Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

PROTECT YOURSELF: MULTI-FACTOR AUTHENTICATION

cyber.gov.au

For more cyber security advice

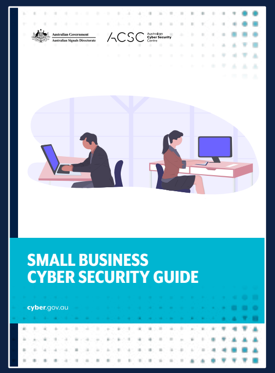
For more information on how to improve your cyber security, see our other guides at **cyber.gov.au**

PERSONAL CYBER SECURITY FIRST STEPS

PERSONAL CYBER SECURITY NEXT STEPS

PERSONAL CYBER SECURITY ADVANCED STEPS

Personal Cyber Security Series



SMALL BUSINESS CYBER SECURITY GUIDE

Small Business Cyber Security Guide

Table of Contents

What is Multi-Factor Authentication?

Multi-factor authentication (MFA) is when you use two or more different types of actions to verify your identify, and you may already be using MFA. For example, when you receive an authentication code by SMS text message after entering your password to log into an online account. MFA is one of the best ways to protect against someone breaking into your account. It makes it harder for cybercriminals to take over your account by adding extra layers of protection.

MFA requires you to use a combination of two or more of the following factors to access your accounts:

- Something you know (e.g. a PIN, password or passphrase);
- Something you have (e.g. a smartcard, physical token, authenticator app, SMS or email); and
- Something you are (e.g. a fingerprint, facial recognition or iris scan).

MFA defends against the majority of password-related cyberattacks. For example, MFA protects against 'credential stuffing' where cybercriminals use previously stolen passwords from one website and try to reuse them elsewhere so they can gain access to more accounts.

Think of adding MFA to your account like adding a house alarm that requires a PIN to deactivate. It provides you with an extra layer of protection from cybercriminals trying to break in. Even if they break through one layer (for example, by guessing your password), they still need to break a second barrier to access your account.

Having an extra step can be inconvenient at first, but remember that taking shortcuts leaves your system more vulnerable. You are better off spending a few seconds entering a one-time code now to avoid spending hours later on trying to regain access to your accounts and dealing with the consequences of your data being stolen.

MFA often goes by different names. You may see it called two-factor authentication (2FA) or two-step verification.

The Australian Cyber Security Centre (ACSC), as part of the Australian Signals Directorate (ASD), provides cyber security advice, assistance and operational responses to prevent, detect and remediate cyber threats to Australia. The ACSC is here to help make Australia the most secure place to connect online.

For more cyber security information, guides and advice visit the ACSC's website cyber.gov.au.

If you think you're a victim of cybercrime report it through ACSC's ReportCyber on cyber.gov.au or call our Cyber Security Hotline on 1300 CYBER1 (1300 292 371).

Keep up to date on the latest cyber threats: Sign up to the ACSC's free alert service online at cyber.gov.au.

Options for MFA

SMS code: This is a random code that you receive to access or use an online service. For example, after you enter your username and password to log in, you will receive an SMS with a 'one-time password' (OTP) to enter to access your account. Another example is when you receive an SMS code when using online banking, before transferring money to a new payee for the first time. Sometimes, you will have the option to receive the OTP by email or voice call. If you choose to receive an OTP by email, make sure that your email account itself is secure; this means that you should enable MFA for this email account in question.

Note that SMS or email authentication is less secure than other forms of MFA.

Authenticator app: Authenticator apps are mobile applications that generate a random OTP and are more secure than receiving a code by SMS. You will first need to download an authenticator app on your device. *Google Authenticator*, *LastPass Authenticator*, *Microsoft Authenticator* and *Authy Authenticator* are a few popular ones. In the settings of your online account (e.g. your social media account), turn on MFA and select the authentication app option. This will reveal a QR code containing a unique key. Use your authenticator app to photograph this QR code, or manually enter the key, to link your account to the authenticator app. Once this step is done, the app will produce a new six-digit code every 30 seconds. Whenever you log in to your online account with your usual username and password, enter this code too. That's it, MFA is on! Consider also using a security key such as a *Yubikey*, as a more secure verification method.

Biometrics: With biometrics, your unique characteristics become the authenticator. An example of biometrics is using your face or fingerprint to access your device or mobile apps. Using biometrics as MFA is convenient, because they are always with you and cannot be misplaced or forgotten.

Physical token: A physical token produces a new numeric code on its screen at regular intervals. Physical tokens tend to be small, like a USB stick or car key fob. A physical token works quite similarly to an authenticator app, except that it is a physical device instead of an app. When you want to access an account, you need to check the token and enter the displayed code.

Security key: A security key is a small physical token without a display screen, which is often plugged into your device via a USB port, or kept in close proximity for wireless versions. It prompts the user to activate authentication processes, and it is a more secure form of MFA than the other options above. An example of a security key is a Yubikey. For more information visit www.yubico.com.

Turn on MFA

You should turn on MFA wherever possible, starting with your important accounts, such as:

- User and email accounts, since a cybercriminal with access to your email accounts can reset passwords for your other accounts.
- Financial services, such as your online banking.
- Accounts that save or use your payment details (e.g. eBay, Amazon, PayPal).
- Social media accounts (e.g. Facebook, Instagram).
- Any other accounts that hold personal information (e.g. myGov).

How to turn on MFA depends on the software or service you are using, however the steps are somewhat similar for most applications. The following list of websites and apps are examples of important accounts that you should protect with MFA. ou can find instructions on how to set up MFA for that service on each service providers' website, or by searching 'Protect yourself MFA' and accessing the relevant link.**User and email accounts.**

- Apple ID
- Microsoft
- Gmail
- Yahoo!

Financial services

- ANZ
- CBA
- Westpac
- NAB
- Macquarie
- PayPal
- Xero

Online shopping

- Amazon
- eBay
- Coles
- Woolworths

Social media and communication

- Instagram
- Twitter
- Facebook and Facebook Messenger
- LinkedIn
- WhatsApp
- Signal

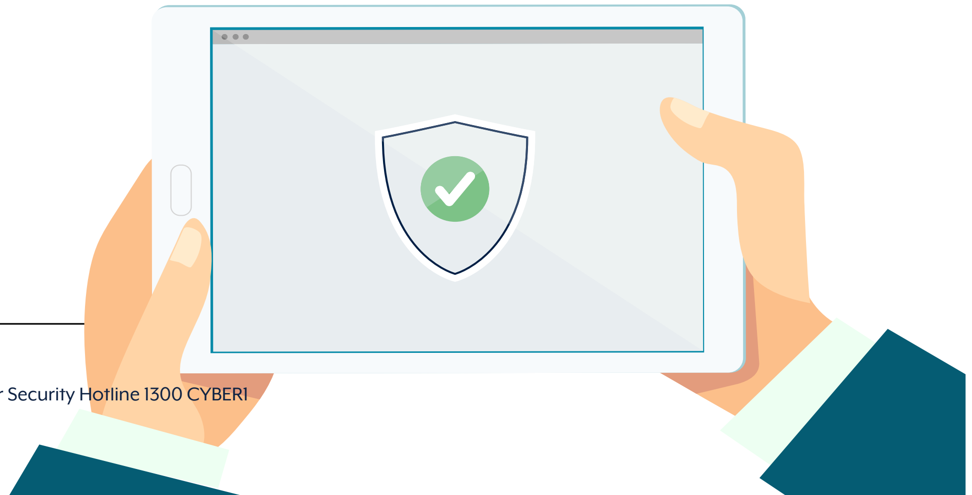
Government services

- MyGov

Gaming

- Steam
- PlayStation
- Microsoft
- Nintendo
- Epic

Note that this list is not exhaustive. If you don't see your account listed above, we recommend searching online for 'how to turn on MFA' for that service, or check the settings of your account. If your account does not have an option for MFA, you should protect it with a strong password or passphrase that is not used anywhere else. Read ACSC's advice on secure passwords. For more information on secure passphrases, visit cyber.gov.au.



Security Tips

Although MFA improves the security of your accounts, motivated cybercriminals may persist and succeed in compromising them. To help keep your account secure, consider the following security tips:

Don't click on account sign-in hyperlinks that you received via SMS or emails.

Scammers may impersonate your bank or a government department, and trick you into clicking a link and give out information such as your account number, password, or credit card numbers. If you have any doubts about a message or call, contact the organisation directly: Visit the official website to find their phone number or to log in to your account via the official website. **Do not** use the links or contact details given to you in the message.

Don't share MFA codes or approve unknown sign-in attempts.

Requests for sign in approvals and the security codes that you receive are the system's way of checking that you are the person who signed in. If you give someone else your MFA code or approve unknown sign-in attempts, then someone else might be able to log into your account. Never approve unknown sign-in attempts or share your MFA code.

Add extra layers of protection.

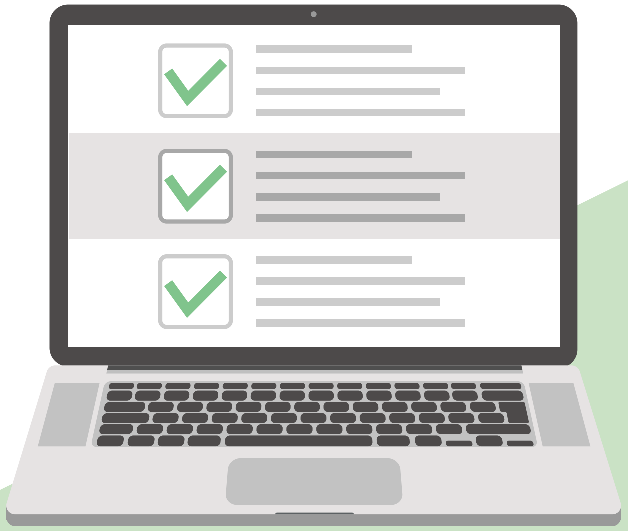
You should use MFA whenever possible, especially when it comes to your most sensitive data, such as your primary email, financial accounts, and health data. To enhance security, your credentials must come from two different categories: for example, something you know (passphrase) and something you are (facial recognition). The more layers of security between your important information and cybercriminals, the better.

Keep up to date

Ensure that any alternative authentication methods such as your recovery email addresses are at least as secure as the primary ones that you use to log into your accounts, and kept kept up to date.

Remember to transfer your authenticator when you change devices

If you are using an authenticator app for MFA and you get a new device, make sure that you transfer it to your new device before disposing of, or resetting, the old one. We recommend adding a recovery method to your account and saving your backup codes in case you lose access to your authenticator app, or delete it. In some cases, you might need to turn off MFA prior to getting a new device and reinstalling the authenticator app. Similarly, if you get a new phone number, make sure that before you lose access to your old phone number, you update your sign-in options for the accounts that normally rely on this number to send you an OTP by SMS.



Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

Copyright

Use of the Coat of Arms

For more information, or to report a cyber security incident, contact us:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre