@ISACA
RELEVANT, TIMELY NEWS
Volume 1, 4 January 2012

# Five Things You Can Do to Increase the Security of Your Mobile Device

By John P. Pironti, CISA, CISM, CGEIT, CRISC, CISSP, ISSAP, ISSMP

1. **Enable device password and associated data wiping.** Enabling a device password on your mobile device helps to ensure that unauthorized users cannot gain access without your knowledge or consent. Avoid using easily guessable dates, patterns or passphrases. It is also recommended that you enable the data wipe capabilities that are often available on modern mobile devices. These capabilities erase the data on the device after a selected number of bad password attempts. This will ensure that an adversary would have limited success using brute-force or password-guessing attacks.

2. **Enable device auto-lock functionality for shorter windows of time.** The auto-lock features that are available on many mobile devices require a password to be reentered after a period of inactivity or if triggered by a user action (i.e., closure of cover on a tablet), similar to the way screen savers work on traditional computers. This security feature is most effective when its enable time is set for the shortest possible period of inactivity. This time should be no more then 10 minutes and shorter, if possible. This reduces the window of opportunity during which an attacker has unrestricted device access if the device is out of your control.

3. **Enable device encryption capabilities.** Data encryption is a useful control for securing data at rest and data in motion, if implemented properly. Many mobile devices have the ability to enable data encryption capabilities with little impact to the user experience after the initial enciphering of the data for data at rest and limited network overhead for data in transit. The use of encryption limits an attacker's ability to obtain usable data from the device's storage without the encryption key material and also prevents the attacker from being able to easily capture sensitive data (such as usernames and passwords) over the airwaves during network data transmissions.

4. **Regularly create encrypted and password-protected backups of your mobile device.** Mobile devices often contain large amounts of critical data and applications because users leverage them for computing activities. It is important

to create and maintain encrypted backups of these devices on a regular basis to ensure resiliency if a device ever malfunctions, is lost or is replaced. Cloud-based mobile device backup solutions can be an attractive option because they typically provide geographic separation between the device and the backup. Regardless of the physical location of the backup, the device should be encrypted and password-protected, when possible. This is especially important in cloud-based offsite backup solutions in which the user has limited visibility into and control over how the data are stored and accessed. If the backup is encrypted and password-protected, there is a higher likelihood of maintaining the confidentiality and integrity of the data, even when the device is out of the direct control of the user.

5. **Use the same risk-aware and security-conscious web-browsing techniques on your mobile device.** Web browsers on mobile devices can be exploited and used to enable attacks just as easily as those on dedicated computers. Mobile devices often contain sensitive information and are used to access secure environments that make them an attractive target to motivated and capable adversaries. Risk-aware and security-conscious web-browsing behaviors should be universally employed, regardless of the technology platform being utilized.

John P. Pironti, CISA, CISM, CGEIT, CRISC, CISSP, ISSAP, ISSMP, is the president of IP Architects LLC.