SecurityAwarenessNews

the security awareness newsletter for security aware people

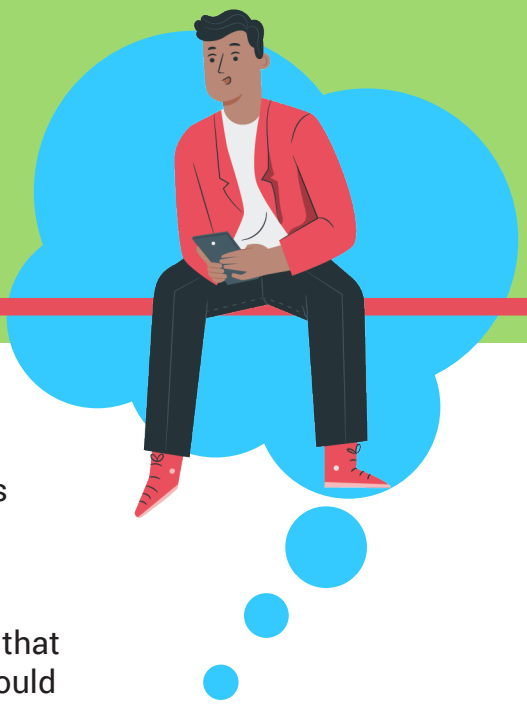
Mobile Device Security

The Physical Side of Mobile Device Security

Mobile Threats and How to Avoid Them

Mobile Security Tips for Travelers

The Physical Side
of Mobile Device Security

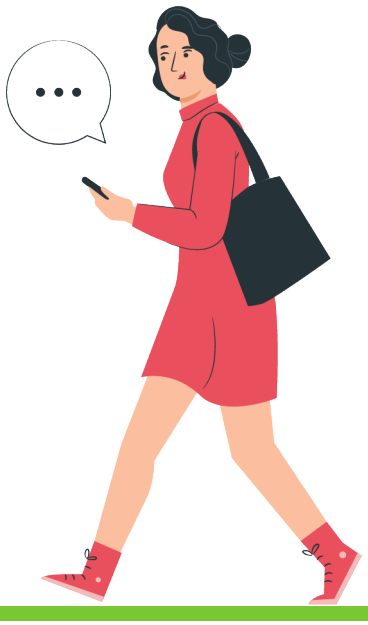


Modern smartphones and tablets come equipped with impressive amounts of power and accessibility. They also place a tremendous amount of confidential data in a dangerous location—the public. **After all, where we go, our sensitive data follows.**

Think about devices and data like this: imagine you own a safe that securely stores the personal items you care the most about. Would you drag that safe out with you in public? Would you pull up a chair for it at a restaurant or throw it on an airplane tray table? **Probably not.** The whole idea is about protecting whatever is in the safe, which means leaving it in a secure location and not subjecting it to potential loss or theft, even though it's locked.

Thanks to mobile devices, we're carrying our "safe" around with us. What would happen if your smartphone ended up in the wrong hands? How much access would someone have to your personal life? All of your contacts, emails, messages, social media accounts, and maybe even your bank accounts, are now at the literal fingertips of a stranger.

You, of course, have strong passcodes protecting your devices, but we use this example to illustrate an important fact: **physical security is just as essential as cybersecurity.** When we're out in public, we need to use situational awareness so that we don't lose mobile devices or have them stolen. We need to make sure no one can see our screens when we access confidential data. We need to use common sense, like not leaving a device unattended in plain sight, such as in a vehicle or a hotel room.



Combining physical security and cybersecurity is the best way to combat threats to privacy. Remember: all a cybercriminal needs to compromise our organization or your privacy is one unsecured door. Mobile devices happen to have a lot of doors. So, remain vigilant, stay alert, and always follow our organization's mobile device policies.

Mobile Threats

And How To Avoid Them

Smartphones and tablets allow us to work from almost any location and improve our quality of life. However, the use of these mobile devices can present significant security challenges from both a personal and professional standpoint. Here are five common threats to watch out for and how to avoid them:

Network Spoofing

A mobile device is only as secure as the network it's connected to, which is why network spoofing is so dangerous. In this attack, cybercriminals set up imposter WiFi networks that look legitimate—*"Airport WiFi," for example*—and use them to steal data. Circumvent this threat by disabling the auto-connect option on your device and verifying the legitimacy of every network before joining.

Unpatched Vulnerabilities

An out-of-date device is susceptible to malware and other unnecessary risks because it does not have the latest security patches. Make sure to keep all software and apps current, and enable automatic updates wherever they're available.

Smishing

With messaging apps exploding in popularity, it's no surprise that smishing—phishing via text message—attacks continue to rise. Never click on links in, or respond to, text messages from unknown users, especially those that use threatening or urgent language, such as claiming that a bank account has been compromised.

Malicious Apps

Scammers create malicious apps—often impersonating legitimate apps—to invade privacy. Before downloading and installing any software, research the developers, and only download from verified sources. Once installed, carefully review permissions and security settings to ensure the app isn't collecting more data than is necessary for it to function.

Malware and Viruses

Malicious apps and small screens—combined with the click-happy nature of humans—increase the likelihood of malware and other infections. Don't let your device get sick! Install antivirus and anti-malware software, and click (or tap) with extreme caution.

The benefits of using mobile devices should never compromise information security. Slow down, think before you click, and always follow our organization's policies.

SAC the security awareness™ COMPANY

Mobile Security Tips for Travelers

Travel brings a mix of concerns that include both cyber and physical security. Situational awareness is a traveler's best friend, particularly at airports and crowded transportation hubs. Use the following tips to prioritize your safety.

Use Common Sense

As obvious as this may sound, never take your eyes off your belongings or allow a stranger to watch them for you. Electronics are popular targets for thieves. Our computers and mobile devices contain massive amounts of highly sensitive information that, if lost or stolen, could lead to data breaches or identity theft.

Avoid Public WiFi

If possible, avoid connecting to public WiFi. But if you must, make sure you use a virtual private network (VPN). VPNs provide an encrypted connection that helps prevent cybercriminals from intercepting your internet traffic and stealing data. Even with a VPN enabled, it's still best to avoid accessing confidential data until you're on a secure, private network.

Don't Trust USBs

When you need to charge your devices, only use the power supplies you own. Public USB charging stations can be compromised and used to infect devices with malware. You should also never plug in a USB charging cable or flash drive that doesn't belong to you.

Privacy Takes Precedence Over Productivity

It's best to wait until you have privacy before accessing or discussing anything that could be deemed confidential. Should you need to work in a public space, use discretion. Make sure no one can peek over your shoulder to see your screen, and lower your voice when using the phone.

Plan Ahead

If there are apps or documents you know you'll need while traveling, download them before leaving. And even though theft or loss of a device is troublesome, you can mitigate the negative consequences by enabling "find my device"—a built-in feature on most modern smartphones that allows you to locate your device from a secondary device, ping the lost device to ring, or completely wipe it and restore to factory default. Alternatively, consider getting a temporary phone that has limited access to sensitive information.

As always, be sure to check our organization's policies before installing any apps on work-issued devices or before connecting to our networks with a personal device. If you have any questions, please ask!