Learning Objectives: Mobile Device Security

# Module Learning Objectives

The purpose of this document is to identify and document the learning objectives of this training module. This information determines the contents of the training module, regardless of how it is communicated.

**Title**: Mobile Device Security

### Target Audience

All organization employees and contractors are welcome, but those employees and contractors who use a mobile device for work purposes are the target audience. These individuals are assumed to be nontechnical.

### Goal

At the conclusion of this course, participants will be able to explain and demonstrate how to secure mobile devices and will be aware of reporting procedures.

### Outcome

The intended outcome from this learning objective is lowering organizational risk when using mobile technology. Specifically, lowering the likelihood of highly sensitive company information being disclosed to the public through unauthorized means stemming from mobile devices.

### Background

Recent unauthorized disclosures of company trade secrets have resulted in approximately $9,500,000 in net losses over a 3 year period. Two of the incidents were caused by laptops left unlocked in common areas, one was caused by a weak password, one by lack of physical controls and in-attentive staff while the last one was caused by over use of privileges. Although it is possible members of the public were in the common areas unescorted, which would be a violation of company policy, the company believes that these disclosures are the result of one or more employees in the company. The culture of our organization revolves around internal collaboration and promotes the use of mobile devices to facilitate this interaction. However, traditional training and security measures appeared to have failed in accounting for the unique risks associated with mobile devices.

### Learning Objectives

1. Learner explains the importance of locking their mobile device screens.
   1. *Individual Metric*: *Learner signs the organization Mobile Computing Policy and correctly identifies threats caused by leaving their system unlocked and unattended.*
   2. *Individual Metric*: *Learner correctly actions to take when they observe a mobile device unlocked and unattended.*
   3. *Organizational Metric*: *Create a scenario where an employee leaves their mobile device unattended and unlocked to see if nearby employees take the appropriate action (lock the system and report it).*
2. Learners explain the importance of maintaining positive control of their mobile devices and to not leave them unattended in common areas.
   1. *Individual Metric*: *Learner signs the organization Mobile Computing Policy and correctly identifies threats caused by failure to maintain positive control of their mobile devices.*
   2. *Organizational Metric*: *A daily inventory of mobile devices shows that all of the company mobile devices are accounted for. Additionally, a sampling of mobile devices shows more than 95% of company mobile devices are configured with a remote wiping capability.*
   3. *Organizational Metric*: A sampling of company mobile devices reveals all of the mobile devices are configured to pull a virtual desktop image for system use to limit the threat from information stored on the mobile device.
3. Learners explain the importance of using multi factor authentication and strong passwords.
   1. *Individual Metric*: *Learner signs the organization Mobile Computing Policy and correctly identifies examples of strong passwords.*
   2. *Individual Metric*: *Learner correctly identifies examples of multifactor authentication.*
   3. *Organizational Metric: A sampling of mobile devices shows that none of the company mobile devices allow logins without multifactor authentication.*

1. Learners explain the importance of only connecting to secure, trusted networks.
   1. *Individual Metric*: *Learner signs the organization Mobile Computing Policy and correctly identifies organization naming conventions.*
   2. *Individual Metric*: *Learner correctly identifies 75% of the possible signs of a suspicious wireless access points.*
   3. *Organizational Metric*: *Stand up a rogue access point with great signal strength, not secured, and an SSID that is significantly different than those hosted by the organization. A sampling of mobile devices shows less than 10% of laptops connected to the rogue access point*.
2. Learners understand the importance to immediately report lost or stolen devices.
   1. *Individual Metric*: *Learner signs the organization Mobile Computing Policy and correctly identifies the email address to send reports of lost or stolen devices.*
   2. *Organizational Metric*: *A daily inventory of mobile devices shows that all of the company mobile devices are accounted for. Additionally, a sampling of mobile devices shows more than 95% of company mobile devices are configured with a remote wiping capability.*
   3. *Organizational Metric*: A sampling of company mobile devices reveals all of the mobile devices are configured to pull a virtual desktop image for system use to limit the threat from information stored on the mobile device.
3. Learners know that they may not access organization’s sensitive information from mobile devices.
   1. *Individual Metric*: *Learner signs the organization Non-disclosure Agreement and Mobile Computing Policy and correctly identifies organizational marking of sensitive information.*
   2. *Individual Metric*: Learners capable of recognizing misuse of sensitive information and can correctly identifies the email address to send reports of sensitive information misuse.
   3. *Organizational Metric*: *A sampling of mobile devices shows that none of the company mobile devices have any sensitive work-related data. Those that do must be immediately inspected then sanitized*.
4. Learners understand the importance of backing up data and are capable of explaining the process to configure a system for regular backups.
5. *Individual Metric*: *Learner correctly identifies the steps to configure their mobile device to back up their data monthly or more frequently.*
6. *Organizational Metric*: *A sampling of mobile devices shows that 90% of mobile systems are correctly configured to backup data monthly or more frequently*.