Cyber Safety Social Media Messaging Campaign

How to use this resource:

It is recommended that you work with your district communications manager or team to coordinate working the following social media posts into the district's ongoing social media notifications.

One option may be to pick a consistent day each week where the district will include a cyber safety/cybersecurity awareness post in social media. For example, start a Cyber Thursday campaign. Another option may be to include cyber safety/cybersecurity messaging in the district's learning management system notifications each week.

Tips for using the pre-packaged social media posts:

- Be creative in how you leverage the messages.
- Use a consistent hashtag for messaging. The sample hashtag provided in this kit is #K12CyberSafe. However, you may choose to replace it with your school district name. For example, #MontgomeryCyberSafe
- Pre-load a social media management tool with messages so you don't have to remember to send them out each week.
- Some of the items below include recommendations to contact the district information technology team for assistance. When you use these, remember to provide the team's contact information.
- Don't worry about repetition. Repeating messages periodically helps people remember the message.

Pre-packaged social media posts for K12 schools

The following messages are broken down by topic areas. You may choose to focus on one topic area at a time or mix and match the messages.

Talk About Cyber Safety

#K12CyberSafe: Everyone has a role in ensuring our remote and hybrid learning environments are safe. Talk about cyber safety with your friends and family.

#K12CyberSafe: If you are experiencing cyber harassment or bullying, tell someone. <Insert district contact and resource information here>

#K12CyberSafe: Who is in your virtual space? Pay attention to who is present in your online meetings and class rooms. Eject uninvited guests from the meeting.

Cyber Safety and Social Media

#K12CyberSafe: Social media posts aren't private. Think carefully about what you share on social media and avoid sharing your personal information such as age, address, school, etc.

#K12CyberSafe: Cybercriminals love it when you overshare on social media – they can learn all about you! Be cyber safe and make it harder for them by avoiding posting real names, places you frequent, and home, school and work locations.

#K12CyberSafe: Once posted, always posted: Protect your reputation and your privacy on social networks. What you post online stays online. Consider this before sharing a post or photo of yourself or others.

Email and Phishing

#K12CyberSafe: Don't talk to strangers. If you're unsure who an email is from—even if the details appear accurate—do not respond, and do not click on any links or attachments.

#K12CyberSafe: Cybercriminals cast wide nets with #phishing tactics, hoping to drag in victims. They may offer a financial reward, threaten you if you don't engage, or claim that someone is in need of help. Stop, take a moment, and think before you click.

#K12CyberSafe: Cybercriminals try to get your personal information by offering gifts and prizes. If it sounds too good to be true, it is. Stop, take a moment, and think before you click. Contact your information technology team for assistance.

#K12CyberSafe: Cybercriminals send emails that demand an urgent response. If someone needs an urgent response right now, do not respond via email. Instead contact your information technology team for assistance.

#K12CyberSafe: Think you've received a phishing email? Report it to your district IT team. Do not respond to the sender or click on any links.

#K12CyberSafe: Tips for Spotting a phishing email: 1) They offer financial reward, threaten you or claim to need help. 2) They ask for your personal info. 3) They want you to download a file or click on a link. For more information: staysafeonline.org/stay-safe-online/online-safety-basics/spam-and-phishing/

#K12CyberSafe: If an email looks phishy, it probably is. When in doubt, throw it out.

#K12CyberSafe: Unsure who sent that email? Just delete it.

Hardware & Software Updates

#K12CyberSafe: If it's connected, make sure it's protected. Outsmart cybercriminals by regularly updating your software.

#K12CyberSafe: The best defense is solid maintenance - Make sure to keep security software, web browsers, and operating systems up to date on all devices that connect to the Internet.

#K12CyberSafe: Unprotected internet-connected devices are open doors for cyber criminals. Secure your internet-connected devices at home and work with strong passwords and up-to-date software.

#K12CyberSafe: Enable automatic application updates in your device settings so your software runs smoothly and you stay protected against cyberthreats!

#K12CyberSafe: Don't ignore that software update! It can be what protects your device and your privacy from a cyber criminal.

#K12CyberSafe: Keep all software on all devices you connect to the internet current. This improves the performance of the devices and improves your security.

Multi Factor Authentication (If You Have It)

#K12CyberSafe: If multifactor authentication is available to protect your personal information, use it!

Mobile Device & Application Security

#K12CyberSafe: Many mobile apps track location. Do they all need to? No. Take a moment to configure the privacy and security settings of your apps and, while you're at it, help someone in your class or home configure theirs.

#K12CyberSafe: Enable automatic application updates in your mobile device settings so your software runs smoothly and you stay protected against cyberthreats!

#K12CyberSafe: Do you know how many of your apps have access to your contacts, photos and location data? Time to find out! Configure your privacy and security settings to limit how much data you give away.

#K12CyberSafe: Don't overshare. You may be revealing more about yourself than you think. Check your privacy and security settings on mobile and desktop software applications to limit how much data you give away.

#K12CyberSafe: Delete apps you don't need or no longer use. They may be continuing to collect and share data about you.

#K12CyberSafe: Do your research before you download an app from the Internet. Only download apps from trusted sources

Passwords and Passphrases

#K12CyberSafe: Make your passwords strong by using passphrases. Keep them long (14+ characters), easy-to-remember, and unique for each account.

#K12CyberSafe: Never share your passwords with anyone, including information technology staff from the district.

#K12CyberSafe: Passwords are like toothbrushes, don't share them.

#K12CyberSafe: Check your passwords to see if they have been compromised or stolen at https://haveibeenpwned.com/ If your password is compromised, change it right away.