Be Cyber Secure

Harris County FEDERAL CREDIT UNION

1. Make sure you have up-to-date and active security software that includes:
    a. 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.
    b. ANTI-VIRUS, ANTI-MALWARE PROGRAMS & OTHER PROTECTION. Don't assume an anti-virus program offers protection against all kinds of malware. Viruses are on 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.
2. Update, Update, Update! Keeping your operating systems, security software programs, and browsers current can help secure your identity. Updates provide new patches for any security weaknesses that might have been found.
3. 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.
4. Explore security options for all Internet-connected devices including gaming systems, phones, TV, tablets and even security systems.
5. Make sure mobile devices aren't set to automatically connect to nearby Wi-Fi, as this can expose you to insecure networks or fraudulent networks.
6. When not in use, disable mobile device features that connect you to other devices like blue tooth or 'near field' connections.
7. Configure mobile phones or tablets to lock automatically after a few minutes or less of non-use. Also ensure you have a complex password or PIN (more than 4 digits) set up on the device.
8. Laptops are popular targets for identity thieves. Don't store personal information on yours and consider using a laptop lock. It is good practice to save your documents and important data to a portable drive or cloud-based storage.
9. Back up your data regularly. If your computer or device is compromised or stolen, you'll still have access to important files.
10. 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, or download malware.
    a. Make sure your wireless router's encryption feature is turned on.
    b. If your wireless router comes with a built-in firewall feature, turn that on too.
    c. Change the default name the manufacturer gave the router to one only you would know.
    d. Routers also come with a default password. Change it to one that's hard to crack. A password that is over 8 characters long and contains upper- and lower-case letters, numbers, and special characters.
    e. Turn off your Wi-Fi network when you're not using it for an extended period. Like when you go on vacation or extended stays away from home.
    f. If possible, turn off 'broadcasting' your Wi-Fi network, which will keep guests or unwanted users from seeing your network as 'available'.

Be Cyber Secure

More Ways to Be Secure Online

1. 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 and consider using passphrases. Change them frequently.
2. Don't use the same password repeatedly or on multiple accounts. If identity stealing hackers get it from one account, they will try it on other accounts.
    a. It is a good idea to use a passkey or a secured password log to save your passwords in – don't use the browsers built in saver.
3. Don't open emails from unknown senders.
    a. Sometimes fraudsters use familiar names on emails to get you to open, respond or download an attachment. Be sure to verify the email address matches your senders name.
4. Never email financial information or your Social Security number.
5. Download software or email attachments only from sources you know are trustworthy and that you're expecting.
6. Read all disclosure information before downloading software and apps.
7. Always type authenticated Web addresses directly into your browser bar instead of clicking on links.
8. Limit what you share on social networking sites. Consider increasing your privacy settings.
    a. It is a good practice to include 2-step authentication on your social networking sites. So that Hackers can not attempt to access your private information.
    b. If your profile is public or you have unknown 'friends', it is not a good idea to share when you will be on vacation or away from your home. Thieves can use this information to steal identity or rob your home.
9. Don't stay signed into accounts. When you are finished, log out and close your browser.
10. Close all pop-up windows by clicking on the X in the title bar. Consider using a pop-up blocker.
    a. Don't click on any unknown links on any unknown web pages. These pages could be built to download malware or a virus onto your device.
11. Don't put unknown flash drives into your computer. They could contain malware or a virus.
12. Before disposing of a computer, mobile device, or any Internet-connected item, completely and permanently remove all personal information from it.
    a. You want to delete all personal documents and pictures from hard drive.
    b. Delete all Internet history, passwords, and sign out of the Internet browser.
    c. Sign out and remove saved passwords from any applications and or programs.
    d. Perform a system restore so that the device is like 'new'.
    e. Consider taking your device to an electronic store for proper disposal.