Identity Theft

BE CYBER SECURE

Always make sure you have up-to-date and active security software to protect yourself.

Firewall Protection

A firewall is basically a software program or a piece of hardware that helps to screen out malware and hackers that try to reach you through the Internet while you are on it.

Anti-Virus and other Anti-Malware Programs

Don't assume an anti-virus program offers protection against all kinds of malware. Viruses are one type of malware. Other types, including the information-stealing malware known as spyware, may not be covered by an anti-virus program. Investigate security software programs and make sure yours is comprehensive.

In addition, here are some additional ways to keep you cyber secure.

1. Always update. Keeping your operating systems, security software programs and browsers current can help secure your identity. Updates provide new patches for any security weaknesses.
2. Evaluate your browser's privacy settings, plus think about limiting or disabling cookies—those tiny bits of data used by web servers to identify users. Some cookies are useful, but others can be used maliciously and collect information about you.
3. Explore security options for all devices that connect to the Internet, including gaming systems.
4. Make sure mobile devices aren't set to automatically connect to nearby Wi-Fi, as this can expose you to unsecured network.
5. When not in use, disable mobile device features that connect you to other devices.
6. Set mobile phones, tablets and laptops to lock automatically after five minutes or less of non-use.
7. Back up your data regularly.
8. Before disposing of a computer, mobile device or any Internet-connected item, completely and permanently remove all personal information from it.
9. If you use an at-home wireless network, take steps to secure it. Otherwise, unauthorized users may be able to access your personal information, see what you're transmitting and download malware.
    - Make sure your wireless router's encryption feature is turned on.
    - If your wireless router comes with a built-in firewall feature (which is typical), turn that on.
    - Change the default name the manufacturer gave the router to one only you would know.
    - Routers also come with a default password. Change it to one that's hard to crack.
    - Many router manufacturers release security updates. Regularly check for new firmware updates.

Identity Theft

BE CYBER SECURE (cont.)

- Create strong passwords that are at least 10-12 characters long and include a combination of capital and lowercase letters, digits and special characters. Don't make them predictable. Change them frequently.
- Consider using a password manager to create complex passwords without needing to remember them.
- Don't use the same password for multiple accounts.
- Don't open emails from unknown senders.
- Never email financial information or your social security number.
- Download software or email attachments only from sources you know are trustworthy.
- Read all disclosure information before downloading software, including apps.
- Always type authenticated web addresses directly into your browser bar instead of clicking links.
- Limit what you share on social media. Consider increasing your privacy settings.
- Don't stay signed into accounts. When you are finished, log off and close your browser.
- Close all pop-up windows by clicking on the "x" in the title bar. Consider using a pop-up blocker.
- Don't put unknown flash drives into your computer. Use two-factor authentication for online accounts when available. This is when you provide two different ways to verify yourself, such as a password and a phone number, to better protect you.