THE UNIVERSITY of TENNESSEE
MUNICIPAL TECHNICAL ADVISORY SERVICE
Provided by Justin O'Hara, IT Consultant

Securing Mobile Devices

Big Things Come in Small Packages!

Mobile computing devices include mobile phones, IP phones, pagers, BlackBerry devices, iPhones, smart phones, and portable storage devices, such as USB drives. Some of these devices are multifunctional and may be used for voice calls, text messages, email, Internet access, and may allow access to computers and/or networks. Some also include Near Field Communication (NFC) capabilities, which allow the user to perform activities such as debit/credit card transactions or utilizing the device as a car and/or house key. Mobile computing devices have become indispensable tools for today's highly mobile society. Small and relatively inexpensive, these multifunction devices are becoming as powerful as desktop or laptop computers. While increased productivity is a positive feature for any organization, the risks associated with mobile devices can be significant and include issues stemming from human factors to technological issues.

The Risky Business of Mobility!

A significant amount of personal, private and/or sensitive information may be stored or accessed via mobile devices. The portable nature of mobile devices makes it more difficult to implement physical controls. Additionally, the fact that some employees are increasingly using their personal mobile devices for business purposes have resulted in heightened risks. Ironically, many of the risks associated with mobile devices exist because of their biggest benefit: portability. Many of these devices can store vast amounts of data, making them vulnerable to unauthorized access to the information from either interception of data in transit or theft or loss of a device. In addition to data loss, mobile computing devices carry the risk of introducing malware. Certain types of malware can infect the devices or can be used as a platform for malicious activity. Devices with onboard microphones and cameras are also vulnerable to unintended activity through publicly available tools, possibly resulting in eavesdropping or tracing the device's location. Cellular and Voice-over IP (VoIP) technologies also have vulnerabilities that can be easily exploited, resulting in intercepted calls.

What Can Be Done to Secure Mobile Computing Devices?

The protection of mobile devices must be a primary task for organizations. The following steps can help you protect your data and your mobile computing device.

- Organizations should have a policy to address the storage of information on mobile devices, including the use of personal devices for business purposes.
- Keep your mobile device physically secure. Millions of mobile devices are lost each year.
- Control what data is stored on the device. Do not store unnecessary or sensitive information.
- Use a secure password or PIN to access your device. If the device is used for business purposes, you should follow the password policy issued by your organization.
- Disable features and services that are not needed (Bluetooth, WiFi, GPS, etc). If the Bluetooth functionality is used, be sure to change the default password.
- Enable storage encryption. This will help protect the data stored on your device in the event it is lost or stolen, assuming you have it password protected.
- If available, consider installing anti-virus software for your mobile device. This may prevent or detect/quarantine malware specific to mobile devices.
- Keep all system and application software patched and up-to-date. Many manufacturers frequently provide updates to address known vulnerabilities.
- Download applications only from vendor-authorized sites. Sites offering "free games" or "ring tones" are sources for distributing malware. If used for work, follow your organization's policy on downloading software.
- Do not open attachments from untrusted sources. Similar to the risk when using your desktop, you risk being exposed to malware when opening unexpected attachments.
- Do not follow links to untrusted sources, especially from unsolicited email or text messages. As with your desktop, you risk being infected with malware.
- If your device is lost, report it immediately to your carrier or organization. Some devices allow the data to be erased remotely. In order to erase data remotely you will need to contact your organization before your carrier disconnects service to the device.
- Before disposing of the device be sure to wipe all data from it. If used for work, follow your organization's policy for disposing of computer equipment.

Resources for more information:

National Cyber Alert System - Cyber Security Tip ST06-007, Defending Cell Phones and PDAs Against Attack
us-cert.gov/cas/tips/ST06-007.html

NIST Special Publication 800-124, Guidelines on Cell Phone and PDA Security
csrc.nist.gov/publications/nistpubs/800-124/SP800-124.pdf

FTC Consumer Alert – The 411 on Disposing of Your Old Cell Phone
http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt044.shtm
ftc.gov/bcp/edu/pubs/consumer/alerts/alt044.shtm

ISACA White Paper – Securing Mobile Devices
isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Securing-Mobile-Devices.aspx