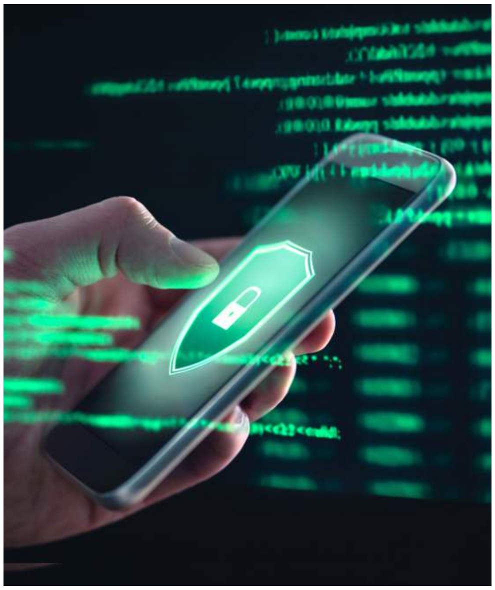
TIP SHEET:

PHONE & MOBILE DEVICE SECURITY

Today's mobile workforce relies on phones, laptops, tablets and other devices to accomplish everyday tasks. As a result, the traditional network perimeter has disappeared, and the risk of mobile device security breaches has increased rapidly.

Whether you deploy company-owned devices, support BYOD, or both, it's important to address mobile device security. Here's a checklist for securing mobile devices in your environment.



☑ Device and Access Control

- Deploy mobile device management software (MDM)
- Vet and limit apps on mobile devices
- Deploy conditional access policies
- Coordinate with remote workers that travel

☑ Mobile Phishing Defense

- Require phishing-resistant MFA
- Disable weak MFA such as phone calls, SMS-based auth, etc.
- Conduct user awareness training which includes SMS phishing, QR code phishing, and other device security issues

☑ Safe User Habits

- Opt out of personal data collection on mobile devices
- Ensure web traffic is encrypted when surfing
- Use a virtual private network (VPN) for browsing

☑ Software Security

- Use a reputable antivirus/antimalware software
- Keep your operating system and apps up to date
- Don't jailbreak or root mobile devices

☑ Mobile Supply Chain Security

- Routinely conduct data & asset inventories
- Know your suppliers (including apps providers & carriers)
- Include suppliers in response & security planning

☑ Physical Security

- Set a strong passcode or use biometric authentication on devices
- Ensure device-level encryption is on
- Backup data on mobile devices
- Maintain a clear process for reporting lost/stolen devices
- Enable remote wipe so that you can remotely erase all data in case a device is lost or stolen.