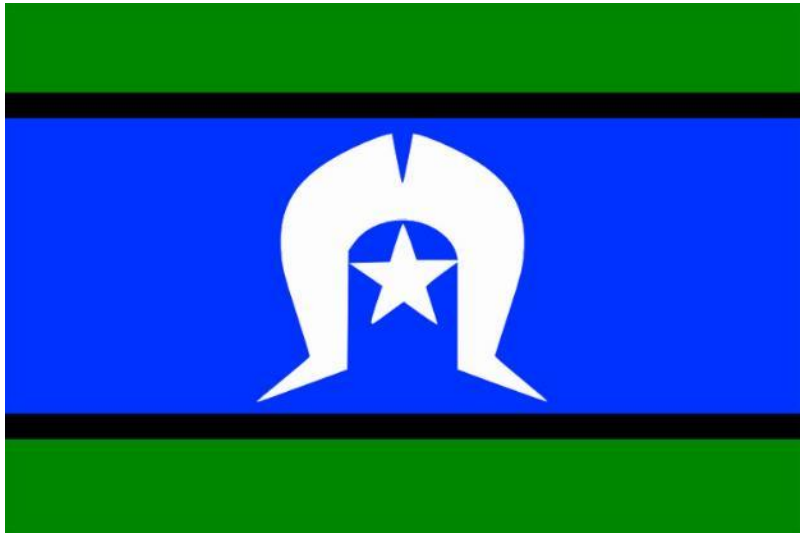
Infoxchange

CYBERSECURITY 101:

DO YOU KNOW HOW TO KEEP YOUR ORGANISATION SECURE?

November 2021

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



Agenda

- A 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

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

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

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

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)

Scams Awareness Week 2021

8 Nov 2021

- Speak up today
- How to talk about scams
- Scam stories: how speaking up helps
- Fun activities
- Take part: campaign resources
- Scamwatch tools and resources

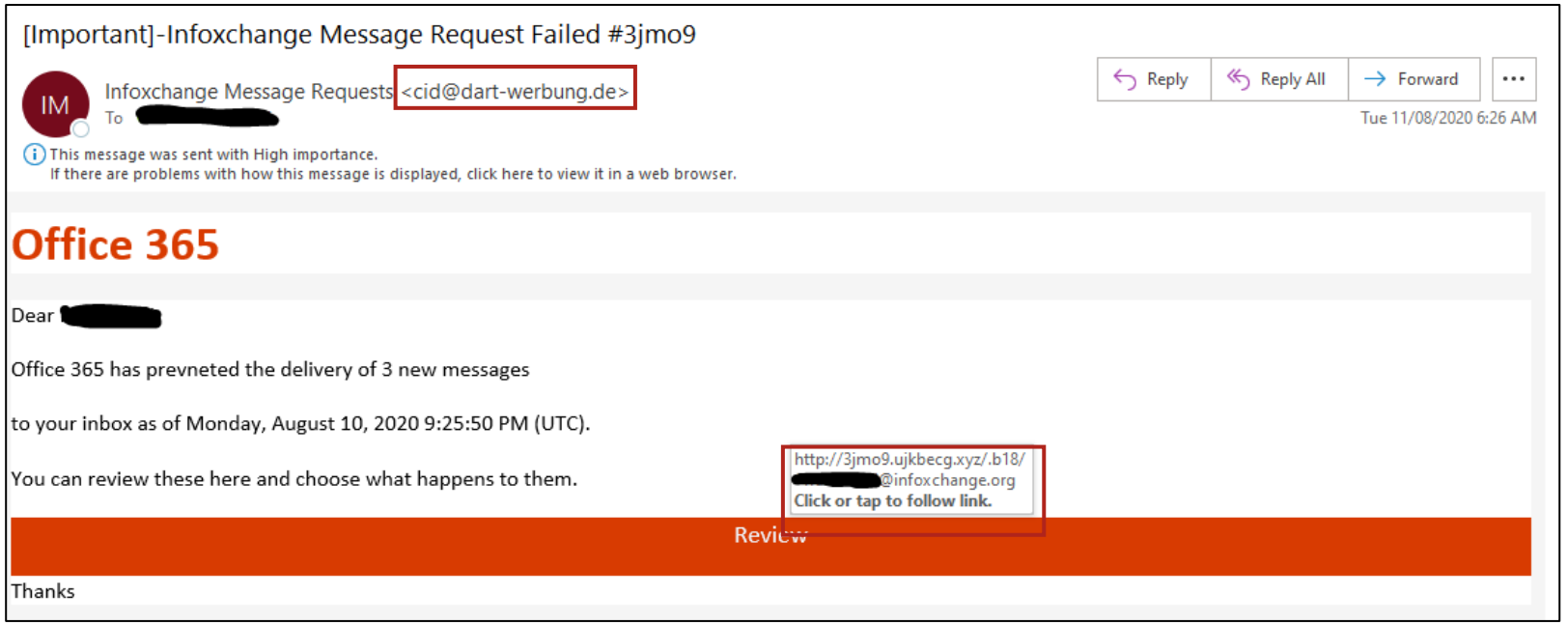
Scams Awareness Week 2021 takes place 8-12 November. This Scams Awareness Week we're encouraging everyone to start a conversation about scams to reduce stigma and help people recognise a scam sooner, or prevent scams from happening in the first place.

Scams cost Australian consumers, businesses, and the economy hundreds of millions of dollars each year and cause serious emotional harm to victims and their families.

In 2020 Australians made more than 216,000 reports to Scamwatch and reported losses of around $178 million. By the end of September this year, Australians had lost even more: Scamwatch received more than 226,000 reports with reported losses of over $222 million.

(Source: https://www.scamwatch.gov.au/news-alerts/scams-awareness-week-2021)

1. Know how to spot a phishing email


[Important]-Infoxchange Message Request Failed #3jmo9

IM Infoxchange 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.

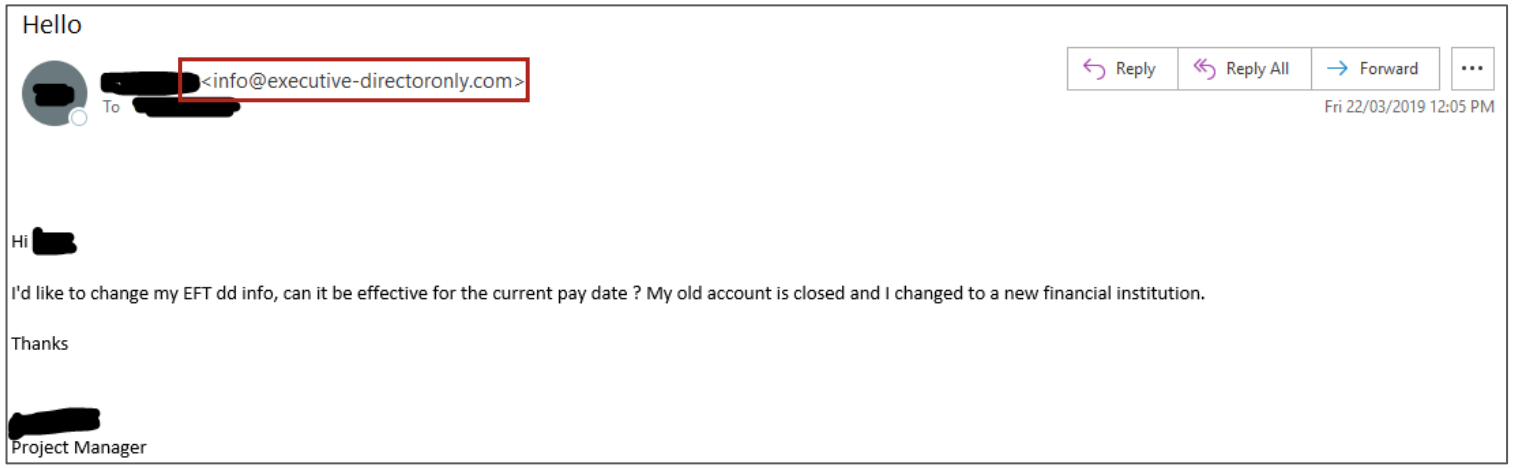
http://3jmo9.ujkbecg.xyz/.b18/[redacted]@infoxchange.org
Click or tap to follow link.

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 SharePoint login page with their username already filled
- They entered their password and clicked Log in
- 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


Hello

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

To [redacted]

Reply | Reply All | Forward | ...

Fri 22/03/2019 12:05 PM

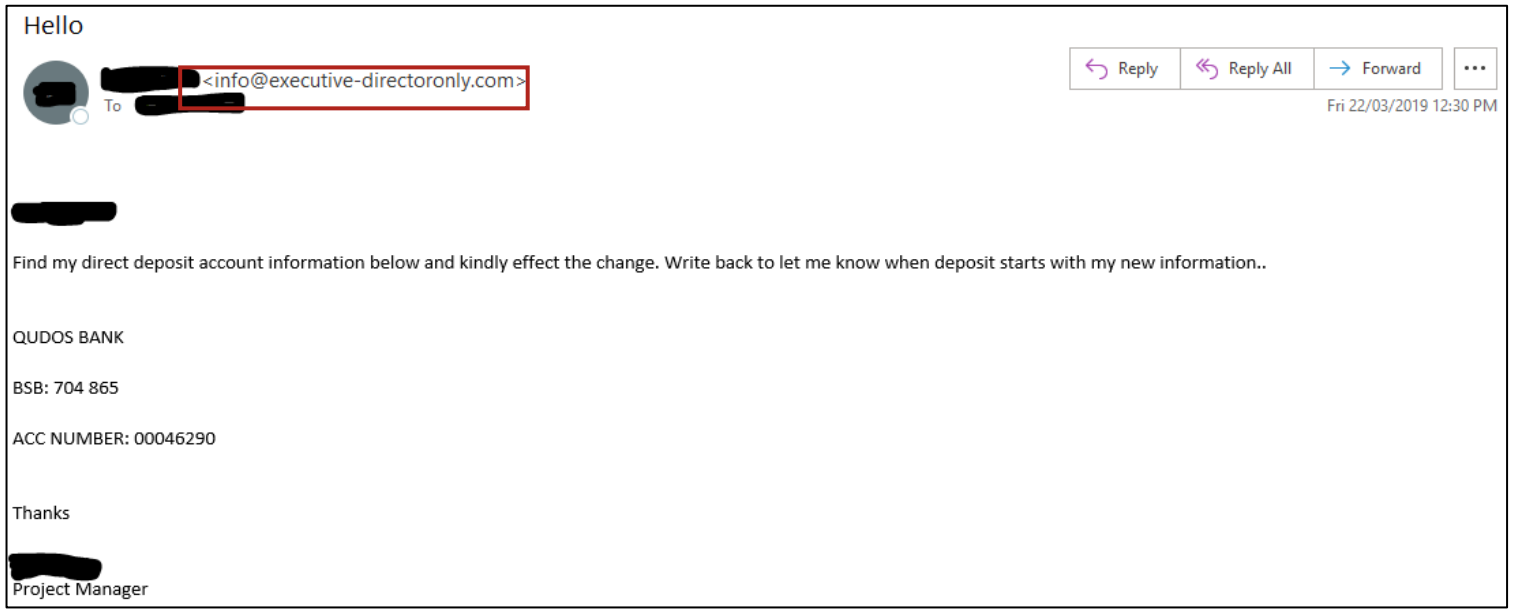
Hi [redacted]

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


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

- Email request received by payroll department appearing to be from a staff member requesting a change of bank details
- 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.

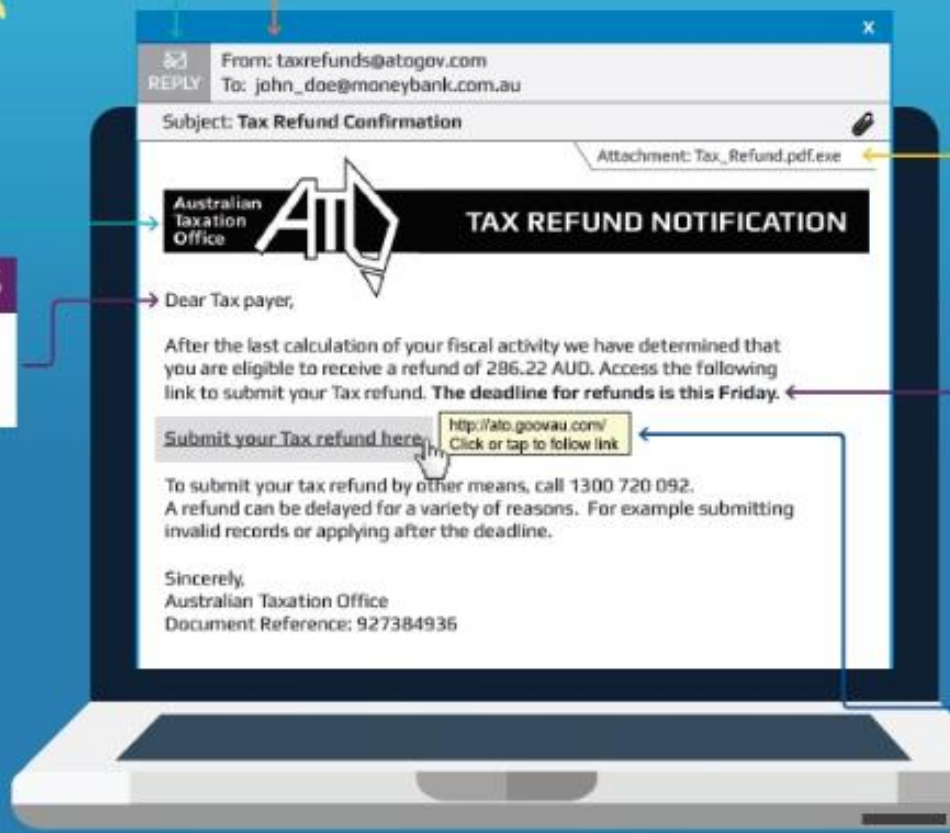
3 Poor spelling, grammar or design

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??



Can you spot a ‘phish’?

You receive this email from myGov asking you to verify your identity. What would you do?

From Australia Government <no-reply@aussie.com>
no-reply@aussie.com
Subject **Australian Government and myGov must verify your identity** 09:26
Reply to no-reply@aussie.com

Australian Government

Please DO NOT REPLY by email as this mailbox is not monitored.

This is a message from the myGov Team.

Australian Government and myGov must verify your identity - (Part 4.2, paragraph 4.2.13 of the AML/CTF Rules).

Click go to myGov and proceed with the verification.

Thank you

Message reference: UE018

- [ ] **Click the link-it looks legitimate**
- [ ] **Delete the email–it’s a scam**

Can you spot a ‘phish’?

Your boss sends you this email – what should you do?

Friday 17/08/20 2.18pm

Doe, John <john@services.com>

URGENT: gift cards needed ASAP for clients

To Sandra@services.com

Hi Sandra

Are you busy? I'm in a meeting for most of the day and forgot I need some gift cards for a big client meeting tomorrow. Can you buy ten $100 gift cards for me ASAP and let me know when you have them?

Email is the best way of contacting me at the moment.

Thanks,

John Doe

The Services Company
Chief Executive Officer
Email: john.doe@services.com

- [ ] **Buy the gift cards**
- [ ] **Ignore the email and contact IT**

2. Know where to store sensitive information

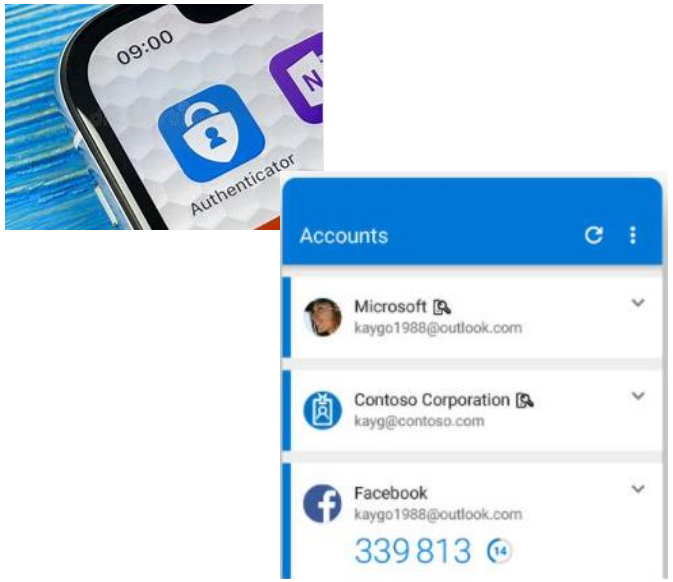
- Sensitive data such as health data and client records should only be stored in certain places e.g. client data in a Client and Case Management System
- If your organisation has not made it clear where you should store certain data so that it is appropriately protected, then you should ask

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. Beware of phishing emails. Email addresses can be ‘spoofed’ and appear to originate from people you know; validate requests if they appear suspicious
3. 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
4. Store sensitive data only in designated locations
5. Use multifactor authentication (MFA) on accounts for important or critical IT systems
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

- **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
- **Scams Awareness Week 2021:** https://www.scamwatch.gov.au/news-alerts/scams-awareness-week-2021
- **ACCC Scamwatch Report a scam**: https://www.scamwatch.gov.au/report-a-scam
- **Can you spot a scam(phishing) message?:** https://www.cyber.gov.au/acsc/view-all-content/programs/stay-smart-online/scam-messages
- **Cybersecurity awareness month resources from ACSC (October 2021)**: https://www.cyber.gov.au/acsc/view-all-content/news/cyber-security-awareness-month-2021
- **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
- **Microsoft Office Training options** https://digitaltransformation.org.au/guides/tech-foundations/training-options-microsoft-office-products