Android Vulnerabilities

23 Critical Vulnerabilities

MOBILE DEVICE SECURITY

Apple iOS Vulnerabilities

45 Critical Vulnerabilities

Mobile devices have become an integral part of our daily lives. With an estimated 302 million smartphone users in the United States alone, more cybercriminals are targeting mobile devices than ever before. Mobile device security is extremely important in order to protect sensitive information stored on and transmitted by laptops, smartphones, tablets, wearables, and other portable devices. **The main goal of mobile device security is to keep unauthorized users from accessing your business/personal devices and in turn keeping them out of your network.** Below is a simple list of cybersecurity best practices that you can use to help improve the security of your mobile devices. As always, if you get stuck feel free to reach out to your local SBDC office for further assistance.

Types of Mobile Device Threats

App Permissions

Allowing apps access to everything on your device (location, camera, etc.)

Insecure Apps

Downloading apps from untrusted app stores or apps containing spyware

Vulnerable Networks

Connecting to insecure public WiFi allow hackers to steal your unencrypted data

Viruses & Malware

Websites can contain malware and/or malicious content that infect your device

Mobile Device Checklist

Authentication

- ☐ Device set to auto-lock when idle for 30 seconds
- ☐ Different password set for each app on device
- ☐ Device two-factor authentication enabled (Fingerprint, Pattern, or Facial recognition)
- ☐ Device secured with at least 6-digit passcode (Longer alphanumeric passcode preferred)

Network Security

- ☐ Avoid public/insecure WiFi
- ☐ Use Virtual Private Networks when connecting to insecure networks
- ☐ Disabling network services when not in use (Bluetooth, NFC, WiFi, GPS)

Spotting Scams

- ☐ Don't click on links in text messages/emails from unknown senders
- ☐ Regularly train to spot suspicious phishing attempts
- ☐ Download content from only trusted apps and emails

Updates

- ☐ All apps are updated and updated regularly
- ☐ Operating system is set to update automatically

Protecting Your Device

- ☐ Device encryption enabled
- ☐ Mobile security software installed
- ☐ Lost device function enabled (Ex: Find my iPhone)
- ☐ Remote wipe enabled (allows you to wipe your device if lost or stolen)
- ☐ Only connect devices to trusted chargers and computers (avoid USB ports in airports and other public ports)

App Security

- ☐ Delete unneeded/unused apps
- ☐ Using least-privilege access on all apps (Ex: Asking apps not to track your data)
- ☐ Using only approved device app store (Apple App Store or Google Play Store)
- ☐ Only allowing apps to use your location when app is in use