Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

Cyber Security and the Healthcare Sector

RACS ‘Preparation for Practice’
July 2023

Nick Sincock
Cyber and Infrastructure Security Outreach

Australian Government
Department of Home Affairs

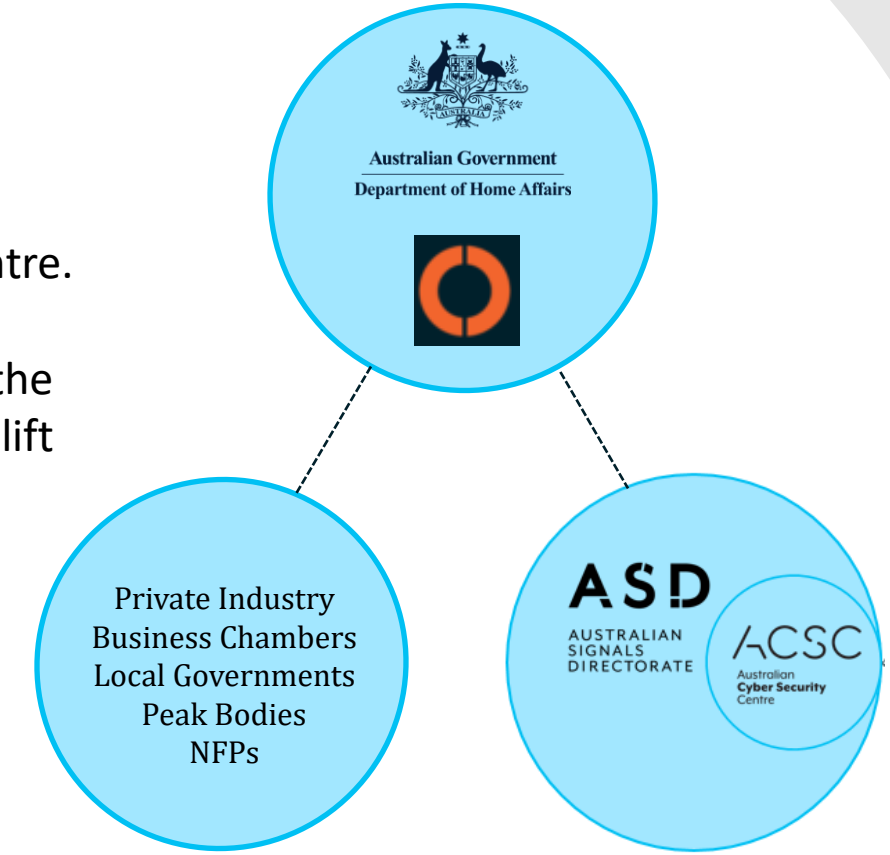
CYBER AND INFRASTRUCTURE SECURITY CENTRE

CISC Outreach Network

The Outreach Network has a national footprint, with officers embedded in each state office of the Australian Cyber Security Centre.

Officers work collaboratively with other areas of the Department, the ACSC, State and Territory Governments, and industry experts to uplift the security and resilience of critical infrastructure entities.

- **Cyber security uplift and advice**
- Insight regarding critical infrastructure reforms
- All-hazards risk management
- Amplification of the Australian Cyber Security Strategy



Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

Critical Infrastructure Sectors and Assets

Energy


Liquid Fuel


Gas


Energy Market Operator


Electricity

Communications


Broadcasting


Domain Name Systems


Telecommunications

Data


Data Storage or Processing

Food & Grocery


Food and Grocery

Defence


Defence Industry

Water & Sewage


Water

Healthcare


Designated Hospitals

Space Tech


Space Industry

Higher Education


Education

Financial Services & Markets


Superannuation


Financial Markets and Infrastructure


Banking


Insurance

Transportation


Ports


Freight Infrastructure


Freight Services


Aviation


Public Transport

Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

What happened in 2021-22 (that was reported)

- 76,000 cybercrime reports via ReportCyber, equivalent to **one report of a cyber attack every 7 minutes**.
- Cost of cybercrime up to **$33 billion** in Australia.
- Average self-reported loss was **$39,000** for **small businesses** and **$88,000** for medium businesses **(on average)**
- Approximately **52%** of **ransomware** cybercrime reports were by small-medium businesses
- No sector of the Australian economy is immune - Government, industry, families and individuals were all targeted.

Who Commits Cyber Crime?

Cybercriminals are individuals or teams of people who use computer technology to steal personal/confidential information and then sell or distribute it.

- **State-Sponsored Actors**
- **Foreign Intelligence Services**
- **Organized Cybercrime Syndicates**
- **Trusted Insiders (Malicious/Neglectful)**
- **Hacktivists**
- **Terrorists**
- **Scammers**
- **Trolls**
- **Internet Stalkers**

Australian Government
Department of Home Affairs

CYBER AND
INFRASTRUCTURE SECURITY
CENTRE

Why the Healthcare and Medical Sector?

Australian Government
Department of Home Affairs

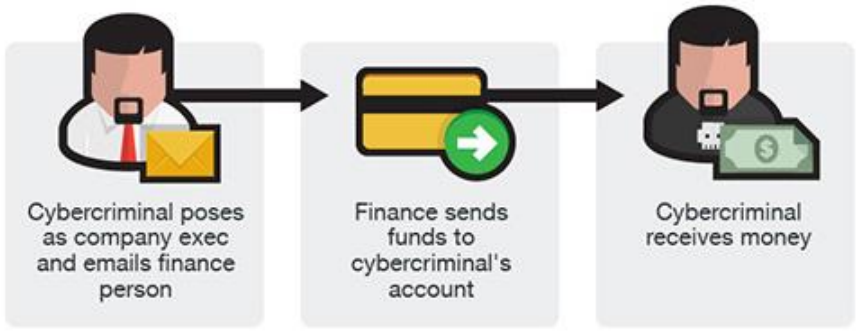
CYBER AND INFRASTRUCTURE SECURITY CENTRE

Why the Healthcare Sector?

Aside from the universal risks faced by every individual and business that operates online, the Healthcare Sector has some unique vulnerabilities:

- **Volume and sensitivity of data holdings**
- **Increasing cyber surface area**
- **Importance of sustained access**
- **Susceptibility to stressed resources**
- **High-trust industry a target for scams**

Common Cyber Security Threats

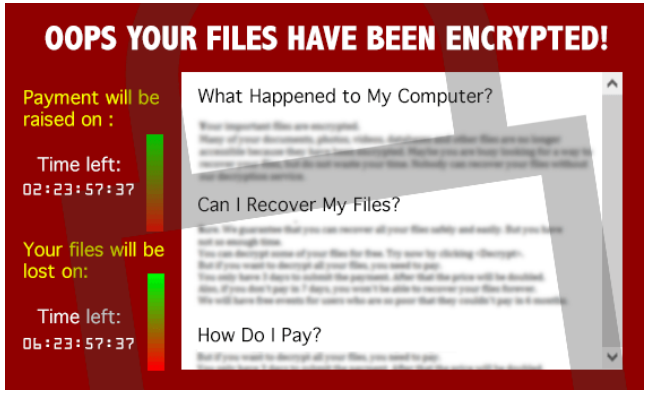


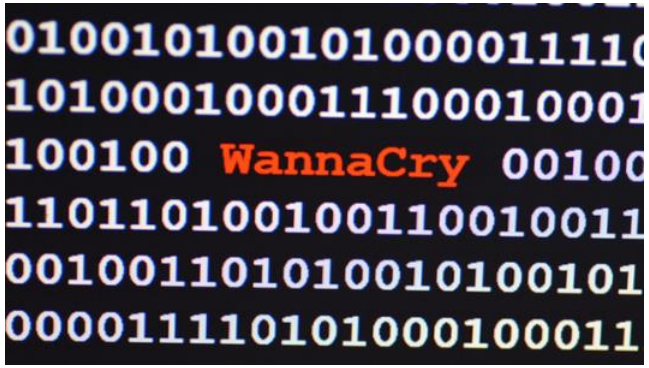
Phishing (scam attempts)
- Malicious links, calls, SMS
- Can be random or targeted
- *Case study: Transportationgov.net*

Ransomware (a nasty type of malware)
- File encryption, ransom demand
- Double/triple extortion
- *Case Study: Colonial Pipeline*

Business Email Compromise (BEC)
- Invoice fraud
- Employee or company impersonation
- *Case Study: Small Biz double invoice*

NHS could have avoided WannaCry hack with 'basic IT security', says report

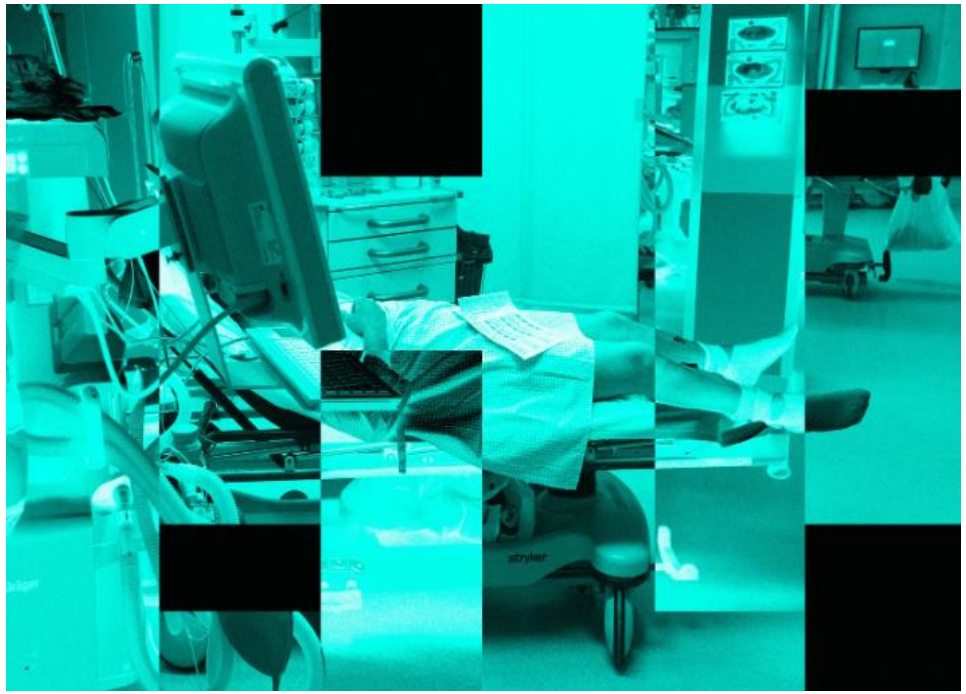




Case Study - WannaCry Ransomware, Sep 2017:

- North Korean cyber actors executed the attack, designed to indiscriminately target Microsoft Windows systems and demand ransom in bitcoin.
- The attack significantly affected hospital systems around the world, including the UK's National Health Service (NHS).
- A large portion of NHS healthcare trusts and providers, such as general practitioners, experienced shutdowns and lockouts of devices and systems, preventing the function and delivery of healthcare services.
- This resulted in the cancellation of over 19,000 medical appointments and caused more than GBP92m in damages and recovery costs.

The untold story of a cyberattack, a hospital and a dying woman



Case Study - German University, Sep 2020:

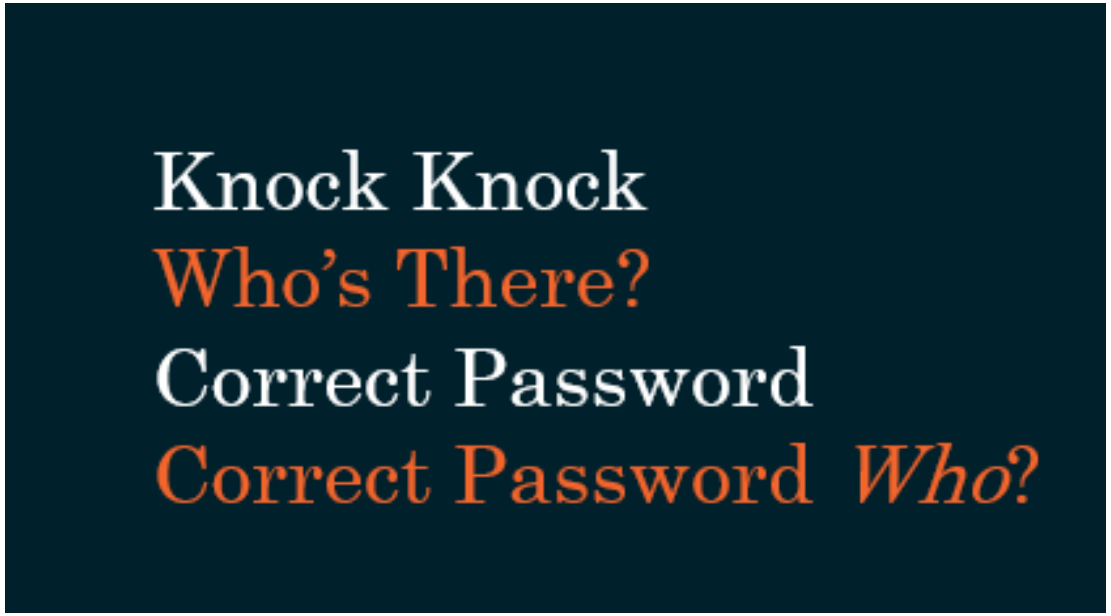
- Cybercriminals deployed ransomware against a German university affiliated with a hospital, disrupting its computer systems.
- An individual being transported to the hospital by ambulance had to be re-routed to another hospital 30km away. She passed away en-route.
- The actors stopped the ransomware attack (by providing the encryption key) after learning they had disrupted the hospital and possibly caused a patient death.

Australian Government
Department of Home Affairs

CYBER AND
INFRASTRUCTURE SECURITY
CENTRE

What can individuals and small businesses do?

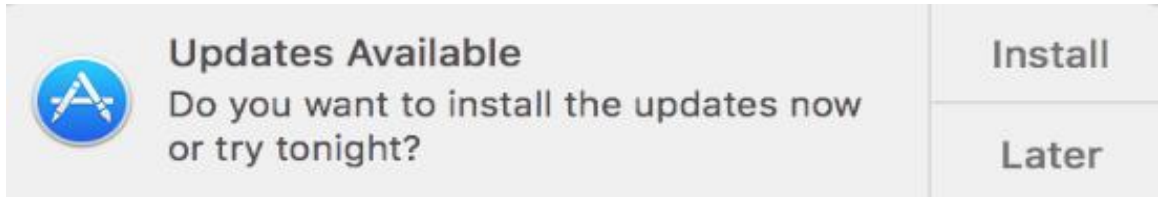
Multi-Factor Authentication



- **Like a free alarm system**
- **Doubles your login security**
- **Easy to set up and use**

Automatic Updates

- **Something you can do *now***
- **Something you can do *once***
- **Set and forget, stay up to date**



Automatic Backups

- **Something you can set up *today***
- **Something you can schedule**
- **Make it automatic and stay secure**

Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

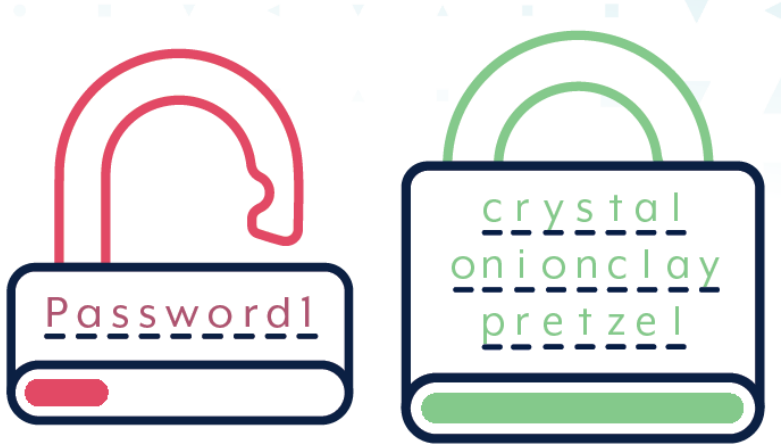
~~P@ssw0rd$~~ - Passphrases

Passwords provide the first line of defence against unauthorized access to your computer and personal information.

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2022

Number of characters	Numbers only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Special Characters
7	Instantly	Instantly	2 seconds	7 seconds	**31 seconds**
8	Instantly	Instantly	2 minutes	7 minutes	**39 minutes**
14	3 minutes	4 years	**64k years**	750K years	16m years

Passphrases



Outs	*Ins*
123456	Number Twenty Two #22
Qwerty!	
Password	Fussy! Messy! Sassy! Bossy?
Mumsname58	
BuddyFranklin23	Spain Sunshine Sausage Band
Wordpass!	
Streetname17	Foggy Camera Mountain Climb

- **Harder to crack against common password attacks**
- **Easier to remember than random characters**
- **Meet password requirements easily**
- **Length beats complexity**

Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

Why use a password manager?

Security & convenience

256-bit AES
Zero Trust
Two-Factor Authentication available
They Are Better Than the Alternative

haveibeenpwned.com

Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

ACSC Resources – cyber.gov.au

Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

1300 CYBER1
2 9 2 3 7 1

Australian Government
Department of Home Affairs

CYBER AND
INFRASTRUCTURE SECURITY
CENTRE

Assess your level of cyber security

[Cyber Security Assessment Tool | Cyber.gov.au]

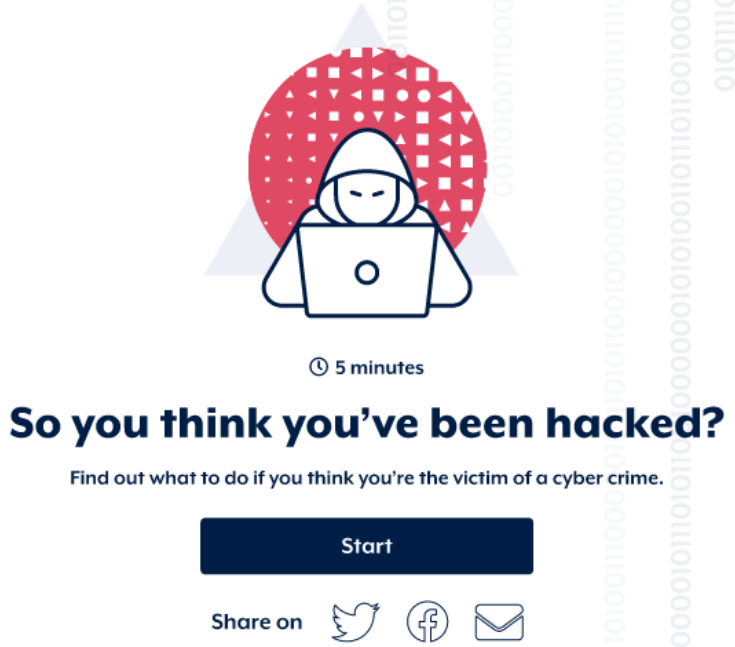
Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

Have you been hacked?

'Have you been hacked?' steps potential victims through a series of scenarios to help assess if they've been hacked, and guide them on how to respond.

Scenarios include ransomware attacks, malware, email compromise and identify theft, as well as phishing and fake website scams accessed via sms and mobile devices.



Tool can be found on cyber.gov.au

Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

Exercise in a Box

All-in-one simulation exercise platform to assess and improve your organisation's cyber security practices and prepare for a cyber incident

- Various options to suit your needs
  - Discussion based exercises
  - Micro exercises
  - Simulation exercises
- Secure and anonymous, guides users through cyber security exercises
- Includes everything you need to plan, set up and deliver cyber exercises to your organisation
- Post activity report function

Scan the QR code or head to cyber.gov.au and search 'Exercise in a Box'

What else can I do?

- **Know how to report a cyber security incident or cybercrime**

  Report the cyber incident to ACSC, via cyber.gov.au/report

  Call the ACSC 24/7 hotline on 1300 CYBER1 (1300 292 371) if you need help.
- **Know your networks -** If you have an IT provider, Managed Service Provider (MSP), and/or cloud services provider, contact them for assistance and advice.
- **Evaluate risks associated with cyber supply chains.**
- **Prepare for a cyber security incident by having incident response, business continuity and disaster recovery plans in place, and testing them.**
- If you or your business have been a victim of identity theft - contact **IDCARE**. They will work with you to develop a specific response plan to your situation and support you through the process. Visit www.idcare.org

Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

Where to Start?

- Sign up to the ACSC's Partnership Program.
- Establish standards on **passwords** & install **MFA** wherever possible.
- Set up **automatic updates** and **backups**.
- Train staff and bring them with you (encourage reporting).
- Visit **cyber.gov.au** and implement their essential mitigation strategies (if you outsource ITS, talk to them about your company's posture).
- Provide feedback / follow up questions via the **QR Code** >>>