13.3.2 Mobile Device Attack Facts

With over 5 billion mobile subscribers worldwide, it's easy to see why mobile devices are a huge target for attackers.

This lesson covers the following topics:

- Mobile device security concerns
- Mobile device security features
- Mobile device threats

Mobile Device Security Concerns

Some security concerns are unique to mobile devices and other concerns have a special emphasis in a mobile environment. The following table lists a few of these concerns.

Security Concern	Description
Malicious websites	Malicious or compromised websites are often used to launch web or network attacks. An attacker can design a website to easily determine what type of device is being used and then use malicious code that specifically targets that type of device.
Unsecure apps	Most users spend more online time using apps than using a browser. These apps may not have the same security protections as a browser.
Phishing attacks	Phishing and other social engineering attacks are often more productive on mobile device users. ▪ Users can be easily distracted when using a mobile device. ▪ Mobile device users share the same kind of information on social media that the mobile attackers are asking for. ▪ On a mobile device, users might not be as alert to sharing sensitive information or downloading malware.
Data loss	Most good apps function within their sandbox so that they are programmatically isolated from other apps. ▪ Many free apps, even those in an official app store, work as advertised, but may also send personal or corporate data to a remote system. ▪ This data is often used by advertisers, but can just as easily be used by cybercriminals.
Lost and stolen devices	Data loss can occur when a mobile device is lost or stolen. ▪ A mobile device's small size makes it easy to carry and easy to lose. ▪ Mobile devices are easy prey for thieves who target them for the information they contain.

Mobile Device Security Features

Mobile device designers have approached security through five key areas.

Security Area	Description
Access control	Access control includes passwords, biometrics, and two-factor authentication methods to gain access to the device. ▪ Once access is gained, access control governs access using the principle of least privilege. ▪ Each app is limited to only those device resources the app needs to perform its functions.
Digital signing	Only digitally signed apps should be installed. A digital signature: ▪ Verifies that an app hasn't been tampered with. ▪ Verifies that the app came from the original author. On an Android device, an app from unknown sources can't be installed. On an iOS device, an app from unknown sources can be installed only if the phone has been jailbroken.
Encryption	Encryption can be used to secure communications to and from a mobile device, including: ▪ Text messages ▪ Email ▪ Outgoing calls The data stored on a mobile device can also be encrypted. This is similar to whole disk encryption on a desktop computer.

	▪ A password must be provided before the mobile device boots to decrypt the data.
	▪ There are both software and hardware options for encryption.
	  ▪ Software-based encryption is slower since it uses the device's computational resources.
	  ▪ Hardware-based encryption uses separate hardware to perform the encryption.

Isolation	Isolation refers to a mobile device's application sandbox that forces applications to run as a separate process. ▪ One process can't use another process's resources unless access is granted. ▪ Malicious apps have been able to exploit OS weaknesses to gain access to another app's sensitive data.
Permission-based access control	Mobile device apps are required to request permission to access sensitive user data. Permission can be granted when prompted, or you can change a setting to automatically grant permissions.

Mobile Device Threats

No mobile device is completely secure. In 2016, the Open Web Application Security Project (OWASP) published their latest Top10 Mobile Risks. They are:

- M1: Improper Platform Usage
- M2: Insecure Data Storage
- M3: Insecure Communications
- M4: Insecure Authentication
- M5: Insufficient Cryptography
- M6: Insecure Authorization
- M7: Client Code Quality
- M8: Code Tampering
- M9: Reverse Engineering
- M10: Extraneous Functionality

The following is a list of conditions that make mobile devices vulnerable:

- Screen-lock passwords are not set.
- Passwords are incredibly weak.
- Unprotected wireless connections are made without the user being aware of the connection.
- Malware has been installed.
- Security software is not installed.
- Operating system software has not been updated.
- Applications have not been patched.
- The mobile device has been rooted or jailbroken.

While not formally classified as malware, spyware can be particularly risky on mobile devices.

- Spyware apps can monitor and log activity on a mobile device, including:
  - Call history
  - GPS location
  - Text messages
  - Email
  - Keystrokes
- Logged activity can be relayed to a remote server without the knowledge or consent of the user.
- Spyware can be used for legitimate reasons.
  - Law enforcement can use it to aid an investigation.
  - Parents might use it to keep their children safe.
  - Businesses might use it to help keep their workers productive.
- A popular spyware app is mSpy, which runs on Android and iPhone mobile devices and Windows and Mac computers.
