Protect your small business

A 'how to' guide for Microsoft Windows

First published: July 2025

The Australian Signals Directorate's Australian Cyber Security Centre has prepared, in consultation with Microsoft, this guidance for small businesses who use Microsoft Windows. For more cyber security advice and guidance, visit cyber.gov.au/smallbusiness

Secure your devices and accounts

Use the strongest security available, such as **Windows Hello**, which uses a PIN and biometrics (fingerprint or facial scan).

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.

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. Microsoft offers several MFA options:

- **Microsoft Authenticator app**
- **Windows Hello** (biometrics or PIN)
- hardware security key.

Hardware security keys and biometrics are typically the most secure MFA methods, while SMS and email are less so.

Use a password manager

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

Use a different password manager for your business accounts and keep your personal accounts separate.

Microsoft Windows offers two types:

- **Windows Hello** (where supported)
- **Microsoft Edge**

Apply software updates

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

1. **Start → Settings**
2. **Windows Update**
3. Enable **Automatic Updates**
4. Under **Advanced options**, enable **receive updates from other Microsoft products**

You should also regularly check and enable automatic updates on third-party software.

Manage antivirus software

Microsoft offers **Windows Defender**, which helps protect your operating system from viruses and malware. It comes pre-installed and enabled by default.

You can also use third-party antivirus software, but be aware this can turn off Windows Defender. If you uninstall third-party software, be sure to turn Windows Defender back on. Go to:

1. **Windows Security**
2. **Virus & threat protection**
3. Toggle on **Real-time protection**

Back up your data

To back up your files, you can use the built-in **Windows Backup** feature. Go to:

1. **Start → Settings**
2. **Accounts**
3. **Windows Backup** (Windows 11) or **Updates & Security → Backup** (Windows 10)

You can also back up to a cloud storage service like **Microsoft OneDrive** for ease of access from any location with an internet connection.

Another backup method is using an external hard drive and storing it in a secure location.