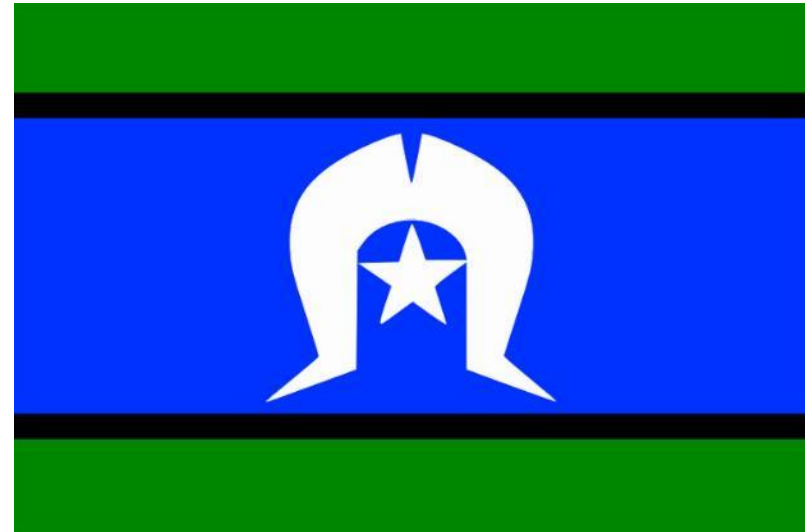


CYBER SECURITY 101:

DO YOU KNOW HOW TO KEEP YOUR ORGANISATION SECURE?

17th August 2022

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>

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>

Security in the headlines

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>

Australian Red Cross clients potentially caught up in international cyber attack

January 2022

Database of International Committee of the Red Cross breached.

Australian Red Cross is contacting clients and reviewing its local systems and services in the wake of a "major" cyber attack on a large database hosted by the International Committee of the Red Cross (ICRC).

The database held case file details on more than 500,000 people worldwide who had sought services for loved ones missing or uncontactable overseas due to disaster or conflict, or that were being held in immigration detention.

Source: <https://www.itnews.com.au/news/australian-red-cross-clients-potentially-caught-up-in-international-cyber-attack-575350>

Russian cyber attacks could inadvertently hit Australia, warns government cyber agency

February 2022

Security experts say it is unlikely new financial sanctions placed on Russia will prompt a direct retaliation, but they warn there is a significant risk Australian firms could be caught up as collateral damage.

And they warn Russian-linked criminal gangs might be encouraged to target all sorts of Western targets, prompting a possible surge in ransomware and other attacks across the globe.

Source: <https://www.abc.net.au/news/2022-02-23/cyber-agencies-warn-ukraine-cyber-attacks-from-russia/100855164>

NDIS case management system provider breached

May 2022

A security breach of a cloud-based client management system used by National Disability Insurance Scheme (NDIS) service providers has exposed a "large volume" of health and other sensitive data.

"This data includes documents containing personal information relating to our customers and their clients and carers."

Other data thought to be compromised includes Medicare and pensioner cards, as well as tax file numbers.

Source: <https://www.itnews.com.au/news/ndis-case-management-system-provider-breached-580729>

Some recent statistics

Australians reported over **566,000 scams** and over **\$1.8b** in losses in **2021**, according to the latest ACCC Targeting scams report. The top 3 scams causing most financial harm to Australians in 2021 are investment, business email compromise and romance scams

(Source: <https://www.accc.gov.au/publications/targeting-scams-report-on-scam-activity/targeting-scams-report-of-the-accc-on-scams-activity-2021>)

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 **464 notifications** under the Notifiable Data Breaches scheme in the reporting period **July – December 2021**. 256 of these were due to malicious or criminal attacks which remain the leading source of data breaches. In 2021, the OAIC received 900 data breach notifications

(Source: <https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-report-july-december-2021>)

Key message

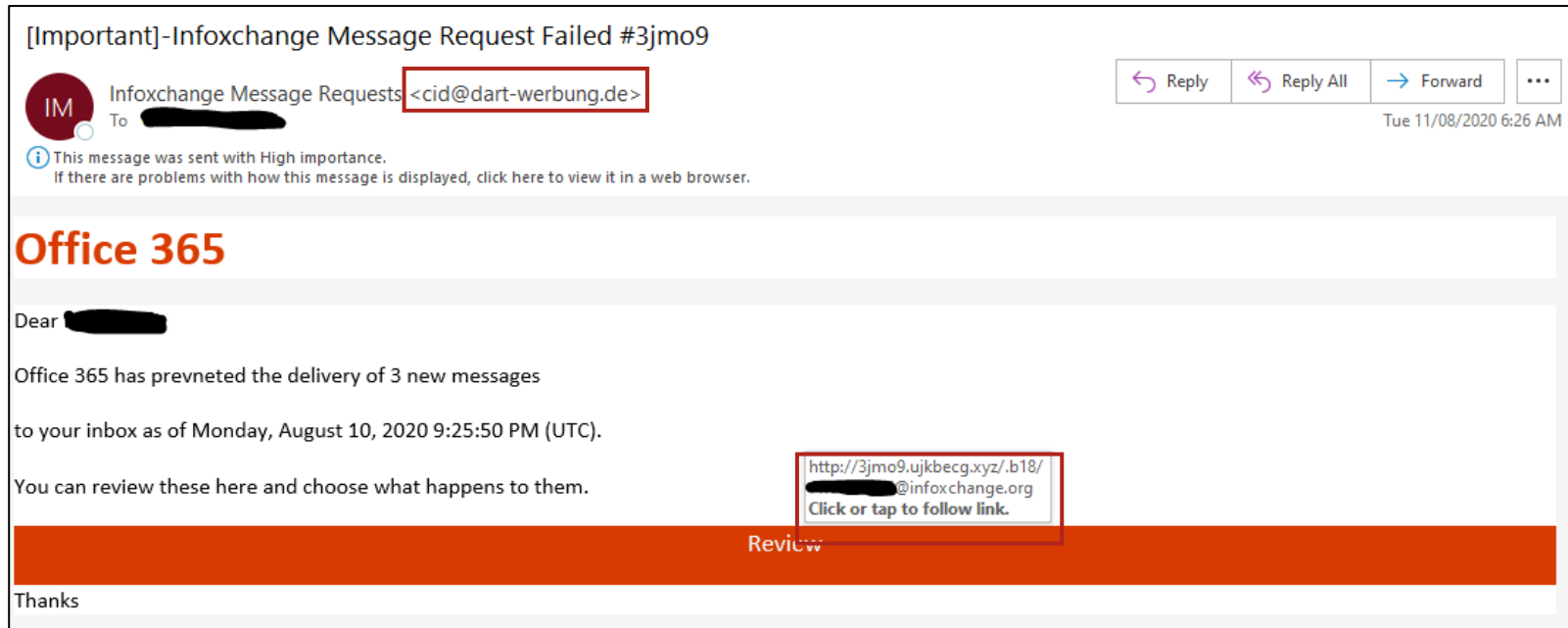
The **human element** continues to drive breaches. From a recent global breach investigation report, 82% of breaches involved the human element.

(Source: Verizon Data Breach Investigations Report 2022)

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

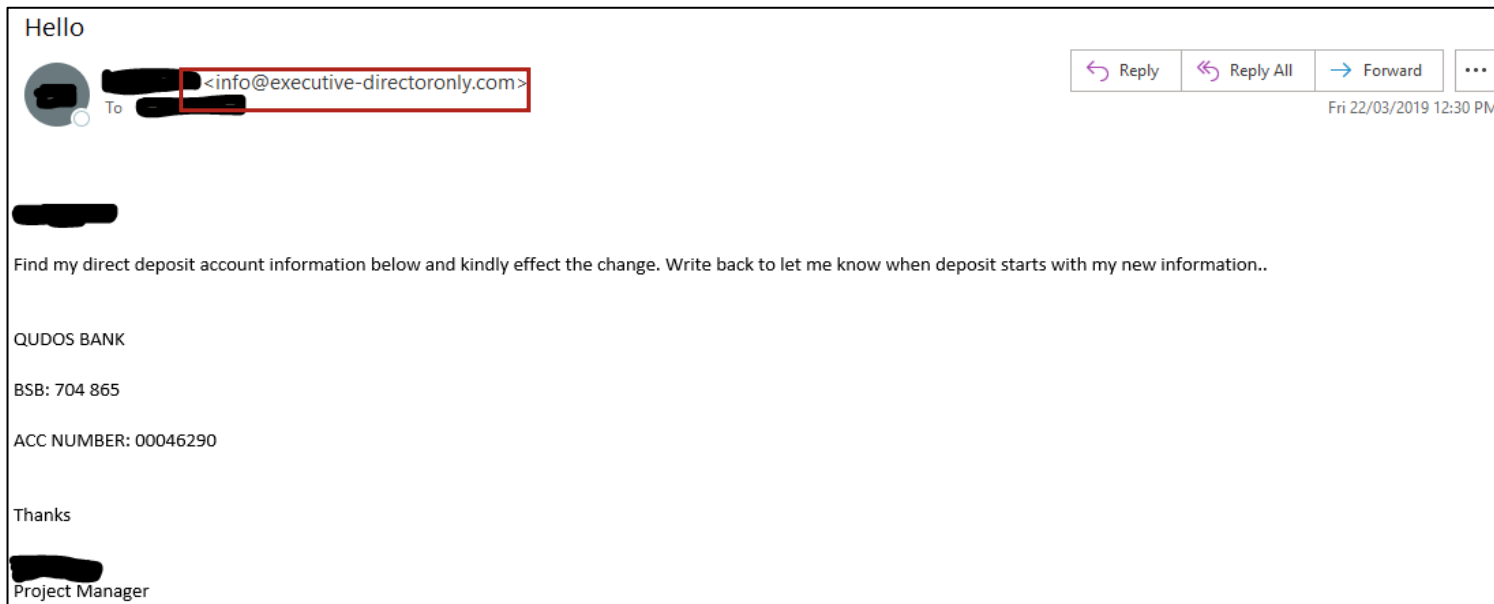
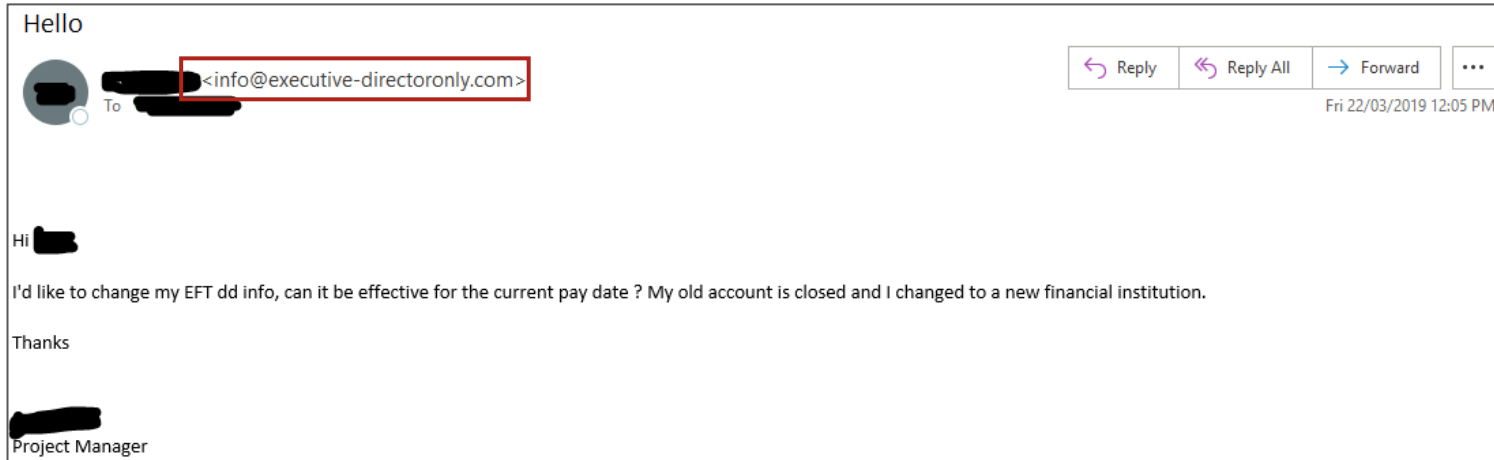
(Adapted from: Awareness is only the first step, <https://www.riscs.org.uk/wp-content/uploads/2015/12/Awareness-is-Only-the-First-Step.pdf>)

1. Know how to spot a phishing email



- » Staff member received this email 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



- » Email request received by a 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

Know how to spot a phishing email

From: Infoxchange Admin INVOICE <info@nextrend.de>
Sent: Tuesday, 7 December 2021 11:29 AM
To: [REDACTED]
Subject: Payment receipt invoice A09828 | December 7, 2021
Importance: High

INVOICE SENT AS FAX

Royal 1 Invoice

Settlement*****

Hi, [REDACTED] Here's invoice INV-0014 for USD 107,097.31.

Invoice Date: December 7, 2021

The amount outstanding of USD 107,097.31 is due on 25 December 2021.

The complete version as been provided as an attachment

Thanks,

 image182235.png

- » Email requests payment of a large amount, and includes an attachment
- » Note the 'from' address

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.

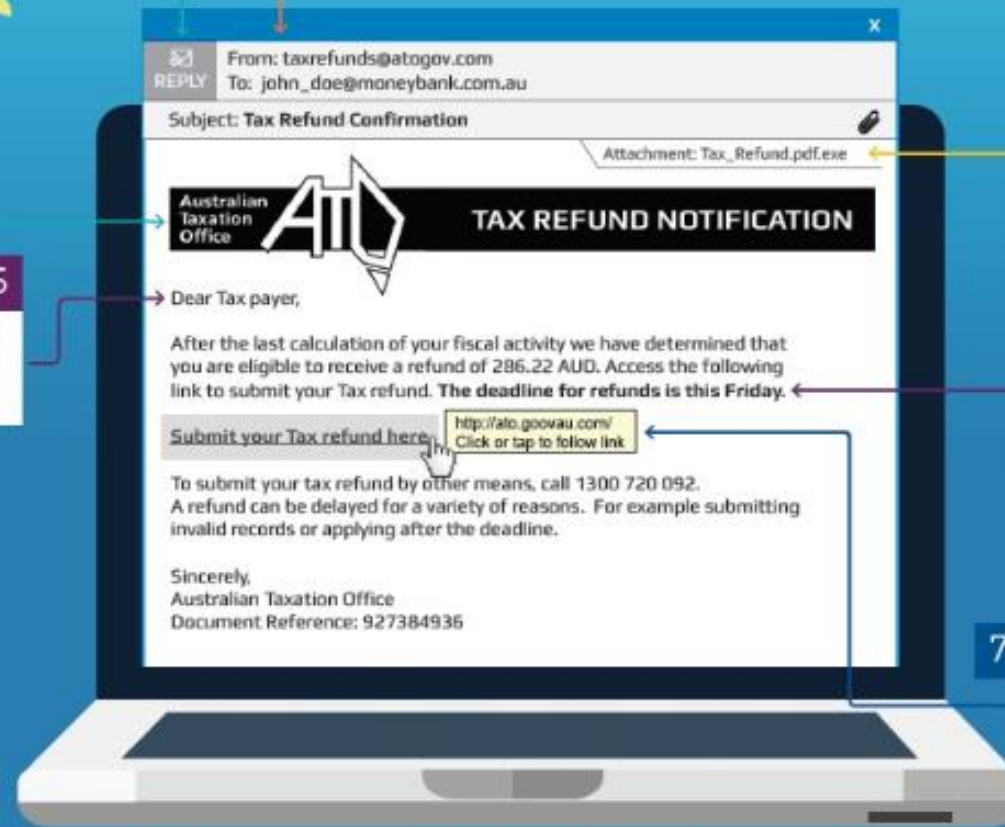
3 Poor spelling, grammar or design

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'?

From: workplacegiving@good2give.ngo <workplacegiving@good2give.ngo>

Sent: Friday, 23 August 2019 2:11 PM

To: jane_doe@gmail.com

Subject: Good2Give password reset request

The logo for Good2Give, featuring the text "good2give" in a white, lowercase, sans-serif font, with the "2" stylized as a heart shape. It is set against a solid orange rectangular background.

Hi Jane,

You have requested to reset your Good2Give password. To do this, simply click on the link below:

[Reset password](#)

<https://signin.good2give.ngo/Account/ResetPassword?userId=6b4551bc-3f7e-2004-9642-8&code=CfDJ8KKFSWQ9i>

Happy giving!

The Good2Give Team

Good2Give | Ground Floor, 12 Holtermann Street, Crows Nest NSW 2065

www.good2give.ngo

Select an option:

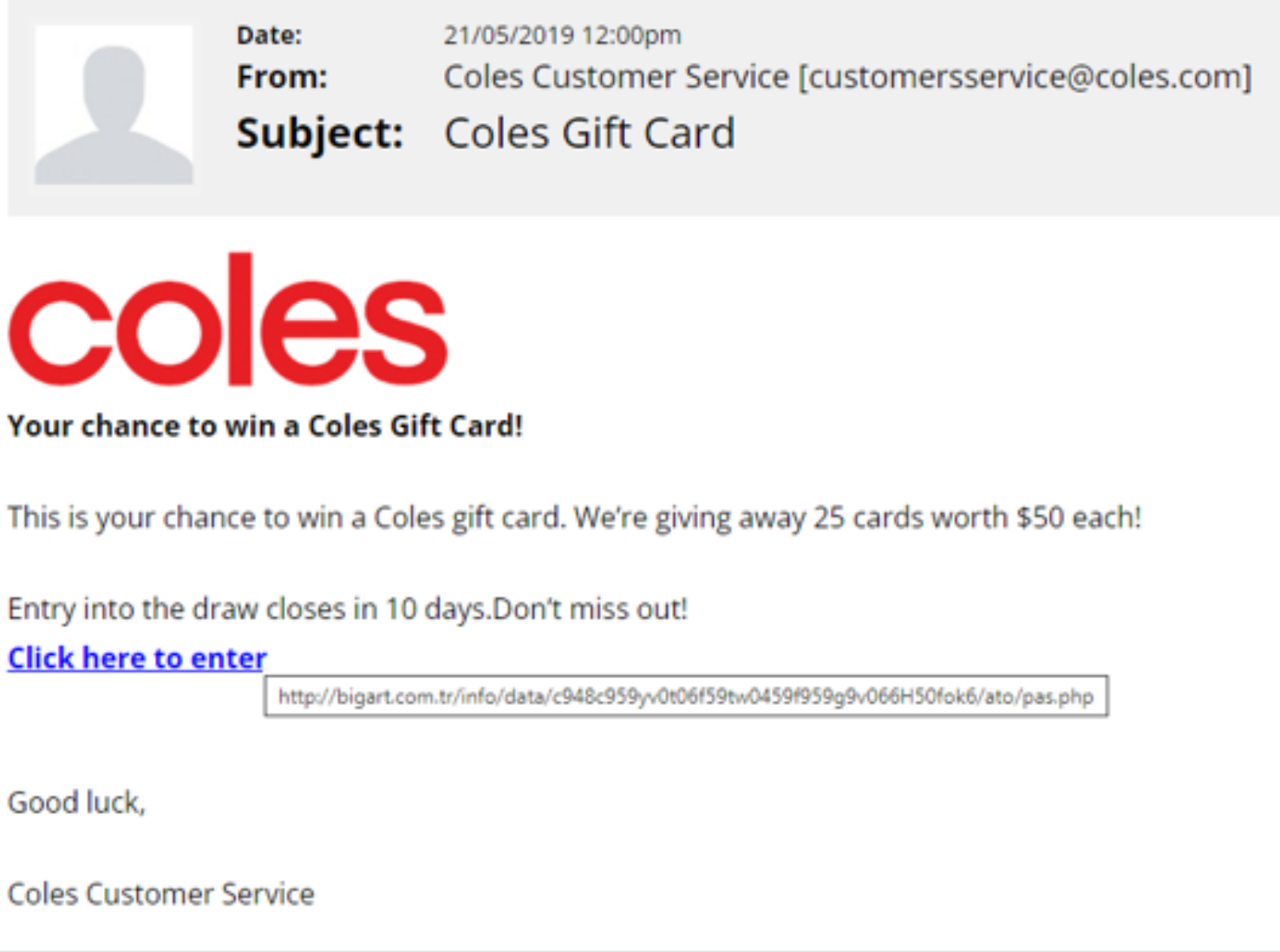
☐

This email is real

☐

Delete the email

Can you spot a 'phish'?



Select an option:

☐

Click and enter my details

☐

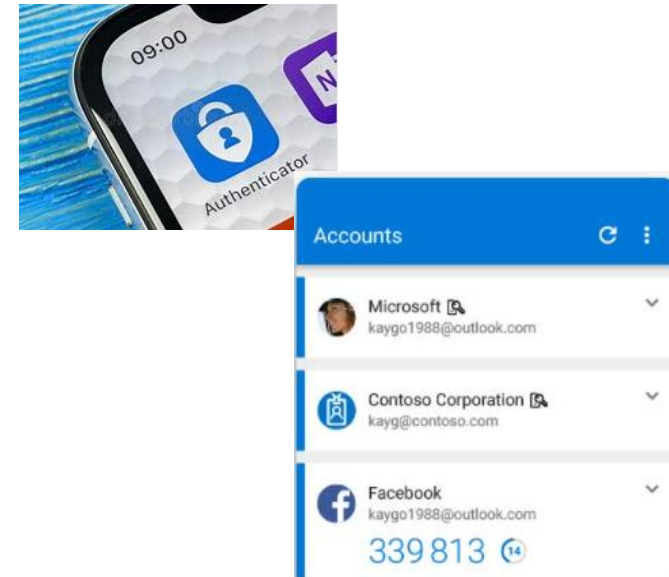
Delete the email

2. Protect important and sensitive information

- » If within your organisation, you collect information considered confidential or sensitive by certain industry standards or laws you must take reasonable measures to protect it.
- » Sensitive data such as health data and client records (for NFPs who may deal with this type of information) should only be stored in certain locations e.g. client data in a Client and Case Management System
- » Awareness among volunteers and staff on how certain types of information is to be handled. If your organisation has not made it clear where you should store certain data so that it is appropriately protected, then you should ask e.g. important data required for your organisation processes must be backed up

3. Use good password practices

- » Know how to pick a strong password or passphrase
 - 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

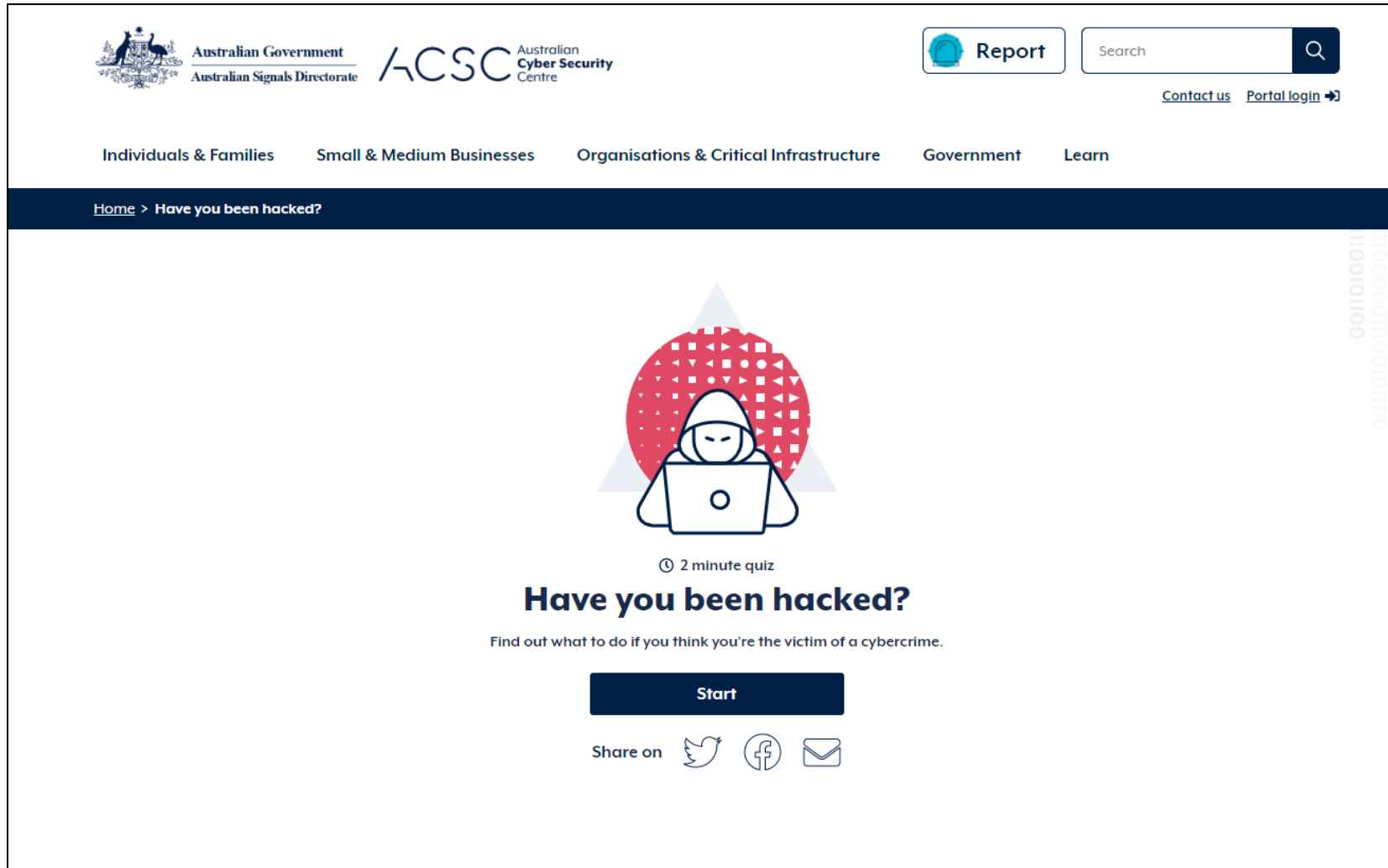
- » Physically protect your device
- » Lock your screen when device is left unattended (Windows: Ctrl + Alt + Del; MAC: Ctrl+ Cmd + Q)
- » Keep devices up-to-date (operating systems, applications such as web browsers)
- » Do not install or use unauthorised software on organisational devices
- » If using your **own device** (BYOD) such as mobile phone or other device for work with your organisation or group:
 - 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 within your organisation
- » Australian Cyber Security Centre national cyber security hotline – 1300CYBER1: <https://www.cyber.gov.au/acsc/view-all-content/news/acsc-call-247>

Australian Cyber Security Centre – “Have I been hacked”



<https://www.cyber.gov.au/have-you-been-hacked>

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, particularly for finance-related matters.
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>
- » **Australian Cyber Security Centre (ACSC):** <https://www.cyber.gov.au>
- » **ACSC tool: Have you been hacked:** <https://www.cyber.gov.au/have-you-been-hacked>
- » **Can you spot a scam(phishing) message?:** <https://www.cyber.gov.au/acsc/view-all-content/programs/stay-smart-online/scam-messages>
- » **ACCC Scamwatch Report a scam:** <https://www.scamwatch.gov.au/report-a-scam>
- » **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/>
- » **Microsoft Office Training options**
<https://digitaltransformation.org.au/guides/tech-foundations/training-options-microsoft-office-products>

Questions and discussion