Mobile Security Best Practices

Mobile devices are commonplace in today's ever connected society. Mobile devices include smart phones, tablets, laptops and PDAs.

Security practices are important for any device, but especially mobile devices as they can be easily lost or stolen.

Below are guidelines that you should follow to secure your mobile device.

Physical Security

A mobile device can be easily lost or stolen. When not in use, be aware of the location of the device and who has physical access to it, especially in public places.

Secure your device(s) with a security code or passphrase

Enable security code/passphrase security on your device. You will be required to enter the security code/passphrase each time you want to use your device. This will prevent others from accessing any applications or data on your device.

- Don't use easy security codes (e.g., 1111, 1234)
- Length of a security code or passphrase is an important factor, more is better
- Use a combination of numbers and letters, when possible
- Use upper and lower case, when possible
- Use first letters of a phrase that will be easy to remember
  ie "I Graduated From Marist in 1963" > 1GfM!$63

Set your device(s) to Auto-lock

Configure your device to require authentication after a certain time of inactivity, the lower the better. This will prevent unauthorized access in the event your device is left unattended.

Enable Remote disable/wipe

Configure your device so in the event the device is lost or stolen you can remotely remove confidential data. Mobile Devices running Lotus Traveler are pre-configured for remote wipe, please contact the Marist Help Desk at (845) 575-4357 in the event of a lost or stolen device.

Enable Data Encryption

Mobile device encryption adds a layer of security to protect your data. Encryption requires a password to encrypt/decrypt the data.(Some devices require a separate password from the device's security code) You should configure your device's platform specific encryption to protect data in the event the device is lost or stolen. External storage media should also be encrypted (eg. SD Cards).

Backup Device data

Make sure the data on your device is routinely backed up. Refer to your device manufacturer documentation for instructions.

Make sure you have the latest Software

Device Firmware and/or Software updates contain many bug fixes and critical security patches; it is imperative to apply the latest updates as they become available to keep your device secure.

Do not allow others to use your device

Be aware of who has access to your device. The device may contain data that is restricted to your eyes only per data confidentiality agreements.

Avoid storing confidential data on device

When possible, disallow confidential data to be stored on your device by applications and do not download offline instances of documents to the device.

Do not jailbreak, root or hack the device

Modifying the device in order to gain unauthorized control or install unauthorized applications could have unintended consequences; Void the Manufacturer's or Service Providers Warranty, Affect Device Functionality, Expose Confidential Data.

Verify permissions on application install/upgrade

Some devices show what permissions applications will need at the time they are installed or upgraded. This may include access to your personal and confidential data. Verify that an application would actually need these permissions before proceeding with the install. If it appears that an application needs permission to your data that it shouldn't, cancel the install/upgrade or alter the permissions (if you are able to do so).

Avoid open/unprotected/unencrypted Wi-Fi networks

Public wi-fi networks are a security risk. If the network is not encrypted, anyone can potentially access any data you transmit or receive. If your device is vulnerable to an attack, it may be possible for someone to access it remotely. Only join trusted networks - data encryption should be enabled on any network you trust.

Immediately Report lost or stolen devices

Any lost or stolen device should be reported immediately to campus security and IT Department. IT will then attempt to delete the device information to prevent compromise of Marist College or personal data. For Marist issued devices, the IT Department will contact the wireless service provider to deactivate the cellular device capabilities to minimize unauthorized use.

Perform hard reset/wipe device before turning in/transferring device

Before any device is retired or transferred the device must be restored to “Factory Defaults”. This can be accomplished by performing a hard reset/wipe on device before turning in. IT can be contacted if assistance is needed in resetting device.

Use a secure password manager application

Password managers like LastPass or 1Password allow users to create and securely store passwords for multiple accounts and are protected by a Master Security Code or Passphrase. Downloading and installing a password manager application on your mobile device will allow for easy and secure access to account credentials.

Avoid storing credentials in apps

Do not store your credentials directly in your mobile browser and applications. Use a secure password manager application to do so.