Protect your small business

A 'how to' guide for Google

First published: July 2025

The Australian Signals Directorate's Australian Cyber Security Centre has prepared, in consultation with Google, this guidance for small businesses that use Google devices running on Chrome OS or Android OS.
For more cyber security advice and guidance, visit cyber.gov.au/smallbusiness

Secure your devices and accounts

Use the strongest security available on your Google device, such as a passcode (PIN) combined with biometrics.

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

- 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.

Google offers MFA across devices running Chrome OS and Android OS, including:

- **Google Authenticator app**
- **Passkeys** (face scan, fingerprint or PIN)
- **Titan Security Key.**

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

For more security options, enroll in Google's **Advanced Protection Program**.

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.

Google offers a free password manager called **Google Password Manager** built into the Chrome web browser and Android devices.

Apply software updates

Most Google operating systems, such as **Android** or **ChromeOS** and other applications, automatically update or will prompt the user if there are updates available.

To improve your cyber security, apply updates as soon as you are notified.

If you are using an older device running Android, check if there is a newer version available – the latest versions of Android are more secure. Go to:

1. your device's **Settings app**
2. **System** or **About Phone**
3. **Check for software updates**

Manage antivirus software

Google offers several security protections for users, depending on which device and software is used.

For Android, **Google Play Protect** is built-in and automatically scans to help disable any malware or harmful apps found.

Other products, such as **Google Messages** and **Gmail** also have built-in spam and phishing protections.

Google's Security Checkup also helps you find added protection. Sign into your Google account and go to:

1. **My Account → Security Checkup**
2. review the recommendations and follow the steps.

Back up your data

Google offers a variety of backup options, including:

- **Google Drive** which provides cloud storage and file sync
- **Google One** which enhances this with more space across Drive and Gmail
- **Google Workspace** which integrates **Google Drive** with essential business tools, providing robust cloud storage and built-in automatic backups.