HELPFUL HINTS

Direct from the Police.

www.police.vic.gov.au/online-identity-theft

To help protect your personal information, you should:

- never open suspicious looking texts, emails or social media messages
- never give credit card, account details or other personal documents to someone you don't know or trust.
- never give strangers remote access to your computer.
- choose passwords that are hard for others to guess.
- be aware of the information you post online and who can see it.
- never log in to personal accounts using shared or public WiFi.
- remove all your personal information before selling or throwing away a computer, mobile phone or other digital device.
- secure networks and digital devices with anti-virus software and a firewall.
- regularly check your bank accounts for suspicious activity.

For more advice to protect yourself from identity theft, visit the Australian Cyber Security Centre website.

Direct from the ATO.

The incident has been reported to the Australian Taxation Office (**ATO**), in order that they can add additional security measures to your Tax File Number. These measures aim to detect fraudulent activity.

There is nothing further you need to do; however, if you have any concerns, you may wish to contact the ATO's specialist Client Identity Support Centre on 1800 467 033 Monday to Friday 8.00am–6.00pm AEST.

More information is available on the ATO's website at www.ato.gov.au/general/online-services/identity-security-and-scams/help-for-identity-theft/data-breach-guidance-for-individuals/

Putting a ban on your credit report.

You can request a ban to 'freeze' access to your credit report.
How to www.idcare.org/fact-sheets/credit-bans-australia

This means that credit reporting agencies can't provide information from your consumer credit file to credit providers.

They can only disclose information if you give them permission in writing, or they are required to by law.

If a ban is placed on your credit report, you can still use your credit cards and repay existing loans.

A ban won't affect your current credit line or credit payments unless your credit card is about to expire.

There are 3 main credit agencies in Australia, and a ban with one will alert the others.

- Equifax
    - www.equifax.com.au/eform/submit/credit-ban
    - Or call 13 83 32
- Illion
    - www.illion.com.au/credit-report-ban-request/
    - Or call 1300 734 806
- Experian
    - www.experian-apac-acb.my.site.com/banrequest/s/ban-request-form
    - Or call 1300 783 684

USEFUL LINKS FOR MORE INFORMATION

Passphrases fact sheet from ACSC website

- www.cyber.gov.au/protect-yourself/securing-your-accounts/passphrases

ABC News Report 28.03.23

- – This is the most detailed portrait yet of data breaches in Australia
    - www.abc.net.au/news/2023-03-28/detailed-portrait-data-breaches-oaic-disclosures/102131586

List of Known bigger Data Breaches

- Updated list that shows news articles of data breaches
    - When on this page, scroll down and see from latest to oldest.
        - www.webberinsurance.com.au/data-breaches-list

Dark Web email checkers

- You can check if your email address has been in a prior data breach.
    - have I been Pwned – www.haveibeenpwned.com
    - Norton - www.au.norton.com/breach-detection

Scam Adviser www.scamadviser.com

- This website will check if websites you want to visit are legitimate.

Free Further Advice and Individual Support

- You can also contact IDCare for Free advice and support.
    - IDCARE – Australia & New Zealand's National Identity and Cyber Support Service
        - Call 1800 595 160 or visit www.idcare.org/

STATISTICS

- 94,000 cybercrime's reported in 22-33, or 1 every 6 minutes according to the ASD Cyber threat report (Australian Signals Directorate – Australian Cyber Security Centre ACSC).
- BUT it's estimated that 75% of data breaches go unreported.
- NAB's Business Insights Report found more than 1 in 10 Australian businesses have been subjected to a data breach or cybercrime in the past 12 months.

POINTS TO REMEMBER

1. NEVER EVER click links in emails/text messages
    a. Open a web browser and type it in yourself or google it.
    b. E.g. above link, google Webber Insurance data breach list and the top choice is the 2018 – 2024 lists page.

2. NEVER EVER give out any personal information on a cold call, as in, a call you are not expecting.
    a. Any legitimate caller will understand your reasoning and give you enough information that you can make your own enquiries on a phone number you find yourself.
    b. If they abuse you or make demands, they are a scammer.

3. Have as many Multi Factor Authentications (MFA) or passcodes set up as possible (where they send you a code via text or email that they have on file, or use an authenticator app)

4. Update passwords frequently/use complicated passwords or where possible, use passphrases.
    a. So, a series of numbers/letters/symbols with a pattern only you will recognise.

5. Lock your credit file, known as a Credit Ban.

6. Closely monitor your banking information
    a. Talk to your bank and ask what safety measures they have that you can implement… this could be a passphrase for phone calls, but most now want MFA before they speak with you anyway, so ensure your details are up to date with them.

7. Do a regular audit of programs and apps you actually use, and those you don't.
    a. Delete those you don't need or use.

8. Keep software/firmware up to date on electronic devices.