7 CYBERSECURITY TIPS TO SECURE YOUR MOBILE DEVICE

Securing your mobile device is an important step to help protect your personal information and prevent cyberattacks.

Below, we guide you through 7 tips to help defend against cybercriminals.

1 USE STRONG PASSWORDS OR PINS

Create a password that is eight or more characters long and contains alphanumeric characters. When using a PIN, it shouldn't be a number that's easy to figure out, like your date of birth, or contain repeating numbers, such as 5555.

Hint: PINs can be easily associated to a word that is easy to remember. Look at your keypad and see what numbers coordinate with a word you choose.

2 ENSURE PUBLIC OR FREE WI-FI IS SAFE

Free Wi-Fi is always appreciated, but not always secure. These open networks allow cybercriminals to access the network and potentially steal your passwords, usernames, and other sensitive information. Make sure you connect to public Wi-Fi that requires a password to help keep your information secure.

3 UTILIZE A VPN

A VPN, or Virtual Private Network, allows you to connect to the internet through a private and secure network. Think of this network like a tunnel between your mobile phone and the internet, and there is no way to see inside. The information passed through it is encrypted, which turns your text into a puzzle that is hard to solve, and it cannot be seen from the outside. This makes it much more difficult for anyone to spy on your online activity. To use a VPN, choose a reputable provider and download their software or app. Then, you can connect and browse the internet as usual, and all your online activity will be encrypted and secure.

4 TAKE PRECAUTIONS WHEN USING BLUETOOTH

While Bluetooth technology on mobile phones offers convenience and ease of use, it can present vulnerabilities that allow hackers to listen in on your conversations, access your data, and transfer malware to your phone. To help minimize these, set your device to non-discoverable, don't accept unsolicited requests, use a Bluetooth headset or speakerphone, regularly review the list of devices that are paired with your phone, and don't download apps from untrusted sources.

BRP

5 SECURE YOUR FILES AND APPS

The files you download and apps you install may contain malicious code or expose vulnerabilities cybercriminals will use to access your personal information. Some ways you can help protect your information include using a mobile antivirus app, keeping all apps up to date with latest security updates, only grant access to data the app needs to function properly, download apps from trusted sources, and refer to the tips above about public Wi-Fi and trusted sources.

6 USE A PASSWORD MANAGER

A password manager can generate strong passwords, store your passwords in an encrypted format (making it harder for cybercriminals to read the passwords even if they gain access), and integrate with two-factor authentication systems to add an additional layer of security by requiring users to provide two ways of confirming their identity.

7 BE DISCERNING

Regardless of the security measures you put in place, misfortunes can happen. Keep a backup so you can restore your data. Automatic backups can save time and take place when you're not using your phone.

Talk to our team about your options to help protect yourself online and offline.

BRP