Banking safely online.

Bendigo Bank

Banking safely online.

Why online banking?	**3**
What we're doing to help keep you safe	**4**
Bendigo Bank and biometrics	**5**
Essential tips for safe online banking	**6**
Common scams and how to identify them	**8**

Why online banking?

Online banking is like traditional banking, just done on the internet.

It's safe, easy to use, and is available 24 hours a day, 7 days a week.

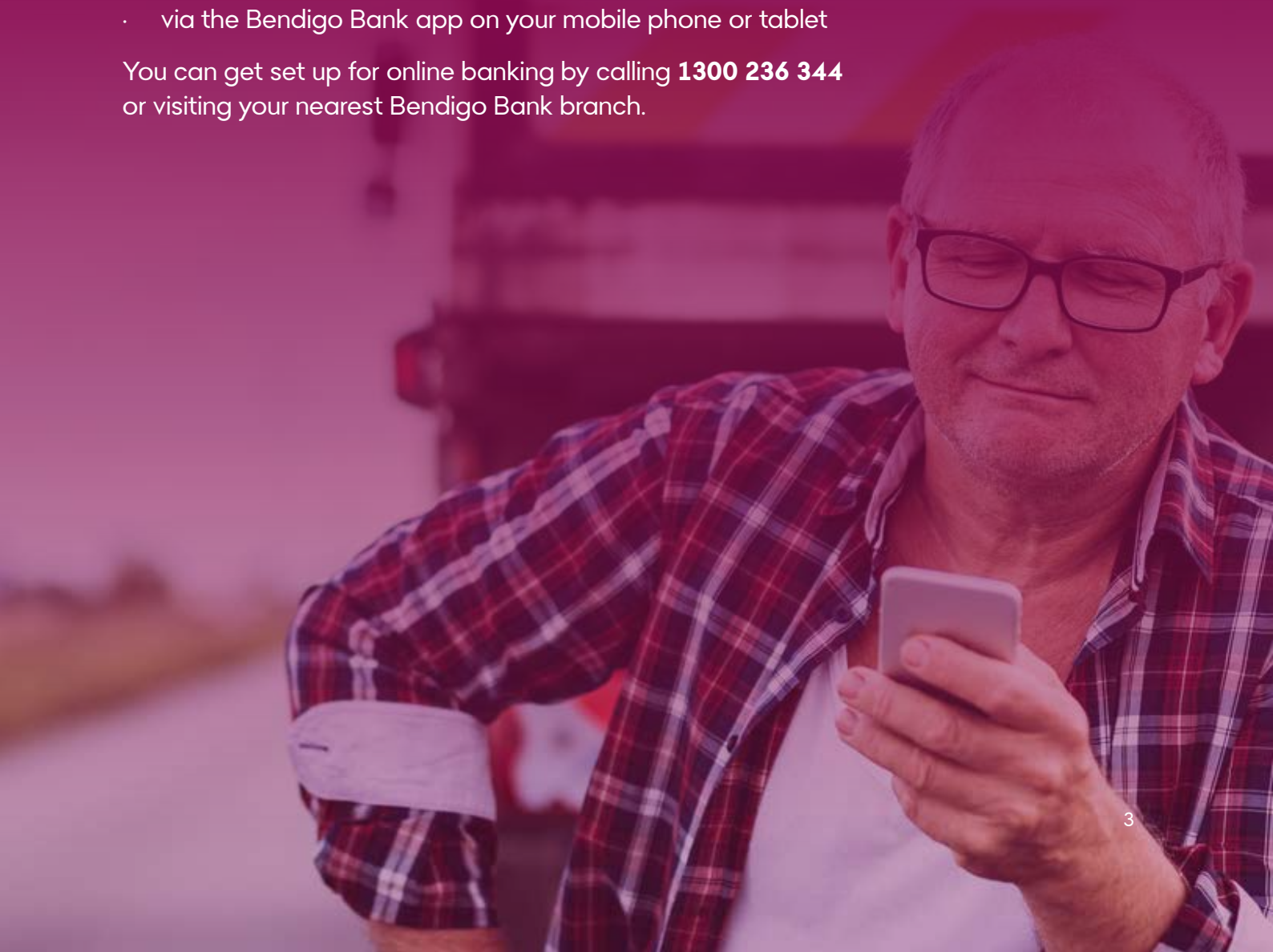
You can do all your banking online, including:

- check account balances
- transfer money
- pay bills
- open select accounts
- view statements, and much more

You can access online banking 2 ways:

- e-banking on Bendigo Bank's website
- via the Bendigo Bank app on your mobile phone or tablet

You can get set up for online banking by calling **1300 236 344** or visiting your nearest Bendigo Bank branch.



What we're doing to help keep you safe.

Helping you stay safe online is important to us. Here's what we're doing to help protect you and your banking:

Multi-factor authentication (MFA)

MFA increases your security by requiring two or more identity verifications to significantly reduce the risk of unauthorised access to your account. MFA can use either your face or fingerprint for verification. These pieces of identification are called biometrics. See page 5 for more information on how to set this up.

Automatic Logout Functionality

Our online banking platforms will automatically log you out when there is inactivity for a period of time. This reduces the risk that someone other than you will get access to your banking.

Dedicated Security Team

We have a specialised security team who are always monitoring our systems for any sign of suspicious activity. This ensures we are proactive in our defense against potential threats.

Automated Alerts and Account Locking

When we detect abnormal or unusual activity, our systems trigger automatic alerts. Inactive accounts are immediately locked as an additional safety measure.

Bendigo Bank is continuously leveraging new technologies so we can help you stay safe when you bank online.

Bendigo Bank and biometrics.

Biometrics is a safe, reliable and convenient way to verify your identity and protect you online.

Biometrics is the bank's way of 'double-checking' it's really you before we grant access to your banking and personal information. Unlike passwords, biometric access can't be duplicated or stolen.

Some examples of biometrics include:

Fingerprint

These are the swirls and lines on your fingertips, which form a unique pattern that only identifies you.

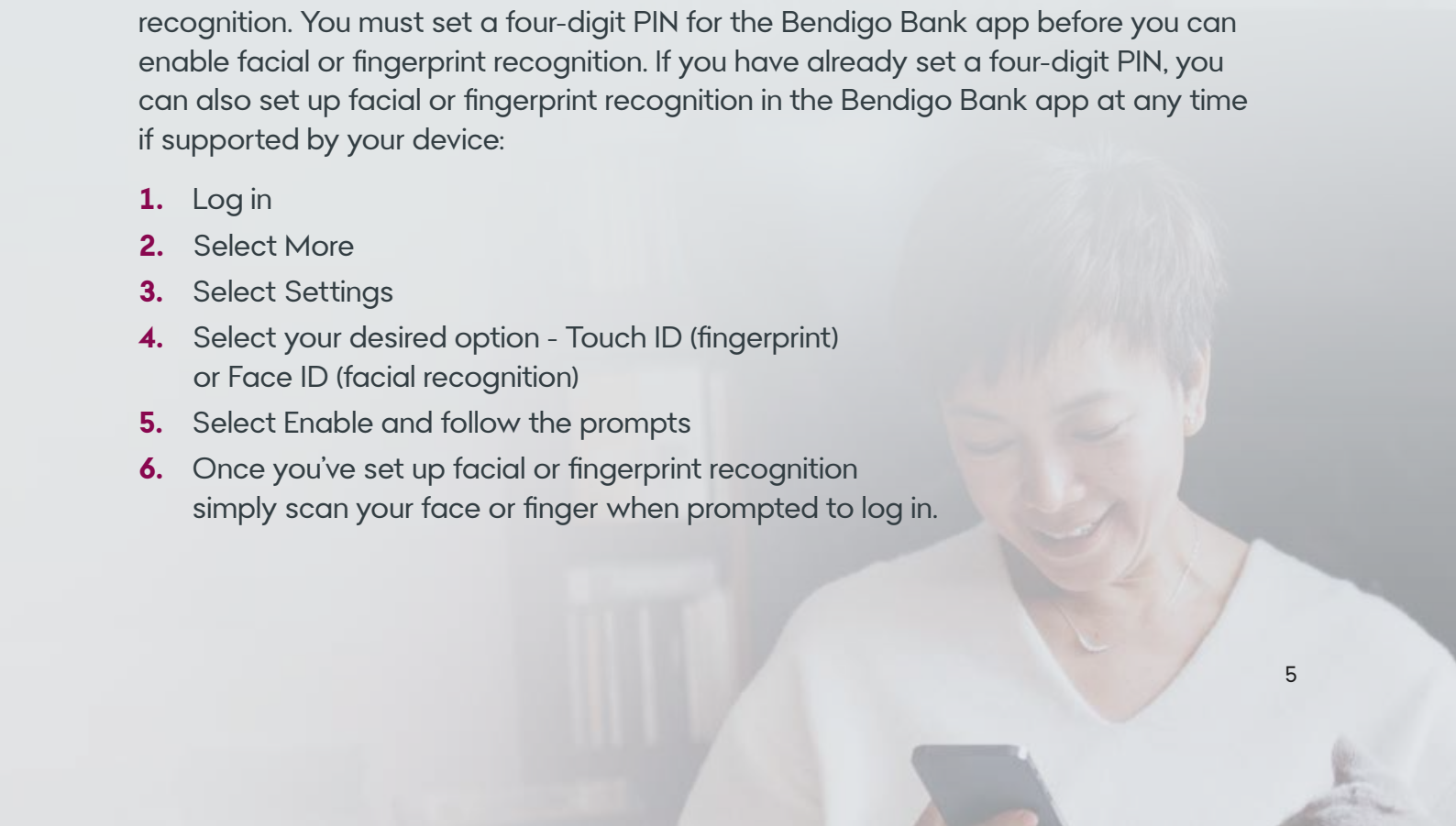
Facial recognition

Facial recognition uses the camera on your phone or tablet to capture an image of your face. It then creates a digital pattern and matches it with your identity, recognising aspects like the distance between your eyes, the position of your nose, and the size of your forehead.

Setting up your biometrics:

When installing the Bendigo Bank app on your mobile or tablet for the first time, you will be given the option to set a four-digit PIN and then enable facial or fingerprint recognition. You must set a four-digit PIN for the Bendigo Bank app before you can enable facial or fingerprint recognition. If you have already set a four-digit PIN, you can also set up facial or fingerprint recognition in the Bendigo Bank app at any time if supported by your device:

1. Log in
2. Select More
3. Select Settings
4. Select your desired option - Touch ID (fingerprint) or Face ID (facial recognition)
5. Select Enable and follow the prompts
6. Once you've set up facial or fingerprint recognition simply scan your face or finger when prompted to log in.



Essential tips for safe online banking.

At Bendigo Bank we try to do all we can to help you stay safe when banking online. Here are some simple ways you can protect yourself:

Choose strong and unique passwords

Creating a strong and unique password is important for keeping your account secure. This means selecting something that isn't obvious or easy to guess - like your birthday or name - and using a mixture of lower and uppercase letters, numbers, and special characters like '!' and "#'.

Keep your account information private

Never give anyone your PIN, password, or 6-digit e-banking security code. Bendigo Bank will never call, text or email you asking for account details, usernames or passwords.

Update your password regularly

To keep your account safe, you should update your password every 3 to 6 months. You can do this anytime with online banking.

Here's some simple steps to changing your password online:

1. Select 'Settings' from the menu options (in the app it's under 'More').

2. Select 'Change Password'.

3. Follow the prompts to change your password.

If you have any concerns or questions regarding your account security, don't hesitate to reach out to us directly. Your security is our priority.

Enable multifactor authentication

Multi-factor authentication or MFA is an extra layer of security when logging in online. This can include facial or fingerprint recognition, or a code sent to your registered email address. For more information on MFA and how to set it up, see pages 4 and 5 of this brochure.

Be careful when using public Wi-Fi

When using public Wi-Fi, make sure the network you're using is trustworthy before logging on to online banking. Examples of trusted public Wi-Fi connections include an airport, supermarket, or well-known restaurant chain.

Using your mobile service provider's 4G or 5G connection on your mobile phone or tablet while you're out is safe, and not considered public Wi-Fi.

Check notifications

Always pay attention to banking alerts and notifications; do not ignore them. These alerts instantly notify you of online activity that requires your approval or rejection of specific activities.

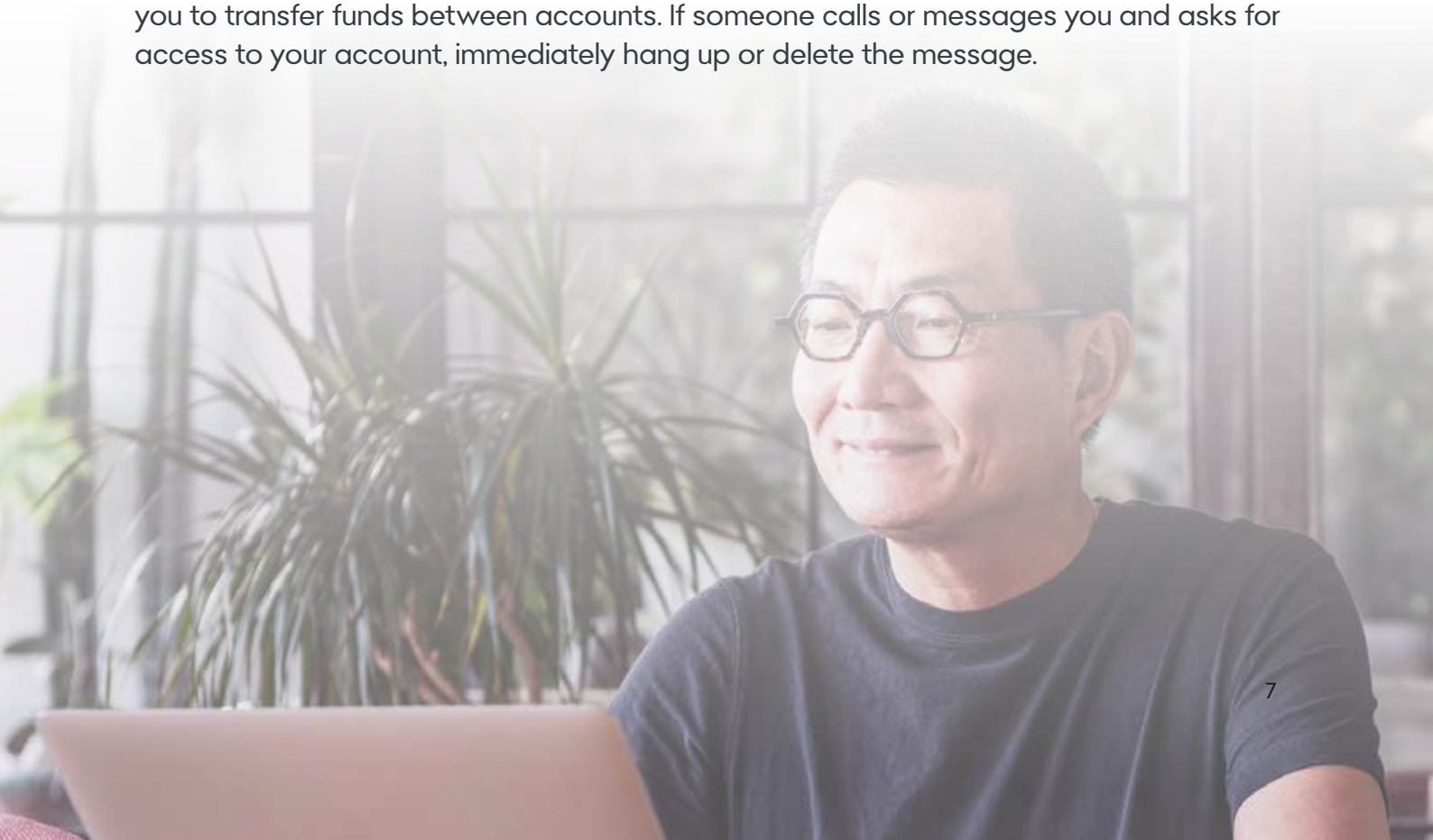
Report phishing scams

Phishing is when someone (a scammer) asks for your banking information or to access your account. They usually do this by email or a phone call, pretending to be a trusted person or business.

If this happens to you, make sure you report it and change your password immediately. Never click on a link or SMS (text message) from someone you don't know or trust.

Stay safe from scams

Bendigo Bank will never ask for remote access to login to your online banking account/s. We will never ask for your PIN, password, or 6-digit security code, and we will never ask you to transfer funds between accounts. If someone calls or messages you and asks for access to your account, immediately hang up or delete the message.



Common scams and how to identify them.

Suspicious Text Messages

Suspicious text messages may urgently request money transfers. You should always verify the sender's identity by calling them on a trusted number before sending money, even if they claim to be a family member. Sometimes, a text message can appear to be from Bendigo Bank, and will prompt you to click on a link. However, we will never send you text messages of this nature, so if you ever receive one, delete it.

Remote Access Scam

A remote access scam occurs when a scammer contacts you via phone, text, or email, claiming to represent a familiar company like your bank, utility provider, or government agency. They may persuade you to install software on your device to gain access to your personal information. If you find yourself in a situation where you think you could be communicating with a scammer, hang up the phone or stop responding and get in touch with the company they're claiming to be from on a trusted number.

Business Email Compromise

Scammers exploit businesses during busy periods, like the end of the financial year. This could involve false billing scams where scammers issue fake invoices for unwanted products or services. If you do not recognise the company, service, or product on the invoice, do not respond or make any kind of payment. Likewise, even if you do recognise the company, make sure you double check the account information is correct before you make payment.

Investment Scam

These scams masquerade as offers to invest in cryptocurrency, business ventures, superannuation schemes, managed funds, shares, or properties. They may create professional brochures, websites, and advertisements to trick people into participating. Stay vigilant and always verify the business by requesting official documentation prior to making any kind of payment.

Romance Scam

Dating and romance scammers create fake profiles on dating websites and social media platforms, often using stolen images. They establish online relationships to extract money from victims. Never send money to anyone you meet online, even if they seem reputable and/or you have met them in person.

Online Shopping Scam

Scammers can create convincing fake websites to lure customers into making purchases. Watch out for unusual payment methods such as wire transfers or prepaid cards, as legitimate online retailers typically use secure payment methods such as virtual cards, digital wallets or PayPal. If you're ever unsure if someone is genuinely from Bendigo Bank, visit **bendigobank.com.au/reportit** for more information.

Cold Calling

Scammers call customers, claiming to have previous knowledge of them. They fabricate information and convincingly impersonate bank fraud or security team members to trick people. If you're ever unsure who you're speaking to, hang up and call the bank back on a trusted number. Bendigo Bank's main customer support number is **1300 236 344**.

Find out more about staying safe online.

To find out more about staying safe when banking online:

- visit your nearest Bendigo Bank branch
- call **1300 236 344**
- search **bendigobank.com.au/security**

Bendigo Bank