Nine essential iPhone and iPad security tips

Lynn Wright

4-5 minutes

Your iPhone and iPad may hold confidential personal information, such as your bank account details, emails, photos, videos and websites that you've visited, so it's vital that you take simple steps to keep your data secure.

Use a strong passcode

A passcode is the easiest way to protect your device. This four or six-digit code unlocks your iPhone or iPad so you can use it. It might seem a nuisance to type in a passcode every time you use your device, but it takes only seconds.

Choose a passcode with care – avoid easily guessed ones such as 1234 or birth years. iOS 9's six-digit passcode boosts security by expanding the number of possible digit combinations to one million.

For extra security, turn on Apple's Erase Data feature (Settings > Touch ID & Passcode), which means the data on your device is wiped after 10 failed passcode attempts.

Use Touch ID

Apple’s newest devices (iPhone 5S and later, iPad Air 2 and iPad Mini 3) feature Touch ID, which scans your fingerprint to unlock it.

To enable Touch ID, tap Settings > Touch ID & Passcode and register your fingerprint.

Remove lock-screen notifications

It’s pointless having a strong passcode if your messages and alerts are visible or you can use Siri, Control Centre and Passbook without unlocking your phone.

Go to Settings > Touch ID & Passcode and turn off the options under ‘Allow access when locked’.

Turn off access to Control Centre under Settings > Control Centre. Messages and notifications can be turned off under Settings > Notifications.

Secure wi-fi connections

By default, iPhones and iPads automatically connect to nearby Wi-Fi networks without your permission. This can leave you vulnerable to fake public Wi-Fi hotspots that connect to your device to steal its data.

It’s safer to turn this off and authorise each Wi-Fi connection when requested. Tap Settings > Wi-Fi > Ask to join networks and turn to 'On'.

Keep iOS updated

Apple delivers regular updates to its mobile operating system that include security fixes.

Set your device to download and install updates when they’re available by tapping Settings > iTunes & App Store and under ‘Automatic Downloads’ toggle the switch next to 'Updates' to 'On'.

Avoid jailbreaking

Jailbreaking uses special software to bypass the restrictions Apple places on iOS devices, in order to run unauthorised apps.

It’s not illegal, but downloading apps that Apple hasn’t approved from places other than Apple’s App Store runs the risk of breaking your phone, or installing a malicious app that steals your data.

Use Find My iPhone and iPad

Find My iPhone shows you where your device is on a map in case it gets lost or stolen.

If there’s no chance of recovering your device, you can use Find My iPhone to remotely erase the data it stores.

To turn on Find My iPhone, sign into iCloud then tap Settings > iCloud and turn on Find My iPhone. You’ll need to turn on location services by tapping Settings > Location Services > On.

Use Apple’s two-step verification

Turn on Apple’s two-step verification for your Apple ID account to stop unauthorised access – it requires a code along with your password when signing into iCloud, iMessage and FaceTime and before making purchases via iTunes. This code is texted to your phone.

Web browser safety

Check Safari’s settings (Settings > Safari) to ensure you’re protected when using the web. Block pop-ups and turn off AutoFill – which automatically fills in login details when you revisit a website – to make it harder for criminals to access accounts on your device.

Source: saga.co.uk