August 2024

Monthly Security Tips Newsletter - Metropolitan Government of Nashville and Davidson County

Cyberbullying

Cyberbullying can range from embarrassing or cruel online posts or digital pictures to online threats, harassment, and negative comments, to stalking through emails, websites, social media platforms and text messages.

Every age group is vulnerable to cyberbullying, but teenagers and young adults are common victims. Cyberbullying is a growing problem in schools and has become an issue because the internet is fairly anonymous, which is appealing to bullies because their intimidation is difficult to trace. Unfortunately, rumors, threats and photos can be disseminated online very quickly.

Help protect kids against cyberbullying with these tips:

Limit where your children post personal information
Be careful who can access contact information or details about your children's interests, habits or employment to reduce their exposure to bullies that they do not know. Limiting the information about them online may also limit their risk of becoming a victim and may make it easier to identify the bully if they are victimized.

Avoid escalating the situation
Responding with hostility is likely to provoke a bully. Depending on the circumstances, consider ignoring the issue. Often, bullies thrive on the reaction of their victims. If you or your child receives unwanted email messages, consider changing your email address. The problem may stop. If you continue to get messages at the new account, you may have a strong case for legal action.

Document cyberbullying
Keep a record of any online activity (e.g., emails, web pages, social media posts), including relevant dates and times. Keep both an electronic version and a printed copy of each document.

Block and report on social media
If the bullying occurs on social media, block the person any platforms and in email. Report the incident to the website; many social media platforms and other websites encourage users to report incidents of cyberbullying.

Report cyberbullying to the appropriate authorities
If you are experiencing cyberbullying yourself – or if your child is being bullied or threatened online, report the activity to the local authorities. Your local police department or FBI branch are good starting points. There is a distinction between free speech and punishable offenses. Law enforcement officials and prosecutors can help sort out legal implications. It may also be appropriate to report it to school officials who may have separate policies for dealing with activity that involves students.

- If the communications become more frequent, the threats more severe, the methods more dangerous and if third-parties (such as hate groups and sexually deviant groups) become involved—the more likely law enforcement needs to be contacted and a legal process initiated.

How to Report Cyberbullying on Social Media and Gaming Platforms

- Instagram
- Twitter
- TikTok
- YouTube
- Reddit
- Snapchat: WikiHow, Parent’s Guide, Wellness Guide
- Twitch
- Discord
- Steam: Community Page
- Epic Games
- Xbox
- Playstation
- Facebook: more info
- LinkedIn
- Pinterest
- WhatsApp

Additional Resources

- StopBullying.gov
- CyberSmile: Bullying and Cyberbullying Helplines
- R;pple Suicide Prevention
- The Sandbox at Madeline’s Place
- Cyberbullying.org: Cyberbullying Resource Center
- RAINN: How to Filter, Block, and Report Harmful Content on Social Media
- The Smart Talk
- Back to School Anti- Cyberbullying: Parents and teachers can watch this video with elementary school children
- Troubleshooting Central: Cyberbullying Statistics to Know

MS-ISAC®
Multi-State Information
Sharing & Analysis Center®

STOP | THINK
CONNECT™

The information provided in the MS-ISAC Monthly Cybersecurity Tips Newsletter is intended to increase the security awareness of an organization's end users and to help them behave in a more secure manner within their work environment. While some of the tips may relate to maintaining a home computer, the increased awareness is intended to help improve the organization's overall cyber security posture. This is especially critical if employees access their work network from their home computer. Organizations have permission and are encouraged to brand and redistribute this newsletter in whole for educational, non-commercial purposes.

Disclaimer: These links are provided because they have information that may be useful. The Center for Internet Security (CIS) does not warrant the accuracy of any information contained in the links and neither endorses nor intends to promote the advertising of the resources listed herein. The opinions and statements contained in such resources are those of the author(s) and do not necessarily represent the opinions of CIS.