Cyber Security Social Media Posts
This month, we are raising awareness about the importance of #cybersecurity and sharing information to help everyone be safer and more secure online. Do your part. #BeCyberSmart #CybersecurityAwarenessMonth
We all have a role to play in ensuring our interconnected world is safer and more resilient for everyone. Empower your friends, colleagues and family to #BeCyberSmart
#BeCyberSmart Tip: If you connect it, protect it. Outsmart cyberthreats by regularly updating your software.
Any device that connects to the internet is vulnerable to risks. The best defense is to keep device software, web browsers, and operating systems up to date. #BeCyberSmart by turning on auto-updates.
Every new internet-connected device is another entry point for a cyber criminal. If you connect it, protect it. Know what steps you need to take to secure all internet-connected devices at work and home. #BeCyberSmart
#BeCyberSmart Tip: Public Wi-Fi networks are not secure – limit what you do on public WiFi and avoid logging in to key accounts like email and financial services.
Public Wi-Fi is not secure or safe. If you must connect, consider using a virtual private network (VPN) or a personal/mobile hotspot. #BeCyberSmart
When it comes to passphrases, it's best to mix it up! Keep them long, easy-to-remember, and unique for each account. #BeCyberSmart
Make your password a passphrase. Remember: length trumps complexity when creating a strong passphrase! #BeCyberSmart
Step up your passphrase game with multi-factor authentication and keep all your private information private. Do your part. #BeCyberSmart
No matter how long and strong your passphrase is, a breach is always possible. Make it harder for cybercriminals to access your account by enabling multi-factor authentication. #BeCyberSmart
Enable multi-factor authentication to ensure that the only person who has access to your account is you. #BeCyberSmart
Cybercriminals use all sorts of tactics in phishing attacks. They may offer you money, threaten you if you don’t engage, or claim that someone is in need of help. Stop and think before you click. #BeCyberSmart
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. Just delete it. #BeCyberSmart
#BeCyberSmart Tips for Spotting a Phish: 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.
Cybercriminals love it when you overshare on social media – they can learn all about you! #BeCyberSmart and make it harder for them by avoiding posting personal information and home, school and work locations.
Once posted, always posted: Protect your reputation on social media. What you post online stays online. Consider this before sharing a post or photo of yourself or others. Do your part. #BeCyberSmart
Do all of your apps need to track your location? No! Take a moment to configure the privacy and security settings of your apps. Then help someone in your community configure theirs. #BeCyberSmart
Enable automatic #app updates in your device settings so your software runs smoothly and you stay protected against cyberthreats! #BeCyberSmart
#BeCyberSmart Rules for Keeping Tabs on Your #Apps: 1) Delete apps you don’t need or no longer use. 2) Review app permissions. Limit how much data you share with the app. 3) Only download apps from trusted sources.
Don’t ignore that software update! It can be what protects you from a #cyber criminal. #BeCyberSmart
Keep all #software on all internet connecting devices current. This not only improves the performance of the devices, but also improves your #security. #BeCyberSmart
#BeCyberSmart tip: If an email looks phishy, it probably is. When in doubt, throw it out. #BeCyberSmart
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. Do your part. #BeCyberSmart
You may be revealing more than you think. Check your privacy and security settings to limit how much data you give away. Do your part. #BeCyberSmart
Your mobile device could be filled with apps running in the background or gathering your personal information without your knowledge. Check your app permissions and delete apps you don't need. #BeCyberSmart

Think before you click! If you receive an enticing offer via email or text, don't be so quick to click the link. Instead, go directly to the company's website to verify it is legitimate. #BeCyberSmart
Links in email, texts, and social media posts are the easiest ways for cyber criminals to get your sensitive information. Be wary of clicking links that come from a stranger or that you were not expecting. #BeCyberSmart
Every time you sign up for a new account, download a new app, or get a new device, immediately configure the privacy and security settings to your comfort level. Check these settings at least once a year. #BeCyberSmart