DIR

Office of the Chief Information Security Officer

Texas Department of Information Resources
Transforming How Texas Government Serves Texans

Cybersecurity Tips for Teens

Best Practices for Staying Safe While Online

Beware of what you share

- Avoid posting sensitive information online, including addresses, phone numbers, your birthdate, social security number, or financial information.
- Anything you post on the internet is there forever. Before you post think to yourself, would I want a future employer to see this?
- Be careful posting details about your life and don't answer questions—online or over the phone—from anyone you don't know.

Know your privacy settings

- Look through the settings on your social media to be sure that only people you trust can see your posts.

Watch out for malicious websites

- Malicious websites can look identical to trusted sites, but the URL or email address might use a different spelling or domain (for example, **.net** instead of **.com**). When in doubt, avoid the website until you're 100% sure it's safe.

Be wary of links and attachments

- Unexpected links and attachments in messages might contain viruses or spyware that the sender doesn't even know about (or even worse, maybe they do). Check with the sender first. If you don't know the sender, just trash the message.

If it sounds too good to be true, it probably is

- Free games and other online websites might be tempting, but they can come at a cost to your privacy. Only download from trusted sources, even if you might have to pay.

Avoid public Wi-Fi

- Many public Wi-Fi hotspots—like those at libraries, coffee shops and malls—aren't secure and might not protect your passwords, messages, photos, and other data. Check with an employee before connecting if you are unsure.
- Public networks are a popular method for scammers to intercept your passwords, bank account numbers, and other sensitive information, so they can use it later to steal your money or identity.
- If you often rely on public Wi-Fi, consider setting up a virtual private network to protect yourself. Otherwise, wait until your internet access is firewalled (secure).

Use strong passwords and enable multi-factor authentication

- Practicing good password hygiene and enabling multi-factor authentication for sensitive accounts are two of the most powerful yet simple ways to boost cybersecurity.
- Use a lengthy and unique password for each account and never share your passwords. Re-using the same password for every account can lead to a hacker gaining control of all of your login credentials. If you're concerned about having to remember all those passwords, set up a password manager! This software-based service creates unique passwords, securely encrypts and stores them, and can auto-fill them when you access your accounts.
- You can use many methods of multi-factor authentication such as your cell phone, emails, backup codes, and authenticator apps.

Keep your software up to date

- Check to be sure you're running the latest computer operating system, antivirus software, and web browsers.
- Install updates as soon as they become available.

Report cyberbullying and harassment

- Harassment that happens in email, text messaging, online games, or on social media is cyberbullying. It might involve trolling, rumors, or photos passed around for others to see—and it can leave someone feeling angry, sad, or upset.
- If you think you or someone you know is the victim of cyberbullying, don't keep it a secret. Reach out to at least one person you trust—such as a close friend, family member, counselor, or teacher—who can give you the help and support you need.
- And don't be a part of the problem. Avoid forwarding inappropriate messages or images and tell others to stop. You can also report cyberbullying to the website or network where you saw it.

Get help

- If you feel that you're in immediate danger, contact your local police department or dial 911.
- If you or someone you know is being bullied and needs immediate help, contact the National Suicide Prevention Lifeline online or call 1-800-273-TALK (8255).

If you think you've been the victim of an online scam, cyberattack, cyberbullying, or other harassment, be vocal about your experience. You're not alone—and there's no reason to feel embarrassed about what happened. Immediately talk to an adult who can contact your local police and your financial institution if money has been taken from your account. You can also report the scam online to the Federal Trade Commission.

For more information, please visit the Cyber Safety Corner.