HELPFUL HINTS

This information is supplied by the Australian Federal Police.

STASTICS

- 94,000 cybercrimes were reported in 2022-23, that is one every 6 minutes, according to the Australian Signals Directorate.

- It is 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.

IMPORTANT POINTS TO REMEMBER

- *Never click on links, web forms, or scan QR codes within an email or text message:* scam messages may try and trick you into giving out your personal information. A scammer might ask for your bank account details, passwords or credit card numbers. They may also ask you to download files, software, or allow remote access to your computer.

- *Never provide personal information on a call you are not expecting:* a 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. A scammer will often seem very demanding.

- *Set up multi-factor authenticator to add an extra layer of security to your online accounts:* multi-factor authenticator is when you need 2 or more proofs of identity to be able to log into your account, this may include using your login details as well as an authentication code, making it harder for someone else to access your online accounts.

- *Install software updates regularly to keep your devices secure:* software updates are new, improved, or fixed versions of software or apps. Check automatic updates are on so you are notified when an update is available. Regular updates help improve your security, so do not ignore prompts to install. The longer you leave it, the more vulnerable you could be to a cyber-attack.

- *Create strong and unique passphrases that are over 14 characters long and use 4 or more random words:* use different passphrases for each of your accounts. If one account gets compromised your other accounts remain safe. A password manager can help you with creating or storing unique passphrases.

- *Use a secure wireless network:* ensure vigilant behaviour when using public wireless networks. Avoid making online transactions or using important information while using public or complimentary Wi-Fi.

- *Be careful about what you share on social media:* be sure to know who you are speaking to on social media, and only share information with people you know and trust. Criminals can use certain combinations of your person information to impersonate you to access money, apply for credit cards and bank loans, or commit crimes.

- *Monitor your accounts for unusual activity or transactions:* closely check your accounts for transactions or interactions you did not make, or content you did not post. If any organisation you deal with sends you an email warning you of unexpected changes to your account, do not click on included links or attachments. Immediately check your account and contact the organisation.

- *Never leave your information unattended:* secure your electronic devices wherever you are.

- *Complete regular audit of programs and apps you use and those you do not:* delete any programs you no longer use or require.

DIRECT FROM THE POLICE

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 do not 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 Wi-Fi.
- 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 and the Australian Signals Directorate Identity Theft page.

PUTTING A BANK ON YOUR CREDIT REPORT

You can request a bank to ‘freeze’ access to your credit report. For advice on ‘how to’, visit the iDcare fact sheet.

In implementing a ban, credit reporting agencies cannot 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 by law.

If a ban is placed on your credit report, you can still use your credit cards and repay existing loans. A ban will not affect your current credit line or credit payments unless your credit card is about to expire.

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

- Equifax
    - Place, Extend or Remove a ban on my Equifax credit report | Equifax Australia
    - Or call 13 83 32
- Illion
    - Credit Report Ban Request - illion
    - Or call 13 23 33
- Experian
    - Request a Ban on Your Credit Report | Experian Australia
    - Or call 13 83 32

USEFUL LINKS FOR FURTHER INFORMATION

Passphrases fact sheet from ACSC website

- Passphrases | Cyber.gov.au

ABC News Report 28.03.2023

- This is a highly detailed portrait of data breaches in Australia.
- This is the most detailed portrait yet of data breaches in Australia - ABC News

List of known substantial data breaches

- Updated list that shows news articles of data breaches.
- List of Data Breaches and Cyber Attacks in Australia 2018-2024 (webberinsurance.com.au)

Dark Web email checkers

- You can check if your email address has been in a prior data breach.
- Have I been Pwned? - Have I Been Pwned: Check if your email has been compromised in a data breach
- Norton - Has Your Email Been Compromised? Free Data Breach Checker (norton.com)

Scam Adviser

- This website will check if websites you want to visit are legitimate.
- ScamAdviser.com | Check a website for risk | Check if fraudulent | Website trust reviews |Check website is fake or a scam

Free Further Advice and Individual Support

- You can also contact IDCare for free advice and support.
    - IDCARE – Australia & New Zealand's National Identity and Cuber Support Service
    - Call 1800 595 1600 or visit IDCARE Official Website | Identity Theft & Cyber Support

Office of Victoria Information Commissioner

- The primary regulator and source of independent advice to the community and Victorian government about how the public sector collects, uses, and discloses information. Office of the Victorian Information Commissioner – Freedom of Information | Privacy | Data Protection (ovic.vic.gov.au)