SAFETY & SECURITY TIPS ON-THE-GO

Smartphones, tablets and other mobile devices carry more personal data than ever before, which means you should take certain precautions to safeguard the information in the event of a lost or stolen device.

10 Security Precautions You Should Take on Every Device...

1. **Keep a clean machine.**

Running the most recent versions of your mobile operating system, security software, apps and Web browsers is the best defense against malware, viruses and other online threats.

2. **Don't lose track of your device.**

Avoid putting down your devices in public places or in a taxi. The small size and portability make them easy to lose or steal. A brightly colored case or sticker on your device will increase the chances you won't leave it behind.

3. **Protect your personal information.**

When using a public, unsecured wireless connection, avoid using apps or websites that require you to enter a password. This applies to the wireless networks provided on many airlines, as well as Wi-Fi connections in places like coffee shops, hotels, airports and libraries.

4. **Connect with care.**

Switch off your Wi-Fi and Bluetooth connections when not in use to help prevent malicious parties from connecting to your device without your knowledge. If you're banking or shopping, remember, a 3G or 4G connection is safer than an unsecured Wi-Fi connection.

5. **Secure your device.**

Activate key-lock features and/or use a passcode. If your device allows for a complex password, take advantage of the feature.

6. **Back it up.**

Sync your contacts, photos, videos and other mobile device data with another device or cloud service on a weekly basis.

7. **Provide contact info.**

Do an Internet search for the best way to add your name and an alternative contact number to your lockscreen, in case a Good Samaritan finds your device. (Don't use highly personal information, such as your home address.)

8. **Activate locator apps.**

Many manufacturers have free apps you can download to help you locate your device in the event it gets lost or stolen. These apps often allow you to remotely lock the device or wipe data.

9. **Think before you app.**

Only download apps from reputable sources, like verified app stores. Understand what information (i.e., location, social networking profiles, etc.) the app would access and share before you download.

10. **Record the serial number.**

By dialing these five characters – *#06# – you can access your phone's unique, 15-digit International Mobile Equipment Identity (IMEI) number. Write this number down and store in a secure location, so you can report it if your phone goes missing.

Other Security Features

In addition to activating locator apps and backing up your phone, there are other ways to safeguard your device. Before purchasing or downloading other services, check with your smartphone carrier or service provider to see what additional security measures it provides. These might include:

- Remote wipe, which enables you to remotely clear all of your data–including email, contacts, texts, and documents–off your device.
- Siren trigger, called the "scream" feature–a high-pitched sound on your smartphone that lasts for about one minute. The scream may be used to draw attention to the smartphone so someone might answer it; or its owner may find the person who has the device.

SMiShing and Spam...

"SMiShing" is the mobile version of phishing, and occurs when someone sends a SMS/text message asking you to provide personal and/or financial information by clicking on a link or responding via text or phone number.

- Think before you act. Be wary of communications that implores you to act immediately, offers something that sounds too good to be true, or asks for personal information.
- When in doubt, throw it out. Just like email, requests for personal information or for immediate action are almost always a scam.
- Place your cell phone number on the National Do Not Call Registry: www.donotcall.gov
- If you receive a spam text, many mobile service providers will allow you to report the message by forwarding it to 7726 or "SPAM."

If you lose it...

If you can't find your smartphone, call your mobile number to make sure it's not just misplaced and nearby. Hopefully, either you will hear your phone or an honest person will answer and assist in returning it to you.

Contact your mobile service carrier immediately to report your device lost or stolen, and to freeze your service. Your service provider may be able to send a "wipe" command that will remotely erase all data and settings. Reporting the loss will also be essential to avoiding any charges (for phone calls or downloaded apps) that may have been incurred while in another person's possession. For more information, visit: www.fcc.gov/stolen-phones-contact-numbers

Change all passwords to any service that is automatically connected to your device, such as email, payment services, texting services, online banking account and social networking account.

Contact the police. For your safety, do not attempt to track and recover your device yourself. Provide as much information as possible to the police. Also, carriers may be able to assist in disabling your device if a police report already has been filed.

After you find it...

Update software. Download updates of your operating system, software, and apps. These updates protect against viruses and malware in the event your device became infected.

Secure your accounts. Recovering a lost device is a good time to create new logins. Strengthen passwords to use upper and lower case letters, numbers and symbols and enable two-factor authentication when offered.

Pay it forward! Be a conscientious citizen if you find an orphaned phone, tablet or other device. Try to contact the owner or turn it over to law enforcement or the property owner.