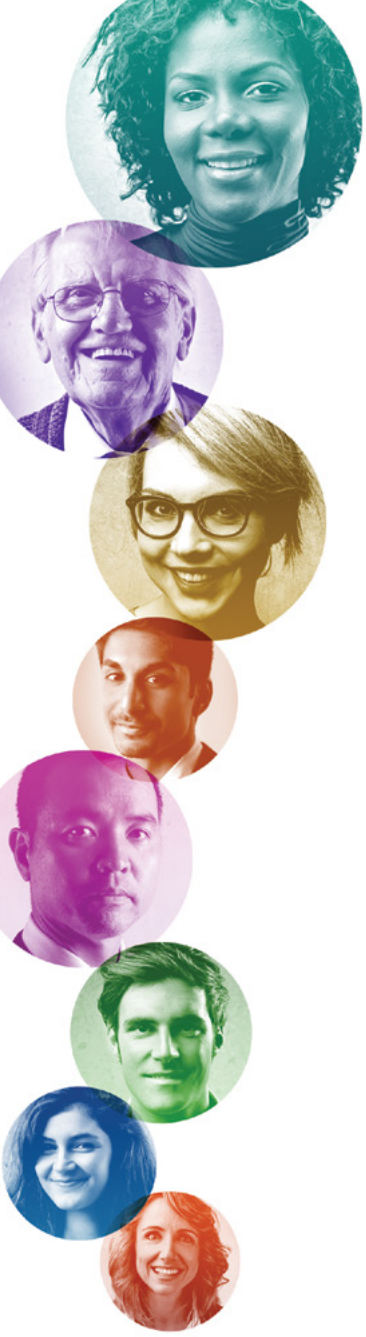
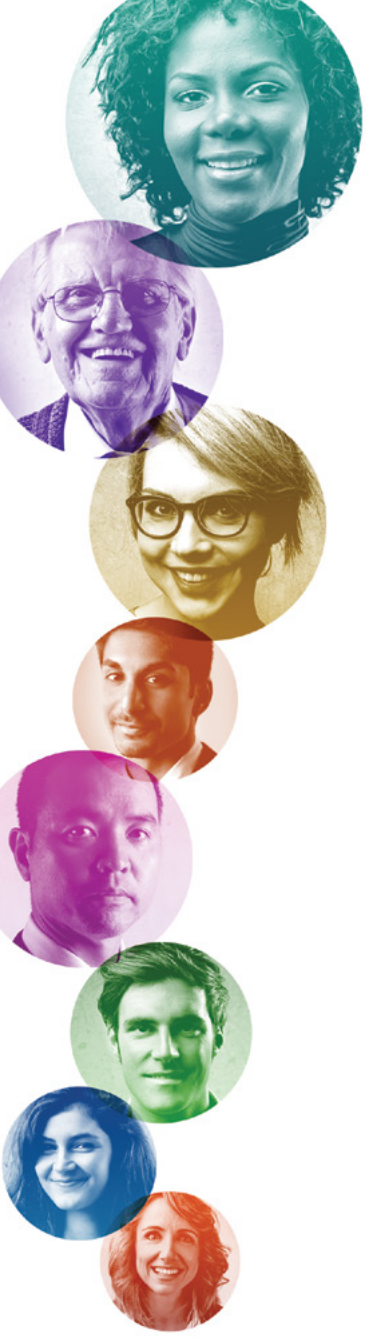


SOCIAL MEDIA GUIDE

Now more than ever, consumers spend increasing amounts of time on the Internet. With every social media account you sign up for, every picture you post and status you update, you are sharing information about yourself with these social media companies and the world. How can you make sure you and your information stay safe online? This Social Media Guide includes tips and resources to help you safely navigate the social media world.

This guide includes the following resources from the Stop.Think.Connect.™ Campaign:

- **Social Media Tips for Students**
- **Social Media Tips for Parents**
- **Cybersecurity Tips for Bloggers**



SOCIAL MEDIA TIPS FOR STUDENTS

As a student, you are more than accustomed to using the Internet in your everyday life, but the risks that come with that use could greatly impact you and your future.

DID YOU KNOW?

- **95 percent** of teens use the Internet.[1]
- **77 percent** of teens use Facebook.[2]
- **53 percent** of teens use Instagram.[3]
- **24 percent** of teens use Twitter.[4]
- **10 percent** of teens use Tumblr.[5]
- The average teen has approximately **300 friends on Facebook** and **79 followers on Twitter**.[6]
- 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.[7]
- 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.[8]

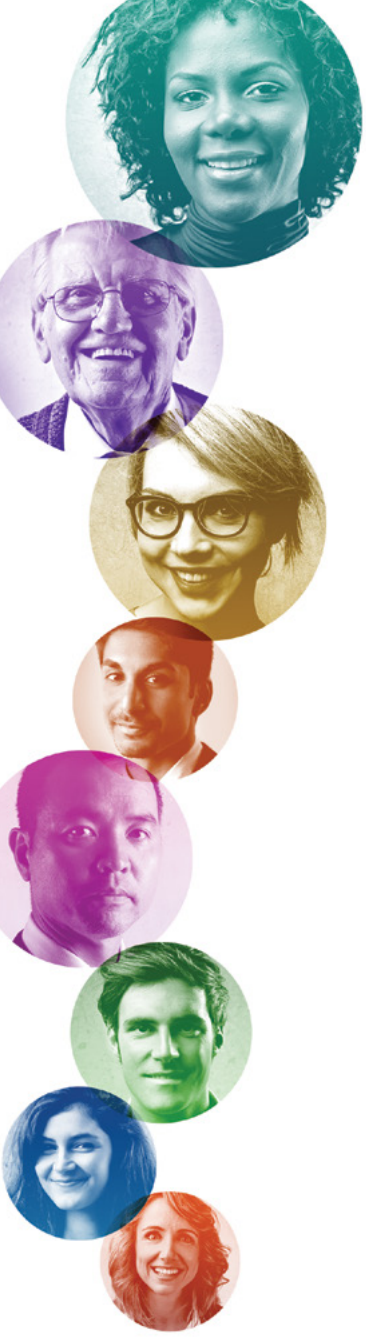
BEWARE OF WHAT YOU POST ONLINE

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.

---

[1] Pew Research Center, "The Pew Research Center's Internet and American Life Project: Teen Fact Sheet." September 2012
[2] Ibid
[3] Pew Research Center, "Social Media Update 2014." January 2015
[4] Pew Research Center, "The Pew Research Center's Internet and American Life Project: Teen Fact Sheet." September 2012
[5] Pew Research Center, "Teens and Libraries in Today's Digital World." April 2014
[6] Pew Research Center, "Teens, Social Media, and Privacy." May 2013
[7] Ibid
[8] Ibid



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 includes 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 YOU

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

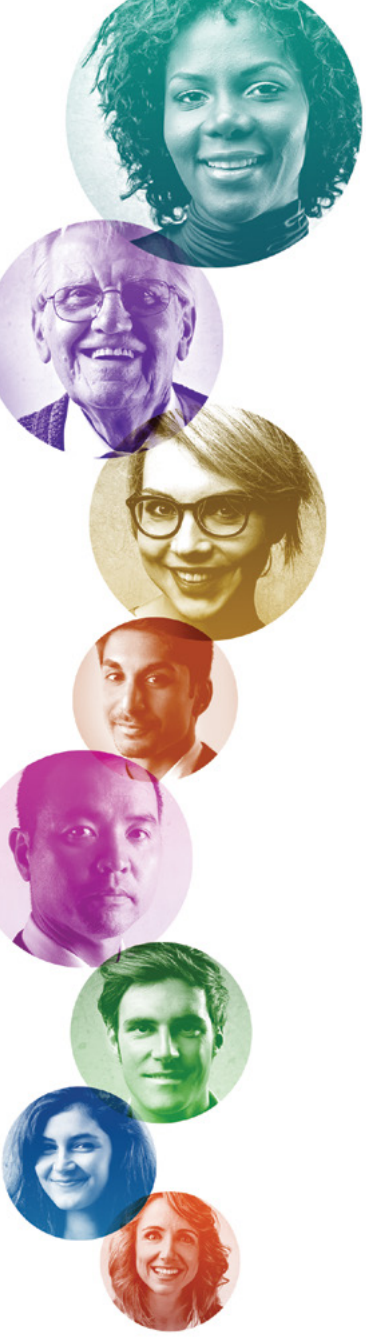
Faux Paw, the Websurfing Techno Cat, is always on an adventure. Read about her trip to Beijing or her experiences with the dangerous download.

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.



SOCIAL MEDIA TIPS FOR PARENTS

As a parent, you have a responsibility to help teach your kids about online safety. But when they're using sites you've never heard of, what do you do?

DID YOU KNOW?

- **95 percent** of teens use the Internet.[1]
- **77 percent** of teens use Facebook.[2]
- **53 percent** of teens use Instagram.[3]
- **24 percent** of teens use Twitter.[4]
- **10 percent** of teens use Tumblr.[5]
- The average teen has approximately **300 friends on Facebook** and **79 followers on Twitter**.[6]
- 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.[7]
- 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.[8]

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.

[1] Pew Research Center, "The Pew Research Center's Internet and American Life Project: Teen Fact Sheet." September 2012
[2] Ibid
[3] Pew Research Center, "Social Media Update 2014." January 2015
[4] Pew Research Center, "The Pew Research Center's Internet and American Life Project: Teen Fact Sheet." September 2012
[5] Pew Research Center, "Teens and Libraries in Today's Digital World." April 2014
[6] Pew Research Center, "Teens, Social Media, and Privacy." May 2013
[7] Ibid
[8] Ibid

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 YOU

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

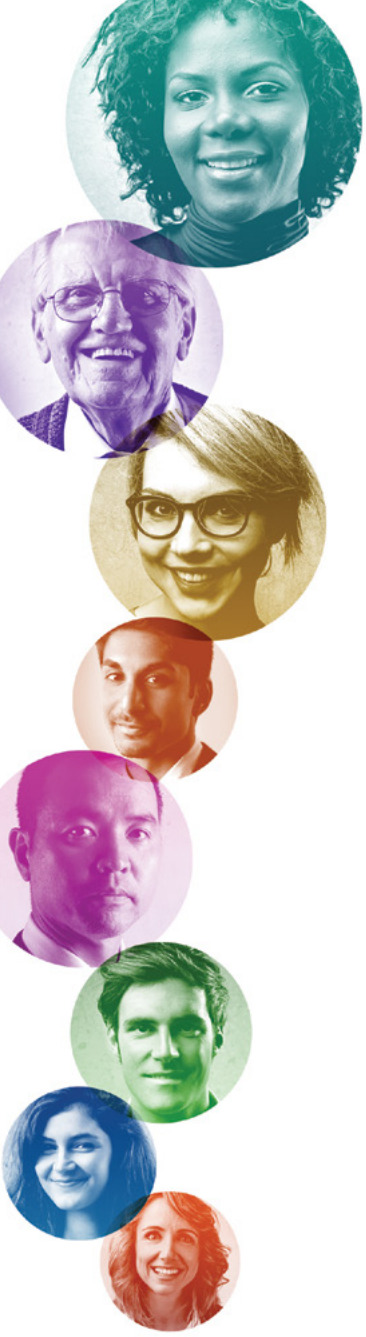
ICE Homeland Security Investigations is one of the leading law enforcement agencies that investigates crimes involving child pornography and the sexual exploitation of minors. Project iGuardian provides resources to help children and teens stay safe online.

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

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.



CYBERSECURITY TIPS FOR BLOGGERS

Blogging is becoming an increasingly popular pastime among Americans. It is an easy way to share opinions, keep up with family and friends, and connect with others. Whether you blog occasionally or blogging is your full-time job, follow these cybersecurity tips to help keep you and your information safe.

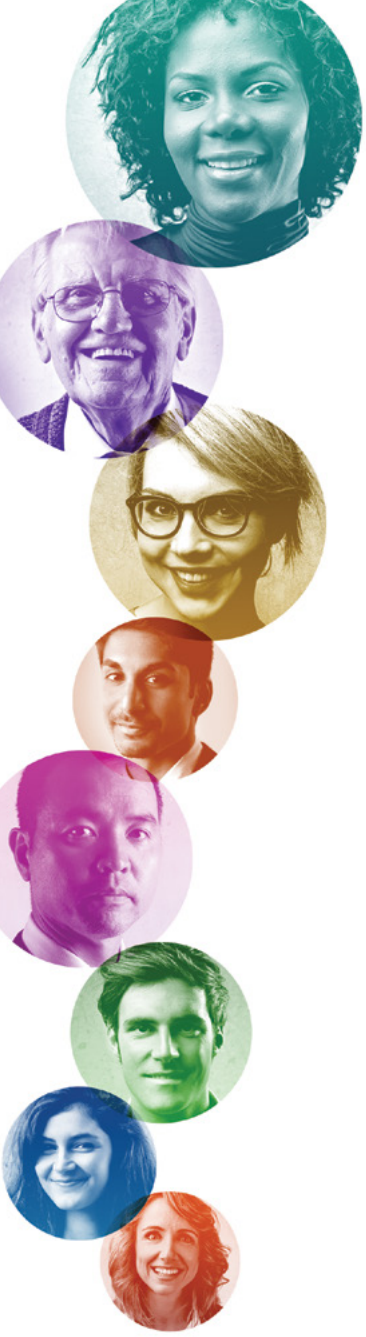
COMMON CYBERSECURITY ISSUES FOR BLOGGERS

- **Data privacy.** Blogging can be a very personal activity, with bloggers sharing their opinions, daily activities, and photos. Sharing these tidbits of personal information may seem harmless, but hackers and other malicious actors can use this information to gain access to your online accounts. People and companies can also take your photos for a variety of uses, including in advertisements or other social media profiles and blogs.
- **Harassment and threats.** Unfortunately, not everyone is nice on the Internet. People, usually acting anonymously, can leave threatening or harassing comments and messages on blogs. Think twice about the information you are posting and be aware that putting information in the public domain may expose you to feedback from others who do not share your views.

SIMPLE TIPS

1. **Remember, there is no delete button on the Internet.** Think before you post. Even if you delete your content, someone could have saved it or taken a screenshot. Before posting, ask yourself: "Am I comfortable with sharing this information with the whole world?"
2. **Keep it private.** If you are blogging for fun and not trying to make a living, consider keeping your blog private so that only people you invite or approve can see what you post. Many blogging services allow you to control whether or not your blog is visible to the public or searchable on search engines.
3. **Keep it anonymous.** If you want to keep your blog public, consider blogging under a pseudonym. Do not share the real names of your family or friends. Do not share information that can help people find out where you live or work. Think about what photos you share and if these photos include people who have not consented to having their images shared online. Take special care when sharing photos of your children. Posting about your children makes it harder for them to control their digital lives and privacy as they get older. And information you post about them can be used by criminals to steal their identity. In 2012, 26 percent of identity theft victims were between the ages of six and ten, and identity theft has doubled in the past year for children age five and younger.[1]
4. **Control the comments.** Some blogging platforms allow you to manage the comments section, allowing you to review and approve comments before they appear on your posts. This would prevent spam comments (often including malicious links) and harassing comments. Or you may be able to disable the comments feature entirely.

[1] FTC Child Identity Theft Report, 2012



5. **Protect your blog from hackers.** The most effective way to do this is to set strong passwords that are long and unique. Use two-factor authentication whenever it is available. Also ensure your computer's operating system, software, and anti-virus protections are updated.
6. **Back up your data.** Regularly back up your data to a hard drive or the cloud. This ensures your data is protected and available should a hacker or malware delete content from your machine or online.
7. **Report suspicious or harassing activity.** Work with your blogging service to report and possibly block harassing users. Report serious threats to law enforcement.

RESOURCES AVAILABLE TO YOU

US-CERT.gov

US-CERT provides tips for both individuals and organizations on how to protect against cyber threats. Visit www.us-cert.gov/ncas/tips for more information.

StaySafeOnline.org

The National Cyber Security Alliance provides information on security updates, free anti-virus software, malware software removal, and other services.

IF YOU ARE A VICTIM OF ONLINE CRIME

- Immediately notify your local authorities and file a complaint with the Internet Crime Complaint Center at www.ic3.gov.
- If someone has had inappropriate contact with you over the Internet, report it to www.cybertipline.com and they will coordinate with the Federal Bureau of Investigation and local authorities.

Stop.Think.Connect.™ is a national public awareness campaign aimed at increasing the understanding of cyber threats and empowering the American public to be safer and more secure online. The Campaign's main objective is to help you become more aware of growing cyber threats and arm you with the tools to protect yourself, your family, and your community. For more information visit www.dhs.gov/stopthinkconnect.