CS CYBER SECURITY & YOU

PROTECTING YOURSELF ON MOBILE DEVICES

As threats continue to evolve and adjust based on user habits, it's important to secure mobile devices properly. Here are some tips to protect you and others from cyber-attacks and viruses on your devices.

ACCESSING YOUR DEVICE

One of the most important things you can do to safeguard your device is to set a **strong passcode**. When setting a passcode, data protection will be turned on and encrypted. For another layer of security, set up **facial recognition** to quickly unlock your device. It is recommended to set your screen to automatically lock within the shortest amount of time possible.

Strong Passcode Tips:
- Avoid personal information and dictionary terms
- Include letters, symbols, and numbers
- Use a minimum of eight random characters

APPLICATIONS

Read the fine print: Did you know that nearly every app collects data which can include your name, date of birth, credit card and bank account information, location history, contact list, photos, and more? That data can be stolen and used by criminals for fraud. Be cautious when downloading any app that requests a lot of permissions. Set up Multi-Factor Authentication when it is an available feature.

LOCATION SERVICES

Apps can use location-tracking services to deliver information such as traffic updates, weather, and driving directions. While useful, keeping these services turned on at all times can be risky. When possible, only allow apps to access location services while they are in use or block access entirely.

MANAGING LOCATION SERVICES

CLICK FOR APPLE INSTRUCTIONS

CLICK FOR ANDROID INSTRUCTIONS

ANTI-VIRUS PROTECTION

Just like desktops and laptops, your mobile device can benefit from having anti-virus installed. They can block potential threats as well as verify Wi-Fi network security. There are many available such as Microsoft Defender, Norton Mobile Security, and McAfee Mobile Security.

OUT-OF-DATE DEVICES

Keeping software **up to date** is essential to protecting yourself against malware and other cyberattacks. However, automatic support ends after a while. It is highly recommended to replace the device before or when this happens. Samsung provides updates for up to four years, Apple provides updates for iPhones between five and six years, and Google supports Pixel phones for a minimum of three years. For other devices, check the manufacturer's website.

PARENTAL CONTROLS

Parental controls can be set up to **restrict children's access on devices** through features like website filtering and screen time management. Settings can apply restrictions based on the child's age, prevent password and account changes, and limit access to certain apps. Apple has a built-in ScreenTime app. Android devices offer Family Link. Of course, other parental control apps are available for download.

QUICK TIP

Keep your smartphone protected by installing new updates as they are released. A good option is to turn on automatic updates.

sources:

watchfuldad.com   apple.com   google.com   verizon.com