

Secure yourself after

# THE OPTUS DATA BREACH

Download these notes from

<https://u3anunawading.com.au/optus-data-breach-2022/>

# Structure of this session

1. What happened and were you affected?
2. What are the main risks?
3. How to protect yourself
  - a) Passwords & 2-factor authentication
  - b) Lock your SIM card
  - c) Change your driver's licence, passport, Medicare card?
  - d) Freeze your credit
  - e) Keep a watch – on bank accounts and email addresses
4. If you do become a victim ...
5. Scams noted so far

# Sources

- How to respond to a data breach notification from the Office of the Australian Information Commissioner
- Optus data breach scams from Scamwatch
- A step-by-step guide from experts at Macquarie and Western Sydney Universities

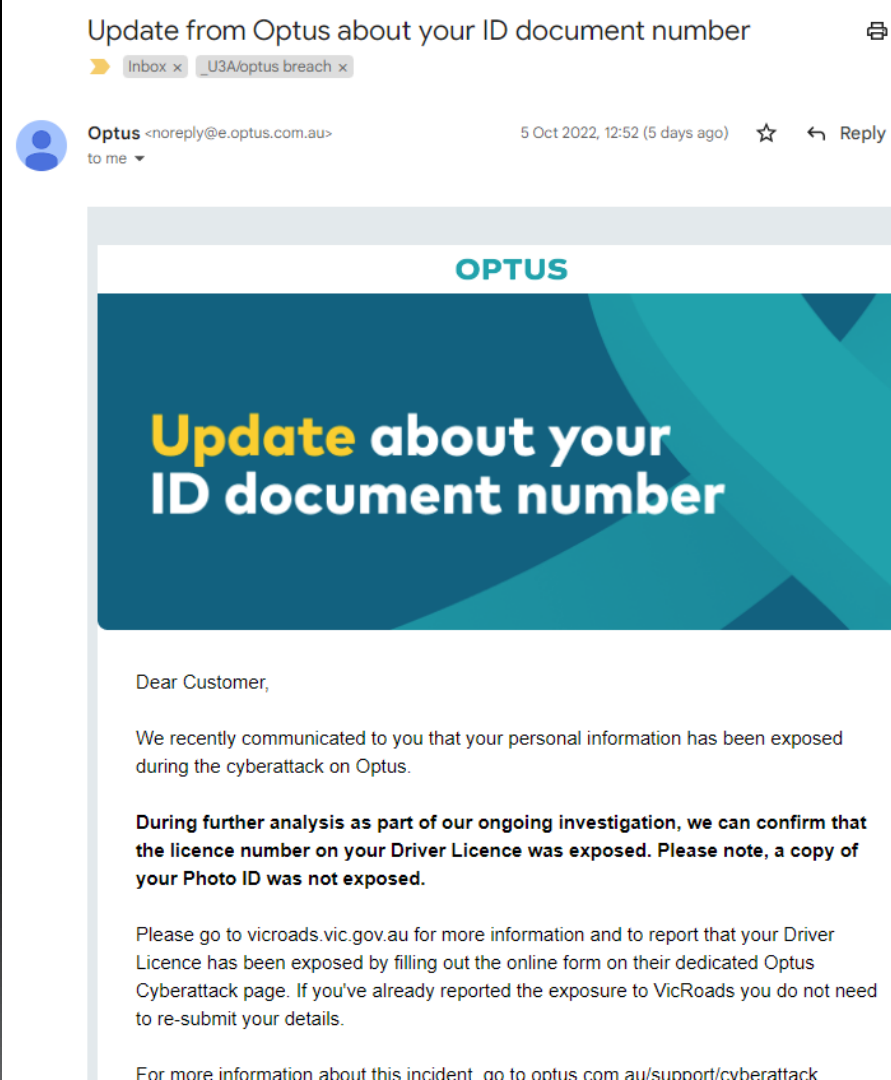


# 1. What happened?

- Optus announced on September 22 that identifying details of up to 9.8 million customers were stolen from their customer database.
- The details, dating back to 2017, include names, birth dates, phone numbers, email addresses, and – for some customers – addresses and driver’s licence or passport numbers.
- Around 10,000 customer details were posted on the “dark web”

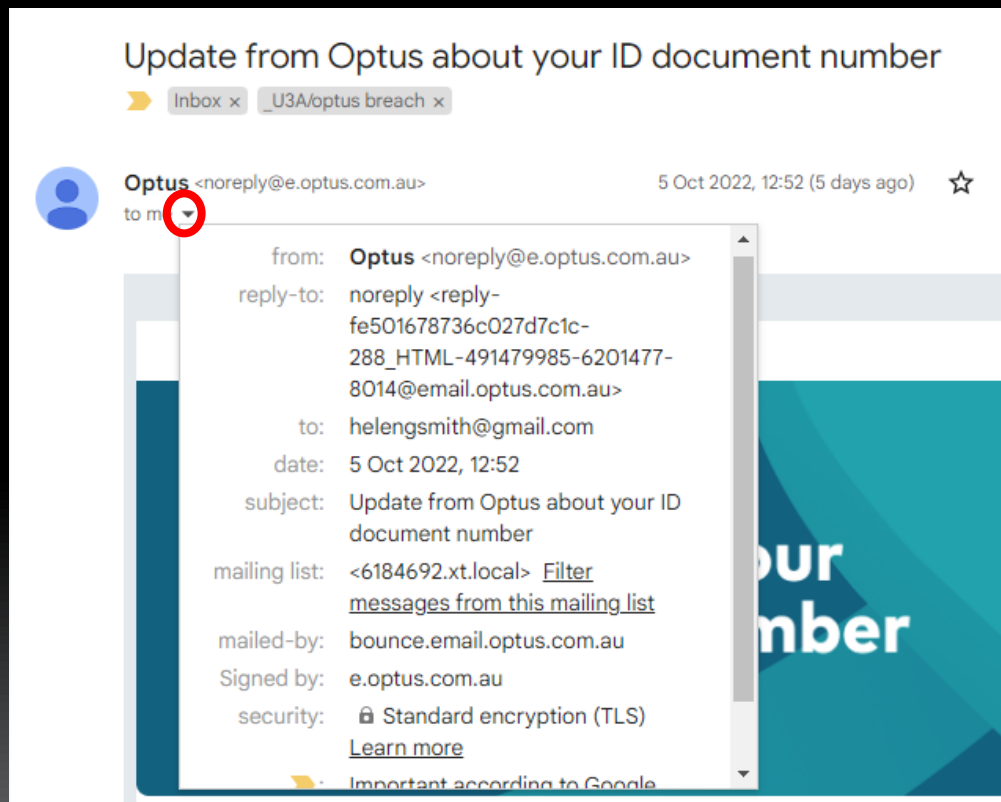
# Were you affected?

- If you were affected you should have had an email from Optus stating what information of yours was stolen.
- My driver licence number was “exposed”



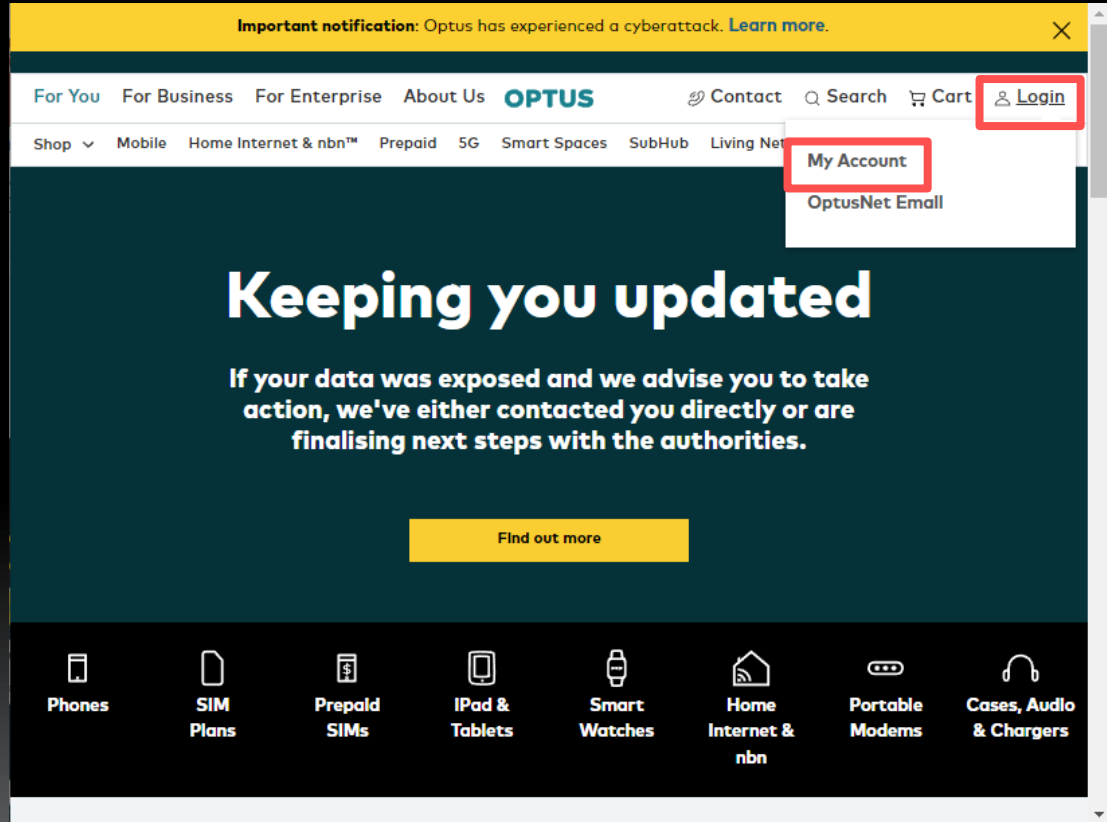
# How do you know this is legitimate?

- Check that the sender is actually Optus
- See Optus advice at <https://www.optus.com.au/support/cyberattack>



# What does Optus know about you?

- Login to Optus to find out



# My Profile shows some of the data

So Optus knows:

- Date of birth
- Phone number (not with Optus)
- My Gmail address
- My Optus email
- My postal address

Doesn't show:

- Driver's licence etc

The screenshot shows the 'MY ACCOUNT' page on the Optus website. The header includes the 'OPTUS' logo, a search bar, and a cart icon. Below the header, there are navigation links: 'Profile & Settings', 'Help & Contact', 'Only on Optus', and 'Shop & Orders'. The main content area is titled 'My Account / My Profile'. It features a greeting 'Hello HELEN,' followed by a message about using contact details for marketing, bills, and invoices. The 'PROFILE' section is highlighted with a red underline. Under 'ABOUT YOU', the 'Name' field shows 'HELEN SMITH'. The 'Date of birth' field is partially visible, showing a date picker. The 'Contact number' field is also partially visible, showing a number starting with '0410'. A 'Change' button is located next to the contact number field. On the right side, there is a 'More options' section with three links: 'Marketing preferences', 'Account permissions', and 'Notifications', each with a brief description and a right-pointing arrow.

**MY ACCOUNT** **OPTUS** **SEARCH** **CART**

Profile & Settings ▾ Help & Contact ▾ Only on Optus ▾ Shop & Orders ▾

[My Account](#) / My Profile

**Hello HELEN,**

We'll use your contact details to communicate with you. This can include [marketing](#), bills, invoices and information relating to your service or account.

**PROFILE**

**ABOUT YOU**

Name  
HELEN SMITH

Date of birth  
[Date Picker]

Contact number  
0410 221 122 [Change](#)

**More options**

- Marketing preferences** ▸  
Select how you stay connected with Optus news, special offers and recommendations tailored to your Optus service so you never miss out.
- Account permissions** ▸  
Control who can manage your Optus account on your behalf.
- Notifications** ▸  
Select how you would like to receive notifications related to your account and services.



## 2. What are the main risks?

The leaked information may make it easier for scammers to:

- send you plausible-looking scam messages
- call you and address you by your name
- attempt to 'port' your phone number
- pretend to be you - 'Identity theft'

# Plausible-looking scam messages

- Using the Optus breach as a reason to offer you a service or threaten you
- Including your name in the message – most scam messages don't do this
- ✓ Check the sender address is real.
- ✓ If in any doubt, contact the organisation using a number you find for yourself.

# Call you and address you by name

- Scam callers often don't have your name
- Breached accounts have provided scammers with lists of names and phone numbers
- Scammers may now be able to use the breached information to sound more legitimate
- ✓ Hang up and call the organisation using a number you find for yourself.

# Attempt to “port” your phone number

- Also called “SIM swapping”
- While there are rules for porting that should prevent it, this still happens.
- ✓ If you lose connection, investigate URGENTLY
- ✓ Set up 2-factor authentication on your Optus account - See <https://www.optus.com.au/connected/news/get-ready-for-multi-factor-authentication>
- ✓ Consider asking Optus to lock your SIM card

# Pretend to be you – Identity theft

If the 'baddies' have enough information they can pretend to be you and:

- Access your bank or superannuation accounts
- Purchase goods in your name with your card
- Take out loans in your name etc

Prevent this by:

- ✓ Checking your credit rating
- ✓ Freezing your credit

# 3. How to protect yourself

- a) Use **strong passwords** & **2-factor authentication** on all your important accounts – including your email account(s)
- b) **Lock your SIM** card to your provider so your number can't be ported
- c) **Freeze your credit** with the credit rating organisations
- d) **Change** your driver's licence, passport, Medicare card if you believe these have been accessed
- e) **Keep a watch** – on bank accounts and email addresses

## Strong passwords

**UNIQUE** – a different password for EVERY account

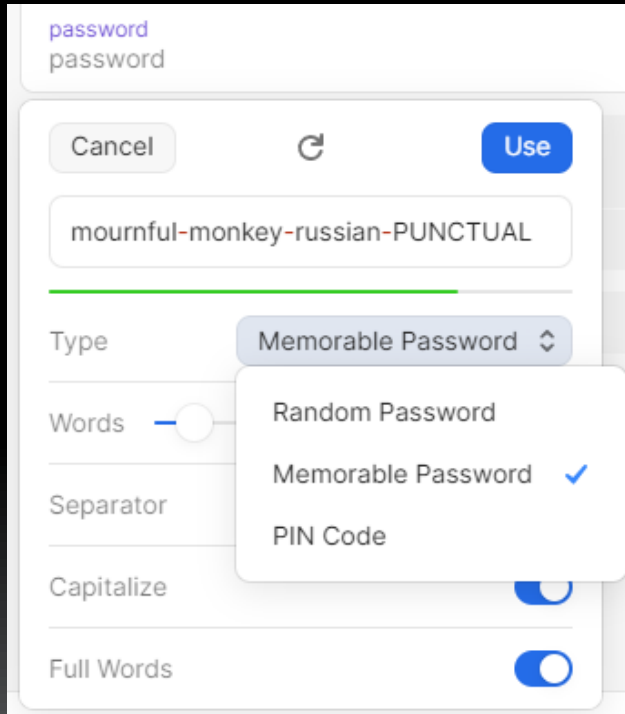
**LONG** – at least 12 characters, 16 or 20 is better

**UNPREDICTABLE** – not your kids' names, dog's name, birth dates or anything about you

**REMEMBERED SAFELY** – Password Managers are best, but written down in a book is fine if kept safe

**EASY TO TYPE / READ** – Passphrases are much easier to use than Passwords. Think “Correct Battery Horse Staple” rather than “DP69TTMTde;+WvVE”

# Generate passwords, don't make them up



My password manager (1Password) allows me to choose either:

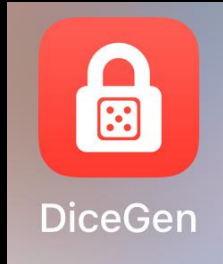
- Passwords (random) or
- Passphrases (memorable – min 3 words)

Some websites don't allow long passwords - use random passwords for these.

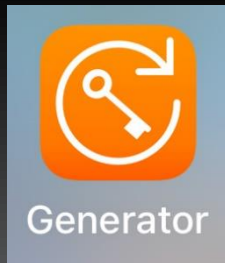


# How do you generate a good password?

- Use an app – one that doesn't connect online

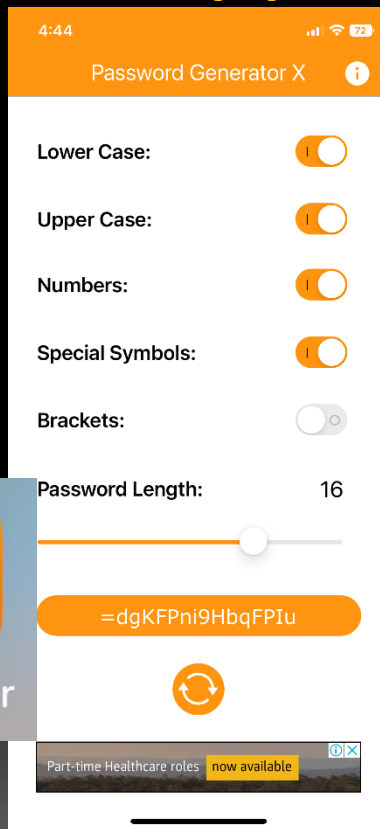
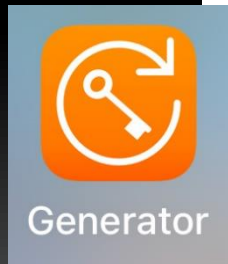
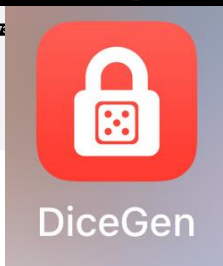
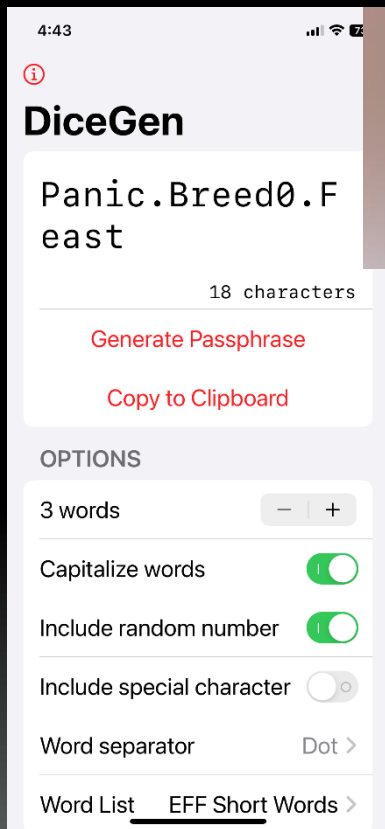


DiceGen generates passPHRASES which are longer and now considered more secure



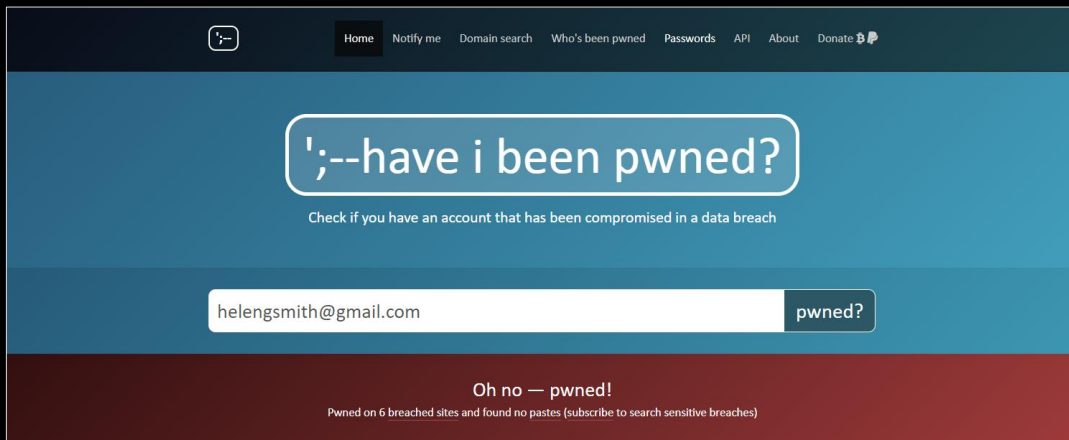
Password Generator X generates 'old-style' random passwords

# Password generator apps



- Adjust for the site as needed
- Write your password down! Don't try to remember it, but store it safely
- If it's a safe password you don't need to change it unless it is stolen

# How do you know if your password is stolen?



The screenshot shows the homepage of 'haveibeenpwned.com'. The navigation bar includes links for Home, Notify me, Domain search, Who's been pwned, Passwords, API, About, and Donate. The main heading is 'have i been pwned?' with a subtext 'Check if you have an account that has been compromised in a data breach'. A search input field contains 'helengsmith@gmail.com' and a button labeled 'pwned!'. Below the search bar, it states 'Oh no — pwned!' and 'Pwned on 6 breached sites and found no pastes (subscribe to search sensitive breaches)'.

Strongly recommended that you:

- Check your email address(es) on this site [haveibeenpwned.com](https://haveibeenpwned.com)
- Register to be notified of any new breaches

## Breaches you were pwned in

A "breach" is an incident where data has been unintentionally exposed to the public. Using the 1Password password manager helps you ensure all your passwords are strong and unique such that a breach of one service doesn't put your other services at risk.

### 500px

**500px:** In mid-2018, the online photography community 500px suffered a data breach. The incident exposed almost 15 million unique email addresses alongside names, usernames, genders, dates of birth and either an MD5 or bcrypt password hash. In 2019, the data appeared listed for sale on a dark web marketplace (along with several other large breaches) and subsequently began circulating more broadly. The data was provided to HIBP by a source who requested it to be attributed to "BenjaminBlue@exploit.in".

**Compromised data:** Dates of birth, Email addresses, Genders, Geographic locations, Names, Passwords, Usernames



**Canva:** 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



**LinkedIn:** In May 2016, LinkedIn had 164 million email addresses and passwords exposed. Originally hacked in 2012, the data remained out of sight until being offered for sale on a dark market site 4 years later. The passwords in the breach were stored as SHA1 hashes without salt, the vast majority of which were quickly cracked in the days following the release of the data.

**Compromised data:** Email addresses, Passwords



**MyHeritage:** In October 2017, the genealogy website MyHeritage suffered a data breach. The incident was reported 7 months later after a security researcher discovered the data and contacted MyHeritage. In total, more than 924 million customer records were exposed and included email addresses and salted SHA-1 password hashes. In 2019, the data appeared listed for sale on a dark web marketplace (along with several other large breaches) and subsequently began circulating more broadly. The data was provided to HIBP by a source who requested it be attributed to "BenjaminBlue@exploit.in".

**Compromised data:** Email addresses, Passwords



**River City Media Spam List** (spam list): In January 2017, a massive trove of data from River City Media was found exposed online. The data was found to contain almost 1.4 billion records including email and IP addresses, names and physical addresses, all of which was used as part of an enormous spam operation. Once de-duplicated, there were 393 million unique email addresses within the exposed data.

**Compromised data:** Email addresses, IP addresses, Names, Physical addresses



**Verifications.io:** In February 2019, the email address validation service verifications.io suffered a data breach. Discovered by Bob Diachenko and Vinny Troia, the breach was due to the data being stored in a MongoDB instance left publicly facing without a password and resulted in 763 million unique email addresses being exposed. Many records within the data also included additional personal attributes such as names, phone numbers, IP addresses, dates of birth and genders. No passwords were included in the data. The Verifications.io website went offline during the disclosure process, although an archived copy remains viewable.

**Compromised data:** Dates of birth, Email addresses, Employers, Genders, Geographic locations, IP addresses, Job titles, Names, Phone numbers, Physical addresses

# Avoid Previously Hacked Passwords

Password1



Home Notify me Domain search Who's been pwned Passwords API About Donate \$P

## Pwned Passwords

Pwned Passwords are 555,278,657 real world passwords previously exposed in data breaches. This exposure makes them unsuitable for ongoing use as they're at much greater risk of being used to take over other accounts. They're searchable online below as well as being downloadable for use in other online systems. [Read more about how HIBP protects the privacy of searched passwords.](#)

 pwned?

Oh no — pwned!

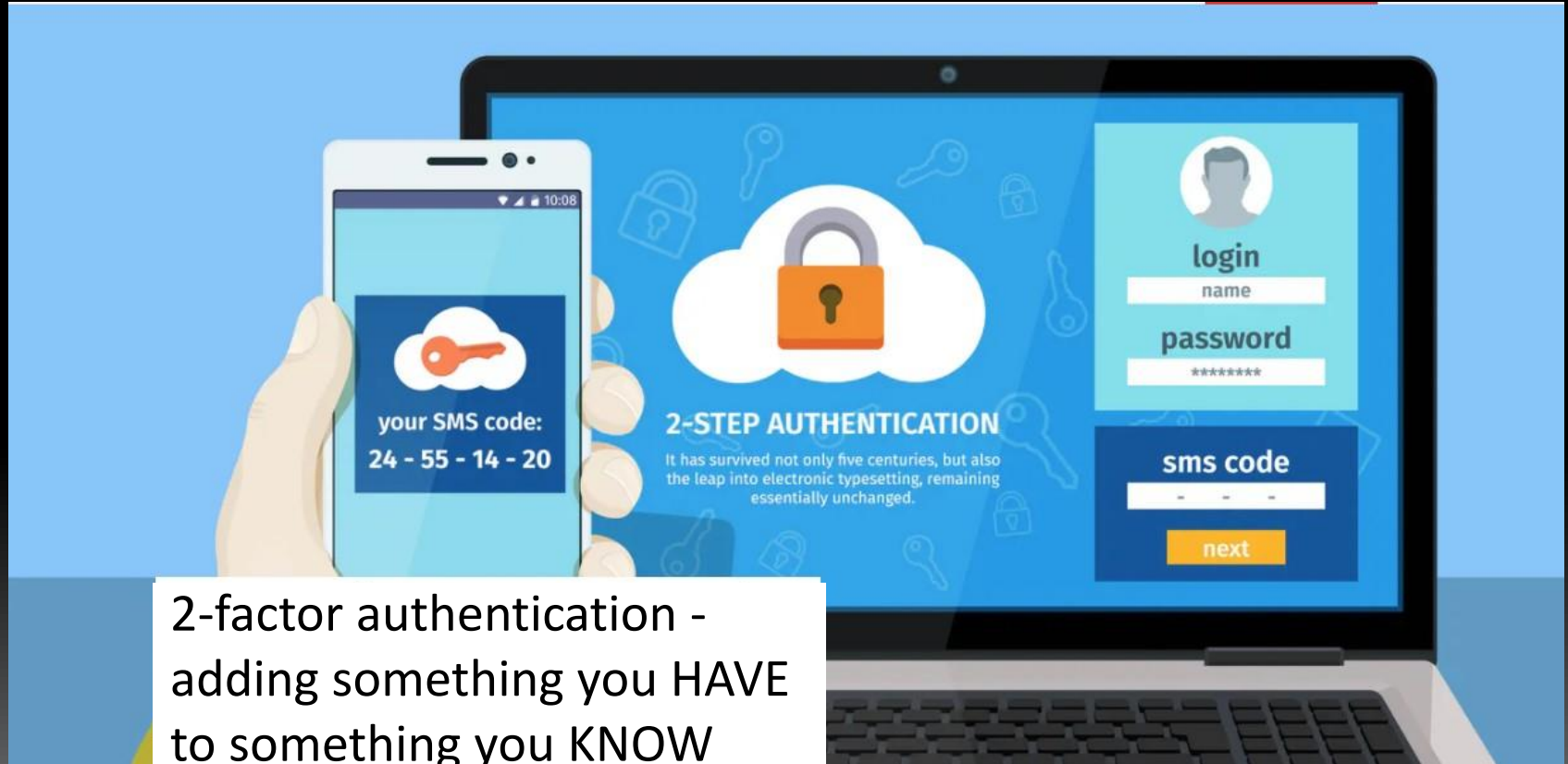
This password has been seen 116,789 times before

This password has previously appeared in a data breach and should never be used. If you've ever used it anywhere before, change it!

NIST's guidance: check passwords against those obtained from previous data breaches

The Pwned Passwords service was created in August 2017 after NIST released guidance specifically recommending that user-provided

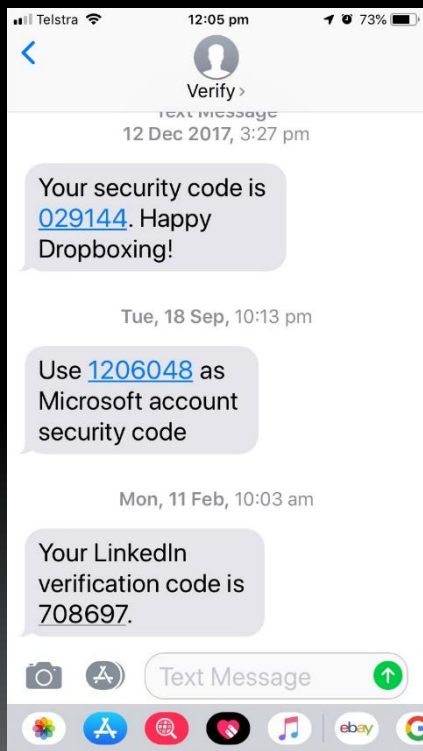
# a) 2-factor authentication (2FA)



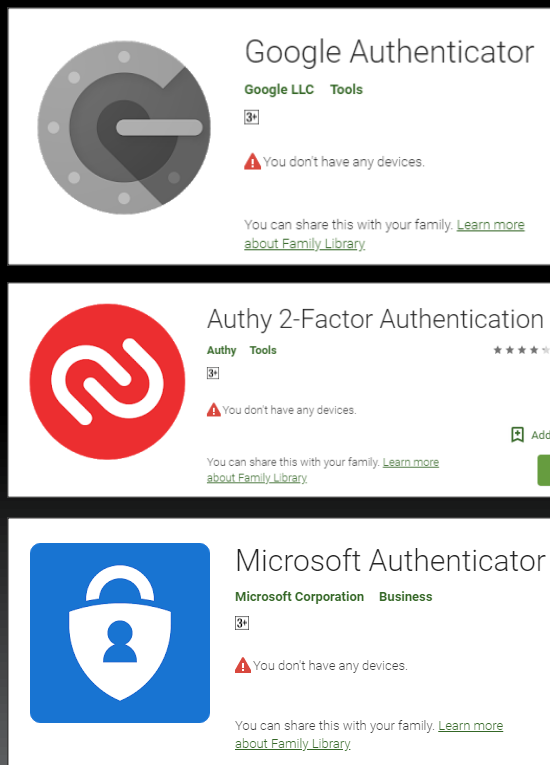
2-factor authentication -  
adding something you HAVE  
to something you KNOW

# 'Flavours' of 2FA

## SMS



## Apps



## Physical devices

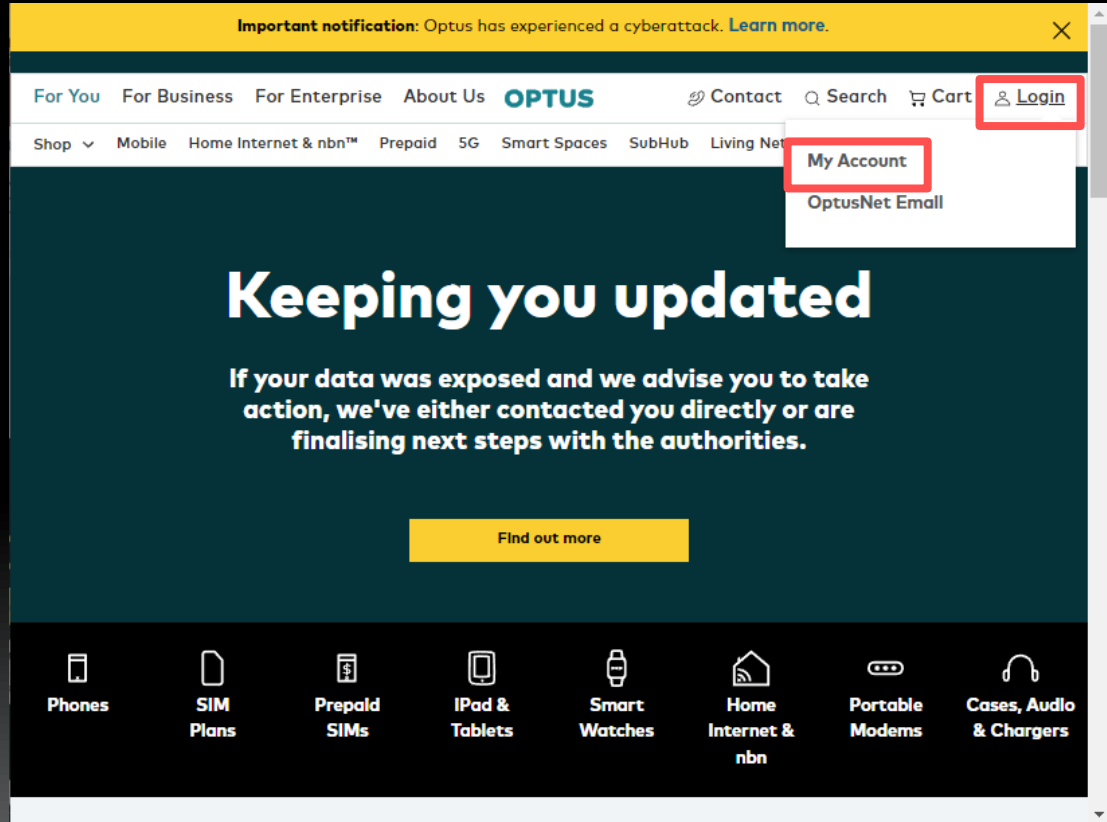


# Do I have to do this EVERY TIME?

- Most systems allow for trusted devices
- 2FA is not required on a trusted device
- trust applies to ONE web browser on ONE computer.
  - If you mark 'trust this device' in Chrome on computer A, you will still need to enter the code:
    - in Firefox and Edge on computer A.
    - in Chrome on computer B.

# SO – change your Optus password

- Login to Optus





# Optus login ...

- I'm using my password manager to remember and fill the username and password

**Important notification:** Optus has experienced a cyberattack. [Learn more.](#)

[For You](#) [For Business](#) [For Enterprise](#) [About Us](#) **OPTUS** [Search](#) [Cart](#) [Login](#)

## Log in to My Account

Manage your Optus account, view and pay your bills, check your usage and message us in My Account.

Email address \*

ⓘ

 Optus MyAccount  
helgarsmith00@optusnet.c...

 Optus Webmail  
helgarsmith00@optusnet.c...

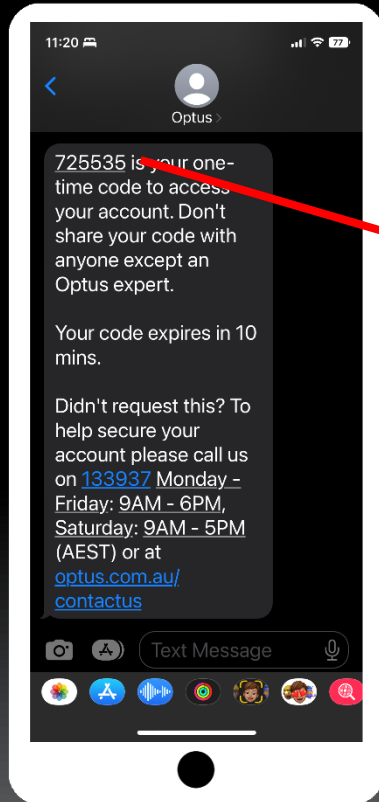
[Forgot password?](#)

Log in

**How to register**

When you first joined Optus, you would've received an email to verify your email address and set up an online account. Can't find this? Provide your

# 2-factor authentication



**OPTUS**

## Verify your one-time code

We've sent a code to your mobile number (\*\*\*\*\*1139)

Enter your 6-digit one-time code 

yes

Optus MyAccount  
helgarsmith00@optusnet.c...

yes

Optus Webmail  
helgarsmith00@optusnet.c...

Didn't receive your code? [Resend code](#) or [verify another way](#)

See <https://www.optus.com.au/connected/news/get-ready-for-multi-factor-authentication>

# Now we're in

- Navigate to My Profile

The screenshot displays the 'My Account' page for an Optus user. The page is divided into several sections. At the top, there's a navigation bar with the 'My Account' title, the 'OPTUS' logo, and search and cart icons. Below this is a secondary navigation bar with links for 'Account summary', 'Profile & Settings', 'Help & Contact', 'Only on Optus', and 'Shop & Orders'. The main content area is split into two columns. The left column features the user's name 'HELEN SMITH', their account number (partially redacted), a 'Postpaid' status, and a '2 Services' indicator. A red rectangular box highlights the 'My Profile' link. The right column contains a 'Payment summary' section with two green checkmarks indicating 'All up to date' and 'Automatic payment: Active', followed by a 'Manage payment method' button. Below this is a list of links: 'Pay my bill', 'Bills & payments', 'My Wallet', 'Bill notifications', and 'Need more time to pay?'. At the bottom of the left column, there's a 'Data Usage' section with a circular progress indicator showing 'Unlimited Data' and a usage of '74.1GB'. Below that, it shows '22 Days to go'. The footer includes an 'Internet' icon and a banner for 'The Living Network'.

My Account **OPTUS** Search Cart

Account summary ▾ Profile & Settings ▾ Help & Contact ▾ Only on Optus ▾ Shop & Orders ▾

**HELEN SMITH** Postpaid  
Account number [REDACTED]  
2 Services  
**My Profile**

**Payment summary**  
✓ All up to date  
✓ Automatic payment: Active  
Manage payment method

**Data Usage**  
Unlimited Data  
74.1GB  
Used of Unlimited Data  
22 Days to go

Pay my bill >  
Bills & payments >  
My Wallet >  
Bill notifications >  
Need more time to pay? >

Internet >

The Living Network

# My Profile shows some of the data

So Optus knows:

- Date of birth
- Phone number (not with Optus)
- My Gmail address
- My Optus email
- My postal address

Doesn't show:

- Driver's licence etc

The screenshot displays the 'MY ACCOUNT' page on the Optus website. The header includes the 'OPTUS' logo, a search bar, and a shopping cart icon. Below the header, there are navigation links: 'Profile & Settings', 'Help & Contact', 'Only on Optus', and 'Shop & Orders'. The main content area is titled 'My Account / My Profile'. It features a greeting 'Hello HELEN,' followed by a message about using contact details for marketing, bills, and invoices. The 'PROFILE' section is highlighted with a red underline. Under 'ABOUT YOU', the 'Name' field shows 'HELEN SMITH'. The 'Date of birth' field is partially visible, showing a date picker. The 'Contact number' field is also partially visible, showing a number starting with '0410'. A 'Change' link is located next to the contact number field. On the right side, there is a 'More options' section with three expandable items: 'Marketing preferences', 'Account permissions', and 'Notifications'.

**MY ACCOUNT** **OPTUS** **SEARCH** **CART**

Profile & Settings ▾ Help & Contact ▾ Only on Optus ▾ Shop & Orders ▾

[My Account](#) / My Profile

**Hello HELEN,**

We'll use your contact details to communicate with you. This can include [marketing](#), bills, invoices and information relating to your service or account.

**PROFILE**

**ABOUT YOU**

Name  
HELEN SMITH

Date of birth  
[Date Picker]

Contact number  
0410 221 122 [Change](#)

**More options**

- Marketing preferences** ▸  
Select how you stay connected with Optus news, special offers and recommendations tailored to your Optus service so you never miss out.
- Account permissions** ▸  
Control who can manage your Optus account on your behalf.
- Notifications** ▸  
Select how you would like to receive notifications related to your account and services.

# Change your Optus password

- Scroll down your profile page to the Password,
- Click “Change”

The screenshot displays a user profile page with several sections. At the top, there are two rows: 'Contact email address' with a text input field and a 'Change' link, and 'Log in email address' with a text input field and a 'Change' link. Below these is a section titled 'LOGIN DETAILS'. Inside this section, the 'Password' label and its corresponding masked input field (showing eight asterisks) are highlighted with a red rectangle. To the right of the password field, another 'Change' link is also highlighted with a red rectangle. Below the 'LOGIN DETAILS' section is an 'ADDRESS' section with a 'Postal address' label and a text input field, followed by a 'Change' link. At the bottom of the page, there is a dark footer bar containing three items: 'MY OPTUS' with a link to 'My Optus App', 'OPTUS GUIDE' with a link to 'Privacy, Security and Safety', and 'FOLLOW US'.

Contact email address [Change](#)

Log in email address [Change](#)

**LOGIN DETAILS**

Password [Change](#)

**ADDRESS**

Postal address [Change](#)

**MY OPTUS**  
My Optus App

**OPTUS GUIDE**  
Privacy, Security and Safety

**FOLLOW US**

# Generate and enter your new password

Note the rules for Optus passwords

- 8-15 characters

Include:

- Uppercase
- Lowercase
- Number or symbol

GENERATE your password!

The image shows a user profile page in the background with the following details:

- Contact email address: helengsmith@gmail.com
- Log in email address: helgarsmith00@optusnet.com.au
- LOGIN DETAILS: Password field with masked characters (\*\*\*\*\*)
- ADDRESS: Postal address 12 Ronald Street, MITCHAM, VIC 3132

Overlaid on this is a 'Profile Change password' dialog box. It contains the following text and fields:

**Profile**  
**Change password**

Your password will change for your Optus accounts excluding OptusNet email (e.g. My Optus app, Optus Sport, Optus SubHub).

Your password must contain:

- 8-15 characters
- 1 uppercase letter
- 1 lowercase letter
- 1 number or symbol

Current Password Field: Enter current password ?

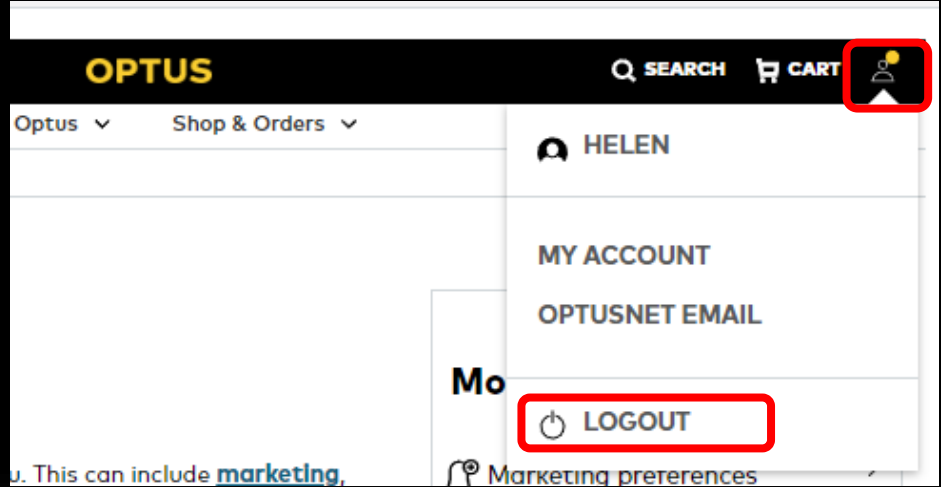
New Password Field: Enter new password ?

Confirm Password Field: Re-enter password ?

At the bottom of the page, there is a footer with 'MY OPTUS' links (My Optus App, Message Us, OptusNet Hub), 'OPTUS' links (Privacy, Standard Agreement, Optus Information Summary), and 'FOLLOW US' social media icons (Facebook, Twitter, YouTube, LinkedIn, Instagram).

# Logout and Login again

It's always a good idea to test that your new password works!



# Change passwords on other accounts

We'll use much the same process as we used for Optus on every account:

1. Login with your current password
2. Find where you change the password (can be tricky!)
3. **Generate** your new password following the site rules for passwords – record this new password
4. Enter your new password and save it
5. Logout and login again with the new password to check it



# Lock your SIM card?

- Note that this is NOT the lock in your phone!
- This refers to a **Network-locked SIM card**
- If your SIM card is locked to the network then you can't take it to another provider
- Most Australian mobile carriers have stopped network locking their phones
- You need to talk to your provider to set this up
- It can be a hassle unlocking the SIM card later – see <https://www.finder.com.au/network-unlock-mobile-phone> for instructions on unlocking



# Change your driver's licence, passport ...?

- Driver's licence: see <https://www.vicroads.vic.gov.au/newsmedia/2022/optus-cyberattack>
  - Request a flag and replacement licence through the online form
- Passport – see <https://www.passports.gov.au/optus-data-breach>
  - No news on replacements yet
- Medicare card - you can ask for a new card by:
  - using your Medicare online account through [myGov](#)
  - the Express Plus Medicare mobile app
  - calling the Medicare program.
  - See <https://www.servicesaustralia.gov.au/get-new-medicare-card-if-it-expires-or-lost-stolen-or-damaged?context=21796>

Only request a replacement if your documentation was exposed!

# Vic Roads form

This form is at

<https://www.vicroads.vic.gov.au/licences/renew-replace-or-update/flag-your-driver-licence>

Fill in:

- First name
- Last name
- Phone number
- Email address
- Driver's Licence Number
- Check the “I request a licence change” box

The screenshot shows a web browser window with the URL [vicroads.vic.gov.au/licences/renew-replace-or-update/flag-your-driver-licence](https://www.vicroads.vic.gov.au/licences/renew-replace-or-update/flag-your-driver-licence). The page contains the following text and form elements:

**All fields must be completed before you click submit. Please check your information carefully to ensure your details are correct.**

If you choose not to provide all or part of the information required, we may not be able to contact you or action your request.

**If you need support completing our online form or have any issues, please call the VicRoads Customer Service team on 13 11 71.**

*\* Indicates a required field*

**First name \***

**Last name \***

**Phone number \***

**Email address \***

**Driver's Licence Number \*** [Help +](#)

☐ I request a licence change

**Privacy statement**

VicRoads collects your personal information for the purpose of driver licence record flagging and the option to request a new learner permit or driver licence number. If you choose not to provide all or part of the information required, we may not be able to contact you or action your request. The data captured in the webform will be accessible to authorised Department of Transport representatives.

Records will also be flagged within the national database.

If you have any questions about how your personal information will be handled or would like to gain access to your personal information, you can contact Department of Transport's Manager Freedom of Information and Information Privacy at [privacy@transport.vic.gov.au](mailto:privacy@transport.vic.gov.au)

For more information, VicRoads has an information page for customers impacted by



# Freeze your credit?

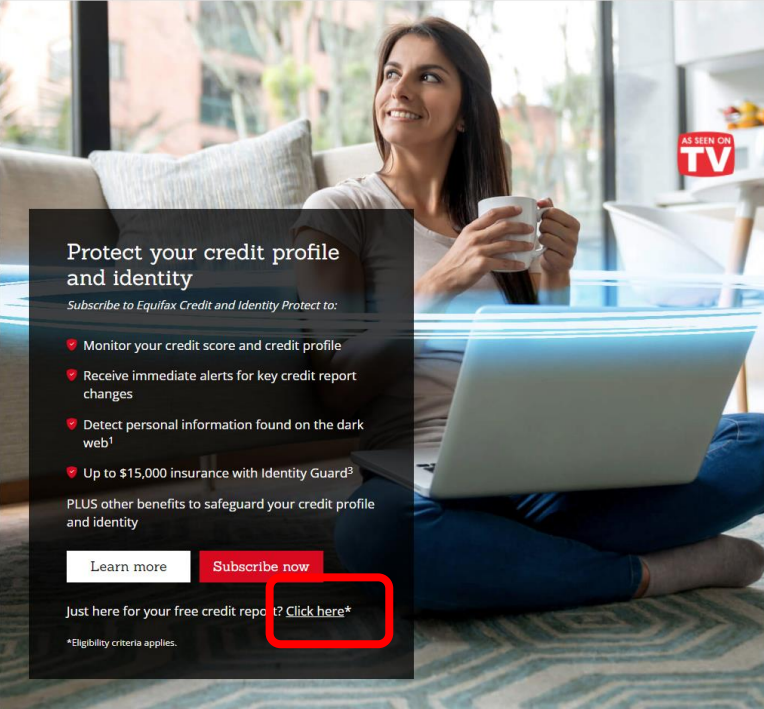
- A credit reporting body must give you access to your consumer credit report for free once every 3 months.
- You can request a copy of your credit report from these credit reporting bodies (1 free copy per year):
  - [Equifax](#), phone 138 332
  - [Experian](#), phone 1300 783 684
  - [illion](#), phone 1300 734 806
- See <https://www.oaic.gov.au/privacy/data-breaches/respond-to-a-data-breach-notification>
- If you freeze your credit you won't be able to get credit either!

# Equifax credit report

**EQUIFAX**<sup>®</sup>[Personal](#)[Small Business](#)[Business & Enterprise](#)[About](#)[Contact](#)

[Products](#)[Blog](#)[Corrections Portal](#)[Help Centre](#)

Login



### Protect your credit profile and identity

Subscribe to Equifax Credit and Identity Protect to:

- ♥ Monitor your credit score and credit profile
- ♥ Receive immediate alerts for key credit report changes
- ♥ Detect personal information found on the dark web<sup>1</sup>
- ♥ Up to \$15,000 insurance with Identity Guard<sup>3</sup>

PLUS other benefits to safeguard your credit profile and identity

[Learn more](#)[Subscribe now](#)

Just here for your free credit report? [Click here\\*](#)

\*Eligibility criteria applies.

**EQUIFAX**<sup>®</sup>

Equifax Credit Report

To get started, answer the three questions below

You are entitled to a free copy of your Equifax Credit Report if:

- ✓ You haven't received one in the last 3 months; or
- ✓ You've been declined credit in the last 90 days; or
- ✓ You've had an item corrected on your credit report.

If you do not meet the criteria, a once-off Equifax credit report is currently available for free.

Have you received your Equifax Credit Report in the last 3 months?

☐ Yes

☐ No

Have you applied for credit and been declined in the last 90 days?

☐ Yes

☐ No

Has your Credit Report information been corrected by Equifax or a Credit Provider?

☐ Yes

☐ No

[BACK](#)[CONTINUE](#)

# Create an account to verify your details

**EQUIFAX**

Equifax Credit Report

This subscription plan includes:

- ✓ View your Equifax Credit Report online. You can also save and download it in PDF format
- ✓ Know your credit history including credit rating and key contributing factors, credit products you currently hold, past applications for credit and repayment history
- ✓ See what credit information some banks and lenders may see from Equifax
- ✓ Please note: Your free Equifax Credit Report will only be available to view and download for 30 days from the time the report is created, after which we are required to delete the credit report and the credit rating associated with this credit report.

By proceeding, you are agreeing to the [Terms & Conditions](#)

[< BACK](#)

Already a member?

Login

CREATE ACCOUNT

**EQUIFAX**

Create Your Credit & Identity account

1

2

3

4

### Why we need to verify your identity

Equifax is committed to keeping Australians' personal data safe and secure. For privacy and security reasons, we need to verify your identity. Once we've done that, we'll activate your account.

### Setting up your account

We've done everything possible to make the process of verifying your identity as quick and painless as possible. Most of the time, our new customers are able to prove they are who they say they are in four easy steps. If we are unable to verify your identity, we'll ask for further documentation which you can provide to us securely.

#### Registration

Email \*

Create password \*

1 uppercase letter

1 number

1 lowercase letter

1 special character !@#\*+<br>No invalid character

8-20 characters

No more than 2 repeated characters

No more than 8 consecutive numbers

Confirm password \*

#### Terms and conditions

Please read the [Terms and Conditions](#) before proceeding. The Privacy Policy can be found [here](#)

☐ I confirm I have read and accept the Terms and Conditions.\*

☐ I confirm I am at least 18 years of age.\*

# Create a password and verify your account

Setting up your account

We've done everything possible to make the process of verifying your identity as quick and painless as possible. Most of the time, our new customers are able to prove they are who they say they are in four easy steps. If we are unable to verify your identity, we'll ask for further documentation which you can provide to us securely.

### Registration

Email \*

helengsmith@gmail.com

Create password \*

1 uppercase letter ✓ 1 number ✓  
1 lowercase letter ✓ 1 special character @!#\$%&\* ✓  
8-20 characters ✓ No invalid character ✓  
No more than 2 repeated characters ✓ No more than 5 consecutive numbers ✓

Confirm password \*

Terms and conditions

Please read the [Terms and Conditions](#) before proceeding. The Privacy Policy can be found [here](#)

☒ I confirm I have read and accept the Terms and Conditions.\*  
☒ I confirm I am at least 18 years of age.\*

Confirm

Please check the box below

☒ I'm not a robot

 reCAPTCHA  
Privacy - Terms

CANCEL VERIFY EMAIL

**EQUIFAX**

### Sign up to get Your Credit & Identity

1 2 3 4

### Verify Email

A verification code has been sent to helengsmith@gmail.com. If you can't find the email, please check your junk / spam or other folders and add no-reply@equifax.com to your contacts.

Enter your verification code

Enter code \*

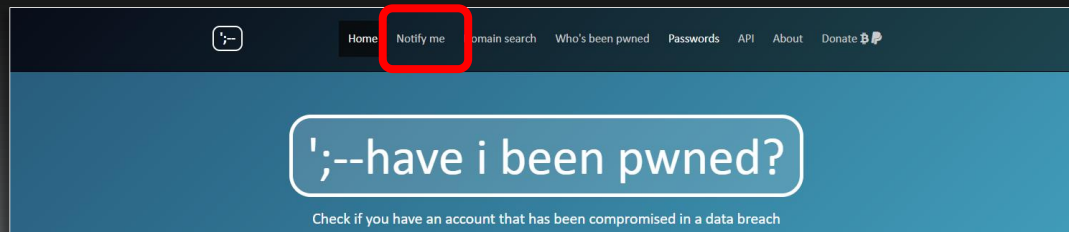
CONTINUE

I haven't got further than this – the email didn't arrive ...

**EQUIFAX** Your Credit & Identity

# e) Keep a watch ...

- on bank accounts:
  - Check your transactions frequently
  - A phone app is safe and easy to check
- email addresses
  - Subscribe to [HaveIBeenPwned.com](https://HaveIBeenPwned.com)





# 4. If you do become a victim

If you become aware of unexplained transactions on your bank or financial accounts:

- call the institution and clarify the situation
- contact [IDCare](#) for guidance
- report cyber crimes through [CyberReport](#)
- act quickly - the faster you act the less damage the scammers will be able to do.

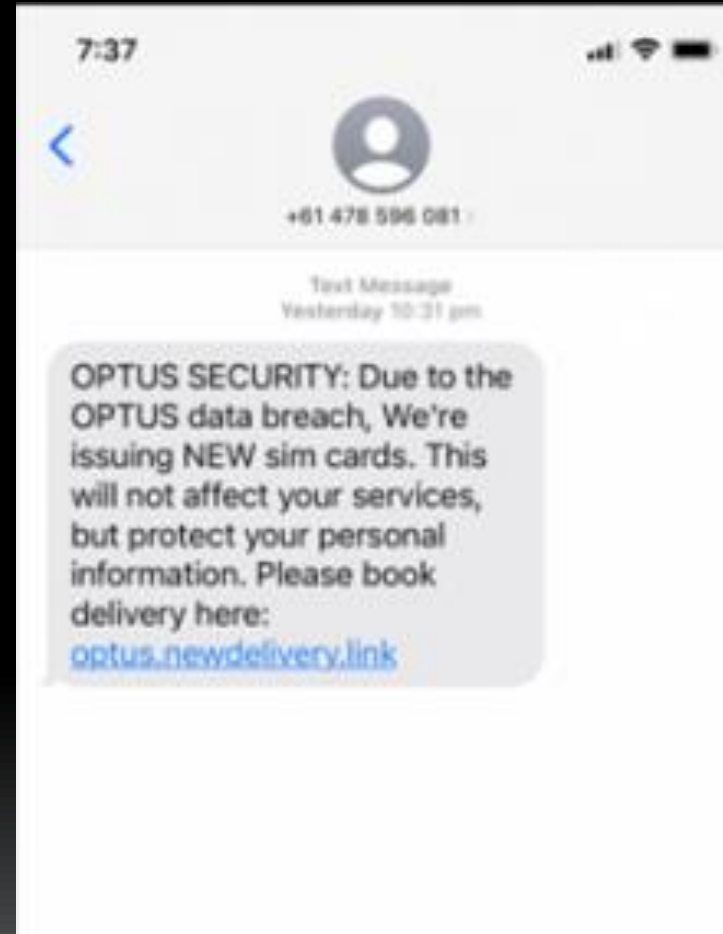


## 5. Scams noted so far

*The following examples are all taken from the  
[Scamwatch page on the Optus data breach](#)*

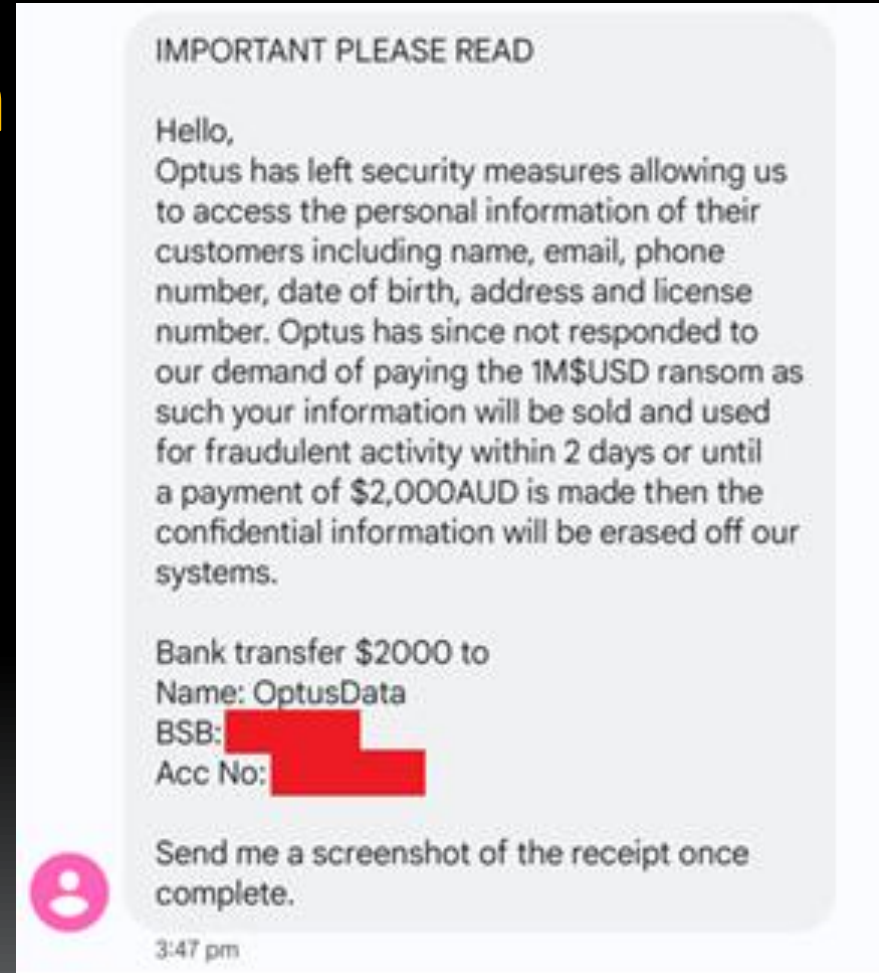
# SIM card scams

- Optus is **NOT** contacting people about issuing new SIM cards.
- Delete these messages



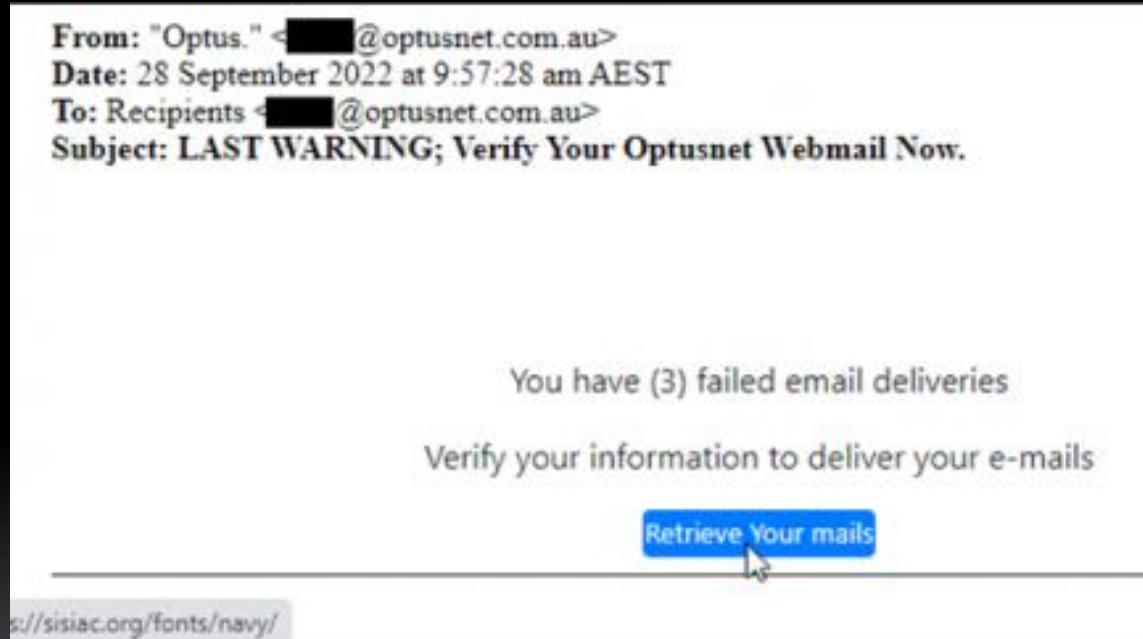
# Blackmail / extortion

- If you receive demands to pay money with a threat that your information will be released, delete the message.
- Scammers are pretending to be hackers to make you give them money.



# Update password or verify scams

Optus is **NOT** threatening email account closure if you do not update your password or verify your personal information.



# Update password scams

Optus is **NOT** threatening email account closure if you do not update your password or verify your personal information.

From: "optusnet.com.au" <[REDACTED]@optusnet.com.au>  
Date: 28/9/22 4:15 am (GMT+10:00)  
To: [REDACTED]@optusnet.com.au  
Subject: Your email account will be temporarily closed

IT HelpDesk  
Sender

Action Required  
password Has Expired

Dear [REDACTED],

Your password for [REDACTED]@optusnet.com.au will expire by today .

Action is required to Fix this below:

[Keep Same Password](#)

Thank you.  
optusnet.com.au Team

*The email is automatically generated upon request. This electronic transmission is confidential information and is for your use only. If this is not the case, please delete the original and all copies and notify the sender immediately.*

Copyright ©2022 . All rights reserved [marpedia.com](https://marpedia.com)

[https://buildone.online/html/webmail/webmail/webmail/?email=\[REDACTED\]@optusnet.com.au](https://buildone.online/html/webmail/webmail/webmail/?email=[REDACTED]@optusnet.com.au)

# Billing issues scams

Optus is **NOT** contacting people about their bills and asking you to update your information.

Dear Customer,

There has been an issue with your monthly direct debit to pay for our services. We require you to update all information below, and pay all unpaid balances via our portal below.

<https://optus.com.au/verification>

This message was sent by a system, do not reply.

Kindest Regards

Optus Billing Department

# Financial restitution scams

There is no financial restitution being sent to individuals caught in the data breach at this time.

Notification ID: UK 1456789 **SCAM**  
Notification Subject: Your Identity Has Been Compromised  
Notification Message:  
We regret to inform you that you have been a victim of identity theft. Your identity and consumer credit files were compromised during a data breach where millions of user profiles were exposed to hackers and used in an identity theft scheme now uncovered by federal authorities and Interpol.

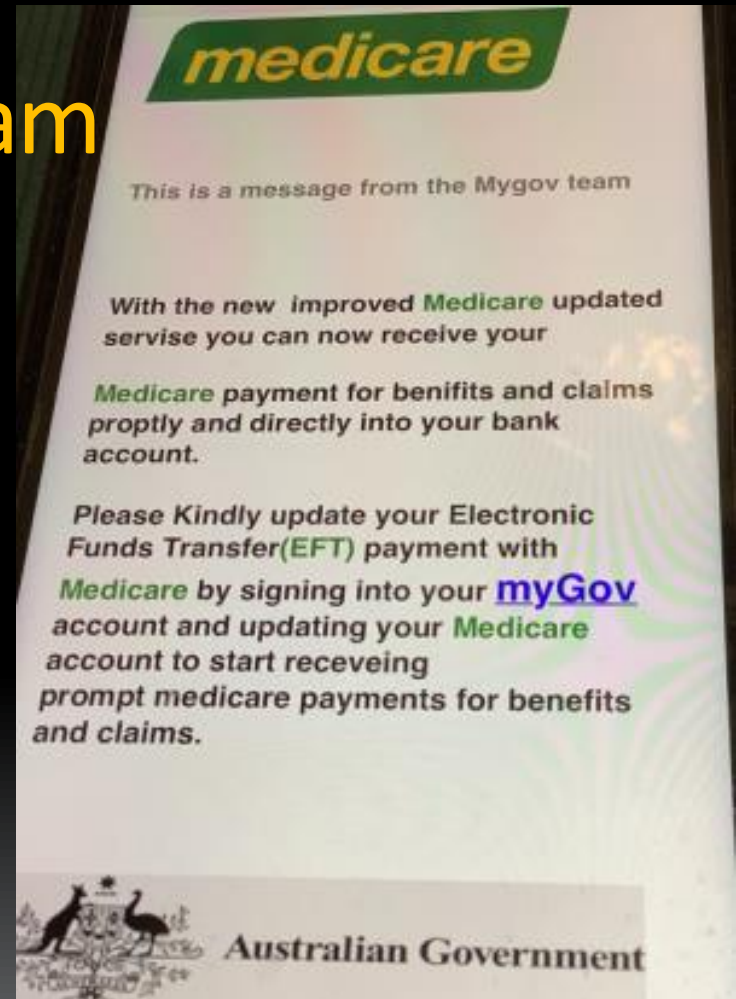
Steps have since been taken to mitigate the issue.

The offenders have been prosecuted and ordered to pay a large settlement in which you are eligible to receive a portion of. You are eligible for reimbursements of false acquisitions, compensation for potential impact on your credit, and any additional claims you may make.



# Medicare / MyGov scam

- This message below is **NOT** from the Australian Government – it is a Medicare / MyGov scam.
- **Do not click on links** in messages. Instead, go to the official Services Australia website for information.





# ANY QUESTIONS ?

*Thank you for attending this U3A Nunawading  
presentation / demonstration*