Smartphone Security Tips

Each day, 200,000 devices are lost, stolen or damaged. Phones today contain a large part of our life. This includes financial, photos, calendars, contacts, messages, passwords, and more. Just like we would protect our wallet, it is very important to protect our phone for peace of mind that your data will not end up in the hands of those who could use it to do you harm. Whether you become a victim of a phone hacker, virus, lose your phone, or just stops working, there is a lot at stake should your phone data get compromised. Today's phones offer many ways to protect you, if you use them right. The most likely cause of a security failure is simply a failure on your behalf to secure your stuff. You are the weakest link.

Phone Setup - Settings

- With the variety of phones and operating system (OS) versions today, it can be hard to find where to change one of the hundreds of settings your phone has. Using the \Setting\Search function can save you a ton of time. Many articles and tips try to help by giving directions on where the setting is located, but in many cases it has moved, is under a different name, or your phone is different. I use the \Settings\Search function almost all of the time now.
- Your screen MUST be locked when you are not using it or when it is turned on to prevent unauthorized access if lost or stolen. As of 2018 only 50% of people use a phone lock. For Android go to Settings\Lock screen. For Apple go to Settings\Touch ID & Passcode.
  - PIN/Passcode - Use 4-7 digits as a first line of defense. I recommend 6-7. Do not use overly simple codes like your year/month/day of birth, phone number, address, or other guessable sequence of numbers.
  - Fingerprint - I recommend, scan two different fingers from each hand to make it easy to open with either hand.
  - Unlock pattern - I don't recommend, too simplistic or easy for thief to recreate.
  - FaceID - I don't recommend, fingerprint is more secure than FaceID.
  - Passwords - I don't recommend it.
- Configure your phone to lock after 1-2 minutes when your phone is idle.
- Enable "Find My Phone" on Apple or "Find my Device" on Android to see the last known location and the ability to lock or erase the phone if needed.
- Record your International Mobile Equipment Identification (IMEI) number in your Password Manager. It usually is found in your phone settings, online account, printed on the phone (near the battery or SIM), or on the original packaging. Also, record the Serial Number of the phone in your Password Manager. You can use this when you file a police report or talk to your service provider.

Backup

- Backup your accounts, contacts, photo/video, text msg, call logs, email, settings, and apps. I recommend backing up to one or more cloud services. Backup allows you to restore the information should the phone be lost, stolen, broken, erased, or even setting up a new phone. Below are the most popular cloud services:
  - Apple iCloud - Apple users get 5 GB for free then pay $0.99 a month for 50 GB.
  - Google Drive - Google users get 15 GB for free then pay $1.99 a month for 100 GB.
  - Samsung Cloud - Samsung users get 5 GB for free and backup is set up by default with Samsung phones.
  - Microsoft OneDrive - 5 GB free. If you are subscribing to Microsoft 365 Office you get 1 TB.
  - For family photos use a site like Amazon Photo, Google Photo, Adobe, and others. For videos use YouTube.
- See previous presentations on backup and cloud services.

Passwords

- You MUST be using a password manager. I recommend the free version of Bitwarden: https://bitwarden.com
  - You don't have to remember each password, so each one can be unique, long, and strong.
  - Available on multiple devices Phone, Tablet, Laptop, and Desktop. Windows, Android, and Apple.
  - Strong passwords can be generated for you.
  - Makes it easy to change passwords.
  - Cloud backup, track old passwords, challenge questions, and store credit card and other sensitive info.
  - Safer than storing Accounts and Passwords in a Browser or other methods.
- Many Apps like Bitwarden Password Manager, banks, or financial apps allow fingerprints to be used.
- See the past presentation "Online Security & Passwords" from April 2022.

Lost or Stolen Phone

- A thief can watch a user unlock their phone, then steals the phone and immediately transfers money from apps like Vemo, Zelle, PayPal, Cash App, or Crypto to the thief's account. Make sure these apps require an additional password or fingerprint to unlock them. Some thieves may also attempt to change the password associated with the owner's Apple ID or Google Account after they steal the phone. This locks the owner out of their phone. Enable

account restrictions to prevent your password from being changed. These thefts happen in places where people tend to be inattentive when drinking and socializing at bars. Self-defense: Cover your screen in public and be aware.
- Thieves who steal a locked phone usually attempt to sell the phone ASAP before the phone gets reported as stolen.

Steps to take when your phone is lost or stolen:
1. Check that it isn't just misplaced by calling it first. If no answer, use the Apple Find My iPhone, Google's Find My Device, or Samsung Find My Mobile. Go to the website, log in using your credentials, and follow the instructions. If it is somewhere you haven't been or appears to be on the move, someone else has your phone and it may be stolen. Thieves usually turn the phone off immediately after stealing, the Find will only show the last location when it was on. It may be tempting to go and confront the supposed thief, law enforcement agencies strongly advise against this.
2. Lock your phone remotely using the Find feature. You can also leave anyone who finds your device a message or a phone number where you can be reached. If you're certain you won't be getting your phone back, you can perform a remote erase.
3. Call your cellular provider to suspend service and prevent unauthorized charges like overseas calls. If you're unable to perform a remote lock, your provider might be able to deactivate the device.
4. Change your email, bank, financial, and shopping passwords if any used auto login or saved passwords.
5. Call your bank to let them know your phone has been stolen and ask if there has been any recent activity on your account/cards. Monitor your accounts in the days and weeks after and watch for any suspicious activity.
6. File a police report via a local non-emergency number or web site. Law enforcement agencies don't have the resources to investigate every case of a stolen phone, if you're able to tell them where your phone is (using a finder), they will be more likely to be able to help you recover it. If your credit card has been used as a result of your phone being stolen, your financial institution or insurance claim may need your police report number as proof your device was stolen before they will reimburse your losses. When reporting your phone stolen, you should provide police with the device's IMEA number to identify it as yours and reunite you with it if found.
7. Contact your insurance company if you have insurance for your phone that protects against loss or theft. You might have purchased it when you bought your phone or it may be covered under your home insurance.
- Practice what to do before things go bad:
  Apple: https://support.apple.com/guide/icloud/erase-a-device-mmfc0ef36f/icloud
  Android: https://support.google.com/accounts/answer/6160491

Other Tips

- Keep Your Phone, OS, and Apps Updated - A Virus or Hacker can exploit vulnerabilities. Manufacturers stop support for the latest operating systems for phones that are 3-5 years old.
- Only install apps from trusted sources.
- Delete apps you don't need anymore.
- Understand app permissions before accepting them. Example: a weather app does not need access to your contacts or photos.
- Watch out for Scams. See the past presentation on Scams.
- Wipe data on your old phone before you donate, resell, or recycle it. Usually in \Settings\About\Reset
- Avoid public charging stations unless there is an emergency. Hackers have been known to set up fake charging stations in scams known as "juice jacking." After you plug in, they can access your phone's data or install malware on the device.
- Some people recommend a VPN service. I recommend you check your browser for the lock symbol for secure sites.
- Do not "Root" your Android or "Jailbreak" your iPhone. This is a process that gives you complete access of your device, but in doing so, removes many of the safeguards that the manufacturers have put in place.
- Turn off Bluetooth and WiFi when you're not using it. This one is especially important if you're in public spaces. If you leave your Bluetooth and WiFi access on, it may make it easier for hackers to connect to your device and gain access to files and information. One way this can happen is a hacker can pretend to be a legitimate device that makes a connection request to your device. Once you grant access, the hacker can exploit security holes in other programs and apps to steal your information or get sensitive files.
- Almost everything we have talked about for a phone pertains to laptops. Protect yourself.

Additional Links and Information

Carondelet Tech Help Resources: https://carondeletvillage.org/tech-help-resources/
Questions or comments can be sent to: TCKreuzer@gmail.com