



OMNICRON
I.T. SERVICES

CYBERSECURITY · GUIDE

Password & MFA Setup Guide

A plain-English guide to strong unique passwords, password managers, authenticator apps and what to do about unexpected MFA requests.

Who this is for

Anyone who wants to protect their work or personal accounts. No technical knowledge is needed.

How to use it

- Read it once from start to finish, then use the checklists to set things up.
- Start with your most important accounts: email, banking and anything used to reset other passwords.

This resource provides general guidance only. It is not legal advice, a formal audit, a compliance certification or an official government assessment. Your obligations depend on your industry, contracts and circumstances.

Keep your secrets secret

Never write passwords, MFA codes, recovery codes or other secret authentication information on this document or share them with anyone, including IT support. Legitimate organisations will never ask you for an MFA code.

1. Create strong, unique passwords

A strong password is long, unpredictable and used for only one account. Length matters more than complexity.

- Use a **passphrase** of four or more random words, such as a short, unrelated phrase only you would think of. Aim for at least 15 characters.
- Avoid personal details such as names, birthdays, pets, sports teams or your street.
- Never use the same password on more than one account.
- Change a password straight away if you think it has been exposed.

2. Why password reuse is dangerous

When a website is breached, criminals publish or sell the email addresses and passwords. They then try those same details on email, banking and shopping sites automatically. If you reuse a password, one breach anywhere can unlock many of your accounts. Unique passwords contain the damage to one account.

3. How password managers help

A password manager is a secure app that creates, stores and fills in your passwords. You only need to remember one strong master password.

- It generates long, random, unique passwords for every account.
- It fills them in automatically, only on the correct website, which helps protect you from fake sign-in pages.
- It syncs securely across your devices.
- Protect the password manager itself with a strong master passphrase and MFA.
- At work, use the password manager your business has approved.

4. How multi-factor authentication works

Multi-factor authentication (MFA) asks for a second proof that it is really you, usually a prompt or code from an app on your phone. Even if someone steals your password, they cannot sign in without that second step.

Method	How it works	Strength
Security key or passkey	A physical key or your device confirms your identity.	Strongest, and resists fake sign-in pages
Authenticator app	An app such as Microsoft Authenticator shows a prompt or a six-digit code.	Strong and recommended for most people
SMS text message	A code is sent to your mobile number.	Better than nothing, but can be intercepted

5. Set up an authenticator app

- 1 Install an authenticator app from your phone's official app store. At work, use the app your business specifies.
- 2 On your computer, sign in to the account and open its security settings. Look for **two-step verification**, **MFA** or **security info**.

- 3 Choose to add an authenticator app. A QR code will appear on screen.
- 4 In the app, choose to add an account and scan the QR code.
- 5 Enter the code or approve the prompt shown in the app to confirm it works.
- 6 Save any backup or recovery codes somewhere secure, such as your password manager. Never store them in email.

6. Protect your recovery methods

Recovery methods let you back in if you lose your phone. Criminals target them too, so keep them current and under your control.

Done	Item
☐	Recovery phone number is current and yours
☐	Recovery email address is current and protected with MFA
☐	Backup codes are stored securely, not in email or on your desktop
☐	A second MFA method is registered in case you lose your phone

7. Unexpected MFA requests

If you get an MFA prompt you did not start, deny it

An unexpected prompt usually means someone already knows your password. Tap **Deny** or **No**, never approve it to make it go away. Then change your password from a device you trust, and tell your IT support or the service provider.

8. If you think an account is compromised

- 1 From a device you trust, change the account's password to a new, unique one.
- 2 Sign out of all other sessions, if the service allows it.
- 3 Check and update your MFA and recovery methods. Remove anything you do not recognise.
- 4 Look for changes you did not make, such as email forwarding rules, new devices or changed payment details.
- 5 Change the password anywhere else you used the same one.
- 6 For work accounts, tell your IT support straight away. For banking, contact your bank immediately.

Need a hand?

Omicron I.T. Services can help you put this into practice. Visit omnicron.com.au/contact-us, call **(03) 9022 1376** or email admin@omnicron.com.au.

This resource provides general guidance only. It is not legal advice, a formal audit, a compliance certification or an official government assessment. Your obligations depend on your industry, contracts and circumstances.