Cyber Threats & Defence

Internet Safety for the Everyday Person.

Ben Short

The views and opinions expressed in this Presentation are those of the speaker and do not necessarily reflect the official policy or position of Tasmanian Government and/or Department of Health Tasmania.

Any content provided by the speaker are of their opinion and are not intended to malign any religion, ethnic group, club, organisation, company, individual or anyone or anything.

The material and information contained in this presentation is for general information purposes only. You should not rely upon the material or information on the website as a basis for making any business, legal or any other decisions. Whilst we endeavour to keep the information up to date and correct, the speaker makes no representations or warranties of any kind, express or implied about the completeness, accuracy, reliability, suitability or availability of the information provided. Any reliance you place on such material is therefore strictly at your own risk. The speaker will not be liable for any false, inaccurate, inappropriate or incomplete information presented.

About Me

- Senior Cybersecurity Operations Officer for DOH
  - SOC Analyst!
- Working for DOH for 14 years
- Member of Australian Information Security Association
- Previous Vice President for IT Professionals Association

What is a SOC Analyst?

"A SOC Analyst is a professional who deals with a company's cyber security and security operations. They are the first to respond to and take action against cyber-attacks. They identify, analyse and resolve the issues related to security"

- Monitor the security access and report probable cyberattacks to a superior employee in the company
- Receive threat intelligence and prepare risk and impact analysis for the employer.
- Find cybersecurity breaches, along with their root cause
- Create reports that will allow management to make changes in the security policies as per the needs of the organisation
- Come up with improvement strategies for better security

Tonight's Topics

- Then and Now - How cyber threats have changed
- Cybercrime Trends
- Common online threats
- Defending against online threats

Threats of the Past

- Simpler Times!
- File based Viruses & Trojans
- Intent primarily to damage/destroy
- File based Antivirus Detection

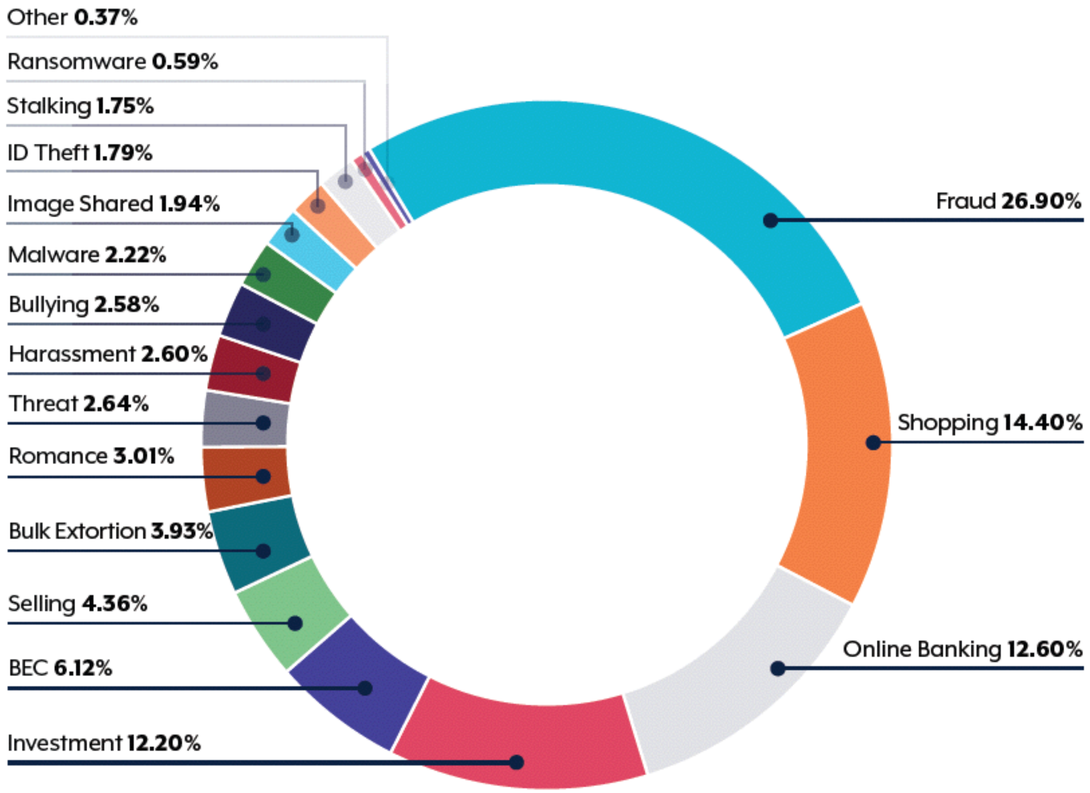
Modern Threats

- More Complex
  - Spread via networks
  - Many different execution methods
- Antivirus is changing.
- Phishing and Social Engineering
- Intent to Leverage Data against you
  - Extort
  - Impersonate
  - Destroy - Last Resort

Australians lost a record amount of more than $3.1bn to scams in 2022, up from the $2bn lost in 2021, according to ACCC figures.

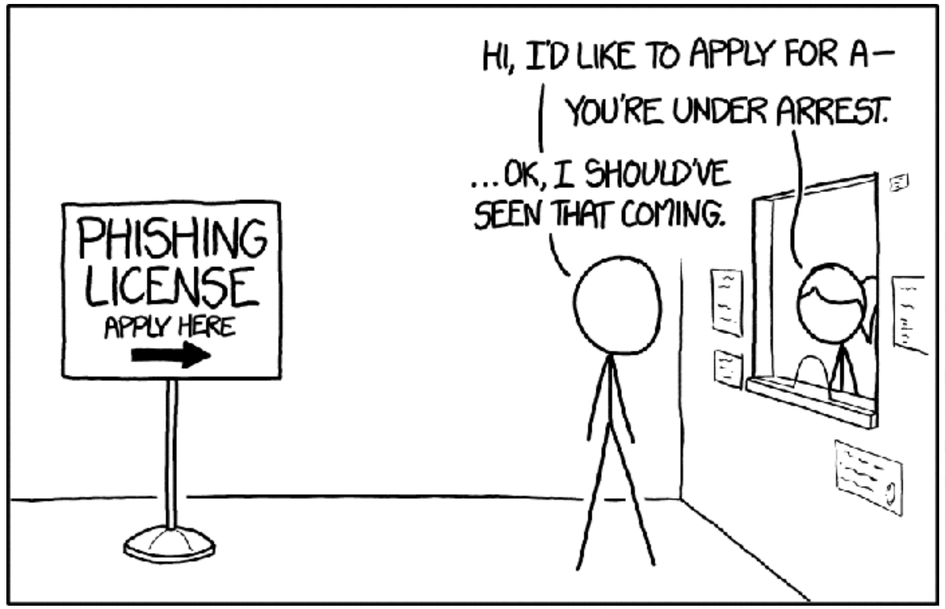
Cybercrime Trends

- An increase in financial losses due to BEC to over **$98 million.** an average loss of **$64,000** per report.
- A rise in the average cost per cybercrime report to over **$39,000** for small business, **$88,000** for medium business, and over **$62,000** for large business an average increase of **14 per cent**.
- A **25 per cent increase** in the number of publicly reported software vulnerabilities worldwide.
- Over **76,000** cybercrime reports
  - an increase of **13 per cent** from the previous financial year.
- A cybercrime report every **7** minutes on average compared to every **8** minutes last financial year.
- **150,000 to 200,000** Small Office/Home Office routers in Australian homes and small businesses vulnerable to compromise including by state actors.
- Fraud, online shopping and online banking were the top reported cybercrime types, accounting for **54 per cent** of all reports.



https://www.cyber.gov.au/about-us/reports-and-statistics/acsc-annual-cyber-threat-report-july-2021-june-2022

Phishing



- Estimated 3.4billion Phishing & Spam emails sent every day. Thats over 48% of all email each day.
- Phishing emails & messages:
  - May have a malicious attachment
  - May send you to a malicious website
  - Might make a threat or demand.

If you suspect the email or message is phishing, delete and do not interact with it.

Phishing - Spotting the Lure

Sender

- Does the email address match the sender?
  - e.g. PayPal Support (support@paypal.com) vs PayPal Support (jerry56b2@gmail.com)
- Is the Sender From: correct in spelling and grammar?
  - e.g. "PayPal Support (support@paypal.com)" vs "Paypal Supp0rt (jerry56b2@gmail.com) "
- Do you recognise the sender?
- Does the subject match the content of the email?
- Is the email a reply to a message I never sent?

Content

- The email asks me to take an action to avoid a negative consequence.
- The email is out of the ordinary, has poor grammar, or spelling errors?
- Do I have an uncomfortable gut feeling about the email's requests to open an attachment or click a link?
- Is the email asking me to view a compromising or embarrassing picture of myself or someone I know?

Attachments and Links

- Hovering over links in the email presents an an unusual or suspicious destination.
- The email only has long hyperlinks with no further information, and the rest of the email is completely blank.
- The email has a hyperlink that is a misspelling of a known website.
- The attachment has a suspicious file type. The only file type that is always safe to click on is a .txt file.

Don't Take the Bait!

Social Engineering

At its core, social engineering is not a cyber attack. Instead, social engineering is all about the psychology of persuasion.

The Nigerian Prince!

Usually seeking you to reply, and asking for personal information or money transfers.

Be particularly careful if buying or selling things online - chargeback scams.

Message headers can be forged to appear to be from someone trusted. If the message seems unusual contact the person directly via phone or in person, not by the medium the message was received.

Typical Social Engineering Scams

Simple:

- Offers of Money (The Nigerian Prince)
- "Legal" Letters of Demand
- Offers of Romance

More Complex

- Impersonation of Executives
- Business Email Compromise
- REAST bank transfer - a close call!

Data Breaches

- Medibank. Latitude. Optus.

- A wealth of different information depending on who/what was breached
- That information will be available online, forever.
- Carefully read any data breach notification you receive to understand how it will affect you and the information disclosed.
    - Update compromised identity documents as soon as possible.

Phone Porting

Phone porting is the way to transfer a phone number to a new carrier.

Fraudulent porting sees a threat actor take over a phone number by social engineering or fraud activities, giving them access to 2FA.

Scary!

Now harder to do than 5 years ago:

https://www.legislation.gov.au/Details/F2020L00179

https://www.abc.net.au/news/2023-08-09/melbourne-identity-theft-victims-lose-money-fraudsters/102701944

Port a mobile phone number

The **Mobile Number Portability Code** sets out the procedures for porting a mobile phone number between telcos.

The key requirements include:

- before porting a number, you must check that the customer is the rights-of-use holder
- 90% of ports must be completed within 3 hours
- 99% of ports must be completed within 2 business days
- if a port is a mistake or unlawful (for example, if someone has stolen a number), follow the port reversal process in the code.

The Industry Standard aims to:

- provide safeguards
- address harms caused by mobile number porting fraud.

It sets out extra steps you (as the gaining telco) must take to verify the identity of those requesting ports prior to the request being actioned. These steps can vary across retail, call centre or online environments. You must also publish customer awareness and safeguard information on your website.

The identity processes:

- Retail—telco calls the mobile number to be ported while customer is in store. Telco verifies the call has been received by the customer's mobile device.
- Call centre—telco calls back the mobile number to be ported to check that the person asking for the port is the actual customer.
- Online—a unique verification code is sent via SMS to the customer's mobile device. This code is then verified by the customer.

You may only verify identity using documents or a government online verification service if you are unable to use one of the above identity processes – such as if the mobile device associated with the number is lost, stolen or damaged.

How to Survive the Internet

1. Become a Password Ninja

"If I had only 1 piece of Advice to give…."

- Do not re-use Passwords!
  - consider having 2-3 different passwords for different login types.
- Ideally, use a password manager
  - Doesn't need to be software!
  - Software managers offer unique passwords for all your logins
  - Some managers provide breach notifications and scoring
- Start using pass phrases instead of passwords.

  e.g. "gladly stifled breach" vs "698Gnau&mXI["

2. Use Multi-factor Authentication

Something you know, something you are, something you have.

MFA is a great extra layer of protection in case your password is compromised.

SMS or Authenticator Apps (even built in to password managers).

Security Tokens & Passkeys

- Passwordless!
- Security tokens are bound to hardware.
- Passkeys are stored in a identity store that can be synced between devices

Can be complex to use, so you may only wish to set up and use for important services like online banking.

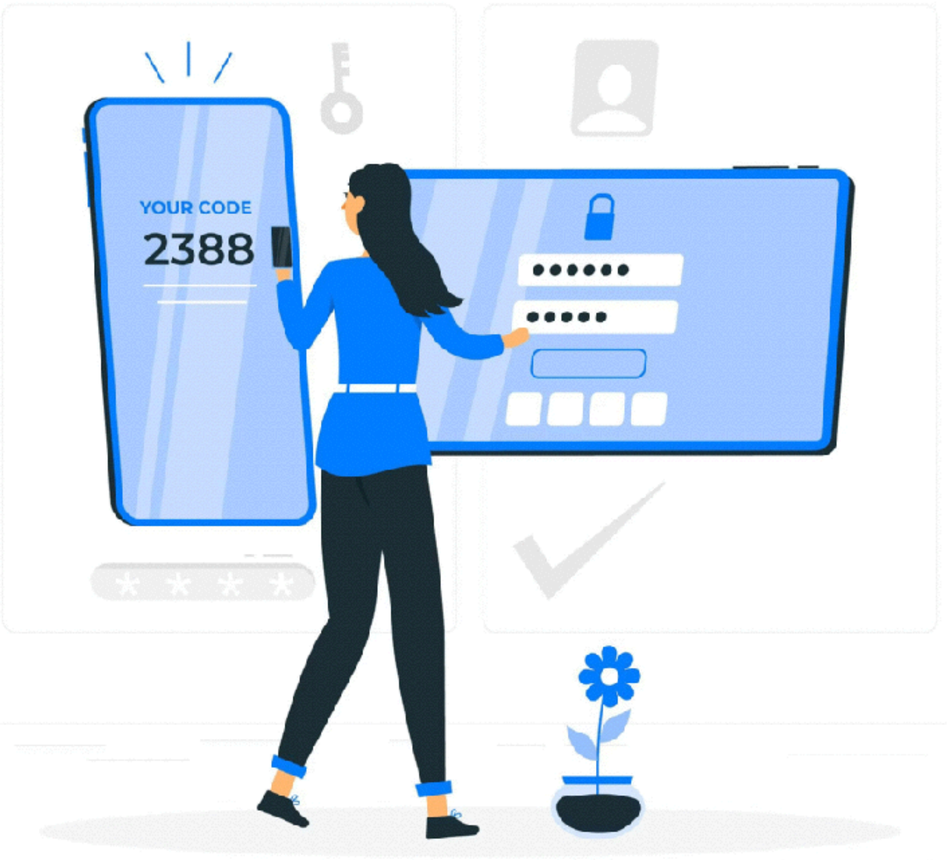


Image by storyset on Freepik

3. The Magic Word

Abracadabra?

A powerful tool to protect against family social engineering.

Share a “Magic Word” with the family.

Can be used in Email, SMS, Phone Calls! Easy 2FA!

4. Have a Second Email Address

Spam Spam, go away, try to phish me again another day…

To protect your personal email address from data breaches, consider setting up a second email address that you use to sign up to websites and other higher risk sites.

Apple Hide My Email, Firefox Relay, Proton SimpleLogin or Trashmail are examples of email alias services.

5. Patch your Devices Regularly

Image by rawpixel.com on Freepik

Patching your computer regularly defends your computer against exploitable attacks from threat actors.

Updates usually come out monthly for operating systems and variable but often for applications.

Pay particular attention to ensuring the following things are regularly updated:

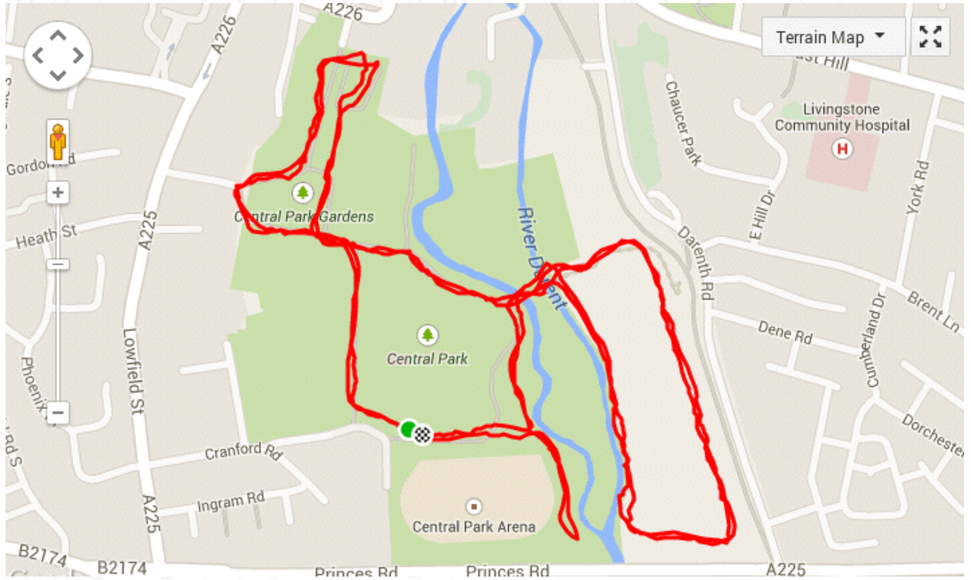
- Operating System
- Web Browser
- Office Suite

6. Be Aware of what you Share

Sharing is caring, or is it?

Everything you share about yourself online can be used to build a profile about you:

- Birthday on Facebook
- Job Information on LinkedIn
- Location Information from Photos
- Callsign on ACMA Database!



Be aware of how that information might be used.

https://www.abc.net.au/news/2023-07-11/russian-military-official-on-ukraine-blacklist-assassinated/102589668

Connected Application/Websites

- Easier for authentication/integration
- Again, be aware of the information they have access to
- Regularly review what you have given access to because sometimes the apps are abandoned and sold/taken over by someone else!

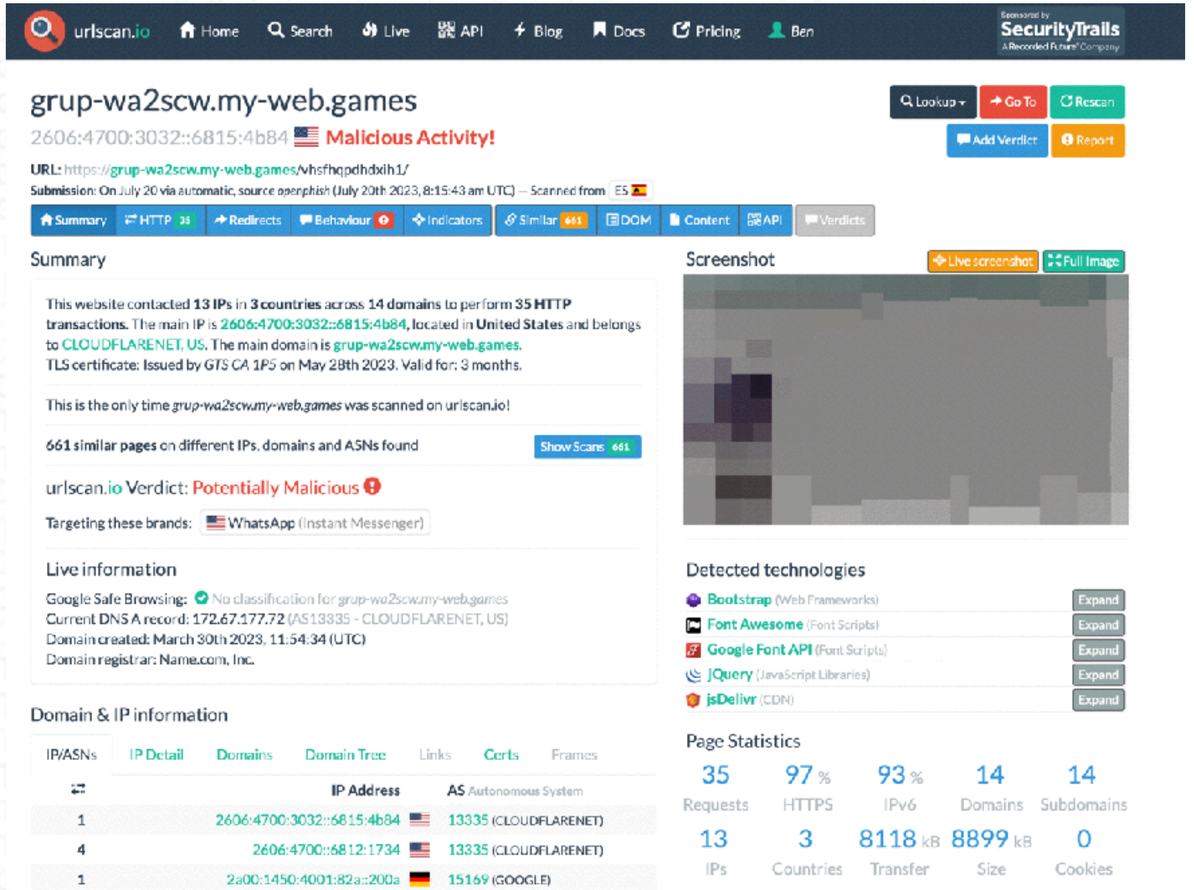
7. Sandbox it!

Sandboxes aren't just for kids

For when you aren't sure.

Tool to safely check URLs and Files (inc. Email) not using your computer.

Its what the Cybersecurity People do!



8. Back it up!

3….2….1….

Image by studiogstock on Freepik

Backups are your best defence against ransomware, or “accidents” too.

Backup Ninjas have the following rules:

- 3 copies of the data (including “live” data)
- 2 different types of backup media
- 1 backup stored offline/offsite.

Don’t leave *all* your backup media plugged into computer.

9. Protect your Data

3….2….1….again…

e-waste is now becoming a significant source of information when devices are disposed without being wiped or reset:

- Wifi Passwords
- ISP Account Details
- Everything Else that is on Mobile Devices, Computers etc..

Always wipe or destroy external storage devices

- In most cases a simple format is not a secure wipe.
- 3-pass secure wipe.

If possible, turn on disk drive encryption (FileVault, Bitlocker etc..).

Always factory reset devices like mobile phones, tablets when disposing/selling.

Question Time!

Image by rawpixel.com on Freepik

Slides & Extra Information from Tonight:

https://www.tribesmanjohn.au/infosec/