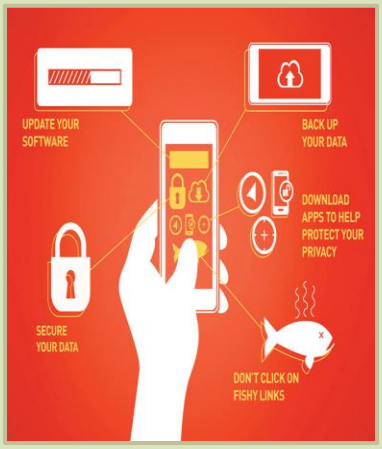
October 25, 2013 Release # 238

-- Begin Transmission --

The Risks of Using Portable Devices – Final Part

As mobile access to sensitive corporate information becomes more popular and the number and type of mobile devices used to access such information increase, security becomes a concern. When using portable devices such as smart phones, security best practices need to be considered.



Recommended Practices for Portable Smart Devices

- Download applications and other programs only from trusted sources.
- Run an updated anti-malware software, scan the entire device periodically and take appropriate action when it identifies suspicious applications.
- Set an idle timeout that will automatically lock the device when you are not using it.

- Password protect the device using strong password and PIN. Don't forget to change it periodically.
- Before downloading applications and programs, find out what access is required on your device.
- Do not "jailbreak" the device. Jailbreaking is a form of privilege escalation, and the term has been used to describe privilege escalation on devices by other manufacturers as well. The name refers to breaking the device out of its "jail".

- Disable Bluetooth, Wi-Fi, and other services when you're not using them.
- When using Bluetooth, set it to "non-discoverable" mode to make the device invisible to unauthenticated devices.

Using portable devices comes with both value and risks, but those risks can be mitigated or at least reduced if you follow the best practices mentioned in this article. As existing products evolve and new ones enter the market, you must use them with caution, always consider their security features, possible vulnerabilities, and ways they could be targeted by malicious attackers.

-- End of Transmission –

Information Security: It's a Shared Responsibility

REFERENCE(S): http://www.us-cert.gov/

 Document Code: 2013ICT_15SECA041