

# Ten Steps to Smartphone Security (Apple)



## Ten Steps to Smartphone Security (Apple)

Smartphones continue to grow in popularity and are now as powerful and functional as many computers. It is important to protect your smartphone just like you protect your computer to avoid growing mobile cyber threats. Mobile security tips can help you reduce the risk of exposure to mobile security threats. Please note that these security tips reflect the latest software updates as of December 2012 and may not be accurate for previous versions:

**1. Set PINs and passwords.** To prevent unauthorized access to your phone, set a password or Personal Identification Number (PIN) on your phone's home screen as a first line of defence in case your phone is lost or stolen. When possible, use a different password for each of your important log-ins (email, banking, personal sites, etc.).

### [Apple iOS \(Understanding passcodes\)](#)

You should configure your phone to automatically lock after five minutes or less when your phone is idle, as well as use the SIM password capability available on most smartphones. You can also use the Touch ID feature to securely and conveniently unlock your iPhone.

**2. Do not modify your smartphone's security settings.** Do not alter security settings for convenience. Tampering with your phone's factory settings, jail breaking, or rooting your phone undermines the built-in security features offered by your wireless service and smartphone, while making it more susceptible to an attack.

**3. Backup and secure your data.** You should backup all of the data stored on your phone – such as your contacts, documents, and photos. These files can be stored on your computer, on a removal storage card, or in the cloud. This will allow you to conveniently restore the information to your phone should it be lost, stolen, or otherwise erased.

### [Apple iOS \(Backup and restore overview\)](#)

**4. Only install apps from trusted sources.** Before downloading an app, conduct research to ensure the app is Legitimate. Checking the legitimacy of an app may include such thing as: checking reviews, confirming the legitimacy of the app store, and comparing the app sponsor's official website with the app store link to confirm consistency. Many apps from untrusted sources contain malware that once installed can steal information, install viruses, and cause harm to your phone's contents. There are also apps that warn you if any security risks exist on your phone.

**5. Understand app permissions before accepting them.** You should be cautious about granting applications access to personal information on your phone or otherwise letting the application have access to perform functions on your phone.

**6. Use the free, built-in security features.** Every iOS device running iOS 7 or later versions comes standard with both Find my iPhone and Activation Lock, features designed to locate and secure your device if lost or stolen. Find my iPhone can locate your device on a map, and Activation Lock can prevent anyone from using the device if lost or stolen. You can also remotely wipe data from the device. These features are free, and all you have to do is sign-up at [iCloud.com](https://www.apple.com/icloud/findmy-iphone.html) or use the Find my iPhone app. More information can be found here: <https://www.apple.com/icloud/findmy-iphone.html>.

**7. Accept updates and patches to your smartphone's software.** You should keep your phone's operating system software up-to-date by enabling automatic updates or accepting updates when prompted from your service provider, operating system provider, device manufacturer, or application provider. By keeping your operating system current, you reduce the risk of exposure to cyber threats.

[Apple iOS \(How to update your iPhone, iPad, or iPod touch\)](#)

**8. Be smart on open Wi-Fi networks.** When you access a Wi-Fi network that is open to the public, your phone can be an easy target of cybercriminals. You should limit your use of public hotspots and instead use protected Wi-Fi from a network operator you trust or mobile wireless connection to reduce your risk of exposure, especially when accessing personal or sensitive information. Always be aware when clicking web links and be particularly cautious if you are asked to enter account or log-in information.

**9. Wipe data on your old phone before you donate, resell, or recycle it.** Your smartphone contains personal data you want to keep private when you dispose your old phone. To protect your privacy, completely erase data off of your phone and reset the phone to its initial factory settings.

[Apple iOS \(Understanding 'erase all contents and settings'\)](#)

Now having wiped your old device, you are free to donate, resell, recycle, or otherwise properly dispose of your phone.

**10. Report a stolen smartphone.** If your phone is stolen, you should report the theft to service provider as soon as possible and report the loss or theft to your local Gardaí station. Your network provider can then ensure your SIM card is suspended and your handset is blacklisted.