Best Practices Protecting Your Mobile Device

Mobile devices such as smart phones, cell phones and PDAs are now essential personal and business communication tools. Among other functions, mobile devices are used for making calls, exchanging multimedia messages, surfing the web, checking emails, paying bills, downloading games, downloading music and more. To support its functions, mobile devices today carry with it confidential information such as email messages, pictures and contact numbers, exposing the owners of these devices to security risks and threats unknown before.

Realising the importance of protecting confidential information, some entities take vital steps to secure information and data within their premises. However, often times protecting confidentiality of data residing in mobile devices is either overlooked or taken lightly, resulting in the loss of important and confidential data either via data theft, accidental loss, or malware infection. As data and information are no longer just residing in static devices like servers and/or storage, protecting data/information in mobile devices is becoming a critical issue.

Mobile devices, similar to personal computers, are vulnerable to spam, viruses, spyware, theft, loss, and even phishing attacks. It might not be as widespread as reported, but it is on the rise. Your mobile device can be infected when you download programs or files that are already infected. Mobile malware can also spread through cell phones that are equipped with Bluetooth, a technology that allows you to transfer data between different devices, such as sending photos from your cell phone to your printer, or transferring addresses stored on your device. If you have Bluetooth enabled on your mobile device and in "discoverable mode" (see the manual that came with your device for more information), and you come within 30 feet of another infected device that also has Bluetooth enabled and is running on the same operating system as your mobile device, then you might get infected.

Challenges of using a mobile device:

- ➔ Observation: This section can be made clearer by grouping the challenges e.g.:
  - current design limitation
    - inadequate, security patches, inability to upgrade

- Size – because it is small and mobile, it tends to be misplaced, stolen, etc., which leads to loss of asset, and data inside the asset, which can be confidential
- Convenience – hence too much information is kept in it → further aggravates the risk of loss of confidential information, etc.

- Most mobile devices are not designed with adequate security protection i.e. some devices are impossible to upgrade, and some have very few patches available for them.
- People may use mobile devices to store confidential information. Since mobile devices can be stolen or misplaced, confidential information can be misused if it falls into the wrong hands.
- If your mobile device is infected with mobile spyware, it can track your calls and report it to a third party.
- Malware infection can corrupt your mobile device operating system software and make it unusable.

Common mobile device platforms

The following are the current popular mobile device operating systems:

- Symbian – the most popular proprietary operating system for mobile phones with millions of users worldwide. 50% of all mobile phones run on this platform.
- Windows CE & Windows Mobile – Microsoft's solution for mobile and embedded systems. Windows Mobile is designed and optimised for devices with minimal storage capacity, and it enables third party developers to develop applications for the device.
- RIM Blackberry – a platform built on proprietary technology that focuses on ease of use and targets business users. There are many third party applications developed for this platform and most models offer full multimedia features.
- iPhone OS – an Internet-ready, multimedia smart phone designed and marketed by Apple Inc.
- Linux – an open source platform used for developing mobile applications by various developers.

- Palm webOS – for mobile devices using the Linux platform.
- Android – an open source (Linux-based) mobile platform developed by Google. It gives flexibility for hardware and software developers to develop mobile applications, and gives access to all aspects of phone operations and functionality.

Common mobile malware

The following are the common mobile malwares that affect mobile devices:

Cabir: Infects mobile phones running on Symbian OS. When a phone is infected, the message 'Caribe' is displayed on the phone's display and is displayed every time the phone is turned on. The worm then attempts to spread to other phones in the area using wireless Bluetooth signals.

Skulls: A Trojan horse piece of code. This malware affects mobile phones on Symbian OS; it replaces all phone desktop icons with images of a skull. It will also render all phone applications, including SMSes and MMSes, useless.

Commwarrior: The first worm to use MMS messages in order to spread to other devices. It can spread through Bluetooth and infect devices running on Symbian OS Series 60. The executable worm file hunts for accessible Bluetooth devices and sends the infected files under a random name to various devices.

What can mobile malware do?

1. Spreads via Bluetooth and MMS, and infects other mobile devices. They can corrupt your data, send messages without your knowledge, and render your device unusable.
2. Enables your phone to be controlled remotely by a third party.
3. Modifies or replaces icons or system applications on your mobile device, making it difficult to use, even performing differently from what is expected.
4. Installs fonts and applications that do not work, rendering the device unusable.
5. Blocks or combats installed antiviruses, antispyware and firewall programs so your device is not protected and the malware can perform desired malicious activity.
6. Installs malicious programs without your knowledge with malicious intent.
7. Blocks memory cards so your data cannot be stored.

8. Drains the mobile's battery power faster than usual as malware makes your device perform activities and processes even when the device is on standby mode.
9. Steals data – the stolen data may be used for unlawful means such as to conduct fraudulent financial transactions.

The following are some tips to protect your mobile device:

1. Install and run antiviruses, antispyware and firewall programs on your mobile. Many antivirus manufacturers nowadays support mobile devices.
2. Use a start-up PIN code or password – This protects your account from immediate abuse and financial liability in case your device falls into the wrong hands. The thief will have a more difficult time using it to make phone calls or access personal information you may have stored on it.
3. Change the PIN Code from the manufacturers default pin code.
4. Do not respond to unknown numbers – In particular, 5 digit numbers sent by an unknown person/company; these are increasingly being used for text spam and phishing.
5. Set Bluetooth in "hidden" mode – This prevents devices other than your 'already paired' devices from accessing your mobile phone.
6. Be careful where you use Bluetooth – Be aware of your surroundings when pairing or joining new devices, and always verify the other device's name.
7. Frequently back-up your device data – This is the only way you can restore the contents of your device such as pictures and contacts, and recover data if your device is lost. Please refer to your user manual on how to backup your device, or install the software on your computer to perform the backup.
8. Never let strangers use your device as they could manually download and install a virus.
9. Only download or accept programs and contents (including photos, video clips, ring tones, mobile device themes and games) from a source you trust especially when it is related to mobile banking. This is similar to personal computing.
10. If you receive an attachment from a stranger or the attachment looks 'fishy' even from a known address, do not open or download it as it could contain malware.

11. If your phone is equipped with Bluetooth, turn it off or set it to non-discoverable mode when you're not using it. Only accept incoming data from a source you trust. For more information, see the instructions that came with your mobile device.
12. If your phone is equipped with an Infrared beam, only allow it to receive incoming beams when you're receiving data from a source you trust
13. Remember to treat your phone or other handheld device as carefully as you would your wallet, especially in places that are prone to theft.
14. Update your mobile device software frequently, but be extra careful when using 3G connection to download the updates as incomplete updates can corrupt the mobile device, especially if the connection is intermittent or unstable.

Incident Reporting Channels

Online Form	Online submission at http://www.mycert.org.my/report_incidents/online_form.html
Telephone	Call +603-8992 6969 (Office hours only: Mon-Fri, 0830 – 1730hrs)
Mobile Phone	**Call +6019-2665850 (24/7)**
SMS	**SMS +6019-2813801**
Fax	**Print form at: http://www.mycert.org.my/en/services/report_incidents/fax_details/main/detail/157/index.html and send to +6019-2665850**
Email	Send email to mycert@mycert.org.my