Protect your small business

A 'how to' guide for Apple

First published: July 2025

The Australian Signals Directorate's Australian Cyber Security Centre has prepared, in consultation with Apple, this guidance for small businesses that use Apple operating systems, such as macOS and iOS.
For more cyber security advice and guidance, visit cyber.gov.au/smallbusiness

Secure your devices and accounts

To unlock your device on iOS and iPadOS, use the strongest built-in security available such as Face ID, Touch ID or Optic ID.

For accounts using a traditional password, make it long, complex and unique:

- at least 15 characters in length
- some capital letters, symbols and numbers
- a passphrase (4 or more unrelated words)
- one that is not used on any other account.

Consider running a **Safety Check** on your Apple iPhone (iOS 16+) for recommended actions.

Use multi-factor authentication

Multi-factor authentication (MFA) adds an extra layer of security to your accounts by requiring two or more different methods to verify your identity.

Apple refers to MFA as two-factor authentication. Options (where supported) include:

- **password and code**
- **Security Keys.**

Use MFA whenever it is available, and choose non-phishable MFA like passkeys or hardware-bound security keys, if possible.

Use a password manager

A password manager helps you store, manage and create complex passwords. ASD recommends the use of a standalone password manager.

Apple offers password management integrated across your devices with the **Passwords App** and **iCloud Keychain**.

The built-in **Passwords App** can warn you of known password re-use, or weak passwords, as well letting you know if a password has appeared in a known breach.

Apply software updates

Turn on automatic updates. This will ensure security fixes are installed early (on supported devices) and keep your device more protected. Go to:

1. **Settings** (**System Settings** for macOS)
2. **General** (for iOS/iPadOS) → **Software Update**
3. Turn on **Automatic Updates**

You should also enable automatic updates on apps from the Apple **App Store** and only download from reputable developers.

Manage antivirus software

Apple offers **XProtect**, as its built-in antivirus software for macOS. By default, XProtect updates itself automatically, ensuring your Mac is guarded against the latest threats.

Products such as iPhones and iPads do not have dedicated antivirus software. Instead, Apple's iOS is designed with security as a core principle, making it less vulnerable to traditional viruses and malware.

Back up your data

There are three backup options offered by Apple:

- **iCloud** (all devices)
- **Local Backup** to a computer (iOS and iPadOS)
- **Time Machine** (macOS)

Automatic iCloud backups run when your device is connected to Wi-Fi, charging and locked. Go to:

1. **Settings** (**System Settings** for macOS)
2. **Apple Account** (or **your profile**) → **iCloud**

You can also back up your iPhone or iPad to your Mac or Windows computer.

Apple devices running macOS can also use Time Machine which stores backups and system recovery images to an external hard drive or USB.

Go to: **Settings** → **General** → **Time Machine**