Digital Education

Bendigo Rotary Club

Bendigo and Adelaide Bank

Meg Parker
Digital Coach, Bendigo Region

Claire Collinge
Digital Adoption Lead

Kendall Beattie
Regional Manager, Bendigo Region

Welcome

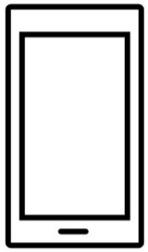
It’s great to be here!

Helping our customers & communities to bridge “the digital divide”

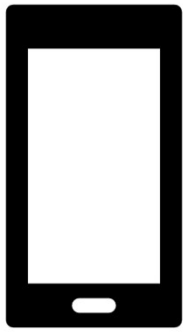
The benefits of banking digitally

How to manage your risk in the digital world

Hands up who has one of these….



Smartphone

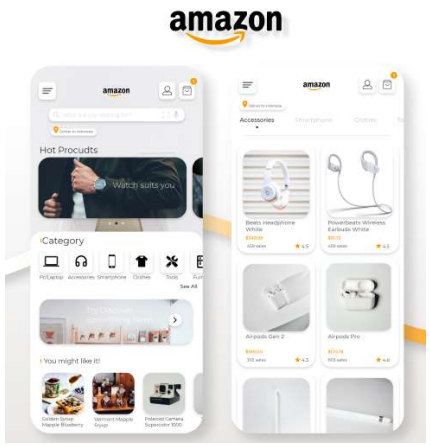


iPad / Tablet

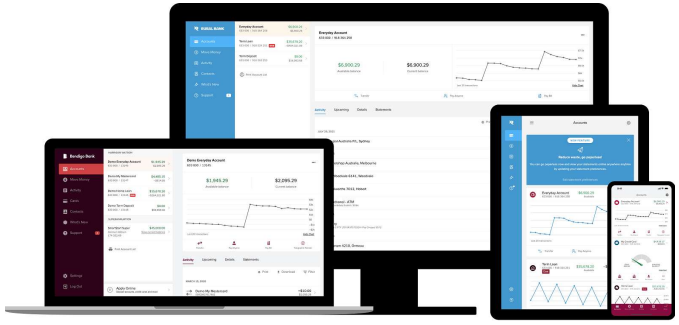
Computer / laptop

Hands up who uses their devices for….

Keeping in touch with friends on social media?



Online shopping?



Online banking?

What is the digital divide?

There are three main factors to the digital divide:

- Access
- Affordability
- Ability

1 in 4 Australians digitally excluded
(ADII 2021)

Source: The Good Things Foundation

44% People with low education have no media literacy
(Dezuanni & Notley, 2021)

1 in 3 low-income families with school-aged children are mobile only users
(ADII 2021)

80% of people aged over 65 years find it difficult to keep up with tech changes
(ACMA, 2021)

New migrants & refugees: Low digital skills and access are barriers to services
(SCoA & GTF 2021)

Digital inclusion supports social inclusion
(Be Connected Evaluation 2020)

Source: The Good Things Foundation

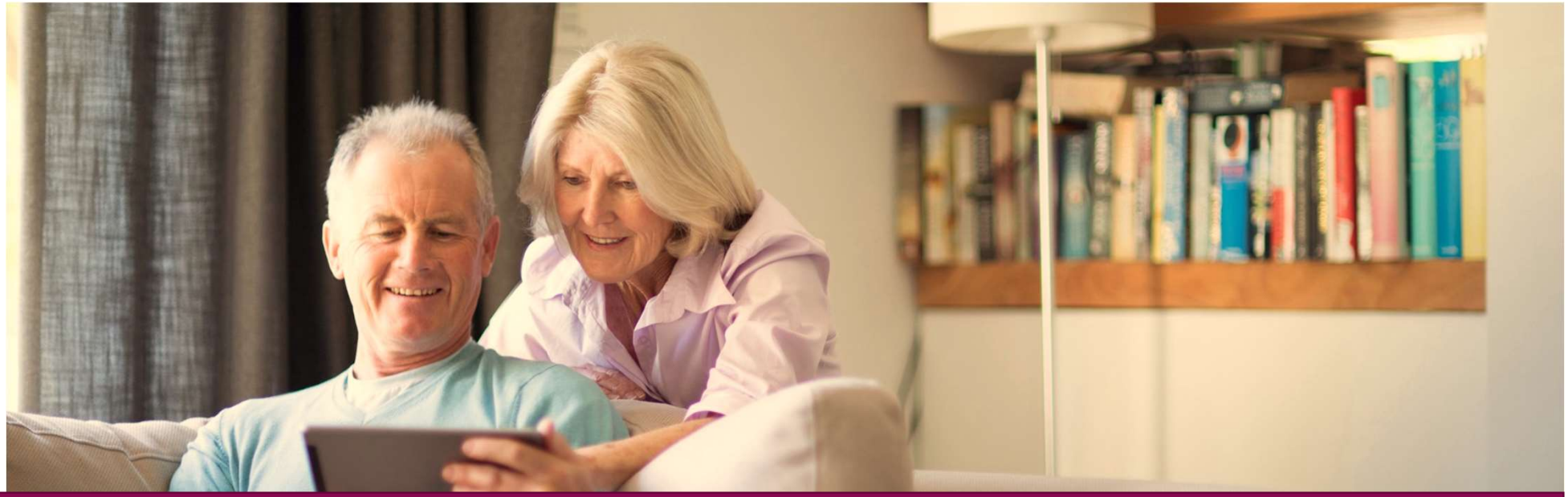
Times when bridging the **Digital Divide** is important…

When you need to connect with loved ones afar.

When you can't physically be somewhere.

When only digital options are available.

Why is it important for us as a Bank to help our communities to bridge this divide



We want our customers to feel supported and safe, as they transition to digital banking solutions and participate in the modern economy.

The benefits of banking digitally

Benefits of banking digitally

1
Monitor your account balances, transaction history and access electronic statements

2
Transfer money between your accounts, pay others using new and fast payment tools such as Osko and BPAY

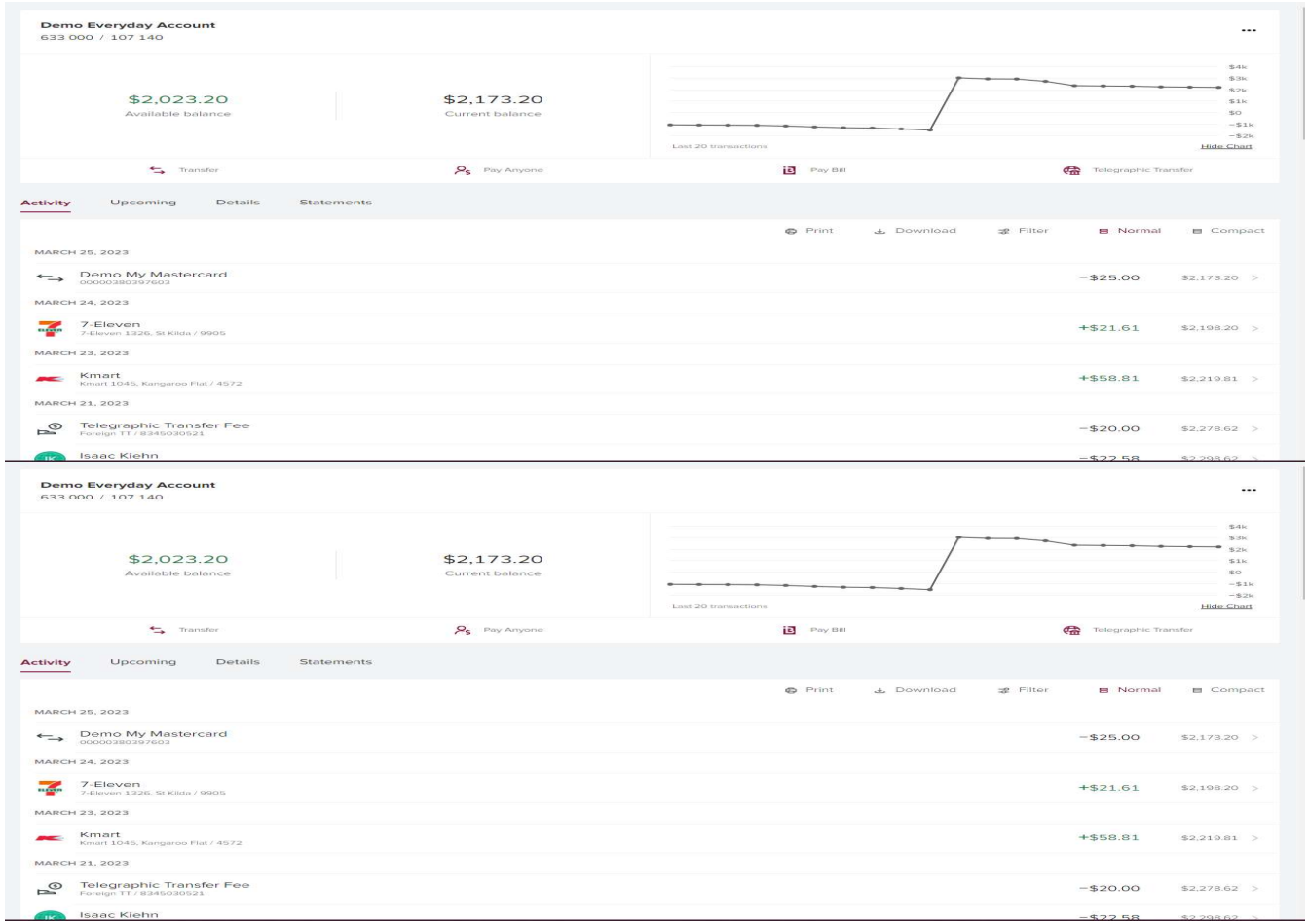
3
Enjoy peace of mind with our extensive safety and security measures

Things you can do in e-banking, to bank more safely

Balances, transactions and statements

Check your balances and view transactions instantly.

Opt out of paper and receive an email as soon as your statement is ready.

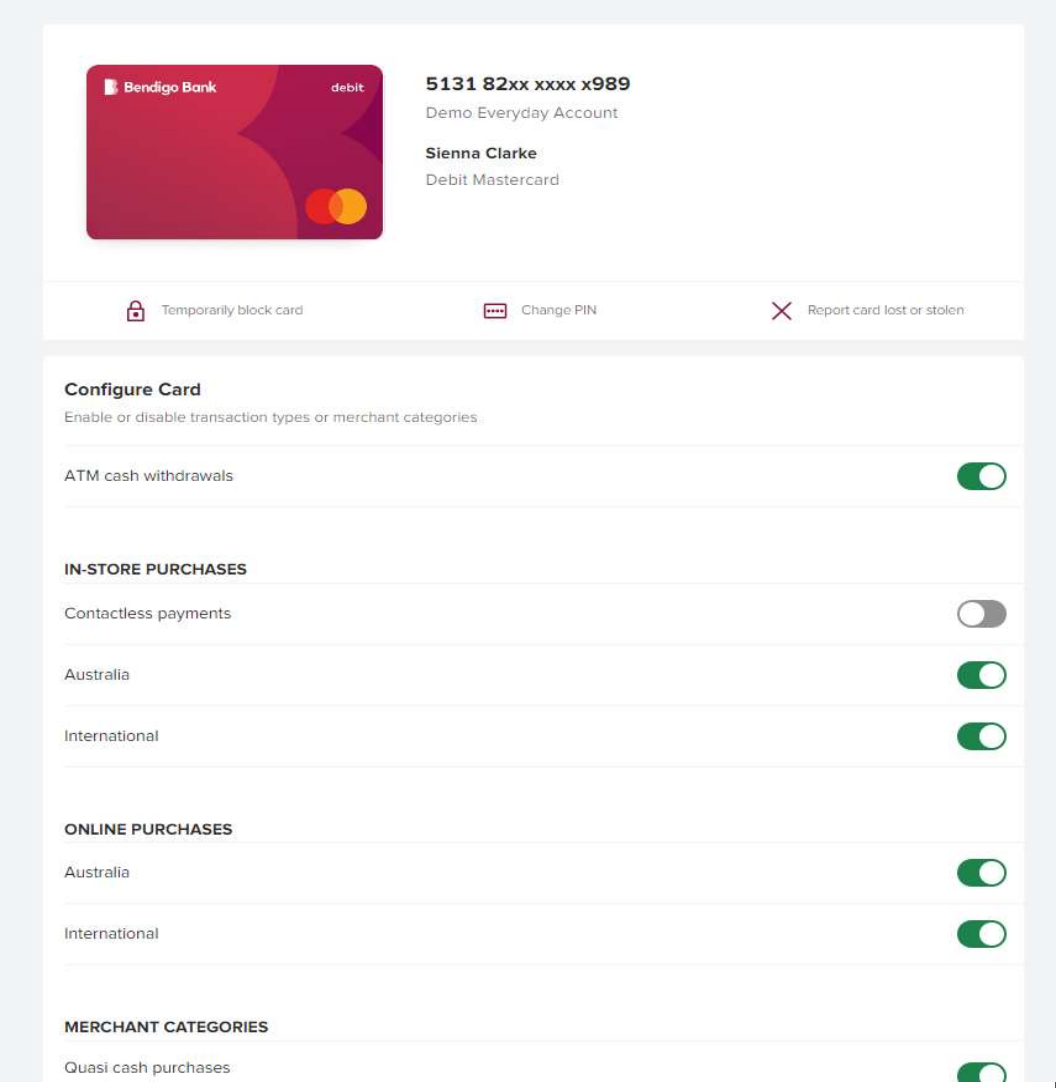


Things you can do in e-banking, to bank more safely

Manage your card

Have control over your card. You can activate, set your PIN, block or report your card as lost or stolen.

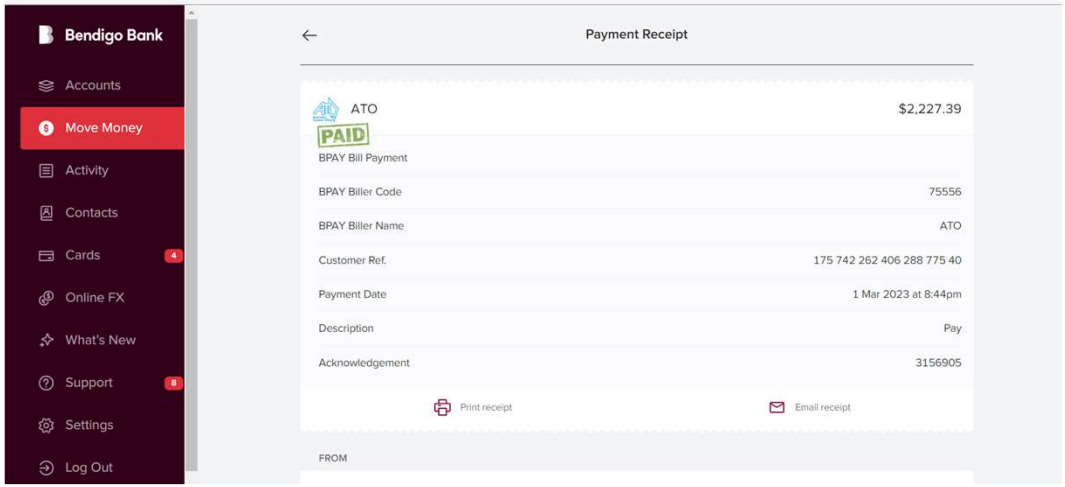
You can even configure what transactions or merchant types are acceptable.



Things you can do in e-banking, to bank more safely

A simple and straightforward way to pay bills

There are plenty of ways to pay bills. But with BPAY, you're in control. Pay your bills more quickly, easily and securely wherever you are — at home, work or on the go.



How to manage your risk in the digital world

Hands up if you have ever received one of these..

Suspicious phone call?

Spam text message?

Spam email?

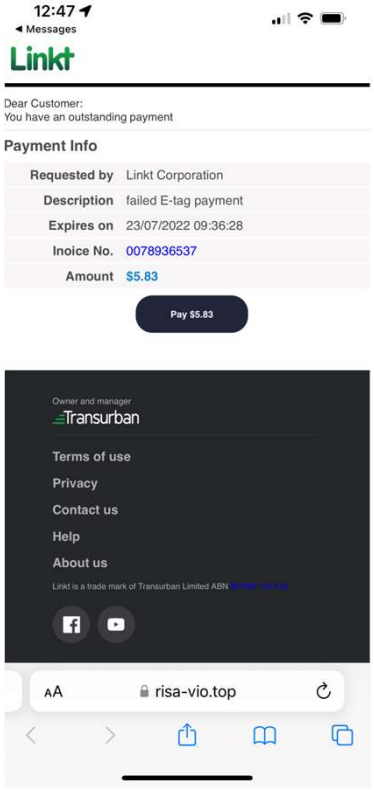
Scams Impacting our Customers

WhatsApp – 'Hi Mum' Scams

- Thousands of Australians are falling victim to a social engineering scam with many 'Hi Mum' scams reported to ACCC in June and July 2022, with reported losses of $2.6M.
- The scammer contacts victims through WhatsApp posing as a family member or friend.

Phishing/Smishing

- Customers who click on links within malicious emails and SMS are at the highest risk of financial loss.



Investment Scams

- Investment scams will be masked as an offer to purchase cryptocurrency, Bonds, business ventures, superannuation schemes, managed funds and the sale, or purchase of shares or property.
- Scammers will create 'opportunities' with professional brochures, websites to trick individuals into taking up the offer.

Remote Access Scam (RAS)

- When a third party, in contact (usually over the telephone) with the Bank's customer is given access to a customers device via remote access software loaded to the device OR a Bank's customer enters password/token information at the request of third party to process a payment.

Romance Scams

- Dating and romance scammers create fake profiles on real dating websites and social media platforms often using images and photos of identities they have stolen from other people.
- The scammer will typically request money to assist them with an illness, travel costs or family issues.

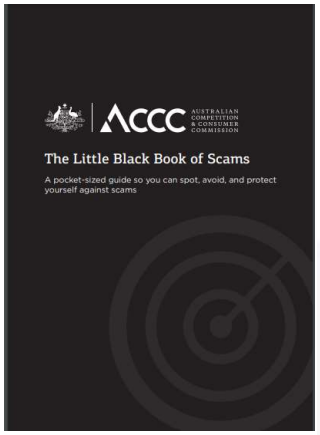
Be wary of **investment scams – currently #1 scam**

Before parting with money into an investment **do some of your own research.** You can check if the company has an Australian Financial Services Licence by visiting www.moneysmart.gov.au

If you are under retirement age, **watch out for offers promoting easy access to your preserved superannuation benefits.**
If super is accessed illegally, there may be penalties under taxation law.

Don't be pressured about making an investment or decision about your money when the opportunity has come out of the blue and don't fall for phony celebrity endorsements.

Remember – if it promises low risk, high returns and seems too good to be true – its likely a scam.



Protect your **personal information**

Don’t provide your personal details to a caller you don’t know over the phone

Never share your login information with anyone over the phone, text or email (your Bank will never ask you for login details), including one time passwords or security tokens

Make sure your letterbox is secure – use a padlock - and shred documents such as bank statements and bills before disposing of them

Don’t get caught out

Never send money or give your personal details to someone you have only met online.

DO NOT open attachments or click on links in emails, social media messages or text messages – just press delete – and **don’t be pressured** by threatening phone calls. **Stop, think and check** whether their story is true.

A government agency or trusted company will **never ask you to pay by unusual methods** such as by **gift card** or **iTunes card**, **wire transfers** or **Bitcoin.**

Verify the identity of the contact **by calling the relevant organisation directly** – find them through an independent source – don’t just return call on the number they contacted you with or with any contact details they provided you.

Tips to stay safe online:

- **Never share your login information** with anyone over the phone, via text or email (your Bank will never ask you for login details)
- Use **strong passwords**
- **Don't click on links** in unexpected emails or text messages from people or organisations you don't know
- **Know who you are buying from**. Only make payments for products via a website's secure payment method. You should not need to pay via wire transfer, prepaid card or cheque
- **Be careful of how much personal information** you share online or on websites you are not familiar with
- **If an email address looks suspicious**, delete it and do not click on any links.
- **If you are being pressured to act quickly**, slow down and take your time

What to do if you fall victim of a scam:

- Tell a loved one or someone you trust
- Visit your local Bendigo Bank Branch
- Contact our call centre 1300 236 344
- If you have received a **suspicious SMS text message** – please forward to: 0429 557 997 or phishing@bendigoadelaide.com.au
- **Or suspicious email** – please forward to phishing@bendigoadelaide.com.au

Resources available to you

Fraud prevention

Bendigo Bank

Five tips to stay safe

We want to help you stay safe and avoid becoming a victim of financial fraud.

Here are five tips to keep your personal and banking information safe.

The information here is general only. While it features important tips, fraudsters are always inventing new ways to defraud the community. It's important to be vigilant and keep up with the latest security advice.

1. Never share your access ID number
2. Never share your 6-digit token number
3. Never store your Access ID, passwords and token details together in the same place
4. We'll never call to request remote access to your computer
5. We'll never ask you to transfer funds

What to do if you're a victim of fraud

Call us immediately on 1300 BENDIGO if:

- You see suspicious activity on your account.
- A card, mobile phone or other payment device is lost or stolen.
- Your PIN, password or any other banking codes have become known to someone else.

Ways to bank with Bendigo

Bendigo Bank

Bendigo e-banking

Access e-banking 24/7 from anywhere in the world via our website or app.

You can:

- ✓ View balances, transactions and statements
- ✓ Make real time payments with Osko
- ✓ Pay bills with BPAY®
- ✓ Set up automatic payments
- ✓ Register a PayID
- ✓ Order, activate, lock and enable your cards
- ✓ Change personal information

You're protected by:

- Fraud monitoring and protection
- Encryption technology
- Added protection with multi-factor authentication

How to get it:

- Talk to your nearest branch or call 1300 236 344

What if I lose my phone?

Call us on 1300 236 344 as soon as you can. We'll disable the app on your phone - but be reassured that no-one can access your details without your Four-digit PIN.

The Little Black Book of Scams

ACCC AUSTRALIAN COMPETITION & CONSUMER COMMISSION

A pocket
yourself

Investment scams

'Risk-free investment' or opportunity for misfortune?

How the scam works

Investment scams come in many forms including cryptocurrency purchase, binary options trading, business ventures, superannuation schemes, managed funds and the sale or purchase of shares or property. Scammers dress up 'opportunities' with professional looking brochures and websites to mask their fraudulent operations. They often begin with a phone call or email out of the blue from a scammer offering a 'not-to-be-missed', 'high return' or 'guaranteed' opportunity. The scammer usually operates from overseas, and will not have an Australian Financial Services licence.

Computer prediction software scams promise to accurately predict stock market movements, the results of horse races, sports events or lotteries. They are simply a form of gambling disguised as investments. Most of the schemes or programs do not work and buyers cannot get their money back. In many cases the supplier simply disappears.

6 Little Black Book of Scams

Bendigo and Adelaide Bank

Questions?

Tips to stay safe online

- **Never share your login information** with anyone over the phone, via text or email (your Bank will never ask you for login details)
- Use **strong passwords**
- **Don't click on links** in unexpected emails or text messages from people or organisations you don't know
- **Know who you are buying from**. Only make payments for products via a website's secure payment method. You should not need to pay via wire transfer, prepaid card or cheque
- **Be careful of how much personal information** you share online or on websites you are not familiar with
- **If an email address looks suspicious**, delete it and do not click on any links.
- **If you are being pressured to act quickly**, slow down and take your time

What to do if you fall victim of a scam:

- Tell a loved one or someone you trust
- Visit your local Bendigo Bank Branch
- Contact our call centre 1300 236 344
- If you have received a **suspicious SMS text message** – please forward to: 0429 557 997 or phishing@bendigoadelaide.com.au
- **Or suspicious email** – please forward to phishing@bendigoadelaide.com.au

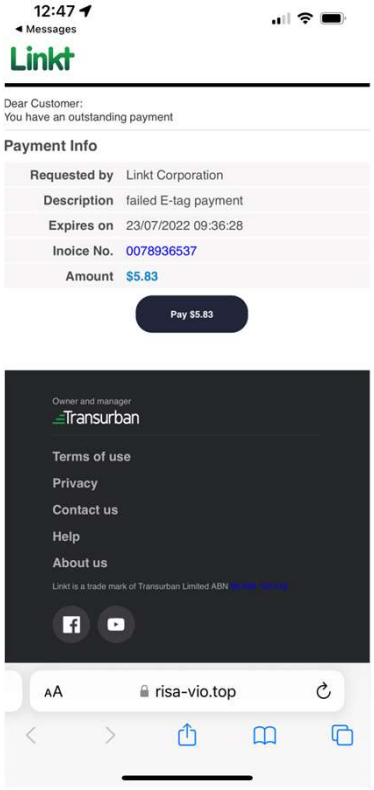
Scams Impacting our Customers

WhatsApp – 'Hi Mum' Scams

- Thousands of Australians are falling victim to a social engineering scam with many 'Hi Mum' scams reported to ACCC in June and July 2022, with reported losses of $2.6M.
- The scammer contacts victims through WhatsApp posing as a family member or friend.

Phishing/Smishing

- Customers who click on links within malicious emails and SMS are at the highest risk of financial loss.



Investment Scams

- Investment scams will be masked as an offer to purchase cryptocurrency, Bonds, business ventures, superannuation schemes, managed funds and the sale, or purchase of shares or property.
- Scammers will create 'opportunities' with professional brochures, websites to trick individuals into taking up the offer.

Remote Access Scam (RAS)

- When a third party, in contact (usually over the telephone) with the Bank's customer is given access to a customers device via remote access software loaded to the device OR a Bank's customer enters password/token information at the request of third party to process a payment.

Romance Scams

- Dating and romance scammers create fake profiles on real dating websites and social media platforms often using images and photos of identities they have stolen from other people.
- The scammer will typically request money to assist them with an illness, travel costs or family issues.

Bendigo and Adelaide Bank