TTWRDC(GIRLS)
,JANGAON

Cybersecurity Awareness

TTWRDC(GIRLS)
B.COM(CA)

Agenda

- State of Cybersecurity/ Current Cyberthreats
- Topics of Interest:
  - Phishing Emails/Scams
  - Ransomware
  - Social Engineering
- How to protect yourself
  - WFH Tips
  - Additional resources
- Q&A

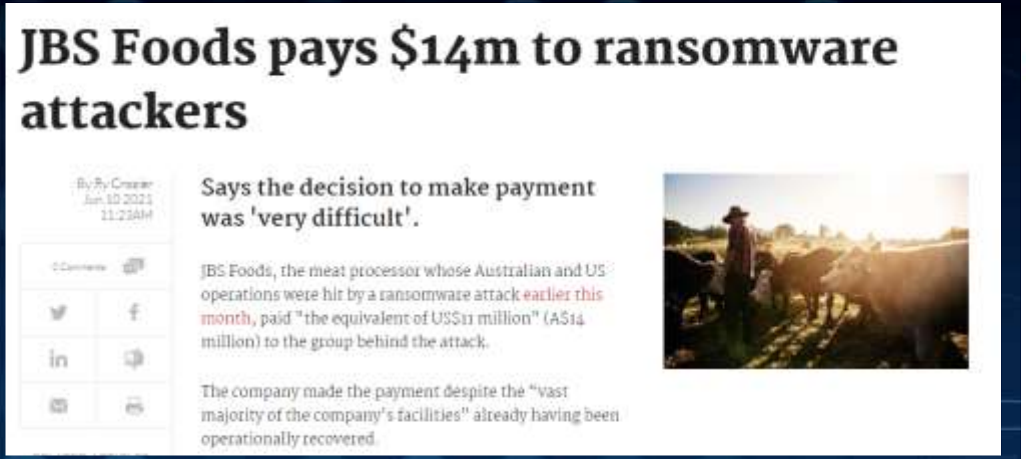
Current state of Cybersecurity

Phishing attacks are still number 1

Ransomware attacks are on the rise

Social Engineering is the leading attack vector for scams

Cost of Cybersecurity Attacks



JBS Foods pays $14m to ransomware attackers

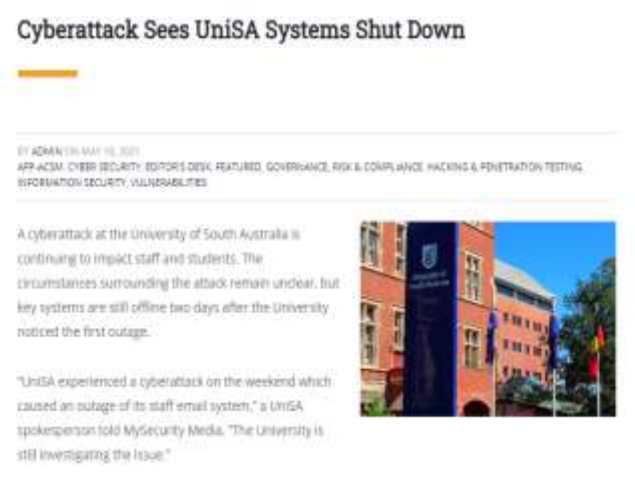
By Ry Crozier
Jun 10 2021
11:21AM

0 Comments

Says the decision to make payment was 'very difficult'.

JBS Foods, the meat processor whose Australian and US operations were hit by a ransomware attack earlier this month, paid "the equivalent of US$11 million" (A$14 million) to the group behind the attack.

The company made the payment despite the "vast majority of the company's facilities" already having been operationally recovered.

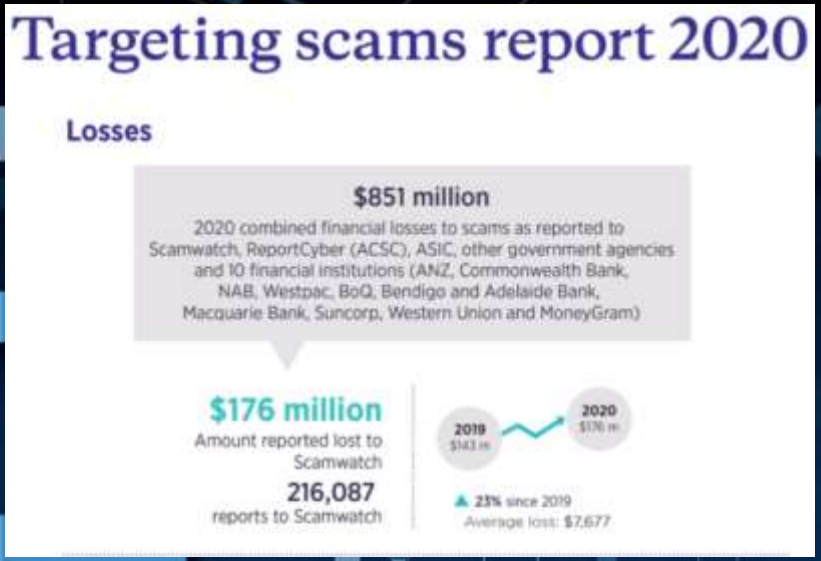


Cyberattack Sees UniSA Systems Shut Down

BY ADMIN ON MAY 18, 2021
APP-ACSM, CYBER SECURITY, EDITOR'S DESK, FEATURED, GOVERNANCE, RISK & COMPLIANCE, HACKING & PENETRATION TESTING, INFORMATION SECURITY, VULNERABILITIES

A cyberattack at the University of South Australia is continuing to impact staff and students. The circumstances surrounding the attack remain unclear, but key systems are still offline two days after the University noticed the first outage.

"UniSA experienced a cyberattack on the weekend which caused an outage of its staff email system," a UniSA spokesperson told MySecurity Media. "The University is still investigating the issue."



Targeting scams report 2020

Losses

$851 million
2020 combined financial losses to scams as reported to Scamwatch, ReportCyber (ACSC), ASIC, other government agencies and 10 financial institutions (ANZ, Commonwealth Bank, NAB, Westpac, BoQ, Bendigo and Adelaide Bank, Macquarie Bank, Suncorp, Western Union and MoneyGram)

$176 million
Amount reported lost to Scamwatch

216,087
reports to Scamwatch

▲ 23% since 2019
Average loss: $7,677

Nine Network under attack by cyber hackers, threatening news services nationwide

By 9News Staff | 7:04am Mar 29, 2021

Tweet

NEW ZEALAND / MEDIA & TECHNOLOGY

Waikato DHB cyber attack: Medical files may have been taken

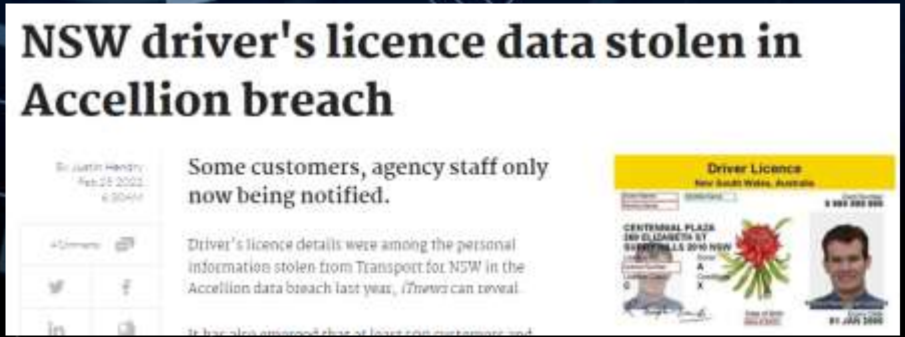
5:46 pm on 24 May 2021

Share this

POLITICS

Colonial Pipeline paid $5 million ransom one day after cyberattack, CEO tells Senate

PUBLISHED TUE, JUN 8 2021-10:17 AM EDT | UPDATED WED, JUN 9 2021-8:24 AM EDT



NSW driver's licence data stolen in Accellion breach

By Justin Hendry
Feb 25 2021
6:30AM

Some customers, agency staff only now being notified.

Driver's licence details were among the personal information stolen from Transport for NSW in the Accellion data breach last year, *iTnews* can reveal.

Phishing Attacks

Phishing emails

e.g. COVID 19 vaccines

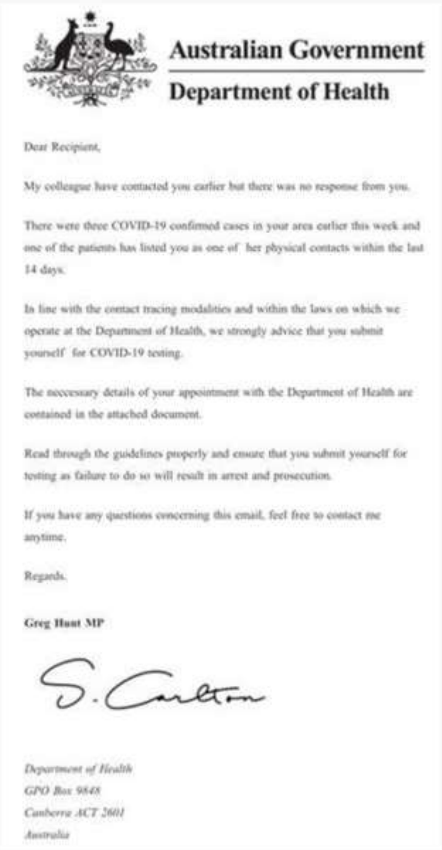
Vishing

e.g. Computer technician call to fix a virus on your machine

Smishing

e.g. ATO text messages to claim a tax refund

Department of Health impersonation email



Australian Government

Department of Health

Dear Recipient,

My colleague have contacted you earlier but there was no response from you.

There were three COVID-19 confirmed cases in your area earlier this week and one of the patients has listed you as one of her physical contacts within the last 14 days.

In line with the contact tracing modalities and within the laws on which we operate at the Department of Health, we strongly advice that you submit yourself for COVID-19 testing.

The necessary details of your appointment with the Department of Health are contained in the attached document.

Read through the guidelines properly and ensure that you submit yourself for testing as failure to do so will result in arrest and prosecution.

If you have any questions concerning this email, feel free to contact me anytime.

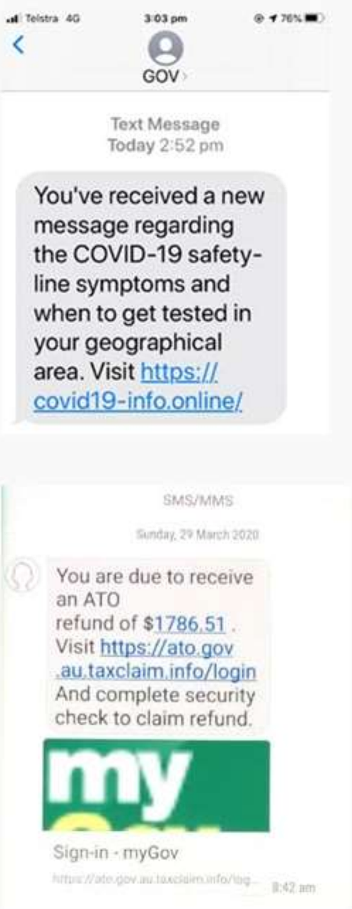
Regards,

Greg Hunt MP

S. Carlton

Department of Health
GPO Box 9848
Canberra ACT 2601
Australia

Fake myGov texts



Telstra 4G 3:03 pm 76%

GOV

Text Message
Today 2:52 pm

You've received a new message regarding the COVID-19 safety-line symptoms and when to get tested in your geographical area. Visit https://covid19-info.online/

SMS/MMS

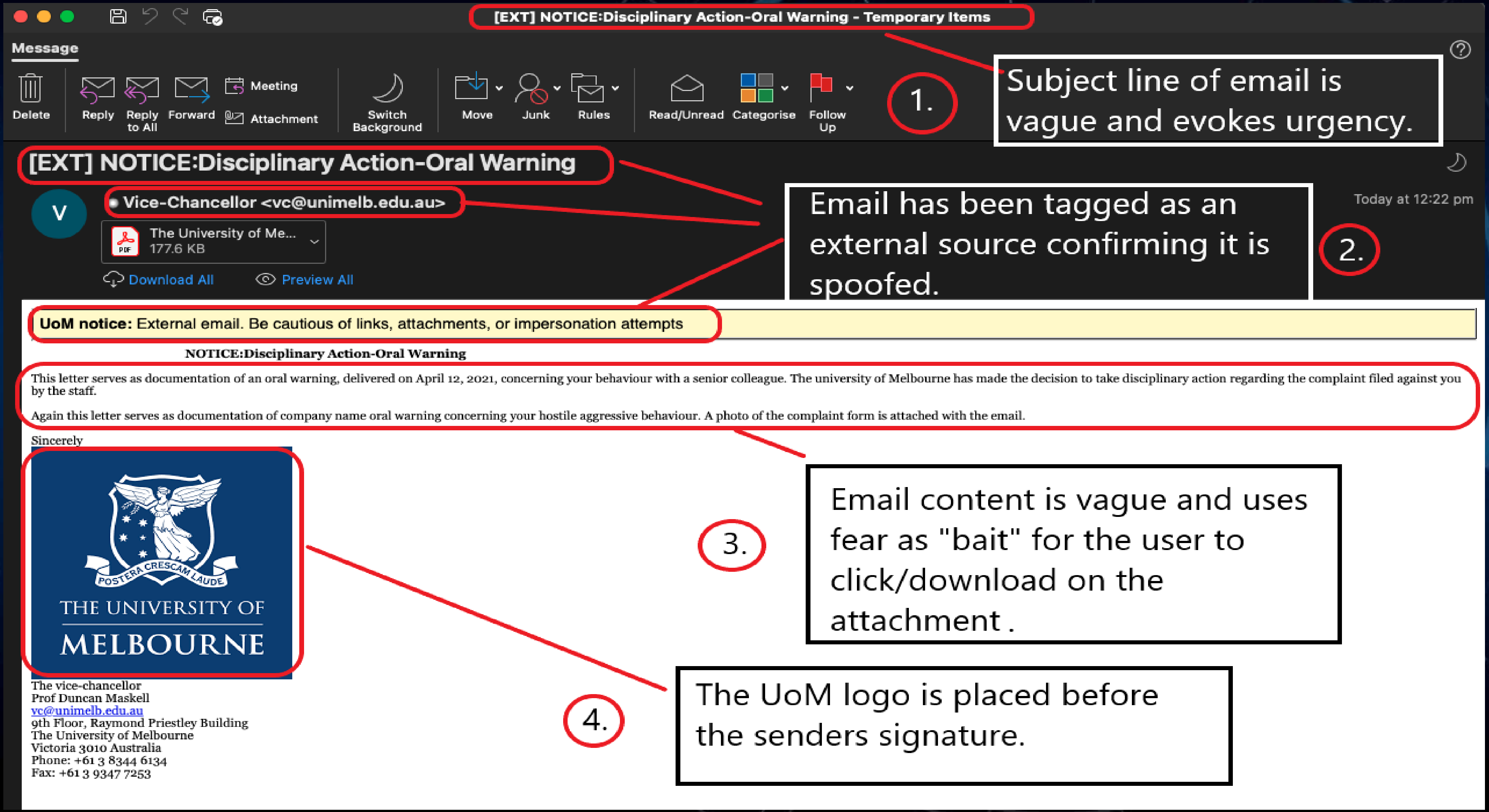
Sunday, 29 March 2020

You are due to receive an ATO refund of $1786.51 . Visit https://ato.gov.au.taxclaim.info/login And complete security check to claim refund.

Sign-in - myGov

https://ato.gov.au.taxclaim.info/log... 8:42 am

Phishing Examples



[EXT] NOTICE:Disciplinary Action-Oral Warning

Vice-Chancellor <vc@unimelb.edu.au>

Today at 12:22 pm

UoM notice: External email. Be cautious of links, attachments, or impersonation attempts

NOTICE:Disciplinary Action-Oral Warning

This letter serves as documentation of an oral warning, delivered on April 12, 2021, concerning your behaviour with a senior colleague. The university of Melbourne has made the decision to take disciplinary action regarding the complaint filed against you by the staff.

Again this letter serves as documentation of company name oral warning concerning your hostile aggressive behaviour. A photo of the complaint form is attached with the email.

Sincerely

The vice-chancellor
Prof Duncan Maskell
vc@unimelb.edu.au
9th Floor, Raymond Priestley Building
The University of Melbourne
Victoria 3010 Australia
Phone: +61 3 8344 6134
Fax: +61 3 9347 7253

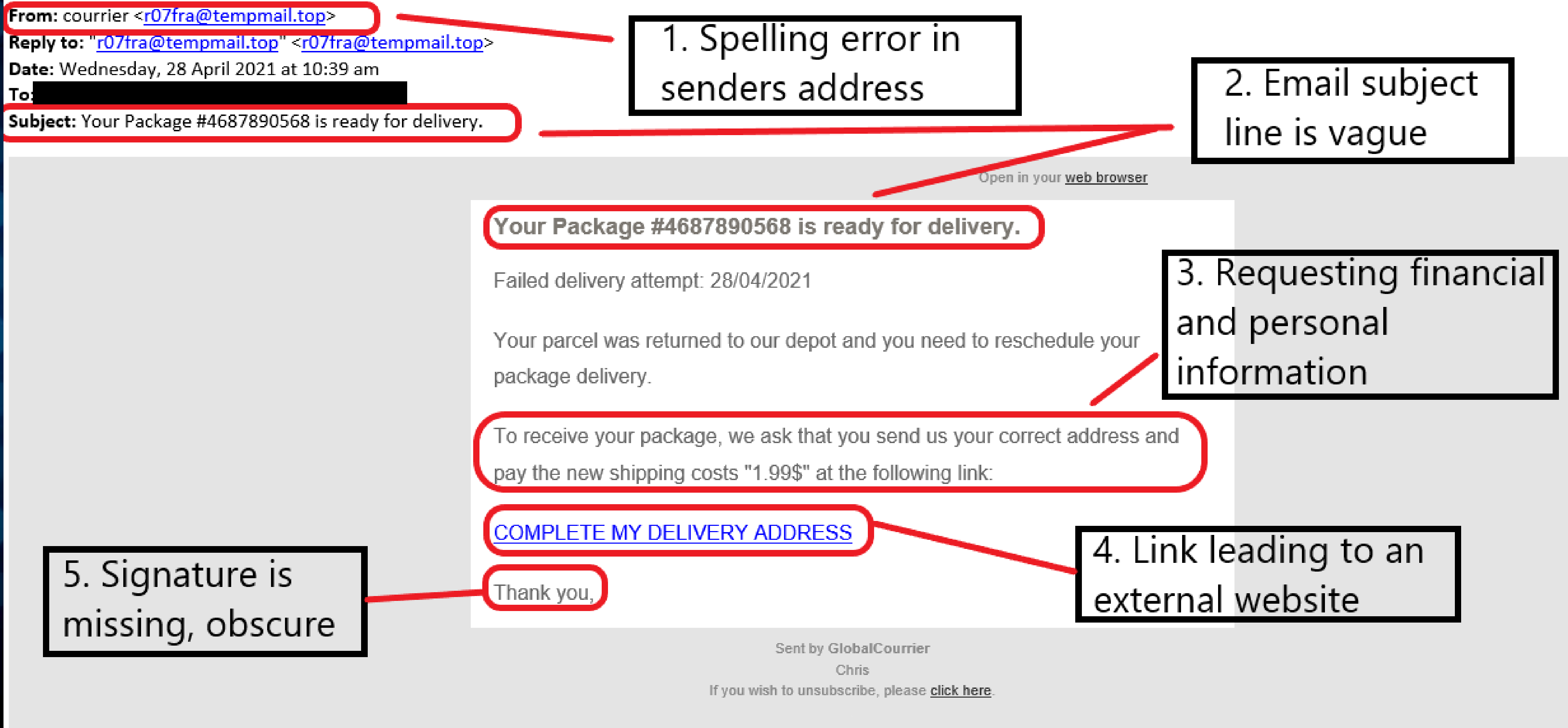
1. Subject line of email is vague and evokes urgency.

2. Email has been tagged as an external source confirming it is spoofed.

3. Email content is vague and uses fear as "bait" for the user to click/download on the attachment .

4. The UoM logo is placed before the senders signature.

Phishing Examples



From: courrier <r07fra@tempmail.top>
Reply to: "r07fra@tempmail.top" <r07fra@tempmail.top>
Date: Wednesday, 28 April 2021 at 10:39 am
To: [redacted]
Subject: Your Package #4687890568 is ready for delivery.

Open in your web browser

Your Package #4687890568 is ready for delivery.

Failed delivery attempt: 28/04/2021

Your parcel was returned to our depot and you need to reschedule your package delivery.

To receive your package, we ask that you send us your correct address and pay the new shipping costs "1.99$" at the following link:

COMPLETE MY DELIVERY ADDRESS

Thank you,

Sent by GlobalCourrier
Chris
If you wish to unsubscribe, please click here.

1. Spelling error in senders address

2. Email subject line is vague

3. Requesting financial and personal information

4. Link leading to an external website

5. Signature is missing, obscure

Ransomware

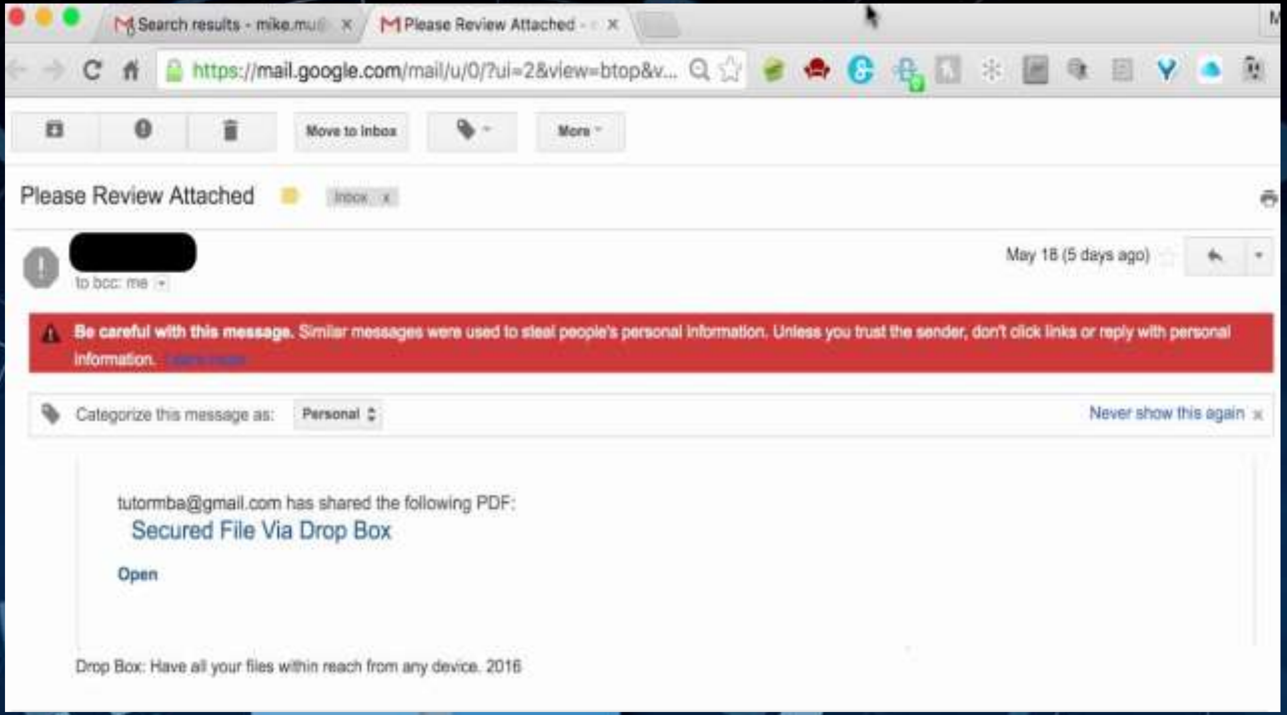
Type of malware that encrypts data specifically asking for payment in order to restore access.

How?

- Email attachments
- Website downloads
- Email links
- Website links

Protect Yourself

- Regular backups
- Updates
- Verify emails
- Don't PAY!



Please Review Attached

[redacted]

to bcc: me

May 18 (5 days ago)

Be careful with this message. Similar messages were used to steal people's personal information. Unless you trust the sender, don't click links or reply with personal information. Learn more

Categorize this message as: Personal

Never show this again

tutormba@gmail.com has shared the following PDF:

Secured File Via Drop Box

Open

Drop Box: Have all your files within reach from any device. 2016

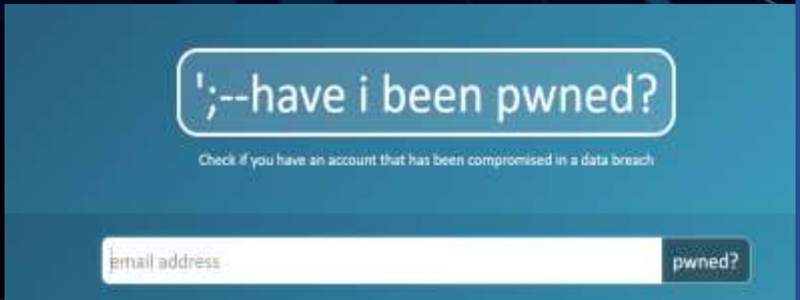
Why is Cyber awareness so important?

- Everything is CONNECTED!
- Personal documents
- Identity
- Finances
- Digital footprint

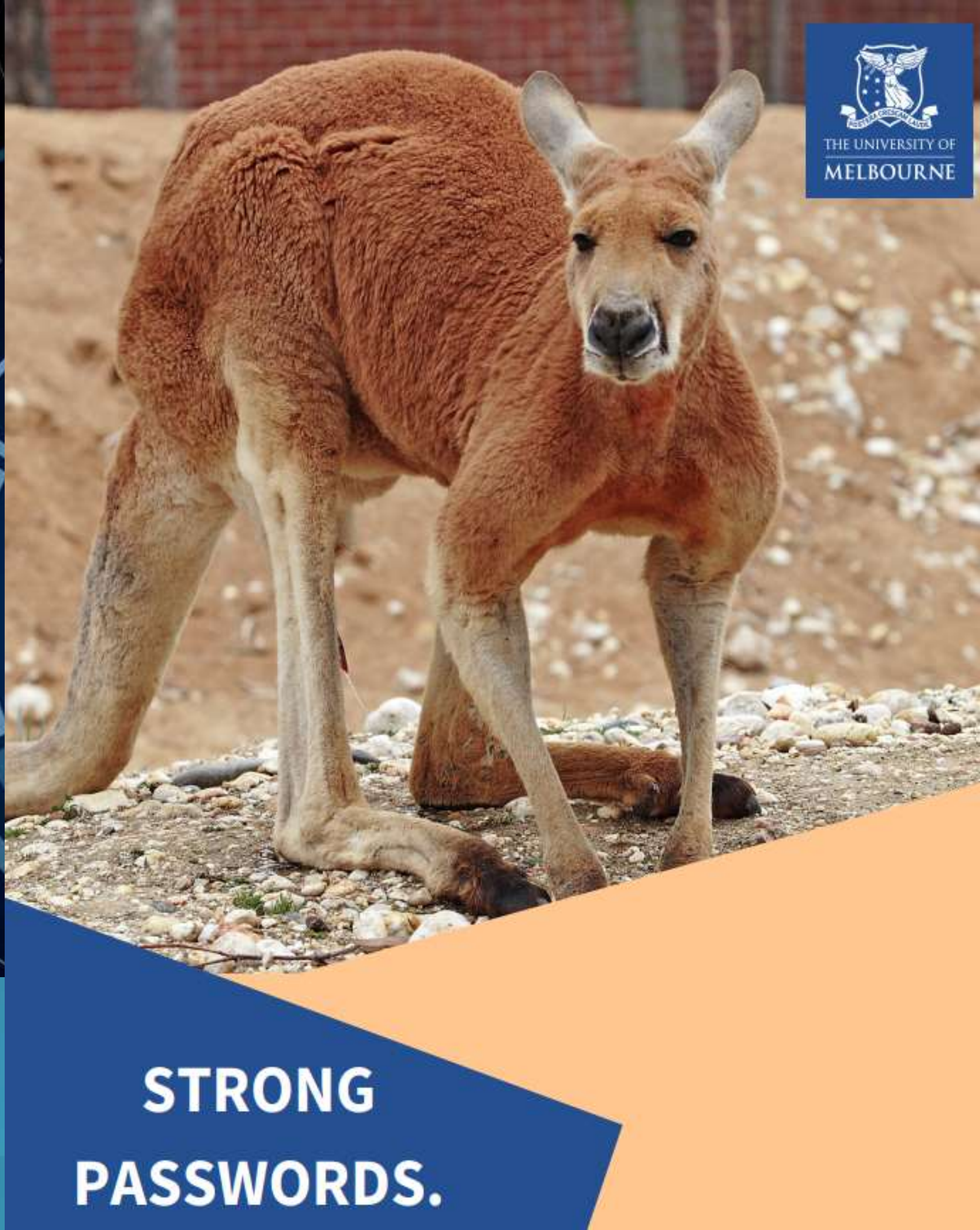
How can I protect myself?

Passwords

- Long and strong. Passphrases
- Enable 2FA where possible
- Change default passwords
- Don’t reuse passwords across accounts
- **Use a Password manager (LastPass is FREE)**

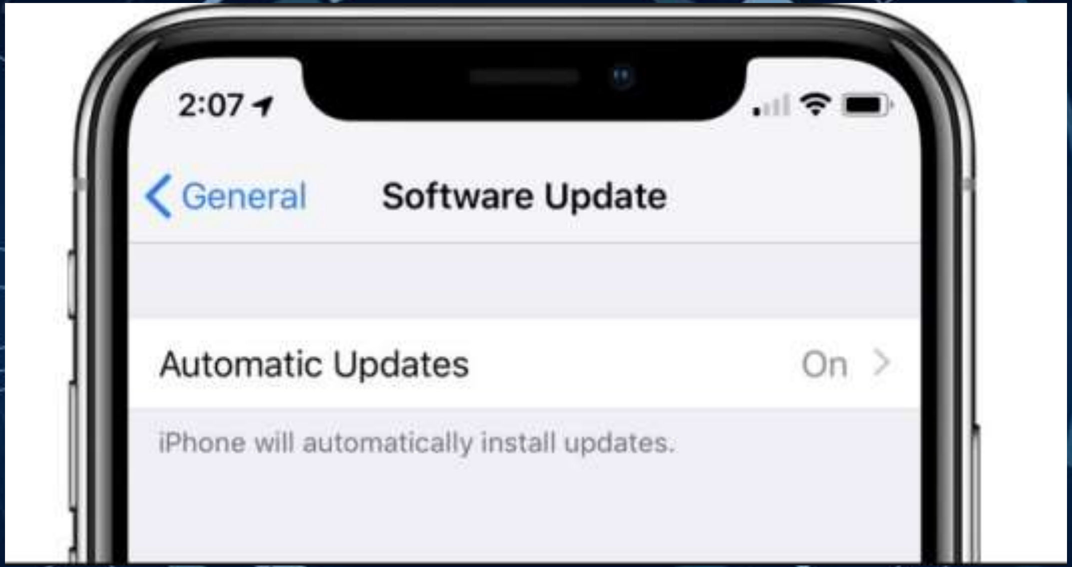

';--have i been pwned?

Check if you have an account that has been compromised in a data breach



Updates

- Ensure all devices are on their latest updates.
- Turn on AUTOMATIC UPDATES
- Make time for updates
- Spring clean your apps regularly



Automatic Updates On

iPhone will automatically install updates.

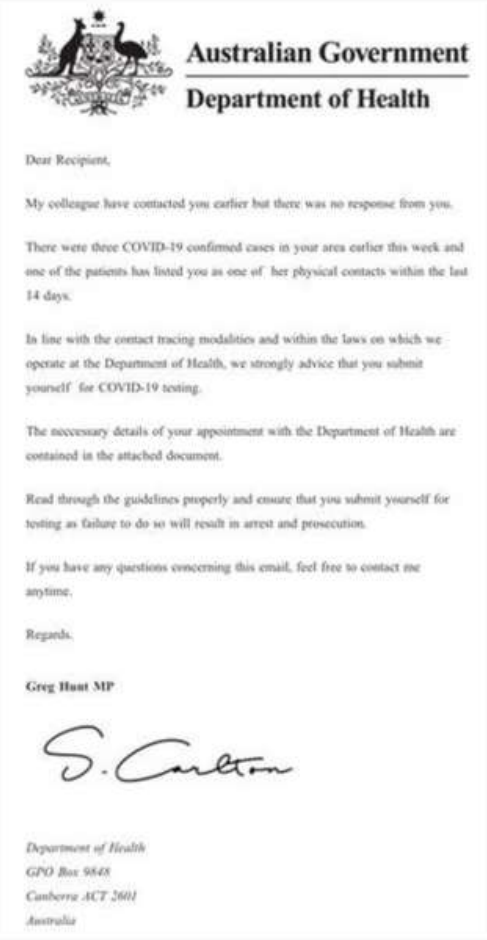
Be aware of Scams

1. Phishing - email
2. Vishing – phone call
3. Smishing – text messages

Look out for:

1. Urgency
2. Asking for personal/financial information
3. Unsolicited
4. Contain links and downloadable files
5. Bad grammar
6. Too good to be true

Department of Health impersonation email



Australian Government
Department of Health

Dear Recipient,

My colleague have contacted you earlier but there was no response from you.

There were three COVID-19 confirmed cases in your area earlier this week and one of the patients has listed you as one of her physical contacts within the last 14 days.

In line with the contact tracing modalities and within the laws on which we operate at the Department of Health, we strongly advice that you submit yourself for COVID-19 testing.

The necessary details of your appointment with the Department of Health are contained in the attached document.

Read through the guidelines properly and ensure that you submit yourself for testing as failure to do so will result in arrest and prosecution.

If you have any questions concerning this email, feel free to contact me anytime.

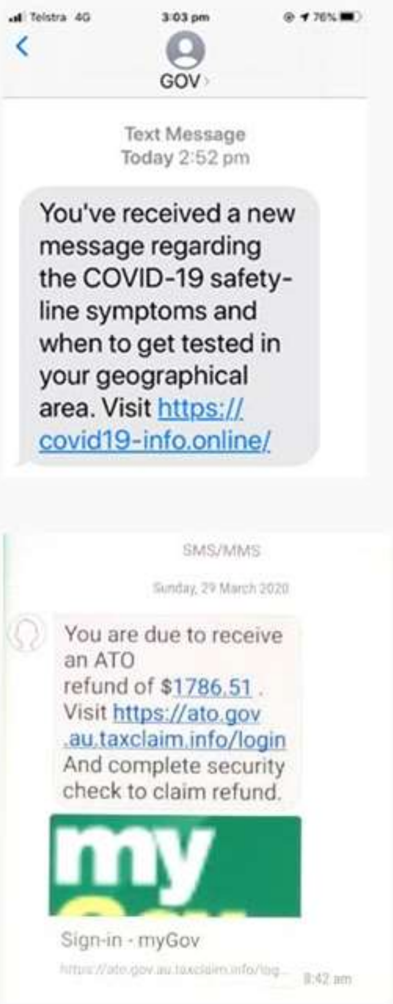
Regards,

Greg Hunt MP

S. Carlton

Department of Health
GPO Box 9848
Canberra ACT 2601
Australia

Fake myGov texts



Text Message
Today 2:52 pm

You've received a new message regarding the COVID-19 safety-line symptoms and when to get tested in your geographical area. Visit https://covid19-info.online/

Sunday, 29 March 2020

You are due to receive an ATO
refund of $1786.51 .
Visit https://ato.gov.au.taxclaim.info/login
And complete security check to claim refund.

Sign-in - myGov
https://ato.gov.au.taxclaim.info/log... 8:42 am

Search Yourself (Digital Footprint)

- Privacy controls
- Be mindful of what you share
- Review app privacy collection

Creating a Cyber secure home checklist

- Are my devices secure?
- Using VPN to access University systems?
- Beware of using FREE Wi-Fi
- Do I have anti virus installed?
- Am I backing up my important files? Cloud & Local
- Are my devices up to date?
- Enable two-factor authentication (2FA) where possible
- STOP. THINK BEFORE YOU CLICK.

How can you help?

- **Report suspicious emails** : spam-report@unimelb.edu.au
- Got a question? Service Now ticket
- Yammer & Slack
- Sign up for free cyber alerts (Australian Cyber Security Centre)
- GET IN TOUCH!

THE UNIVERSITY OF MELBOURNE

Helpful Websites

- Scamwatch
- Stay Smart Online
- SANS Security Awareness Blog

SCAMWATCH

STAYSMARTONLINE

SANS Security Awareness Blog

Read the latest in security awareness, walk away with actionable tips and insight in keeping your organization secure.

Thank you!