9.7.2 Mobile Device Security Facts

Mobile devices are used for everything from making phone calls to managing bank accounts, and everything in between. As such, they pose a unique security threat. A single smartphone sometimes contains more personal information than a desktop computer. And all that information is in a device that can be lost essentially anywhere. The following table lists methods for securing your mobile device:

Security Method	Description
Screen Locks	To secure access to a mobile device, such as a tablet or smart phone, configure the device's lock screen to use some sort of authentication. Several different types of lock screen authentication methods include: ▪ Swipe lock. Most mobile devices are configured to use a swipe lock screen. This means that anyone can unlock the device with a simple swipe of the screen; there's no authentication at all. For obvious reasons, this is not very secure. ▪ Biometric locks. The two most common biometric locks are fingerprint and facial recognition. With fingerprint recognition, the finger of the user is scanned and used to unlock the device. With facial recognition, the device's camera is used to scan the user's face and unlock the device. ▪ PIN. A PIN allows a user to enter the correct four or six numbers in order to unlock the mobile device. ▪ Pattern Unlock. Pattern unlock allows the user to create a line pattern on a nine point grid, used to unlock a mobile device. ▪ Passcode. Passcode authentication uses a user-defined password to unlock the device. The password can be a mix of letters, numbers, and symbols
Biometric Authentication	Biometric authentication is a type of authentication that relies on the unique physical characteristics of individuals to verify their identity for secure access. Some mobile devices support biometric authentication on lock screens. The two most common ones are fingerprint and facial recognition.
Multifactor Authentication	Multifactor authentication is a type of authentication that requires multiple authentication credentials to verify the user's identity for a login or other transaction. For example, you might require a user to enter a username, password, pin, and fingerprint before authenticating to a computer system.
Failed Login Attempts	Most mobile devices are configured by default to allow only a set number of failed login attempts, which is usually ten. If more than ten failed logins are attempted, the mobile device will automatically wipe the entire contents of the device and reset it to the factory defaults. It's important to make sure that this feature is enabled on all mobile devices. This is one of the best lines of defense you can provide to a mobile device. Even if the passcode or PIN aren't very secure, it will be pretty hard to guess the right one with only ten attempts at your disposal.
Device Encryption	Another line of defense that can be implemented, and is used by default on most new devices, is encryption. Encryption prevents someone from accessing the stored information in any capacity. This means even if someone got a hold of a device and were somehow able to copy the contents of the device, they wouldn't be able to view any of the information. It would be encrypted. There are two types of encryption methods used by mobile devices: ▪ Partial device encryption. With this method, only the sections of the device's storage that contain files are encrypted. This type of encryption is fast, but it doesn't encrypt deleted files, which can be recovered using special software. ▪ Full device encryption. This method encrypts every single sector of the device's storage, regardless of whether it has data or not. This protects the entirety of the device, including deleted files. If a mobile device doesn't encrypt contents by default, it's important to make sure that full device encryption is enabled and configured.
Remote Wipe	Remote wipe is used to remotely format a mobile device. It's a feature that's built into a lot of mobile devices, especially smart phones. But, it's also possible to use third-party software, such as Windows Intune, to achieve this functionality. Remote wipe requires some sort of connection to the device. This means that in order to send a remote wipe command, the device needs to be powered on and have cellular or Wi-Fi connection.
Device Locator	Many smart phones and tablets have a device location feature to locate a lost or stolen device. This feature is usually a proprietary service specific to the device manufacturer; however, there are also third-party apps that offer location services. If the service has been set up on a device, the owner can use a website or software application to identify the approximate location of the device on a map. The service can also tell the device to take a picture with both the front and back cameras, then send the pictures to you. This can further help identify the device's exact location.

Remote Backup Applications	Remote backup applications allow you to recover important business data and personal files (e.g., pictures and texts) from a lost, stolen, or broken phone. Most cellular providers offer some type of cloud backup service. In addition, each mobile OS offers their own proprietary backup service:
	▪ iOS devices have two different backup tools:
	  ▪ The desktop application iTunes can be used to backup and restore iOS devices. iTunes requires mobile devices to be connected to the desktop computer via a USB cable.
	  ▪ Apple devices can also use the iCloud service to backup and synchronize files and settings across all Apple devices (i.e., mobile and desktop devices). iCloud is a cloud-based backup service and requires the user to have

	an Apple ID, which needs to be logged into and configured on each Apple device. Apple devices can then synchronize and backup files over the internet.
	▪ Android devices use the Google sync service to sync and backup mail, contacts, calendar, and files across all android devices. Google sync is a cloud-based service and requires a Google account.
	▪ Windows Mobile devices have two backup tools:
	  ▪ OneDrive is Microsoft's cloud-based backup service and requires a Microsoft account.
	  ▪ Windows Mobile devices can also be backed up using a desktop computer with the Windows OS installed.

Authenticator Applications	An authenticator application is a specialized app called an "authenticator." The app is pre-set by you to work with the service and provides a constantly rotating set of codes that you can use to utilize two-factor authentication or verification. The codes in authenticator apps sync across your accounts and provide an extra layer of security. For example, implementing two-factor authentication on your Gmail account would require you to use your username, password and one of the generated codes from the authenticator apps to log in to your Gmail account. It may take a little longer to log in, but it provides you with an added layer of security.
OS Updates and Patches	Always keep the device's operating system up-to-date. Hackers are constantly trying to find new ways to exploit various technologies, and mobile devices are no exception. These exploits can be anything from relatively harmless adware to dangerous Trojans that take complete control of a device. The way a device receives an update depends heavily on the type of mobile device, the manufacturer, and, if it's a smart phone, the cellular carrier.
Trusted vs. Untrusted Apps	Applications for mobile devices can be placed into two categories: trusted and untrusted. ▪ Trusted apps are those that have been reviewed and approved by the device's app service. When approved, the app is signed with a certificate that identifies it as a trusted app. For the most part, this means the app is safe to install and does not contain malicious code. ▪ Untrusted apps are those that have not been verified and approved by the app service. While it's possible that an untrusted app could be entirely safe, it's just too risky to install one. In fact, most devices won't allow them to be installed by default. Software for mobile devices should be restricted to trusted app stores such as Google Play, the Microsoft Store, or Apple App Store.
Antivirus and Anti-Malware	It is a good idea to install an anti-malware app on mobile devices, especially devices that are used by an organization or connect to a company network. This will protect the device from malicious email attachments, downloads, or applications. It will also help prevent the spread of viruses onto a network.
Firewalls	Use a firewall to inspect network traffic and to allow or block traffic based on a set of rules.
Unauthorized Access	Because smart phones connect to so many networks, it is possible for someone unauthorized to access your data, mobile device account, location, camera, and microphone. There are several things you can do to mitigate this risk: ▪ Data: your phone is a unique vulnerability because it is so portable--it is very easy for someone to steal. In addition to protecting your data with basic security practices like locking your phone with a strong password, be aware of data theft from the inside as well. Mobile phones are computers that hackers can access using the same methods they use for desktop and laptop computers. Any financial, personal, or sensitive information on your phone is equally vulnerable, if not more so. Many social media applications allow third-party app developers to collect and sell information about their users. ▪ Account: share your mobile device account information only with authorized vendors and people who share your mobile device plan. Carefully select who to share a mobile phone plan with. Ensure they have proved themselves honest and trustworthy because when you share a mobile phone plan, you share a lot of personal information. If you suspect a plan provider's employee has accessed your account without authorization, contact your provider and explain your concerns as soon as possible. ▪ Location: any time you turn on your cell phone's GPS tracking ability, you make yourself vulnerable to unauthorized location tracking. To mitigate this risk, turn the GPS location feature off when you aren't using GPS navigation and be wary of apps that ask to track your location, especially if they don't need to track your location to perform their function. ▪ Camera and microphone: be wary of any app that accesses your camera and microphone, especially if it doesn't need to access those features to function. If your camera and microphone are hacked, anything visual or auditory data your phone collects becomes accessible to the hacker.

Prevent Unintended Connections	Some mobile devices are configured to automatically connect to open Wi-Fi networks or accept other types of wireless connections (e.g., Bluetooth). This presents a serious security threat. For example, if a mobile device were to connect to an AP owned by a malicious individual, any information sent by the device can be captured by the malicious person.
	▪ To prevent against unintended Wi-Fi connections:
	  ▪ Configure Wi-Fi settings to always ask for permission to connect to unknown wireless networks.
	  ▪ If Wi-Fi is not being used, consider turning off the Wi-Fi adapter.
	  ▪ If a mobile device has already connected to an unknown wireless network, remove the network from the saved networks list in order to prevent future connections.
	▪ To prevent against unintended Bluetooth pairing:
	  ▪ Unless Bluetooth is actively being used, turn it off. This will not only prevent Bluetooth pairing and discovery, but also increase the device's battery life.

	▪ If a the mobile device has been accidentally paired with another device, navigate to Bluetooth settings and delete (unpair) the device.
Policies and Procedures	Use policies and procedures to secure your mobile devices. ▪ BYOD vs. corporate owned. Some organizations implement security policies that forbid users from connecting their personal mobile devices to the organizational network (wired or wireless). Some organizations allow mobile devices; in fact, they may even provide users with mobile devices. However, there is a risk in this situation that company data may be copied to these devices that could be compromised if a device is lost. As a safeguard, many of these organizations require that remote wipe be enabled on the device so that if it is lost or stolen, a command can be sent remotely to the device to remove all data on it. ▪ Profile security requirements. Utilize an Acceptable Use Policy to specify how users: ▪ Connect their personally-owned mobile devices to the organization's wireless network. If they can, the policy may also specify rules for what internet resources they are allowed to access using those devices. ▪ Use company-owned computers for personal uses, such as shopping for personal items on ecommerce websites.
Device Management	In addition to policies, mobile devices can be secured by using special Mobile Device Management (MDM) tools, which allow for remote management of multiple mobile devices. By using an MDM tool, an IT administrator can: ▪ Test configuration settings before deploying them. ▪ Create and enforce mobile device security policies. ▪ Remotely wipe mobile devices. ▪ Push OS updates to devices. The specific MDM you use depends on the mobile device's operating system. ▪ iOS devices use the Apple Configurator tool. ▪ Windows Mobile devices use the Microsoft Intune tool, which is a cloud-based mobile management app. ▪ Android devices can be managed using a variety of free or paid third-party MDM tools, including the Microsoft Intune tool.