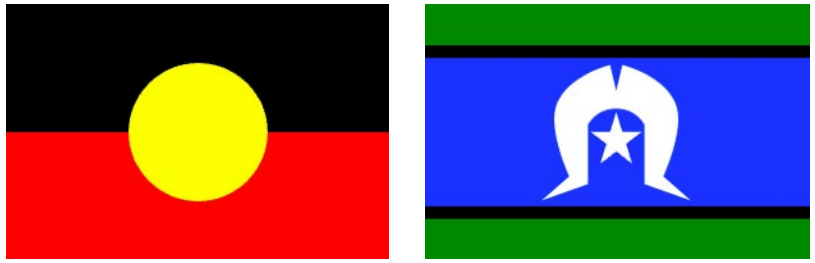
Securing the future

Cyber security and My Health Record insights

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

- Beyond the adoption of electronic medical records or new software
- Reimagining engagement with patients, consumers and the broader community
- Not a one-size-fits-all proposition
- Making healthcare accessible

Navigating the Digital Frontier

- Connecting technology systems and sharing data
- Improving accessibility, promoting preventive care, and enhancing patient engagement
- Technology is the enabler, strategy is the navigator

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

Why we need to talk about cyber security

- 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

Common cyber threats

Phishing

Business Email Compromise (BEC)

Ransomware

Phishing

Types of Phishing

Email

SMS (smishing)

Phone call (vishing)

QR code (quishing)

Sydney man charged with sending 17m scam texts

Impersonated Australia Post and Linkt to steal credit card details.

By Denham Sadler on Dec 14 2023 12:01 PM

A Sydney man has been charged with allegedly sending more than 17 million scam SMS messages impersonating the likes of Australia Post and Linkt to obtain the credit card details of unsuspecting victims.

Detectives from NSW Police's Cybercrime Squad executed a search warrant in Moorebank in Sydney's west on Tuesday morning, and arrested a 39-year-old man in relation to the alleged

A 39-year old Sydney man was arrested for sending 17 million scam texts. Photo: NSW Police

Source: https://ia.acs.org.au/article/2023/sydney-man-charged-with-sending-17m-scam-texts.html

Why are phishing attacks so successful?

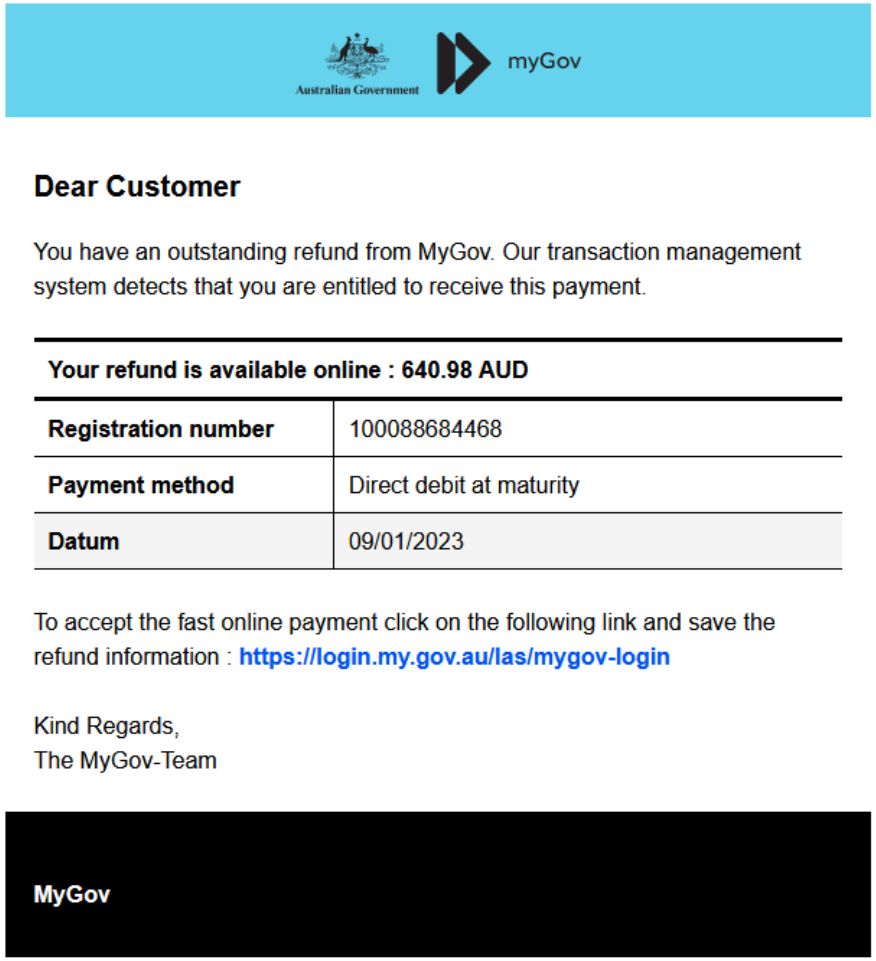
44% of people think an email is safe when it contains familiar branding

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

Source: Proofpoint (2023) State of the Phish Report

How to identify a phishing email

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



Australian Government myGov

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

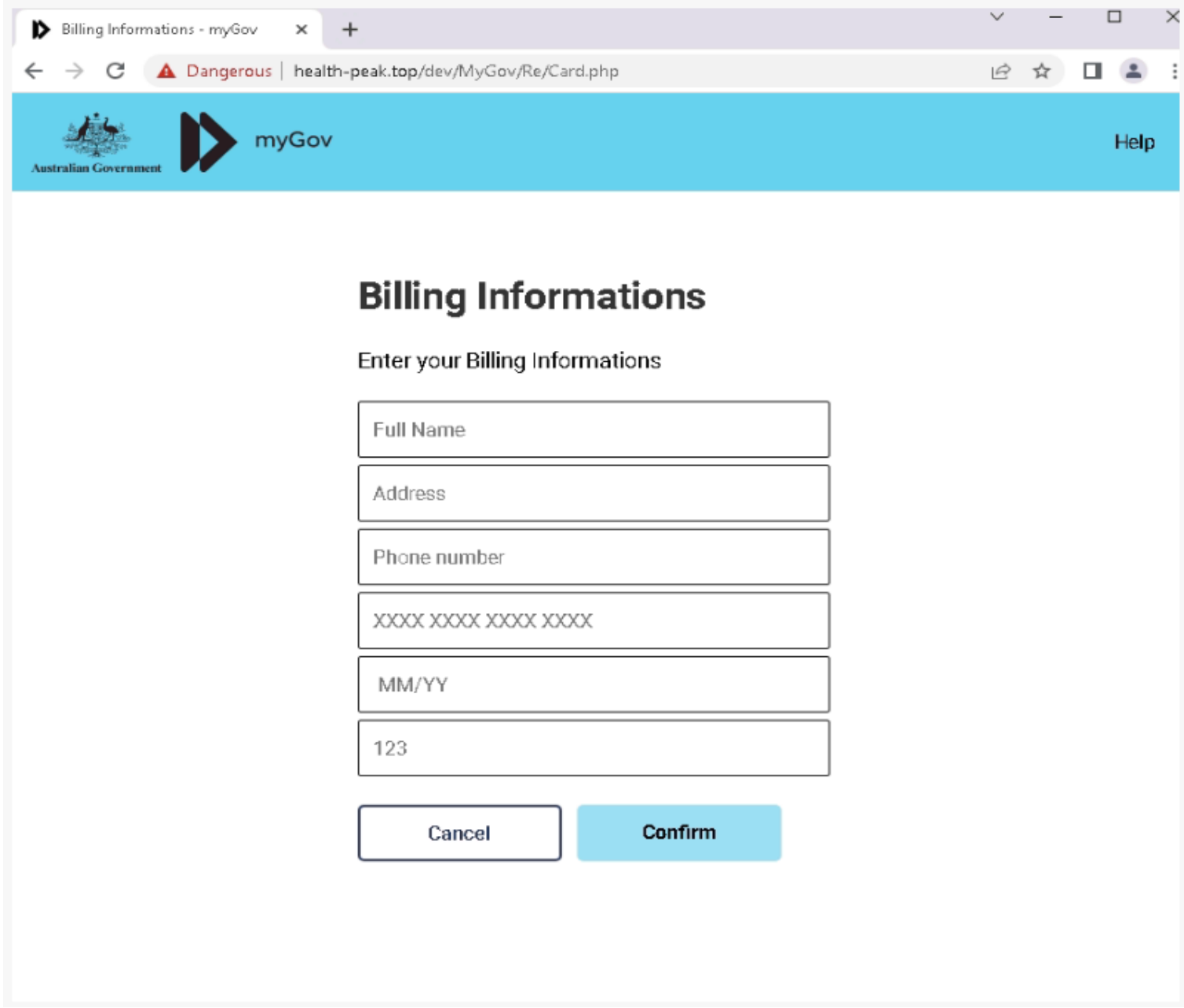
To accept the fast online payment click on the following link and save the refund information : **https://login.my.gov.au/las/mygov-login**

Kind Regards,
The MyGov-Team

MyGov

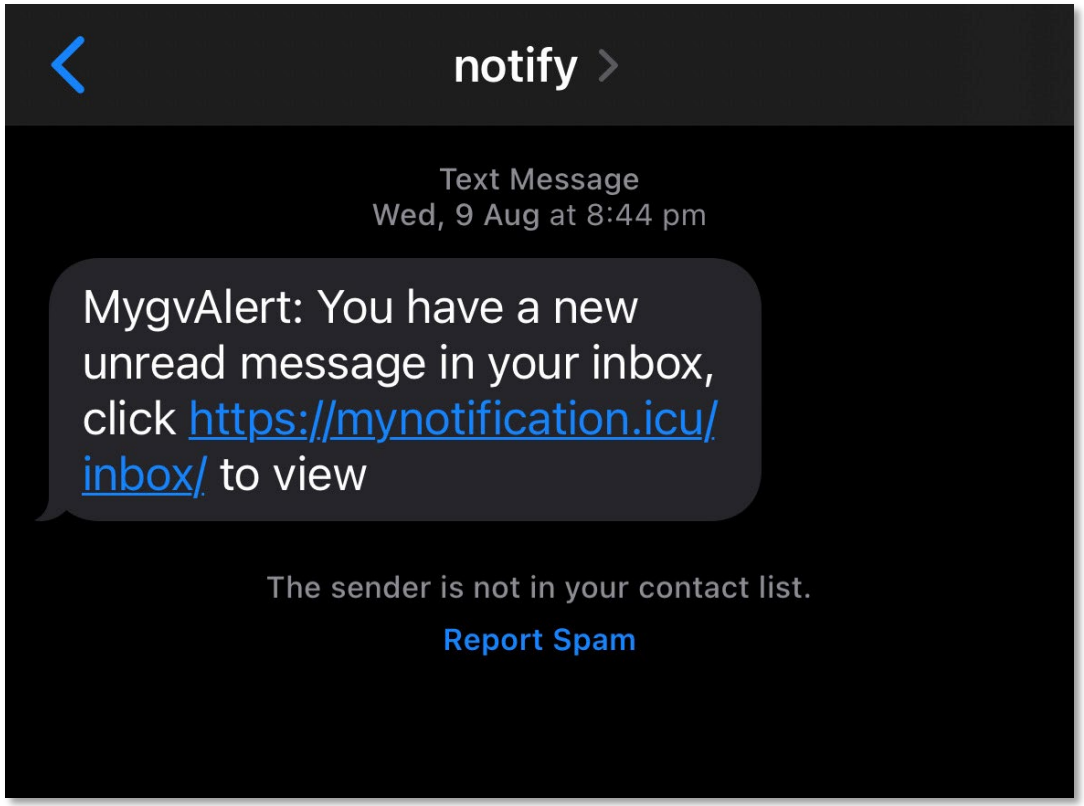
1. The email address is incorrect
2. Generic greeting (dear customer)
3. Unsolicited or unexpected
4. Too good to be true
5. *May* contain spelling, grammar or formatting errors.
6. It has a malicious link or attachment:
   - Directs to a website that steals information
   - Installs malware

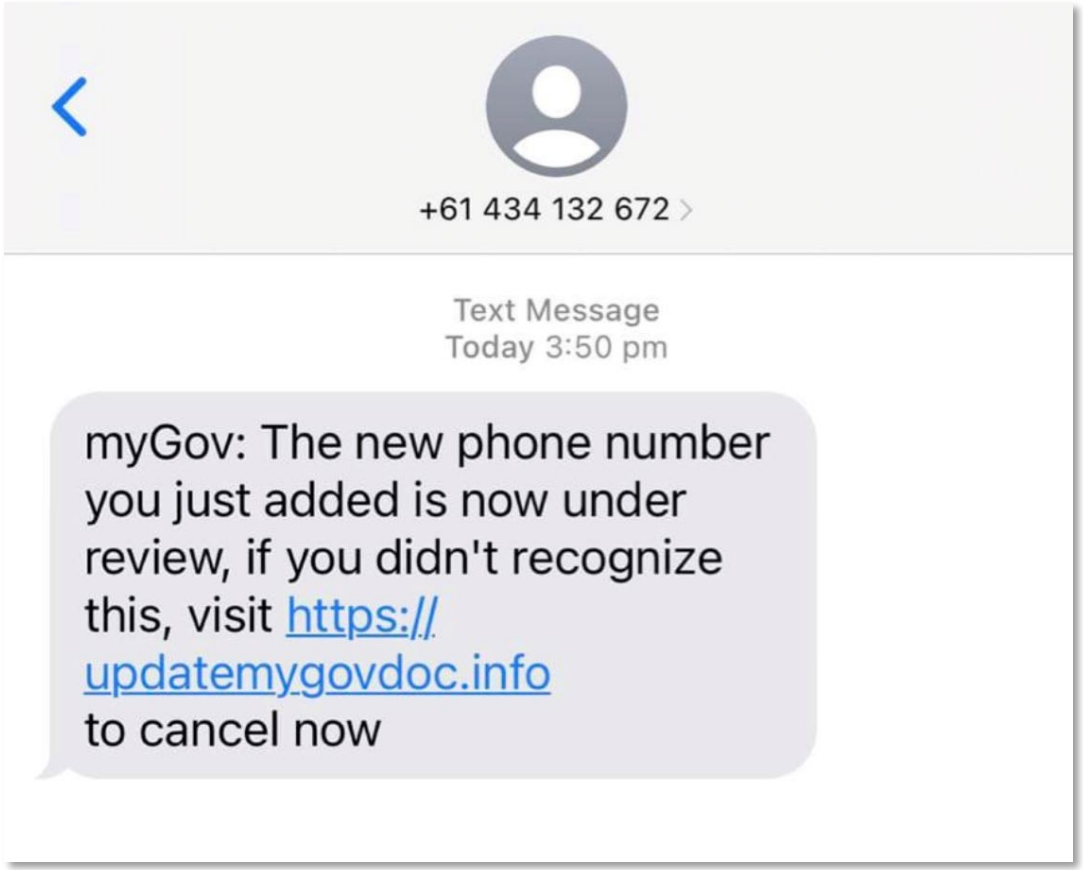
Source: Mail Guard (2023)



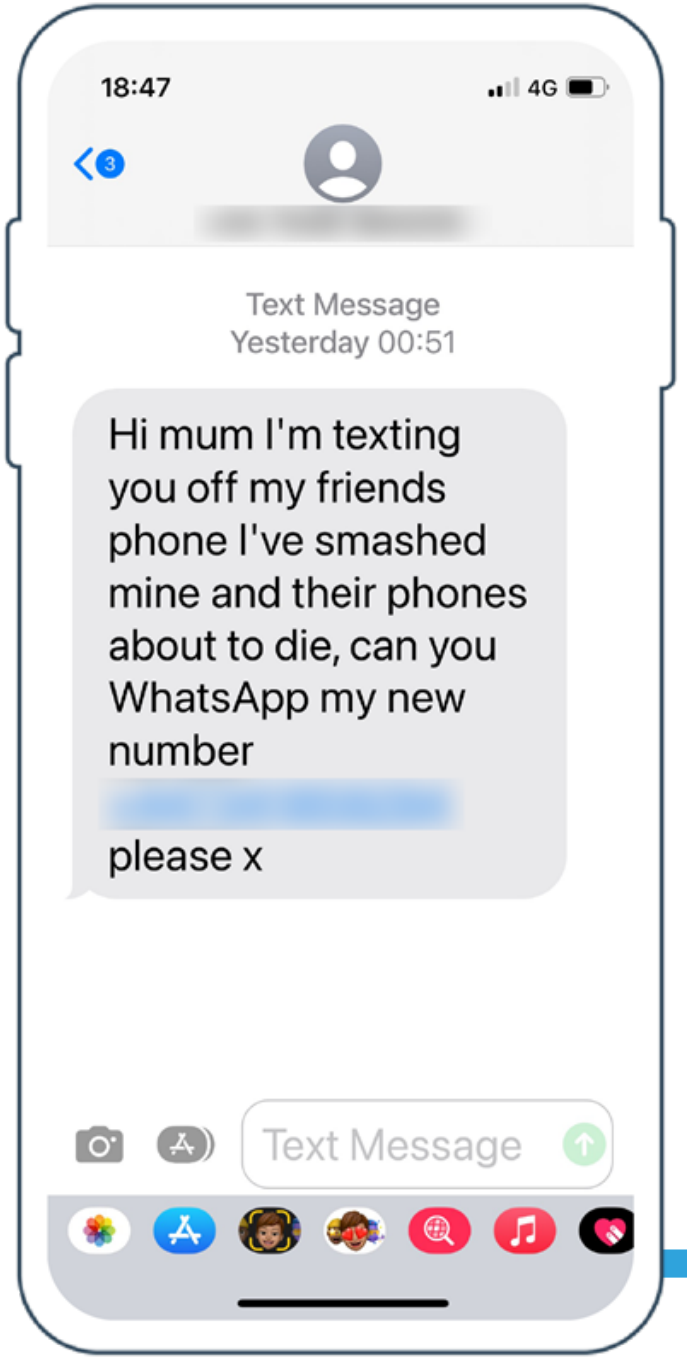
Source: Mail Guard (2023)

Smishing or safe?

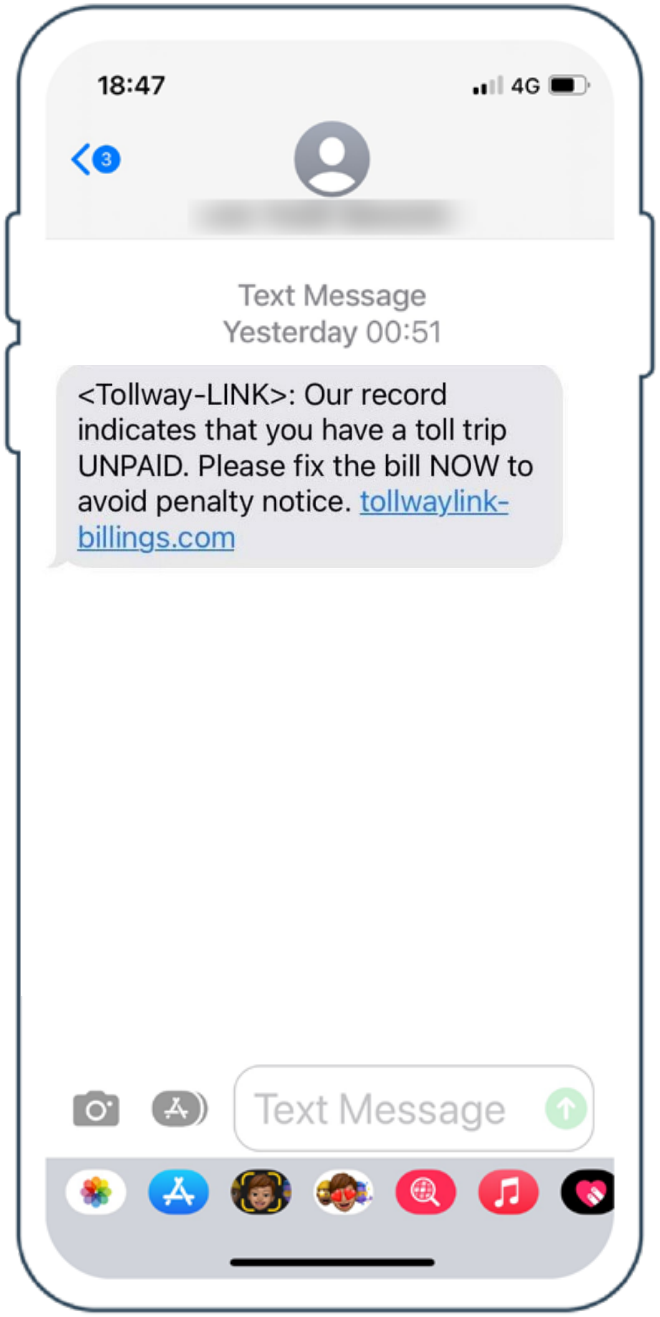


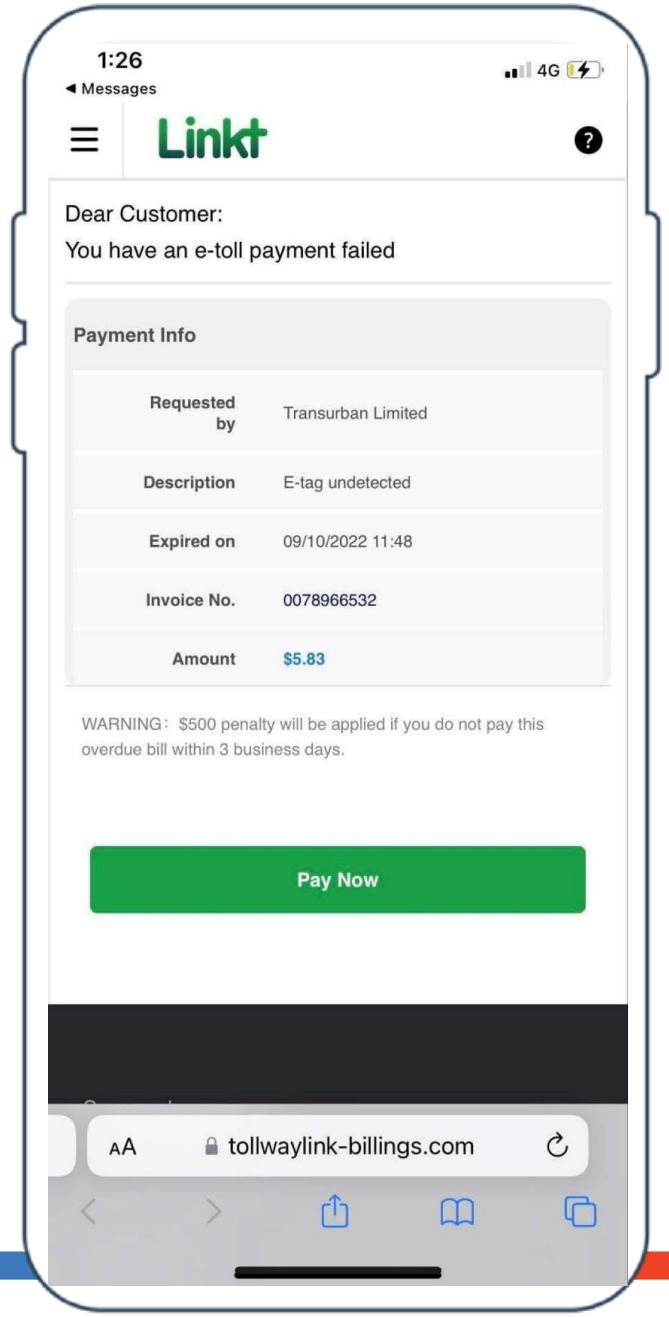


SAFE

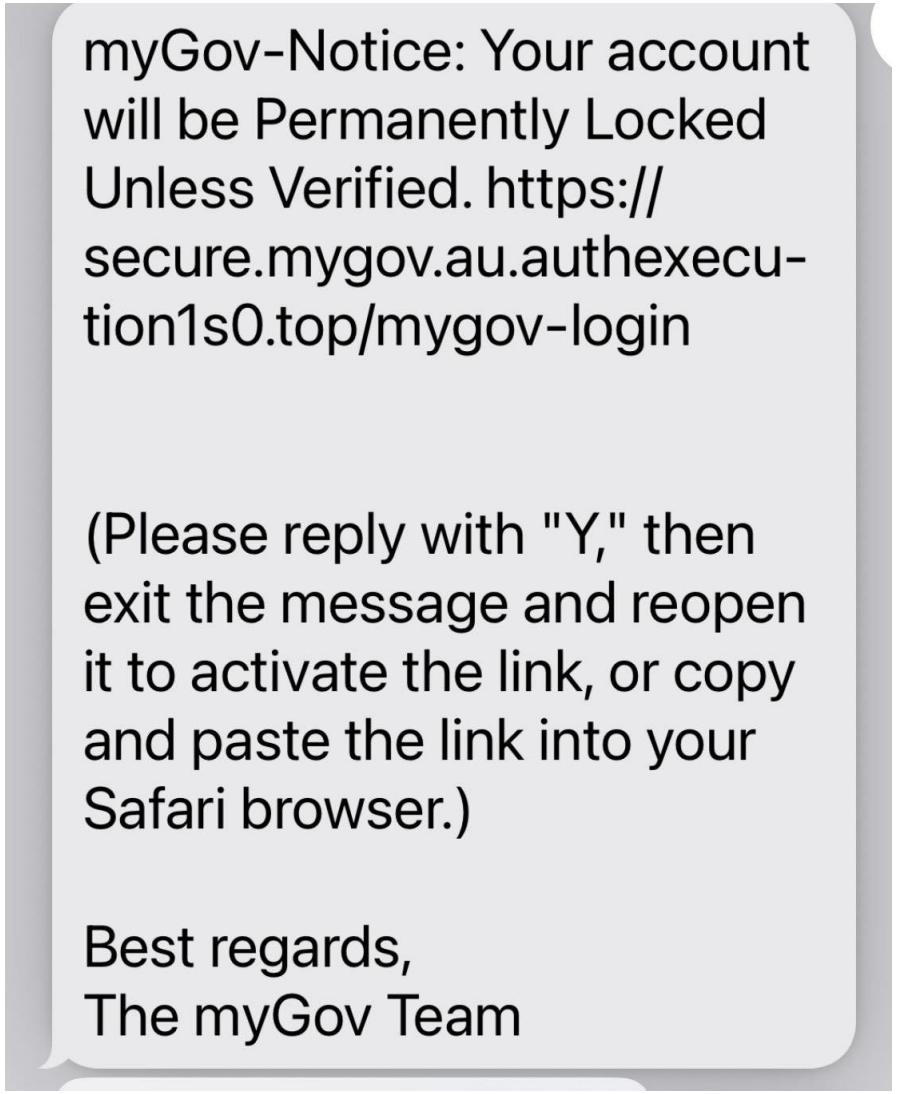

18:47
4G
Text Message
Yesterday 00:51
Hi mum I'm texting you off my friends phone I've smashed mine and their phones about to die, can you WhatsApp my new number
please x
Text Message

UNSAFE


18:47
4G
3
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
Text Message


1:26
Messages
4G
Linkt
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.
Pay Now
AA
tollwaylink-billings.com

SAFE


myGov-Notice: Your account will be Permanently Locked Unless Verified. https://secure.mygov.au.authexecu-tion1s0.top/mygov-login
(Please reply with "Y," then exit the message and reopen it to activate the link, or copy and paste the link into your Safari browser.)
Best regards,
The myGov Team

UNSAFE

Updated MFA requirements

M

MFA_Authenticater <no-reply_MFAauthentication@micosoft.mfaupdate.com>

To Kym Clarke

Reply | Reply All | Forward

Wed 25/10/2023 1:31 PM

Follow up. Completed on Wednesday, 25 October 2023.

CAUTION: **Cyber Security Awareness**: This email originated from outside our organisation. Before acting on instructions contained in the email, clicking on links or opening attachments, please ensure that you recognise the sender and that you are confident the content is authentic and safe. If you suspect the email is not legitimate, then click on the **Report Message** option.

Hello

You are required to update your MFA authorization for security purposes.

Please scan the code below to update.

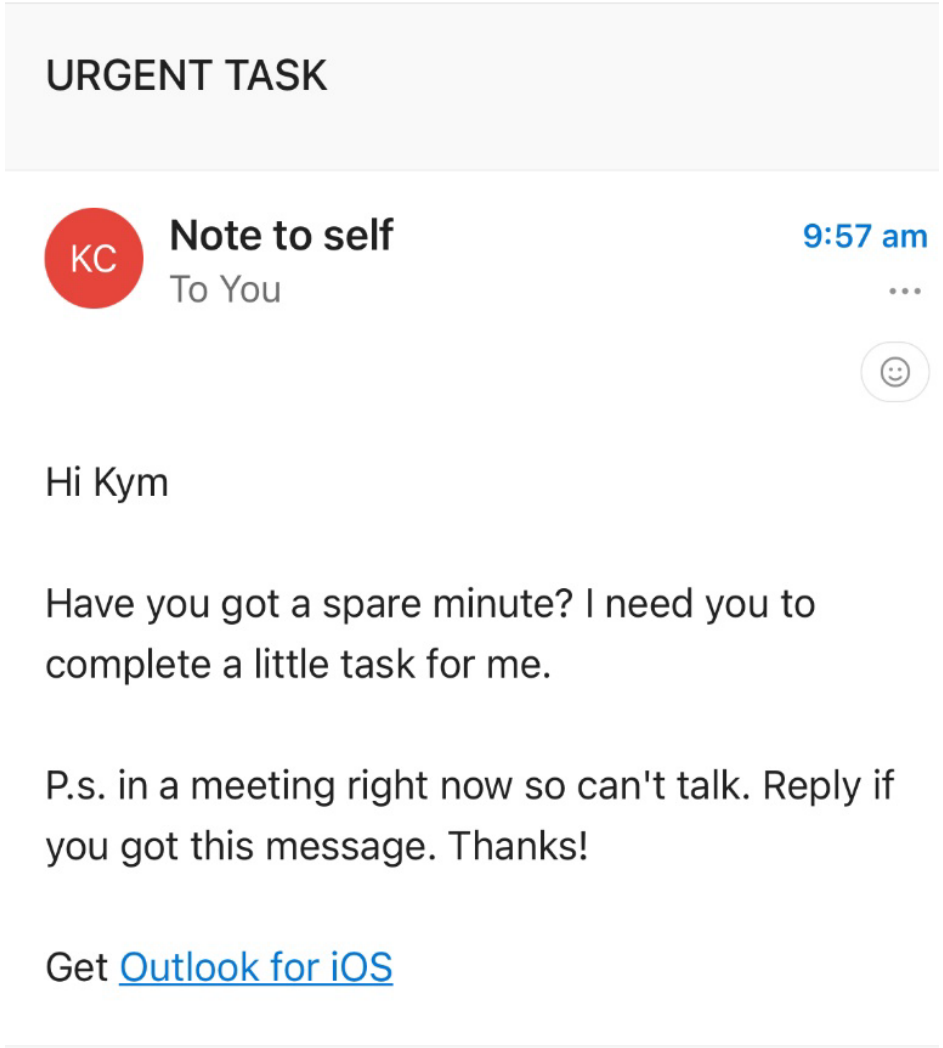
QR code not working?
Not worries. Follow the link below to update.

UPDATE NOW

$84 M

total self reported losses from **Business Email Compromise** in Australia last financial year (2023-2024)

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



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

“Ransomware remains a highly destructive cyber crime threat”

- Australian Cyber Security Centre 2023

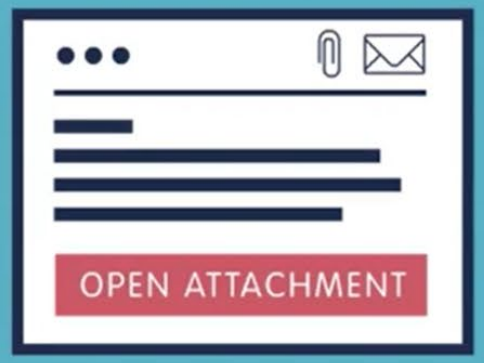
“Compromised credentials were the number one root cause of ransomware attacks against healthcare organisations”

- Sophos State of Ransomware in Health 2023

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)

Reasons why cyber attacks are successful and how we need to retrain our brain…

We’re very busy and stressed

52% of people surveyed admitted that stress causes them to make more mistakes

47% of those who had fallen for a phishing attack attributed it to being distracted

Source: https://www.tessian.com/blog/why-we-click-on-phishing-scams/

Our brains try to make us efficient as possible

“Aoccdrnig to a rscheearch at Cmabrigde Uinervtisy, it deosn’t mttaer in waht oredr the ltteers in a wrod are, the olny iprmoetnt tihng is taht the frist and lsat ltteer be at the rghit pclae. The rset can be a toatl mses and you can sitll raed it wouthit porbelm. Tihs is bcuseae the huamn mnid deos not raed ervey lteter by istlef, but the wrod as a wlohe.”

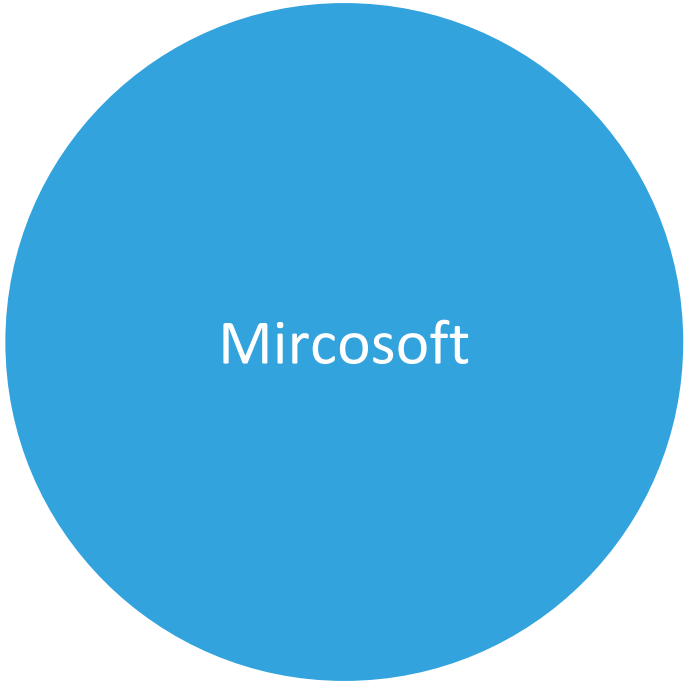
Source: https://www.dictionary.com/e/typoglycemia/

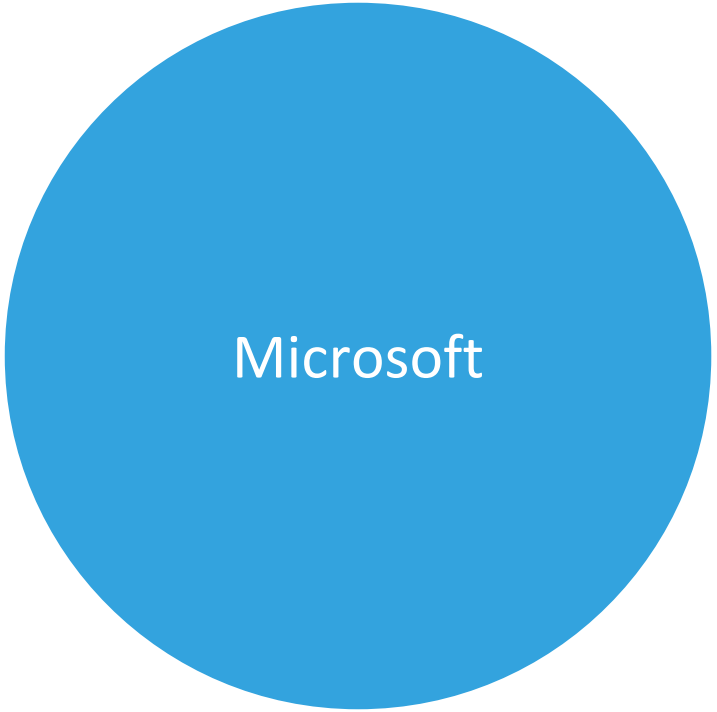
Which doesn’t help when trying to analyse phishing scams…

“According to a researcher (sic) at Cambridge University, it doesn't matter in what order the letters in a word are, the only important thing is that the first and last letter be at the right place. The rest can be a total mess and you can still read it without problem. This is because the human mind does not read every letter by itself but the word as a whole.

Source: https://www.dictionary.com/e/typoglycemia/

Spot the difference





As humans we are instinctively biological than logical

Authority

Is the message claiming to be from someone official?

Like your bank, a government department, a utility company, your doctor or a solicitor. Criminals pretend to be important people or organisations to trick you into doing what they want.

Urgency

Are you told you have a limited time to respond?

For example, 'within 24 hours' or 'immediately'. Criminals often threaten you with fines or other negative consequences.

Emotion

Does the message make you panic, fearful, hopeful or curious?

Cybercriminals use threatening language, make false claims of support, or tease you into wanting to find out more.

Scarcity

Is the message offering something that seems too good to be true?

Like concert tickets, money or a cure for medical conditions? Fear of missing out on a good deal or opportunity can make you respond quickly.

Events

Are you expecting to see a message like this?

To make their scam seem more real, criminals can exploit current news stories and events. For example, some cybercriminals pretend to be from the tax office at tax time to make their scam seem more relevant.

Source: Australian Cyber Security Centre (2023)

This is Westpac. We are seeing large sums of money being transferred from your account. We're suspending it immediately unless you can confirm your account details to us.

This is Microsoft, we have identified some security issues on your computer, we need to remote in to fix them

Hi there, this is the Australian Taxation Office. There is a serious matter regarding your unpaid taxation bill.

I know we only just started talking and we've never met but I think I'm falling in love with you

Congratulations Swiftie, you have won 2 tickets to the Taylor Swift concert. Click here to claim your prize

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?

Secure your accounts

- Use strong passwords
- Multi-factor authentication

Passwords

“Now I need a new name because someone guessed my owner’s password”.

How easy would it be to get your password?


HOLLY
The truth of the matter is, we need to do a better job

Top 15 passwords found in data breaches

123456	princess	nicole
12345	1234567	daniel
123456789	rockyou	babygirl
password	12345678	monkey
iloveyou	abc123	lovely

Source: The Most Common Passwords 2025 - More than 14.3 million passwords

How to create a strong passphrase

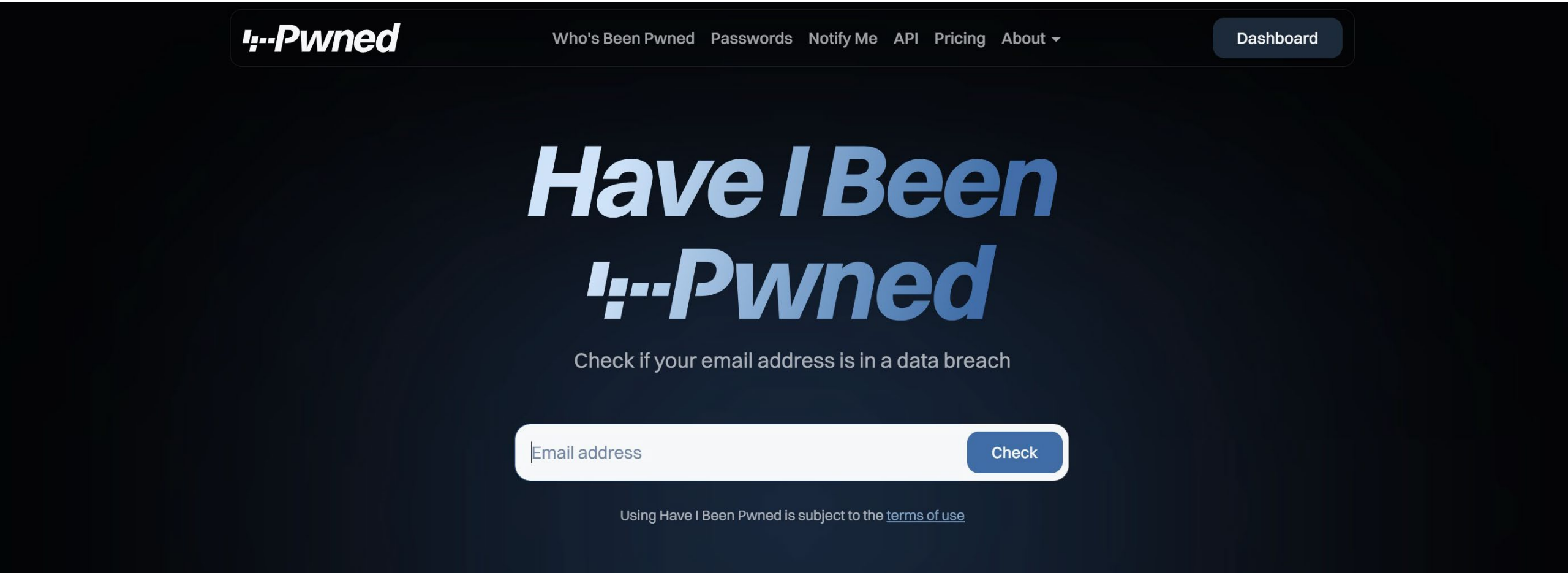
Four words mashed:

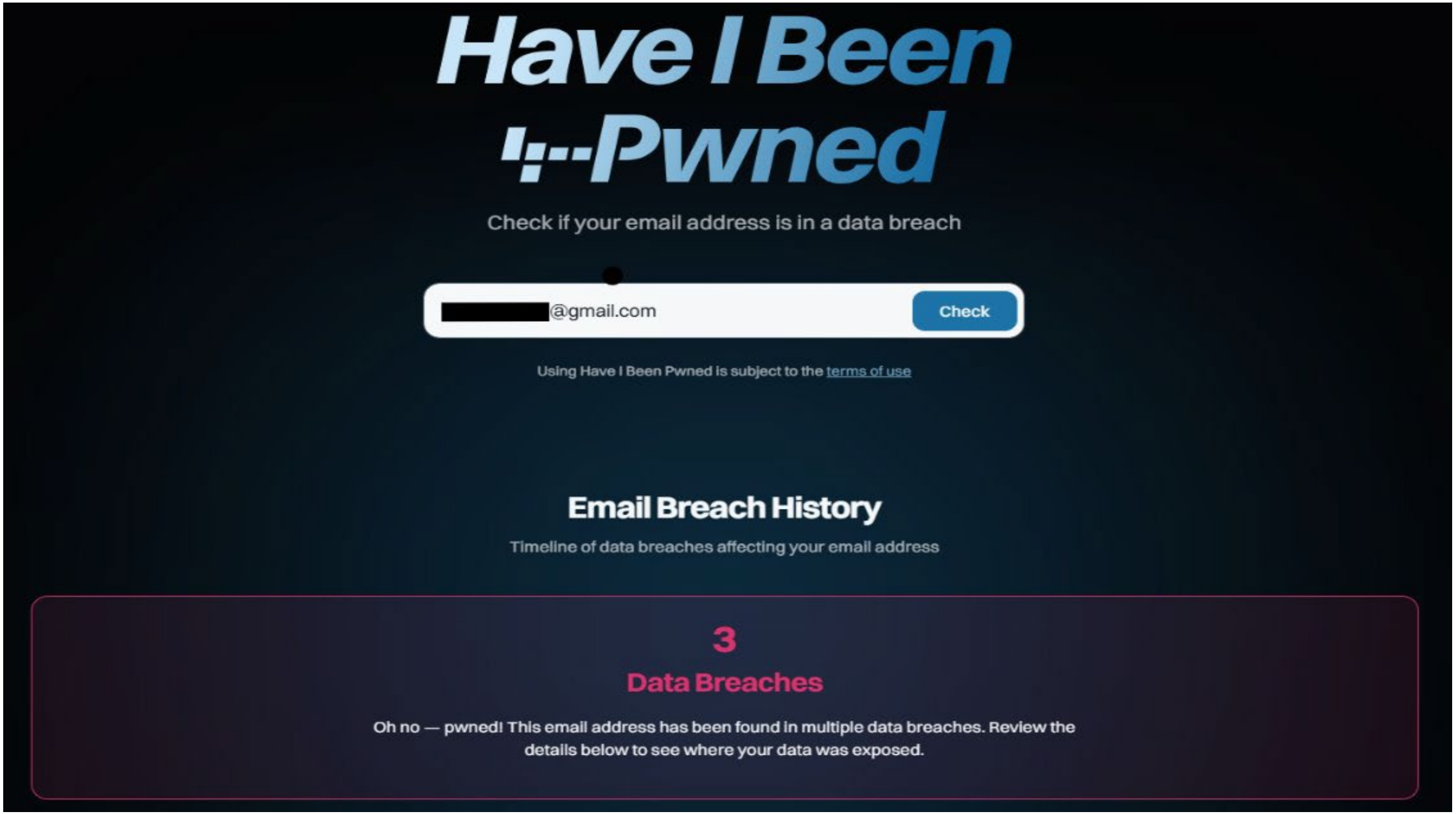
KittenChocolatePuppyHappy99!

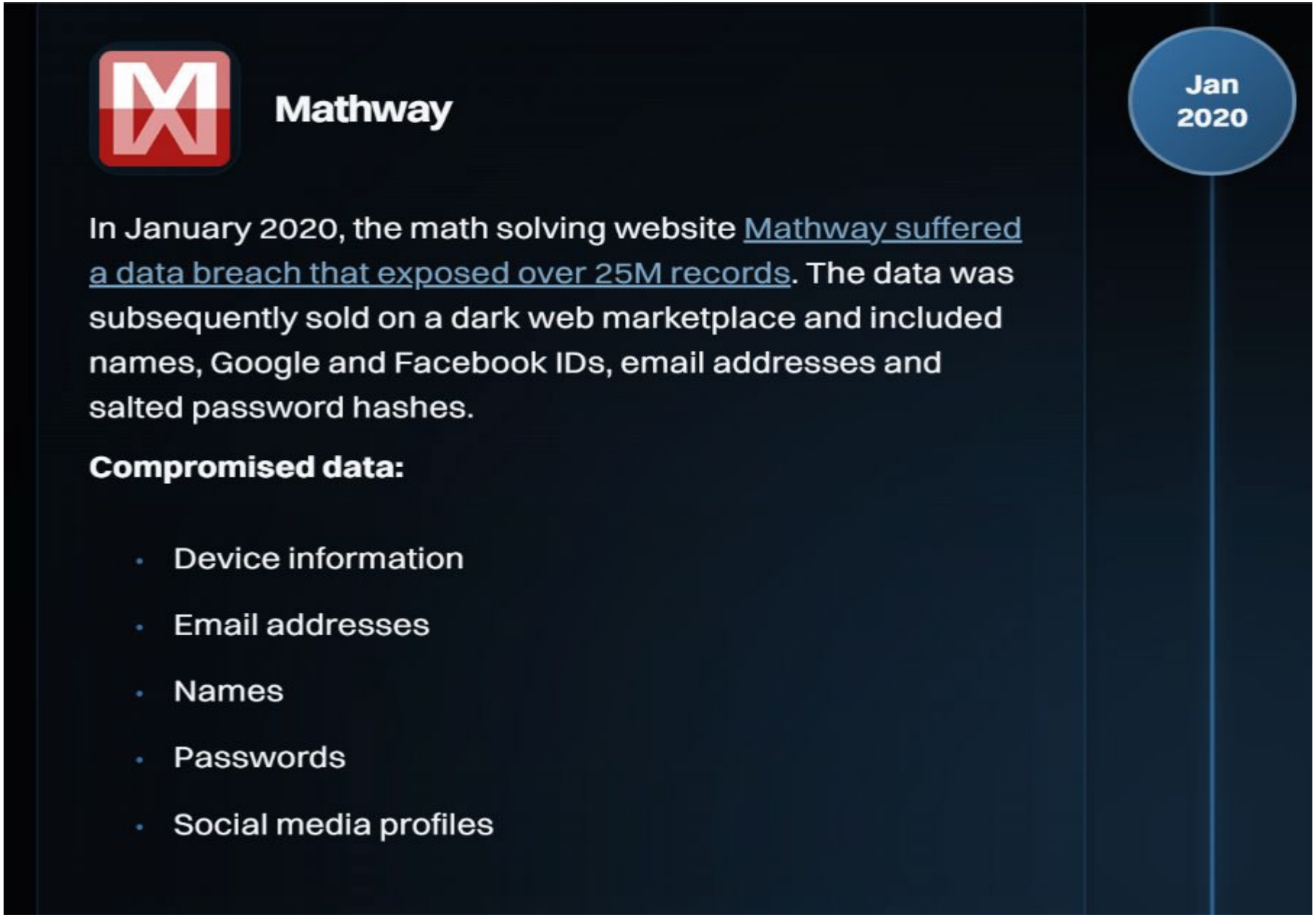
TortoiseTurtlePurpleApple#35

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

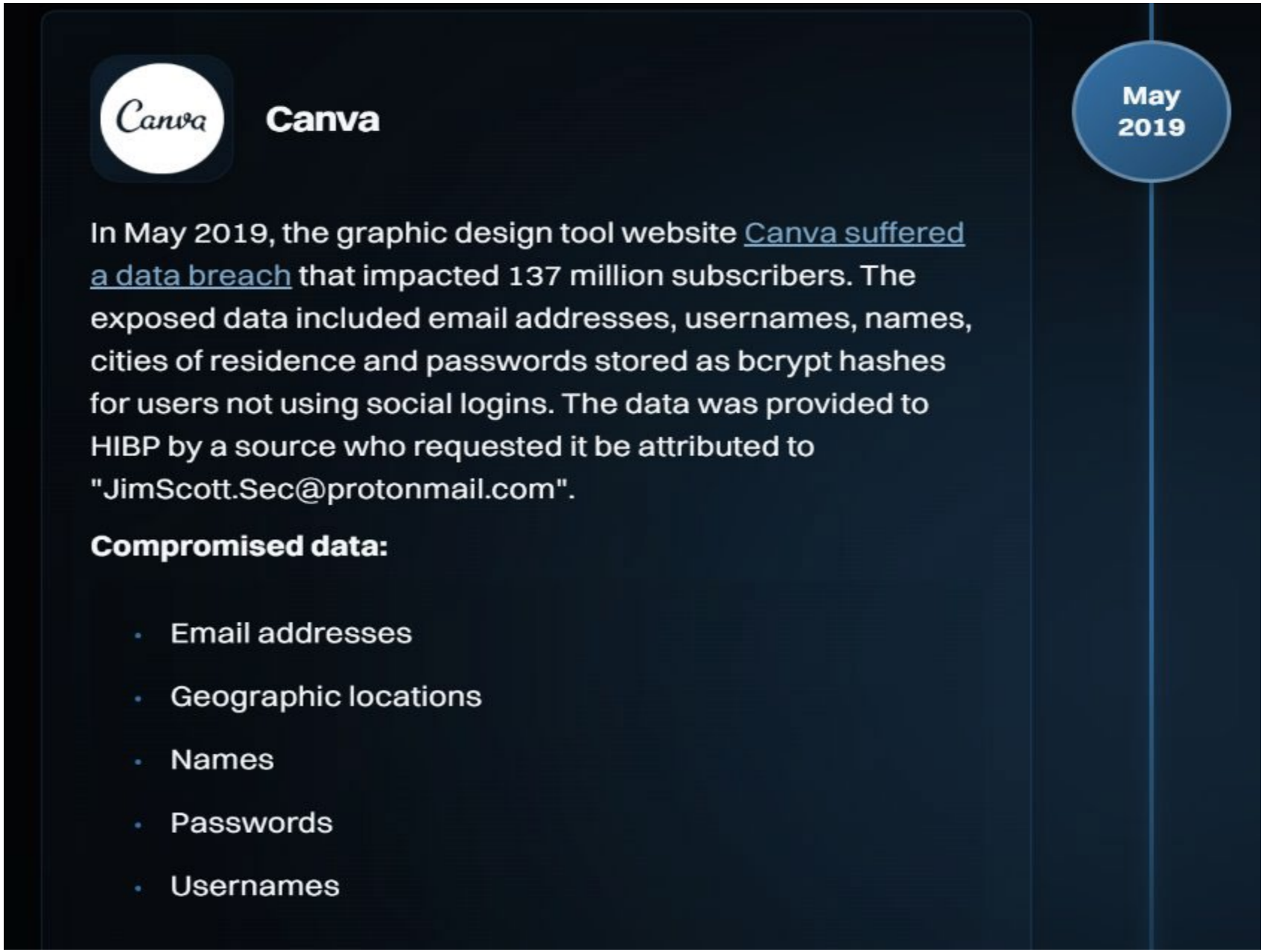
https://haveibeenpwned.com/



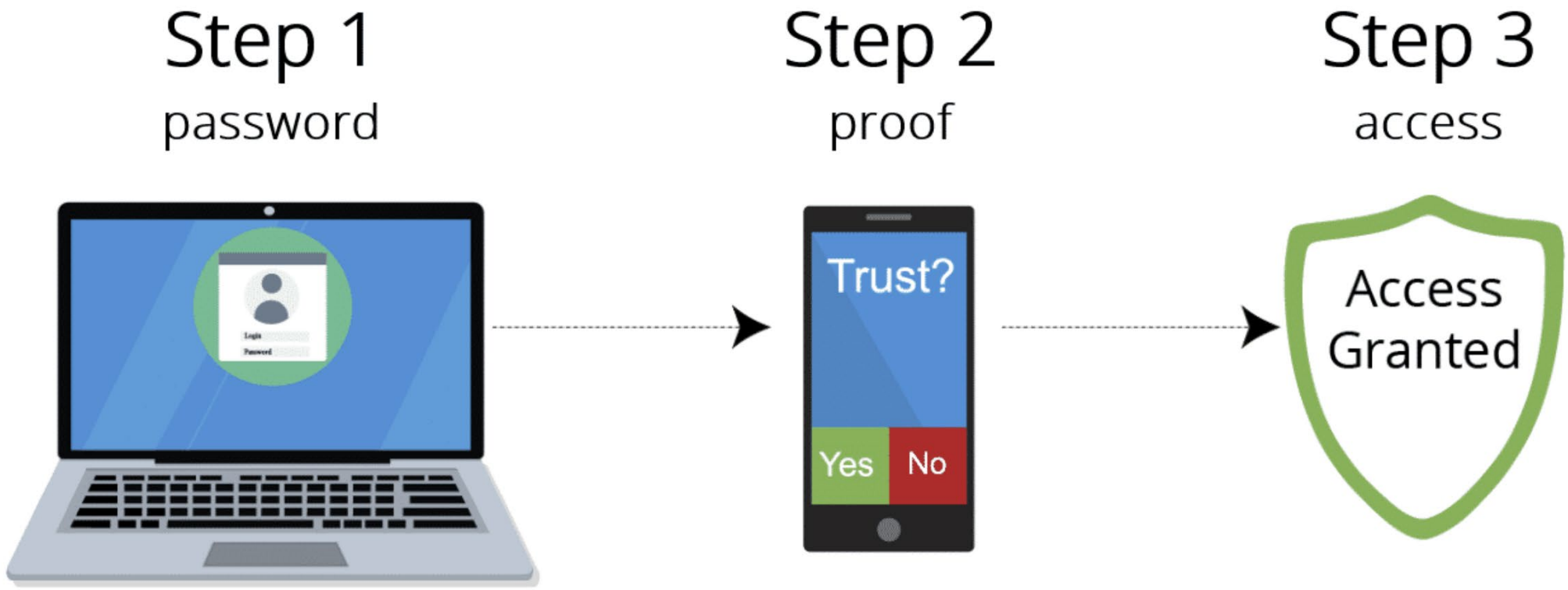

Have I Been Pwned
Check if your email address is in a data breach
[redacted]@gmail.com
Check
Using Have I Been Pwned is subject to the terms of use
Email Breach History
Timeline of data breaches affecting your email address
3
Data Breaches
Oh no — pwned! This email address has been found in multiple data breaches. Review the details below to see where your data was exposed.


Mathway
Jan 2020
In January 2020, the math solving website Mathway suffered a data breach that exposed over 25M records. The data was subsequently sold on a dark web marketplace and included names, Google and Facebook IDs, email addresses and salted password hashes.
Compromised data:
Device information
Email addresses
Names
Passwords
Social media profiles


Sept
2019
zynga
Zynga
In September 2019, game developer Zynga (the creator of Words with Friends) suffered a data breach. The incident exposed 173M unique email addresses alongside usernames and passwords stored as salted SHA-1 hashes. The data was provided to HIBP by dehashed.com.
Compromised data:
Email addresses
Passwords
Phone numbers
Usernames
View Details


Canva
Canva
May 2019
In May 2019, the graphic design tool website Canva suffered a data breach that impacted 137 million subscribers. The exposed data included email addresses, usernames, names, cities of residence and passwords stored as bcrypt hashes for users not using social logins. The data was provided to HIBP by a source who requested it be attributed to "JimScott.Sec@protonmail.com".
Compromised data:
Email addresses
Geographic locations
Names
Passwords
Usernames

Multi-factor authentication (MFA) or two-factor authentication (2FA)



Source: Digital Health Security Awareness eLearning course

Lock your device when unattended to:

- Protect patient privacy and sensitive information
- Prevent unauthorised use
- Avoid data being tampered with
- Reduce the chance of cyber attacks
- Protect your practice’s reputation

Tracey’s jingle to locking your computer…

Press Alt, Ctrl + Delete before you leave your seat

Or, ‘Windows’ + L, works as well!

Adopt a cyber resilience strategy

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

Digital Health **Cyber Champions** Network

An initiative from

Australian Government
Australian Digital Health Agency

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.

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

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. S
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 genera
development, pharmacies, aged care, and disability services.

While the Agency commits to delivering timely reports on relevant cyber threats, we strongly encourage y
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.

My Health Record insights

Zac Woodalba

Australian Government

Australian Digital Health Agency

What is My Health Record?

An online summary of an individual's key health information

Personally controlled

Part of a national system

Accessible at all times

Protected

Who here is using My Health Record?

Yes, its deadly

No, not yet

My Health Record documents

Healthcare provider documents

- Shared health summaries
- Discharge summaries
- Event summaries
- Prescription and dispense records
- Specialist letters
- Pharmacist Shared Medicines List
- Diagnostic Imaging reports
- Pathology reports
- Goals of care
- eReferrals
- Residential care transfer reason
- Residential care health summary
- Residential care medication chart

Medicare information

- Prescription information
- Australian Immunisation Register
- Australian Organ Donor Register
- Medicare Services -MBS and DVA items

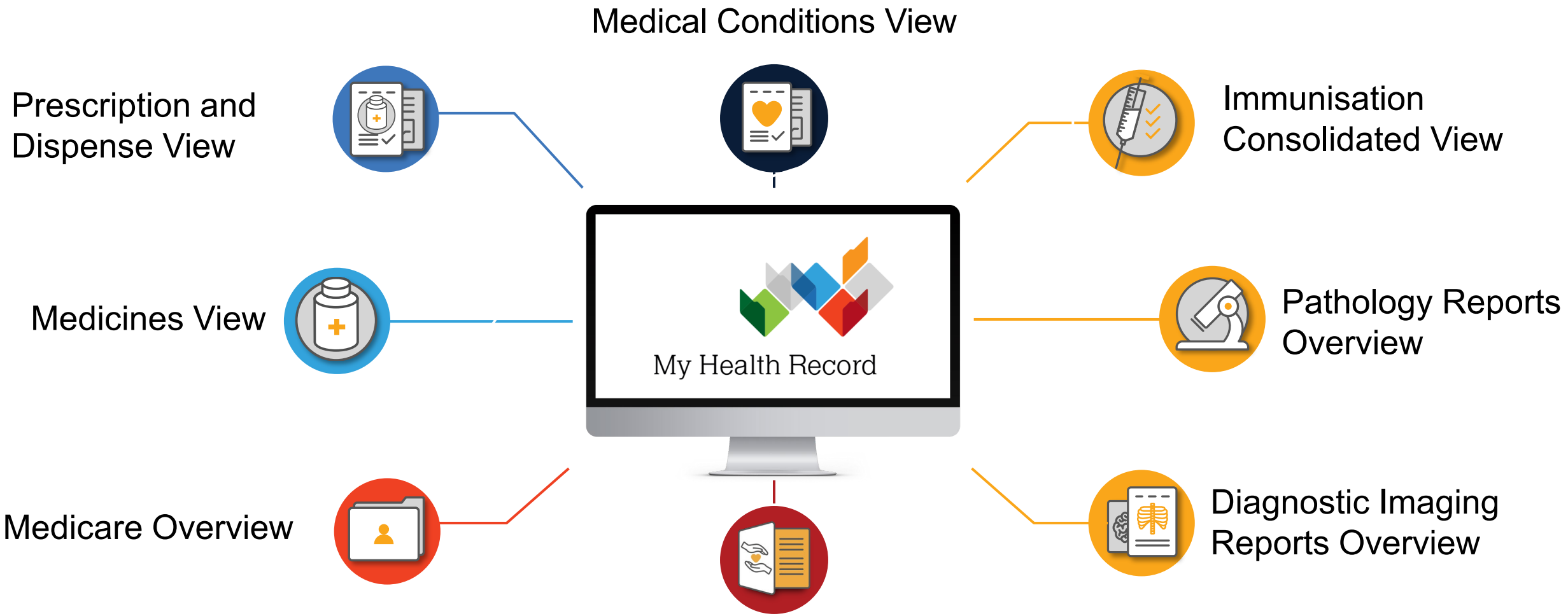
Consumer entered information

- Personal health summary
- Advance Care Planning documents
- Emergency contacts
- Childhood development

Shared with My Health Record

- Care and support plans
- MyMedicare registration

Overviews


Medical Conditions View
Prescription and Dispense View
Immunisation Consolidated View
Medicines View
My Health Record
Pathology Reports Overview
Medicare Overview
Diagnostic Imaging Reports Overview
Residential Care Transfer Overview

My Health Record - benefits

Quick, Centralised Access to Health Information

Safer, More Efficient Care

Better Health Management

Convenient and Secure Access

How to access My Health Record?

Healthcare providers

View

- Conformant software
- National Provider Portal

Upload

- Conformant software

Consumers

View

- Log in to My Health Record through myGov
- **my health** app
- Other conformant apps

Add information

- Log in to My Health Record through myGov
- Some information can be added through **my health** app

If a new patient comes into your clinic, how do you find out their story?

What do you think of Electronic Prescriptions?

Deadly

Not deadly

How do individuals use ASL?

An individual attends their preferred pharmacy and requests to be registered for an ASL

The individual attends the doctor and requires a prescription

If the individual chooses, an electronic prescription is provided and is automatically added to the ASL

The individual then presents to their preferred pharmacy, validates their identity, and medicine is dispensed from the ASL via conformant software (MySL)

The repeats, if any available, will be added to the ASL by the pharmacy

Did you know more pathology and radiology results will be on My Health Record soon?

Of course I did!

No idea

Any questions?

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

Australian Digital Health Agency

@AuDigitalHealth

@AuDigitalHealth