CHAPTER 9
MOBILE DEVICE AND MOBILE APPLICATION PROTECTION

9.1 Security Concerns of Mobile Devices

9.1.1 As technologies advance, the computational power of mobile devices continues to increase. A number of schools have adopted the Bring Your Own Device (BYOD) policy to further exploit the advantages of using mobile computer devices in learning. While there are many obvious advantages with these devices, they also bring security concerns that need to be addressed.

9.1.2 Security threats to mobile devices come from many directions. Mobile devices often need additional protection because their nature generally places them at higher exposure to threats than other client devices, such as a workstation in the office area. Major threats to mobile devices can come from the device itself, network (e.g. mobile, internet) or applications (e.g. mobile app, mobile web app). The security concerns of mobile technologies are highlighted below:

(a) As the devices' mobile nature makes them much more likely to be lost or stolen than other devices, their data is at increased risk of compromise.

(b) Insufficient control to accessories in mobile devices such as cameras and microphones, and inappropriate video capturing, audio recording and photo taking may cause a security concern. Moreover, sensitive information in video / audio records or photos might be retrieved by unauthorised persons if the mobile device is not properly protected.

(c) Use of untrusted mobile devices, particularly those that are privately owned, are not necessarily trustworthy and can pose security risks.

(d) Use of untrusted networks such as external Wi-Fi or cellular networks for Internet access can place sensitive information transmitted at risk of compromise.

(e) Use of unsecure communication technologies such as bluetooth, near field communication (NFC) for data connection, have their own security risk. If sensitive information is intercepted over an unsecure communication media, this would lead to a security breach.

(f) Use of untrusted apps may poses obvious security risks, especially when mobile device platforms and mobile app stores do not place security restrictions or other limitations on the published applications developed by third parties.

(g) Mobile apps may induce untrusted inputs from malicious source that are not common to other types of devices. An example is the 2D barcode, which are now commonly used because camera is a built-in component in today's smartphones and tablets. This could induce targeted attacks, such as placing malicious 2D barcodes at a public location.

(h) Mobile devices with location services enabled are at increased risk of targeted attacks because it is easier for potential attackers to determine where the user and the mobile device are, and to correlate that information with other sources to launch attacks such as spear phishing.

9.2 Information Security Policy for Mobile Devices

9.2.1 Schools should establish a mobile device security policy to specify the operation and security requirements for mobile device access.

9.2.2 A formal usage policy and procedures should be in place, and appropriate security measures should be adopted to protect against the risks of using mobile computing and communication facilities.

9.2.3 The usage policy and procedures should include the requirements for physical protection, access controls, cryptographic techniques, backup and malware protection. Besides, they should also include rules and advice on connecting mobile facilities to networks and guidance on the use of these facilities in public areas.

9.2.4 The types of approved mobile devices and the approval mechanism should fulfil the operation and security requirements.

9.2.5 IT Heads should disseminate the acceptable use policy (AUP) and security reminders to users to remind them to apply security best practices. They should obtain users' acknowledgement on receiving the acceptable use policy, security reminders and the mobile devices in good condition. The acknowledgement can be a signed agreement or email.

9.2.6 Schools should maintain a list of approved desktop or mobile applications for mobile devices which are defined on the basis of actual needs and trust level.

9.2.7 User training is an important activity to promote user security awareness of using mobile devices. Schools should understand security requirements from mobile user's point of view so that human error can be minimised. Training to mobile users should be arranged so that a certain level of understanding of security requirements in mobile devices, security measures and security threats can be delivered to users.

9.3 Data Communication and Storage for Mobile Devices

9.3.1 Users should be cautious when connecting to public available WiFi hotspots and avoid access sensitive data.

9.3.2 Users are not recommended to process sensitive data in mobile devices unless with encryption feature on or secure end-to-end connection.

9.3.3 Schools should ensure that all data has been completely erased before disposal or re-use of the mobile devices.

9.3.4 Users should turn on the encryption in the backup / synchronisation software for storing the data.

9.3.5 Users are recommended to install mobile security software such as anti-malware software to protect the device and data.

9.3.6 Users should keep their mobile devices in a secure place, especially when not in use.

9.4 User and Device Authentication for Mobile Devices

9.4.1 Schools should maintain an inventory record for mobile devices with users' information and a list of installed mobile applications.

9.4.2 Schools should deploy mobile device login requirements such as enabling a power-on password, deploying minimal password length and complexity requirements according to the school's security requirements, and configuring the mobile device in such a way that it locks automatically after a period of inactivity.

9.4.3 Users should not store password (e.g. email, network login) on mobile devices. The password auto-save function should be disabled.

9.5 Security Control for Mobile Device Application

9.5.1 Schools are recommended to install security control tools, such as Mobile Device Management (MDM), Data Loss Prevention (DLP), personal firewall software and anti-malware solution whenever feasible, and perform security hardening and deliver hardened mobile devices to users.

9.5.2 Users should keep the system and applications up-to-date and ensure the security features of the OS and installed applications are enabled. The latest malware signatures and definitions should be applied.

9.5.3 Users should only install trusted apps from official app stores or approved applications as provided by the school. They should not download programs and contents from unknown or untrusted sources, or install illegal or unauthorized software on the mobile devices.

9.5.4 Users should not try to perform jailbreaking / rooting or exploit the OS of a mobile device by using unauthorised tools.

9.6 Mobile Device Management (MDM) Solution

9.6.1 MDM solution provides management capabilities in policy, inventory, security and service for mobile devices such as mobile phones and computer tablets. Schools could enforce technical measures uniformly with MDM technologies on all mobile devices in accordance with their own IT security policy.

9.6.2 MDM software could be used to control the location of using mobile devices, create profile and apply security group policy for the devices.

9.6.3 The technical capabilities of MDM solutions are as follows:

(a) Provide an isolated environment for processing data via physical, virtual or per-app container.

(b) Wipe remotely when mobile device is lost or stolen.

(c) Wipe data after repeated logon attempt failure.

(d) Deploy and configure mobile devices with pre-configured setting.

(e) Enforce security controls such as using VPN for encrypting information transmission over wireless network.

(f) Provide audit trailing details on data accessing.

(g) Monitor abnormal activities.

(h) Control mobile application installation and removal.