Fraud Prevention Tips

Keep a clean machine

Keep security software current
Having the latest security software, web browser and operating system is the best defense against viruses, malware and other online threats.

Automate software updates
Many software programs will automatically update to defend against risks. Turn on "automatic updates" if the option is available.

Plug & Scan
USBs and other external devices can be infected by viruses and malware. Use security software to scan them.

Protect your passwords

Create strong passwords
Strong passwords are at least 12 characters long and contain a combination of letters, numbers and symbols. Consider using positive sentences or phrases that you like to think about and are easy to remember. For example, “I love country music!#1”

Unique account, unique password
Use strong and unique passwords for each account, and separate your work and personal accounts.

Write it down and keep it safe
Store your passwords in a safe, secure place away from your computer.

Lock down your log in
Enable the strongest authentication tools available, such as biometrics, security keys or a unique one-time code through an app on your mobile device. This is particularly important for accounts like email, banking, and social media.

Connect with care

When in doubt, throw it out
Links in emails, social media posts and online advertising are often how cyber criminals try to steal your personal information. Even if you know the source, if something looks suspicious, delete it.

Be careful about Wi-Fi hotspots
Limit the type of business you conduct on Wi-Fi hotspots and adjust the security settings to limit who can access your device.

Protect your money
When banking and shopping, check that the site is security enabled. Look for web addresses with “https://” which means the site takes extra measures to help secure your information. “http://” is not secure.

Be web wise

Stay current
Keep pace with new ways to protect yourself online. Check trusted websites for the latest information and encourage friends and family to be web wise.

Think before you respond
Be wary of messages that offer something too good to be true, ask you to share personal information, or pressure you to act immediately.

Own your online presence

Protect your personal information.
Personal information, such as your purchase history or location, has value to cyber criminals. Be thoughtful about who gets that information and how it’s collected through apps and websites. Also, consider what your posts reveal about you and who might see them.