Learning Objectives: Mobile Device Security



# Module Learning Objectives

The purpose of this document is to identify and explain the learning objectives of this training module. Learning objectives identify specific, measurable outcomes from a particular training module. In the case of security awareness training, the learning objectives enable staff to perform their day-to-day duties in a safe and secure manner, dramatically reducing risk to our organization.

**Title**: Mobile Device Security

### Target Audience

All organizational employees and contractors who use a mobile device for work purposes are the target audience. These individuals are assumed to be nontechnical.

### Goal

Course participants will learn the need for and will be able to explain and demonstrate how to secure their work or personal mobile devices. The decisions people make as a result of this training will lower both organizational and personal risk when using mobile devices.

### Background

Mobile devices have become one of the primary ways people communicate and interact with information, both in their personal life and for work. However, as our workforce uses mobile devices more and more for work, and as their world of personal and work-related activities combine, these behaviors expose our organization to growing risks. This module teaches the steps individuals can take to safely use mobile devices.

### Learning Objectives

1. Learners can explain the need for a screenlock on mobile devices and demonstrate how to enable one on their mobile device.
   1. *Individual metric*: *The learner correctly identifies or matches what a screenlock is in a test question or interactive training session.*
   2. *Organizational metric*: *A sampling of mobile devices demonstrates that a certain percentage of mobile devices have some type of approved screenlock enabled*.
2. Learners can explain the need for downloading apps only from trusted sources as well as can distinguish trusted versus untrusted sources.
   1. *Individual metric*: *The learner correctly identifies or matches the trusted versus untrusted sources for downloading mobile apps in a test question or interactive training session.*
   2. *Organizational metric: A sampling of mobile devices shows that less than a certain percentage are infected due to malicious apps.*
   3. *Organizational metric: Send a phishing email inviting people to download and install a certain mobile app.*
3. Learners can explain the reason for backing up their mobile devices, explain how to do it, and perform a backup on at least on a monthly basis.
   1. *Individual metric*: *The learner correctly identifies or matches the reason for backing up a mobile device in a test question or interactive training session.*
   2. *Organizational metric*: *A sampling of mobile devices shows that a certain percentage of mobile devices were backed up in the past 30 days*.
4. Learners can explain the security need to run the latest version of their mobile device’s operating system and mobile apps and can demonstrate how to enable automatic updating.
   1. *Individual metric*: *The learner correctly identifies or matches the reason for updating mobile devices and apps in a test question or interactive training session.*
   2. *Organizational metric*: *A sampling of mobile devices shows a certain percentage are running the latest version of the operating system approved by their organization and that all apps are configured to automatically update*.
5. Learners can demonstrate how to report a lost, infected, or stolen mobile device issued by work and whom to contact.
   1. *Individual metric*: *The learner correctly identifies or matches the proper reporting method in a test question or interactive training session.*
   2. *Organizational metric: When surveyed, a certain percentage of people can explain proper reporting procedures.*