Bp Premier

SUMMIT 2025

Protecting YOUR Practice from Cyber Threats

Danielle Pentony & Tracey Weeks

Bp Premier

SUMMIT 2025

Please take a seat,

your session starts soon.

Acknowledgement of Country

Best Practice Software acknowledges the Traditional Custodians of Country throughout Australia and recognise their unique cultural and spiritual relationships to the land, waters, and seas and their rich contribution to society. We pay our respects to ancestors and Elders, past, present, and emerging.

Best Practice Software respects Māori as the tangata whenua and Treaty of Waitangi partners in Aotearoa New Zealand.

Right: Ginmine design from corner, radiating outwards.
Designed for the Bp Bundaberg Operations Hub Mural Project, 2021

Artist: Nicole Wone

Addresses themes of: Evolution – Adaptation of Universe and traditional Indigenous beliefs across the globe.

Beginning of time, darkness. Movement in the cosmos. Rainbow Serpent – Creation being. Ancestral lineage without our DNA

Bp Premier
SUMMIT 2025

Protecting YOUR Practice from Cyber Threats

Danielle Pentony

With over 18 years in Technology and Cyber Security across Healthcare, Government and Financial Services, Danielle leads the Cyber Security team securing key digital health solutions and sensitive information at the Australian Digital Health Agency. She also supports healthcare providers and technology partners through sharing cyber threat information and education. Known for her innovative and inclusive leadership, she delivers secure outcomes for the organisation. Outside the Agency, Danielle volunteers to uplift small and medium businesses' cyber security and advocates for more women in Cyber roles.

Tracey Weeks

With a career spanning 28 years in the State and Federal Government and over a decade's experience in the field of Cyber Security in the Healthcare sector, Tracey leads her team within Cyber Security Branch driving cultural change across Australia in cyber security awareness with the focus on the workforce being the key to ensuring the protection of the Agencies information and service delivery.

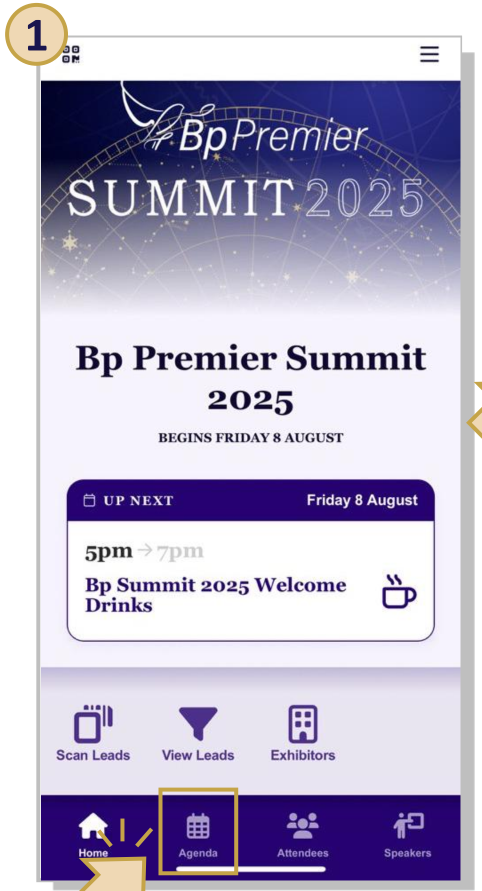
BpPremier
SUMMIT 2025

Ask any questions using The Event App

Download the app
By scanning the QR code

The EVENTAPP

1


Bp Premier SUMMIT 2025

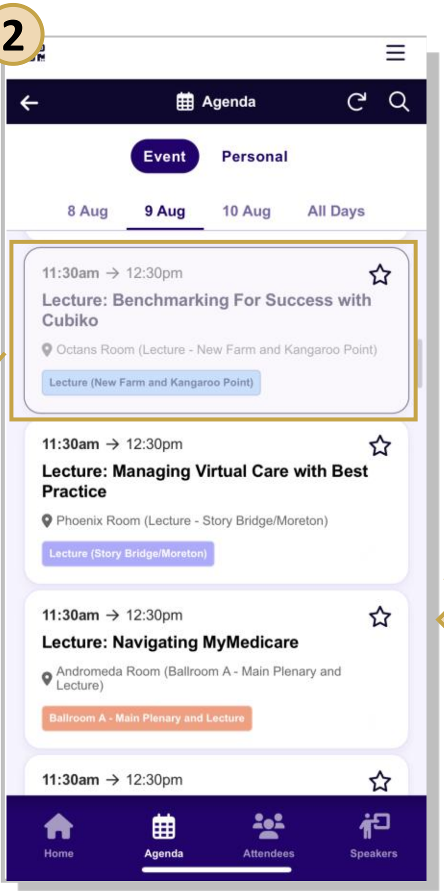
Bp Premier Summit 2025

BEGINS FRIDAY 8 AUGUST

UP NEXT Friday 8 August

5pm → 7pm
Bp Summit 2025 Welcome Drinks

2


Agenda

Event | Personal

8 Aug | 9 Aug | 10 Aug | All Days

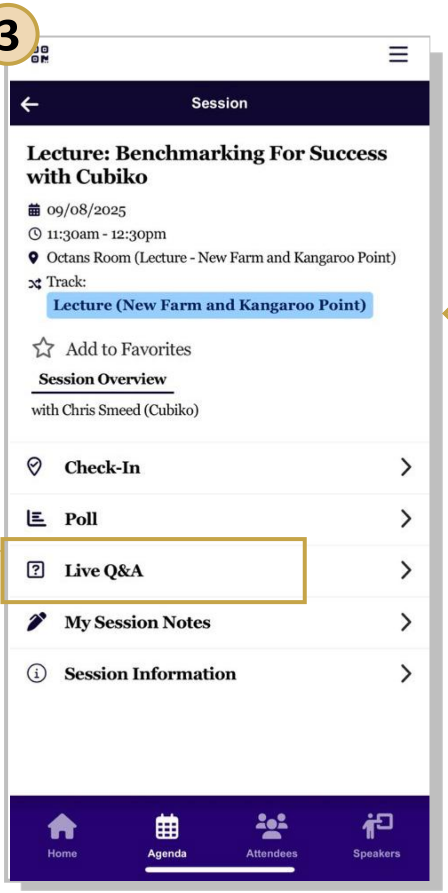
11:30am → 12:30pm
Lecture: Benchmarking For Success with Cubiko
Octans Room (Lecture - New Farm and Kangaroo Point)
Lecture (New Farm and Kangaroo Point)

11:30am → 12:30pm
Lecture: Managing Virtual Care with Best Practice
Phoenix Room (Lecture - Story Bridge/Moreton)
Lecture (Story Bridge/Moreton)

11:30am → 12:30pm
Lecture: Navigating MyMedicare
Andromeda Room (Ballroom A - Main Plenary and Lecture)
Ballroom A - Main Plenary and Lecture

11:30am → 12:30pm

3


Session

Lecture: Benchmarking For Success with Cubiko
09/08/2025
11:30am - 12:30pm
Octans Room (Lecture - New Farm and Kangaroo Point)
Track:
Lecture (New Farm and Kangaroo Point)

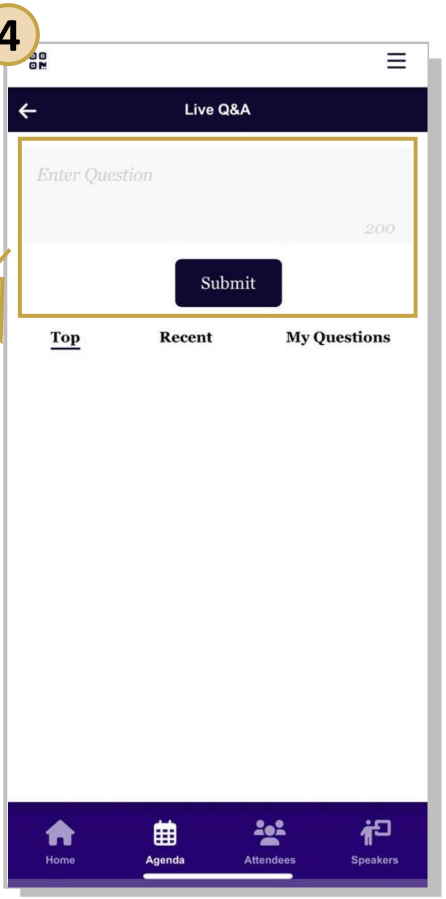
☆ Add to Favorites

Session Overview

with Chris Smeed (Cubiko)

Check-In
Poll
Live Q&A
My Session Notes
Session Information

4


Live Q&A

Enter Question
200

Submit

Top | Recent | My Questions

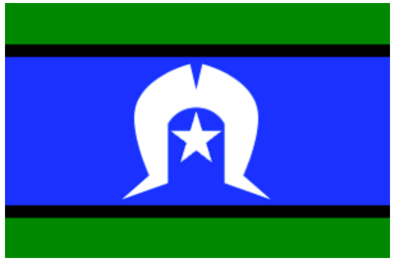
Building Cyber Resilience

Danielle Pentony, Chief Information Security Officer

Tracey Weeks, Manager Cyber Awareness and Education

Australian Government
Australian Digital Health Agency

Acknowledgement of Country



The Australian Digital Health Agency acknowledges the Traditional Custodians of Country throughout Australia, and their continuing connection to land, sea and community. We pay our respects to Elders past and present.

Navigating the Digital Frontier

- Making healthcare accessible
- Understanding the multifaceted needs of consumers
- Bridging cultural and linguistic gaps
- Reimagining engagement with consumers and the broader community
- Improving accessibility, promoting preventive care, and enhancing consumer engagement

Navigating the Digital Frontier

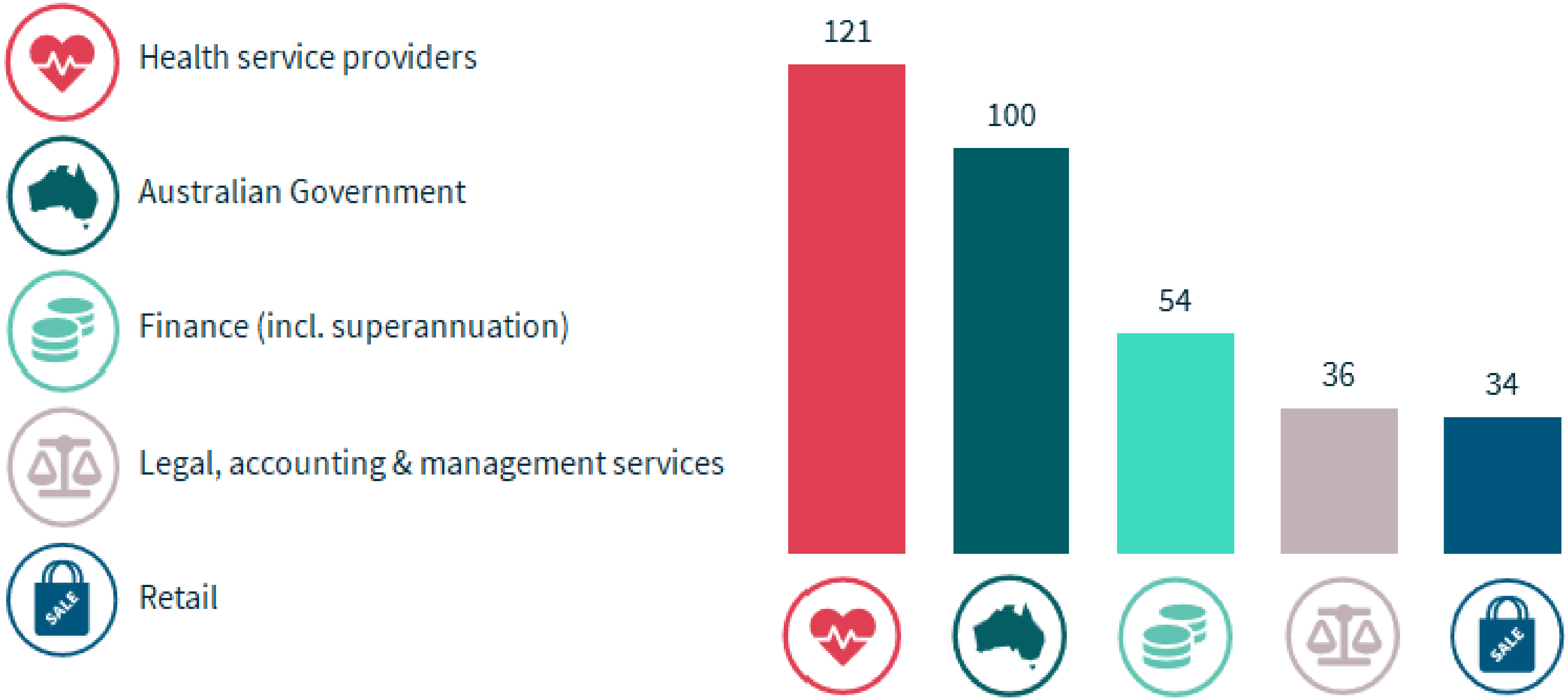
- Holistic and personalised approach to healthcare management
- Connecting technology systems and sharing data is a key element of delivering cost-effective, high-quality care
- Not a one-size-fits-all proposition
- Security and privacy as enablers

Cyber threat landscape

Healthcare Sector Update

- Rise of cyber crime
- Social engineering
- Ransomware
- Data breaches
- Denial of service attacks
- Malware
- Supply chain attacks
- Poor security practices
- Abuse of AI

Top 5 Sectors Notifiable Data Breaches

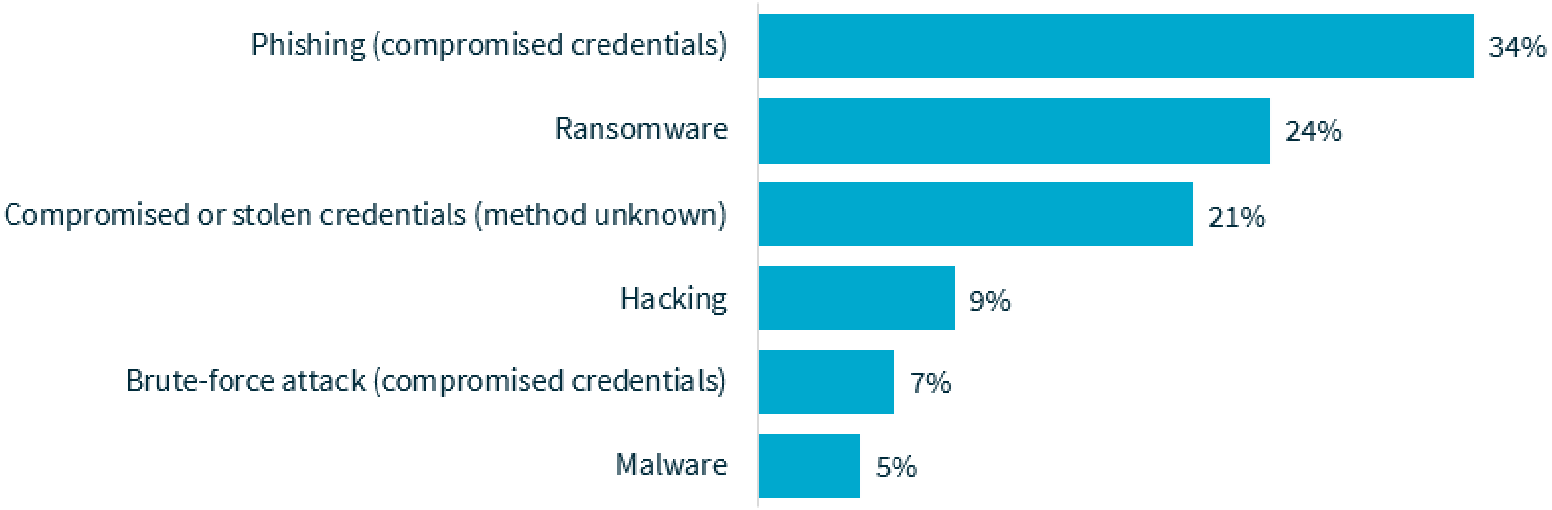


Source: Notifiable data breaches report Jul – Dec 24

Incident Breakdown

42% of all data breaches resulted from cyber security incidents (247 notifications; 61% of malicious or criminal attacks)

Cyber incident breakdown



Source: Notifiable data breaches report Jul – Dec 24

Top 5 reported sources of breaches in healthcare in Australia

- Malicious or criminal attack
- Cyber incident
- Social engineering / impersonation
- Rogue employee / insider threat
- Theft of paperwork or data storage device

Source: Notifiable data breaches report Jul – Dec 24

Global Review

> "The Global Health-ISAC 2025 Health Sector Cyber Threat Landscape highlights a continued escalation of cyberattacks.

Growing Threats

- The healthcare sector continues to face **escalating cyber threats**.
- **Ransomware** remains the most prevalent and damaging threat.
- **Nation-state actors, Hacktivists** and **supply chain vulnerabilities** are growing concerns.
- **Internet of Medical Things (IoMT)** devices introduce new attack surfaces.
- **Artificial Intelligence (AI)** opened new vectors of security and privacy risks
- Urgent need for **resilience, visibility, and vendor risk management**.

Source: Health-ISAC_2025-Annual-Threat-Report.pdf

Digital transformation continues to improve many aspects of our daily lives – including health care outcomes

Why we need to talk about cyber security

- Cyber safety is patient safety
- Cyber criminals aim to find weaknesses in an organisation that they can exploit through cyber attacks.
- Healthcare sector is a prime target.
- An attack can lead to:
    - loss or theft of sensitive health information
    - significant disruptions to service delivery
    - reputational damage
    - loss of consumer confidence

Cyber security is everyone’s responsibility

Understanding Resilience

Integrating cyber security in day-to-day life

Employee training

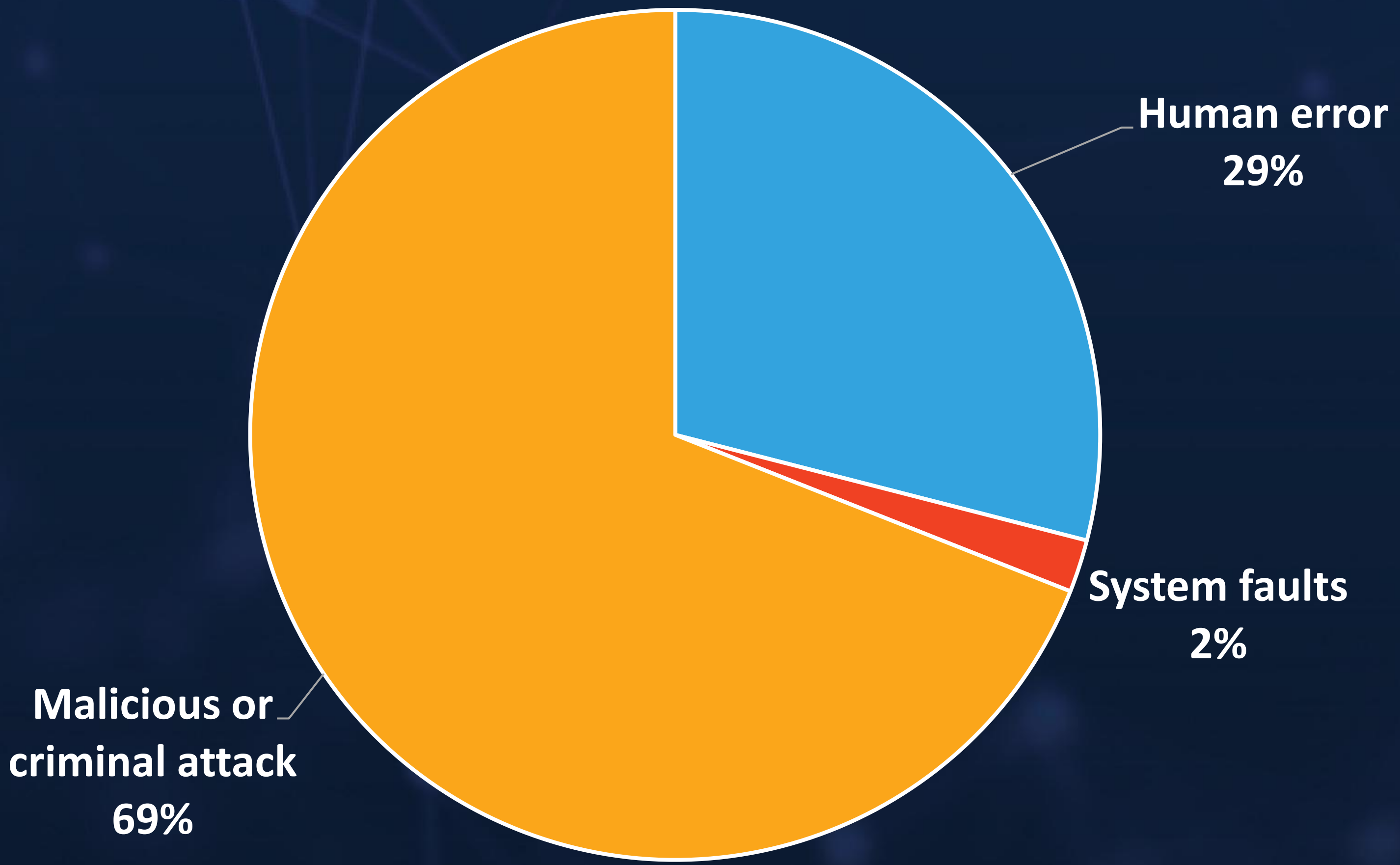
Secure by Design

Understanding the root cause

How do cyber attacks eventuate?

98% of data breaches are the result of **human error or malicious intent**

Sources of data breaches



Australian Government
Australian Digital Health Agency

Source: Office of the Australian Information Commissioner (2024)

34%

of reportable data breaches were from Phishing

Source: Notifiable data breaches report Jul – Dec 24

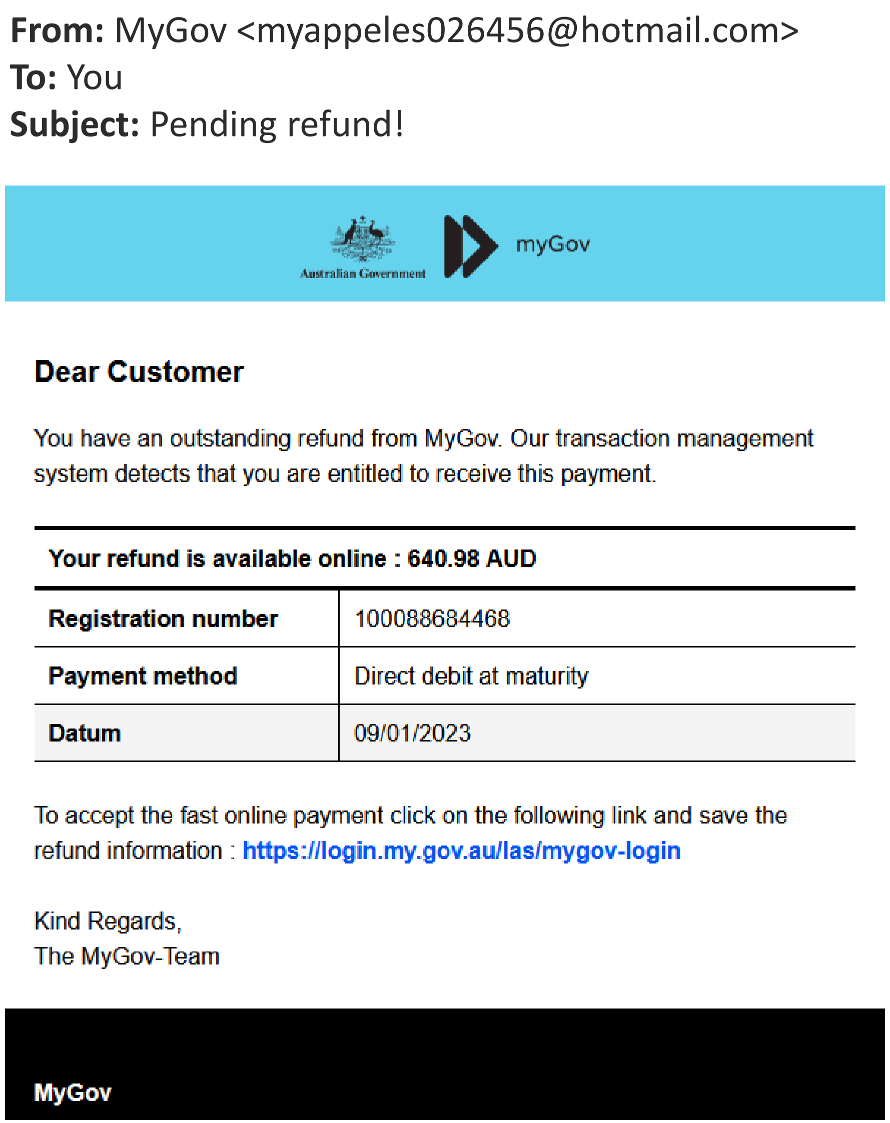
What is phishing?

Why are phishing attacks so successful?

44% of people think an email is safe when it contains familiar branding

1 in 3 people admit to taking risks when faced with a phishing threat

Attackers exploit human emotions and trust



From: MyGov <myappeles026456@hotmail.com>
To: You
Subject: Pending refund!

Dear Customer

You have an outstanding refund from MyGov. Our transaction management system detects that you are entitled to receive this payment.

Your refund is available online : 640.98 AUD

Registration number	100088684468
Payment method	Direct debit at maturity
Datum	09/01/2023

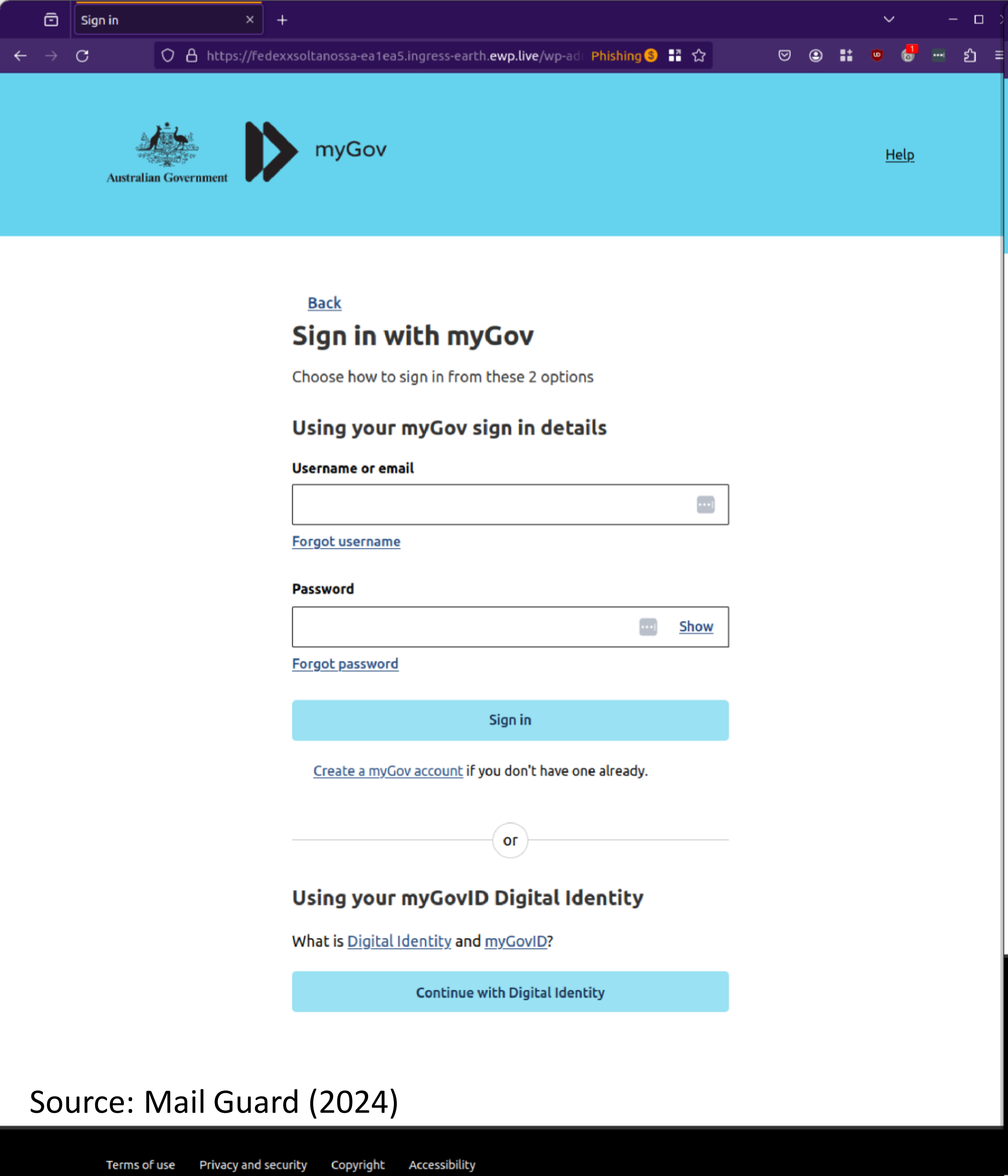
To accept the fast online payment click on the following link and save the refund information : **https://login.my.gov.au/las/mygov-login**

Kind Regards,
The MyGov-Team

MyGov

How to identify a phishing email

1. The email address is incorrect
2. Generic greeting (dear customer)
3. Unsolicited or unexpected
4. Too good to be true
5. *May* contain spelling, grammar or formatting errors.
6. It has a malicious link or attachment:
   - Directs to a website that steals information
   - Installs malware



Sign in

https://fedexxsoltanossa-ea1ea5.ingress-earth.ewp.live/wp-ad

Phishing

Australian Government

myGov

Help

Back

Sign in with myGov

Choose how to sign in from these 2 options

Using your myGov sign in details

Username or email

Forgot username

Password

Show

Forgot password

Sign in

Create a myGov account if you don't have one already.

or

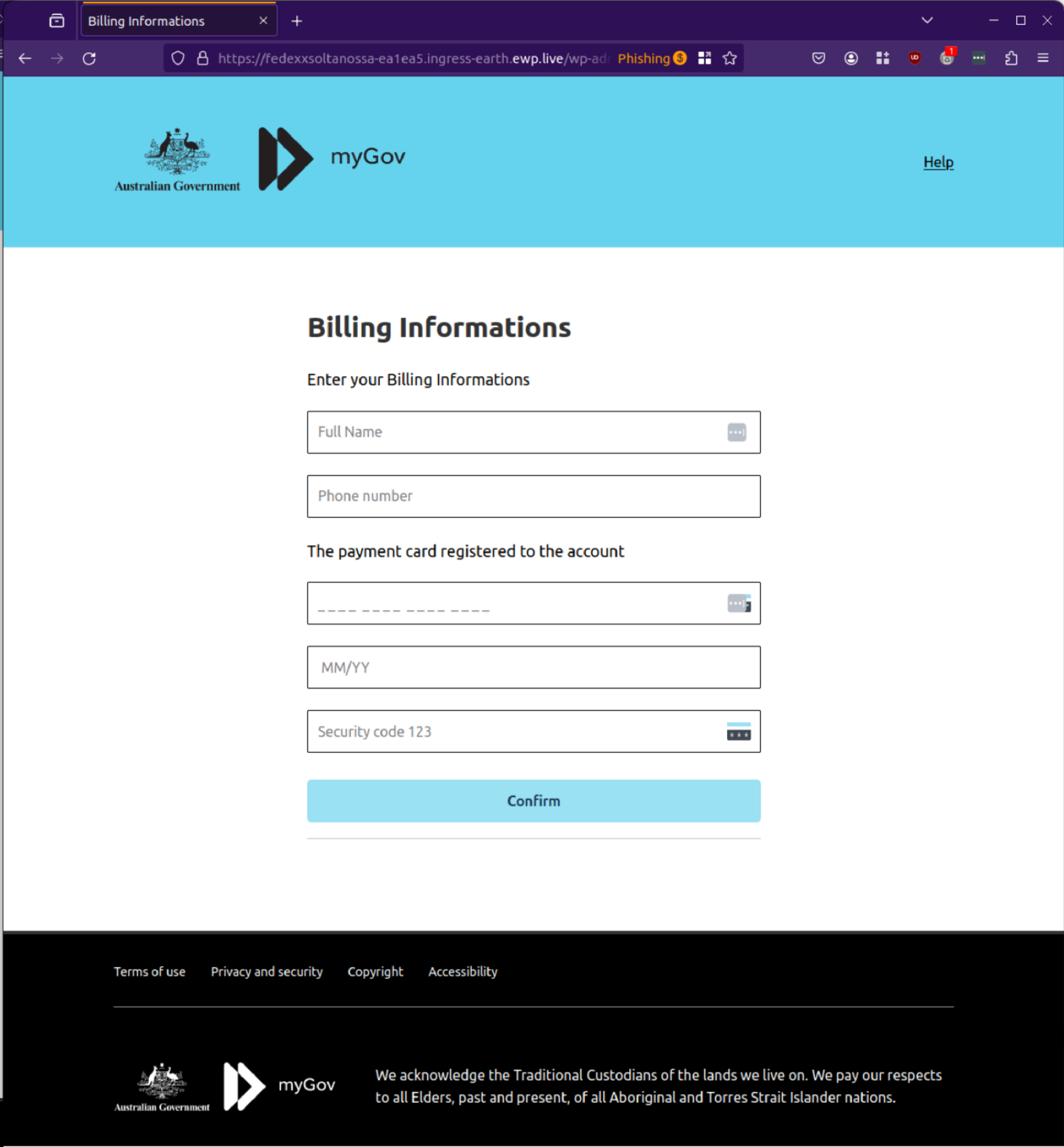
Using your myGovID Digital Identity

What is Digital Identity and myGovID?

Continue with Digital Identity

Terms of use · Privacy and security · Copyright · Accessibility

Source: Mail Guard (2024)



Billing Informations

https://fedexxsoltanossa-ea1ea5.ingress-earth.ewp.live/wp-ad

Phishing

Australian Government

myGov

Help

Billing Informations

Enter your Billing Informations

Full Name

Phone number

The payment card registered to the account

____ ____ ____ ____

MM/YY

Security code 123

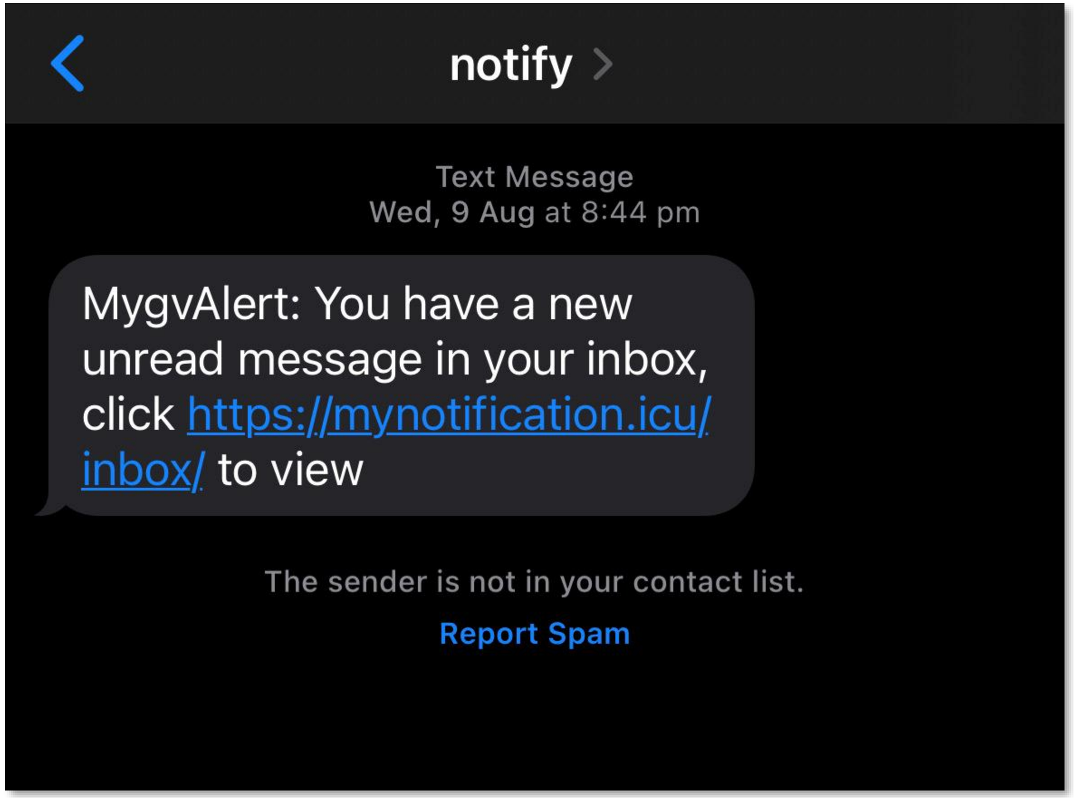
Confirm

Terms of use · Privacy and security · Copyright · Accessibility

Australian Government

myGov

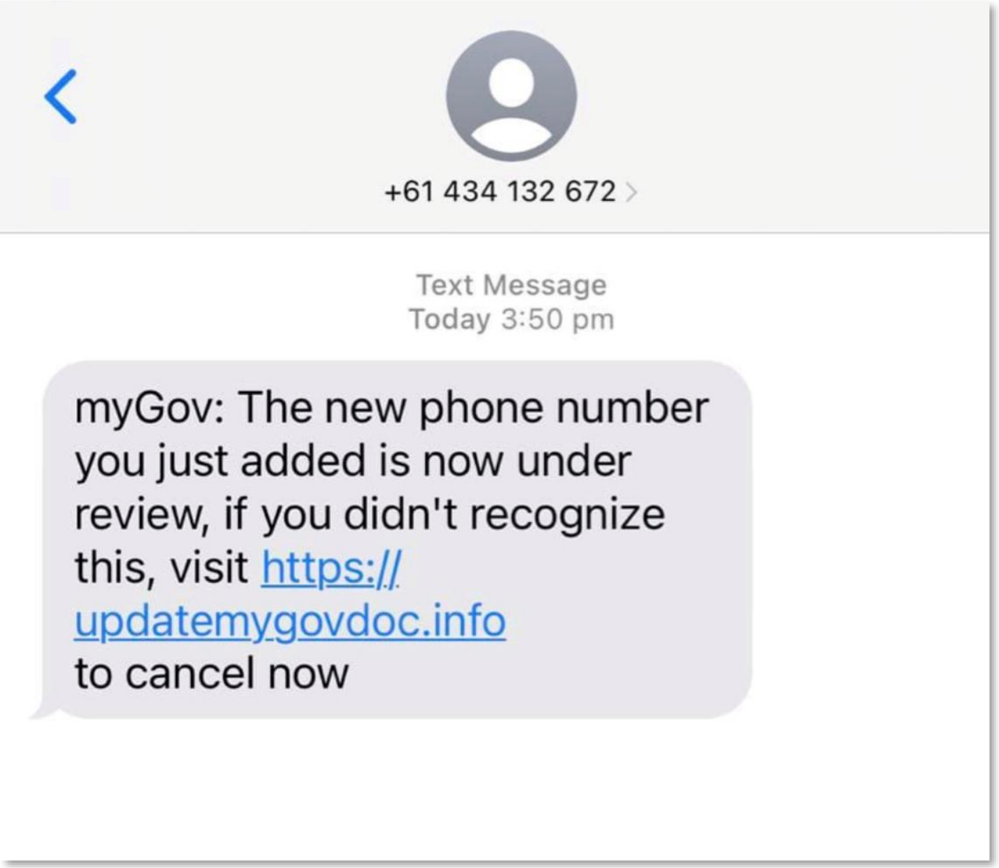
We acknowledge the Traditional Custodians of the lands we live on. We pay our respects to all Elders, past and present, of all Aboriginal and Torres Strait Islander nations.



Text Message
Wed, 9 Aug at 8:44 pm

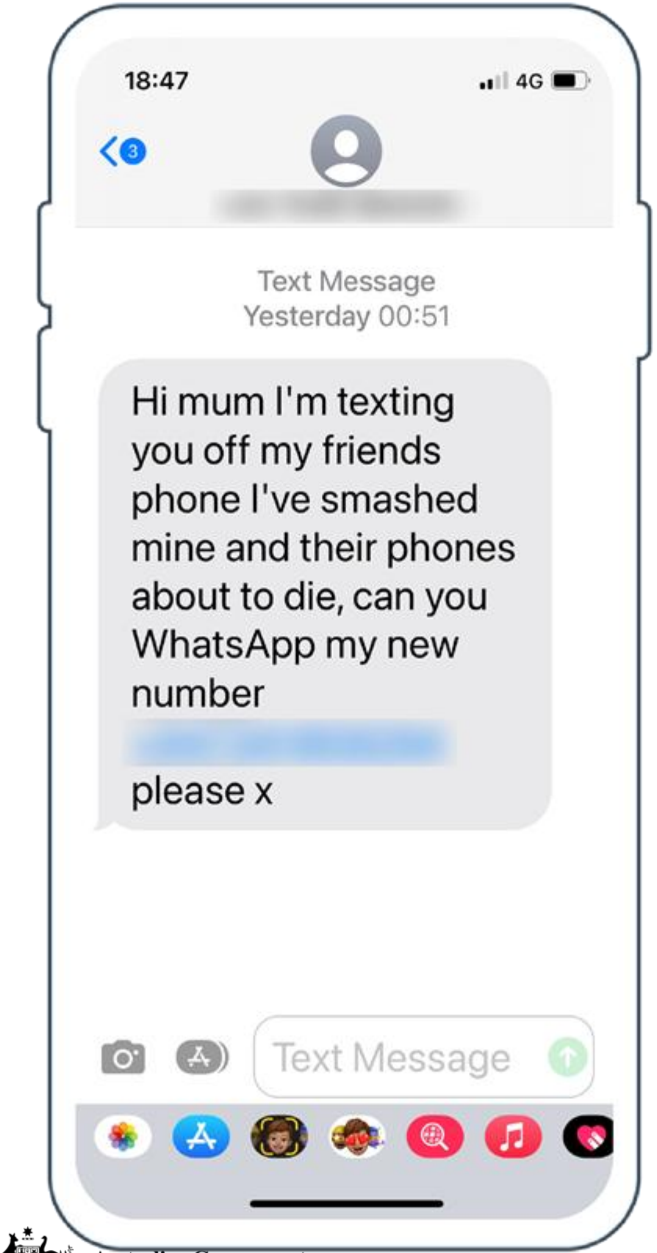
MygvAlert: You have a new unread message in your inbox, click https://mynotification.icu/inbox/ to view

The sender is not in your contact list.



Text Message
Today 3:50 pm

myGov: The new phone number you just added is now under review, if you didn't recognize this, visit https://updatemygovdoc.info to cancel now

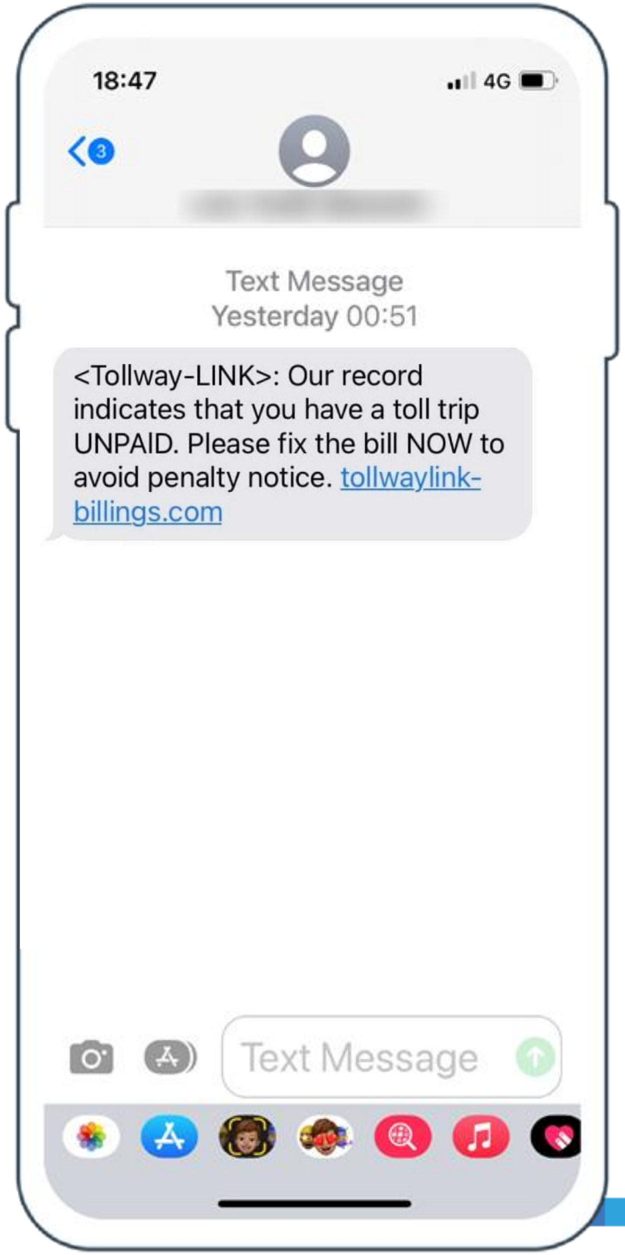


18:47 4G

[redacted]

Text Message
Yesterday 00:51

Hi mum I'm texting you off my friends phone I've smashed mine and their phones about to die, can you WhatsApp my new number [redacted] please x

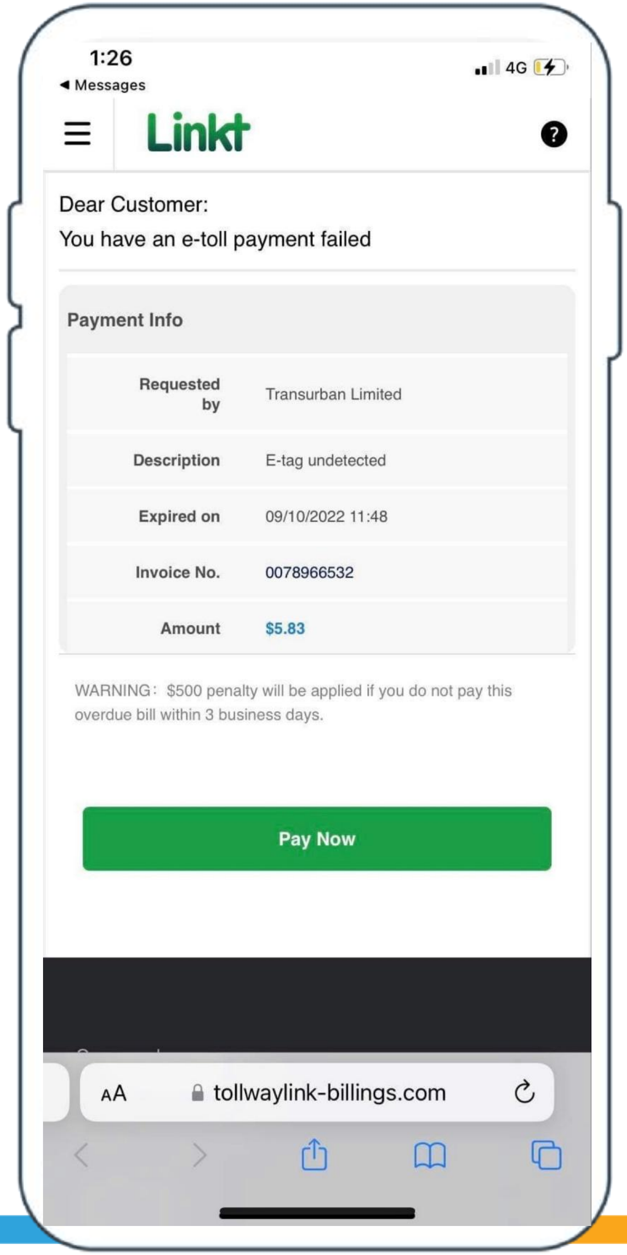


18:47 4G

[redacted]

Text Message
Yesterday 00:51

<Tollway-LINK>: Our record indicates that you have a toll trip UNPAID. Please fix the bill NOW to avoid penalty notice. tollwaylink-billings.com



1:26 4G
◂ Messages

Dear Customer:
You have an e-toll payment failed

Payment Info

Requested by	Transurban Limited
Description	E-tag undetected
Expired on	09/10/2022 11:48
Invoice No.	0078966532
Amount	$5.83

WARNING: $500 penalty will be applied if you do not pay this overdue bill within 3 business days.

How to spot a phishing scam

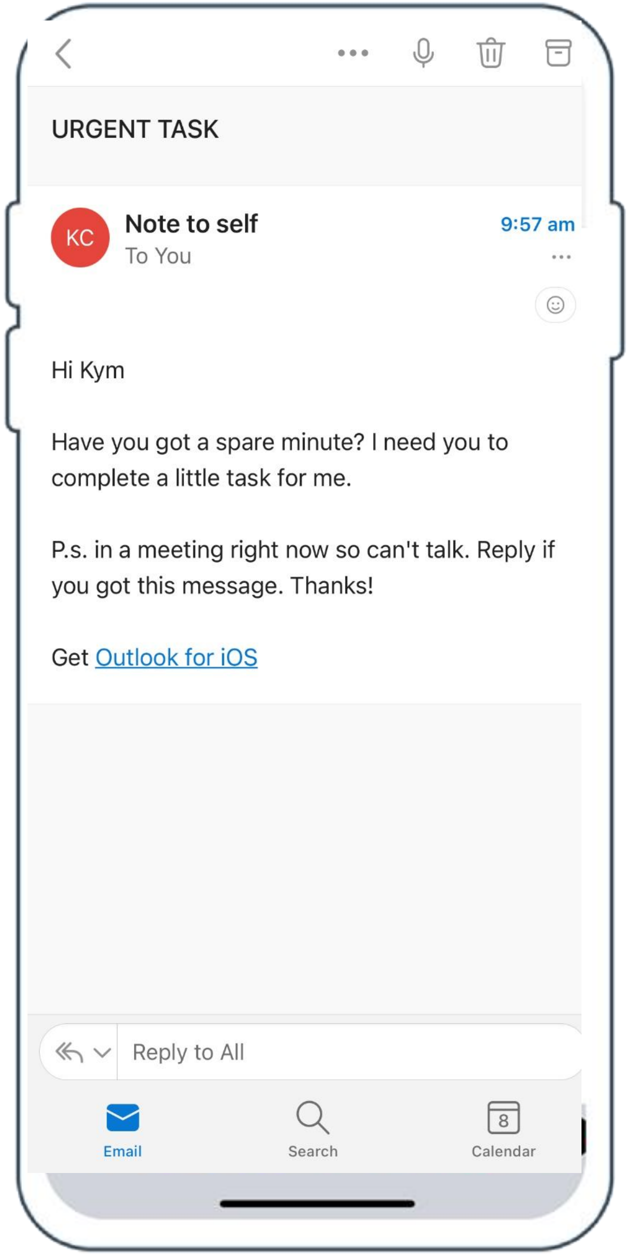
Before clicking on any links or attachments or sharing personal details ask yourself:

- Are my emotions heightened?
- Is there a sense of urgency?
- Can this person prove their identity?
    - Did this message come from a legitimate sender (e.g., correct email address, phone number or social profile)
    - Did my colleague/friend send this message to me (e.g., has their account been hacked)?
- Are there attachments or links in the message?
- Does this offer sound too good to be true?

$84 M

total self reported losses Business Email Compromised in Australia during FY 2023-2024

Source: Annual Cyber Threat Report 2023-2024 | Cyber.gov.au



URGENT TASK

KC Note to self
To You
9:57 am

Hi Kym

Have you got a spare minute? I need you to complete a little task for me.

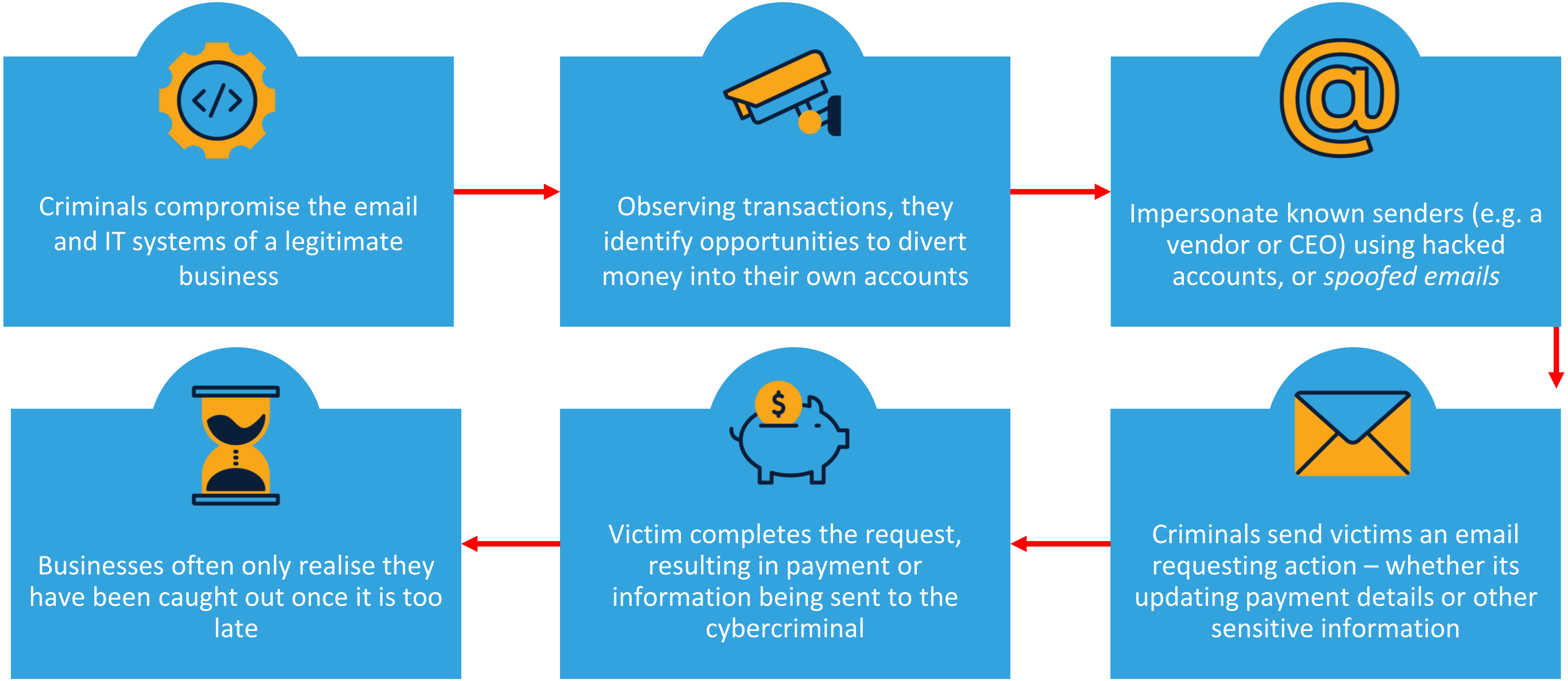
P.s. in a meeting right now so can't talk. Reply if you got this message. Thanks!

Get Outlook for iOS

Business Email Compromise (BEC)

- Targeted to a specific organisation or person
- Impersonate (or have compromised) known contacts and send scam emails and text messages
- Common BEC scams:
  - CEO/Executive fraud
  - Invoice fraud
  - Data theft

Anatomy of BEC attacks



Criminals compromise the email and IT systems of a legitimate business

Observing transactions, they identify opportunities to divert money into their own accounts

Impersonate known senders (e.g. a vendor or CEO) using hacked accounts, or *spoofed emails*

Criminals send victims an email requesting action – whether its updating payment details or other sensitive information

Victim completes the request, resulting in payment or information being sent to the cybercriminal

Businesses often only realise they have been caught out once it is too late

How BEC/targeted attacks eventuate

Staff, supplier or partner's email is compromised

Phishing

Data breaches

Website/social media scraping

How to mitigate BEC

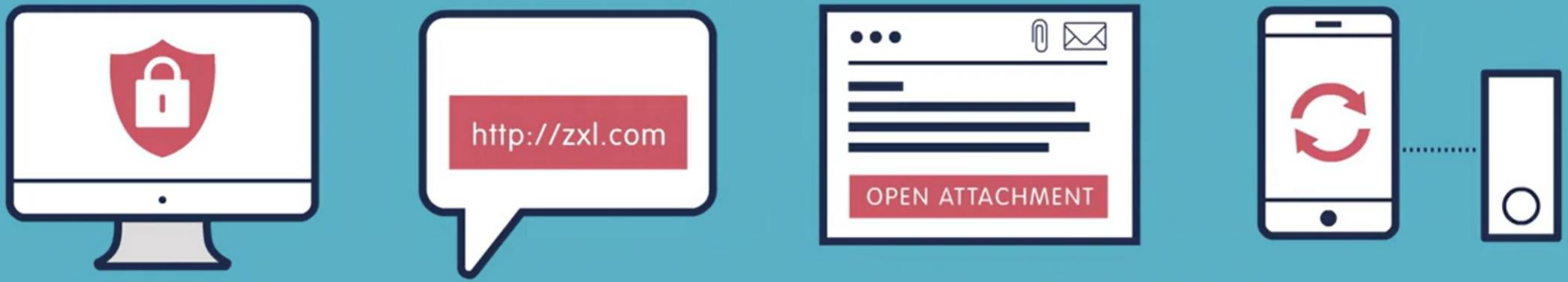
- The best defence against email attacks is **training and awareness.** When staff receive suspicious emails, the most effective mitigation is to call the sender to confirm they are legitimate.
- Do not use the contact details provided in the email as these could be fraudulent.
- Organisations should also have a formal process for staff to follow when payment requests are received or requests for changing bank details are made.

"Ransomware remains a highly destructive cybercrime threat"

- Australian Cyber Security Centre 2023

What is ransomware?

How can I prevent a ransomware attack?



Install software updates

NEVER click on suspicious links

NEVER open suspicious attachments

Backup your devices regularly

Source: Australian Cyber Security Centre (2023)

If your device is infected with ransomware

1. Disconnect from the internet and network (e.g. turn on airplane mode, turn off the Wi-Fi)
2. Take a picture or screenshot of the ransom message
3. Call your IT Provider; call the ACSC on **1300 CYBER1** (1300 292 371)

Practical tips to protect yourself from cyber threats

Secure your accounts

- Use strong passwords
- Multi-factor Authentication (MFA)

How to create a strong passphrase

Four words mashed:

KittenChocolatePuppyHappy99!

TortoiseTurtlePurpleApple#35

Note: please do not use these examples as your password or passphrase.

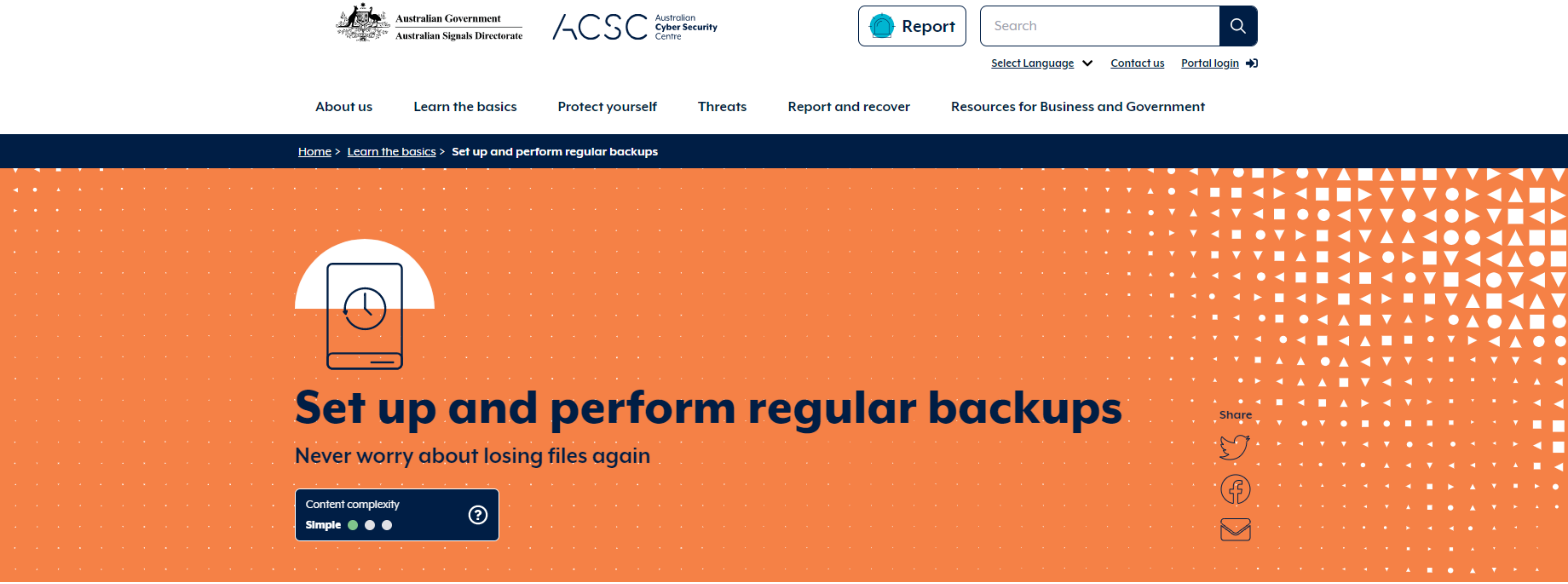
Multi-factor authentication

- **Turn on MFA** wherever you can.
- **Start with your important accounts** like email, banking, document storage and social media.
- MFA is often set up through the security settings on your account. If you're not sure how to set it up, **read the ACSC's advice on MFA** or **do a separate search online** (for example, 'facebook mfa').
- Some services may use a different name for MFA, such as "two-factor authentication" or "two-step verification", so don't be surprised by these terms in your search.

Keep software up to date

- OS systems software
- Apps and web browsers
- Set up automatic updates

https://www.cyber.gov.au/learn-basics


Australian Government
Australian Signals Directorate
ACSC Australian Cyber Security Centre
Report
Search
Select Language
Contact us
Portal login
About us
Learn the basics
Protect yourself
Threats
Report and recover
Resources for Business and Government
Home > Learn the basics > Set up and perform regular backups
Content complexity
Simple
Share

Set up and perform regular backups

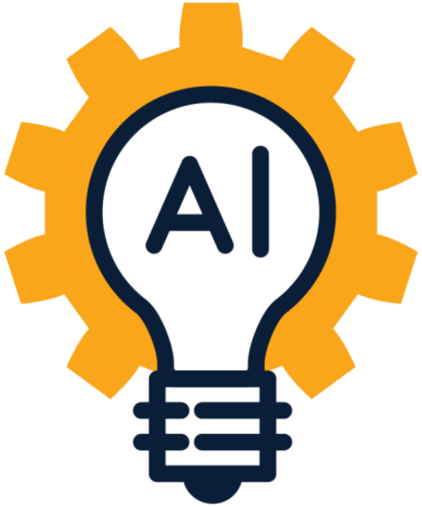
Never worry about losing files again

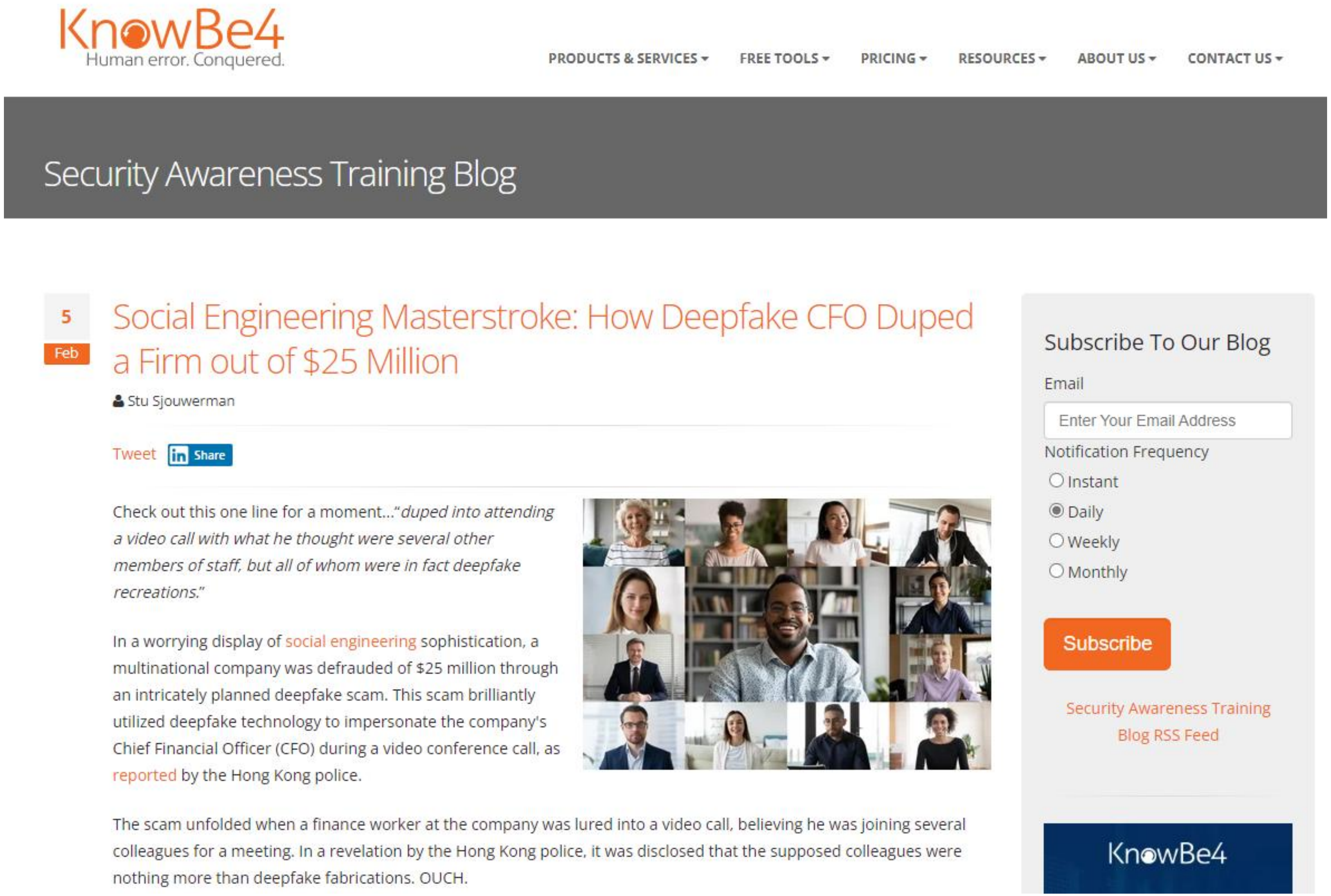
Artificial Intelligence

- AI systems are among the fastest growing applications globally. Common AI systems you may be familiar with include but are not limited to:
  - Generative AI chatbots (e.g., Microsoft Copilot, ChatGPT, Google Bard, Jasper)
  - Virtual assistants (e.g., Siri, Google Assistant, and Alexa)
  - Search Engines (e.g., Bing, Google) use AI to provide more relevant and personalised search results based on user history, location, and other factors.
- While AI has the potential to increase efficiency, it can cause harm through:
  - User account compromise (confidentiality risk)
  - Disclosure of confidential information (confidentiality risk)
  - Providing inaccurate responses (integrity risk).

Dark side of generative AI

- **Helping cybercriminals to create believable phishing and BEC scams**
- Deepfake Images, videos & voice recordings
- **Data privacy/confidentiality impacts**
- Fake product reviews
- Mis-information
- Romance fraud bots





Security Awareness Training Blog

5
Feb

Social Engineering Masterstroke: How Deepfake CFO Duped a Firm out of $25 Million

Stu Sjouwerman

Check out this one line for a moment…"*duped into attending a video call with what he thought were several other members of staff, but all of whom were in fact deepfake recreations.*"

In a worrying display of social engineering sophistication, a multinational company was defrauded of $25 million through an intricately planned deepfake scam. This scam brilliantly utilized deepfake technology to impersonate the company's Chief Financial Officer (CFO) during a video conference call, as reported by the Hong Kong police.

The scam unfolded when a finance worker at the company was lured into a video call, believing he was joining several colleagues for a meeting. In a revelation by the Hong Kong police, it was disclosed that the supposed colleagues were nothing more than deepfake fabrications. OUCH.

Subscribe To Our Blog

Email

Enter Your Email Address

Notification Frequency

○ Instant
● Daily
○ Weekly
○ Monthly

Security Awareness Training Blog RSS Feed

Source: https://blog.knowbe4.com/social-engineering-masterstroke-how-deepfake-cfo-duped-a-firm-out-of-25-million

How to protect yourself from AI generated scams

- Remember the basic indicators of a scam:
  - Contact email address / phone number correct
  - Created an emotional reaction
  - Unsolicited unexpected
- Always critically analyse online content. If in doubt, contact the person directly using details you have sourced independently.
- Create family codeword or password
- Limit the amount of public content available about you online - social media profiles on private

Cyber considerations around the use of AI

- Assess how your use of AI could impact the confidentiality and privacy of information
- Consider whether your use could impact your organisation's reputation
- Be cautious of using your work credentials to sign up for free/external AI systems and chatbots
- Be aware of potential inaccuracies, biases and misinformation from free/external AI systems
- For decision makers – ensure information security risk assessments are conducted before implementing any new AI technologies

Adopt a cyber resilience strategy

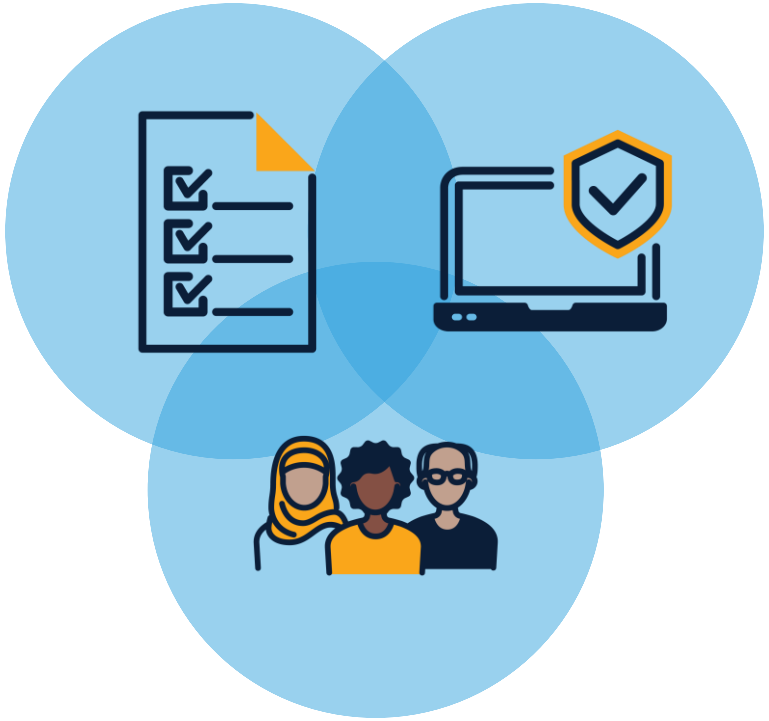
Cyber resilience: the ability to continuously deliver business objectives and organisational services despite cyber incidents, events and attacks.

Building cyber resilience

PROCESSES

Is there a cyber security policy? What does it cover and are staff following the practises?

Is there a cyber incident response plan in place? Has it been tested?



TECHNOLOGY

What risks do the technologies pose? Is the organisation running unsupported or outdated software? Are regular backups maintained and tested

Does the IT manager/provider know what the *ACSC Essential Eight* is? Can maturity be assessed?

PEOPLE

Are staff trained to recognise and respond to cyber attacks?

Digital Health Cyber Champions Network

An initiative from Australian Government
Australian Digital Health Agency

Digital health security awareness courses

- The Australian Digital Health Agency has developed a free eLearning course for people who work in healthcare.
- The Digital Health Security Awareness course has been developed by the Agency's cyber security team, in consultation with representatives from a range of healthcare settings and disciplines, including medicine, nursing, pharmacy, practice management and allied health.

Source: https://training.digitalhealth.gov.au/

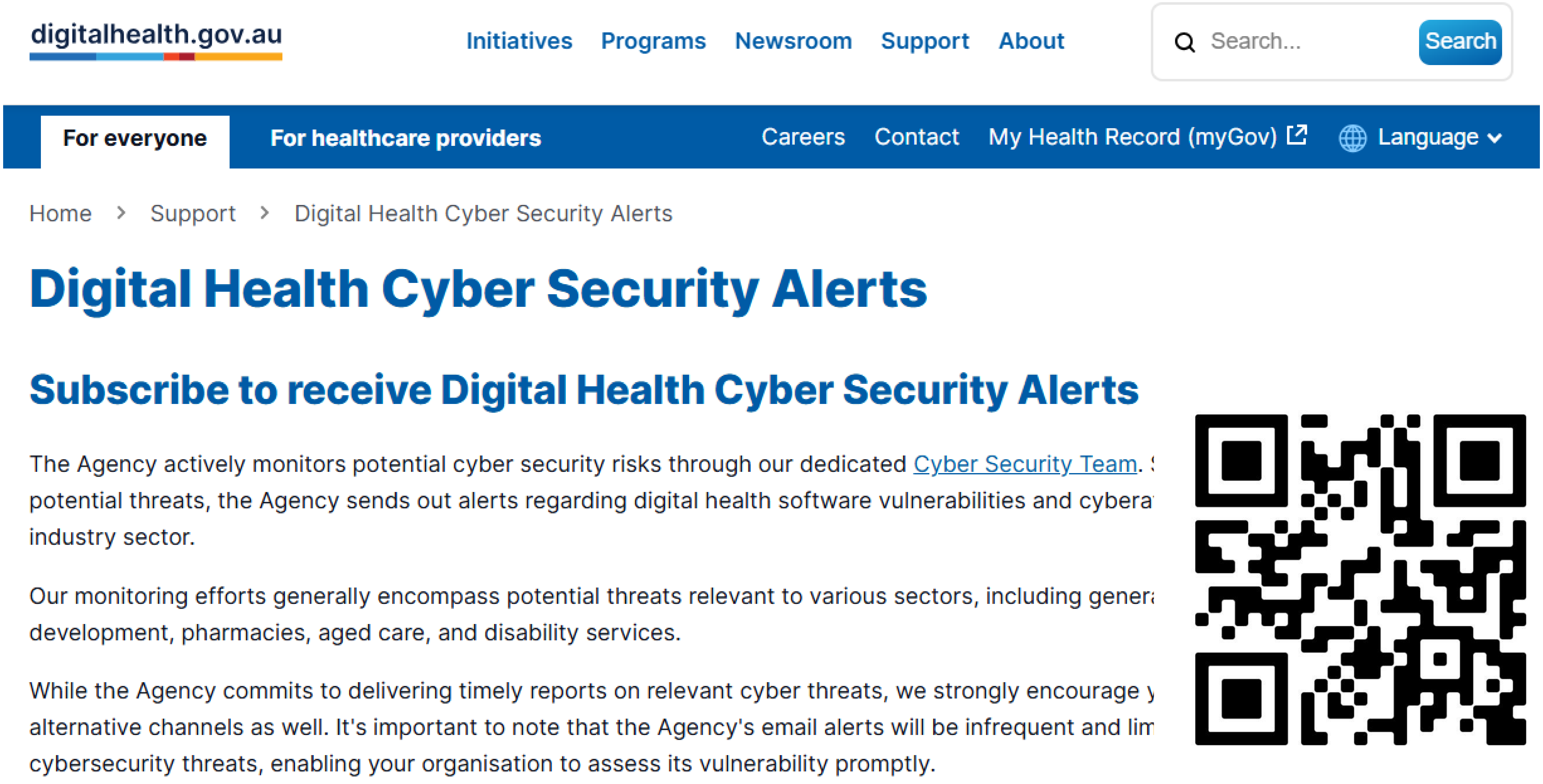
Additional digital health courses

Using online conferencing and telehealth technologies securely

Cyber security considerations when working remotely or working from home

Australian Government
Australian Digital Health Agency

Source: https://training.digitalhealth.gov.au/



Digital Health Cyber Security Alerts

Subscribe to receive Digital Health Cyber Security Alerts

The Agency actively monitors potential cyber security risks through our dedicated Cyber Security Team. potential threats, the Agency sends out alerts regarding digital health software vulnerabilities and cybera industry sector.

Our monitoring efforts generally encompass potential threats relevant to various sectors, including gener development, pharmacies, aged care, and disability services.

While the Agency commits to delivering timely reports on relevant cyber threats, we strongly encourage alternative channels as well. It's important to note that the Agency's email alerts will be infrequent and lim cybersecurity threats, enabling your organisation to assess its vulnerability promptly.

Australian Government
Australian Digital Health Agency

https://www.digitalhealth.gov.au/support/digital-health-cyber-security-alerts

Building the future with confidence

- Security and Privacy in healthcare should be reflexive, evolving, accessible, user friendly and implemented across the continuum.
- Healthcare technology is secure by design and secure by default
- Privacy by design across the software and information life cycle
- Routinely assessed for cyber security risks and protected to ensure its safe, secure and timely use
- Confidentiality, integrity and availability should be placed at the forefront when developing health technology
- A secure healthcare ecosystem is one that is sustained by active partnership and information sharing between entities
- Preparedness response, resilience strategies to enable confidentiality, integrity and availability of healthcare systems

Bp Premier
SUMMIT 2025

Questions & Answers

Contact

Australian Digital Health Agency

WEB:	digitalhealth.gov.au
EMAIL:	help@digitalhealth.gov.au
PHONE:	General enquiries 1300 901 001
	My Health Record Helpline 1800 723 0471

in	Australian Digital Health Agency
f	@AuDigitalHealth
X	@AuDigitalHealth

Bp Premier
SUMMIT 2025

Thank you for joining us!

Our Bp Summit Presentations and Resources are available via our Knowledge Base

Protecting YOUR Practice from Cyber Threats

Danielle Pentony & Tracey Weeks