Protect your bank account from scammers

According to the ACCC's Scamwatch statistics, Australians reported a total of $568.6 Million lost to scams in 2022, with 39% of the losses for people aged 55 and over[1], which makes for big business for scammers, and a cause for concern for all Australians.

According to research by the Commonwealth Bank (CBA) (September 2022)[2], 60% of Australians reported having personally been a victim of a scam or knew someone who had, and 57% of Australians reported becoming more concerned about scams over the last 12 months. This is unsurprising given the constant flow of suspicious emails, texts, phone calls, and more that Australians are bombarded with. CBA's research shows that Australians receive roughly five scam calls, emails, or messages a week, equating to over 250 attempts a year. Not to mention the recent rise in high profile data breaches and cyber-attacks that seem to have become a consistent theme in the media.

Like many Australians, if you've been caught up in one of these breaches, you might be left wondering what information was exposed and how this could be used.

Unfortunately, data breaches and scams often go hand in hand with scammers using the accessed information to target individuals.

Following the 2022 Optus data breach, the ACCC's Scamwatch urgently warned Australians to be on the lookout for increased scam activity and to take steps to further protect themselves.

Unfortunately, there's no shortage of ways fraudsters and scammers might attempt to get you to part with your hard-earned cash, from phishing for information to impersonation of family members, from "Hi Mum" texts to puppy scams, nothing seems to be off limits.

It's important to always be on the lookout for anything suspicious and to make sure you're taking steps to keep your money safe.

Here are some action steps that you can take to protect yourself today:

1. Take a moment to pause…

Before you click that link to "confirm" your personal details or open that attachment, **STOP**.

How legitimate does the message look and feel? If there are spelling errors in the email or the email/web address looks strange, it's best to ignore it.

You can always contact the business directly to ask if the contact is legitimate.

2. Password123

If any of your passwords are likely to make the top 10 most common passwords list, it's time for a change.

---

[1] Scamwatch.gov.au

[2] www.commbank.com.au *'Research shows the average Australian receives over 250 scam attempts a year' (accessed 14/10/2022)*

Passwords for all online accounts should be strong and unique. It's also best to avoid using the same password for multiple accounts. Lastpass used to be the go-to for password security, but they too have been recently hacked.

Keeping safe online

When accessing your accounts online, there are a number of steps that can be taken to keep your information safe:

- Ensure you have up to date anti-virus software on devices used to access banking.
- Do not store banking information on your computer.
- Use a secure browser when logging into online banking.
- Avoid using public Wi-Fi to log into online banking.

3. Multi-Factor Authentication

Multi-Factor Authentication requires a second verification process to be able to access an account. This is often an SMS or email code or through the use of an authenticator app.

Enabling this provides an extra hurdle for anyone trying to access your accounts.

4. Regular monitoring

It's important to make sure you're regularly checking your accounts and bank statements for any scam activity. If you see something suspicious, contact your bank straight away!

For the time being it looks like scammers are here to stay. You can better secure your future by taking the necessary steps to protect yourself and your bank accounts. The steps outlined above are a great start to keeping your accounts safe.

If you've been scammed, or believe you might be at risk of being scammed, it's important to take immediate action:

- Contact your bank and financial institutions immediately to report the suspected scam and seek their advice on what to do next.
- If you think your online password has been compromised, take steps to secure your accounts by changing your password.
- Report the scam to the ACCC via their "Report a Scam" webpage.

You can also check out ScamWatch for more information on scams and where you can go for further help. https://www.scamwatch.gov.au/get-help/where-to-get-help