VICTORIA State Government | Government Services

Cyber Security Awareness Month

October 2024

Communication kit

EMBARGOED UNTIL 1 OCTOBER 2024

Must not be distributed or shared publicly until 1 October, 2024.

Purpose

What's the purpose of this pack?

This kit is designed to help share the key messages, themes and tools for Cyber Security Awareness Month 2024, and help Victorians stay safe online.

The themes and messaging align with the Australian Federal Government's public messaging for Cyber Security Awareness Month.

The kit includes content you can adjust for different channels, and tailor to your audiences to help us reach as many Victorians as possible.

What's included?

- Newsletter / email content
- Social media material
- Videos (including digital signage) that can be embedded across websites, emails and social media channels.
- A4 Posters (including digital)

Background

Cyber Security Awareness Month

October is recognised worldwide as Cyber Security Awareness Month. It's an ideal time for Victorians to educate themselves about protecting their digital identity. The month follows four national themes, covering the essential steps to digital security.

Victorians are increasingly at risk from cybercriminals wanting to steal their personal information. The Victorian Government is encouraging the community to reduce their cyber risks and protect their personal data by:

- using strong passwords that are long, unique and unpredictable
- turning on multi-factor authentication (MFA)
- turning on automatic software updates
- recognising and reporting phishing scams.

These simple actions can greatly reduce the risk and impact of cyber threats.

The Victorian Government has launched an online **cyber safety check** to help people understand how cyber-secure they are.

Website

vic.gov.au/stay-safe-online

Cyber Safety Check

service.vic.gov.au/cybersafe

Audiences

Who is this content for?

The Victorian Government has identified vulnerable cohorts within Victoria through community research in May 2024.

Passwords

Young (16-24) and older (65+) women are less likely to have strong passwords (such as, using a passphrase of four or more random words). Young Victorians (16-24, men and women) are less likely to have different passwords for each online account. Young (16-24) and older (65+) women are less likely to use a password manager.

Multi-factor authentication (MFA)

Rural residents and women (young and older) are less likely to use MFA for online accounts.

Automatic software updates

Young Victorians (16-24) and multicultural Victorians are less likely to keep software, browsers and apps updated on all their devices.

Phishing

Young men (16-24) are less likely to take defensive behaviours such as this. Young Victorians (16-24) and multicultural Victorians are less likely to avoid clicking on links or attachments when they're not certain who sent an email, message, or SMS.

Spread the word

To help Victorians protect themselves from cyber threats, we need your help to share these messages. Please use the content within this pack and adapt it to share within your own networks in the Victorian community.

Cyber Security Awareness Month follows four weekly themes – you may wish to follow these themes during the month.

You can also follow us and tag us in your posts:

- DGS LinkedIn page - @department-of-government-services
- DGS Facebook page - @VicGovDGS

A full suite of creative can be downloaded from our campaign assets website.

We greatly appreciate any insights, analytics, or feedback on your Cyber Security Awareness Month communications. To contact us, please email communications@dgs.vic.gov.au

For future partnership opportunities, contact cybersafe@dgs.vic.gov.au

Key messages

October is **Cyber Security Awareness Month**. It focuses on four key themes, each week highlighting a step you can take to keep yourself safe online.

- **Week 1** emphasises the need for **strong passwords** to secure your accounts. Use long, unique and unpredictable passwords for each account. Try making 'passphrases' – passwords made up of 4 or more random words – as they're easier to remember.
- **Week 2** highlights why you should turn on **multi-factor authentication (MFA)** to add an extra layer of protection to your accounts. MFA requires a second step to prove it's you logging in – protecting your account even if your password is leaked or stolen.
- **Week 3** emphasises the importance of turning on **automatic software updates** on your devices and apps to protect against software weaknesses and keep your data safe.
- **Week 4** focuses on **protecting yourself against phishing**, a common scam tactic used by cybercriminals. Look out for red flags – such as urgent language. Be cautious with unsolicited links or messages.

By following these steps, you can greatly reduce your risk of falling victim to cyber threats.

For more information about online risks and how to protect yourself, visit vic.gov.au/stay-safe-online

Get a personalised cyber safety check today. Visit: service.vic.gov.au/cybersafe

Suggested newsletter / email content

Subject: Protect yourself online: Essential tips for Cyber Security Awareness Month

In today's increasingly digital world, cyber security is more important than ever. From personal data protection to preventing cyber threats, knowing the risks and how to protect yourself online is key.

This October, as part of Cyber Security Awareness Month, [we/I/organisation name] are encouraging you to focus on four steps you can take to keep yourself safe online.

Use long and unique passwords
Strong passwords are your first defense against people trying to access your online accounts without permission. Protect yourself by making your passwords stronger, today – use long, unique and unpredictable passwords for each account. Try making 'passphrases' (passwords made of 4 or more random words). You can check how strong a password is with Service Victoria's password strength tester: vic.gov.au/passwords

Turn on multi-factor authentication (MFA)
MFA adds an extra layer of protection by asking you to prove in 2 or more ways that it's you logging in. It makes it much harder for others to access your online accounts. Learn more: vic.gov.au/multi-factor-authentication

Turn on automatic software updates
Turning on automatic software updates for your devices and apps is one of the easiest ways to protect yourself online. Check your devices settings to do this. Learn more: vic.gov.au/update-your-devices

Protect yourself from phishing
Phishing is one of the most common scams cybercriminals use to steal personal and financial information. Look out for red flags – such as urgent language. Be cautious with unsolicited links or messages. Learn more: vic.gov.au/phishing

By following these four steps, you can greatly lower your risk of falling victim to cyber threats.

For more tips on staying safe online and to learn more about Cyber Security Awareness Month, visit: vic.gov.au/stay-safe-online

Get a personalised cyber safety check today. Visit: service.vic.gov.au/cybersafe

Visit the **Stay Safe Online** website to learn about:

- **Cyber safety check**
- **Cyber safety tips**
- **Online risks**
- And **Get help** - resources to help you report cybercrime and get support.

NOTE: For additional weekly email content by theme, visit: http://www.vic.gov.au/cyber-security-awareness-month-campaign

Suggested social media content

Images available for use

Week 1

Stay safe online:
Use long and unique passwords
VICTORIA State Government
Government Services

Week 2

Stay safe online:
Turn on multi-factor authentication (MFA)
VICTORIA State Government
Government Services

Week 3

Stay safe online:
Turn on automatic software updates
VICTORIA State Government
Government Services

Week 4

Stay safe online:
Protect yourself from phishing
VICTORIA State Government
Government Services

Download all digital artwork at our campaign assets website.

Week 1: Use long and unique passwords

Example copy text - targeting general population and senior audiences

October is Cyber Security Awareness Month. Over the next four weeks we'll be sharing some simple tips to stay safe online.

Make your passwords long and unique. Longer is stronger.

Try making 'passphrases'. A passphrase is a password made up of 4 or more random words. They're tricky for cybercriminals to crack, but easy for you to remember.

Examples:

🔑 glowering-armour-permanently-jackets

🔑 umbrella-spherical-thunder-lightbulb

🔑 magazine-bottle-alligators-escalator

Test whether a password is strong enough with Service Victoria's password strength checker: https://service.vic.gov.au/find-services/personal/password-strength-tester

Get a personalised cyber safety check today. Visit: service.vic.gov.au/cybersafe

Learn more: vic.gov.au/stay-safe-online

Tags (LinkedIn only): #StaySafeOnline #CyberSecurityAwarenessMonth

Example copy text - targeting youth audiences

October is Cyber Security Awareness Month. Over the next four weeks we'll be sharing some simple tips to stay safe online.

🔑 Make your passwords long and unique. Longer is stronger.

🔑 Try making 'passphrases' – passwords made of 4 or more random words.

It only takes seconds to create a stronger password. Get some passphrase inspiration: https://service.vic.gov.au/find-services/personal/password-strength-tester

Get a personalised cyber safety check today. Visit: service.vic.gov.au/cybersafe

Visit: vic.gov.au/stay-safe-online

#StaySafeOnline #CyberSecurityAwarenessMonth

Example copy text - video

Will your password pass the test of time?
Learn how strong passwords protect your online accounts from cybercriminals: https://youtu.be/2svRjq_4iZg?si=F6Gnx0G-R2ggoFgM

Week 2: Turn on multi-factor authentication (MFA)

Stay safe online:
Turn on multi-factor authentication (MFA)
VICTORIA State Government
Government Services

Example copy text - targeting general population and senior audiences

It's week 2 of Cyber Security Awareness Month – have you turned on multi-factor authentication (MFA)?

MFA is an extra layer of security that makes it harder for cybercriminals to get into your account. For example, using a password and a code sent to your phone to log in.

We recommend turning on MFA for your most important accounts, such as your:

🔒 email

🔒 accounts that save payment details

🔒 financial services

🔒 social media.

Get a personalised cyber safety check today. Visit: service.vic.gov.au/cybersafe

Learn more at vic.gov.au/stay-safe-online

Tags (LinkedIn only): #StaySafeOnline #CyberSecurityAwarenessMonth

Example copy text - targeting youth audiences

It's week 2 of Cyber Security Awareness Month – have you enabled multi-factor authentication (MFA)?

MFA adds an extra layer of protection by asking you to prove in 2 or more ways that it's you logging in.

It only takes a few minutes to enable MFA on your most important accounts:

🔒 email

🔒 accounts that save payment details and personal info

🔒 gaming accounts

🔒 financial services

🔒 social media.

Get a personalised cyber safety check today. Visit: service.vic.gov.au/cybersafe

Visit: vic.gov.au/stay-safe-online

#StaySafeOnline #CyberSecurityAwarenessMonth

Top tips for cyber security
In today's digital world,
VICTORIA State Government

Example copy text - video

Key steps for cyber security

Understand the importance of creating strong passwords, activating multi-factor authentication (MFA), ensuring your device software is always up to date, and safeguarding yourself against phishing.

Link to video (Full-length version)
Link to video (30 secs version for social media channels)

Week 3: Turn on automatic software updates

Example copy text - targeting general population and senior audiences

It's week 3 of Cyber Security Awareness Month – have you turned on automatic software updates?

Turning on automatic software updates for your devices and apps is one of the easiest ways to protect yourself online. Updates fix weaknesses in software – and stop hackers getting in. Make this protection automatic, today.

Get a personalised cyber safety check. Visit: service.vic.gov.au/cybersafe

Learn more at vic.gov.au/stay-safe-online

Tags (LinkedIn only): #StaySafeOnline #CyberSecurityAwarenessMonth

Example copy text - targeting youth audiences

Turning on automatic software updates for your devices and apps is one of the simplest things you can do to protect yourself online. Updates fix weaknesses in software – and stop hackers getting in. Make this protection automatic, today.

Get a personalised cyber safety check today. Visit: service.vic.gov.au/cybersafe

Learn more at vic.gov.au/stay-safe-online

#StaySafeOnline #CyberSecurityAwarenessMonth

Top tips for cyber security
In today's digital world,
VICTORIA State Government

Example copy text - video

Key steps for cyber security

Understand the importance of creating strong passwords, activating multi-factor authentication (MFA), ensuring your device software is always up to date, and safeguarding yourself against phishing.

Link to video (Full-length version)
Link to video (30 secs version for social media channels)

Week 4: Protect yourself from phishing

Stay safe online:
Protect yourself from phishing
VICTORIA State Government
Government Services

Example copy text - targeting general population

In week 4 of Cyber Security Awareness Month, we're encouraging you to learn more about phishing to protect yourself from this increasingly sophisticated scam.

⚠️ Phishing is a common scam tactic used by cybercriminals to steal personal and financial information. ⚠️

Victorians have already lost over $2 million to phishing scams in 2024.

Protect yourself from phishing by keeping the following red flags in mind:

🚩 something sounds too good to be true

🚩 you receive an unexpected email, text, or call asking for personal information

🚩 you're pressured to act quickly

🚩 you're asked to help someone out with money

🚩 you're asked to pay in an unusual way

🚩 there are strange links or attachments

🚩 the subject line or greeting is generic or unspecific

🚩 someone you know is behaving in an odd way.

Get a personalised cyber safety check today. Visit: service.vic.gov.au/cybersafe

Learn more at vic.gov.au/stay-safe-online

Tags (LinkedIn only): #StaySafeOnline, #CyberSecurityAwarenessMonth

Example copy text - targeting senior audiences

⚠️ Victorians aged over 65 years old have lost more than $400,000 to phishing scams so far this year. ⚠️

Recognising phishing scams is easy if you know the red flags to look for:

🚩 you receive an unexpected email, text, or call asking for personal information

🚩 you're pressured to act quickly

🚩 there are strange links or attachments

🚩 the subject line or greeting is generic or unspecific.

Trust your instincts – if something feels off, it's ok to hang up immediately.

Get a personalised cyber safety check today. Visit: service.vic.gov.au/cybersafe

Visit: vic.gov.au/stay-safe-online

#StaySafeOnline #CyberSecurityAwarenessMonth

Week 4: Protect yourself from phishing

Example copy text - targeting youth audiences

⚠ Phishing scams trick you into giving away your personal or financial information. ⚠

Links and attachments in an email or text are used by scammers to steal your personal information, financial details, or install harmful software.

Scammers may text, call, email or contact you on social media. Look out for red flags such as:

🚩 pressure to act quickly

🚩 strange links or attachments

🚩 requests for personal information.

Get a personalised cyber safety check today. Visit: service.vic.gov.au/cybersafe

Visit: vic.gov.au/stay-safe-online

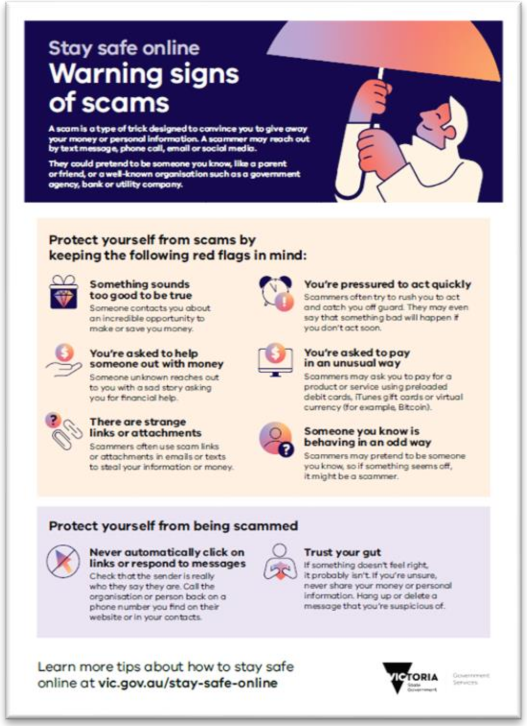
#StaySafeOnline #CyberSecurityAwarenessMonth

Example copy text - video

What is phishing? How can you spot it?
A deep dive into what phishing scams are and tips on how to stay safe online.

Link to video (Full-length version)
Link to video (30 secs: socials)

A4/A3 factsheets, posters, and digital signage



Stay safe online

Warning signs of scams

A scam is a type of trick designed to convince you to give away your money or personal information. A scammer may reach out by text message, phone call, email or social media.

They could pretend to be someone you know, like a parent or friend, or a well-known organisation such as a government agency, bank or utility company.

Protect yourself from scams by keeping the following red flags in mind:

Something sounds too good to be true
Someone contacts you about an incredible opportunity to make or save you money.

You're asked to help someone out with money
Someone unknown reaches out to you with a sad story asking you for financial help.

There are strange links or attachments
Scammers often use scam links or attachments in emails or texts to steal your information or money.

You're pressured to act quickly
Scammers often try to rush you to act and catch you off guard. They may even say that something bad will happen if you don't act soon.

You're asked to pay in an unusual way
Scammers may ask you to pay for a product or service using preloaded debit cards, iTunes gift cards or virtual currency (for example, Bitcoin).

Someone you know is behaving in an odd way
Scammers may pretend to be someone you know, so if something seems off, it might be a scammer.

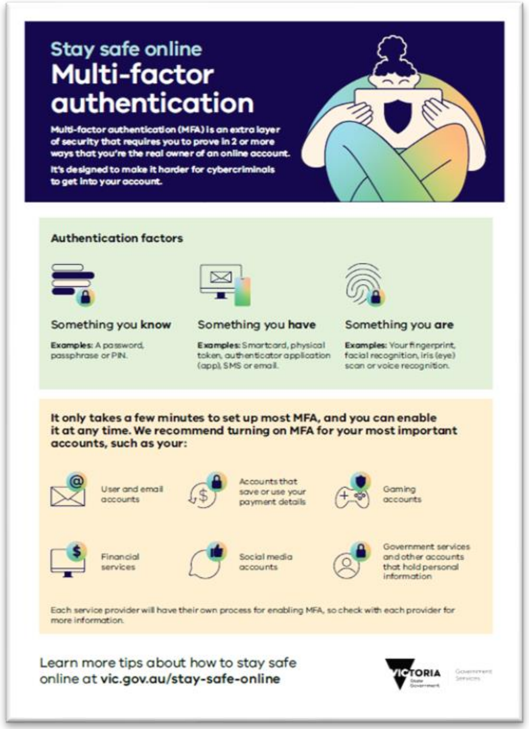
Protect yourself from being scammed

Never automatically click on links or respond to messages
Check that the sender is really who they say they are. Call the organisation or person back on a phone number you find on their website or in your contacts.

Trust your gut
If something doesn't feel right, it probably isn't. If you're unsure, never share your money or personal information. Hang up or delete a message that you're suspicious of.

Learn more tips about how to stay safe online at **vic.gov.au/stay-safe-online**

A4 Factsheet



Stay safe online

Multi-factor authentication

Multi-factor authentication (MFA) is an extra layer of security that requires you to prove in 2 or more ways that you're the real owner of an online account.

It's designed to make it harder for cybercriminals to get into your account.

Authentication factors

Something you **know**
Examples: A password, passphrase or PIN.

Something you **have**
Examples: Smartcard, physical token, authenticator application (app), SMS or email.

Something you **are**
Examples: Your fingerprint, facial recognition, iris (eye) scan or voice recognition.

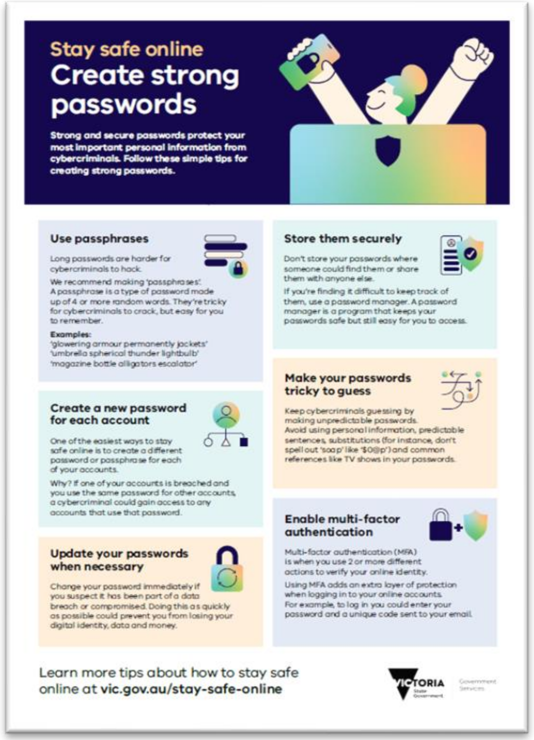
It only takes a few minutes to set up most MFA, and you can enable it at any time. We recommend turning on MFA for your most important accounts, such as your:

- User and email accounts
- Accounts that save or use your payment details
- Gaming accounts
- Financial services
- Social media accounts
- Government services and other accounts that hold personal information

Each service provider will have their own process for enabling MFA, so check with each provider for more information.

Learn more tips about how to stay safe online at **vic.gov.au/stay-safe-online**

A4 Factsheet



Stay safe online

Create strong passwords

Strong and secure passwords protect your most important personal information from cybercriminals. Follow these simple tips for creating strong passwords.

Use passphrases
Long passwords are harder for cybercriminals to hack.
We recommend making 'passphrases'. A passphrase is a type of password made up of 4 or more random words. They're tricky for cybercriminals to crack, but easy for you to remember.
Examples:
'glowering armour permanently jackets'
'umbrella spherical thunder lightbulb'
'magazine bottle alligators escalator'

Create a new password for each account
One of the easiest ways to stay safe online is to create a different password or passphrase for each of your accounts.
Why? If one of your accounts is breached and you use the same password for other accounts, a cybercriminal could gain access to any accounts that use that password.

Update your passwords when necessary
Change your password immediately if you suspect it has been part of a data breach or compromised. Doing this as quickly as possible could prevent you from losing your digital identity, data and money.

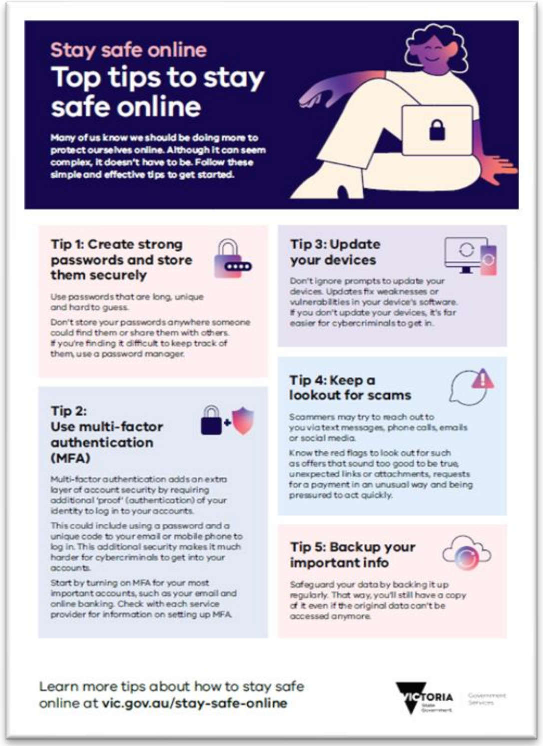
Store them securely
Don't store your passwords where someone could find them or share them with anyone else.
If you're finding it difficult to keep track of them, use a password manager. A password manager is a program that keeps your passwords safe but still easy for you to access.

Make your passwords tricky to guess
Keep cybercriminals guessing by making unpredictable passwords. Avoid using personal information, predictable sentences, substitutions (for instance, don't spell out 'soap' like '$0@p') and common references like TV shows in your passwords.

Enable multi-factor authentication
Multi-factor authentication (MFA) is when you use 2 or more different actions to verify your online identity.
Using MFA adds an extra layer of protection when logging in to your online accounts. For example, to log in you could enter your password and a unique code sent to your email.

Learn more tips about how to stay safe online at **vic.gov.au/stay-safe-online**

A4 Factsheet



Stay safe online

Top tips to stay safe online

Many of us know we should be doing more to protect ourselves online. Although it can seem complex, it doesn't have to be. Follow these simple and effective tips to get started.

Tip 1: Create strong passwords and store them securely
Use passwords that are long, unique and hard to guess.
Don't store your passwords anywhere someone could find them or share them with others. If you're finding it difficult to keep track of them, use a password manager.

Tip 2: Use multi-factor authentication (MFA)
Multi-factor authentication adds an extra layer of account security by requiring additional 'proof' (authentication) of your identity to log in to your accounts.
This could include using a password and a unique code to your email or mobile phone to log in. This additional security makes it much harder for cybercriminals to get into your accounts.
Start by turning on MFA for your most important accounts, such as your email and online banking. Check with each service provider for information on setting up MFA.

Tip 3: Update your devices
Don't ignore prompts to update your devices. Updates fix weaknesses or vulnerabilities in your device's software. If you don't update your devices, it's far easier for cybercriminals to get in.

Tip 4: Keep a lookout for scams
Scammers may try to reach out to you via text messages, phone calls, emails or social media.
Know the red flags to look out for such as offers that sound too good to be true, unexpected links or attachments, requests for a payment in an unusual way and being pressured to act quickly.

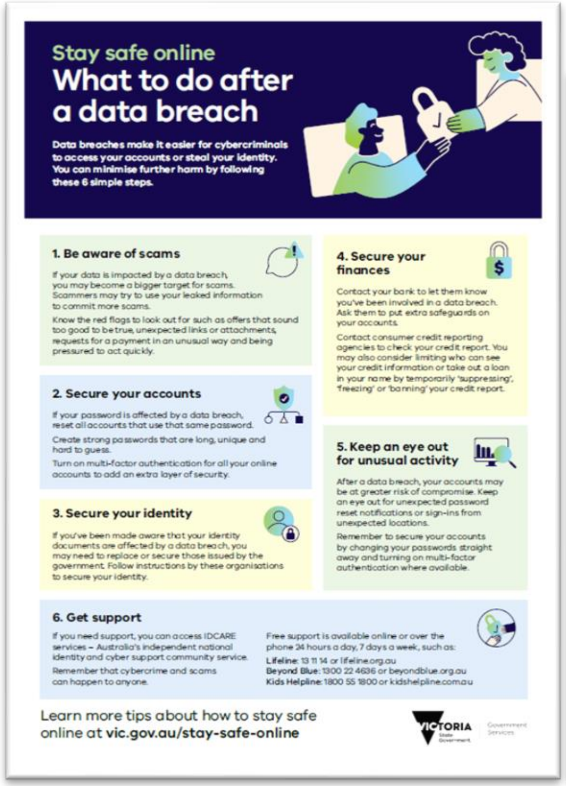
Tip 5: Backup your important info
Safeguard your data by backing it up regularly. That way, you'll still have a copy of it even if the original data can't be accessed anymore.

Learn more tips about how to stay safe online at **vic.gov.au/stay-safe-online**

A4 Factsheet

Download all digital artwork at our campaign assets website.

A4/A3 factsheets, posters, and digital signage



Stay safe online

What to do after a data breach

Data breaches make it easier for cybercriminals to access your accounts or steal your identity. You can minimise further harm by following these 6 simple steps.

1. Be aware of scams

If your data is impacted by a data breach, you may become a bigger target for scams. Scammers may try to use your leaked information to commit more scams.

Know the red flags to look out for such as offers that sound too good to be true, unexpected links or attachments, requests for a payment in an unusual way and being pressured to act quickly.

2. Secure your accounts

If your password is affected by a data breach, reset all accounts that use that same password.

Create strong passwords that are long, unique and hard to guess.

Turn on multi-factor authentication for all your online accounts to add an extra layer of security.

3. Secure your identity

If you've been made aware that your identity documents are affected by a data breach, you may need to replace or secure those issued by the government. Follow instructions by these organisations to secure your identity.

4. Secure your finances

Contact your bank to let them know you've been involved in a data breach. Ask them to put extra safeguards on your accounts.

Contact consumer credit reporting agencies to check your credit report. You may also consider limiting who can see your credit information or take out a loan in your name by temporarily 'suppressing', 'freezing' or 'banning' your credit report.

5. Keep an eye out for unusual activity

After a data breach, your accounts may be at greater risk of compromise. Keep an eye out for unexpected password reset notifications or sign-ins from unexpected locations.

Remember to secure your accounts by changing your passwords straight away and turning on multi-factor authentication where available.

6. Get support

If you need support, you can access IDCARE services – Australia's independent national identity and cyber support community service.

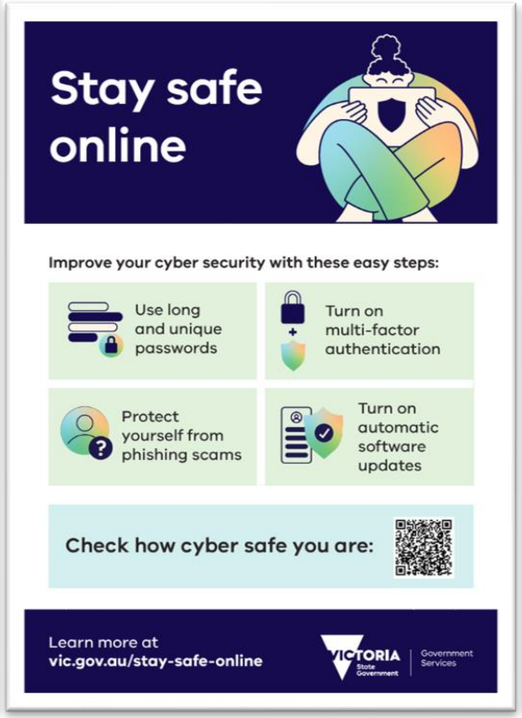
Remember that cybercrime and scams can happen to anyone.

Free support is available online or over the phone 24 hours a day, 7 days a week, such as:

Lifeline: 13 11 14 or lifeline.org.au
Beyond Blue: 1300 22 4636 or beyondblue.org.au
Kids Helpline: 1800 55 1800 or kidshelpline.com.au

Learn more tips about how to stay safe online at **vic.gov.au/stay-safe-online**

A4 Factsheet



Stay safe online

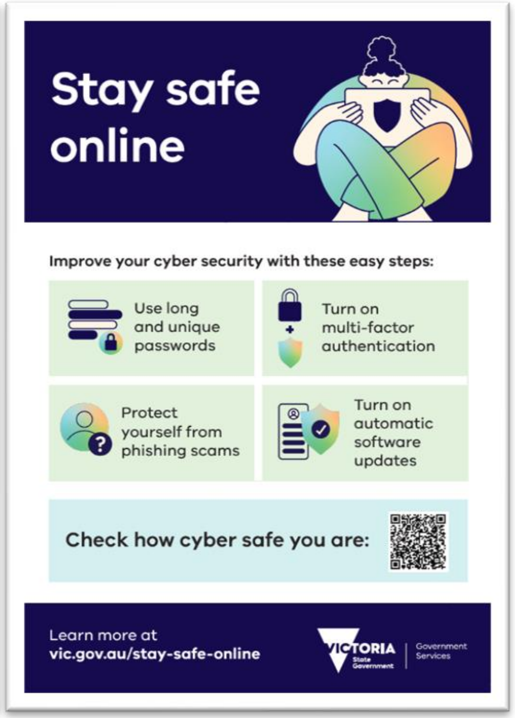
Improve your cyber security with these easy steps:

Use long and unique passwords	Turn on multi-factor authentication
Protect yourself from phishing scams	Turn on automatic software updates

Check how cyber safe you are:

Learn more at **vic.gov.au/stay-safe-online**

A3/A4 Poster



Stay safe online

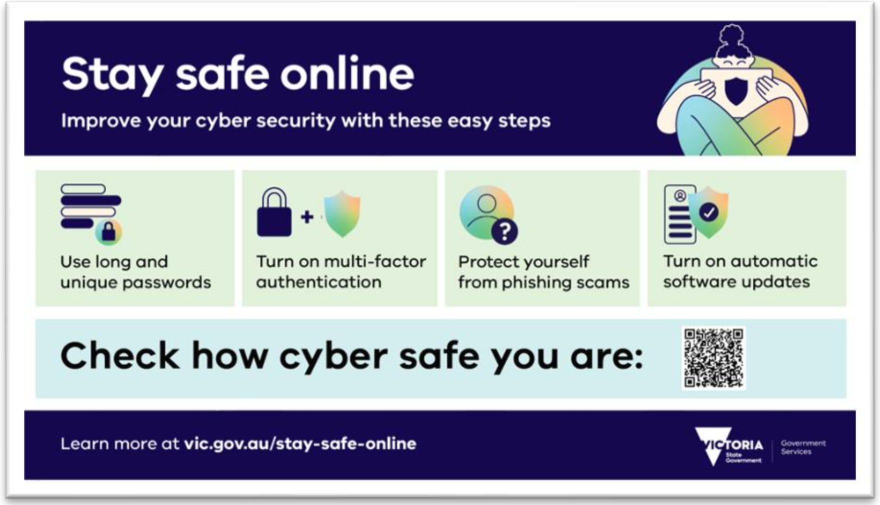
Improve your cyber security with these easy steps:

Use long and unique passwords	Turn on multi-factor authentication
Protect yourself from phishing scams	Turn on automatic software updates

Check how cyber safe you are:

Learn more at **vic.gov.au/stay-safe-online**

Outdoor digital signage
(1080x1920 300 dpi)



Stay safe online

Improve your cyber security with these easy steps

Use long and unique passwords	Turn on multi-factor authentication	Protect yourself from phishing scams	Turn on automatic software updates

Check how cyber safe you are:

Learn more at **vic.gov.au/stay-safe-online**

Outdoor digital signage
(1920x1080 300 dpi)

Download all digital artwork at our campaign assets website.

More information

Follow Department of Government Services (DGS) on social media

Please follow DGS's social channels and share its resources, including its Stay Safe Online content.

- DGS LinkedIn page - @department-of-government-services
- DGS Facebook page - @VicGovDGS

To contact us, please email communications@dgs.vic.gov.au

For future partnership opportunities, contact cybersafe@dgs.vic.gov.au