more than money

Cyber Security Threat Landscape

Group Security Advisory & Awareness
2023

$33B

The amount of self reported losses from cybercrime

(July 20-June 21, ACSC Annual Threat Report)

$88,407

Average reported loss for medium businesses

(July 21-June 22, ACSC Annual Threat Report)

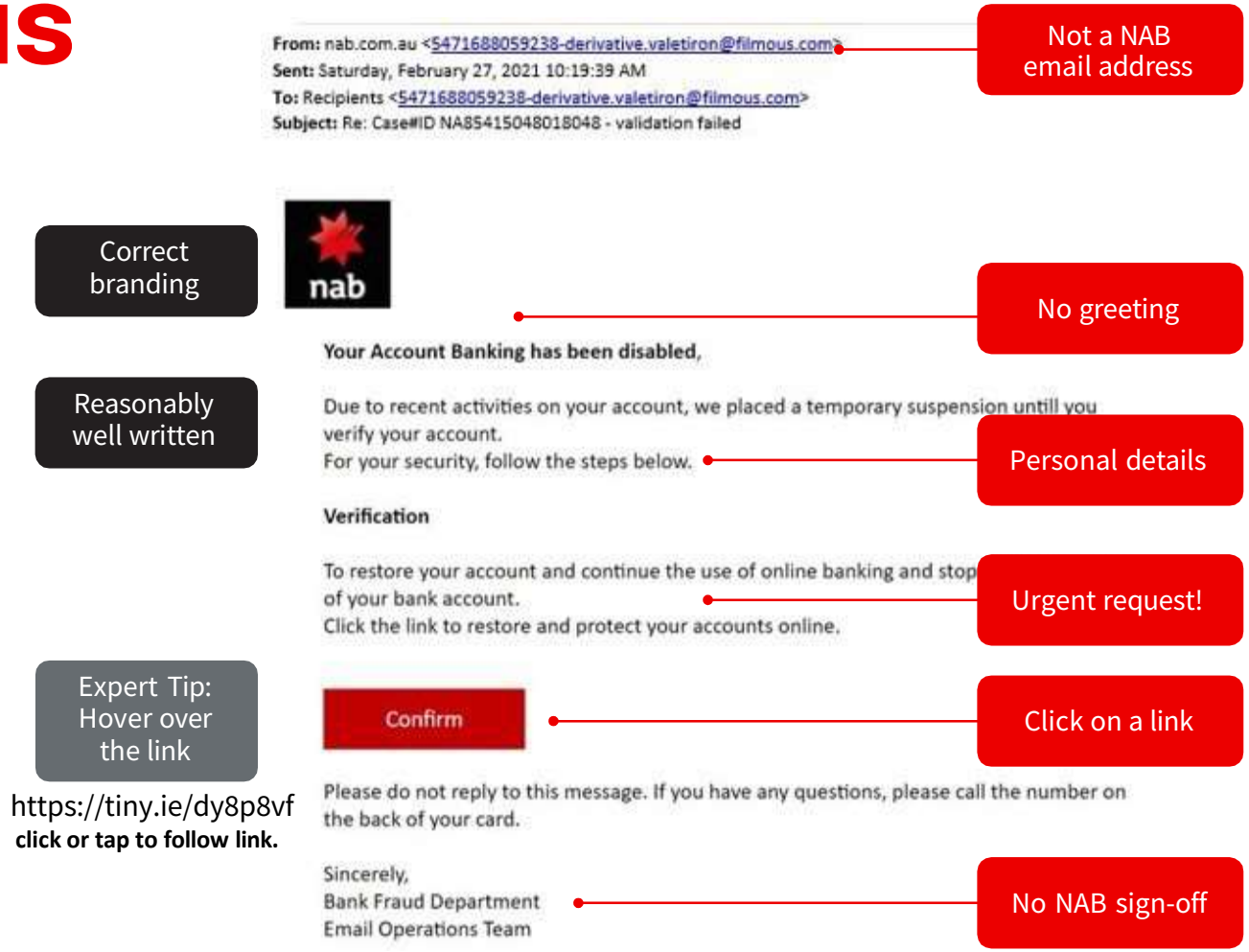
The use of emails with malicious attachments or links continue to be the most common initial infection vector

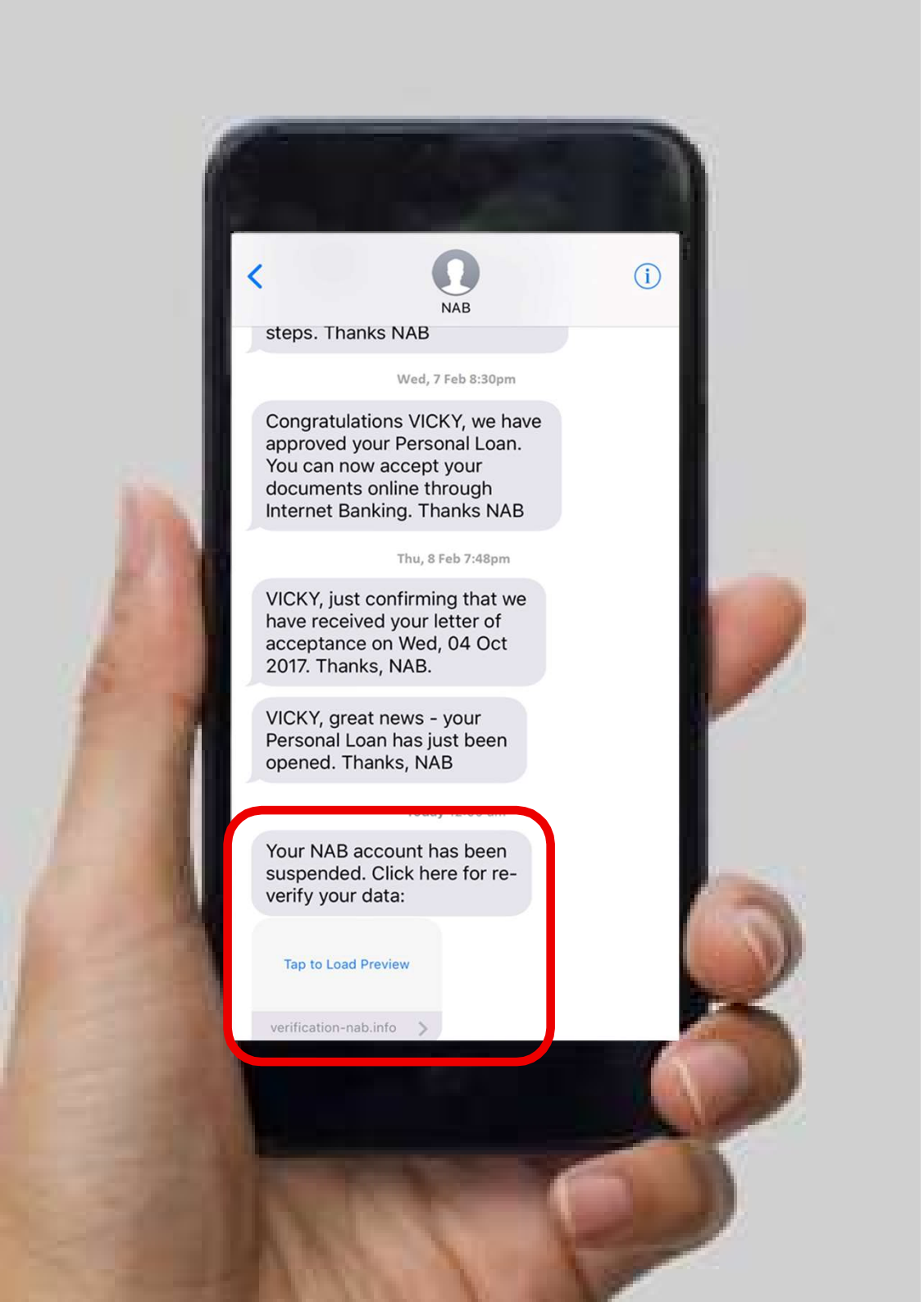
(July 20-June 21, ACSC Annual Threat Report)

A report is made to report cyber every 7 minutes

How to spot a suspicious email

- Senders email address does not match the organisation
- Generically addressed/ Not personalised
- Requests personal details
- Offers a threat or reward
- Link/button to click on, and the underlying website doesn't match
- No official sign off





SMS phishing

More common than email phishing

The website address can't be hidden

Report to **phish@nab.com.au** or **0476 220 003**

NAB - Your Internet Banking services have been suspended pending device verification. Visit https://nab.com.au.clientconfirm.info/ to perform verification.

Your debit card may be suspended. To confirm recent activity, simply log into your account. No further action is needed: nabconfirm.com/details

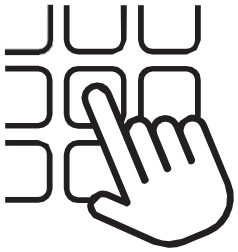
Your one-time passcode is 441761. If this wasn't you, CANCEL this transaction: cancelnab.link

We have flagged your account due to an unusual payee request. To CANCEL the payee request, immediately visit: https://nab365.live

Business email compromise

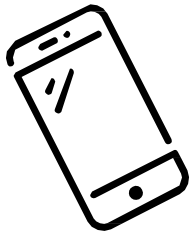
- Business emails are being targeted by criminals
- To send malicious messages to the address book
- To intercept payment details
- To make fake payment requests

- **Be aware of phishing messages**
- **Have 2FA or MFA turned on for email accounts**
- **Utilise a PayID**



1

Something you know



2

Something you have

3

Something you are

Safeguards

Safeguards
ACSC Essential Eight

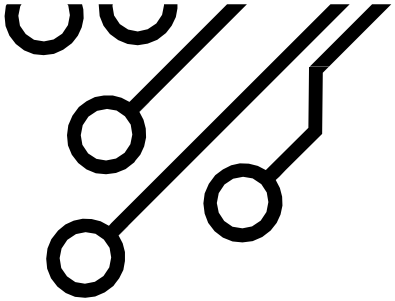
01 To prevent malware running

1. Application Whitelisting
2. Patch Applications
3. Disable untrusted Microsoft Office macros
4. User Application Hardening

02 To limit the extent of incidents and enable data recovery

5. Restrict Admin Privileges
6. Patch Operating Systems
7. Two/Multi-factor Authentication
8. Daily Backup of Important Data

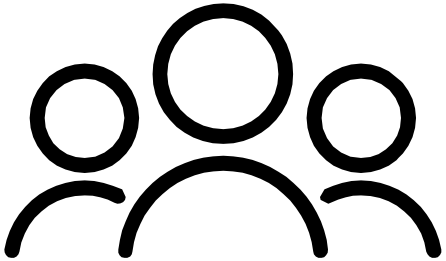
Safeguards



Technology

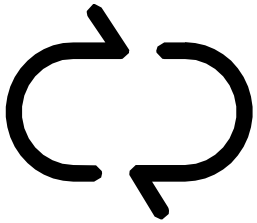
NAB Connect

- Security Tokens
- Payment limits
- Segregation of duties
- Multiple Authorisers
- Implement the Essential 8
- Use a PayID



People

- Be aware of suspicious messages
- Use different passwords for different log ins and their own log in details
- Use different computers to create and approve transactions
- Have an awareness program in place



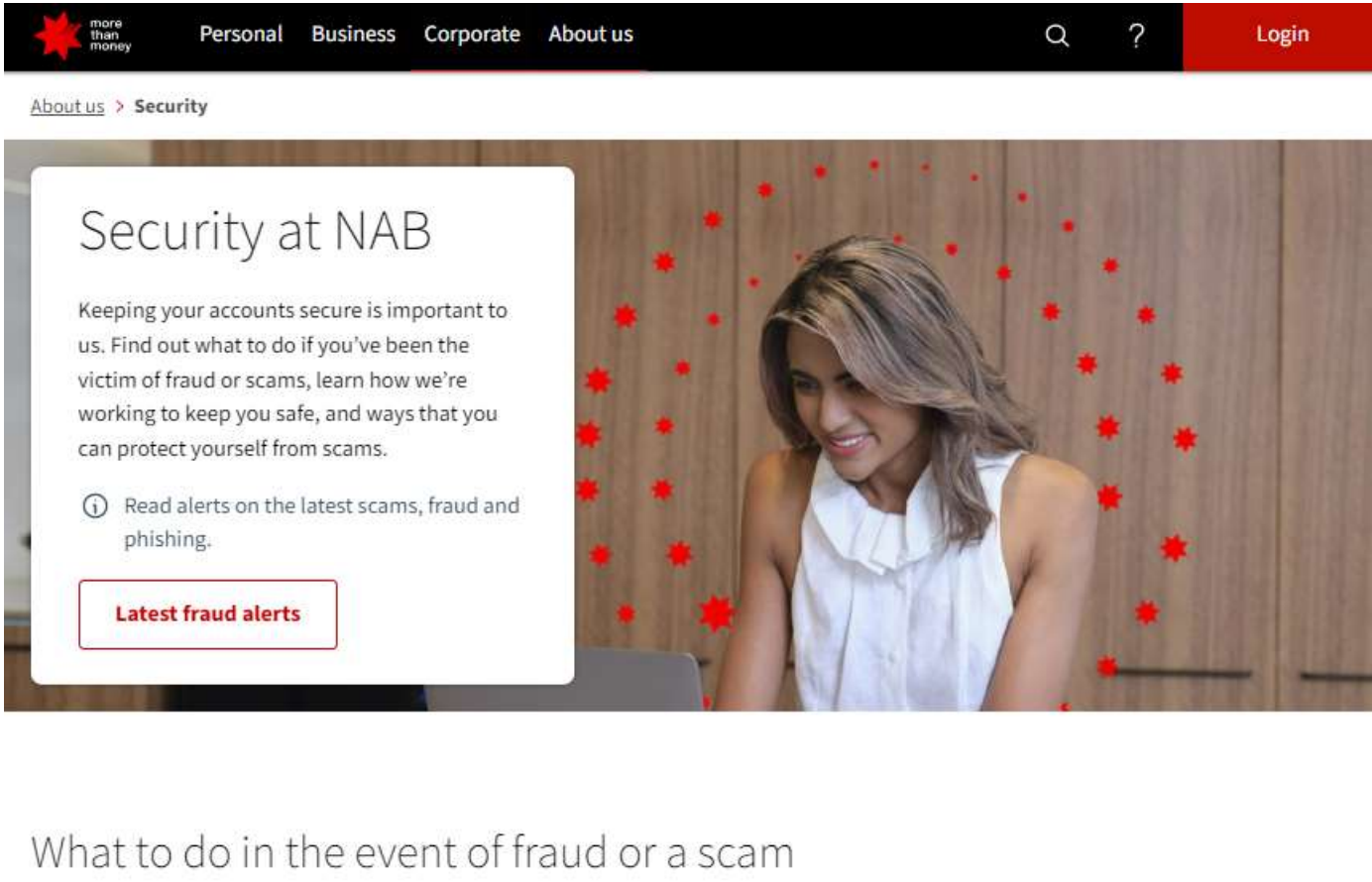
Process

- Validate new accounts or changes to payment instructions by calling on a know number
- Have an agreed process for making payments for executives
- Ensure business risk reviews include the topic of cyber security

nab.com.au/security

Resources

- Up to date articles with practical advice
- Regular webinar series
- Cyber Toolkit for Businesses
- Security alerts on latest threats
- Security podcast for businesses



Reporting an incident

1

If you've been affected by fraud or a scam

- Report immediately
- 13 10 12 – Business
- 13 22 65 – Personal, quote "Fraud Assist"
- 1300 557 081 – Corporate
- Fraud and scam cases can take a number of weeks to resolve

2

If you receive an email or SMS pretending to be NAB

- phish@nab.com.au
- 0476 200 003

3

Cyber events

- Australian Cyber Security Centre cyber.gov.au/report
- Office of the Australian Information Commissioner - if the incident is a reportable data breach oaic.gov.au

Where to go for more info

1

nab.com.au/security

- Training – including webinars
- Podcasts
- Articles
- Updated alerts
- Toolkit for Businesses

2

cyber.gov.au

Australian Cyber Security Centre

- Advice and information
- Report incidents
- Alert Service

3

scamwatch.gov.au

- Advice and information for individuals and businesses
- Report incidents
- Alert Service

Top 5 to do's

1

Implement Australian Signals Directorate: Essential 8

cyber.gov.au/acsc/view-all-content/essential-eight

2

Turn on MFA

cyber.gov.au/mfa

3

Turn on segregation of duties

nab.com.au/nabc-content/nab-connect-help/security

4

Back up your data and set up auto updates

- Practise restoring your data from the back up

5

Empower your team

- Red flags of suspicious messages
- How to report
- Set the tone from the top
- Invite them to our webinars nab.com.au/cyberandfraudsessions