International Journal of the Whole Child
2023, VOL. 8, NO. 1

Tech Talk
Cyber Safety Efforts for Children: Are They Working? What Can We Do?

Nancy Caukin[a]

[a]North Greenville University

Nancy Caukin, Ed.D. is the Associate Dean for Undergraduate Programs at North Greenville University. She began her career working in outdoor education before her fifteen-year tenure as a high school science teacher. She has been a teacher educator in higher education since 2013. Her research interests include teacher candidate beliefs and sense of self-efficacy. She is on a journey of being an EdTech learner along with her teacher candidates.

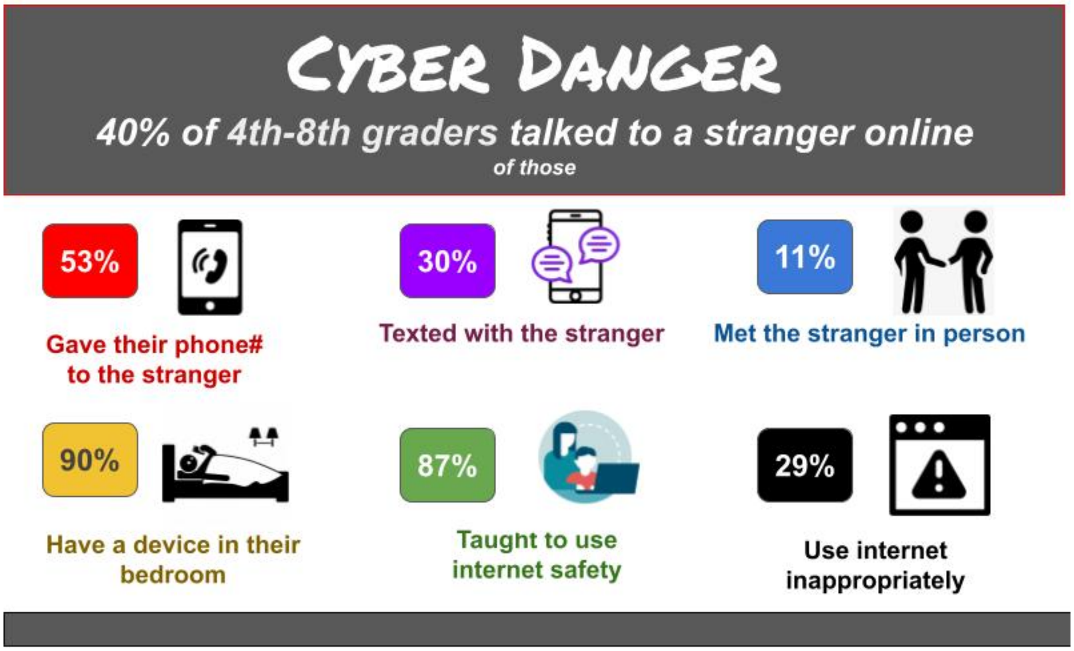
Introduction

Connectivity, particularly in an online environment, is ubiquitous. Everywhere you look, you see people engaging with devices that are connected to the internet. Many children have access to the latest information and communication technologies, immersing themselves and connecting with others in a myriad of online sites, games, chats, etc., which make them vulnerable and at a high risk of exploitation (United Nations Office on Drugs and Crime, 2015). In 2018 there were more than 45 million instances of child sexual abuse material on tech companies' platforms (End Violence Against Children, 2022b; Turban, 2020).

What Do the Statics Indicate?

According to the U.S. Center for Cyber Safety and Education's pre-pandemic Children's Internet Usage Study (2019), 40% of 4th – 8th graders reported talking to a stranger online. 53% of those revealed their phone number; 11% met a stranger in their home, the stranger's home, park, mall, or restaurant; 21% spoke to the stranger by phone; 30% texted with the stranger; 15% tried to meet the stranger; and 6% revealed their home address. 87% of those students reported being taught to use the internet safely and 90% of those students have either a cell phone, tablet, or computer in their bedroom. 29% use the Internet in ways their parents would not approve of and 31% lied about their age to access adult websites. Kids are spending an average of two hours a day online for something other than homework and 33% are online after midnight on a school night. Disconcerting statistics indeed.

The Pew Research Center (Vogels, Gelles-Watnik, & Masserat, 2022) surveyed more than 1,300 American teens (13-17 years old) in 2022 and found that 95% of teens have a smartphone, 97% say they use the internet daily (with 46% indicating they are on it almost constantly), 95% use YouTube, 67% use Tik Tok, 60% use Snapchat and Instagram, and 32% use Facebook. 35% report being on one of those platforms nearly constantly. Of those, about 55% believe that they are spending about the right amount of time on social media, about 36% believe that they are spending too much time on social media, and about 8% believe they are spending too little time on social media. When asked how hard it would be to give up social media, 54% said it would be hard and 46% said it would be at least somewhat easy.



CYBER DANGER

40% of 4th-8th graders talked to a stranger online

of those

53% Gave their phone# to the stranger

30% Texted with the stranger

11% Met the stranger in person

90% Have a device in their bedroom

87% Taught to use internet safety

29% Use internet inappropriately

Adapted from the Center for Cyber Safety and Education

In 2018, the Ohio Attorney General's Human Trafficking Commission requested a study on human trafficking be conducted by Dr. Celia Williamson and her team at the University of Toledo. They found that 58% of victims were trafficked after they met their traffickers face-to-face and 42% were trafficked having never met their traffickers face-to-race, rather having met them only online. Traffickers lurk on social media sites like Facebook, Instagram, and Snapchat, as well as dating sites like Tinder, Blendr, and Yellow, or webcam sites like Chatroulette and Monkey. The perpetrators study posts that indicate low self-esteem, posts like, "Nobody gets me", "I am so ugly", "I need to get out of here", etc. Traffickers begin to get involved and build trust with victims by saying things like, "I understand you", "I think you're beautiful. I'll encourage you to show your body. Use your body.", "I'll protect you", etc. (Billau, 2018). This is truly alarming.

In the European Union (EU), one in five digital users is a child and 62% of all child and sexual abuse materials were hosted in Europe. In 2021, 85 million pieces of child sexual abuse material were reported online, a 35% increase from 2020 (End Violence Against Children, 2022b; Turban, 2020).

What Are We Doing to Protect Children from Online Threats?

There are many more disturbing statistics and stories to be told. Suffice it to say that too many children are susceptible to devastating threats when connecting online in unhealthy, and unsafe ways. So, what are we doing to protect children from the dangers of being online? There are laws in the United States designed to protect children online dating back to 1998 and more recent bills struggling to gain traction.

In 1998, COPPA – Children's Online Privacy Protection Rule, was created to identify what information must be included in the privacy policy of United States website sources that are directed at children 13 years of age and younger, and when and how to seek consent from parents. This rule mandates that these website sources divulge that they are collecting information online from children 13 years of age and younger and provides parents control over what information is collected about their children online (Federal Trade Commission, 1998). COPPA was amended in 2013 to update definitions, for example, personal information now includes photographs, geolocation (street name, city), video or audio files, and persistent identifiers that can be used to recognize children over time and across platforms. Persistent identifiers include IP addresses, customer numbers held in a cookie, processor or in device serial numbers, and unique device identifiers (Hunton Andrews Kurth, 2013; Privacy and Information Security Law Blog, 2013).

Schools and libraries are subject to the Children's Internet Protection Act (CIPA) of 2000, which mandates that an internet safety policy be adopted and implemented, and the online activity of minors must be monitored. CIPA also mandates that minors be educated about appropriate online behaviors, including interacting with other individuals on social networking websites and in chat rooms, and cyberbullying awareness and response (cyberbullying is bullying that takes place over digital devices) (Federal Communications Commission, 2019). Of course, students don't necessarily use only school computers to access online content. As noted above in the Center of Cyber Safety and Education report (2019), 87% of the 4th – 8th graders surveyed reported as being taught how to use the internet safely; however, statistics demonstrate that many children still do not heed that instruction. Training on how to use the internet safely does not seem to be enough. While CIPA has protocols in place, it does not protect children from cyberbullying, inappropriate content (sexually explicit and/or unsolicited obscene materials), sexting (sharing or receiving sexually explicit emails or pictures via messages or apps), or sextortion/Ransomware (threats to distribute private and sensitive information if not provided with images of a sexual nature, sexual favors, or money) (Readiness and Emergency Management for Schools, n.d.).

In 2021, 85 million pieces of child sexual abuse materials were reported online

In 2020, the UK's Information Commissioner's Office, introduced the Age Appropriate Design Code, also known as the Children's Code, which took effect in 2021. This 15-point code focuses on privacy issues, inappropriate advertising, and tactics to keep children online for long periods of time (Wakefield, 2021). New legislation is proposed in the EU to make it mandatory to detect, report, and remove childhood sexual abuse and materials; use grooming detection and deterrence mechanisms that prevent childhood sexual exploitation and abuse; and establish a center devoted to fighting and preventing childhood sexual abuse (End Violence Against Children, 2022b). Currently the practice is voluntary and unfortunately, at the time of writing this article, the legislation in the EU is being held up amidst "legislative limbo" (Bertuzzi, 2022).

Some bills in the US that are struggling to gain traction are COPPA 2.0, Kids Online Safety Act (KOSA), and the American Data and Privacy Protection Act (ADPPA). The latter bill is more comprehensive, and some feel that it should take precedence over the two smaller bills focusing on children specifically (Osano Staff, 2022).

What More Can We Do to Protect Children?

In 2022, the World Health Organization published a report titled, "What Works to Prevent Online Violence Against Children." This report focuses specifically on two types of violence: child sexual abuse, including grooming and sexual image abuse; and cyber aggression and harassment in the form of cyberbullying, cyberstalking, hacking, and identity theft. The report delineates what works and what does not. The report indicates that prevention education works, but it must have multiple and varied learning modalities and tools to engage students in learning, for example, videos, games, infographics, readings, guided discussion, role play, and direct instruction. Prevention education is not effective as one-off sessions, but rather should be multiple engagements with numerous exposures to messages. Whole-school involvement as well as peer engagement and interaction has proven successful. The report also indicates that parent involvement through homework materials and activities is also important (World Health Organization, 2022).

In 2022 The Global Partnership to End Violence Against Children, a global collaborative of more than 700 organizations, including governments, UN agencies, NGOs, etc., invested $15 million through its Safe Online arm towards eighteen projects world-wide that will strengthen systems to protect children against online child exploitation and abuse. Since 2016, they have invested more than $68 million for 80 projects in 75 countries for this purpose (End Violence Against Children, 2022a).

What Resources are Available?

The National Center for Missing and Exploited Children has created NetSmartz (2023), an online platform of free resources for parents/guardians, educators and the community in English and Spanish. There are presentations, videos, tip sheets, informational slides, and classroom activities.

"Be Internet Awesome", is a free Google platform for children, parents, and educators with the purpose of teaching students the fundamentals of digital citizenship and safety. They promote five tenets they call the Internet Code of Awesome. They are: Be Internet Smart - Share with Care (communicate responsibly); Be Internet Alert – Don’t Fall for Fake; Be Internet Strong – Don't Share Your Secrets; Be Internet Kind – It's Cool to Be Kind; and Be Internet Brave - When in Doubt, Talk it Out.

For children, there is an ISTE endorsed (International Society for Technology in Education), free, interactive, online game called Interland which is designed to make learning about digital safety and citizenship fun. Players (internauts) practice skills they need to be good digital citizens as they combat hackers, phishers, over sharers and bullies.

For parents there is a free, easy-to-follow Be Internet Awesome Family Guide (in English and Spanish) that breaks down each of the five tenets into modules that provide goals, pre-information, explanations, vocabulary, scenarios, family activities, and guidance. Families are invited to practice the skills they are learning by engaging in Interland after each of the five modules. There are additional free resources including Family Tips and Activities, Exploring YouTube Confidently Guide and accompanying YouTube playlist, a downloadable Be Internet Awesome Coloring Book, a Digital Wellbeing Family Guide, and more.

For educators, the entire free Be Internet Awesome curriculum for teaching the five tenets with multiple, sequential lesson plans and instructions on how to approach the curriculum based on grade bands is provided. The lesson plans are aligned with ISTE standards for students and include interactive activities, vocabulary, scenarios, and discussion guides.

Another resource is Common Sense Digital Passport, (n.d.), an interactive learning tool that teaches digital citizenship, safety, and equity. It interfaces with Google Classroom and consists of a series of six interactive games: Password Protect - Security, Twalkers –Multitasking (media balance and well-being), Share Jumper -Privacy, E-volve – Upstander (cyberbullying, digital drama, and hate speech), Search Shark- Search (news and media literacy), Mix-n-Match – Creative Credit (news and media literacy). There is also an Educator Guide that provides a scope and sequence with detailed lesson plans.

Online dangers are here to stay, and children have access to the online world at a very early age. Knowing the choices that children can make to put them in harm’s way, knowing that predators are lurking at every turn, and knowing that there are entities who may exploit children’s privacy, cyber safety is of utmost importance. There are numerous resources for parents and educators to raise awareness of the potential dangers of online connectivity and we know that education is key for training children and adults how to engage online safely. Let’s be proactive to protect our children and ourselves. Let’s be intentional in our efforts to be cyber safe.

References

Be Internet Awesome (n.d.). Google. https://beinternetawesome.withgoogle.com/en_us/

Bertuzzi, L. (2022). *The EUs temptation to break end-to-end encryption*. IAPP. https://iapp.org/news/a/the-eus-temptation-to-break-end-to-end-encryption/#:~:text=Currently%2C%20EU%20legislation%20allows%20online,measure%20that%20expires%20in%202024.

Billau, C. (2018). *UToledo study details link between social media and sex trafficking*. The University of Toledo. https://news.utoledo.edu/index.php/10_08_2018/ut-study-details-link-between-social-media-and-sex-trafficking

Center for Cyber Safety and Education (2019). *Kids need stronger parental oversight online: Children's internet usage study*. https://isc2-center.my.salesforce.com/sfc/p/#G0000000iVSt/a/0f000000fyoc/TYQ9XvDATBA78rR00G.PGJ9fmaLm1vQfAW9HCpy3GWk

Common Sense (n.d.) Digital passport. https://www.digitalpassport.org/

End Violence Against Children (2022a). *Safe online invests an additional $15 million in combating online child sexual abuse and exploitation*. https://www.end-violence.org/articles/safe-online-grantees-2022

End Violence Against Children (2022b). *EU's proposed new legislation promises a brave new (online) world*. https://www.end-violence.org/articles/eus-proposed-new-legislation-promises-brave-new-online-world

Federal Communications Commission (2019). *Children's Internet Protection Act*. https://www.fcc.gov/consumers/guides/childrens-internet-protection-act

Federal Trade Commission (1998). *Children's Online Privacy Protection Rule* ("COPPA"). https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa

Hunton Andrews Kurth (2013). *Amended COPPA law comes into effect.* Privacy and Information Security Law Blog. https://www.huntonprivacyblog.com/2013/07/01/amended-coppa-rule-comes-into-effect/

National Center for Missing and Exploited Children (2023). NetSmartz. https://www.missingkids.org/netsmartz

Osano Staff (2022). *What's going on with the Children's Online Privacy and Protection Act?* https://www.osano.com/articles/whats-new-coppa

Readiness and Emergency Management for Schools (n.d.). Cyber safety considerations for K-12 schools and school districts. https://rems.ed.gov/docs/Cyber_Safety_K-12_Fact_Sheet_508C.pdf

Turban, J. (2020). The coronavirus puts children at risk for online sexual exploitation: One conversation could keep your kids safe. *Scientific American*. https://www.scientificamerican.com/article/the-coronavirus-pandemic-puts-children-at-risk-of-online-sexual-exploitation/

United Nations Office on Drugs and Crime (2015). *Study on the effects of new information technologies on the abuse and exploitation of children*. https://www.unodc.org/documents/Cybercrime/Study_on_the_Effects.pdf

Vogels, E.A., Gelles-Watnik, R., & Masserat, N. (2022). *Teens, social media and technology, 2022*. Pew Research Center. https://www.pewresearch.org/internet/2022/08/10/teens-social-media-and-technology-2022/

Wakefield, J. (2021). *Children's Internet Code. What is it and how will it work?* BBC News. https://www.bbc.com/news/technology-58396004

World Health Organization (2022). *What works to prevent online violence against children?* https://www.who.int/publications/i/item/9789240062061