website: https://www.unicef.org/end-violence/how-to-stop-cyberbullying
[25] Wilcox, S. (2019, August 8). *How do kids' social media habits change during the summer holidays?* Retrieved August 15, 2023, from The Social Element website: https://thesocialelement.agency/kids-social-media-habits-summer-holiday