

Mobile Device Safety & Security Tips



Here are 10 tips for Mobile Device Safety:

Texting & Driving

Don't text and drive - it can kill you or someone else. Don't text and walk - you can get hurt badly. It's not just common sense; maintaining situational awareness is also important for officer and public safety. If you get a message you have to answer, you can afford to take a few minutes to find a safe place to do it. Guard your emotional safety as well as your physical safety: pay attention to the world and the people around you, because your mobile device use can intrude on personal relationships. Even when nothing inappropriate is going on, allowing yourself to be distracted can let you miss important moments with your loved ones. Set limits for yourself and your family, like no texting at the dinner table, or no phone for half an hour before bed. (Studies show that prolonged bright-screen use before bed can fool your brain's sleep switches, and thus degrade the quality of your sleep. Shift workers are even more at risk.)

Inappropriate Texts & "Stranger Danger" (seriously...)

Never send nude or suggestive pictures of yourself or talk or text with strangers about sex using your mobile device. You never know where your pictures or words will end up, or who will see them. The consequences can be devastating. It seems like every month there's a story like this: a police officer is caught on camera, posing (or worse) with someone, the picture or video ending up on YouTube or Facebook. When in doubt, do what the digital natives in your agency do: assume there's no privacy. Anywhere. People like to film police on duty these days, and even off duty, there is always a risk of being recognized and identified. Your new rule of thumb: don't do it, even if it seems harmless; maybe even *especially* if it seems harmless.

Protect your Mobile Device (Phone, PDA, iPad, etc...)

Protect your mobile device like you would your purse or wallet. The information it potentially contains, and the device itself are valuable to a thief. An iPhone or Samsung thief may never get into your device if s/he is only interested in the money the device can fetch on the black market - but the person who buys it might. Keep your device on your person at all times, secured either within a bag or pocket that's hard to reach into and snatch valuables from. If you use a GPS device in your vehicle, don't leave it in plain view. Store as much of it as possible in a glove compartment or under the seat, or even take it with you when you go places.

GEO-Tags/BlueTooth

Only keep geo location, Bluetooth, and Wi-Fi features on your mobile devices active when you are using them. Be aware that social networking sites may automatically post your location if you have geo location enabled. Don't "check in" with your location if you're alone. It's not about how confident you are in your defensive tactics - it's common sense officer safety. Worst case, why invite an ambush or stalker?

Passcodes or Fingerprint

Secure your phone or tablet by using a pass code and, if your device has it, encryption. An unauthorized user will have a much more difficult time making calls, sending texts, or stealing your personal information.

Downloading Applications

Only install applications from trusted sources, and read the privacy policy to be sure you understand what data you're sharing. Applications from unknown sources can contain spyware or malware, and even trusted applications may gather information you're not comfortable sharing. If your smartphone has an Android operating system, this is even more important: there are no controls over what shows up in the Android apps directories, compared to iTunes. Nonetheless, malware has shown up on both iPhone and BlackBerry platforms, so don't assume that either one is totally safe.

Software/Operating Systems

Keep your device software up to date. Keeping your mobile device's software and the applications on it up to date helps keep your device secure against compromise, as developers are always fixing security holes and other bugs in their tools.

Malware Protection

Install and use virus and malware protection software on your mobile device, and make sure you keep it up to date. This software will help to warn you if your device has been compromised. A good third-party source for software reviews is Cnet.com, which provides both editorial and consumer community ratings and reviews.

To Click or Not To Click

Don't click on links in emails or text messages unless you trust the sender and were expecting to receive a link from them. As with larger computers, malware, spyware and phishing attacks against mobile devices are often initiated by clicking on links. The same goes for social networking sites. Here the "bad" links can be harder to spot because of the constant flow of information and the bad guys' adapting their language to seem less suspicious. Be alert for out-of-character posts from your friends or followers, including both public and private messages. If you think their account has been compromised, be a good friend and tell them.

Beware of Signs

Be aware of the signs of potential compromise of your mobile device **including** decreased device performance, random functions, or calls, texts or emails to numbers and email addresses you don't recognize. Do you apps behave strangely; other than normal...You call or message history have unknown entries... Excessive Data Usage (unexplainable)...

Conclusion

Do mobile devices and social networking security take work? Absolutely!! Fortunately, though, resources both online and off are available help you to research the right tools, use the right features on your device in the right way, and stay on top of changes as they occur. The risks are not simply immediate to your safety but are also hidden and potentially long term. It's unfortunately, but true, that in today's modern world, "Officer Safety" isn't just about defensive tactics and situational awareness anymore; it includes technology awareness and understanding as well.