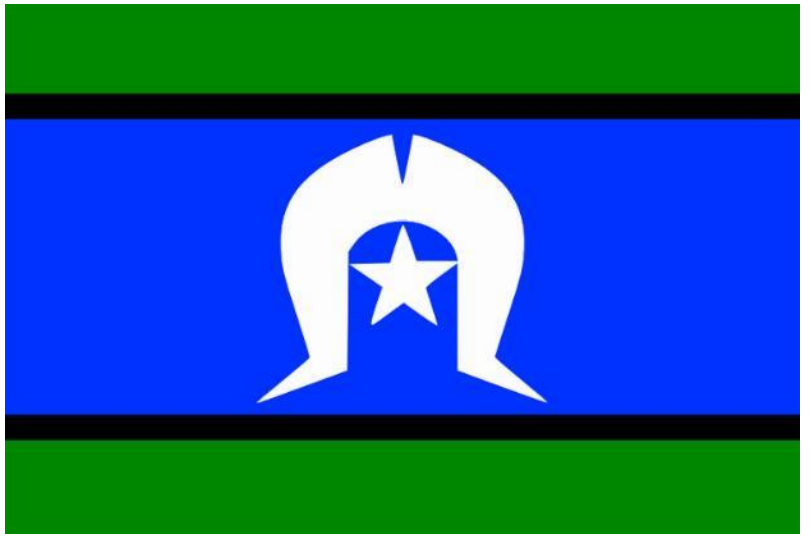
Infoxchange

CYBER SECURITY FOR NFP IT MANAGERS

David McLean, August 2023

We acknowledge the traditional custodians of the land and pay our respects to Elders past, present and emerging.



Today

- Current cyber security landscape
- An overview of cyber security practices organisations should have in place
- Top cyber security incident entry points
- Phishing – real life stories
- Cybersecurity in the NFP sector
- Key takeaways
- Useful resources
- Questions & discussion

Housekeeping

- Please keep your video on & stay on mute (when not asking questions)
- Enter your questions in the chat or raise your hand (virtually or physically). We also have time in the Q&A session at the end
- This webinar is being recorded and will be shared within 2 business days together with a copy of the presentation

Security in the headlines

Oxfam Australia inv... suspected data brea...

Oxfam Australia is investigating a su... that has allegedly impacted the data... supporters.

The database is alleged to have con... addresses and phone numbers, for...

Source: https://www.itnews.com.au/news/... breach-560690

medibank medibank

An update on o... cyber incid...

Dear xxx,

Since I last wrote to you there has be... ...ient relating to our current cyber incident.

As we have wo... ...ta breach, ...g transparent about what we ...and the broader community

Top Stories

Medibank confirms client data posted on dark web after ransom deadline passes

UnitingCare ... attack

Australia's biggest skin cancer study has been hit by an ... with the personal details of more than 1,000 people fear... by hackers.

The ABC can reveal cyber criminals last year broke into servers holding highly sensitive data collected by QIMR Berghofer, a medical research institute based in Brisbane.

...https://www.itnews.com.au/news/unitingcare-queensland-hit-by-cyber-attack-563812

Latitude Financial confirms data hack is far worse than expected with 8 million people's data believed to be stolen

Key points:

- QIMR Berghofer says names, addresses and Medicare numbers ... based ... to the *9News* report.

OPTUS

Urgent update about your personal information

Dear Former Optus Customer,

It is with great disappointment I'm writing to let you know that Optus has been a victim of a cyberattack. As a former Optus customer this has resulted in the disclosure of some of your personal information.

Importantly, no financial information or passwords have been accessed. The information which has been exposed is your name, date of birth, email, phone number, address associated with your former account, and the numbers of the ID documents you provided such as drivers licence number or passport number. No copies of photo IDs have been affected.

Ex-worker who was investigated over child sex accessed sensitive data 260 times in each March 2021

A former caseworker who was investigated for an alleged child sex offence managed to access confidential information on a program for vulnerable kids for months after leaving their job, a report from Victoria's privacy regulator has found.

Source: https://www.abc.net.au/news/2021-03-13/former-contractor-accessed-vic-government-child-data-260-times/13243230

Legislation before Parliament will lift the maximum fine for serious or repeated breaches of the Privacy Act from $2.2m to up to $50m

The latest ACSC statistics

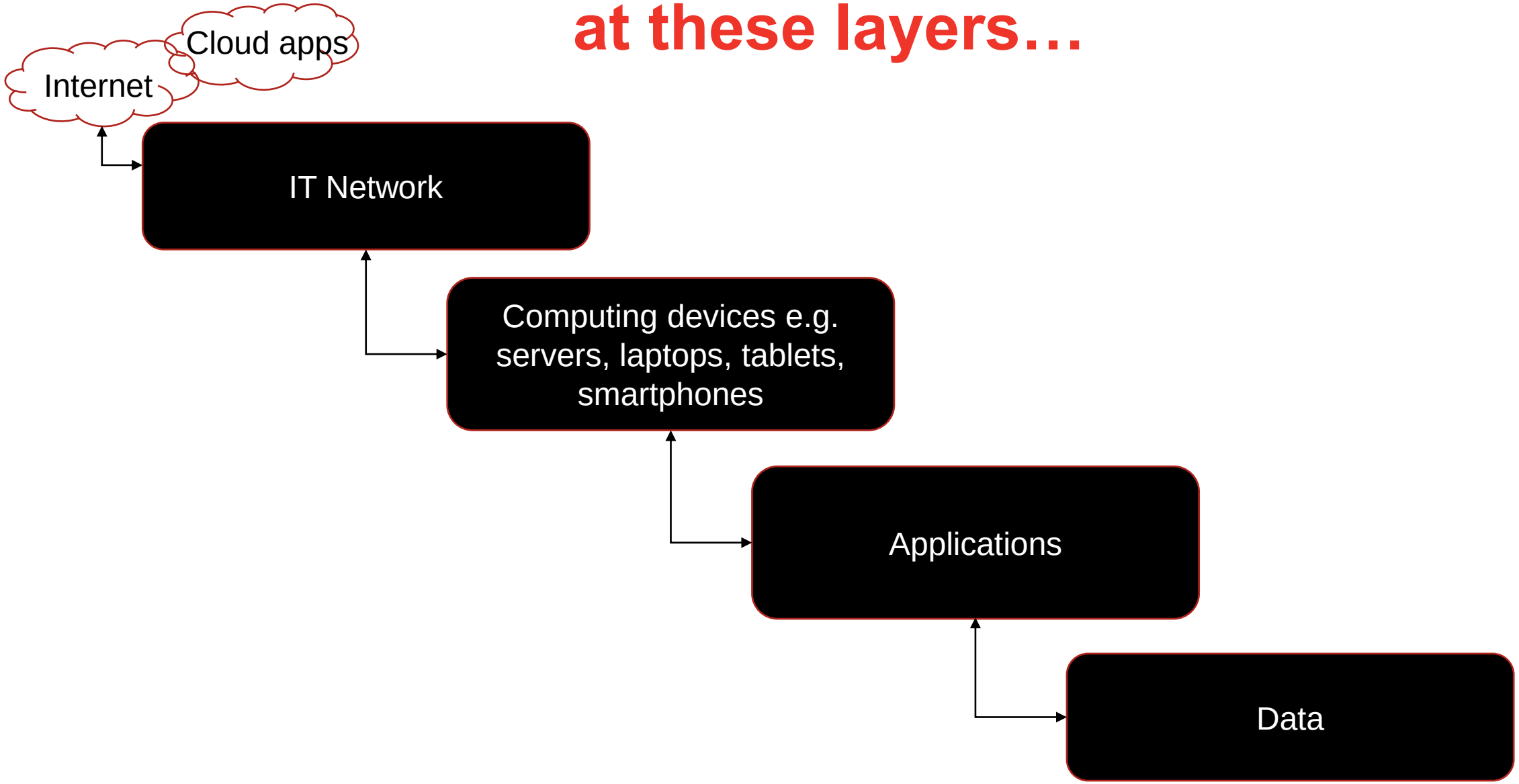
- An increase in financial losses due to email compromise to over $98 million, average loss of $64k per report
- 14% rise in the average cost per reported cybercrime to over $39k for small, $88k for medium & $62k for large businesses
- 25 per cent increase in the number of publicly reported software vulnerabilities (Common Vulnerabilities and Exposures – CVEs) worldwide
- Over 76,000 cybercrime reports an increase of 13 per cent from the previous financial year
- Over 25,000 calls to the Cyber Security Hotline - 69 per day, a 15% increase from last FY
- 150,000 to 200,000 Small Office/Home Office routers in Australian homes and small businesses vulnerable to compromise including by state actors.

Ref: ACSC Annual Cyber Threat Report 2022 (published 4 Nov)

Our challenge

1. NFPs often hold highly sensitive data
2. NFP staff can be more comfortable talking to people than working with technology
3. The human element continues to be a major factor in breaches - a recent global breach investigation report, found 82% of breaches involved the human element
   (Source: Verizon Data Breach Investigations Report 2022)
4. Good system, device and data security practices are also critical to protect our information

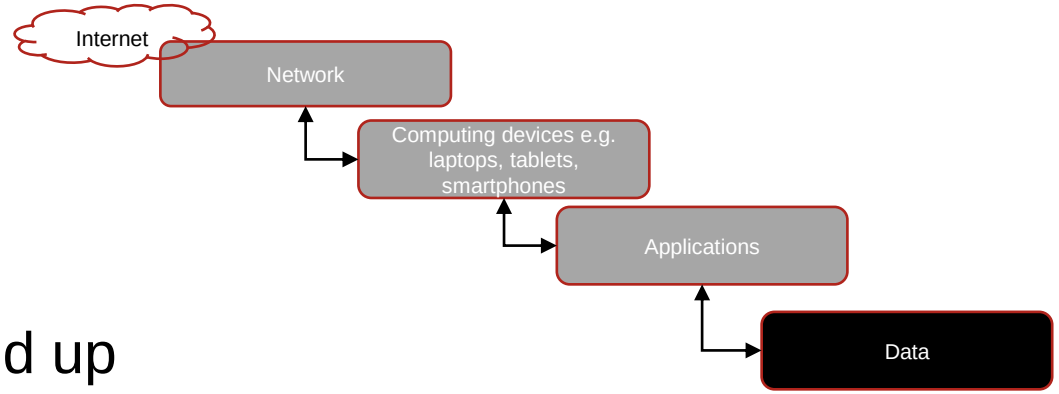
Your organisation should have protection at these layers…



Ask the audience:
Do you provide documented guidance for staff on where to save information?

- Yes
- No
- Not sure

Data protection



- Where to store organisational data so it is backed up
- Handling information of a confidential nature e.g encrypt it before emailing, do not store on removable media such as USBs prior to approval
- How to handle physical documents with information e.g. shred prior to disposal, do not leave documents with personal information on desks

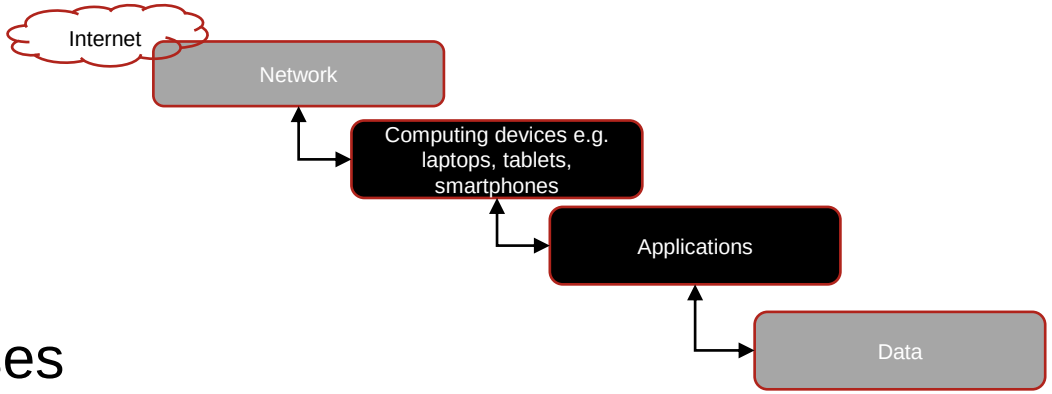
Ask the audience:
Is multi-factor authentication enabled for all your internet facing systems with sensitive data?

- Yes
- No
- Not sure
- Yes, when data is being stored in a risky country

Ask the audience:
How many different systems are used across your organisation?

- 3 or less
- 4 - 8
- 9 - 12
- More than 13
- No idea; people & teams start using new systems by themselves

User access security

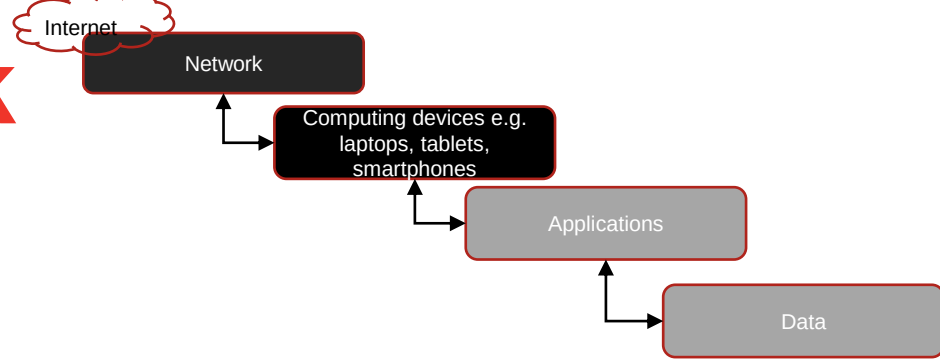


- Length and composition of passwords/passphrases
- Multi-factor authentication: the practice of using a password/passphrase and another factor to log into a user's account. Examples of additional factors include those provided via Google Authenticator or Microsoft Authenticator
- Do not reuse passwords across user accounts
- Change your password if it has been compromised
- Not to share passwords with other staff.
  If this cannot be avoided ensure the password is shared only with those who need it, there is an understanding of who is using the account with the shared password and the password is changed if someone who knows it leaves the organisation.

Ask the audience:
Do you provide staff with guidance on whether users can work using their own devices?

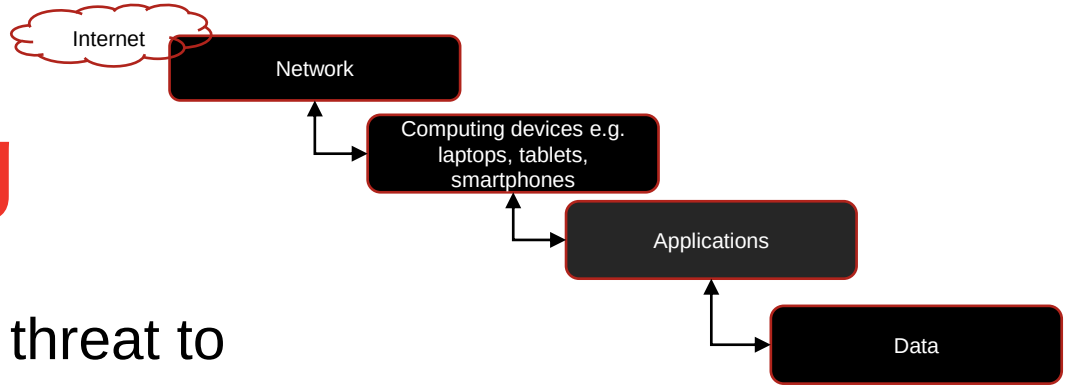
- No - we value flexibility & trust
- Yes – they can use their own devices
- Yes – they must use our PC, & can use their own mobile phone
- Yes – they must use our PC & mobile phone
- Don’t know

Computing device and network protection requirements



- Physically protect your device
- Lock your screen when device is left unattended (Ctrl + Alt + Del; Win + L)
- Do not install or use unauthorised software
- Keep devices up-to-date
- Expectations on the use of Bring-Your-Own-Device (BYOD) to access and store organisational data e.g.
  - must be PIN/passcode/fingerprint protected
  - must never store personal information about clients
  - keep devices and installed apps updated
  - install antivirus software
  - have remote wipe capability to be used if lost or stolen
- Network security: firewall configurations, secure network protocols, anti-malware software, VPNs for remote access, wireless network configuration, email filtering

Security incident reporting

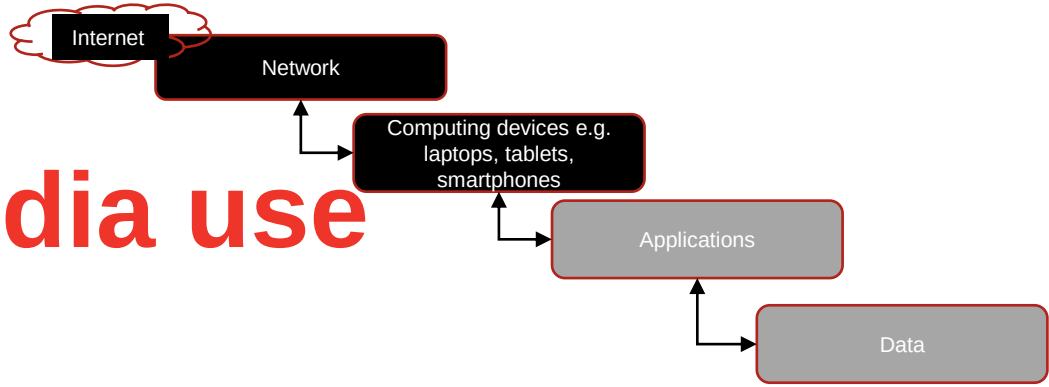


Security incidents are adverse events which pose a threat to an organisation's information systems and services

Important to have a contact point for staff to report potential security incidents (e.g. IT Support) such as:

- Any unfamiliar activity on their devices
- Disclosure of information to unauthorised person
- Lost devices, removable media with organisation's information
- Unescorted person on office premises
- Lost or stolen physical access cards

Email, Internet and Social Media use



» Important advice for staff includes:

- Beware of phishing emails
- Use organisational email and the Internet responsibly
- Act responsibly when using social media sites such as Facebook, Twitter, LinkedIn
- Organisational information must not be sent via unauthorised messaging platforms

We have run ***free*** monthly webinars for NFP staff that explain phishing basics & how to keep information secure – recordings are available online. We are about to launch a replacement, an online self-paced short training session

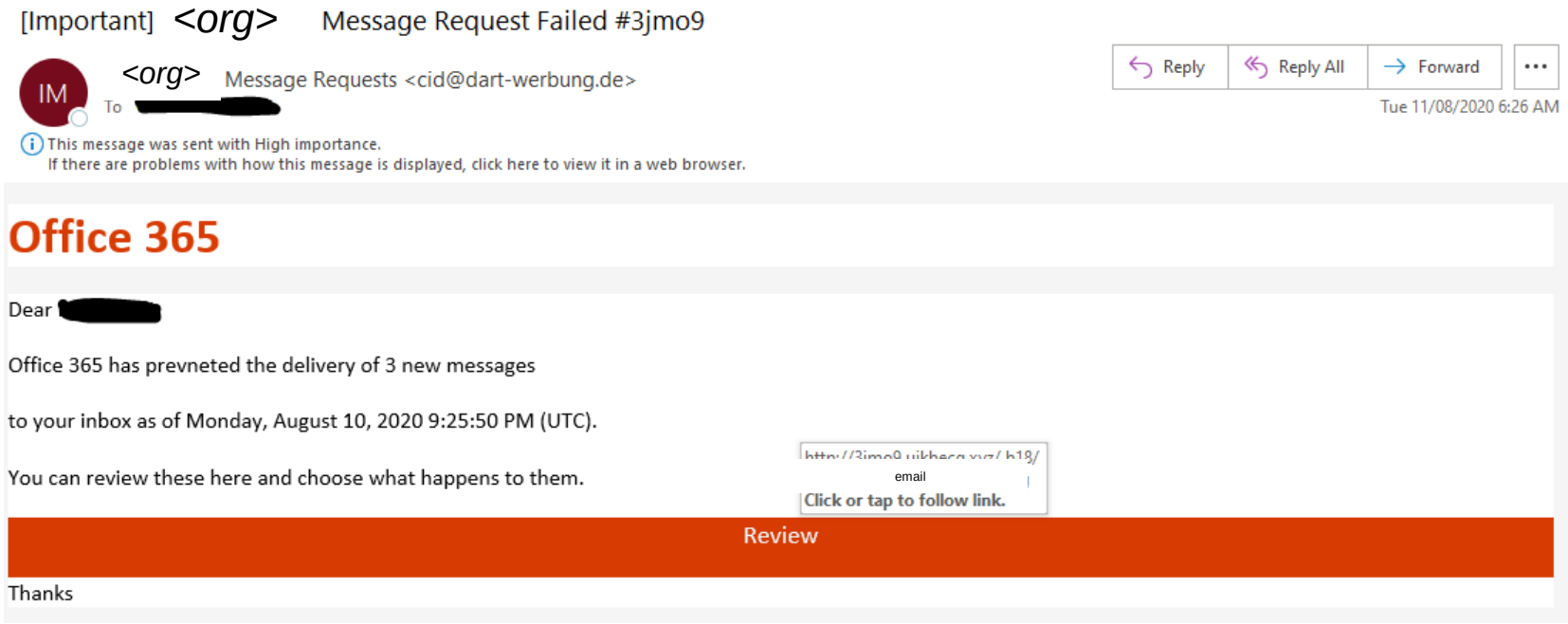
(with a certificate at the end for those who pay attention!)

Top security incident entry points

- **Phishing**: email sent to users with the purpose of tricking users into revealing personal information or clicking on web links. Could also be via voice calls, instant messaging apps, SMS
- **Ransomware**: malicious software installed on machines causing data to be locked up and inaccessible. Could be installed by clicking on links in phishing emails, gaining access to a user account or exploiting a security vulnerability
- **Business email compromise**: email interception or email accounts compromised to divert funds to illegitimate accounts
- **Use of stolen credentials**: usernames and passwords stolen from online services and then used to gain access to user accounts
- **Supply chain attacks**: compromise of supplier systems impacting customer organisations
- **Misconfiguration**: e.g. user access not revoked when required
- **Misdelivery**: information of a sensitive nature (e.g. personal information, organisation's confidential information) sent to unintended recipients

Source: Verizon 2021 Data Breach Investigations Report, May 2022; ACSC Cyber Threat Report (July '20- June '21), Sept 2021

Real life stories - phishing


[Important] <org> Message Request Failed #3jmo9

IM <org> Message Requests <cid@dart-werbung.de>

To [redacted]

Reply | Reply All | Forward | ...

Tue 11/08/2020 6:26 AM

This message was sent with High importance.
If there are problems with how this message is displayed, click here to view it in a web browser.

Office 365

Dear [redacted]

Office 365 has prevneted the delivery of 3 new messages

to your inbox as of Monday, August 10, 2020 9:25:50 PM (UTC).

You can review these here and choose what happens to them.

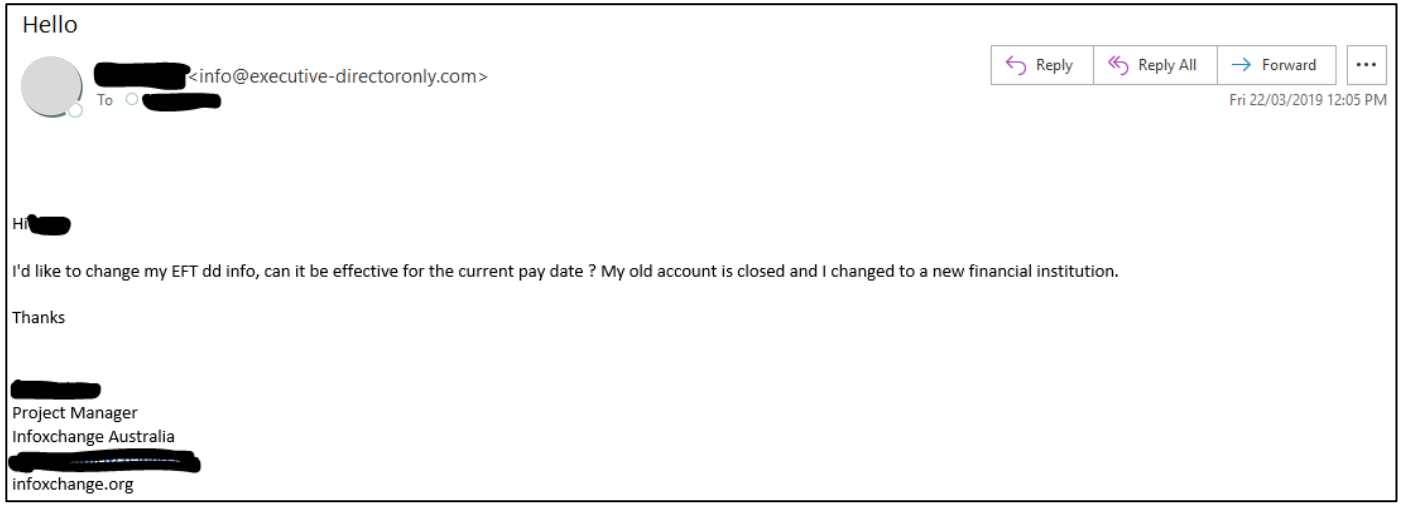
email
Click or tap to follow link.

Review

Thanks

- Staff member received this email about messages that could not be delivered
- Clicked on the ‘Review’ button. Was presented with a what looked like a standard MS SharePoint login page with their username already filled.
- They entered their password and clicked login
- Fortunately, Multi-factor authentication was employed and account access was blocked
- The staff member was still asked to change their password

Real life stories - phishing



Hello

[redacted] <info@executive-directoronly.com>

To [redacted]

Reply | Reply All | Forward | ...

Fri 22/03/2019 12:05 PM

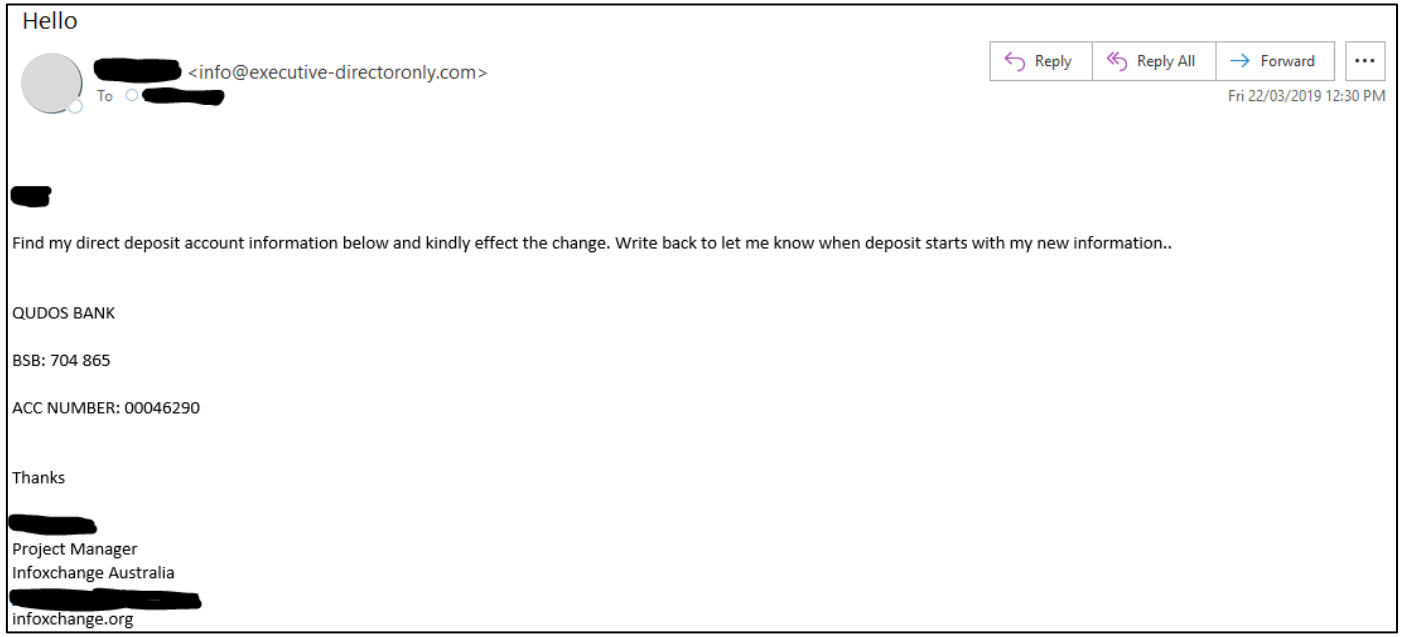
Hi [redacted]

I'd like to change my EFT dd info, can it be effective for the current pay date ? My old account is closed and I changed to a new financial institution.

Thanks

[redacted]

Project Manager
Infoxchange Australia
[redacted]
infoxchange.org



Hello

[redacted] <info@executive-directoronly.com>

To [redacted]

Reply | Reply All | Forward | ...

Fri 22/03/2019 12:30 PM

[redacted]

Find my direct deposit account information below and kindly effect the change. Write back to let me know when deposit starts with my new information..

QUDOS BANK

BSB: 704 865

ACC NUMBER: 00046290

Thanks

[redacted]

Project Manager
Infoxchange Australia
[redacted]
infoxchange.org

- Email request to change bank account details received by payroll department, signed off from a staff member
- Payroll department responded requesting new bank details and not noticing the 'from' email address
- The second email was received by payroll at which point, due to the grammar in the email they realised this was not legitimate

7 TIPS TO CATCH A PHISH

A phishing message will generally feature some of these attributes:

1 Strange "From:" address

2 "Reply to" address different to the "From:" address.

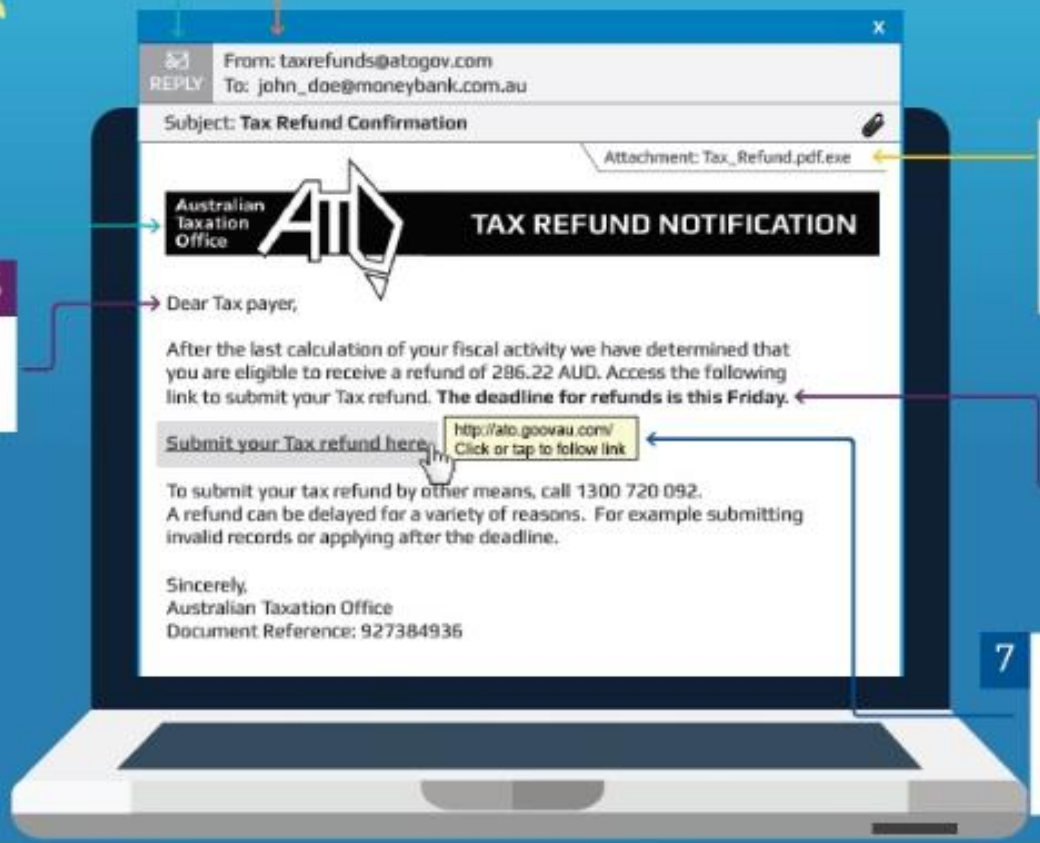
3 Poor spelling, grammar or design

4 Attachments you didn't ask for. Don't open them.

5 Generic greetings

6 Urgent calls to action

7 Strange links - position your cursor to 'hover' over a link without clicking. Does the address look right??



Ask the audience:
Have you been affected by data theft or IT system compromise?

» Yes

» No

Some organisational processes requiring a security lens

» Finance:

- Ensure delegations of authority are appropriate and reviewed regularly
- Ensure that for large amounts of spend, double signatures are required
- Verify change of bank account details via alternate channels e.g. request made via email, use phone call to verify

» HR:

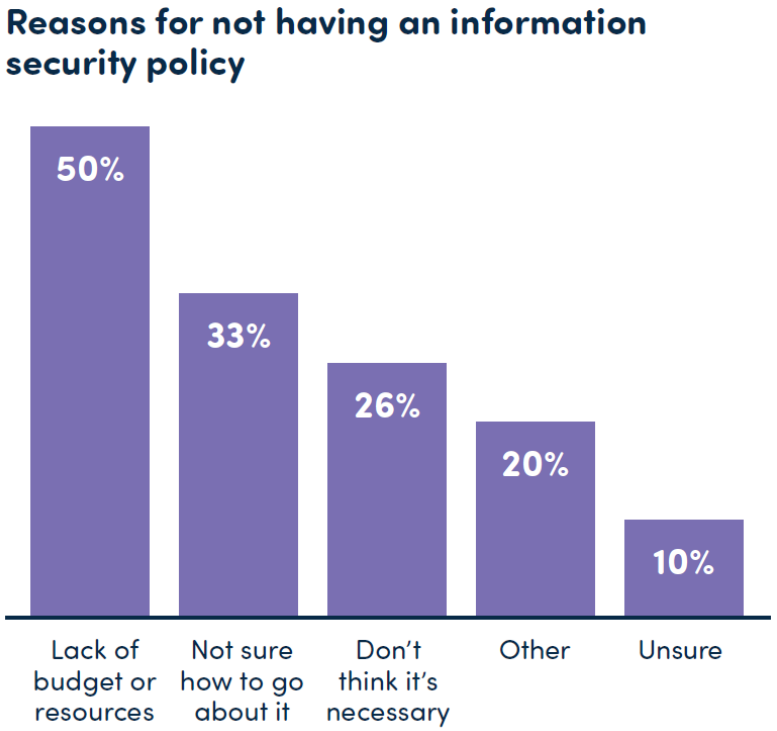
- Make sure on-boarding and off-boarding activities are conducted in a timely manner and are holistic i.e. if you use software provided by third parties, remember to off-board as required e.g. Training software packages; Financial management software packages, Car and or Resource booking etc.
- Conduct security awareness refresher training regularly
- Ensure your organisation takes a grateful approach for reports of lost or potentially stolen devices, rather than a punitive one.

Cyber Security in the sector

Only 47% of not-for-profits provide cyber security and privacy awareness training for staff

Recorded webinar on Cyber Security for NFP staff - *https://www.connectingup.org/webinars/topic/Information%20Security*

Digital Transformation Hub launching an online self-paced short course

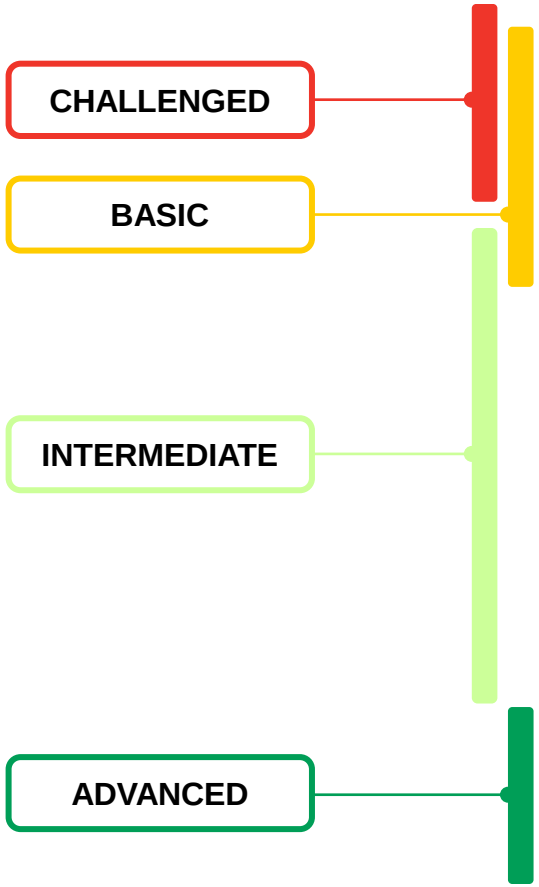


Source: Digital technology in the NFP sector report, Nov 22; 625 participants

Our NFP information security framework

Category	Challenged	Basic	Intermediate	Advanced
User access & authentication	User accounts are not well managed.	MFA is effectively configured on Microsoft 365/Google Workspace & sensitive internet-facing systems. Shared user accounts are eliminated or minimised & effectively managed (e.g. pswd vault). System access is reviewed on a scheduled basis.	Strong passwords are required. Processes exist to manage account breach risk – e.g. alerts, lockouts and/or log review. Admin rights are minimised, requires approval, time limited & protected (via MFA, VPN, SSH etc)	Access to important IT systems/applications employs Single-Sign on a secure, core authentication service.
Information classification & security	Information is not classified and the backup approach for information stores has not been thought through.	Data backup has been considered and configured as appropriate for all important information stores. A simple data recovery test is performed annually.	Information categories are defined (sensitive, confidential, public, etc) and implemented (e.g. sensitive data is encrypted). A system register records approved information categories for each system. Backups are reliable, secure and meet retention / recovery requirements. A significant restore is performed annually.	Technical controls restrict staff from storing or transmitting sensitive data incorrectly. Data retention requirements are known and addressed in line with organisational needs and compliance obligations
Device & network management	Device security and network threats are not managed.	Windows PCs have antivirus protection. Only vendor-supported operating systems & applications are used. Device OS & applications are reliably patched through manual or auto-update processes. Default Infrastructure admin passwords have been changed.	User devices have appropriate, centrally monitored firewall & antivirus software. Sensitive information is securely encrypted & can be remote-wiped. Patch management is undertaken centrally. Critical patches are deployed rapidly. Perimeter firewall and wifi configuration minimises security risk.	A process to identify, prioritise & manage technical vulnerabilities exists. A vulnerability scanner is used effectively. Devices that don't comply with policies (encryption, patching etc) are blocked. Devices are built & maintained to best practices standards (least privilege access, secure baselines, logging etc)
Polices, risk management & compliance	Policies and compliance processes are not well established.	An end-user security policy, information security policy and privacy policy exist. Third parties with access to the organisation's information are required to keep information safe. Cyber security risks and protections are discussed at the executive level at least twice annually.	An assessment against the ACSC's Essential 8 has been performed and key risk addressed. An effective security risk management process exists. Annual security tests identify & remediate risks. A security incident response process is defined. Reasonable steps are taken to meet legal, regulatory & contractual obligations.	The organisation has been independently assessed and confirmed as compliant against an information security standard such as ISO/IEC 27001.
User Education	Staff educate themselves.	Induction & annual refresh training effectively covers staff obligations, security risks BYOD, good password practice, sensitive information & who to contact for help.	Quizzes or phishing tests check knowledge annually. Specific training & processes support high-risk staff (accounts, CEO, CFO, IT etc) – e.g. phone call required to verify bank account changes.	Training is engaging, tailored by role, available on demand & effective. A strong security culture exists – staff actively consider it their responsibility.

NFP Information security roadmap



1. Get the basic protections in place – multi-factor authentication, patching, user education, data backups, spam filtering, antivirus, firewalls and user accounts are confirmed
2. Begin the governance journey - develop and communicate an end-user security policy while engaging also the management team to manage cybersecurity risks
3. Classify organisation's information, define where it should be stored, how it must be protected and control who has access to it
4. Enhance the organisation's cybersecurity protections – improve patch and asset management, password practices, user access rights, administrative privileges and incident response processes
5. The organisation's legal, regulatory & contractual obligations are understood, and reasonable steps are taken to comply
6. Strengthen your backup protections and document these
7. Assess the organisation against the Australian Cyber Security Centre's Essential 8 and mitigate important risks
8. Implement a risk-based approach to managing cybersecurity, validated by planned penetration tests, phishing tests, vulnerability scans
9. Continue the cybersecurity journey through a continuous improvement program, and certification to external security standards.

Key takeaways to stay secure

1. **Multi-factor authentication for each of your core systems**
   - An extra layer of protection for core systems is critical to securing access
   - Use strong passwords/passphrases that are unique for each account i.e. do not reuse these
2. **User Education**
   - Exercise caution with emails you receive that ask you to click on web links, open attachments or provide information
   - Never respond to emails requesting your personal, financial information and passwords
   - Email addresses can be 'spoofed' and appear to originate from people you know. Be on the lookout for any requests you receive via email
   - Remember fraudsters can create websites that look like the real supplier or banks to capture your information. Do not log in to a web page that you have reached through a link in an email
3. **Essential Eight**
   - Eight core technical security measures recommended by the Australian Cyber Security Centre to protect your organisation against a range of risks
4. **Make cybersecurity risk management and governance a priority**
   - Have the conversations on prioritizing cybersecurity within your organisation
   - Provide IT security policies for your organisation which should outline how to keep devices and information safe
   - Have a contact point for staff to talk to if they're not sure about an email they receive, or experience unusual activity on their device

Source: https://digitaltransformation.org.au/guides/cyber-security/cyber-security-essentials-where-begin

Useful resources

- **Hub cybersecurity resources:** https://digitaltransformation.org.au/guides/cyber-security
- **Cybersecurity webinars for NFP staff and IT Managers:** https://www.connectingup.org/webinars/topic/Information%20Security
- **End user security policy template:** https://digitaltransformation.org.au/guides/cyber-security/diy-end-user-security-policy
- **IT security policy template:** https://digitaltransformation.org.au/guides/cyber-security/information-security-policy-not-profits
- **Privacy guidelines and privacy policy template**: https://digitaltransformation.org.au/guides/cyber-security/privacy-guidelines-not-profits
- **The 5 Knows of cybersecurity**: https://www.telstra.com.au/content/dam/tcom/business-enterprise/security-services/pdf/5-knows-of-cyber-security.pdf
- **Report CyberCrime to Australian Cyber Security Centre 'ReportCyber':** https://www.cyber.gov.au/acsc/report
- **Check if your personal details have been compromised in a data breach:** https://haveibeenpwned.com/
- **Guidance on Identity Theft:** https://www.idcare.org/

Questions and discussion