Texas Department of Information Resources
CYBER SECURITY TIPS
Monthly Newsletter
Office of the Chief Information Security Officer July 2009 | Volume 3, Issue 6

Security of Mobile Communication Devices

ALL THIS FUNCTIONALITY IN ONE DEVICE!

Mobile communication devices (includes Blackberrys, iPhones, smart phones in general) have become indispensable tools for today's highly mobile society. Small and relatively inexpensive, these multifunction devices can be used not only for voice calls but also text messages, email, and Internet access along with standalone applications similar to those performed on a desktop computer. A significant amount of personal, private, and/or sensitive information may accumulate or be accessed via these devices. Additionally, some of these devices may allow you to access your home computer or your corporate network.

WHAT RISKS DO THEY PRESENT?

While the devices offer many benefits and conveniences, they also pose risks to you and/or your organization's security. As these devices continue to take on the characteristics of personal computers, they also inherit the same potential risks. Some of the primary risks include:

- The portability of the device leads to a higher likelihood of loss of the device. Millions of mobile communication devices are lost each year.
- When Bluetooth and/or wireless (not cellular) communications are enabled, these devices are subject to the risk of eavesdropping and *hijacking*.
- *Malware* available, that if installed on your device, can allow a perpetrator remote access to your device to listen to and record all of your calls, send text messages to the perpetrator whenever you make or receive a call, read all of your messages, make calls on your behalf from your phone, access all of the information on your phone, trace your location, and enable the speaker functionally on the phone to listen in on conversations even when the phone is not in use.
- Sites purporting to offer *free games or ring tones* are major vectors for distributing malware.
- While the reports of worms and viruses impacting these devices are relatively low, this is expected to increase in the future.

Despite the risks outlined above, many users do not understand how vulnerable their mobile device is or how to deploy important security settings and controls.

WHAT CAN I DO TO SECURE MY MOBILE COMMUNICATION DEVICE?

The following guidelines will help to protect your mobile communication device. Please note that some of the steps depend on the functionality of your device.

- Use a password to access your device. If the device is used for work purposes, you should follow the password policy issued by your organization.
- If the Bluetooth functionality is not used, ensure that this setting is disabled. Some devices have Bluetooth-enabled by default. If the Bluetooth functionality is used, change the default password for connecting to a Bluetooth-enabled device.

- 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. Again, 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.
- Review the security setting on your device to ensure appropriate protection. Encrypt data transmissions whenever possible.
- Enable storage encryption to help protect the data stored on your device in the event it is lost or stolen, assuming you have it password protected.
- Beware of downloading any software to your device. If the device is used for work, follow your organization's policy on downloading software.
- Before disposing of the device, wipe all data from it and/or or follow your organization's policy for disposing of computer equipment.

ADDITIONAL RESOURCES

For additional information on keeping your mobile communication device secure, please visit:

- National Cyber Alert System – Cyber Security Tip ST06-007, Defending Cell Phones and PDAs Against Attack: **www.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: **www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt044.shtm**
- WTHR News – Tapping Your Cell Phone: **www.wthr.com/Global/story.asp?s=9346833**
- McAfee – The Web's Most Dangerous Search Terms: **us.mcafee.com/en-us/local/docs/most_dangerous_searchterm_us.pdf**

For previous issues of the Monthly Cyber Security Tips Newsletter, please visit **www.dir.state.tx.us/security/reading**.
For more information on Internet security, please visit the SecureTexas website at **www.dir.state.tx.us/securetexas**.
SecureTexas provides up-to-date technology security information as well as tips to help you strengthen your part of Texas' technology infrastructure. Report serious information security incidents as quickly as possible to your agency's Information Security Officer and to DIR's 24/7 Computer Security Incident Notification hotline: (512) 350-3282.

Brought to you by: MS-ISAC **www.msisac.org**

Powered by: US-CERT UNITED STATES COMPUTER EMERGENCY READINESS TEAM **www.us-cert.gov**

Distributed by: DIR Secure Texas **www.dir.state.tx.us/securetexas**