Security on the go

Keeping your mobile devices secure[1]

Mobile security is more important now that everyone is walking around with personal and professional data in their pockets. Follow good mobile security habits to keep your information protected.

Public Wi-Fi

When using public Wi-Fi, you send data across a network controlled by someone else. Hackers use Wi-Fi hotspots to lure users onto their own networks and steal their information. Never do anything with sensitive data on an open wireless network!

Check your connection settings and turn off "auto-connect to Wi-Fi." This will ensure that you don't accidentally connect to an open, possibly dangerous Wi-Fi network.

Encryption

Encryption is the process of turning your information and data into a code that is unreadable to anyone else. This prevents unauthorized users from accessing your data.

Use your organization's approved VPN provider on work devices. A VPN creates a secure tunnel that encrypts all of your internet traffic, keeping you and your organization safe from hackers.

Downloading apps

When downloading apps to your mobile devices or other smart devices, it is important to only download from a reputable app store!

Organizations often control downloadable apps. Many apps out there aren't held to a high security standard. Consider this when downloading apps on your personal device as well.

SMiShing and vishing

SMiShing (SMS phishing) is a form of phishing that comes to you as a text message. It could be an obvious spam text, or it might appear to be from someone you know and trust.

Most people don't have anti-malware software installed on these devices. That means that these attacks could be very dangerous.

Vishers make phone calls or leaving voice messages impersonating reputable companies to get people to hand over personal information like credit card numbers or Social Security numbers.

Lock it and secure it!

"Slide to unlock" is the easiest way to get into a phone or other device. This was the standard lock screen for many years until security became the focus of the lock screen.

The slide-to-unlock format is called a **gesture-based lock screen**. It is the most basic and the least secure. Its main goal is to protect your phone from unintentionally opening.

The most popular lock screen as of now is the **key-based lock screen**. A key-based lock screen uses a variety of alphabet, symbols, numbers, or a combination of them. This form of locking is beneficial for security purposes and unwanted gestures for opening the device.

And finally, the most cutting-edge security feature for lock screens is the **biometric-based lock screen.** This encompasses both a positive user experience and a high level of security. This form includes fingerprint and iris scanners and facial recognition. This type of security has some drawbacks, as the readers are prone to errors; however, if security is your top priority, this could outweigh the annoyances.

E-TECH