st.george

Be safe and secure

Learn how to look out for scams and fraud.

What's included?

01

Protecting yourself online

Every year, more and more people fall victim to scammers' tricks. So how do you reduce your risk? Start by arming yourself with the right information.

To help protect your personal and financial information, it pays to be aware of the tools you have at your fingertips.

Read on to find out how to improve your online security and be sure to share what you learn with your family and friends.

Staying secure when browsing online

Keeping your computer protected

- Install anti-virus software, turn on automatic updates and scan your computer regularly.
- Ensure your operating system and browsers are up to date and have the latest security enhancements installed.
- Password protect your computer's log in, especially if you use browser password managers.
- Avoid saving your credit card details in your browser.
- Research software before downloading it on to your computer. A quick search (e.g. Google), could save you and your family a lot of grief.

It's important to protect all your devices (such as smart phones and tablets) from viruses, malware, and internet fraud. Check out the 'Protecting your mobile' section of this guide to learn more.

Keeping your banking and identity safe

- Get an extra layer of protection by generating a one-time-password with a St.George Secure Code. Don't share that code with anyone (not even friends or family), because it's one of the ways we verify you are genuinely performing the activity.
- Create unique passwords and change them regularly (try setting a calendar reminder for each time). Avoid using the same passwords for social media, email accounts and your banking.
- Never give out your personal or security details (like your Card or Customer access number, passwords or security codes) in response to an email or SMS, even if it looks legitimate.
- Review your payee list regularly, and call us immediately on **13 33 30** (8am – 8pm AEST Monday - Saturday) if you don't recognise a payee.
- Check your accounts regularly for any suspicious transactions. Contact us immediately on **13 33 30** (8am – 8pm AEST Monday - Saturday) if you find anything unusual.
- Don't simply throw old bills, letters or documents containing personal information in the bin, instead, dispose of them thoughtfully by shredding them.
- Secure your mailbox or PO Box with a padlock and make sure you report any missing mail to the relevant senders.
- Avoid using shared computers or devices. They may have malware that could compromise the security of your online activity.
- Be careful about the information you share online and on social media. Think before you post photos, personal information and financial information (whether it's about yourself, your friends or your family). Check your privacy settings regularly and register for two factor authentication to help make your social media and email accounts more secure.

Staying a step ahead of scammers

This starts by being aware. Use caution when receiving phone calls, emails, or texts claiming to be from a reputable organisation and consider what they're asking for.

Ask yourself:

- Does this sound right?
- Would someone really ask me to do this?

Also make sure you:

- **Never** give an unsolicited caller access to your computer (via 'remote access') or download software at their request. Remote access software allows a user to access and control your PC and see any information visible on your screen or stored on your computer. If you need to remotely share your desktop (such as for work), never logon to Internet Banking.
- Use caution when opening emails as links or attachments may infect your computer with malware. Delete any suspicious emails right away. Also, don't open suspicious text messages or pop-up windows. To stay in the loop about scams targeting St.George customers, visit our **latest scams page**.
- Never click on a link in an email or text message that asks you to logon, update, or validate any details. Instead, type the site address manually into your web browser or visit the genuine mobile app, then logon and follow up on any requested actions.
- Register for **Australian Cyber Security Centre Alert Service** or **Scamwatch Radar** alerts. These are free Government initiatives that alert you to new online threats as they're identified.

We want you to have the knowledge and confidence to have great online experiences. That's why we're working closely with a range of government and community partners to raise online safety and privacy awareness. To stay up to date with what we're doing, visit our St.George Security Centre at **stgeorge.com.au/security**.

02

Protecting your mobile

Think about how much confidential and personal information you may be carrying around on your devices.

From card details to email passwords to contact lists. All of this represents valuable data that fraudsters can target, be it through phishing emails, text messages or malware.

Mobiles are also easy to misplace, making them easy targets for thieves. And with mobile malware on the rise, it's becoming vital that you know how to protect your mobile devices.

Securing your mobile devices

The St.George Mobile Banking App gives your mobile devices the same high level of security that Internet Banking gives your computer.

How to make your mobile even more secure

For a more secure device, keep your Mobile Banking apps up to date, and make sure you provide the St.George App with the requested security permissions.

Want to know more about the permissions we ask you for?

- If you have an Android device, **click here**.
- iPhone users, **click here**.

Your security guarantee.

Don't forget – when using mobile banking, you're still covered by our St.George Secure security guarantee. That means we'll refund your money if your account is compromised due to internet fraud, as long as you comply with our Internet Banking Terms and Conditions. This includes keeping your access codes and passwords private.

Mobile security tips

- **Regularly update your device and its apps.**
  By always keeping your operating systems and apps up to date, you'll ensure your device has the latest security features. Try setting them to automatically update to make this easy.
- **Back up your mobile devices regularly.**
  Keep your valuable messages, contacts, calendar appointments, videos, photos, and documents safe by backing up to a PC or a cloud-based solution so you can restore them to your device if something happens.
- **Auto-lock all mobile devices with a strong passcode.**
  Make sure all your devices have auto-lock activated and have a strong passcode. A simple pattern or swipe passcode isn't much of a deterrent. Features like fingerprint scanning and facial recognition also increase your security significantly.
- **Only download apps from trusted sources.**
  Malicious software (malware) can be installed when downloading apps or software from untrusted sources, enabling fraudsters to take control of your device and launch attacks against you, or people you may be connected with. Only download apps from sources you trust, like the App Store or Google Play store, and always check reviews and ratings before downloading.

- **Be careful connecting to public WiFi – it's not always secure.**
  Free public WiFi may be convenient but it may expose your device to risks like eavesdropping or malicious content. If you have to connect to WiFi, avoid logging into any accounts that contain personal or sensitive information such as your banking, email, and social media. Be careful when using the automatic WiFi connection feature on your devices.
- **Don't pair or accept files from unknown Bluetooth devices.**
  Bluetooth is used to share information between devices, for example text messages on wearables like smart watches. We strongly recommend you avoid pairing with unknown devices and decline any unexpected file transfer requests when you don't know the source.
- **Know the risks of jailbreaking/rooting.**
  Manufacturers place security restrictions and safeguards on devices to protect your devices and data. Jailbreaking, also known as rooting, removes these safety controls, leaving the system more vulnerable to malware and other threats.
- **Be wary of unsolicited calls or messages.**
  Scammers use a variety of methods to get users to download malware or reveal their personal information, including calls and text messages. Use a security scan from a security provider like McAfee. Verify any messages, calls, or emails from unknown senders before opening.
- **Remove apps correctly.**
  We often give our name, email address and other personal information when signing up to apps. When removing an app from your device, make sure you also unregister your account.
- **Sign out of apps containing sensitive information.**
  Instead of closing an app, browser window, or laptop screen, make sure you use the app or website's logout feature. That way, your information will be safer if your device is stolen or compromised.
- **Limit the personal information you share with apps and websites.**
  Be wary of revealing too much when signing up for a new app or service. Always do research on how secure the application or site is before logging on. It's also a good idea to review your privacy settings as new updates can impact your existing choices.

Think your security has been compromised?

Contact us immediately on **13 33 30** (8am – 8pm AEST Monday - Saturday).
You may need to reset your mobile device to factory defaults.

03

Protecting your card details

Anyone who has access to your PIN, Internet or Phone Banking passwords or access codes, other personal and financial information could access your accounts.

That's why it's so important that you treat this information as confidential and make sure your details never fall into the wrong hands.

Keeping your card secure

Card security tips

- Never share your PIN; not even with friends or family. The bank will never ask you for this information.
- Make sure your home, work and mobile phone numbers, along with your email addresses, plus any other contact details are up to date.
- If you're travelling overseas, let us know where and when, and whether you intend to use your card. That way, we'll know whether to alert you if an overseas transaction occurs and looks suspicious. You can do this in branch through Internet Banking or the mobile app. Find out more **here**.
- Take a backup card when travelling, just in case your card is lost or stolen. Travelling usually puts you at more risk of fraud, as you're in unfamiliar territory.
- Be particularly careful with your card when visiting countries that could have pickpockets. Your bags and pockets aren't always as safe as you'd think.
- Always report lost and stolen cards immediately by calling us, visiting a branch or through online banking.
- Destroy expired or unwanted cards by cutting through the signature panel and magnetic strip.
- Keep a list of your card numbers somewhere secure. It will be helpful if you need to report lost or stolen cards.
- Treat your card like it's cash. Always know where your cards are and never leave them unattended in places like your car, workplace or behind a bar. Don't give or lend your card to anyone and be present for all transactions.
- Be suspicious of anyone who phones and seeks personal information or bank details without properly identifying themselves. It is always best to verify these requests by contacting the company directly on a number you have independently sourced.
- Never write your PIN down and make sure it's a number that can't be found in your wallet, such as a date of birth or the last four digits of your phone number.
- Check your account for unrecognised transactions on a regular basis.

04

Protecting your business

There's more to improving the online security of your business than you might realise.

These tips can help you and your employees keep your business safe online.

Keep your business secure

Keeping your business' data safe

- Keep all your systems, applications, software, and Point-of-Sale (PoS) systems up to date with the latest upgrades.
- Back up your systems and critical data regularly, and store that data in a secure location. This includes using a cloud-based solution or removing hard drives from your network once a backup is complete.
- Put in place a cyber security strategy to counter ever-evolving cyber threats (for example, have a remote access protocol for employees working from home, and set up firewall rules).
- Use two-factor authentication wherever you can.

For more information, read the **Australian Cyber Security Centre (ACSC) guide for small businesses**.

Preventative measures

- Enhance your security with Trusteer Rapport™. Trusteer adds an additional layer of protection against potential online identity theft and fraudulent transactions. For more information, visit **stgeorge.com.au/trusteer**
- Ensure your anti-virus and other security software is up to date, and double check the level of protection suits the needs of your business.
- Get an extra layer of protection by generating a one-time-password with a St.George Secure Code.
- If using St.George Business Banking Online (BBO), make sure all users have correctly applied to access your banking. If you don't already have multiple signatories set up, talk to your local banking representative or review your payment settings online.
- Review your payees regularly and call us immediately on **13 33 30** (8am – 8pm AEST Monday - Saturday) if you don't recognise something, or someone, on your list.
- Regularly check your accounts for any suspicious transactions. Contact us immediately on **13 33 30** (8am – 8pm AEST Monday - Saturday) if you detect anything unusual.

Staying ahead of scams

- Educate your staff so they know how to recognise scams. Make sure they understand it's ok to question anything they consider suspicious, and give them an official, easy-to-follow reporting process.
- Verbally validate every email or SMS request that involves sensitive information, urgent payments, or change of account details, on a phone number you trust. Never use the contact details provided in the message. This can save your business from financial harm.
- Beware of impersonators – criminals can trick you into fulfilling their requests by posing as well-known organisations, suppliers, or even employees in your own company. Common impersonations include ASIC, the ATO, telco, internet, energy or utility companies.
- Recommend your staff register for **Australian Cyber Security Centre Alert Service** or **Scamwatch Radar Alerts**. These are free Government initiatives that alert of new online threats as they are identified.

st.george

We're here if you need us

stgeorge.com.au/security

13 33 30 8am – 8pm AEST Monday - Saturday

Visit your nearest branch

STG90041 0521