Beyond Basics: increasing the security of your digital finances

Financial and technology-facilitated abuse are serious types of domestic violence that can increase isolation and impact women's financial wellbeing. For more information, follow the below link to our Women's Financial Wellbeing guide: **commbank.com.au/content/dam/commbank/business/women-in-focus/womens-financial-wellbeing-guide.pdf**.

If you are experiencing domestic violence and you are considering leaving an abusive relationship, things can get complicated and risky, so we recommend seeking support from a professional domestic and family violence support service who can help you make a safety plan that works for your situation. If you are worried your devices are being monitored, make sure to use a safe unmonitored device to reach out to a support service.

You may find it useful to first have a look at our guide on How to secure your digital finances **commbank.com.au/content/dam/commbank-assets/support/docs/how-to-secure-your-digital-finances.pdf**

Technology can be misused in a number of ways to gain access to a victim-survivor's digital finances and use them as a means of control. It is not uncommon for abusers to coerce or force their partner to share their login details and passwords in order to gain access to devices, accounts and apps. Or an abuser may use the personal information they already know to 'impersonate' the victim-survivor to gain access to one kind of account, that perhaps doesn't generally need a high level of security, and then use that as a stepping stone to gain access to more important accounts, including those with important digital financial information.

An abuser can use your personal identifying information to:

- setup or assign themselves as the account holder or administrator for your, or your children's devices, online accounts and apps,
- change the settings in your, or your children's devices, online accounts and apps to allow themselves to access and receive notifications without your knowledge.

If it's safe for you to do so, there are steps you can take to increase your digital financial security. Here are some things to consider:

Syncing linked devices, online accounts and apps

Syncing is a process where changes made on one device, account or app automatically update across all linked devices, online accounts, or apps. Syncing can happen in real-time, or manually, and you may not be aware it is occurring if you are not set up to receive notifications alerting you. Syncing means, the information can be viewed by anyone with access to a linked device, online account or app. In relationship separation, it is often through an abusive person's access to their partner or children's linked devices, online accounts and apps that technology-facilitated abuse can occur.

Children's devices and online accounts

Your children's devices and accounts can be misused to threaten the security and privacy of your own devices and accounts. It's important to check and strengthen security and privacy settings across all devices, accounts, apps and social media accounts that you and your children use, especially if those devices spend time at the abusive person's home. Check the email or app purchases on your child's device that could expose your digital financial information to an unauthorised person. You can check within the device 'Settings' for the presence of apps or subscriptions you may not have downloaded or signed up for, and which family member sharing permissions have been enabled. Some abusers have gained access to private information by obtaining login credentials via the child's online school, banking or tuck-shop account, so it's important to check these too. Consider using totally separate devices in shared custody arrangements if you are concerned about your children's devices being compromised. Be aware of the need to balance security considerations with the potential impact changes may have on your parent/guardian-child relationship.

More advanced security for your (and your children's) devices, online accounts, apps, and social media

- Ensure you are using a device that has not been compromised by an abuser before making changes to any online accounts or apps. If you are unsure, consider using a safe device, for example a trusted friend or at a public library.
- Setup devices and their associated online accounts (like Google, Apple ID and Microsoft) yourself, when you have time, so that you control them and can learn what each privacy and security setting does. For information on how to do this see: **techsafety.org.au/resources/resources-women/newphone/**
- Where possible, ensure you are the primary account holder and administrator on telco, internet, cloud storage and email accounts and that account recovery details are sent to devices and online accounts that only you can access.
- Use the highest security and privacy features available in the settings of your devices, online accounts and apps. Use 2-step verification or multi-factor authentication when available, and consider using an authenticator app or physical security key for additional security.
- Modify device, online account and app notification settings so personal information does not display on the screen when the device is locked.
- Review the privacy and security settings on your device to understand where your information is synced to, and stored (back up), including your device hard drive and SIMs, online accounts, cloud storage, apps and emails.
- If you have to replace your devices, always buy new, still-wrapped devices from a trustworthy supplier and only install apps from reputable online sources i.e. the App Store (iOS) or Google Play store (Android).
- Before connecting a new device, make sure your home Wi-Fi router is secure and use the device data or another safe network if you are uncertain. For information on how to do secure your router see: **techsafety.org.au/resources/resources-women/securing-home-wi-fi/**

Other things to consider - accounts, apps and member cards

- Superannuation, investment, insurance and loan (including student loan) accounts
- MyGov, MyHealth Record, Centrelink, Immigration, Medicare, Tax
- Car registration, licencing, parking, toll and public transport accounts
- Retail rewards or member cards or apps (these are often overlooked, and are less secure and may be easily accessible to an abuser)
- Rental or post-paid accounts (car, furniture, electronics, clothes etc.)
- Food or grocery delivery accounts
- Library accounts, veterinary accounts, donation to charity accounts.

Watch out for the warning signs of technology-facilitated abuse:

These may not sound like things that are related to digital financial security, but they can be warning signs that an abuser may still have access, and therefore be able to access and control you through data and finances.

- Unknown devices appearing as logged into your accounts
- Unknown devices pairing with your device through Bluetooth
- Getting locked out of your email, or having messages or files disappear
- Getting locked out of your accounts or devices
- Your child receiving a new device or having a new online account set up for them by the abuser
- Financial transactions in your account that you cannot recall or reconcile
- Be wary of an abusive person offering to pay for things like mobile phones, cloud storage, anti-virus or other software subscriptions. This may be offered as a gift but may indicate they want to maintain control over your devices or accounts.
- Getting locked out of apps and accounts when 2-step verification or multi-factor authentication codes expire prematurely
- Unknown phone numbers, email addresses or devices that are tethered to your accounts and listed as authorised contacts

Financial and technology-facilitated abuse can be isolating, but you are not alone and it's not your fault. Trust your instincts as you think about your safety and what's right for you, especially before making digital financial changes or documenting abuse. You can find more information about this in our guide Beyond Basics: increasing the security of your digital finances, here: **commbank.com.au/support/next-chapter**

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.*

WESNET
The Women's Services Network

Commonwealth Bank