The Impact of Technology and Social Media on Students, and a Whole Family / Whole Community Approach to Increasing Online Safety

Reese Weber, MBA, CISSP
May 26, 2022

Reese Weber, MBA, CISSP works with Federal, Tribal and Urban healthcare facilities throughout California and the to improve their cybersecurity posture, technical infrastructure, privacy and security policies, and HIPAA compliance. She served as both the System Administrator and Information System Security Officer (ISSO) before becoming the California Area Office CISO. Reese is a dedicated civil servant who has spent 22 years working for the federal government. She holds an MBA from Brandman University, a graduate certificate in Public and Non-Profit Leadership, a BBA in Information Systems, and possesses the highest information security credential, Certified Information Systems Security Professional (CISSP).

Disclosure Statement

• Faculty Disclosure Statement: As a jointly accredited provider of continuing education, the IHS Clinical Support Center must ensure balance, independence, objectivity, and scientific rigor in its educational activities. Course directors/coordinators, planning committee members, faculty, reviewers and all others who are in a position to control the content of this educational activity are required to disclose all relevant financial relationships with any commercial interest related to the subject matter of the educational activity. Safeguards against commercial bias have been put in place. Faculty will also disclose any off-label and/or investigational use of pharmaceuticals or instruments discussed in their presentation. All those who are in a position to control the content of this educational activity have completed the disclosure process and have indicated that they do not have any relevant financial relationships or affiliations with any manufacturers or commercial products to disclose.

• There is no commercial interest support for this educational activity.

Disclaimer

The views expressed in this presentation are those of the speaker and do not necessarily represent the views, policies, and positions of the Indian Health Service (IHS) or the U.S. Department of Health and Human Services (HHS).

Learning Objectives

By the end of this presentation, participants will be able to:
• Articulate the risks and impacts of social media on youths’ emotional, physical and financial well-being.
• Execute limits and establish online behavior expectations for children
• Utilize provided free resources to teach youth how to protect and conduct themselves online.
How much time are kids really spending on screens?

- Schools use technology for instruction as early as 5 years old
- Children ages 8-10 spent 8+ hours a day on various forms of media — and that time increases as they age
- Two thirds of kids report “no rules” by parents regarding their media use

Study conducted by the Center for Cyber Education and Safety

Technology and Youth: A Double-Edged Sword

**Benefits**
- Education Tool
- Inspire children to pursue tech careers
- Improve visual-special reasoning
- Can be leveraged for remote learning during emergencies
- Virtually unlimited access to information

**Risks**
- Cyberbullying
- Inadvertent exposure of private information
- Lowered attention span
- Financial risks to youth and parents
- Complete lack of oversight
- Virtually unlimited access to information

2016 Study on Children’s Internet Usage

Pressing Issues

- Youth Identity Theft
- Cyber-Molestation
- Child Sex Trafficking

If you or anyone you know is a victim of cyber sexual abuse, please reach out to Sanctuary for Families for legal assistance, clinical support, and other resources.
Youth Identity Theft: Vulnerable and Valuable to Identity Thieves

• Creditors don’t always verify Social Security numbers with birthdates
• Thieves can use a youth’s identity for years or even decades without notice
• Child’s identities are appealing – young persons don’t typically have established credit
• Young people are less likely to be cautious with their private/personal information

Online Child Abuse/Cyber Molestation

• Children do not need to be physically accessible in order for sexual abuse to occur
• Kids can be easily tricked into believing they’re chatting online with other kids

• Photos sent to perpetrators frequently end up on the dark web for pedophiles to view, sell and trade
• This is referred to as Self Generated Child Sexual Abuse Material, or SG-CSAM).

Child Sex Trafficking and Exploitation

• Children can be sexually exploited online by being forced/extorted into creating explicit content.
• Sites like Only Fans have minimal age verifications in place, and have monetizing structures that make “pimping” financially beneficial.
• 25% of “Sextortion” victims are under the age of 13, over 80% are under the age of 18.

Parents: Setting Technology Boundaries

• Teach your kids about the risks
• Use technology together when they’re young
• Set and enforce time and content limits
• Limit and monitor online activity using built in controls like Google for Families or Apple Family Sharing
• Share your own negative experiences with technology with them – lessons learned
• Do not share your Wi-Fi password with them
• Set up time limits on your Wi-Fi router
Parents: Setting Social Media Boundaries

- All US based social media platforms have a minimum age of 13 – use that as a *minimum* age to allow social media interaction
- Ensure your child’s profile is set to private
- “Friend” or “follow” your children so that you can peripherally monitor activity
- Enforce a “real life friends only” restriction on social media accounts
- Model good online behavior

Teaching Children to Report Online Abuse

- All social media platforms and online games have methods of reporting any sort of online abuse.
- Help them understand that their reports will stay anonymous, fears or threats of retribution are unfounded.
- If they also engaged in unacceptable activity, don’t shame them if they come to you for help – empower them.
Safe and Secure Online is a fully developed youth online safety curriculum, with different resources for each age group. These free resources are provided by the Center for Cyber Safety and Education—which is the outreach arm of the International Security Certification Consortium (ISC2) and offers downloadable PowerPoint presentations, videos, handouts and lesson plans.

Children's Presentation Cyber Safety Middle School (iamcybersafe.org)
Safe and Secure Online Parent Presentation (iamcybersafe.org)
Safe and Secure Online (safeandsecureonline.org)

Safe and Secure Online is a fully developed youth online safety curriculum, with different resources for each age group. These free resources are provided by the Center for Cyber Safety and Education—which is the outreach arm of the International Security Certification Consortium (ISC2) and offers downloadable PowerPoint presentations, videos, handouts and lesson plans.

Children's Presentation Cyber Safety Middle School (iamcybersafe.org)
Safe and Secure Online Parent Presentation (iamcybersafe.org)
Safe and Secure Online (safeandsecureonline.org)

FBI-SOS is a free, fun, and informative program that promotes cyber citizenship by educating students in third to eighth grades on the essentials of online security. For teachers, the site provides a ready-made curriculum that meets state and federal Internet safety mandates, complete with online testing and a national competition to encourage learning and participation. A secure online system enables teachers to register their schools, manage their classes, automatically grade their students' exams, and request the test scores.

FBI Kids — FBI

Consider Freezing Child’s Credit

To place a child credit freeze, contact each of the three credit bureaus separately:

- Experian.com/help 888-EXPERIAN (888-397-3742)
- TransUnion.com/credit-help 888-909-8872
- Equifax.com/personal/credit-report-services 1-800-685-1111

References

- Social Media Internet Safety Tips for Parents (iamcybersafe.org)
- Children, Adolescents, and the Media | Pediatrics | American Academy of Pediatrics (aap.org)
- Impact of Technology on Kids Today and Tomorrow. (wgu.edu)
- Children’s Online Privacy Protection Rule (“COPPA”) | Federal Trade Commission (ftc.gov)
- Children’s Internet Usage Study
- Families (google.com)
- IdentityTheft.gov/creditbureaucontacts
- The Surge In Online Child Exploitation, Trafficking, And Abuse — And What To Do About It (ibtimes.com)
- Suicide of Amanda Todd - Wikipedia
Additional Resources for Educators

OnGuardOnline – Federal Trade Commission
- Main website
- Resources for educators

StopBullying.gov - Department of Health and Human Services & Government Partners
- Main website
- Additional resources

StaySafeOnline – National Cyber Security Alliance
- Main website
- Resources for educators, including Cyber-Safe Assessments, Internet Education (CSAI)

STOP.THINK.CONNECT – Various Public and Private Partners
- Main website
- Information on cyberbullying

Be Internet Awesome – Google and Partners
- Main website
- Interactive online adventure game
- Parent guide and explainer
- Parent-friendly online resources

NetSmartz/KidSmartz – National Center for Missing and Exploited Children (NCMEC)
- Main NCMEC website
- NetSmartz online safety education program for children ages 5-17
- KidSmartz safety program on preventing child abductions

Presenter Contact Information

Reese Weber, MBA, CISSP
Chief Information Security and Privacy Officer
Indian Health Service, California Area Office
Theresa.weber@ihs.gov
916.930.3981 x 307