

Digital Financial Security



What is digital financial security?

For many people, banking has moved to online platforms. We access and manage our funds using our mobile phones and computers.

Digital financial security is about keeping your electronic data and information private and safe. This can include protecting your PINs and passwords, and securing yourself against technology-facilitated abuse.

Why is digital financial security important?

Having your own safe bank account and being able to protect your funds and assets may help you to leave an abusive relationship and regain your financial independence. If you are in an abusive relationship, there are resources and supports to help you plan for your safety and manage your finances before you leave, after you leave and as you reach stability and financial independence.

Recognise and Recover

commbank.com.au/support/recognise-and-recover

Always consider your personal circumstances before acting on financial advice.

What is financial abuse?

Financial abuse (also called economic abuse) is a serious form of domestic violence that occurs when someone uses money as a means to gain power and control over their partner.

Financial abuse is one of the most powerful ways to keep someone trapped in an abusive relationship, and it may also impact on that person's ability to stay safe once the relationship is over.

Financial abuse may continue even once the relationship has ended. Withholding child support payments or refusing to pay for joint debts are both common ways to control an ex-partner.

What is technology-facilitated abuse?

Technology-facilitated abuse is a type of domestic violence where technology is used as a tool by the abuser to gain and maintain power and control over another person. Common forms include sending abusive messages, making threats, having control of all the technology in the household, monitoring activities and devices, or preventing someone from having control of their accounts by demanding access or sharing passwords.

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.*

How do I increase my digital financial security?

For many of us, access to our banking is via our technology/devices. Keeping our devices secure is a crucial step in achieving digital financial security.

To help secure your finances the following may be useful, but trust your instincts about whether these are safe actions for you to take, particularly if you are still with an abuser.

- Having an email account that only you can access and providing a safe mailing address are important steps to keeping bank and other details private. Set up and use your account on a secure device that your abuser cannot access, particularly if monitored.
- If safe, use multi-factor authentication (MFA) to log into systems and services securely. MFA uses two or more identifying factors.
- Use strong passwords that you haven't used before or that your abuser may know or be able to guess, such as your birthday, pets' names, anniversary dates or facts specific to your children. If it is not possible for you to secure your devices and/or accounts, consider using a safer device and different accounts that your abuser either doesn't know about or cannot access.
- Make sure the backup or recovery email and phone details for your accounts belong to you and are ones an abuser cannot easily access.
- If you have shared, or been forced to share, passwords to your accounts - especially iCloud, Google and/or MyGov - consider changing these on a safe device.
- Open a new bank account - you will need ID documents like an Australian driver's licence, a Medicare card, a passport or an Australian birth certificate. Banks are able to support customers to open accounts without standard identification in some instances e.g. you may be able to use a letter from a doctor or refuge, or correspondence from a government authority in order to open an account.
- Make copies of your important documents and store them safely, for example, locked at work, on a hidden USB or with a trusted friend.
- If safe to do so, place a stop or block on your joint accounts, and/or remove the secondary cardholder on your credit cards.

- Review all account security and privacy settings and perform software updates when notified.
- Be careful about what you share on social media and avoid signing into other accounts using your social media, Google or Apple ID.

Abuse using banking platforms

Abuse can happen using digital channels that you might not expect including banking notifications from an abusive partner or via transaction descriptions.

Most banks have procedures in place to respond to inappropriate language or abuse in the free text description fields of electronic transactions. They may be able to block or prohibit messages, or have acceptable use policies to help stop the abuse.

Banks are required in most instances to keep customer's documentation for 7 years, including statements which may contain offensive content. This may be useful to know if you need to obtain or provide documentation of the abuse when reporting to police, for example.

CommBank is taking steps to address the issue of technology-facilitated abuse to provide a safer banking experience for customers. Any customer found to be using NetBank or the CommBank app to engage in unlawful, defamatory, harassing or threatening conduct, promoting or encouraging physical or mental harm or violence against any person may have their transactions refused or access to digital banking services suspended or discontinued.

Resources – Where to get help

WESNET Women's Technology Safety & Privacy Toolkit

techsafety.org.au/resources

National Identity & Cyber Support

idcare.org/

