st.george

What's next if you've reported an Online scam or fraud case?

This leaflet contains important steps and information to help you navigate our fraud and scam process and stay protected in the future.

My case number

Now that you have alerted our Fraud and Scams team about your recent activity, here's what will happen next.

Step 1: Things we will do.

- We'll attempt to stop any payments where we can intervene.
- We'll attempt to recover your funds by reporting the transactions to other financial institutions.
- We may add extra security to your Internet Banking through keywords or additional security questions.
- We may reset your Internet or Phone Banking with a new password.
- We'll cancel and replace any compromised cards.
- You can locate your Digital Card in the St.George App. For help to access visit ***stgeorge.com.au/digitalcard***
- We'll advise you of our timeframes (which may vary from case to case).
- We'll send you an email or SMS to confirm your case has been created.

Step 2: Things you can do.

- Contact us immediately if you identify further unusual transactions.
- Report any financial loss to the Australian Signals Directorate (ASD) Cyber team at ***cyber.gov.au/report***

IDCARE:

- Engage IDCARE for free, confidential support at ***idcare.org***
- St.George has partnered with IDCARE, Australia and New Zealand's National Identity & Cyber Support Service to provide guidance to people who have been targeted by fraud, scams, identity theft or compromised data.

- IDCARE can help create a tailored response plan for your financial accounts and any other personal details, mobile phone or email accounts, utilities and social media accounts.

Step 3: During the investigation.

- Want an update on your case? Visit ***stgeorge.com.au/scamcase*** or call us on ***1300 301 217.***
- We'll contact you via email on a weekly basis with progress on your case.
- We'll contact the receiving bank, with all attempts made to recover your money, where possible.
- We'll investigate if your activity qualifies for our St.George Secure Guarantee. If you're eligible for a refund, we'll notify you and credit the funds back to the account where your transactions were debited. For more information visit ***stgeorge.com.au/secure***
- If your activity is deemed a scam where we can recover funds from the recipient's bank, it will be processed back to your account.
- Your banking may remain blocked during our investigation if we are concerned that reinstating access would expose you to further loss.

FAQs

Please find below answers to some of our most common customer questions.

1. How did my Internet Banking get compromised?

There are multiple ways your Internet Banking can be compromised.

- Your details are stolen from unsecured mailboxes, by visiting unsafe websites or through phishing websites that mimic St.George or other trusted entities.
- By SMS or email phishing that prompts you to click a link and enter your details.
- By sharing codes you received or access to your computer/mobile. Be cautious of callers claiming that your banking has been compromised and asking for personal information.

2. Will I receive a new customer access number?

No, your customer access number will remain the same. However, you will receive a new password and security number with additional security measures added to your profile.

3. How long will the investigation take?

For standard cases the investigation will take up to 21 days. More complex cases may require additional time. You will receive weekly updates on your case.

4. How can I stop this from happening again?

You can take precautions to protect yourself from fraud and scams by the following:

- Check the email sender's addresses. You can check links received in emails by hovering over the link, which will display the address.
- Be cautious about where you enter your Internet Banking or card details. Never share your customer number, password or Secure Codes with anyone.
- If you're investing in something always use a reputable site and service, do your research and get a second opinion. Investment scammers often create genuine looking websites or pose as knowledgeable experts. If something seems too good to be true, it probably is.
- Regularly explore our Security Centre for frequently updated information on the latest scams or trends. Visit ***stgeorge.com.au/security***
- If you have public social media profiles, ensure there is no information that could be used to guess your passwords and be aware that people may impersonate you with information that's available. Keep your social media profiles private and use second factor authentication where possible.

Where to get more help.

Additional Support Services.

- Scamwatch – create an account via ***scamwatch.gov.au*** and receive your credit report from ***equifax.com.au*** to ensure no false lines of credit have been applied for.
- Accessibility support – If you are deaf and/or find it hard hearing or speaking with people who use a phone, you can reach us through the National Relay Service (NRS). To use the NRS you can register at ***accesshub.gov.au/about-the-nrs***
- Lifeline – Lifeline provides all Australians experiencing a personal crisis with access to 24-hour support and suicide prevention services. Call Lifeline 24-hours on ***13 11 14.***

St.George Bank services.

Criminals constantly look for ways to steal your money and personal information. Remember, St.George will never send you any links requesting your personal or financial information or ask you to share your password or Secure Code, install software to connect to your device or send you a link that directly opens our logon page.

Explore our Security Centre for regularly updated educational resources.

Visit ***stgeorge.com.au/security***

St.George Secure: If your St.George account is compromised due to Internet Banking fraud, we guarantee to repay any missing funds, provided you complied with our Internet Banking Terms and Conditions. This includes keeping your logon details (including passwords, St.George Secure codes) private, not participating in the unauthorised transaction, and immediately notifying us when you suspect an unauthorised transaction or potential fraud on your accounts. This information is general in nature and has been prepared without taking your personal objectives, circumstances and needs and into account. You should consider the appropriateness of the information to your own circumstances and, if necessary, seek appropriate professional advice.