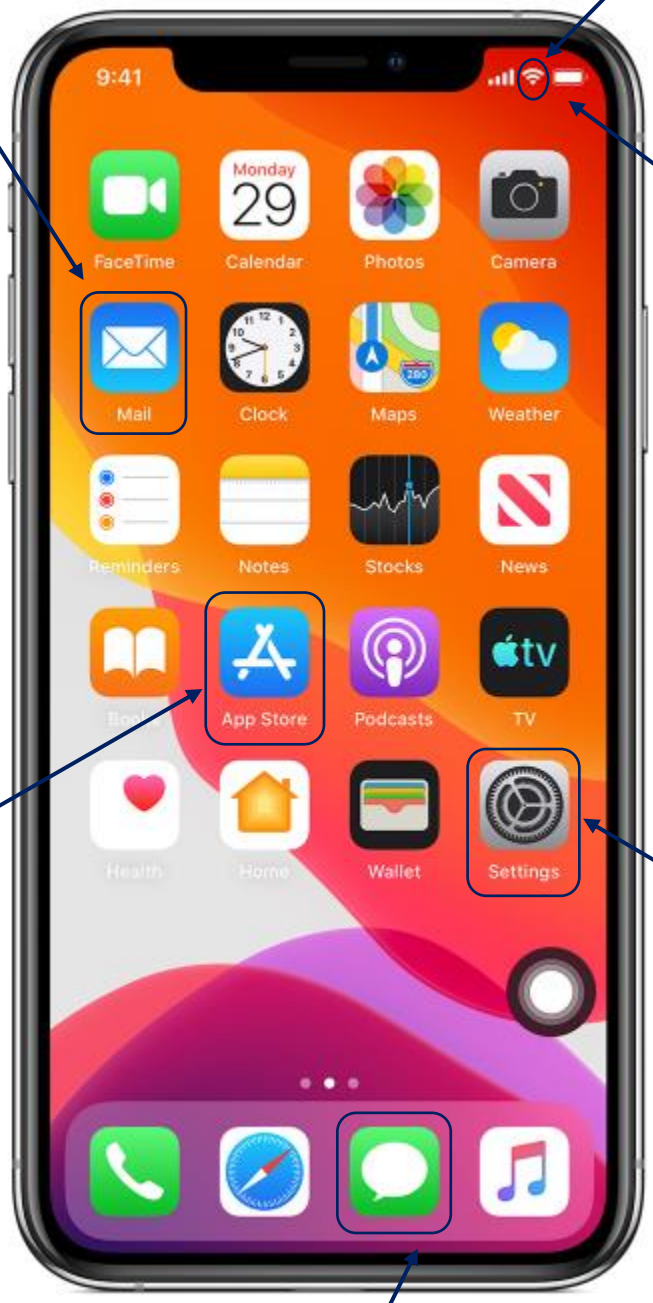
Mobile Device Security

Wi-Fi: Do not connect to public Wi-Fi networks. Disable Wi-Fi when not needed.

Don't fall for phishing schemes! Avoid potential phishing schemes and malware threats by avoiding clicking on links or opening e-mail attachments from untrusted sources.



Did you know, any time you connect to another organization's network, you're increasing your risk of exposure to malware and hackers?

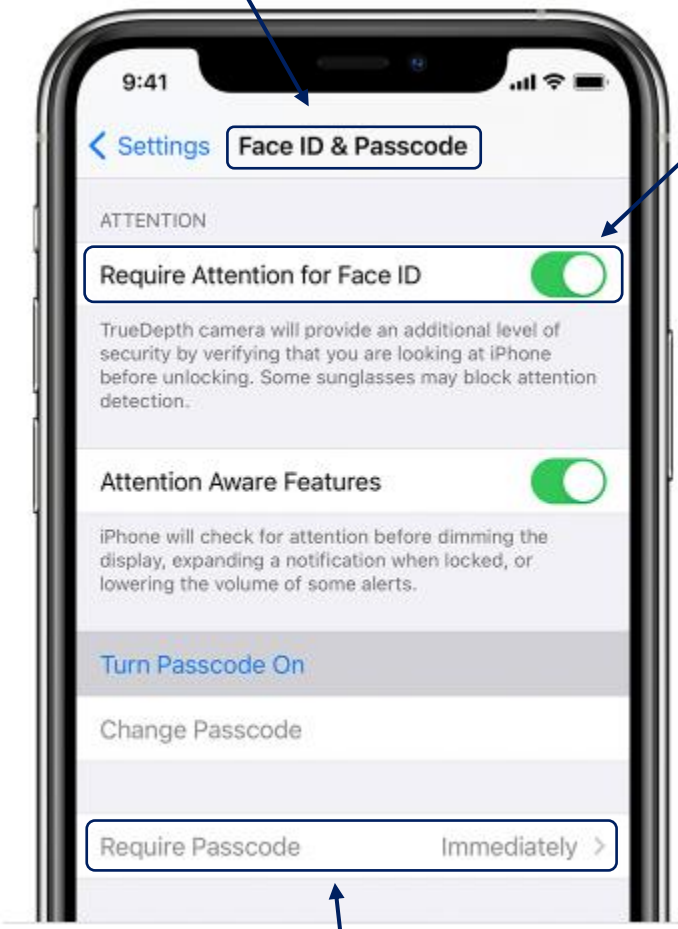
Applications: Install a minimum amount of applications and only ones from official application stores. Be cautious of personal data entered into applications.

Software Updates: Vendors such as Apple, Google, and Microsoft are constantly providing security updates to stay ahead of security vulnerabilities. Make sure you have automatic software updates turned on by default on your mobile devices. Regularly updating your operating system ensures you have the latest security configurations available.

Text Messages: Do not have sensitive conversations on personal devices, even if you think the content is generic.

Source: *National Security Agency*

Authentication: By requiring authentication before a mobile device can be accessed, the data on the device is protected in case of accidental loss or theft of the mobile device. Ensure the use of a strong password to make it more difficult for a potential thief to access the device.



Biometrics: Consider using Biometrics (e.g., fingerprint, face) authentication for convenience to protect data of minimal sensitivity.

Passwords: Use strong lock-screen pins/passwords: a 6-digit PIN is sufficient if the device wipes itself after 10 incorrect passwords. Set the device to lock automatically after 5 minutes.

Source: *National Security Agency*