

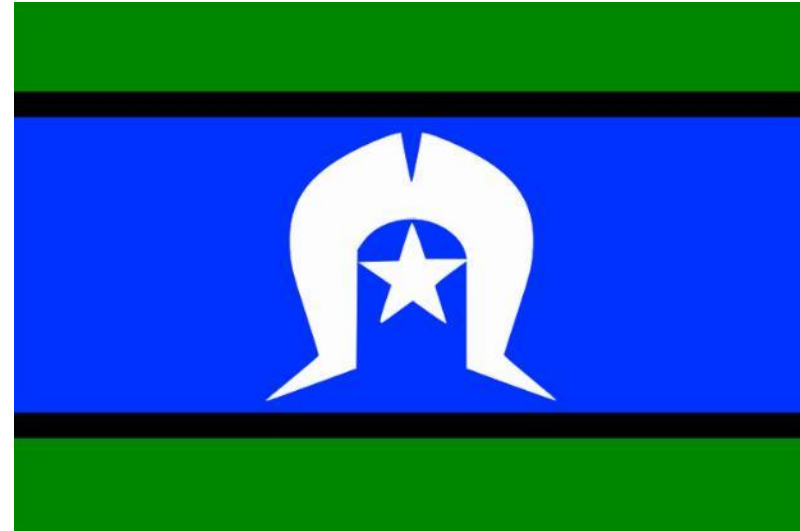


CYBERSECURITY ESSENTIALS

TO KEEP DATA SAFE

September 2021

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



Agenda

- 360 view of current cybersecurity threats facing organisations
- The top 5 things all non-profit staff must know to keep their organisation's data safe
- High-level overview of imperative cybersecurity measures every organisation needs to have in place
- Resources to get the basics in place
- Live Q&A for issues specific to your organisation's IT environment

Security in the headlines

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>

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>

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>

Are Australians at a 'turning point' on cybersecurity or still unprepared? Jan 2021

Australians are on high alert about the threat of cyber attacks following Prime Minister Scott Morrison's warning in June that Australia was targeted by a sophisticated "state-based" cyber-attack.

The Prime Minister said while such intrusions on Australia's cyber network were "not new", the "frequency has been increasing".

Source: <https://www.abc.net.au/news/2021-01-11/australians-turning-point-on-cyber-security-cyberattacks-crime/13018884>

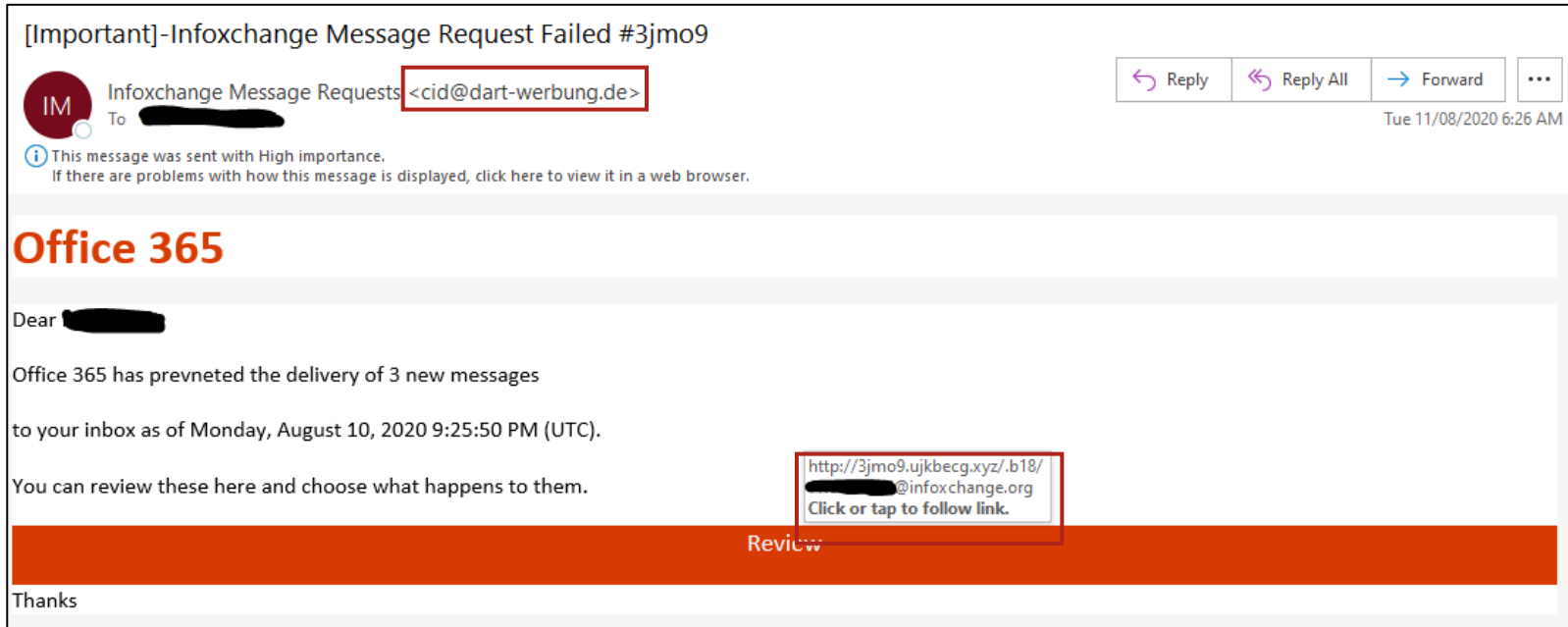
Key message

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

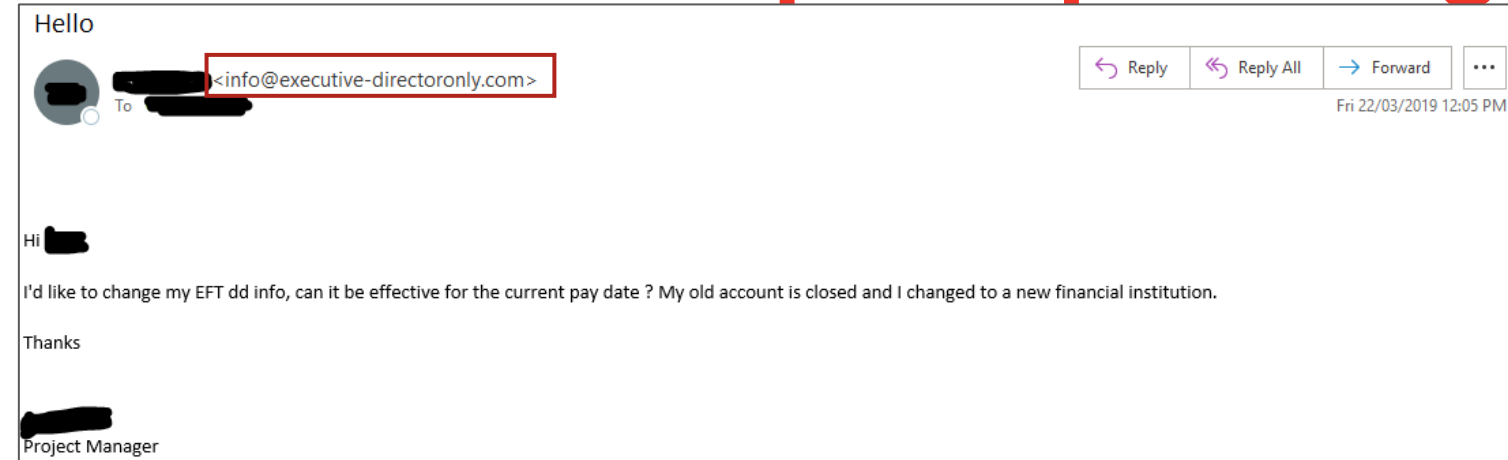
(Adapted from: Awareness is only the first step, <https://www.riscs.org.uk/wp-content/uploads/2015/12/Awareness-is-Only-the-First-Step.pdf>)

1. Know how to spot a phishing email

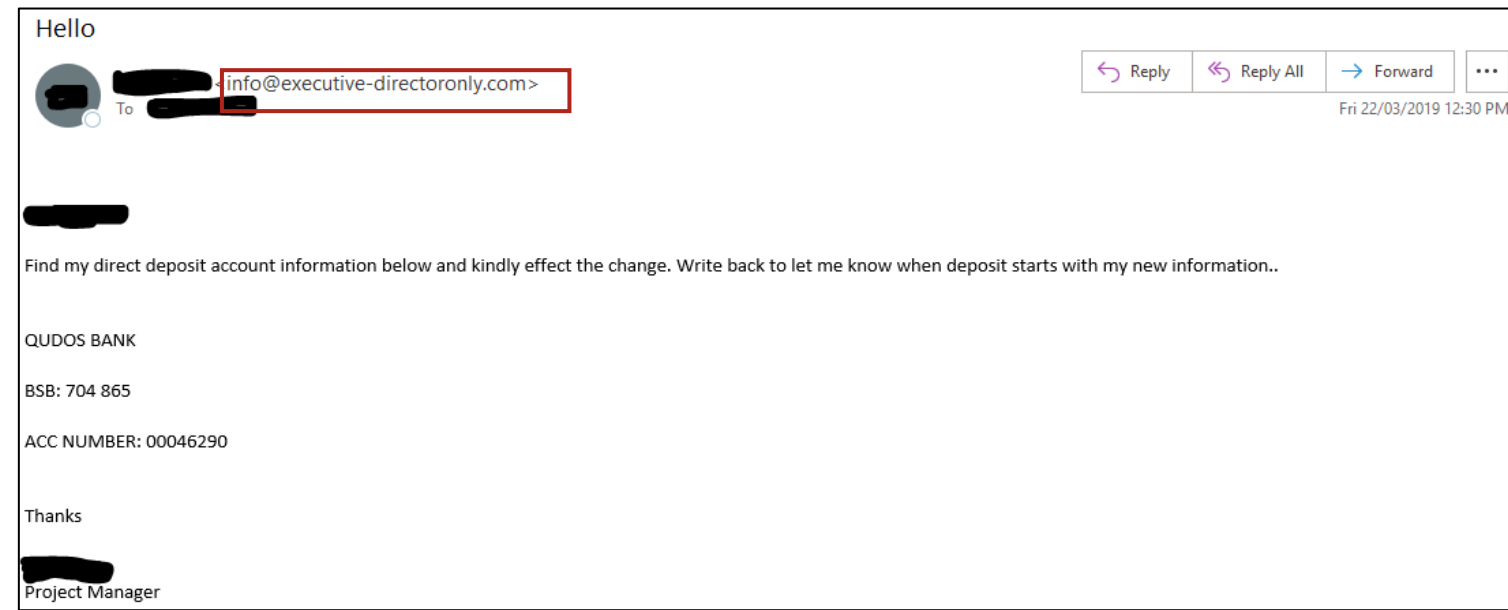


- » Staff member received this email
- » Clicked on the 'Review' button. Was presented with a what looked like a standard SharePoint login page with their username already filled.
- » They entered their password
- » Fortunately, Multi-factor authentication is employed and account access was blocked
- » The staff member was still asked to change their password

Know how to spot a phishing email



- » Email request received by payroll department 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.

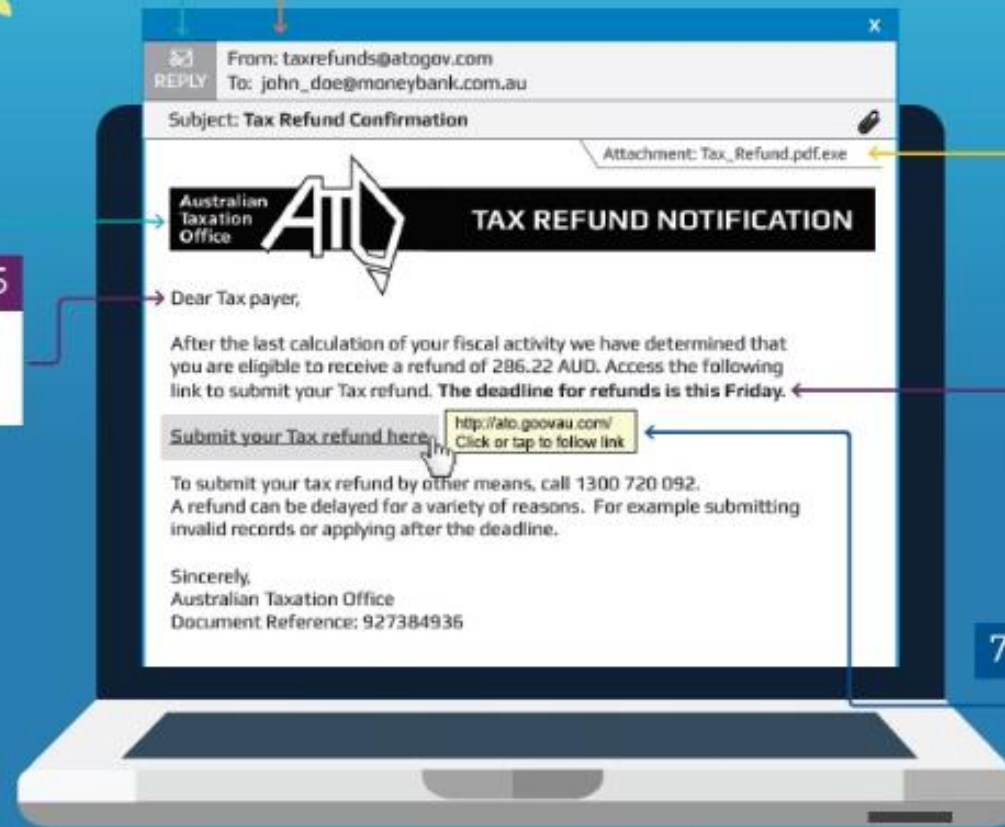
3 Poor spelling, grammar or design

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

5 Generic greetings

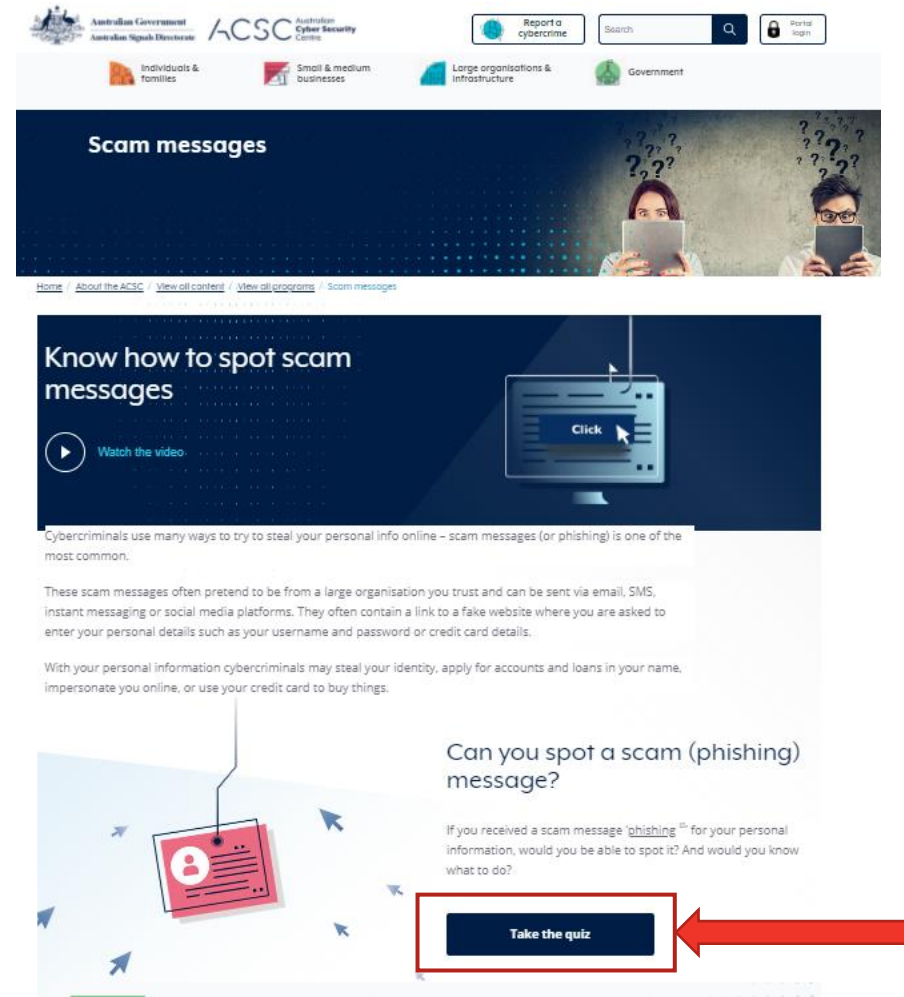
6 Urgent calls to action

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



**Has your organisation (or have you) been affected
by data theft or IT system compromise?**

Can you spot a 'phish'?



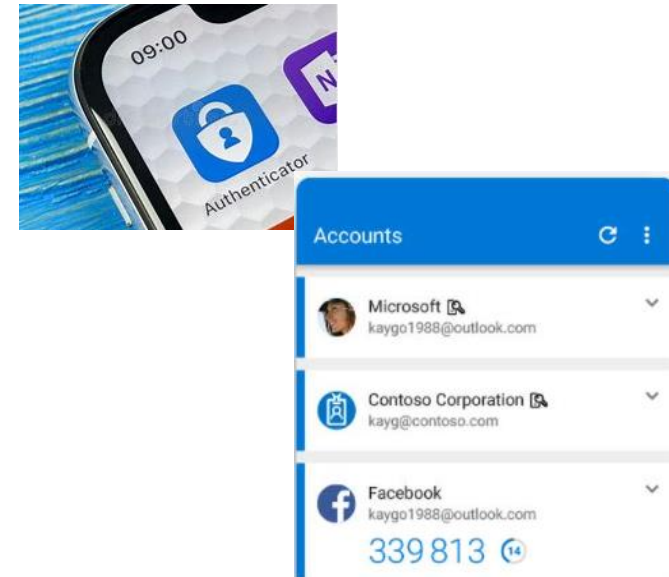
» <https://www.cyber.gov.au/acsc/view-all-content/programs/stay-smart-online/scam-messages>

2. Know where to store sensitive information

- » Sensitive data such as health data and client records should only be stored in certain places e.g. client data in a Client and Management System
- » If your organisation has not made it clear where you should store certain data so that it is appropriately protected, then you should ask

3. Use good password practices

- » Know how to pick a strong password
 - Longer, alphanumeric passwords or a phrase not containing your personal information and that only you know is best
 - Do not reuse passwords
- » Use multi-factor authentication: the practice of using a password and another factor to log into a user's account. Examples of additional factors include Google Authenticator or Microsoft Authenticator
- » Do not share accounts or passwords



4. Keep your device secure

- » Physically protect your device
- » Lock your screen when device is left unattended (Windows: Ctrl + Alt + Del; MAC: Ctrl+ Cmd + Q)
- » Do not install or use unauthorised software
- » If using your **own device** (BYOD) such as mobile phone or other device for work
 - Only store information your organisation is comfortable for you to store
 - Ensure the device has appropriate security controls e.g.
 - PIN, passcode, fingerprint to unlock
 - Security updates are installed
 - Remote wipe capability

5. Report anything you're not sure about

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

» Report anything you're worried about e.g:

- Any unfamiliar activity on your devices
- Disclosure of information to unauthorised person
- Lost devices, removable media with organisation's information
- Unescorted person on office premises acting suspiciously

» Ensure you know who to report potential security incidents to

Key takeaways for you

1. Always use strong unique passwords
2. Store sensitive data only in designated locations
3. Use multifactor authentication (MFA) on accounts for important or critical IT systems
4. Beware of phishing emails. Email addresses can be 'spoofed' and appear to originate from people you know; validate requests if they appear suspicious
5. Remember fraudsters can create websites mimicking 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
6. Know your IT and security policies provided by your organisation
7. Know who to report something suspicious to if you're worried or unsure

Useful resources

- » **Report CyberCrime to Australian Cyber Security Centre 'ReportCyber':**
<https://www.cyber.gov.au/acsc/report>
- » **ACCC Scamwatch Report a scam:** <https://www.scamwatch.gov.au/report-a-scam>
- » **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>

- » **Digital Transformation Hub cyber security Guides**
<https://digitaltransformation.org.au/guides/cyber-security>
- » **Book a consultation with NFP Digital Technology advisor**
<https://digitaltransformation.org.au/book-expert>
- » **Microsoft Office Training options**
<https://digitaltransformation.org.au/guides/tech-foundations/training-options-microsoft-office-products>

Questions and discussion

Appendix

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

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 refresher training in IT security regularly
- ensure your organisation takes a grateful approach for reports of lost or potentially stolen devices, rather than a punitive one.

Key things your organisation should have in place

1. Guidance on how to construct a strong password/passphrase
2. Multifactor authentication for important or critical IT systems
3. Security policies that outline where sensitive data should be stored
4. Guidance on how to keep organisational devices and your devices used for work safe
5. A contact point to report events that staff are worried or concerned about

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: Office of the Australian Information Commissioner, Information Matters June 2021 edition)


So far this year scammers have stolen **more than \$7.2 million** from Australians by gaining access to home computers, an increase of 184% compared to the same period last year. ACCC's Scamwatch, indicates almost 6,500 Australians have reported phone calls from scammers trying to convince them to download software that gives access to home computers and their bank accounts.

(Source: <https://www.scamwatch.gov.au/news-alerts/computer-takeover-scams-on-the-rise>, 12 July 2021)

The OAIC received **539 notifications** under the Notifiable Data Breaches scheme in the reporting period **July – December 2020**. This is a 5% increase compared to the previous 6 months and a 2% increase compared to the same period in 2019.

(Source: Office of the Australian Information Commissioner, NDB statistics July – December 2020)

The Digital Transformation Hub



Assess overall readiness

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

Take Digital Quiz →




Digital Guides



Expert advice



Case studies



Training resources



Technology discounts for not-for-profits

Digital Transformation Hub