Security for Mobile/Smartphones

With ever advancement in technologies, cell and smart phones, tablets and notebook computers are commonplace and increasing capabilities. Mobile devices (or mobile computing devices) are information systems capable of storing and processing large amounts of information without having a fixed physical location, and they are highly portable. While mobile devices by default are inherently insecure, we need to embrace them as they will continue to proliferate and be used for both business and personal purposes.

A stolen or lost mobile device with unprotected storage allows an attacker or malicious person to access the data on it. If the device is infected with malware, it may lead to use of services running in the background, or leaking sensitive information. Here are some general tips for maintaining the security of your mobile device.

Securing your mobile device

- Enable a power-on password or other device password management tool if available.
- Configure the mobile device in such a way that it locks automatically after some inactive time.
- Use strong passwords to unlock the device.
- Install mobile security software, such as anti-virus software and firewall on mobile device if available.
- Apply the latest patches and fixes for your mobile operating system and related backup/synchronization software. Upgrade the software to its latest version where applicable.
- Scrutinize thoroughly all permission requests, for example those involving privileged access, when installing applications/services.
- Use encryption to lock sensitive data stored on the mobile device and removable media, if available.
- Set up a remote data wiping feature if available.
- Turn off wireless connections such as Wi-Fi, Bluetooth and/or infrared connectivity when not in use.
- Turn off location services setting in your mobile device if it is not necessary to run location-based application.
- Do not "jailbreak" or hack the mobile device (to override usage and/or access limitations).

When using your mobile device

- Do not leave a mobile device unattended, EVER.
- Do not process sensitive data in the mobile device unless with encryption feature on or secure end-to-end connection, ie, VPN.
- Do not open or follow links in SMS/MMS or email from misleading URL, suspicious or un-trusted sources.
- Do not download or accept programs and content from unknown or un-trusted sources.
- Be cautious when connecting to publicly available Wi-Fi hotspots, and avoid accessing sensitive data unless with adequate security protection.

Backup data in your mobile device

- Turn on the encryption option in the backup/synchronization software for storing the data in encrypted mode if available.
- Make sure the backup copies are encrypted no matter stored in desktop PC or in removable media.

Prior to disposing your mobile device

- Completely clear all data and settings on your mobile device before disposal.

At all times

- Keep your mobile devices in a secure place, especially when not in use.
- Stay alert on security vulnerability on mobile devices, and apply the latest patches and fixes when available.
- Do not install illegal or unauthorized software on the mobile device.
- Do not allow wireless connections from unknown or un-trusted sources on your device.