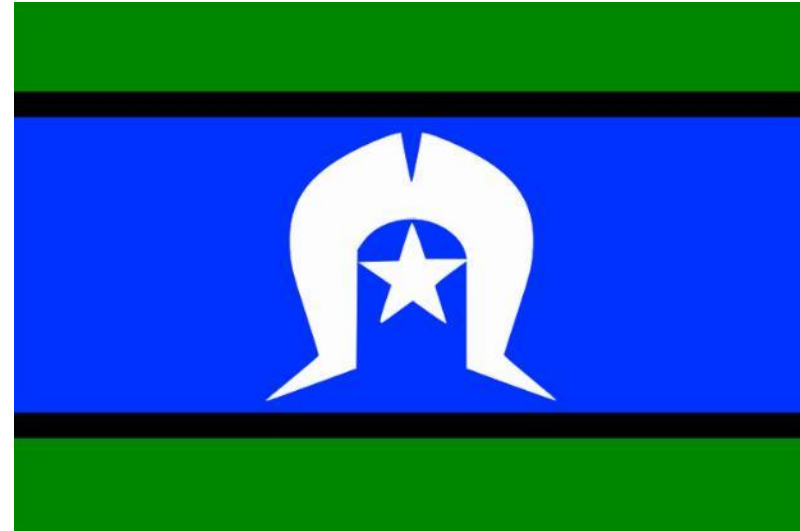# Infoxchange

CYBERSECURITY ESSENTIALS

TO KEEP DATA SAFE

October 2021

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

www.digitaltransformation.org.au

Digital
Transformation
Hub

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

www.digitaltransformation.org.au

Digital
Transformation
Hub

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

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

www.digitaltransformation.org.au

Digital Transformation Hub

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)

Technology for social justice | www.infoxchange.org

www.digitaltransformation.org.au

Cyber Security Awareness Month 2021

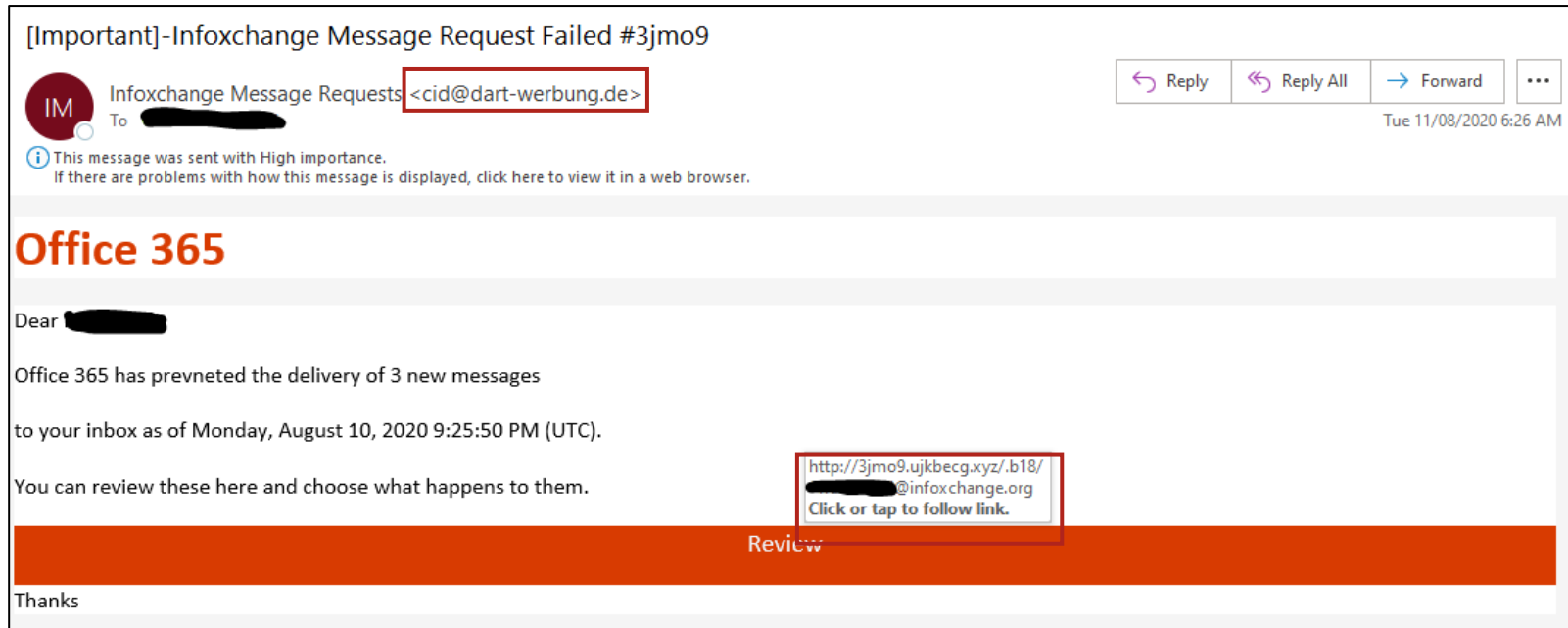Home > About the ACSC > View all content > View all news > Cyber Security Awareness Month 2021

October is Cyber Security Awareness Month.

Australians are urged to take simple steps to better protect themselves from common online threats and cybercrime during Cyber Security Awareness Month during October. The 2021 theme is: "Do your Part. #BeCyberSmart."
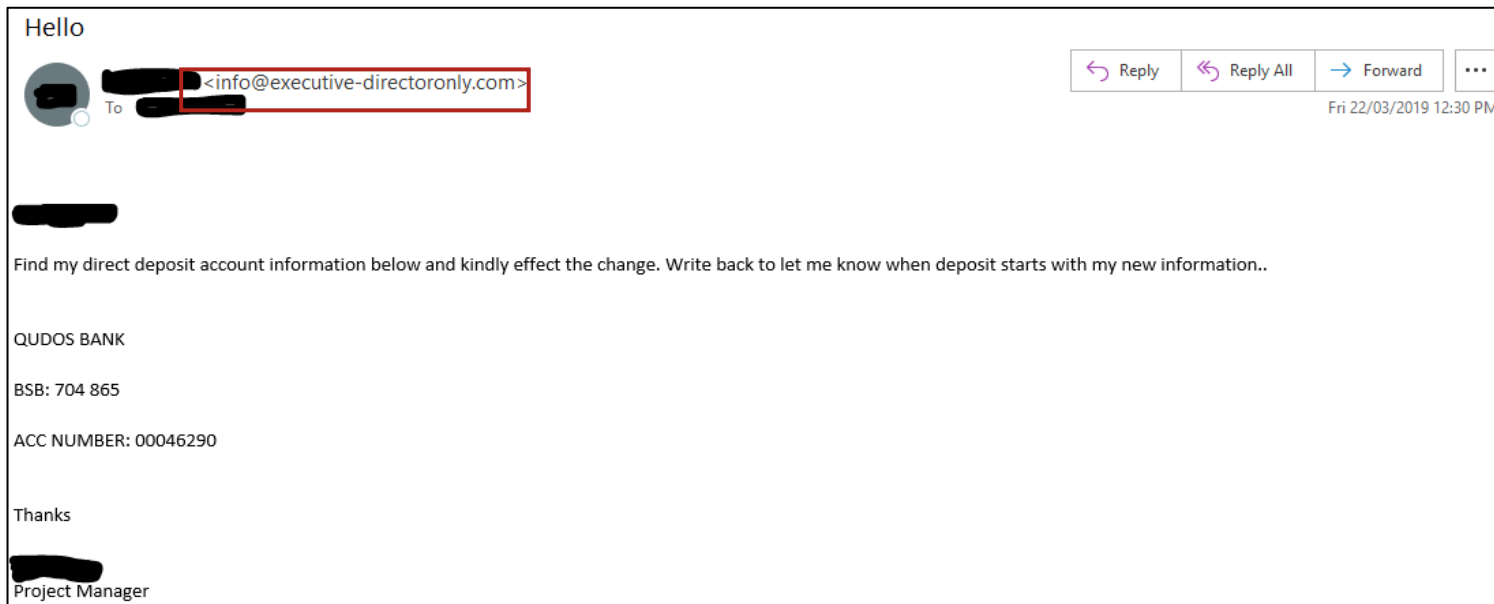
(Source: https://www.cyber.gov.au/acsc/view-all-content/news/cyber-security-awareness-month-2021)

www.digitaltransformation.org.au

Digital Transformation Hub

1. Know how to spot a phishing email

- » 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

www.digitaltransformation.org.au

Digital Transformation Hub

Know how to spot a phishing email

Hello

<info@executive-directoronly.com>
To

Fri 22/03/2019 12:05 PM

Hi ▮

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

Project Manager

Hello

<info@executive-directoronly.com>
To

Fri 22/03/2019 12:30 PM

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

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

www.digitaltransformation.org.au

Digital Transformation Hub

7 TIPS TO CATCH A PHISH

A phishing message will generally feature some of these attributes:

1 Strange "From:" address

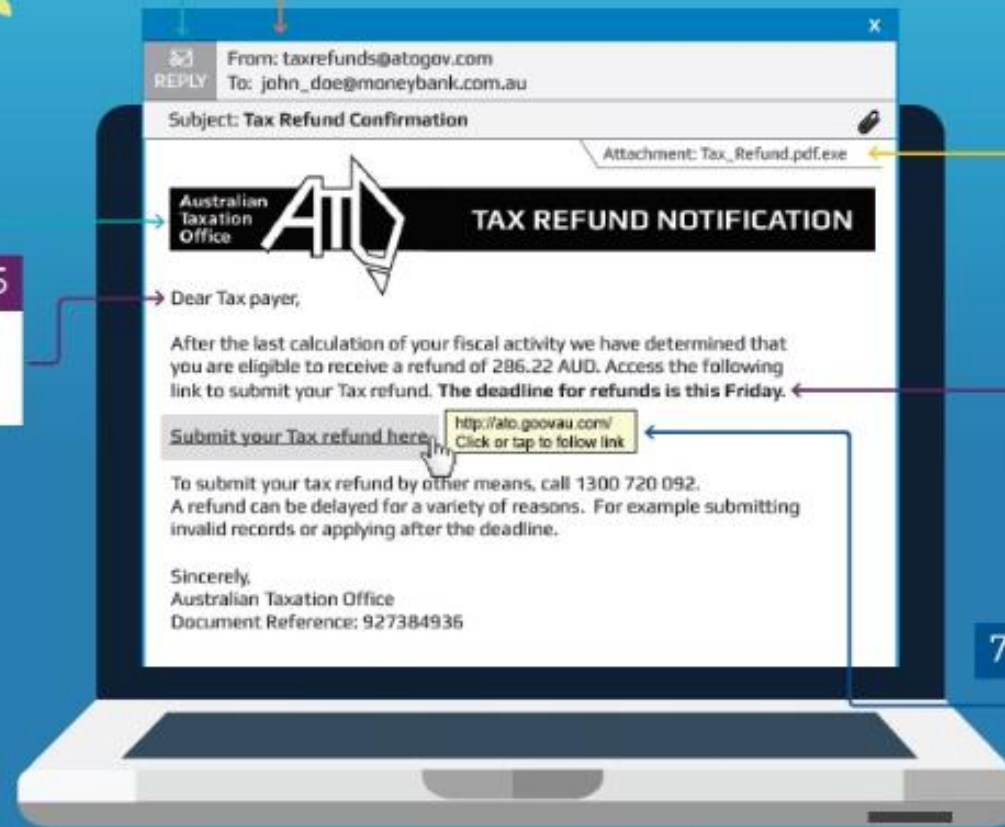**2** "Reply to" address different to the "From:" address.

> To: taxrefunds@gmail.com
> SEND 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

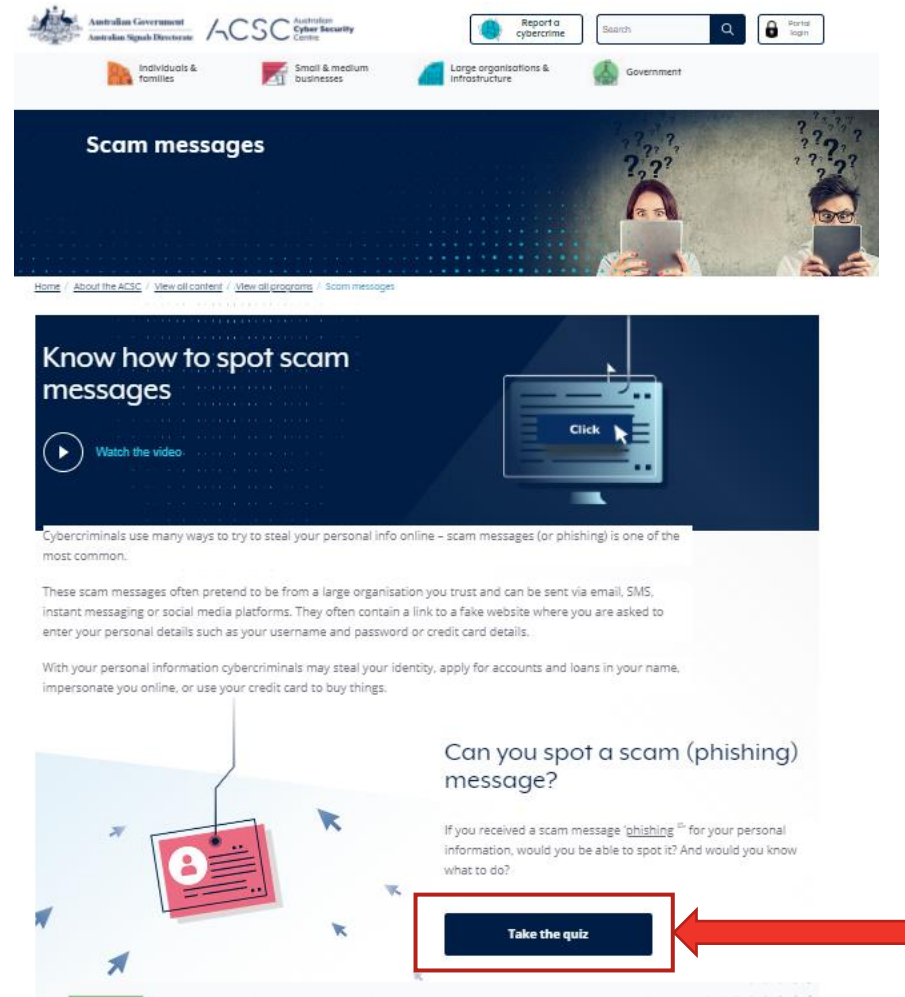**6** Urgent calls to action

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

REPLY

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

Subject: **Tax Refund Confirmation**

Attachment: Tax_Refund.pdf.exe

Australian Taxation Office — **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

9

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

Technology for social justice | www.infoxchange.org

www.digitaltransformation.org.au

Digital
Transformation
Hub

Can you spot a 'phish'?

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

Technology for social justice | www.infoxchange.org

www.digitaltransformation.org.au

Digital
Transformation
Hub

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

Technology for social justice | www.infoxchange.org

www.digitaltransformation.org.au

Digital
Transformation
Hub

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

www.digitaltransformation.org.au

Digital
Transformation
Hub
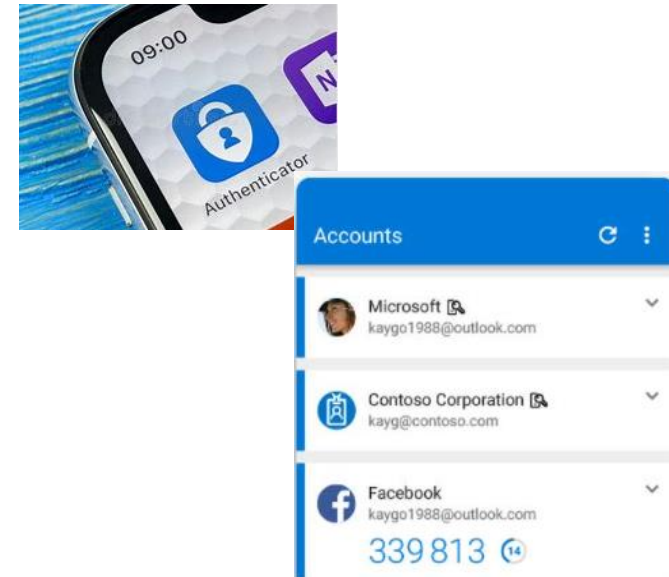
4. Keep your device secure

» 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

www.digitaltransformation.org.au

Digital Transformation Hub

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

www.digitaltransformation.org.au

Digital Transformation Hub

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

Technology for social justice | www.infoxchange.org

www.digitaltransformation.org.au

Digital
Transformation
Hub

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

» **Cybersecurity awareness month resources from ACSC**:
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

» **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

» **Microsoft Office Training options**
https://digitaltransformation.org.au/guides/tech-foundations/training-options-microsoft-office-products

www.digitaltransformation.org.au

Digital Transformation Hub