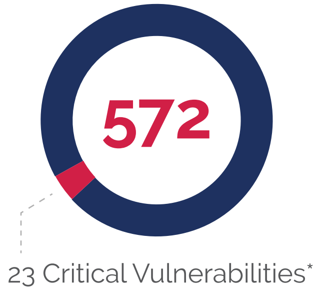
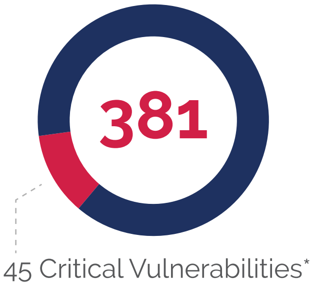
Android Vulnerabilities



MOBILE DEVICE SECURITY

Apple iOS Vulnerabilities



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 crucial to protect sensitive information stored on and transmitted by laptops, smartphones, tablets, wearables, and other portable devices. Stopping unauthorized users from accessing your business/personal devices and in turn keeping them out of your network is the primary goal of mobile device security. Use this list of cybersecurity best-practices to improve the security of your mobile devices. For further assistance, find your local SBDC office at AmericasSBDC.org.

Types of Mobile Device Threats

App Permissions

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

Unsecure Apps

Downloading apps from untrusted app stores or apps containing spyware

Vulnerable Networks

Connecting to unsecure 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/unsecure WiFi
- □ Use Virtual Private Networks when connecting to unsecure 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
- □ Seek consistent training to help
- □ Download content only from trusted apps and emails

Updates

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

Protecting Your Device

- □ Device encryption enabled
- □ Mobile security software installed (aka Antivirus)
- □ 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
- □ Only allow the minimum privileges/access needed by apps
- □ 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

North Star
Small Business Data/Cyber Protection Awareness

AmericasSBDC.org/Cybersecurity

*Data obtained November of 2022

AMERICA'S SBDC