CYBER SECURITY & YOU

AUGUST 2022

LASERS

SMARTPHONE SECURITY

Smartphones are now just as powerful and functional as many computers. With mobile cybersecurity threats out there, it is vital to protect your smartphone. Here are some tips from the Federal Communications Commission that can help reduce the risk of exposure to threats:

Set a passcode for unlocking your device.

To prevent unauthorized access to your phone, set a passcode or Personal Identification Number (PIN) as a first line of defense in case your phone is lost or stolen. Configure your phone to automatically lock after five minutes or less when your phone is idle.

Do not modify your smartphone's security settings.

Do not alter security settings for convenience. Tampering with your phone's factory settings, jailbreaking, or rooting your phone undermines the built-in security features offered by your wireless service and smartphone, and makes it more susceptible to an attack.

Backup and secure your data.

You should backup all the data stored on your phone, such as contacts, documents, and photos. These files can be stored on your computer or in the cloud. This will allow you to conveniently restore the information to your phone should it be lost, stolen, or erased.

Only install apps from trusted sources.

Before downloading an app, conduct research to ensure the app is legitimate. Check app reviews to confirm the legitimacy of the app, and compare the app sponsor's official website with the app store link to confirm consistency. Many apps from untrusted sources contain malware that once installed can steal information, install viruses, and cause harm to your phone's contents. There are also apps that warn you if any security risks exist on your phone.

ADDITIONAL RESOURCES:

Apple iOS: *https://support.apple.com/guide/iphone/use-built-in-security-and-privacy-protections-iph6e7d349d1/ios*

Google Android: *https://www.android.com/safety/*

Understand app permissions before accepting them.

Be cautious about granting applications access to personal information on your phone or letting the application have access to perform functions on your phone. Also check the privacy settings for each app before installing.

Enable remote device location and wiping.

An important security feature widely available on smartphones, either by default or as an app, is the ability to remotely locate and erase all the data stored on your phone, even if the phone's GPS is off. In the case that you misplace your phone, some applications can activate a loud alarm, even if your phone is on silent. These apps can also help you locate and recover your phone when lost.

Update your smartphone's software.

Keep your phone's operating system software and installed apps up-to-date by enabling automatic updates or accepting updates when prompted. By keeping your operating system current, you reduce the risk of exposure to cyber threats.

Be smart on open Wi-Fi networks.

When accessing public Wi-Fi, your phone is an easy target of cybercriminals. Limit your use of public hotspots and instead use protected Wi-Fi from a network operator you trust or mobile wireless connection to reduce your risk of exposure. Always be aware when clicking web links and be particularly cautious if you are asked to enter account or log-in information. ■

QUICK TIP

Wipe the data on your old phone before you donate, resell, or recycle. Your smartphone contains personal data you want to keep private when disposing of it.

source: *www.fcc.gov*