

How to secure your digital finances



Most domestic and family violence involves some form of financial¹ and/or technology-facilitated² abuse.

For many people, implementing more secure online banking habits can help them feel their technology and money is safer. For others, especially anyone who is controlled or abused, making these changes may feel difficult or even be unsafe. It's important to trust your instincts and only make digital financial changes if you feel they are safe for you to do so.

Keeping technology private and secure can help keep your finances safe and build better digital financial security, but other types of safety are important, too.

Where you can get help

If you or someone you know are experiencing domestic and family violence or financial abuse, or remain unsure, there are support services you can access. Please note that the bank, domestic and family violence support services, and local police stations are still open and helping to provide support and assistance.

Community Wellbeing Team

Our Community Wellbeing specialists are bank staff that are specifically trained to ensure the financial safety and wellbeing of our customers experiencing domestic and family violence. You can call a Community Wellbeing specialist on **1800 222 387** between 8am and 6pm, Monday to Friday (Sydney/Melbourne time – excluding public holidays).

1800RESPECT

Always consider your personal circumstances before acting on financial advice. For confidential information, counselling and support, we recommend calling **1800RESPECT** on **1800 737 732**. This is a free and confidential service that is not part of Commonwealth Bank.

If you need an interpreter or translator, you can use the telephone Translating and Interpreting Service (TIS National) on **131 450**, specify your required language and ask them to contact the **Community Wellbeing Team** or **1800RESPECT**. TIS National is available free of charge.*

1 commbank.com.au/content/dam/caas/newsroom/docs/UNSW-report1-Financial-Abuse-and-IPV-newsroom.pdf

2 wesnet.org.au/about/research/2ndnatsurvey/

Here are some things you can do to increase digital security where it's safe for you to do so:

Account log ons and passwords

- Choose strong, unique passwords and security questions and answers that no one else knows or can easily guess.
- Avoid keeping username/password details anywhere unsecured or in easily accessible places and update passwords regularly. Resist sharing login details with others or saving login details on the browser.
- Protect accounts using two-step verification or multi-factor authentication. Adopt a mix of passcodes, PINS, patterns and/or face or fingerprint recognition tools to secure access to devices.

Updates and apps

- Keep your device and computer operating systems up-to-date.
- Keep your apps up-to-date and perform software updates when prompted. Most software updates are designed to fix security or other problems so that your experience is more secure. But make sure you only update through your device's App Store, not from random text messages or emails.
- Consider deleting and uninstalling any apps or accounts that are unfamiliar or no longer used.
- Try not to save secured sites, such as internet banking, to your favourites tab you could be accessing an out-of-date site where security or other problems have not been fixed.

Safer account and device use

- Use Private or Incognito browsing options to limit tracking of website searches. Log out of important online accounts when finished and delete the browser history afterwards.
- If you are worried that someone is accessing your communications through your accounts, emails or your physical devices, consider using a safer device that they do not have access to. You could for example, borrow a trusted friend or family member's phone if you need to reach out for legal or domestic violence advice.

Additional tips when securing your banking

- Hide PIN numbers and login details from others when engaging digital banking services.
- For general data security, avoid using public computers or public Wi-Fi to access and manage financial accounts.

Additional tips when updating your passwords

- Avoid using things such as birth dates, pet names, anniversary dates or facts specific to children.
- Consider using a reputable password manager to generate and store strong, unique passwords. For more information see: techsafety.org.au/resources/resources-women/passwords/.

CommBank – What to do if you suspect fraud or disputed transactions

- If you suspect fraud or if you want to dispute a transaction contact us immediately at commbank.com.au/support/faqs/355.
- For extra control and security over your account, you can put a temporary lock on your debit or credit card in NetBank or the CommBank app.
- Get a copy of your credit report – you can request your credit score report for free on sites like My Credit File at mycreditfile.com.au/.
- Report the matter to the police – for police assistance where there is no immediate danger or to report non-urgent crime call 131 444.

If you would like more information about the above, please visit our disputing a transaction page at commbank.com.au/support/disputing-a-transaction.

If you would like specific information on what you should do if you suspect credit card fraud please visit our credit card fraud page at commbank.com.au/articles/credit-cards/what-should-you-do-if-you-suspect-credit-card-fraud.

Tips on how to document technology-facilitated financial abuse safely

If you are experiencing financial abuse, it may be useful to document what has been happening (see techsafety.org.au/resources/resources-women/documentation-tips/). Here are some tips on what to do if it is safe to do so:

- Take screenshots or save bank or other statements that include abusive messages or threats. If the messages have hidden meaning only known between you and your abuser, it's a good idea to include the context and how it makes you feel as well.
- Print off evidence of possible suspect transactions, ATM or EFTPOS details, app or website account activity.
- Check statements for payment irregularities (e.g. proof of spyware purchase).
- Screenshot (see techsafety.org.au/resources/resources-women/how-to-take-a-screenshot/) suspect transactions, odd account activity and failed login attempt notifications, and consider saving evidence on a hidden USB.
- Write down what is happening including transaction specifics, including physical location of activity. Keep documents safe and secure, even if that means off-site, locked at work or with a trusted friend.
- Check the history, privacy and security settings of your major accounts to make sure only devices you know are logged in. Document anything that looks unusual.

How to access support

- Call 1800 RESPECT on 1800 737 732 or visit 1800respect.org.au/violence-and-abuse/financial-abuse/toolkit/next-steps
- See CommBank's Addressing Financial Abuse information at commbank.com.au/factsheet
- Access free, confidential advice from the National Debt Hotline on 1800 007 007 or visit ndh.org.au/
- You can call a Community Wellbeing specialist on 1800 222 387 between 8am and 6pm, Monday to Friday (Sydney/Melbourne time – excluding public holidays).
- Research solutions on the Australian Competition & Consumer Commission website at acc.gov.au/consumers/debt-debt-collection/help-when-youre-in-debt

Additional Resources – Where to get help

Help in languages other than English

tishnational.gov.au/

Recognise and Recover Guide at commbank.com.au/support/recognise-and-recover

WESNET Women's Technology Safety and Privacy Toolkit

techsafety.org.au/resources

National Identity and Cyber Support

idcare.org

