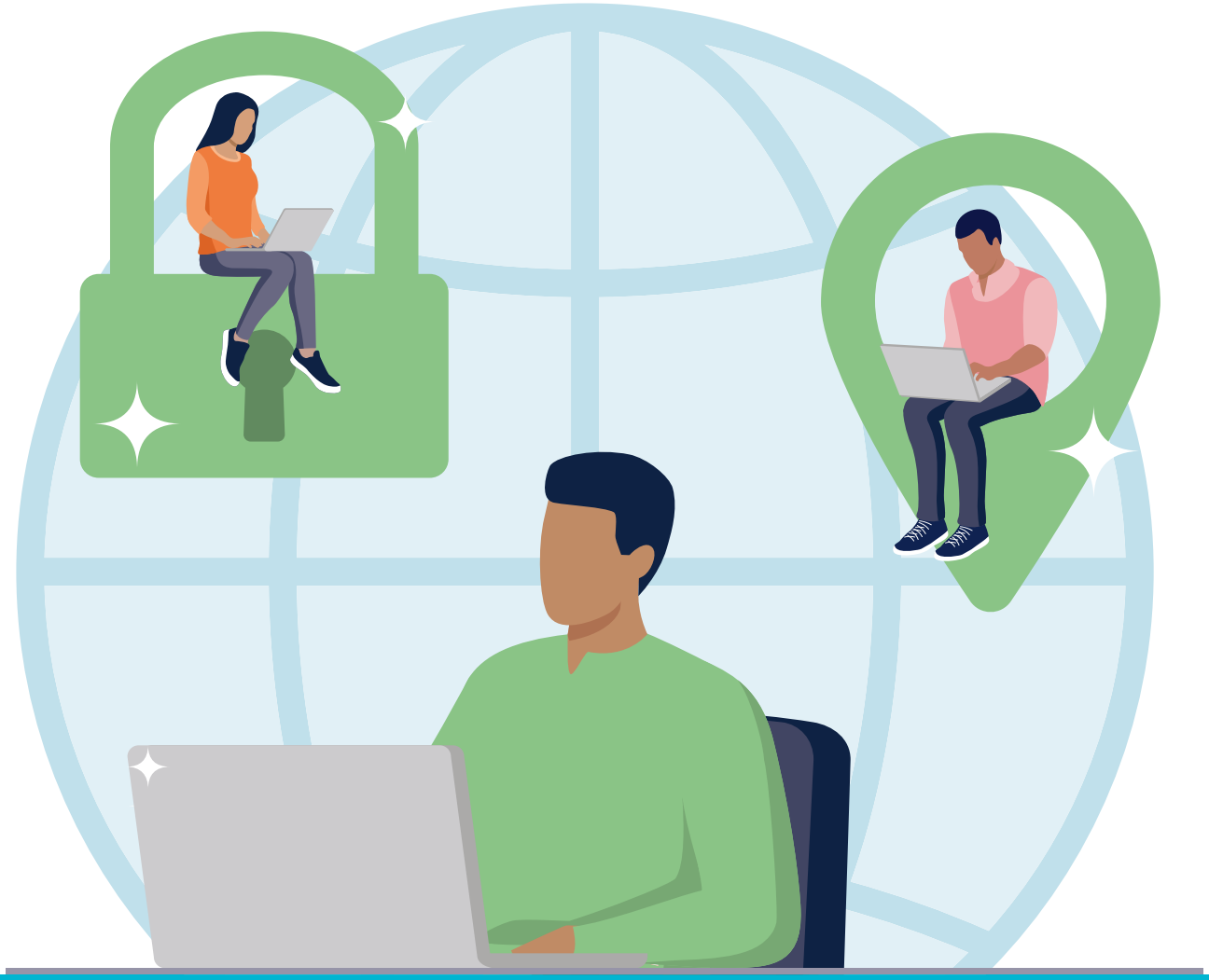
Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre



# Security tips for remote working

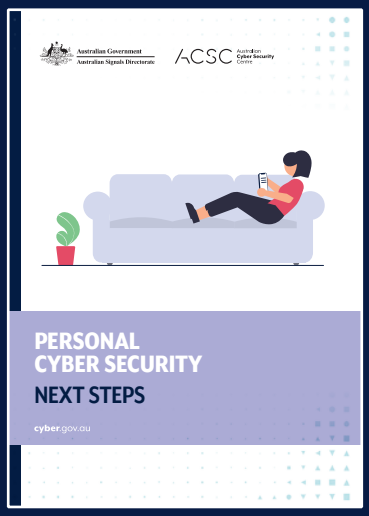
Content Complexity
**SIMPLE**

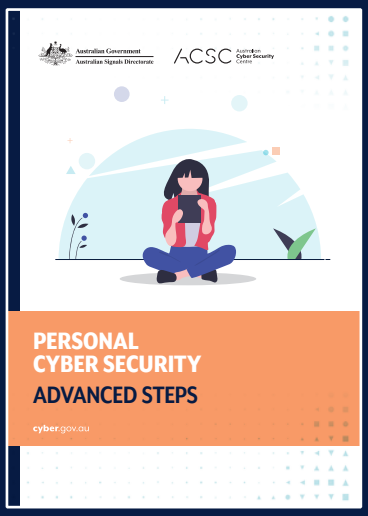
cyber.gov.au

# 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*** series


***Secure your mobile phone***


***Small business cyber security guide***

# Table of contents

Working from home or remotely carries different risks than working from an office. You may not have the same security measures in place as you would in your workplace. This could make you vulnerable to cyber attacks.

Whether this is your first time or your regular routine, it is important to stay vigilant. Follow our tips to secure your accounts, devices, connection and information. If your workplace has a remote work policy, it is best to check what their requirements are.

# Secure your accounts

There are several ways to make your work accounts more secure. Start by using multi-factor authentication and strong passwords.

## Turn on multi-factor authentication

Multi-factor authentication (MFA) is one of the best ways to protect your accounts from cybercriminals.

MFA adds an extra layer of security. You need 2 or more steps to verify your identity before you can log in. For example, using your login details as well as an authentication code.

You should turn on MFA where possible, starting with your most important work accounts.

To find out more, visit cyber.gov.au/mfa

## Use strong passwords

A passphrase is a more secure version of a password. They have 4 or more random words like 'crystal onion clay pretzel'. Passphrases are easy to remember but hard for a cybercriminal to guess.

Create passphrases that are:

- long (14 characters or more)
- unpredictable (a mix of 4 or more random words)
- unique (use a different passphrase for each account).

Don't include personal details or share your passphrases with anyone, including people you work with.

You can use a password manager to create and manage strong passwords and passphrases. There are many secure options available for both companies and individuals.

To find out more, visit cyber.gov.au/passphrases

# Secure your devices

The way you store, manage or move your data and devices is crucial. Adopt secure habits as part of your regular work routine.

## Lock and secure your devices

Lock your computer, laptop, tablet or phone whenever you leave it unattended. Even if it is only for a short period. Make sure your devices are set to automatically lock after a short time (less than 5 minutes).

You should be careful of who has access to your devices. Don't share your devices with anyone. They could expose and delete important information, or infect the device with malware.

## Transfer files securely

Avoid using removable media to transfer files between devices. Portable storage devices such as USB drives are easy to lose, steal or infect with malware.

Use secure methods of file transfer such as cloud storage. Your workplace may already use this for online file management. If you don't have this option, you should encrypt your storage device with a strong passphrase.

## Keep devices and software up to date

Regular updates are crucial for keeping your devices secure. Cybercriminals hack devices by using known weaknesses in systems or applications. Updates have security upgrades to fix these weaknesses.

Make sure your devices and software are up to date. Check automatic updates are on and install updates as soon as possible. The longer you leave it, the more vulnerable you could be to a cyber attack.

Updates may not be available if your device or software is too old. In this case, you should consider upgrading to a newer product to stay secure.

To find out more, visit cyber.gov.au/updates

# Secure your connection

Using an unsecured network at home or in public is risky. Use and maintain a secure connection and avoid public Wi-Fi. Depending on your workplace requirements, you could also use a VPN.

## Improve your network security

Make sure to secure your Wi-Fi network and router to prevent unwanted access. Cybercriminals will target weaker networks, putting your sensitive data at risk.

To improve your network security you should:

- change your default Wi-Fi network name and password
- change your router's default username and password
- use the strongest Wi-Fi encryption available
- keep your router up to date
- disable remote management and Universal Plug and Play
- enable guest Wi-Fi.

To find out more, search 'secure your Wi-Fi and router' on cyber.gov.au

## Avoid public Wi-Fi

Public networks are convenient but can also be unsecure. Cybercriminals will target public networks to gain access to your sensitive information. If you are working in public spaces such as an airport or café, avoid using their Wi-Fi.

Only use trusted networks such as your home Wi-Fi or your personal hotspot. Where this isn't an option, think twice about what you share or access on a public network.

To find out more, seach 'connecting to public Wi-Fi and hotspots' on cyber.gov.au

## Use a VPN

A virtual private network (VPN) can help protect you when using a public network. VPNs hide your identity and activity from other users on the same network. But it won't protect you from threats such as malware, phishing or software security flaws.

If you need to use a VPN, check with your workplace on how to use one securely. Not all VPNs offer the same security, so make sure you choose a reputable VPN provider.

# Secure your information

There are more ways to protect your sensitive information. Creating regular backups and a work user account is crucial. Also be wary of scams and exposing your online meetings or other communications.

## Be aware of your surroundings

Avoid accessing sensitive information when in public locations. You could expose confidential work and customer details to anyone passing by. You should access this type of information when in a private or trusted location.

Check what your workplace requirements are on information security and privacy.

## Back up your data

A backup is a digital copy of your important data such as documents and emails.

If you lose your data, you can use a backup to restore it. You can create backups using the cloud or an external hard drive. Without a backup, you may not be able to recover your data if you fall victim to a cyber attack.

You should back up data that is most important to you and your workplace, if not against company policy. You can turn on automatic backups to reduce the risk.

To find out more, visit cyber.gov.au/backups

## Create a work user account

You should have different user accounts for work and personal use. If a cybercriminal gains access to your personal account, your work files may still be secure.

Avoid using an admin account for everyday tasks such as emailing or web browsing. A standard user account limits access to files, programs and settings on your device.

To find out more, search 'secure your user account' on cyber.gov.au

## Be wary of scams

Cybercriminals can use scams to trick you into compromising yourself or your workplace. Common scams may include asking you to:

- send money or gift cards
- open malicious links or attachments
- reveal sensitive information such as passwords.

Scammers often pretend to be a person or organisation you trust. Be aware that scammers can mask their name and number to appear like the real one.

To avoid falling victim to a scam you should:

- use caution if you're asked to do something with urgency or to log into a website
- avoid opening links or attachments you didn't expect or from someone you don't know
- check for spelling errors in the email or website address
- contact the sender in another way such as through an official website or in person.

Be wary of emails asking you to change your bank account details or make urgent payments. This could be a sign of business email compromise.

To find out more, visit cyber.gov.au/scams and cyber.gov.au/emailsecurity

## Use secure web conferencing systems

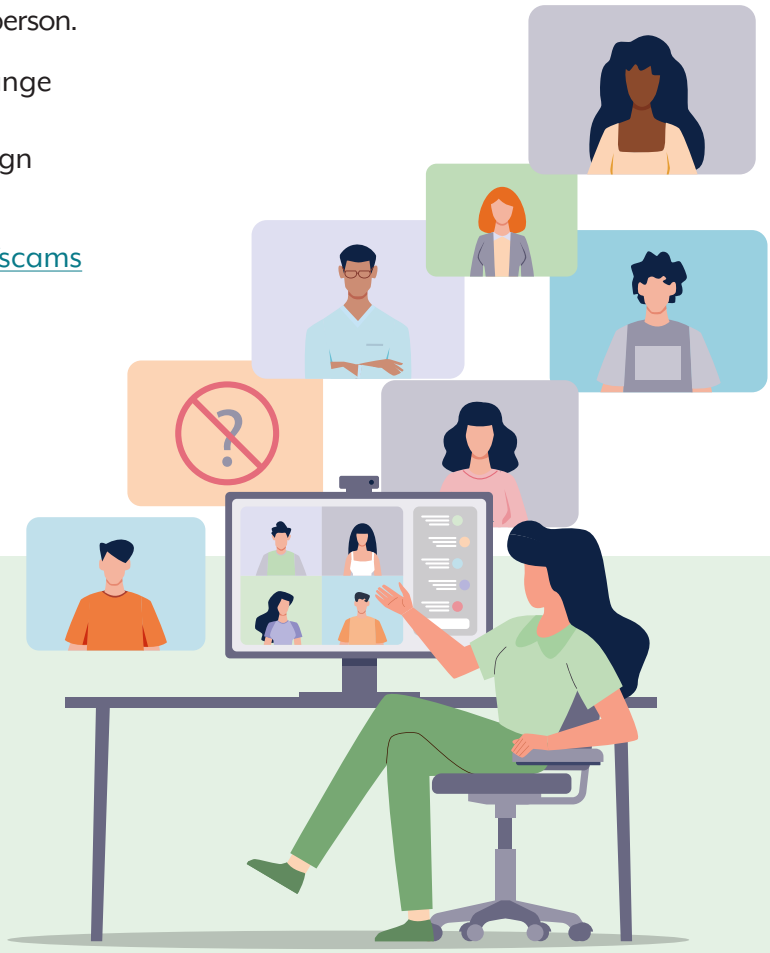
Take extra precautions when using web conferencing tools. This will help stop cybercriminals or unwanted guests from having access to your meetings.

When conducting online meetings be aware of:

- any unidentified participants
- your surroundings and conversations
- what you share on screen.

Make sure the web conferencing system you use has good privacy, security and reputation. Check if your workplace has an approved service provider.

To find out more, search 'web conferencing security' on cyber.gov.au



**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.



**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

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre