Protecting yourself from scams.

Be aware of scams to help keep yourself and your money safe.
If you think something seems too good to be true, then it probably is.

Common Scams

Computer and mobile device scams

Example: You receive a phone call or email advising that your device is infected by a virus. They will sell you anti-virus protection however the software tracks your device and gives access to your passwords, social media, email and your banking.

Gift card scams

Example: Some scammers will ask you for a payment using gift cards, making it hard to trace if you end up reporting the scam later.

Dating and romance scams

Example: Scammers build a relationship with a vulnerable (or any) person and eventually request financial help or a gift.

Remote access scams

Example: They ask you to provide them with remote access to your device in order to help you detect the virus, catch the hacker or fix the 'problem' they claim you have.

Family member SMS scams

Example: These messages appear to be targeting parents and purporting to be their children or other family members. Scammers will use a different phone number and ask for money.

Investment scams

Example: A risk-free investment with a guaranteed return. For example, invest $100,000 and receive a $300,000 return.

Phishing scams

Example: They impersonate a government agency, business or your bank via email, phone or text message. The attention to detail is normally poor and you should be able to see some errors in language, grammar or the email address.

Impersonation scams

Example: Phone calls or emails pretending to be from your bank saying that your account has been compromised and they can help you. Scammers may ask you to provide your passwords, codes sent via SMS or email, or to transfer funds to another account.

Inheritance scams

Example: You are told that you have an inheritance from a relative (generally overseas) but to access the inheritance you must send a sum of money.

Online shopping scams

Example: Scammers pretend to be online shops, either with a fake website or a fake ad on a genuine retail site. They often request unusual payment methods such as upfront payment via money order, wire transfer, international funds transfer or gift cards.

If you are not expecting a phone call, email or text message, do not provide any personal information.

Do not call the number provided or click on any links. Find your institution's phone number or website and contact them directly to verify.

How might scammers contact you?

Phone calls
Unexpected phone calls from individuals claiming to be from your bank, insurance or utility company. They may ask for personal information.

Text messages
A text message asking you to click on a link or sign up to win or verify something.

Emails
Links in emails normally impersonating someone else.

Beyond Bank Australia Limited ABN 15 087 651 143
AFSL/Australian Credit Licence 237856.

Beyond Bank AUSTRALIA

How to protect yourself?

Check your bank accounts – Check your bank accounts regularly so that you notice any suspicious transactions quickly.

Be alert that scams exist – If you receive uninvited contact from people, a business or financial institution via phone, email, text message or social media – consider that it may be an impersonation scam. You should call the relevant party back on the phone number listed on their website to validate the call. Please note, banks will never contact you asking you to provide personal information, passwords or passcodes, or to transfer funds to another account.

Know who you are dealing with – If you meet someone online or are unsure if it is legitimate contact from a business, then take some time to research it first. If it is someone purporting as a family member or friend, double check their usual number to confirm it's them and think before you reply.

Keep your personal details personal – Place a lock on your letter box, shred any documents that have personal information and keep important documents secure. Be careful what you share on social media.

Passwords are only for you – Never share your passwords or pin numbers. Make sure that you change your passwords regularly and maintain good password security (use a combination of numbers, capitals, lowercases and symbols).

Keep your phone and computer secure – Make sure you protect your phone and computer with a password, use security and anti-virus software and back up your content. Avoid using public WiFi to access banking and personal information.

How can I get help?

If you think you have been scammed, start by calling us on **13 25 85** or visiting your local branch. You will also find a list of organisations that may be able to assist you on our website. Visit **beyondbank.com.au/scamaware**

You can contact these organisations if you need more help:

Type of scam	How to contact
Fraud and theft	**Your local police** 131 444
Financial and investment scams	**ASIC** asic.gov.au
Centrelink, Medicare, Child support and myGov	**Services Australia – Scams and Identity Theft Helpdesk** 1800 941 126
Cybercrime	**Australian Cyber Security Centre** cyber.gov.au/report
Spam	**Australian Communication and Media Authority** www.acma.gov.au
Tax related scams	**Australian Taxation Office** www.ato.gov.au

Any scam can be reported online to scamwatch at scamwatch.gov.au

Beyond Bank Australia Limited ABN 15 087 651 143
AFSL/Australian Credit Licence 237856.

MS189B251122

Beyond Bank AUSTRALIA