Homeland Security

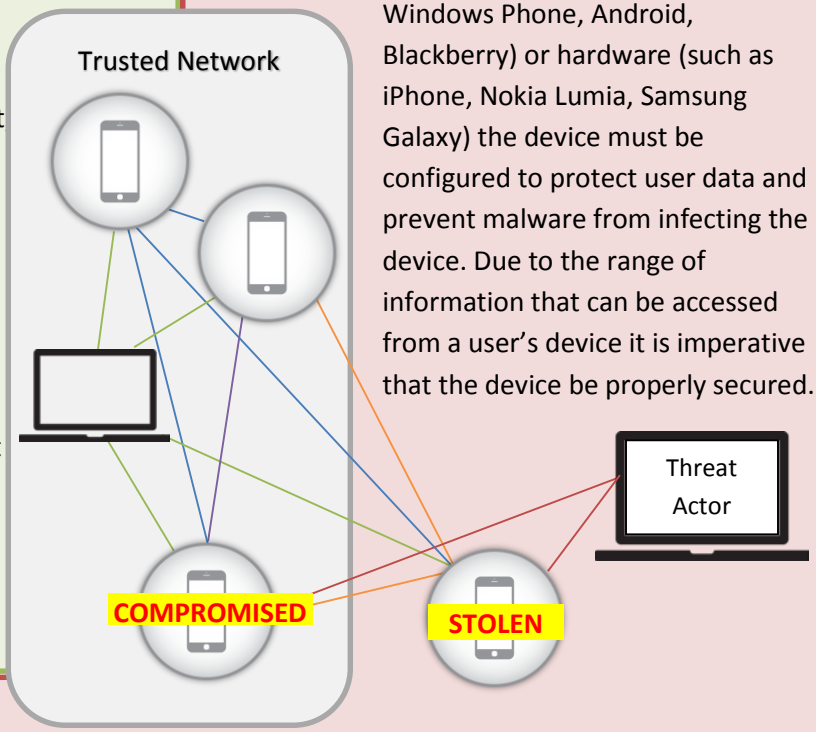
Office of Emergency Communications

MOBILE DEVICE ADOPTION BEST PRACTICES

As a first responder, you may be using mobile devices for daily operations or during emergencies. Next-generation mobile devices, also known as "smartphones" or "tablets", are enhancing responder safety, informing incident management enabling mobility, and improving productivity. The list of device examples is growing rapidly and will likely soon include in-car head units, wearable devices, and a litany of Internet-connected machines. Mobile devices are improving public safety response and easing the burden of first responders. Yet, use of these devices can pose substantial risks to you, your data, and the network.

….Mobile Device Risks?

Regardless of the operating system (such as iOS, Windows Phone, Android, Blackberry) or hardware (such as iPhone, Nokia Lumia, Samsung Galaxy) the device must be configured to protect user data and prevent malware from infecting the device. Due to the range of information that can be accessed from a user's device it is imperative that the device be properly secured.



Stolen or compromised mobile devices can—

- allow unauthorized access to sensitive information
- infect a database with false information
- infect a network with malicious software
- deny legitimate users access to network resources
- collect and distribute information (such as location) to unauthorized persons

Please note: Mobile devices present significant operation, security, interoperability, and performance risks. This document provides basic best practices for maintaining device security in the public safety community. These actions are designed specifically for you, the user, and should be used in conjunction with any policies that your agency has established. Not all recommended actions may be possible based on your agency policies and/or network configuration. However, this guidance should be used in conjunction with or deferred in the case of more formal mobile device management functions and processes provided by your organization.

For more information on mobile device or mobile application adoption, please visit dhs.gov/maps.

Homeland Security

Office of Emergency Communications

Seek Approval and Define Benefits

Seek Leadership Approval

Users should verify with command staff, network, and/or system administrators whether a mobile device is approved for use before beginning to employ it for operational purposes, especially if it is a personal device. Use of a personal device further complicates security, particularly if an organization allows operational apps on the device.

Determine if Desired Function & Operation Will be Achieved

The device should work well with existing processes and use universally familiar functions; for example, a common dial pad for dialing. In addition, the device should maintain capabilities that meet both operational needs and any necessary evidentiary standards. Ease of use and maintenance and availability of technical support should also be considered when selecting a device.

Test Regularly

Check the availability, reliability, responsiveness, resiliency, scalability, and accuracy of the device before using in a response/operations environment and periodically thereafter. Testing the device may include reviewing documentation, assessing operation under various circumstances (e.g., roaming, no network connectivity, large scale events), and evaluating results against known values. Testing may also evaluate functionality, performance, and interoperability of device apps.

Avoid Security Threats

Allow Onlv Authorized Users

Devices should employ a personal identification number (PIN) or password to unlock the device and automatically lock after a period of inactivity. Passwords of at least eight characters, using a combination of uppercase, lowercase, special characters and numbers are recommended. Users may be required by their organization to authenticate to the device using two "factors" of authentication. Generally, this is a PIN/password/ gesture in combination with data provided by the organization such as a common access card (CAC), personal identity verification (PIV) card, biometric authenticator, or certificate.

Update Software Frequently

Whether issued by the organization, the device manufacturer, or an app developer, users should download only authorized apps and apply the most recent software updates to their devices to ensure that they are secure.* Before accepting an update, be sure to determine if any permissions have been changed, such as access to location information or PII. A device with an organization's software installed may automatically update the software depending on the policies set by the administrator.

Limit Data Input and Output

Ensure the device cannot inadvertently send data to non-authorized places. Do not store or transmit sensitive information on any device that has not been approved for use by command staff, network and/or system administrators. Also, enable any available data protection capabilities (e.g., media encryption) on the device.

Maintain Caution

Limit Location-Based Services

When not being used during a tactical situation users should consider decreasing the accuracy of their location. Additionally, users should disallow the use of GPS by applications for that are not enhanced by location information.

Avoid Unfamiliar Networks

Regardless of network type (e.g., cellular, Wi-Fi or Bluetooth), networks may track the actions of the user and copy data that is being sent across the network. Users should not use unfamiliar networks to conduct activities that involve confidential information. In order to prevent unauthorized connections, users should request guidance from their network administrator on disabling automatic connection to networks.

Report Loss/Theft Immediately

Device loss/theft should be reported immediately and maintaining security software to remotely delete the data from the device may be advised. However, only software approved by, and registered to, the network administrator should be used for this function, as other software may provide device tracking to third parties.

Report Unexpected Behavior

In the case of unexpected behavior from a device (for example, crashing, freezing), be sure to report the behavior to network/system administrators.

* For more information on mobile app adoption, please visit dhs.gov/maps for the "Mobile Application Adoption Best Practices Guide"