Mobile Phone Security

Mobile phones are becoming ever more popular and are rapidly becoming attractive targets for malicious attacks. Mobile phones face the same security challenges as traditional desktop computers, but their mobility means they are also exposed to a set of risks quite different to those of a computer in a fixed location. Mobile phones can be infected with worms, trojan horses or other virus families, which can compromise your security and privacy or even gain complete control over the device. This guide provides the necessary steps, do's, don'ts & tips to secure your mobile devices.

Steps to be followed before Mobile Phone usage :

STEP 1 : Read the manufacturer's manual carefully and follow the guidelines as specified to setup your mobile phone.

STEP 2 : Record the IMEI (International Mobile Equipment Identity) number for tracking your mobile in case you lose it.

Note: This is usually printed on the phone below the battery, or can be accessed by keying *#06# on most of the phones.

✔ *FOR MORE INFORMATION REFER MANUFACTURER MANUAL*

Mobile Phone Security Threats Categories

- ***Mobile Device and Data Security Threats***

  Threats related to unauthorised or intentional physical access to mobile phone and Lost or Stolen mobile phones.

- ***Mobile Connectivity Security Threats***

  Threats related to mobile phone connectivity to unknown systems, phones and networks using technologies like Bluetooth, WiFi, USB etc.

- ***Mobile Application and Operating System Security Threats***

  Threats arising from vulnerabilities in Mobile Applications and Operating Systems .

Typical impact of attacks against Mobile Phones

- Exposure or Loss of user's personal Information/Data, stored/transmitted through mobile phone.
- Monetary Loss due to malicious software unknowingly utilizing premium and highly priced SMS and Call Services.
- privacy attacks which includes the tracing of mobile phone location along with private SMSs and calls without user's knowledge.
- Loosing control over mobile phone and unknowingly becoming zombie for targeted attacks.

Mitigation against Mobile Device and Data Security Attacks

Do's and don'ts for Mobile Device

Do's:

Record IMEI number:

- Record the unique 15 digit IMEI number. In case Mobile phone is stolen/lost, this IMEI number is required for registering complaint at Police station and may help in tracking your mobile phone through service provider.

Enable Device locking:

- Use autolock to automatically lock the phone or keypad lock protected by passcode/ security patterns to restrict acess to your mobile phone.

Use a PIN to lock SIM card:

- Use a PIN (Personal Identification Number) for SIM (Subscriber Identity Module) card to prevent people from making use of it when stolen. After turning on SIM security, each time phone starts it will prompt to enter SIM PIN.
- Use password to protect information on the memory card.

Report lost or stolen devices

- Report lost or stolen devices immediately to the nearest Police Station and concerned service provider. *Use mobile tracking feature.*
- Use the feature of Mobile Tracking which could help if the mobile phone is lost/stolen. Every time a new SIM card is inserted in the mobile phone, it would automatically send messages to two preselected phone numbers of your choice, so that you can track your Mobile device.

Don'ts:

- Never leave your mobile device unattended.
- Turn off applications [camera, audio/video players] and connections [Bluetooth, infrared, Wi-Fi] when not in use. Keeping the connections on may pose security issues and also cause to drain out the battery.

Do's and Don'ts for Data Security:

Do's:

Backup data regularly

- Backup data regularly and set up your phone such that it backs up your data when you sync it. You can also back up data on a separate memory card. This can be done by using the Vendor's document backup procedure.

Reset to factory settings:

- Make sure to reset to factory settings when a phone is permanently given to another user to on sure that personal data in the phone is wiped out.

Mitigation against Mobile Connectivity Security Attacks

Bluetooth:

Bluetooth is a wireless technology that allows different devices to connect to one another and share data, such as ringtones or photos. Wireless signals transmitted with Bluetooth cover short distanes, typically 30 feet (10 meters).

Do's:

- Use Bluetooth in hidden mode so that even if the device is using Bluetooth it is not visible to others.
- Change the name of the device to a different name to avoid recognition ofyour Mobile phone model.

Note: The default name will be the mobile model number for Bluetooth devices.

- Put a password while pairing with other devices. The devices with the same password can connect to your computer
- Disable Bluetooth when it is not actively transmitting information.
- Use Bluetooth with temporary time limit after which it automatically disables so that the device is not available continuously for others.

Don'ts:

- Never allow unknown devices to connect through Bluetooth.
- Never switch on Bluetooth continuously.
- Never put Bluetooth in always discoverable mode.

Note: Attackers can take advantage of its default always-on, always discoverable settings to launch attacks.

Wi-Fi :

Wi-Fi is short for "Wireless Fidelity." Wi-Fi refers to wireless networking technology that allows computers and other devices to communicate over a wireless signal.

Many mobile devices, video game systems, and other standalone devices also include Wi-Fi capability, enabling them to connect to wireless networks. These devices may be able to connect to the Internet using Wi-Fi.

Do's:

- Connect only to the trusted networks.
- Use Wi-Fi only when required. It is advisable to switch off the service when not in use.
- Beware while connecting to public networks, as they may not be secure.

Don'ts:

- Never connect to unknown networks or untrusted networks.

Mobile as USB:

The mobile phones can be used as USB memory devices when connected to a computer. A USB cable is provided with the mobile phone to connect to computer. Your mobile's phone memory and memory stick can be accessed as USB devices.

- Your mobile's phone memory and memory stick can be accessed as USB devices.

Do's:

- When a mobile phone is connected to a personal computer, scan the external phone memory and memory card using an updated anti virus.
- Take regular backup of your phone and external memory card because if an event like a system crash or malware penetration occurs, at least your data is safe.
- Before transferring the data to Mobile from computer, the data should be scanned with latest Antivirus with all updates.

Don'ts:

- Never keep sensitive information like user names/passwords on mobile phones.
- Never forward the virus affected data to other Mobiles.

Mitigation against Mobile Application and Operating System Attacks

Application and Mobile Operating System:

- Update the mobile operating system regularly.
- Upgrade the operating system to its latest version.
- Always install applications from trusted sources.
- Consider installing security software from a reputable provider and update them regularly.
- It's always helpful to check the features before downloading an application. Some applications may use your personal data.
- If you're downloading an app from a third party, do a little research to make sure the app is reputable.

Location tracking services allow the whereabouts of registered cell phones to be known and monitored. While it can be done openly for legitimate purposes, it may also be used for malicious purposes.

Check the source of all your files and apps to make sure they're safe before you download.