# Phishing: Don’t get caught

### *What is Phishing and how does it happen?*

Phishing is a common way scammers trick you into revealing your personal or banking information (such as passwords, identification details or account numbers) through emails, SMS, phone calls or online content. Often you'll be asked to click on a link, download software or open an attachment, which may lead to fake websites or malicious software.

Scammers often impersonate well-known businesses that you are likely to deal with such as banks, energy companies, telcos (including internet providers), and government agencies. Scams may even replicate marketing material or other collateral these types of companies may send.

---

### *You might have been involved in Phishing if:*

- ❑ You’ve received an unsolicited email, SMS, phone call or social media message, asking you to click a link or provide personal information
- ❑ You’re asked to complete steps or answer questions to prove your identity
- ❑ The requestor claims to be from law enforcement, the government, a bank, telco, well known organisation or internet provider
- ❑ You’re asked to provide banking details, transfer money or make a payment via an unusual method e.g. crypto currency
- ❑ You’ve received a deposit to your account and asked to return part or all of the amount
- ❑ You’re asked to provide remote access, or download software or apps, to your computer or device., e.g. AnyDesk, TeamViewer etc.
- ❑ The branding, spelling, grammar (or simply something about the request) doesn’t feel quite right
- ❑ You’re threatened, pressured, or asked to complete something in secret.

### *Take action now if you’ve:*

- Clicked on a suspicious link OR replied to a suspect email, SMS or social media message AND/OR;
- Shared/entered banking or personal information

- ❑ Report your personal information as potentially compromised to St.George or your Bank
- ❑ Review and report any suspicious or unusual transactions immediately. Confirm recent payments were paid to the intended account
- ❑ Request Security Keyword/questions be added to your account, along with any additional security measures your Bank may offer
- ❑ Change the password for your Internet Banking, using a different device. Ensure you're registered to receive Secure Codes
- ❑ Run an anti-virus check on your computer, laptop or mobile device
- ❑ If you think you have fallen for a scam, report it to the police via cyber.gov.au/report

# Phishing: Don’t get caught

*If you had a conversation that requested you do any of the following:*

- Provide your personal information
- Complete a task at their request
- Provide financial information or transfer money to another account, e.g. to keep it safe or provide the bank an alternate reason for the purpose of the funds
- Download software that allowed someone to access your laptop or mobile device.

*Stop! Take these actions as soon as possible:*

- ❑ Turn off the device you shared remote access to
- ❑ Speak to St.George or your Bank
- ❑ Report your personal information as potentially compromised
- ❑ Review and report any suspicious or unusual transactions immediately
- ❑ Change the password on your Internet Banking, on a different device
- ❑ Ensure you are registered for Secure Codes to receive One Time Passcodes
- ❑ Before accessing your banking on this device, ensure it has been cleaned by an IT professional
- ❑ Request Security Keywords be added to your account, along with any additional security measures your Bank may offer.

*If you didn’t provide personal information*

- ❑ Forward any suspicious emails posing as St.George to hoax@stgeorge.com.au or messages to 0457 114 629 then delete them from your device/email account
- ❑ Report all suspicious activity to the Australian Cyber Security Centre at cyber.gov.au/report
- ❑ Report the scam to the ACCC Scamwatch website at scamwatch.gov.au/report-a-scam
- ❑ Run your devices anti-virus or anti-malware software, to ensure that your device is not infected with malware
- ❑ Consider updating your passwords for your banking, email or social accounts – it’s best to be security cautious
- ❑ Keep up to date on your bank’s scam information, visit ours at stgeorge.com.au/scams
- ❑ If you have received a message from a suspected scammer on social media or other platforms/apps, you should report the activity through the relevant party, and block the profile.

*Protect your personal Information*

- ❑ 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 think someone may have accessed your online accounts, report it to the relevant company
- ❑ Change your passwords on all other online accounts immediately, including your social media account, apps, emails etc. preferably using a different device
- ❑ Report suspicious emails to the relevant company
- ❑ Alert your family and friends if someone has taken over your social media accounts, your email address or is impersonating you. Tell them to report the account and block any further contact.

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