

Students and Internet Safety



Metropolitan Government of Nashville and Davidson County

As students, kids are more than accustomed to using the Internet in their everyday life, but the risks that come with that use could greatly impact them and their future.

DID YOU KNOW?

- **95 percent** of teens use the Internet.
- **77 percent** of teens use Facebook.
- **53 percent** of teens use Instagram.
- **24 percent** of teens use Twitter.
- **10 percent** of teens use Tumblr.
- The average teen has approximately **300 friends on Facebook** and **79 followers on Twitter**.
- Among Twitter users aged 12 to 17, **64 percent made their tweets public**.
- **19 percent of teen users have posted things they regret**, including photos, videos, status updates, tweets, or comments.
- Only **18 percent** of young adults claim they are **comfortable with what their friends post about them online**, and **32 percent** say that the information about them online is what they choose for the public to see.

Securing the internet is our shared responsibility, and one way we can spread awareness is to talk to our kids about online safety. Please review the information below with the kids in your life.

TIPS FOR STUDENTS: BEWARE OF WHAT YOU POST ONLINE

No matter what social media platform you use, consider the type of information you choose to share with others. Here are the common cyber risks you may face when using social media:

- **Sharing sensitive information.** Sensitive information includes anything that can help a person steal your identity or find you, such as your full name, Social Security number, address, birthdate, phone number, or where you were born.
- **Posting questionable content.** Remember future employers may look at your social media accounts before hiring you. Questionable content can include pictures, videos, or opinions that may you seem unprofessional or mean and can damage your reputation or future prospects.
- **Tracking your location.** Many social media platforms allow you to check in and broadcast your location, or automatically adds your location to photos and posts.

SIMPLE TIPS

1. **Remember, there is no 'Delete' button on the Internet.** Think before you post, because even if you delete a post or picture from your profile only seconds after posting it, chances are someone still saw it.
2. **Don't broadcast your location.** Location or geo-tagging features on social networks is not the safest feature to activate. You could be telling a stalker exactly where to find you or telling a thief that you are not home.
3. **Connect only with people you trust.** While some social networks might seem safer for connecting because of the limited personal information shared through them, keep your connections to people you know and trust.
4. **Keep certain things private from everyone.** Certain information should be kept completely off your social networks to begin with. While it's fun to have everyone wish you a happy birthday, or for long-lost friends to reconnect with you online, listing your date of birth with your full name and address gives potential identity thieves pertinent information. Other things to keep private include sensitive pictures or information about friends and family. Just because you think something is amusing does not mean you should share it with the world.
5. **Speak up if you're uncomfortable.** If a friend posts something about you that makes you uncomfortable or you think is inappropriate, let him or her know. Likewise, stay open-minded if a friend approaches you because something you've posted makes him or her uncomfortable. People have different tolerances for how much the world knows about them, and it is important to respect those differences. Also report any instances of cyber bullying you see.

RESOURCES AVAILABLE TO STUDENTS

- NetSmartzKids.org
Clicky, a yellow robot, along with brother-and-sister team Nettie and Webster, teach kids what to watch out for online in this interactive website with videos and games.
- iKeepSafe.org
Faux Paw, the Websurfing Techno Cat, is always on an adventure. Read about her trip to Beijing or her experiences with the dangerous download.
- NSTeens.org
Real-life stories, games, and comics that explore potential online dangers and how to avoid them.
- iSafe.org
Become an iMentor and promote cyber safety in your home, school, and community.

TIPS FOR PARENTS: BE AWARE OF WHAT YOUR KIDS POST ONLINE

Understand the cyber risks kids face when using social media. Talk to your kids about the following risks:

1. **What they are posting:** Talk to your kids about the information they post online. Many of them don't understand the damage they could do to their reputation or future prospects with unkind or angry posts, and compromising photos or videos. Ensure your kids are not sharing or posting:
 - Sensitive information: Sensitive information includes anything that can help a person steal your child's identity or find them, such as their/your full name, Social Security number, address, birthdate, phone number, or place of birth.
 - Compromising content: This includes photos or status updates that may damage your child's reputation or future prospects.
 - Unkind or angry content: This includes anything malicious directed at themselves or another person, as well as opinions that are probably better left unshared.
2. **Who they are connecting with:** Social media allows kids to connect with their friends, but there is also a risk of connecting with someone they do not know or who is only pretending to be a kid.
3. **What level of privacy they are using:** Many social media platforms have privacy settings that allow users to limit who sees their content. There are also settings for location tracking and geo-tagging of photos or statuses.

SIMPLE TIPS FOR PARENTS

1. **Talk to your children.** Help your children understand the importance of owning their digital lives and only sharing things that will not put them in danger, negatively affect their future, or harm others.
2. Emphasize the concept of credibility to teens: not everything they see on the Internet is true and people on the Internet may not be who they appear to be.
3. Watch for changes in behavior. If your child suddenly avoids the computer, it may be a sign they are being bullied or stalked online.
4. Review security settings and privacy policies for the social media sites kids frequent. These settings are frequently updated so check back regularly.

RESOURCES AVAILABLE TO PARENTS

- [Cybersecurity Awareness Volunteer Education Program \(C-SAVE\)](#)
The National Cyber Security Alliance developed the C-SAVE program to provide age-appropriate resources to discuss Internet safety with students.
- [OnguardOnline.gov](#)
This website, run by the Federal Trade Commission (FTC), is a one-stop shop for online safety resources available to parents, educators, kids, and others.
- [Project iGuardian](#)
ICE Homeland Security Investigations is one of the leading law enforcement agencies that investigates crimes involving child pornography and the sexual exploitation of minors. Project iGuardian provides resources to help children and teens stay safe online.
- [Cybertipline.com](#)

The Congressionally-mandated CyberTipline, which is part of the National Center for Missing and Exploited Children (NCMEC), receives online child solicitation reports 24-hours a day, seven days a week. Submit an online report or call 1-800-843-5678.

- [ConnectSafely.org](https://connectsafely.org)

ConnectSafely is an organization for everyone engaged in and interested in the impact of social media and mobile technology. You'll find tips, safety advice, and other resources to promote the safe, effective use of connected technology.

Provided By:



The information provided in the Monthly Security 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.