Mobile Security Best Pracəces

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

Security pracəces 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 locaəon 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 se-

Enable Data Encrypəon

Mobile device encrypəon adds a layer of security to protect your data. Encrypəon requires a password to encrypt/decrypt the data.(Some devices require a separate password from the device's security code) You should conÞgure your device's plaùorm speciÞc encrypəon 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 rouənely backed up. Refer to your device manufacturer documentaəon for instrucəons.

Make sure you have the latest SoÞware

Device Firmware and/or SoÞware updates contain many bug Þxes and criəcal security patches; it is imperaəve 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 conÞdenəality agreements.

Avoid storing confidenəal data on device

When possible, disallow conÞdenəal data to be stored on your device by applicaəons and do not download o ine instances of documents to the device.

Do not jailbreak, root or hack the device

Modifying the device in order to

Avoid open/unprotected/unencrypted Wi-Fi networks

Public wi-Þ networks are a security risk. If the network is not encrypted, anyone can potenəally access any data you transmit or receive. If your device is vulnerable to an ağack, it may be possible for someone to access it remotely. Only join trusted networks - data encrypəon 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 ağempt to delete the device informaəon to prevent compromise of Marist College or personal data. For Marist issued devices, the IT Department will contact the wireless service provider to deacəvate the cellular device capabiliəes to minimize unauthorized use.

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

Before any device is reəred 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 rese ǩ ng device.

Use a secure password manager applica