Data Breach Checklist

A data breach happens when personal information is accessed, disclosed, or lost without your permission. If your data has been breached from an organisation, they have an obligation to inform you.

If you have received a notification that your personal information has been compromised in a data breach, here are some steps you should take immediately.

1 *Speak to your Bank:*

- ❑ Report your Personal details as potentially compromised
- ❑ Request Security Keywords added to your account, along with any additional security measures your Bank may offer
- ❑ Change the password for your Internet Banking
- ❑ Review and report any suspicious or unusual transactions immediately
- ❑ Report any suspicious emails to hoax@stgeorge.com.au or forward texts to 0457 114 629
- ❑ Perform the Security Wellbeing check in the St.George App ensuring you have activated all recommended security features.

2 *Speak to IDCARE*

- ❑ Contact IDCARE - Australia and New Zealand's national identity & cyber support service. IDCARE provides free, confidential support and guidance to people who have been targeted by fraud, scams, identity theft or compromise.
  Visit idcare.org or call 1800 595 160.

If you've been notified of your personal details being compromised as part of a data breach, make sure you understand what information may be impacted and any actions you are required to take to secure your identity.

3 *If Government ID documents have been compromised*

- ❑ Contact the relevant agency who issued your driver licence to report this as lost, stolen or potentially compromised
- ❑ Contact Medicare via medicare.gov.au to report your details or cards as lost, stolen or compromised
- ❑ Refer to the Office of the Australian Information Commissioner (OAIC) for further data breach information oaic.gov.au
- ❑ Inform the credit reporting agencies your personal information has been compromised
- ❑ You can request a copy of your credit report from these credit reporting bodies:
  - Equifax, phone 138 332
  - Experian, phone 1300 783 684
  - illion, phone 1300 734 806
- ❑ Carefully review and ensure you authenticate all 'enquiries' made to your credit history. Contact all companies and organisations that have made enquiries under your name that you did not authorise.

4 *Enhance your Personal Security*

- ❑ Change your passwords on all online accounts straight away, including social media, apps, emails etc. and keep your passwords unique
- ❑ Review any online account security settings. Some online services allow you to view what devices have recently accessed your profile, including any recent transactions
- ❑ If you think someone may have accessed any of your online accounts, report it to the relevant company
- ❑ Alert your family and friends if someone has taken over your social media accounts, your email account or is impersonating you in any way. Tell them to report the account and block any further contact
- ❑ Be sure to confirm any communications from an organisation with an official source. Scammers might try to take advantage of you because of a data breach. For example, you may receive an email asking you to reset your password because it was compromised. Go to the official organisation website or their official app to do this instead of using any links provided in the email.

Data Breach Checklist

Actions you can take to protect your personal information

1 *Check what information is already available on the internet about you and your family*

- ❑ Check the website: haveIbeenpwned.com to see if your email address or phone number has been involved in a data breach
- ❑ Do an internet search of your name to see what information comes up
- ❑ Have a look at your social media privacy settings to ensure they match your intent
- ❑ Limit the personal information you share about yourself on social media (e.g., date of birth, address etc.)
- ❑ Delete any information and apps you no longer use
- ❑ Watch out for targeted phishing attacks from scammers claiming they know you using your public personal information. Once you know what information is publicly available about you, you can protect yourself from potential scams and phishing attempts
- ❑ Always validate all requests for your information (via email, phone, social media, SMS etc.) using a different channel from the request itself.

2 *Passwords are the keys to all your personal information and accounts so make them hard to crack*

Never use the same password on multiple services or websites – especially for your most important accounts, internet banking, email accounts and social media.

- ❑ Create strong, unique passwords for every account, enable Two Factor Authentication (2FA) where available. Never share your passwords and passcodes with anyone, including people you trust
- ❑ When you are out and about, access personal information (e.g. your banking, email accounts and social media) using mobile data rather than a free Wi-Fi network
- ❑ Remember to change default passwords on other connected devices, such as your home Wi-Fi router, Smart TV etc.

3 *Always keep your devices updated and secure*

- ❑ Check and install the latest updates on your devices as soon as these are available as they protect you from the latest threats and vulnerabilities. You can usually do this through 'Settings' on your device. Get anti-virus software to protect you and your devices from malware (malicious software). Learn more about our McAfee anti-virus offer: stgeorge.com.au/mcafee

4 *Final tips to help you stay safe*

- ❑ Back up your important data and photos and store them separately offline on an external hard drive or USB, or secure cloud-based storage. If you are unsure on which storage service is appropriate for your needs, we recommend engaging an IT Professional
- ❑ Review your payment history to make sure you recognise every transaction. You can do this through your Bank or other account statements.

For more helpful information, visit:
stgeorge.com.au/security