TIP SHEET

CYBER SECURITY BASICS: SOCIAL MEDIA

CYBERSECURITY BASICS FOR SOCIAL MEDIA

Now more than ever, consumers spend an increasing amount of time on the Internet. For every social media account with which you interact, every picture you post, and status you update, you are sharing information about yourself with the world. This information is permanent in cyberspace. It is imperative to be proactive and secure your online safety. Take these steps to connect with confidence and safely navigate the social media world.

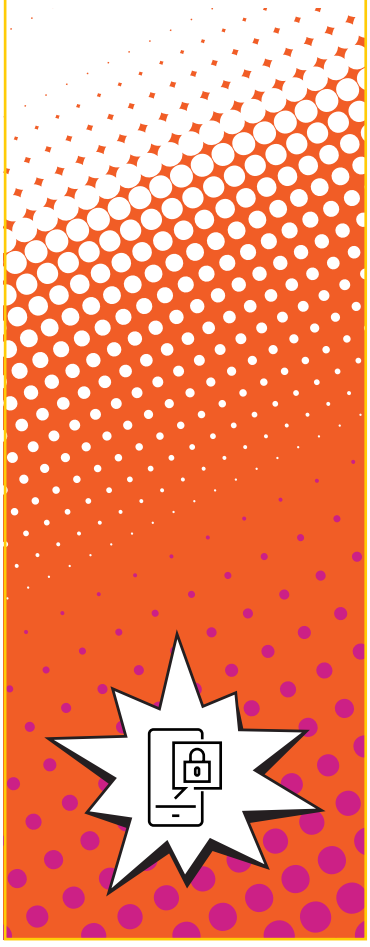
CYBER CRIMINALS AND SOCIAL MEDIA

Cybercriminals use social media to spread malware, malicious links, and malicious advertising. They can also leverage hacked credentials to refine their malware and scamming targets. In addition, they will use the "oversharing" of personal information to target online accounts. It is critical that you practice good cyber hygiene by understanding their tactics and knowing the cyber basics.

- **Never click and tell.** Limit what information you post on social media—from personal addresses to where you like to grab coffee. What many people do not realize is that these seemingly random details are all a criminal needs to know to target you, your loved ones, and your physical belongings—online and in the real world. Keep Social Security numbers, account numbers, and passwords private, as well as specific information about yourself, such as your full name, address, birthday, and even vacation plans.
- **Connect only with people you trust.** While some social networks might seem safer for connecting because of the limited personal information shared within them, keep your connections to people you know and trust. If communication from a post seems strange or odd, delete it.
- **Speak up if you're being cyberbullied online.** Report any and all instances of cyberbullying you see or experience to the appropriate social platform.
- **Report suspicious or harassing activity.** Work with your social media platform to report and possibly block harassing users. Report an incident if you have been a victim of cybercrime. Local and national authorities are ready to help you.

FOLLOW-ON RESOURCES

- CISA's Multi-Factor Authentication Website
- Phishing Tip Sheet
- StaySafeOnline.org
- Report a Cyber Crime



CONTINUED ON NEXT PAGE ▸

TIP SHEET

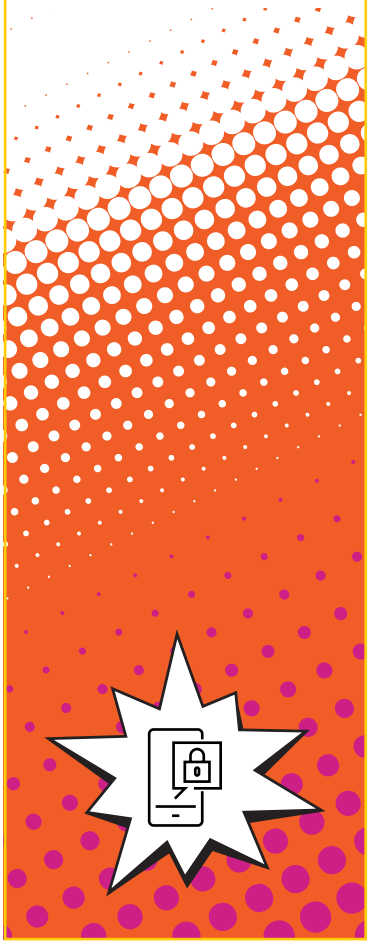
CYBER SECURITY BASICS: SOCIAL MEDIA

KNOW YOUR CYBER BASICS

- **Remember, there is no 'delete' button on the internet.** Share with care, because even if you delete a post or picture from your profile seconds after posting it, chances are someone still saw it, and information is permanent in cyberspace.
- **Update your privacy settings.** Set the privacy and security settings to your comfort level for information sharing. Disable geo-tagging, which allows anyone to see where you are—and where you are not—at any given time.
- **If You Connect IT, Protect IT.** Whether it is your computer, smartphone, game device, or other network device, the best defense against viruses and malware is to update to the latest security software, web browser, and operating systems. Sign up for automatic updates, if you can, and protect your devices with anti-virus software.

FOLLOW-ON RESOURCES

- CISA's Multi-Factor Authentication Website
- Phishing Tip Sheet
- StaySafeOnline.org
- Report a Cyber Crime



LEARN MORE DURING CYBERSECURITY AWARENESS MONTH

Thank you for your continued support and commitment to Cybersecurity Awareness Month and helping all Americans stay safe and secure online. Please visit www.cisa.gov/cybersecurity-awareness-month to learn more.