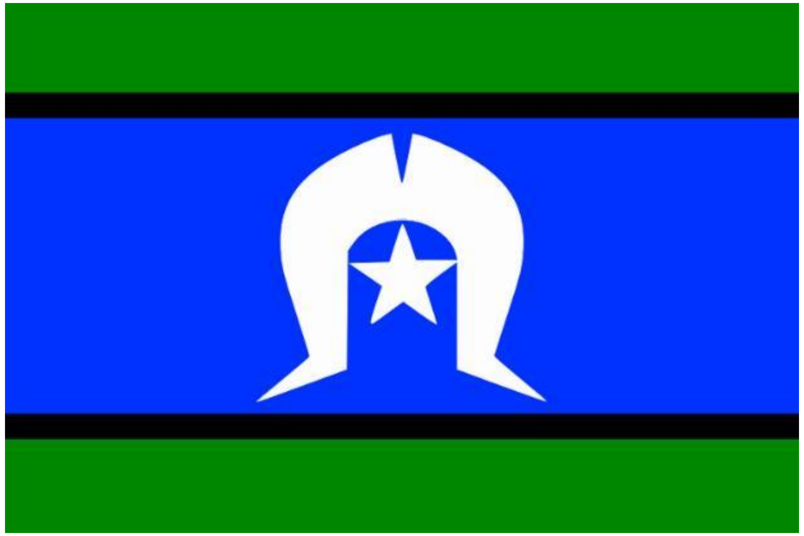
Infoxchange

CYBERSECURITY ESSENTIALS FOR IT MANAGERS

Marise Alphonso with Marcus Harvey, 1st December 2021

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

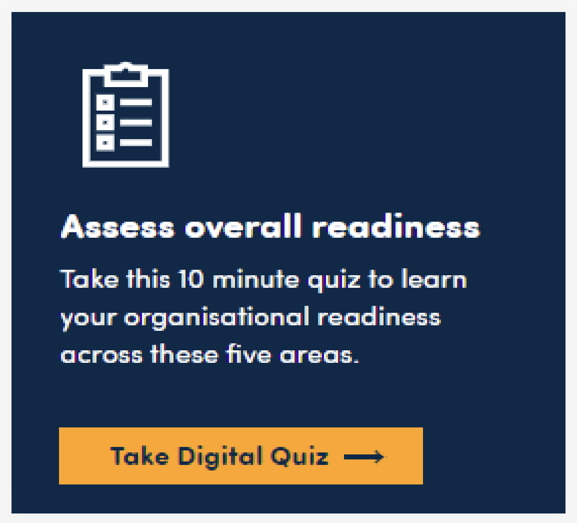


Agenda

- Digital Transformation Hub – overview
- 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
- Key takeaways
- Useful resources

Digital Transformation Hub

Technology to transform non-profit operations



Assess overall readiness

Take this 10 minute quiz to learn your organisational readiness across these five areas.

Take Digital Quiz ⟶

Digital Guides

Expert advice

Launch Housing
Benefits of good data management

Hornsby Women's Shelter
Social media campaign fundraising

Jabiru
Moving to the cloud

Redkite
User-centred digital service design

Cerebral Palsy Network
Increasing sustainability and reach

Heart for Kids
Secure collaboration

Cancer Wellness Support
Creative use of CRM on a budget

Settlement Council
Effective advocacy

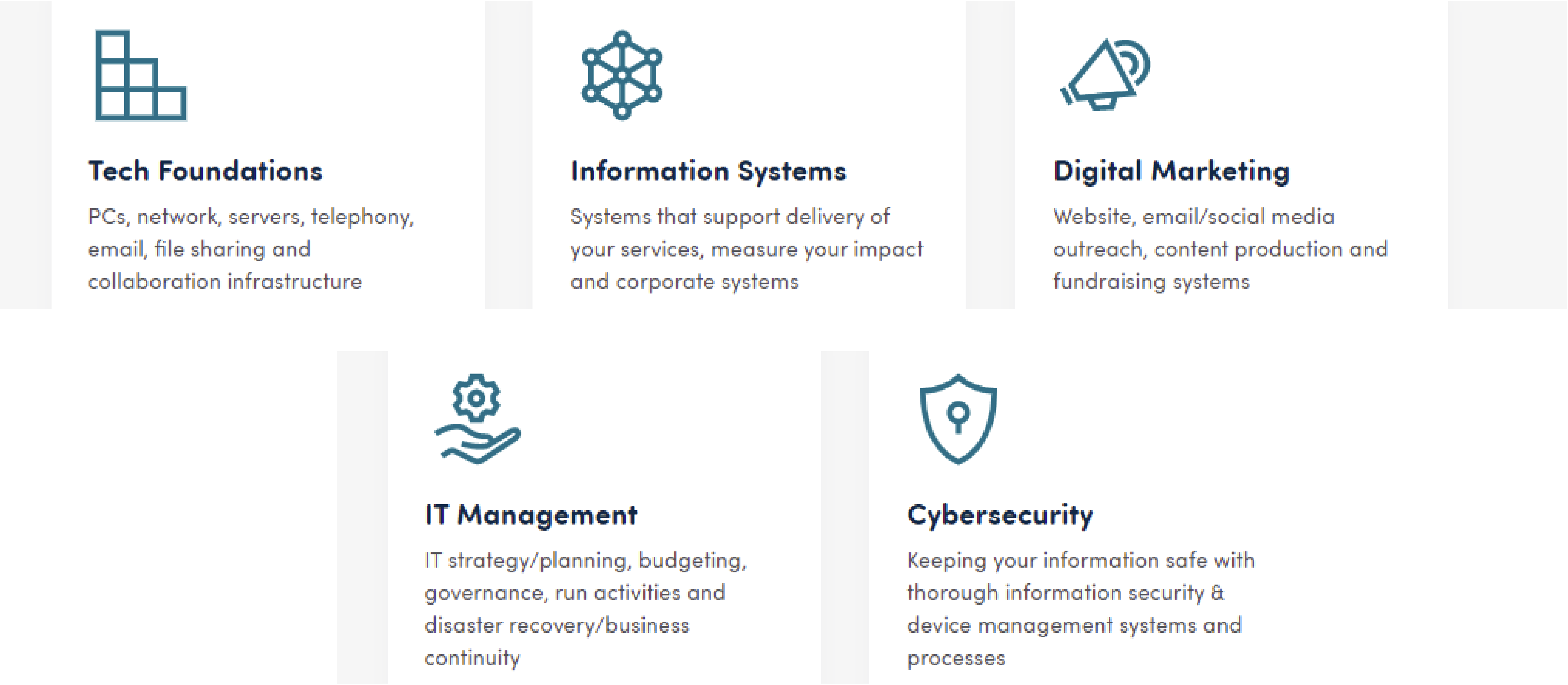
Wombat Housing Tech Foundation
Secure and flexible working

Case studies

Training resources

Technology discounts for not-for-profits

Five domains structure the technology jungle



Tech Foundations

PCs, network, servers, telephony, email, file sharing and collaboration infrastructure

Information Systems

Systems that support delivery of your services, measure your impact and corporate systems

Digital Marketing

Website, email/social media outreach, content production and fundraising systems

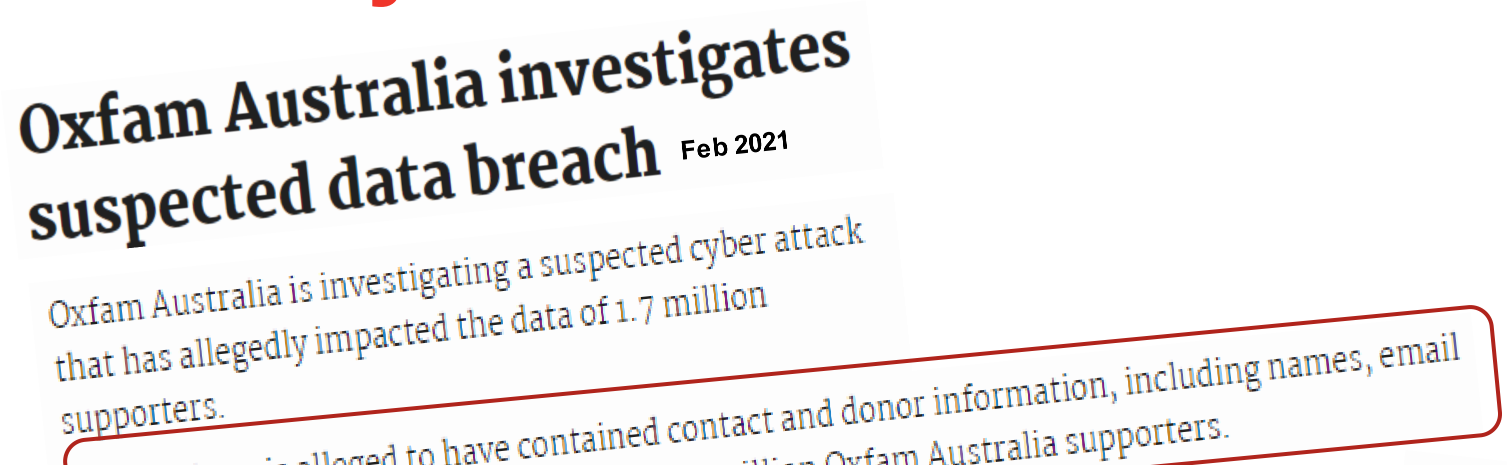
IT Management

IT strategy/planning, budgeting, governance, run activities and disaster recovery/business continuity

Cybersecurity

Keeping your information safe with thorough information security & device management systems and processes

Security in the headlines



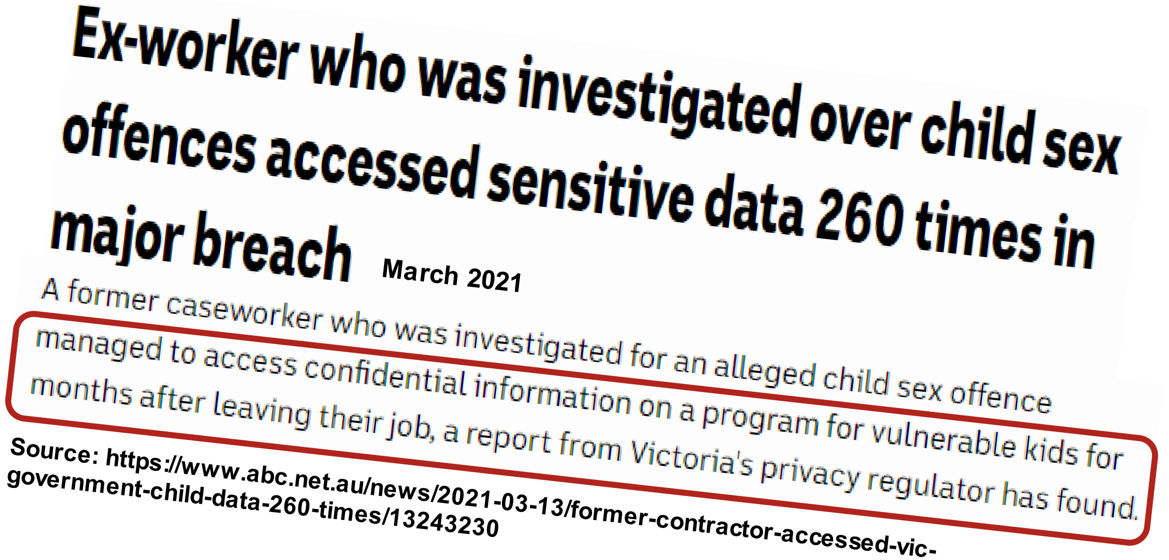
Oxfam Australia investigates suspected data breach

Feb 2021

Oxfam Australia is investigating a suspected cyber attack that has allegedly impacted the data of 1.7 million supporters.

The database is alleged to have contained contact and donor information, including names, email addresses and phone numbers, for about 1.7 million Oxfam Australia supporters.

Source: https://www.itnews.com.au/news/oxfam-australia-investigates-suspected-data-breach-560690

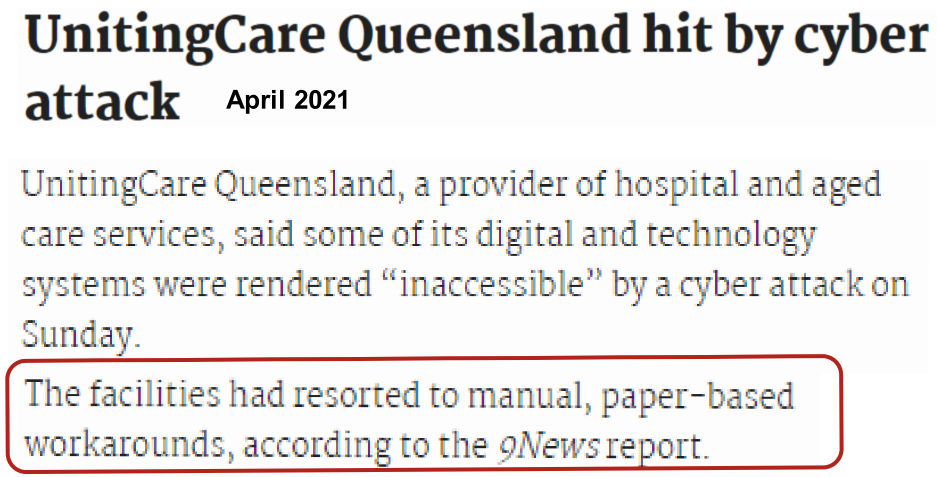


Ex-worker who was investigated over child sex offences accessed sensitive data 260 times in major breach

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



UnitingCare Queensland hit by cyber attack

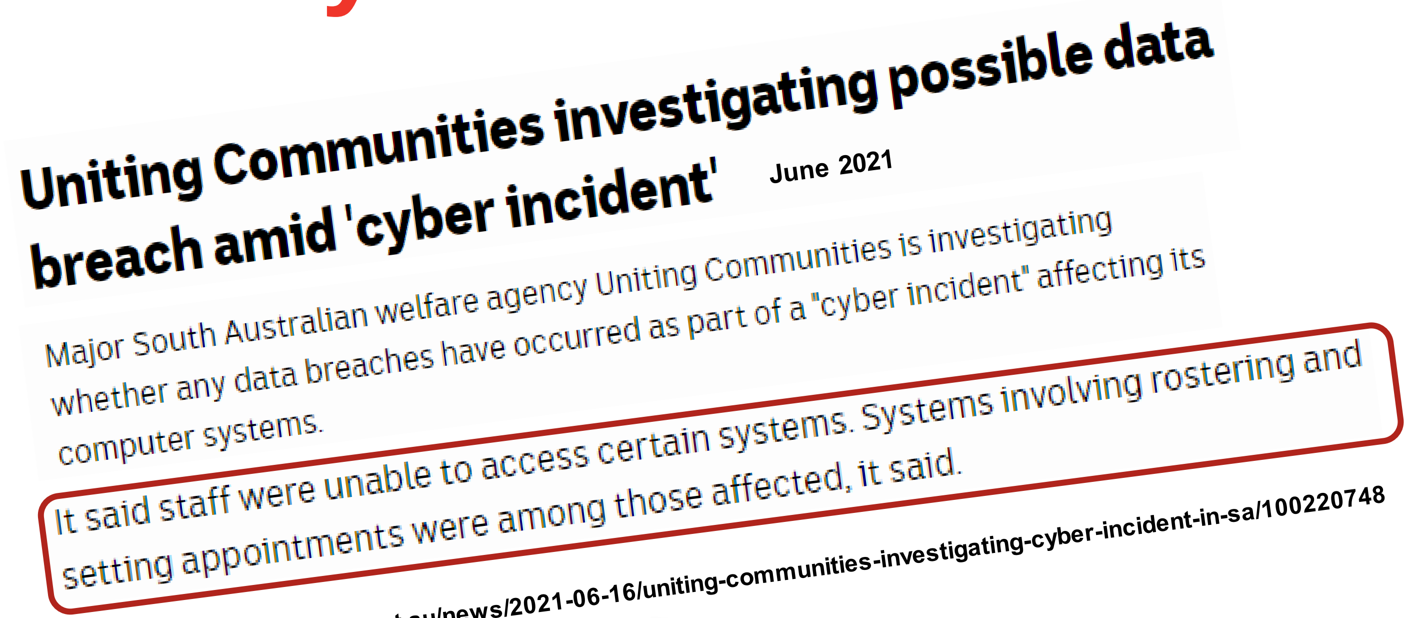
April 2021

UnitingCare Queensland, a provider of hospital and aged care services, said some of its digital and technology systems were rendered “inaccessible” by a cyber attack on Sunday.

The facilities had resorted to manual, paper-based workarounds, according to the *9News* report.

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

Security in the headlines



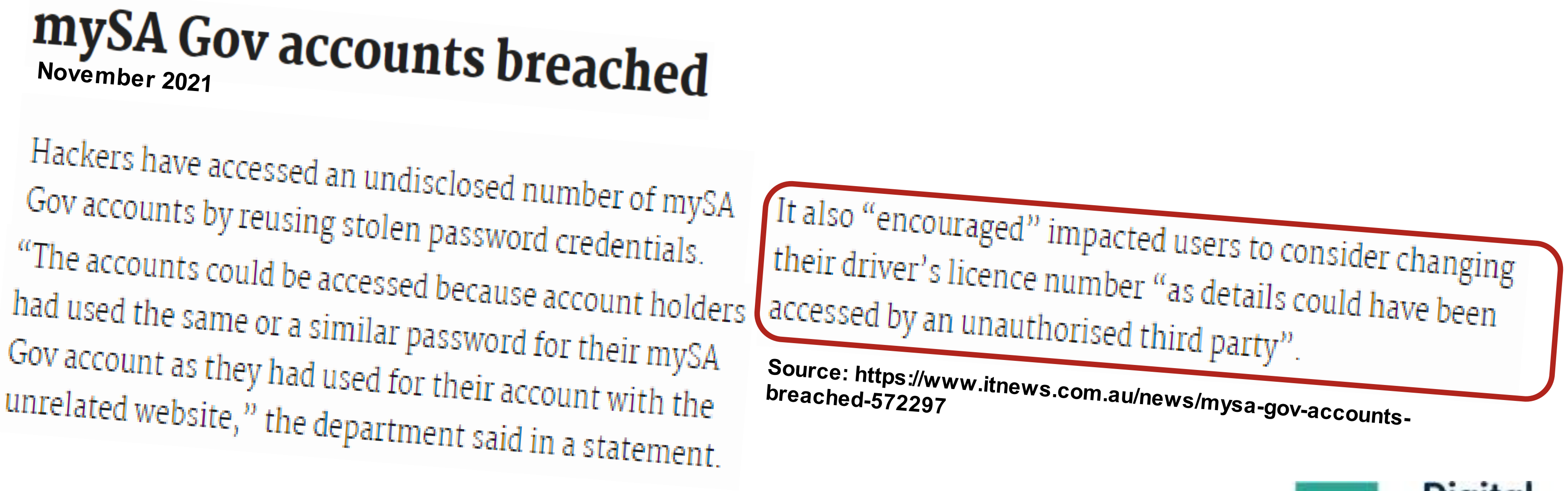
Uniting Communities investigating possible data breach amid 'cyber incident'

June 2021

Major South Australian welfare agency Uniting Communities is investigating whether any data breaches have occurred as part of a "cyber incident" affecting its computer systems.

It said staff were unable to access certain systems. Systems involving rostering and setting appointments were among those affected, it said.

Source: https://www.abc.net.au/news/2021-06-16/uniting-communities-investigating-cyber-incident-in-sa/100220748



mySA Gov accounts breached

November 2021

Hackers have accessed an undisclosed number of mySA Gov accounts by reusing stolen password credentials.

"The accounts could be accessed because account holders had used the same or a similar password for their mySA Gov account as they had used for their account with the unrelated website," the department said in a statement.

It also "encouraged" impacted users to consider changing their driver's licence number "as details could have been accessed by an unauthorised third party".

Source: https://www.itnews.com.au/news/mysa-gov-accounts-breached-572297

Some recent statistics

Australians reported **444,164 scams** and over **$850 million** in losses in **2020**, according to the latest ACCC Targeting scams report.

A quarter of all scam reports involved the loss of personal information, up from 16% in 2019.

(Source:https://www.accc.gov.au/publications/targeting-scams-report-on-scam-activity/targeting-scams-report-of-the-accc-on-scam-activity-2020)

Over the 2020–21 financial year, the ACSC received **over 67,500 cybercrime reports**, an increase of nearly 13 per cent from the previous financial year. The increase in volume of cybercrime reporting equates to **one report of a cyber attack every 8 minutes** compared to one every 10 minutes last financial year.

(Source: https://www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/acsc-annual-cyber-threat-report-2020-21)

The OAIC received **446 notifications** under the Notifiable Data Breaches scheme in the reporting period **January – June 2021**. 289 of these were due to malicious or criminal attacks which remain the leading source of data breaches

(Source:https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-report-january-june-2021)

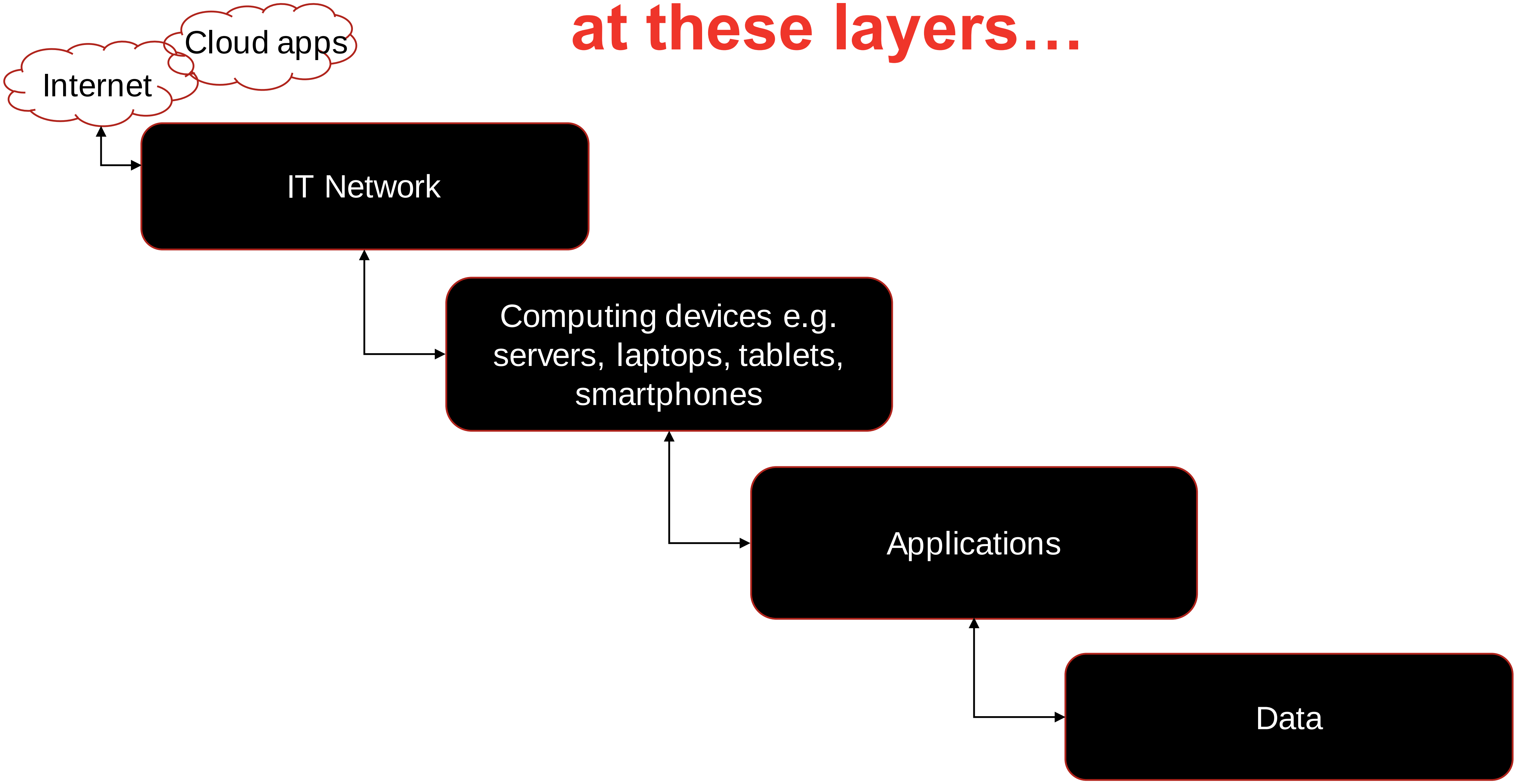
Key message

The **human element** plays a significant role in the successful delivery of security in today's organisations.

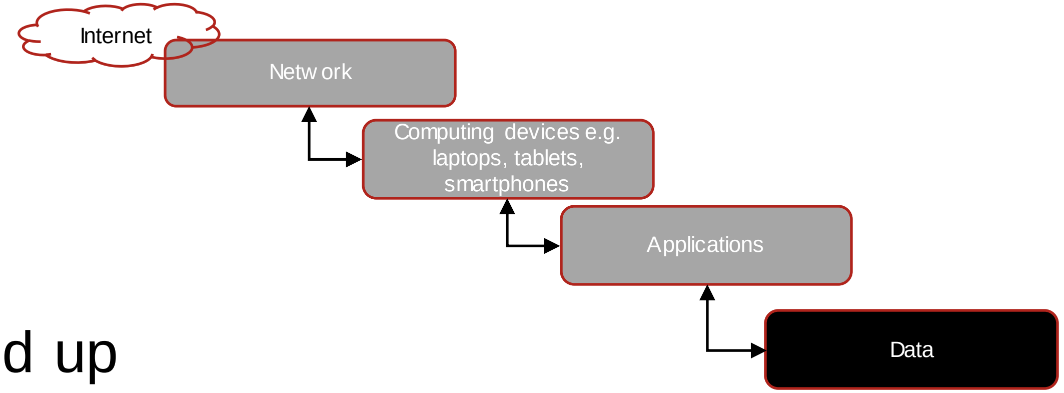
Security behaviour is greatly influenced by you and your perception of risk. These perceptions can be changed.

(Adapted from: Awareness is only the first step, https://www.riscs.org.uk/wp-content/uploads/2015/12/Awareness-is-Only-the-First-Step.pdf)

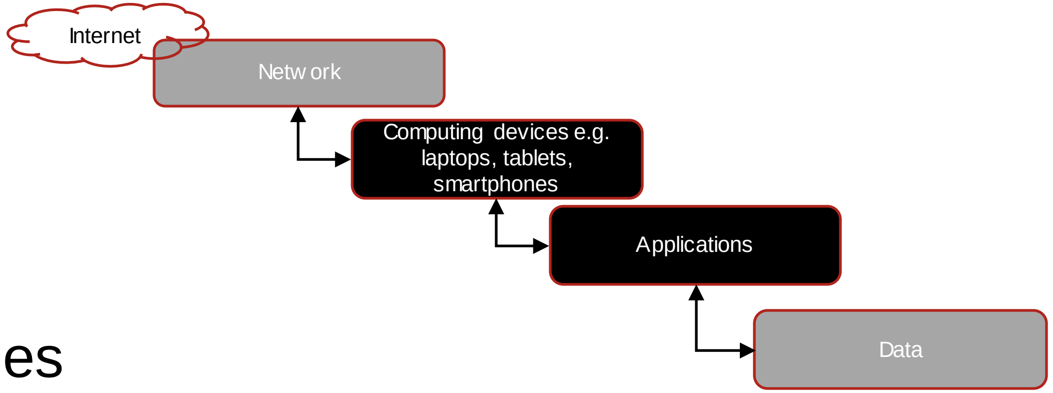
Your organisation should have protection at these layers…


Cloud apps
Internet
IT Network
Computing devices e.g. servers, laptops, tablets, smartphones
Applications
Data

Data protection



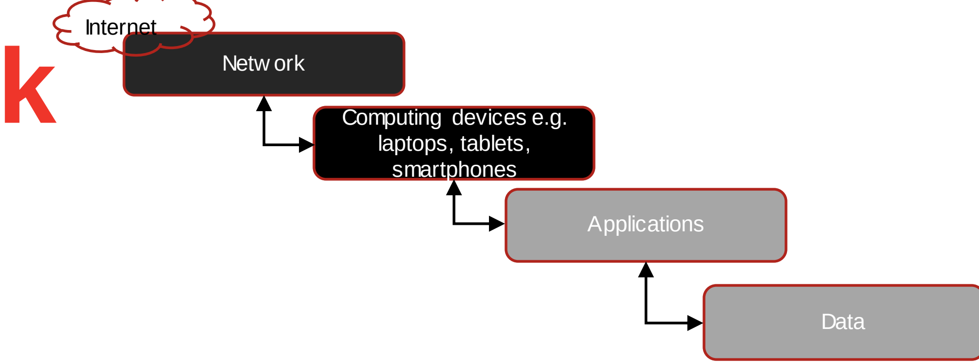
- Where to store organisational data so it is backed up
- Handling information of a confidential nature e.g encrypt it before emailing, do not store on removable media such as USBs prior to approval
- How to handle physical documents with information e.g. shred prior to disposal, do not leave documents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



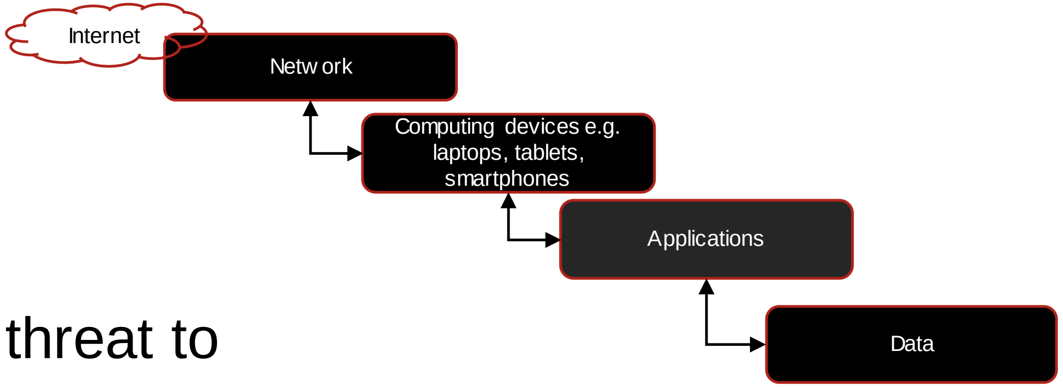
User access security

- » 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.

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

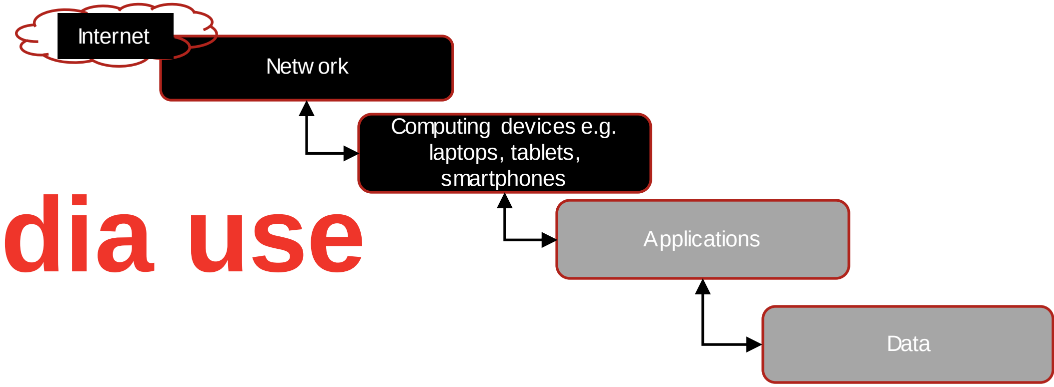


Security incident reporting

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:

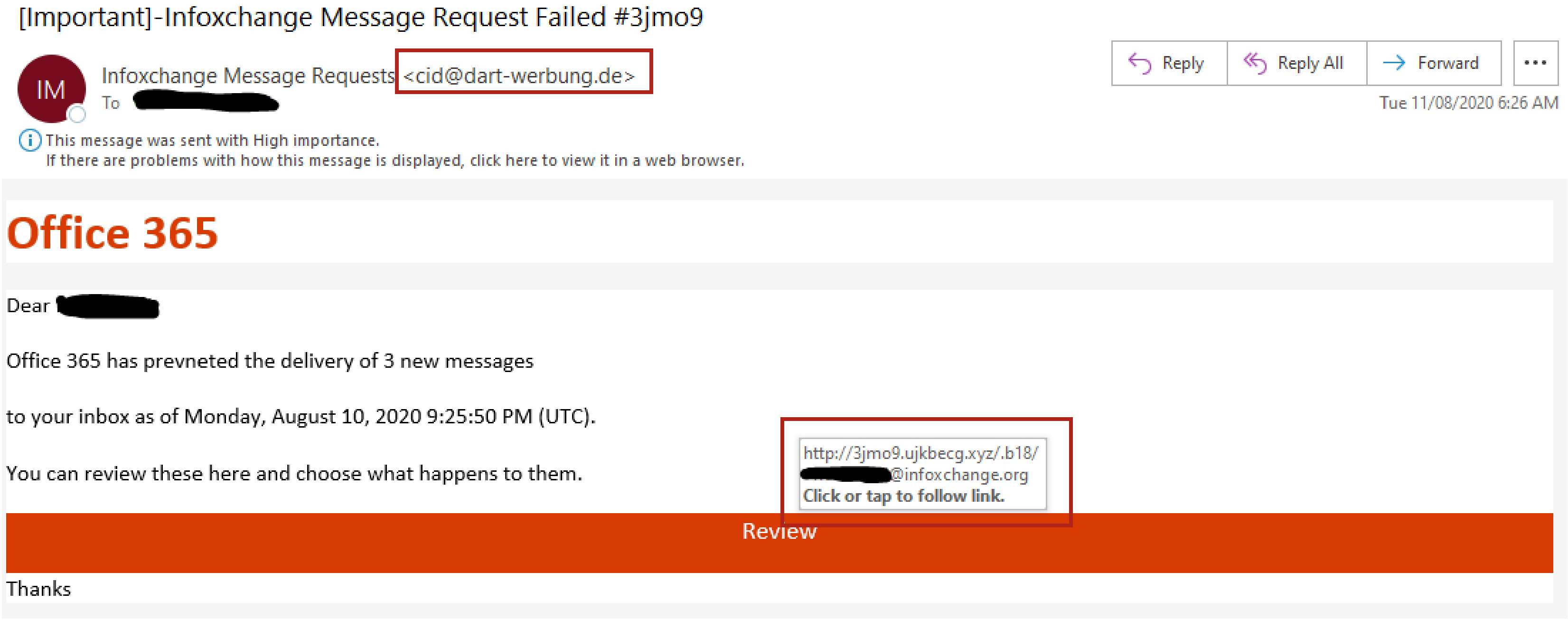
- Beware of phishing emails
- Use organisational email and the Internet responsibly
- Act responsibly when using social media sites such as Facebook, Twitter, LinkedIn
- Organisational information must not be sent via unauthorised messaging platforms

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 or by gaining access to an account
- » **Use of stolen credentials**: usernames and passwords stolen from online services and then used to gain access to user accounts
- » **Misconfiguration**: e.g. user access not removed when it must be
- » **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 2021

Real life stories - phishing



[Important]-Infoxchange Message Request Failed #3jmo9

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

To [redacted]

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.

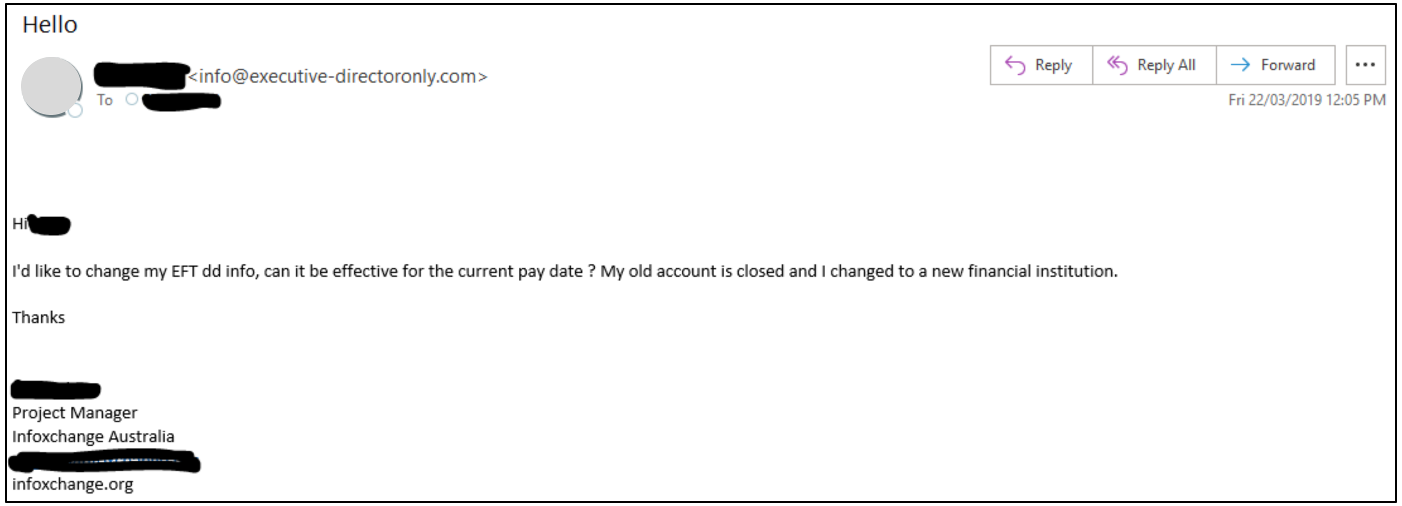
http://3jmo9.ujkbecg.xyz/.b18/
[redacted]@infoxchange.org
Click or tap to follow link.

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 is 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]

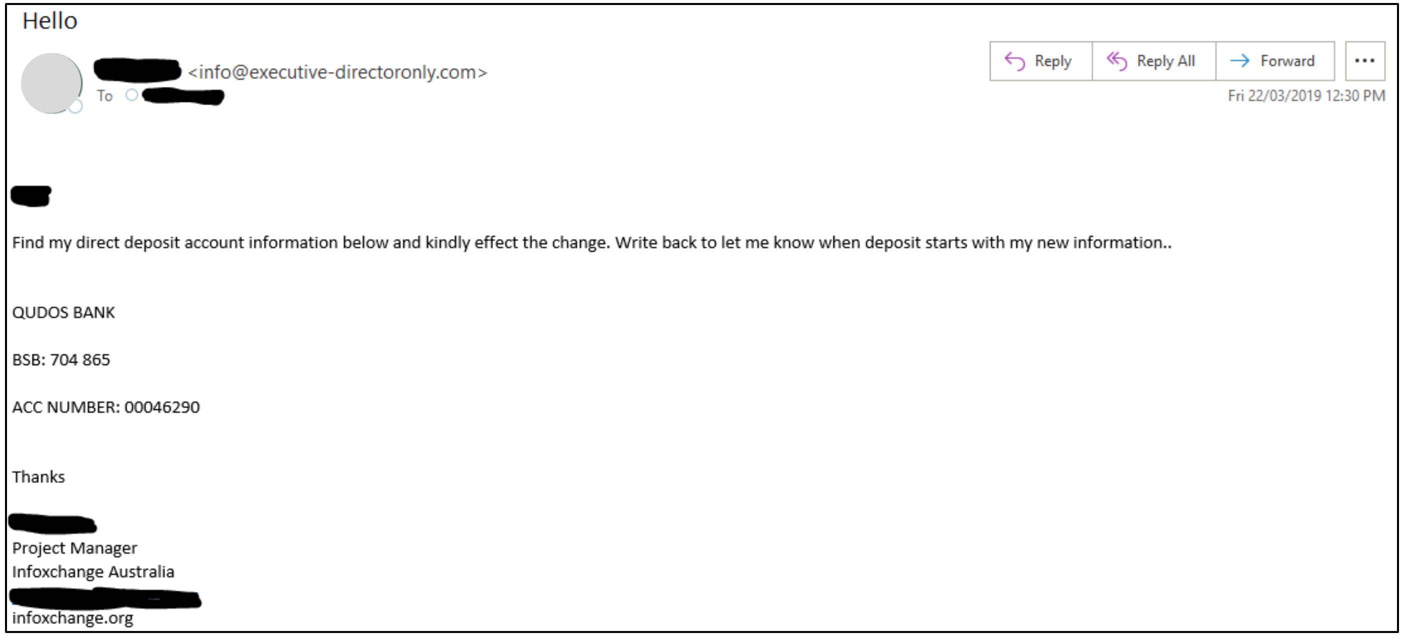
Fri 22/03/2019 12:05 PM

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]

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

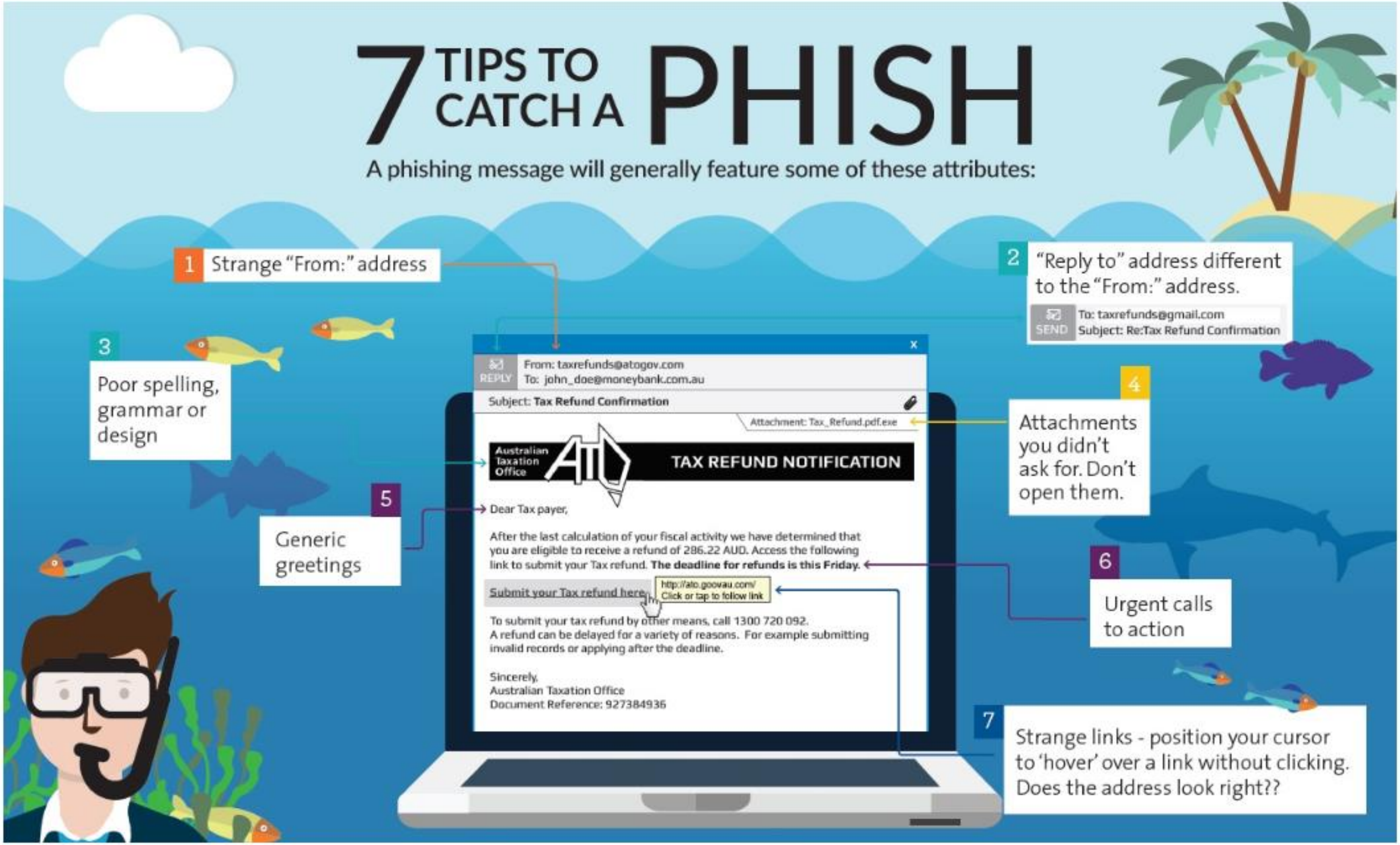
BSB: 704 865

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.

To: taxrefunds@gmail.com
Subject: Re:Tax Refund Confirmation

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??

From: taxrefunds@atogov.com
To: john_doe@moneybank.com.au

Subject: **Tax Refund Confirmation**

Attachment: Tax_Refund.pdf.exe

TAX REFUND NOTIFICATION

Dear Tax payer,

After the last calculation of your fiscal activity we have determined that you are eligible to receive a refund of 286.22 AUD. Access the following link to submit your Tax refund. **The deadline for refunds is this Friday.**

Submit your Tax refund here

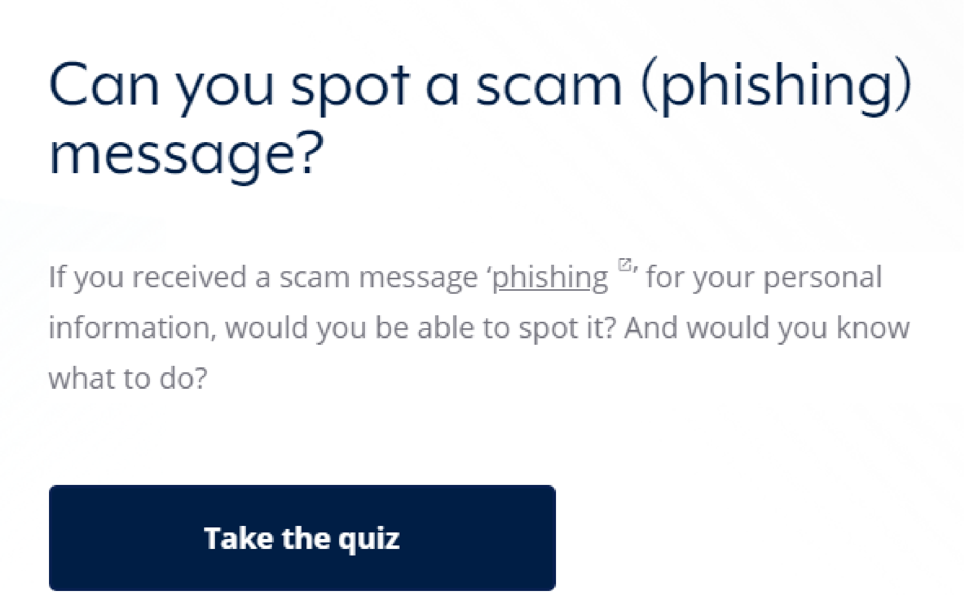
http://ato.goovau.com/
Click or tap to follow link

To submit your tax refund by other means, call 1300 720 092.
A refund can be delayed for a variety of reasons. For example submitting invalid records or applying after the deadline.

Sincerely,
Australian Taxation Office
Document Reference: 927384936

Poll question: Have you been affected by data theft or IT system compromise?

Can you spot a ‘phish’?



Can you spot a scam (phishing) message?

If you received a scam message ‘phishing’ for your personal information, would you be able to spot it? And would you know what to do?

» https://www.cyber.gov.au/acsc/view-all-content/programs/stay-smart-online/scam-messages

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.

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

Useful resources

- **Hub cybersecurity resources:** https://digitaltransformation.org.au/guides/cyber-security
- **Cybersecurity: what it is & why it matters:** https://digitaltransformation.org.au/guides/cyber-security/cyber-security-what-it-why-it-matters
- **Template end user security policy:** https://digitaltransformation.org.au/guides/cyber-security/diy-end-user-security-policy
- **IT security policy:** will be available on the hub soon
- **Cybersecurity 101 – Do you know how to keep your organisation secure:** https://digitaltransformation.org.au/guides/cyber-security/cyber-security-training, Wednesday, 16th Feb 1 - 1.30pm
- **Privacy guidelines**: 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
- **Australian Cyber Security Centre national cyber security hotline – 1300CYBER1:** https://www.cyber.gov.au/acsc/view-all-content/news/acsc-call-247
- **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/
- **SANS Security Awareness Tip of the Day:** https://www.sans.org/tip-of-the-day

Questions and Discussion