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**

VICTORIA State Government | Government Services

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**

VICTORIA State Government | Government Services

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:

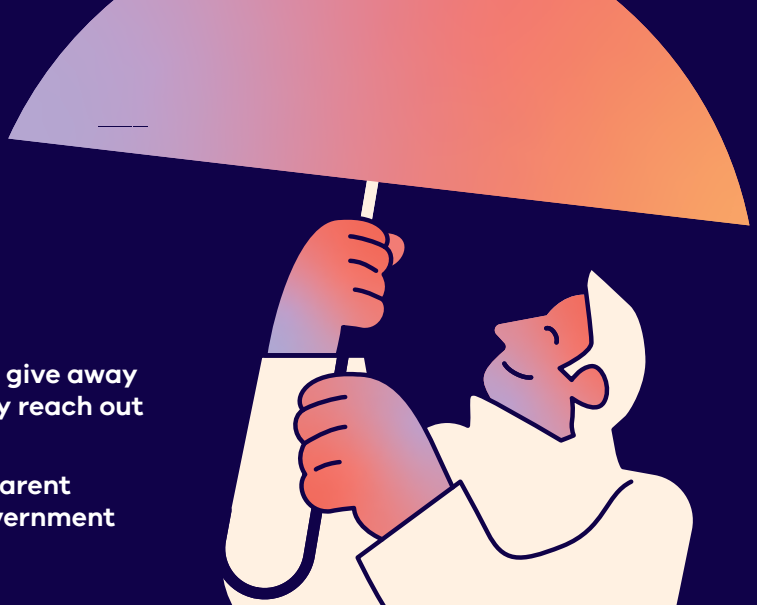
Lifeline: 13 11 14 or lifeline.org.au
Beyond Blue: 1300 22 4636 or beyondblue.org.au
Kids Helpline: 1800 55 1800 or kidshelpline.com.au

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

VICTORIA State Government | Government Services

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**

VICTORIA State Government | Government Services

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**

VICTORIA State Government | Government Services