Australian Banking Association

Keep yourself safe:
be aware of scams and fraud

COVID-19 themed scams and fraud are likely to increase over the coming months.

Scammers use fake emails, phone calls or text messages to try and obtain personal information. They pretend to be from your bank, the World Health Organization, government, charities or legitimate businesses like travel agents, electricity, phone or internet providers, or your local supermarket.

Protect Yourself

Your bank will NEVER send an email or text message asking for any account or financial details, this includes updating your address or log in details for Phone, Mobile or Internet Banking.

Government and other legitimate organisations will NEVER ask you to update details by clicking a link. If in doubt, talk to a friend or family member, or contact the organisation directly and ask.

If you receive a phone call from someone you don't know asking for personal information, HANG UP. Call the company directly and check if they called.

NEVER open attachments from people or organisations you don't know. Always be wary of offers that sound too good to be true or ask for too much information.

Your bank can help, contact them immediately if:

- you shared your banking details in response to a hoax phone call, email or text
- you accidentally clicked on any links or downloaded any attachments
- you noticed any unusual transactions on your accounts.

How to spot a scam

- You're asked to update or confirm personal details, including address, date of birth, bank account details, tax file number or any PIN or password.
- The email or text message contains links that look suspicious. If you're not sure, ask a friend or family member for help.
- You are asked for immediate payment or an up-front deposit.
- If the offer sounds too good to be true, it probably is.
- The email address doesn't match the company.
- The caller asks to remotely access your computer.

Australian Banking Association

www.ausbanking.org.au

Top tips to protect your financial information from scams and fraud

- Hang up on suspicious phone calls, instead go to the company's website or find their number and ring them directly.
- Never share passwords or PINs. Password-protect your devices. If you are using a shared computer, never save passwords and always log out of your account.
- Regularly check your bank accounts so that you notice suspicious transactions quickly.
- Avoid swiping your card to make purchases. Tapping and inserting are often more secure.
- Block cash advances on credit cards.
- Talk to your bank about the best way to protect your account.
- If you think you have been scammed report it to your bank immediately.

There are many ways that crooks will try to steal from you, here are the main ones.

Phishing – An email or text is used to obtain your personal information by pretending to be from a trustworthy source like a bank, a charity, or government. The message looks real and will often ask you to enter personal information on fake websites or ask you to click a link – this will allow the crook access to your computer and your personal information.

Online shopping scams – scammers pretend to be real online shops, either with a fake website or a fake ad on a genuine retail site. Fake online shopping sites will often request unusual payment methods such as upfront payment via money order, wire transfer, international funds transfer or gift cards.

Investment scams – scammer claims to be a stockbroker or portfolio manager offering financial or investment advice. They will ask you to hand over money for an investment opportunity that may, or may not, be real, they then keep your money.

Remote access scams – scammer will claim there is something wrong with your computer or internet connection, or that it has become infected with malware. They will try to convince you to install an application or give them access to your computer. They will use this to access your personal information or demand a 'fee' for fixing the problem.

Relationship and dating scams – scammer forms a relationship with you to extract money or gifts. They develop the relationship over time and may ask you to transfer assets into their name or ask to become a beneficiary of your will. Often, they will ask for money to fix a health, travel or family problem.

USEFUL LINKS:

www.ausbanking.org.au/safe-savvy-a-guide-to-help-older-people-avoid-abuse-scams-and-fraud

www.esafety.gov.au/seniors/staying-safer-online

www.scamwatch.gov.au/