Phriendly Phishing

CYBERSECURITY AWARENESS MONTH

We will commence shortly...

Cyber Security

AWARENESS MONTH

Phriendly Phishing

CYBERSECURITY AWARENESS MONTH

Have a Question?
Use the Q&A feature during the webinar to ask your questions along the way!

Cyber Security

AWARENESS MONTH

Today's Agenda

- Benefits of Cyber Security Awareness Month
- Employee Toolkit
- Cyber Security Awareness Training Timeline
- How to Schedule Training and Spear phishing
- Enabling Additional Security Features
- Q&A

Have a Question?
Use the Q&A feature during the webinar
to ask your questions along the way!

CYBERSECURITY
AWARENESS
MONTH

Poll: Why is Cyber Security Education important to your business?

#SeeYourselfInCyber

Cyber Security Awareness Month

What is it?

- **October** is the nationally recognised month for Cyber Security Awareness
- **International theme: See Yourself in Cyber**
- **Australian theme: Have you been hacked?**
- **New Zealand theme: Get Cyber Smart**

Why it matters:

- Empower individuals to improve their online security so they're less vulnerable to cyber attacks
- Opportunity to promote security awareness training courses and additional metrics of testing
  - Enable Multi-factor Authentication
  - Passwords & Paraphrases
  - Recognise and Report Phishing

70%
Are majorly concerned about protecting personal information

85%
Understand the importance of protecting personal information

87%
Want more choice over how their personal information is used

82%
Believe children should be empowered to use online services, however their data privacy must be protected

84%
Consider privacy extremely important when selecting a digital service

84%
Want personal information to be used in a way that does not cause harm, loss, or distress.

Source: Australian Community Attitudes to Privacy Survey 2020

Benefits

What will your employees get out of it?

- Empower individuals to make better decisions about cyber security for themselves, their organisations and their family
- Simple steps everyone can take to protect from cyber threats
- Resources to share with their family and friends

What will businesses get out of it?

- Increase knowledge and training to provide to your team
- Help reduce your risk of human error

What is the ask to staff?

- Review the email content weekly
- Complete any scheduled training (~5 minutes each course)
- Start a conversation about the importance of cyber security

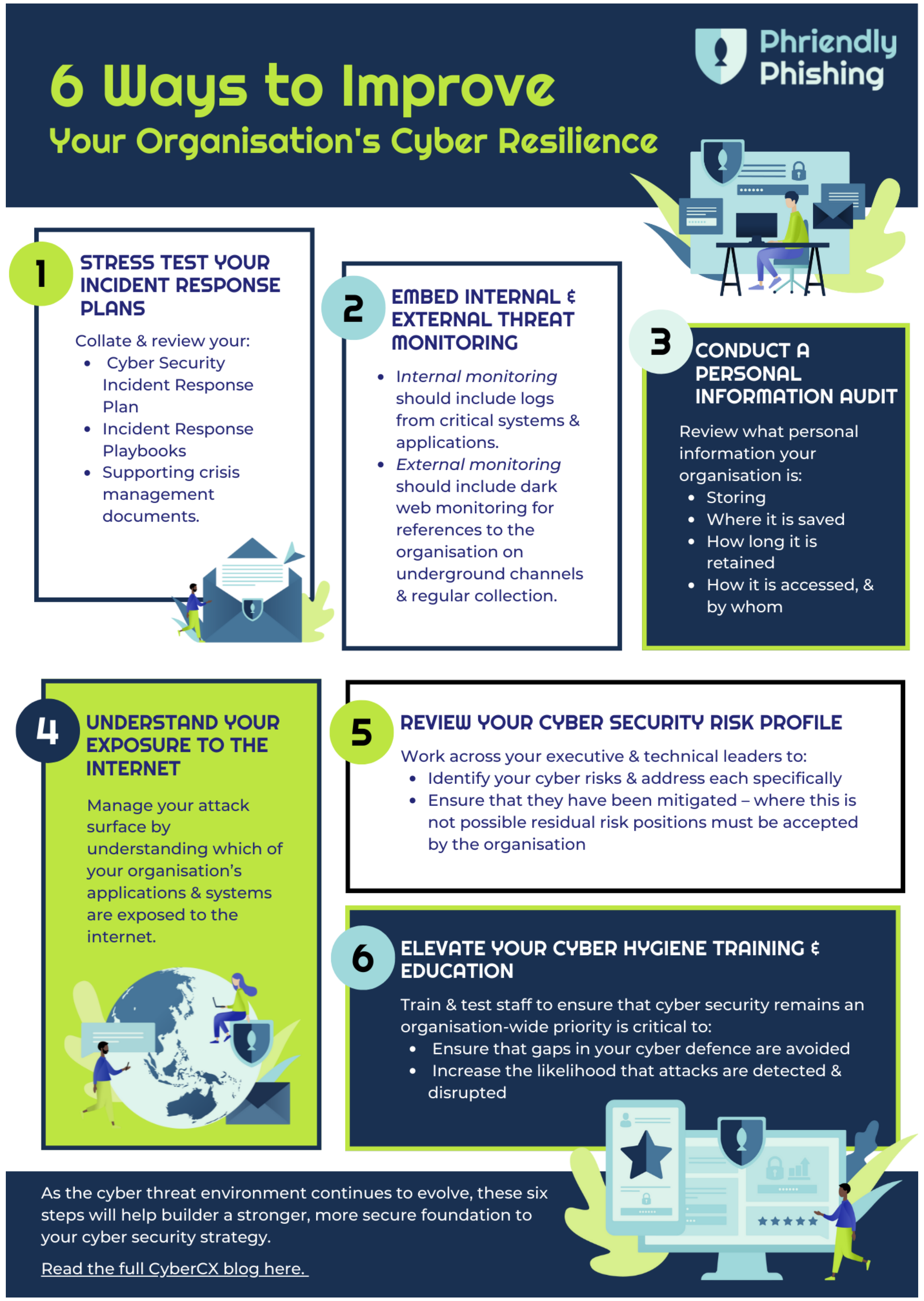
ACSC Australian **Cyber Security** Centre

Want more resources?

The Australian Cyber Security Centre have a tonne of content available on its website.

Scan the QR code for more:

How to guides:



Phriendly Phishing

6 Ways to Improve Your Organisation's Cyber Resilience

1 Stress test your incident response plans

Collate & review your:

- Cyber Security Incident Response Plan
- Incident Response Playbooks
- Supporting crisis management documents.

2 Embed internal & external threat monitoring

- *Internal monitoring* should include logs from critical systems & applications.
- *External monitoring* should include dark web monitoring for references to the organisation on underground channels & regular collection.

3 Conduct a personal information audit

Review what personal information your organisation is:

- Storing
- Where it is saved
- How long it is retained
- How it is accessed, & by whom

4 Understand your exposure to the internet

Manage your attack surface by understanding which of your organisation's applications & systems are exposed to the internet.

5 Review your cyber security risk profile

Work across your executive & technical leaders to:

- Identify your cyber risks & address each specifically
- Ensure that they have been mitigated – where this is not possible residual risk positions must be accepted by the organisation

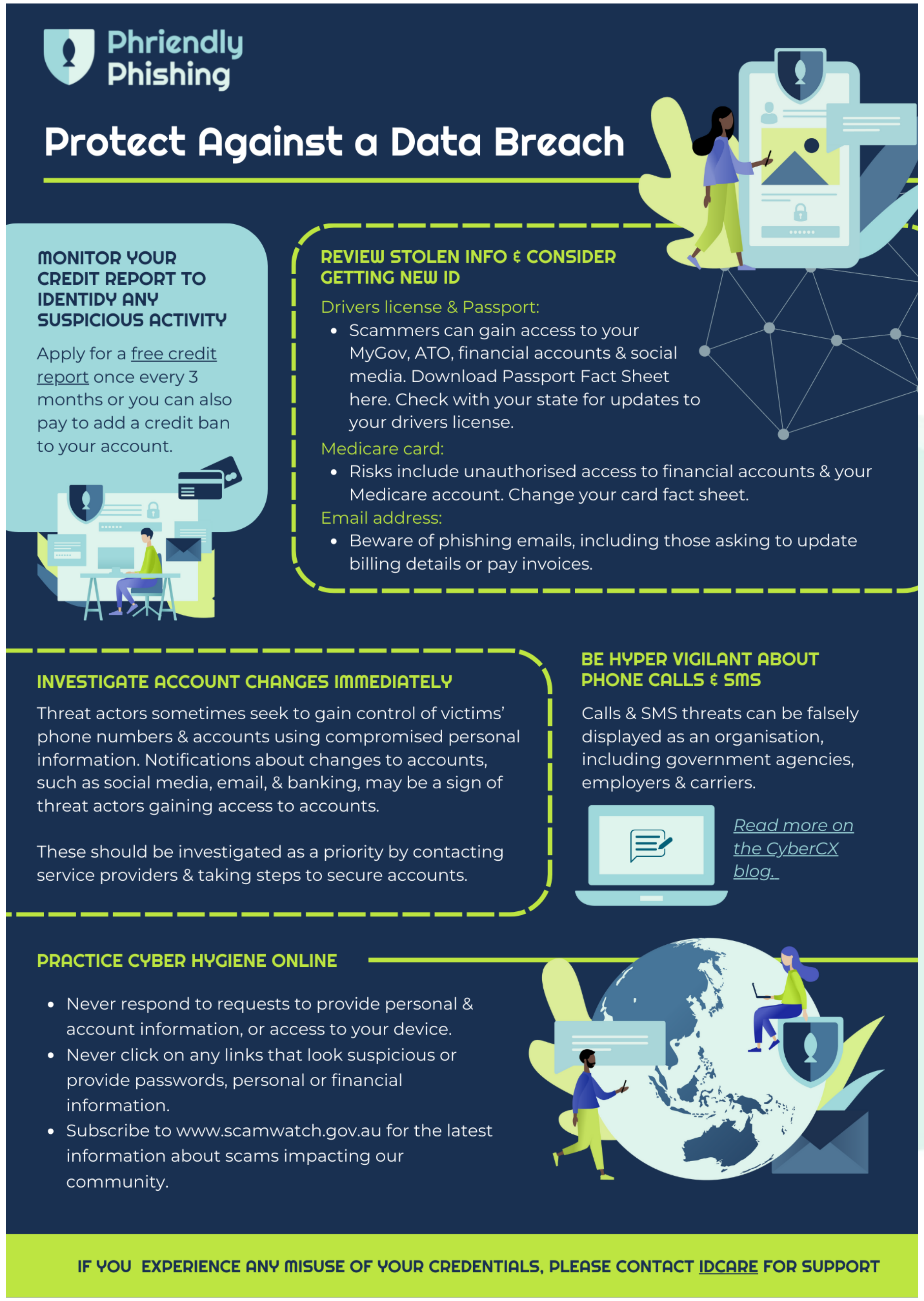
6 Elevate your cyber hygiene training & education

Train & test staff to ensure that cyber security remains an organisation-wide priority is critical to:

- Ensure that gaps in your cyber defence are avoided
- Increase the likelihood that attacks are detected & disrupted

As the cyber threat environment continues to evolve, these six steps will help builder a stronger, more secure foundation to your cyber security strategy.

Read the full CyberCX blog here.



Phriendly Phishing

Protect Against a Data Breach

Monitor your credit report to identify any suspicious activity

Apply for a free credit report once every 3 months or you can also pay to add a credit ban to your account.

Review stolen info & consider getting new ID

Drivers license & Passport:

- Scammers can gain access to your MyGov, ATO, financial accounts & social media. Download Passport Fact Sheet here. Check with your state for updates to your drivers license.

Medicare card:

- Risks include unauthorised access to financial accounts & your Medicare account. Change your card fact sheet.

Email address:

- Beware of phishing emails, including those asking to update billing details or pay invoices.

Investigate account changes immediately

Threat actors sometimes seek to gain control of victims' phone numbers & accounts using compromised personal information. Notifications about changes to accounts, such as social media, email, & banking, may be a sign of threat actors gaining access to accounts.

These should be investigated as a priority by contacting service providers & taking steps to secure accounts.

Be hyper vigilant about phone calls & SMS

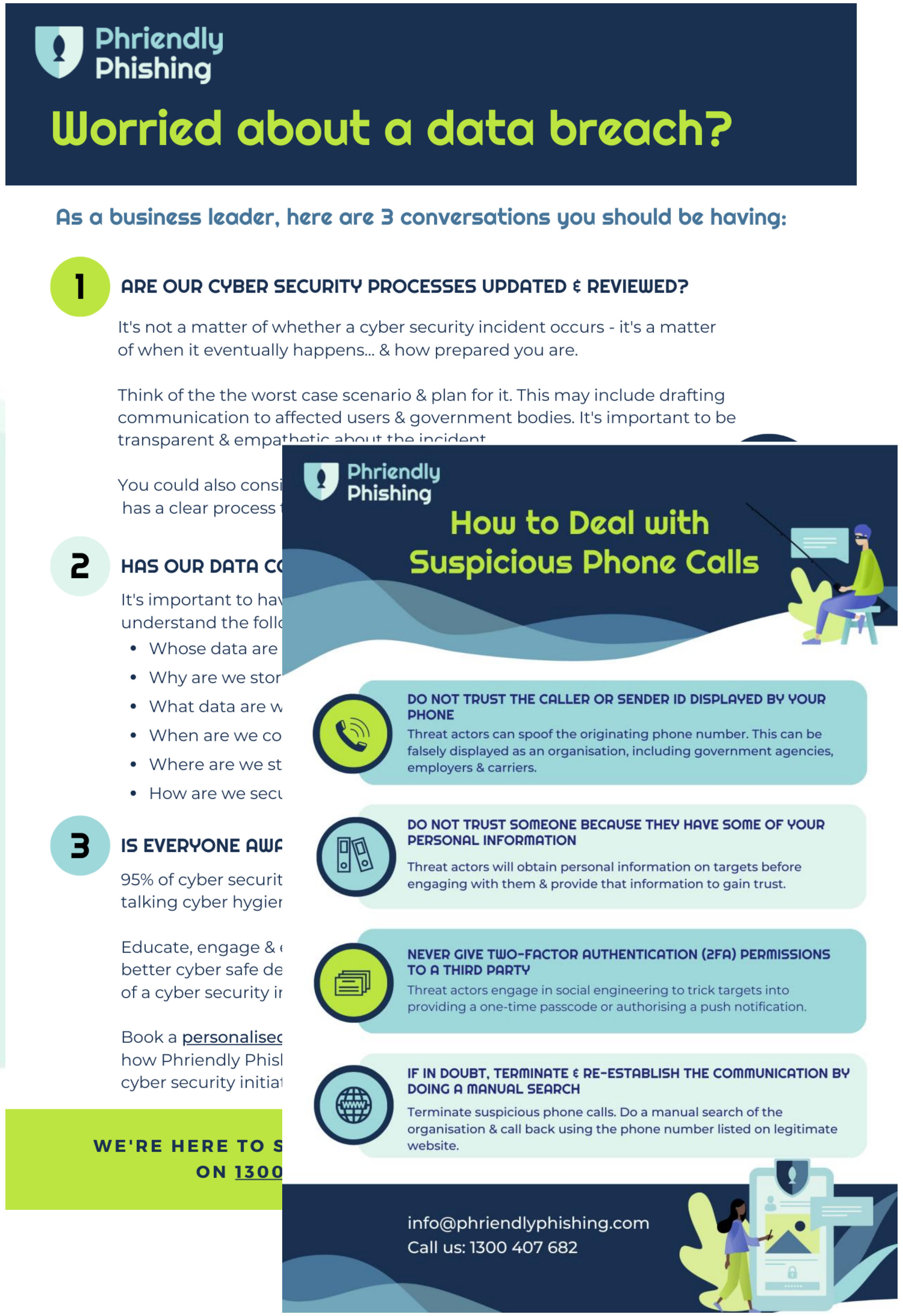
Calls & SMS threats can be falsely displayed as an organisation, including government agencies, employers & carriers.

Read more on the CyberCX blog.

Practice cyber hygiene online

- Never respond to requests to provide personal & account information, or access to your device.
- Never click on any links that look suspicious or provide passwords, personal or financial information.
- Subscribe to www.scamwatch.gov.au for the latest information about scams impacting our community.

IF YOU EXPERIENCE ANY MISUSE OF YOUR CREDENTIALS, PLEASE CONTACT IDCARE FOR SUPPORT



Phriendly Phishing

Worried about a data breach?

As a business leader, here are 3 conversations you should be having:

1 Are our cyber security processes updated & reviewed?

It's not a matter of whether a cyber security incident occurs - it's a matter of when it eventually happens... & how prepared you are.

Think of the the worst case scenario & plan for it. This may include drafting communication to affected users & government bodies. It's important to be transparent & empathetic about the incident

You could also consi
has a clear process

2 Has our data co

It's important to hav
understand the follo

- Whose data are
- Why are we stor
- What data are w
- When are we co
- Where are we st
- How are we secu

3 Is everyone awa

95% of cyber securit
talking cyber hygien

Educate, engage & e
better cyber safe de
of a cyber security in

Book a personalised
how Phriendly Phish
cyber security initiat

WE'RE HERE TO S
ON 1300

Phriendly Phishing

How to Deal with Suspicious Phone Calls

Do not trust the caller or sender ID displayed by your phone

Threat actors can spoof the originating phone number. This can be falsely displayed as an organisation, including government agencies, employers & carriers.

Do not trust someone because they have some of your personal information

Threat actors will obtain personal information on targets before engaging with them & provide that information to gain trust.

Never give two-factor authentication (2FA) permissions to a third party

Threat actors engage in social engineering to trick targets into providing a one-time passcode or authorising a push notification.

If in doubt, terminate & re-establish the communication by doing a manual search

Terminate suspicious phone calls. Do a manual search of the organisation & call back using the phone number listed on legitimate website.

info@phriendlyphishing.com
Call us: 1300 407 682

Employee Tool Kit

□ **Send kick off email to your team**

Launch Monday, October 3

This year's Cyber Security Awareness Month theme is "See Yourself in Cyber" which demonstrates that at the heart of cyber security, it's really all about people. The kick off email will explain the upcoming content and recognise the importance of cyber security awareness month.

□ Week 1: Safety Online

Launch October 5

Helping users have a safer, more enjoyable online experience

Posters & Downloads:

- Avoid online scams
- Stay safe online

Videos:

- Safety online
- Credential harvesting

□ Week 2: Passwords & Passphrases

Launch October 12

Encourage staff to use safer passwords & passphrases.

Posters & Downloads:

- Password Safety
- Passphrases

Videos:

- Passwords & passphrases
- Passwords for Kids

□ Week 3: Social Engineering

Launch October 19

Protect yourself from social engineering and train your employees to keep a look out.

Posters & Downloads:

- Social engineering
- Zoom background

Videos:

- Social engineering attacks' and how to avoid them

□ Week 4: Cyberbullying

Launch October 26

Anyone and everyone can be vulnerable to cyberbullying.

Posters & Downloads:

- A guide to cyberbullying
- Social media safety

Videos:

- Nice on the Net

#SeeYourselfInCyber

Courses you can schedule…

WEEK 1: Safety Online
Course to schedule: Safety Online and Protecting your Digital Identity.

WEEK 2: Passwords and Passphrases
Course to schedule: Passwords and Paraphrases. (Kid-friendly video (mp4) available.

WEEK 3: Social Engineering
Course to schedule: Scam and Social Engineering.

WEEK 4: Cyberbullying
Course to schedule: Smishing & Social Media. (Kid-friendly – Be Nice on the Net video (mp4) available.

Have you already scheduled on of these courses? Switch it out from the list below:

Lite

- S.C.A.M 101 – 301

Plus

- Online and Remote threats

Premium

- Protecting your digital identity
- Mobile phones & tablets
- Social media
- Smishing
- Vishing

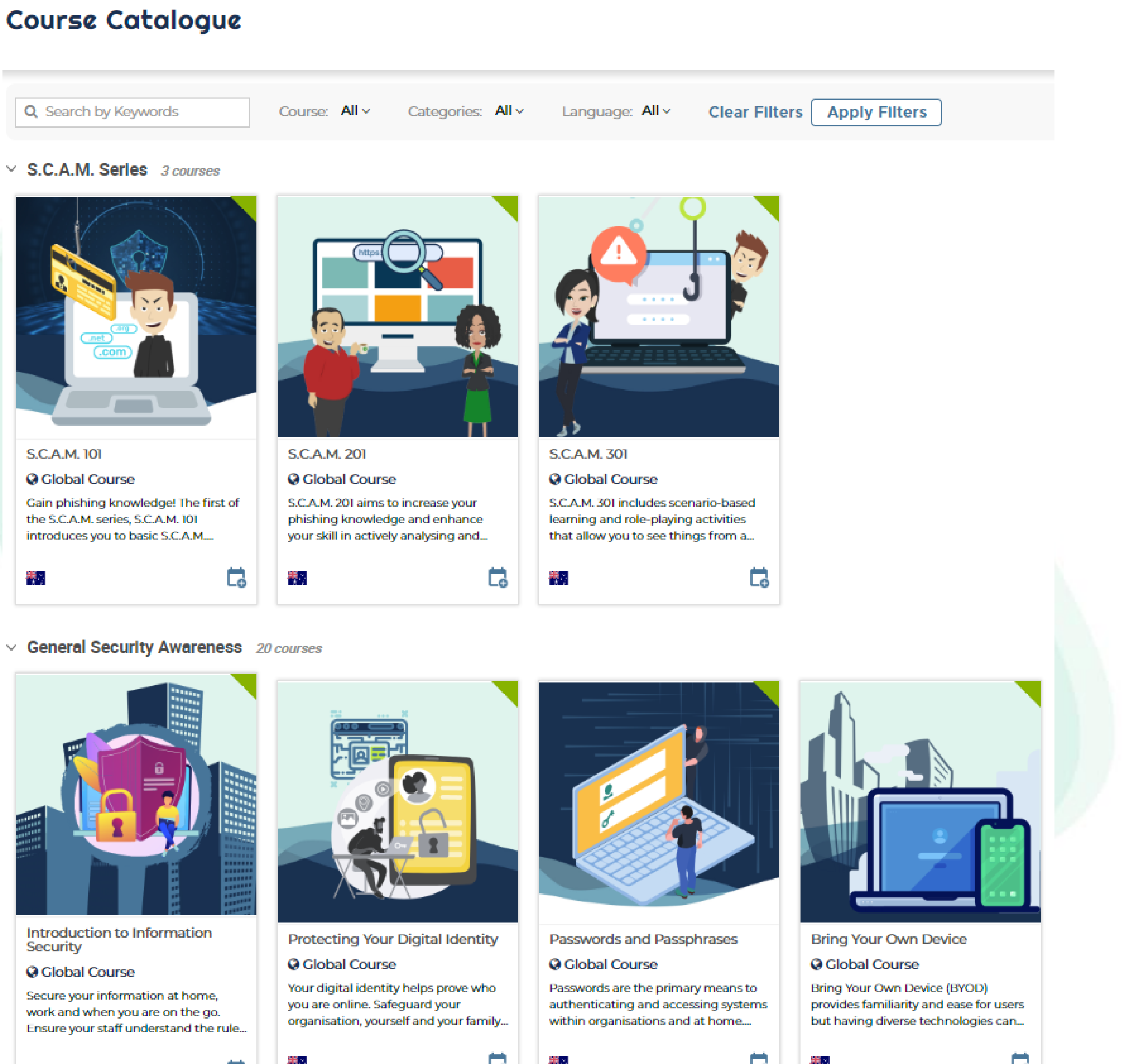
Scheduling Training Courses

Key Features:

- Preview each training course on the Course Catalogue tab
- Over 50+ training courses to choose from
- Customise training email templates
- Enable reminder emails by default

Why it matters:

- Quickly advance staff with wider cyber security training – relevant and current!



Course Catalogue

Search by Keywords · Course: All · Categories: All · Language: All · Clear Filters · Apply Filters

S.C.A.M. Series *3 courses*

S.C.A.M. 101
Global Course
Gain phishing knowledge! The first of the S.C.A.M. series, S.C.A.M. 101 introduces you to basic S.C.A.M....

S.C.A.M. 201
Global Course
S.C.A.M. 201 aims to increase your phishing knowledge and enhance your skill in actively analysing and...

S.C.A.M. 301
Global Course
S.C.A.M. 301 includes scenario-based learning and role-playing activities that allow you to see things from a...

General Security Awareness *20 courses*

Introduction to Information Security
Global Course
Secure your information at home, work and when you are on the go. Ensure your staff understand the rule...

Protecting Your Digital Identity
Global Course
Your digital identity helps prove who you are online. Safeguard your organisation, yourself and your family...

Passwords and Passphrases
Global Course
Passwords are the primary means to authenticating and accessing systems within organisations and at home....

Bring Your Own Device
Global Course
Bring Your Own Device (BYOD) provides familiarity and ease for users but having diverse technologies can...

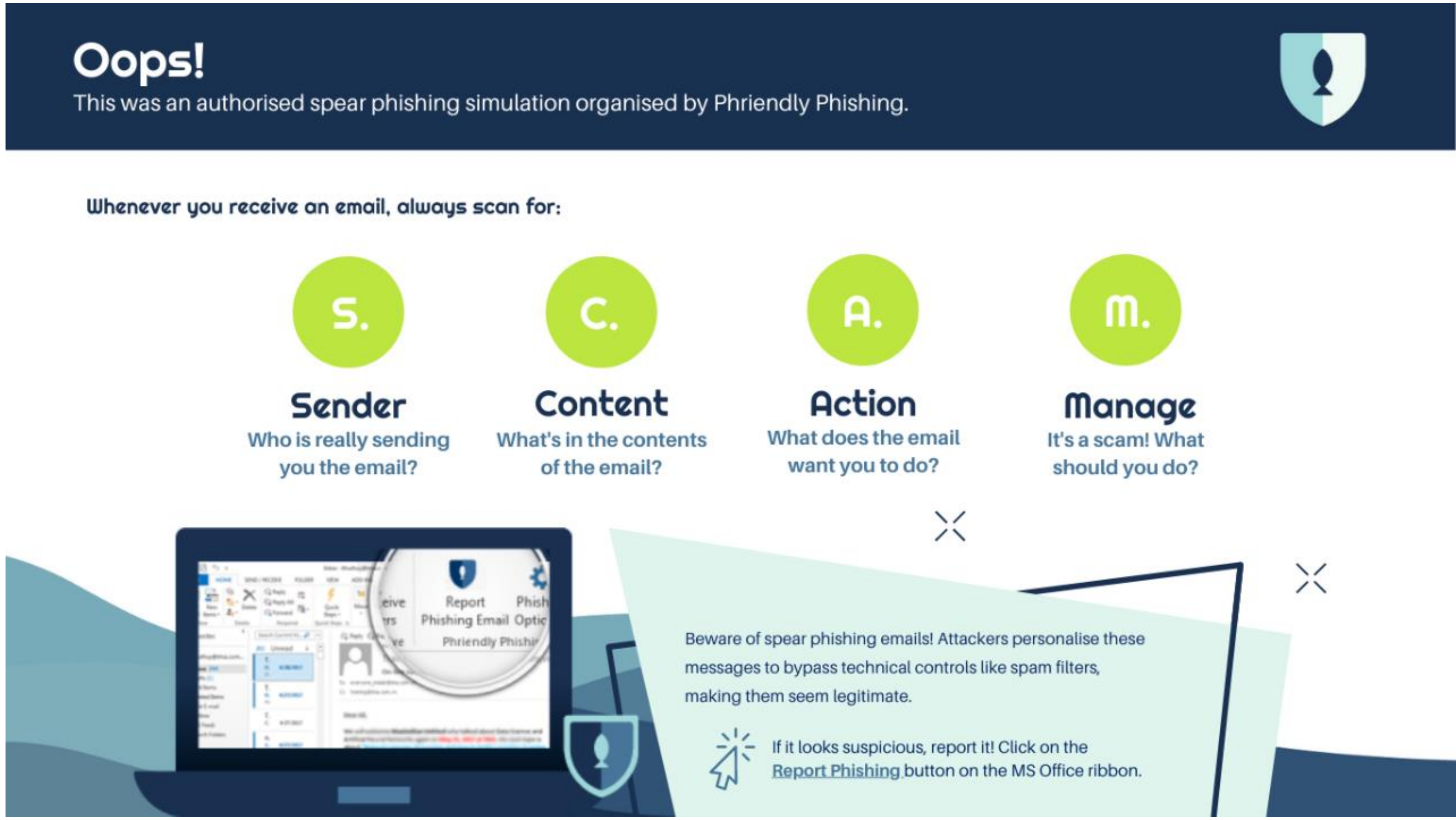
Sophisticated Targeting Campaigns

Key Features:

- Smart Groups to dynamically target teams based on attributes or segments
- Spear phishing campaigns with customised experience
- New branded templates with logos!

Why it matters:

- Target high risk teams or individuals
- Uplift sophistication with legitimate email templates
- Determine frequency to gather data points



Oops!

This was an authorised spear phishing simulation organised by Phriendly Phishing.

Whenever you receive an email, always scan for:

S. Sender
Who is really sending you the email?

C. Content
What's in the contents of the email?

A. Action
What does the email want you to do?

M. Manage
It's a scam! What should you do?

Beware of spear phishing emails! Attackers personalise these messages to bypass technical controls like spam filters, making them seem legitimate.

If it looks suspicious, report it! Click on the Report Phishing button on the MS Office ribbon.

CYBERSECURITY
AWARENESS
MONTH

Poll: Do you need to test your cyber superheroes?

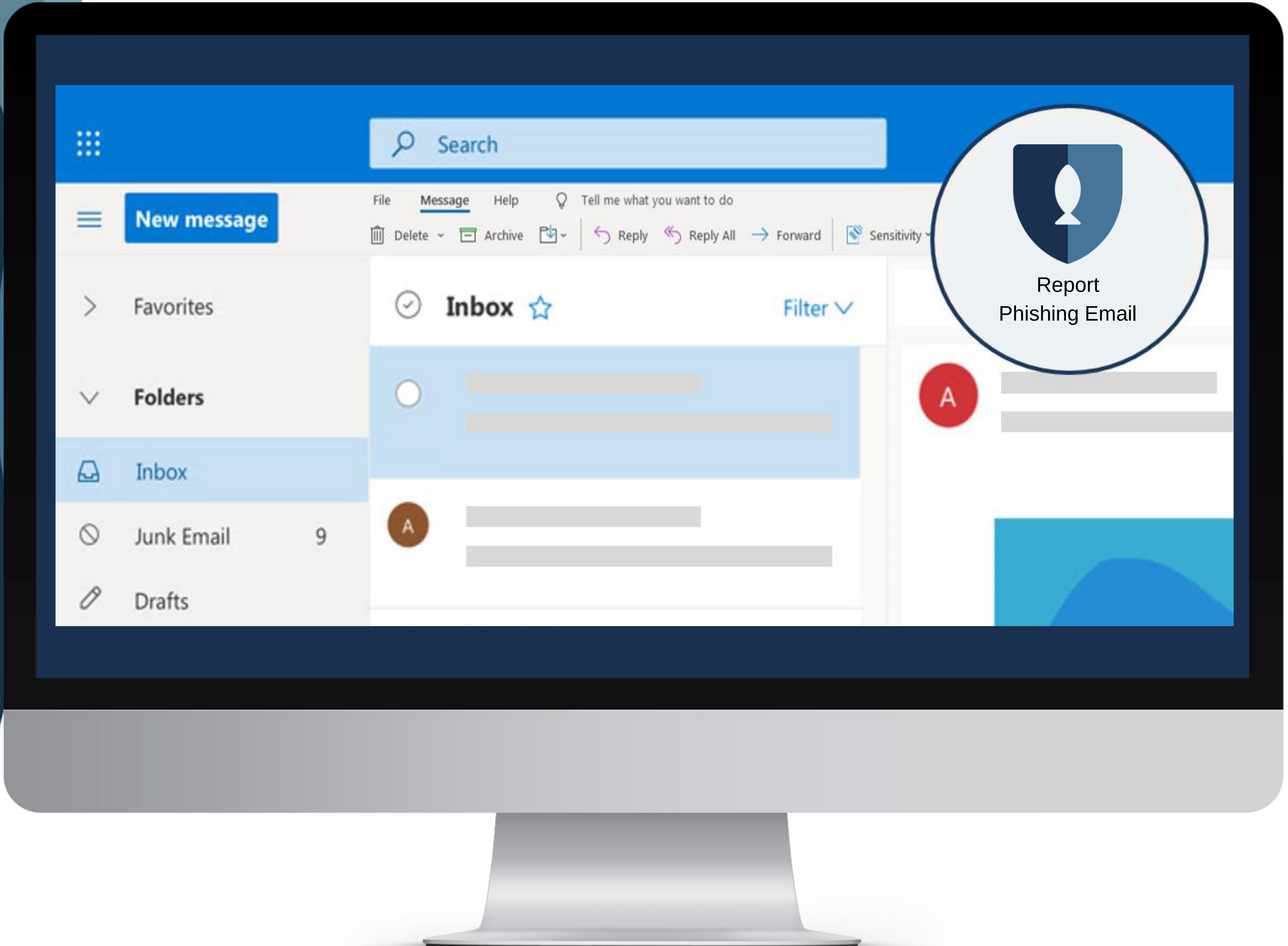
#SeeYourselfInCyber

Phish Reporter

Empower your staff to report phishing emails with one click.

The sooner you know about a phishing attack, the sooner you can do something about it. Phriendly Phishing's Phish Reporter add-in empowers your employees to report suspicious emails with one click for analysis and mitigation.

Customise the message and experience for reported emails

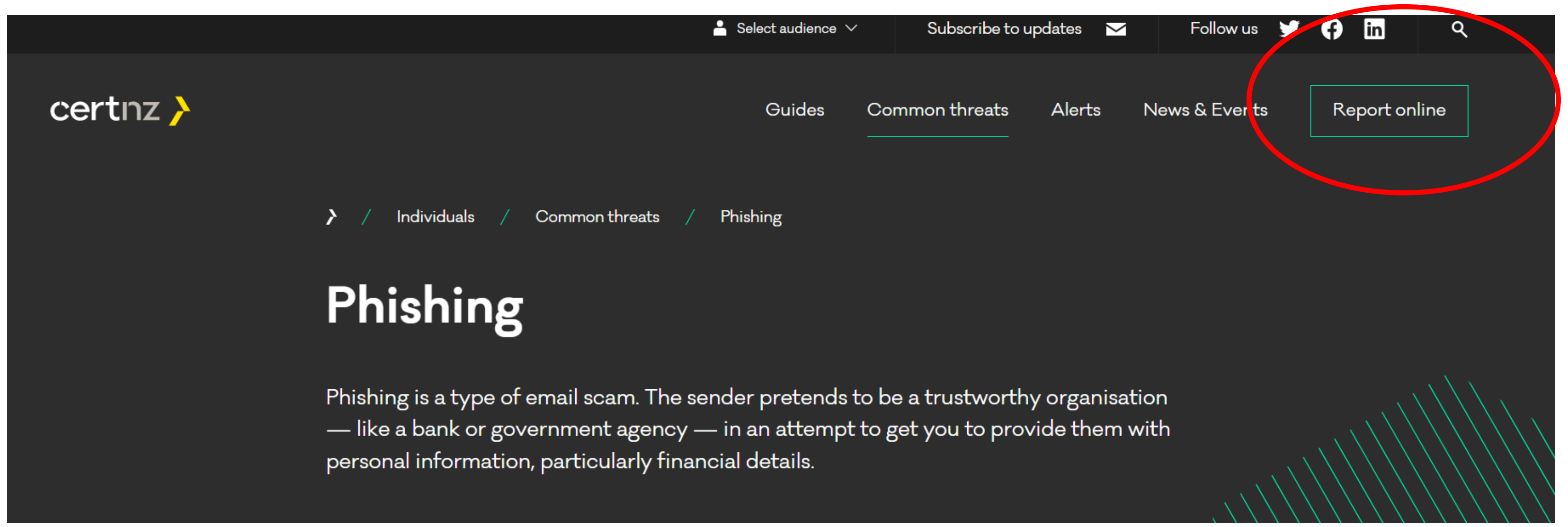


Report SCAMs locally

Other Phriendly Resources for you!

Government support to report phishing and scam

New Zealand - phishpond@ops.cert.govt.nz

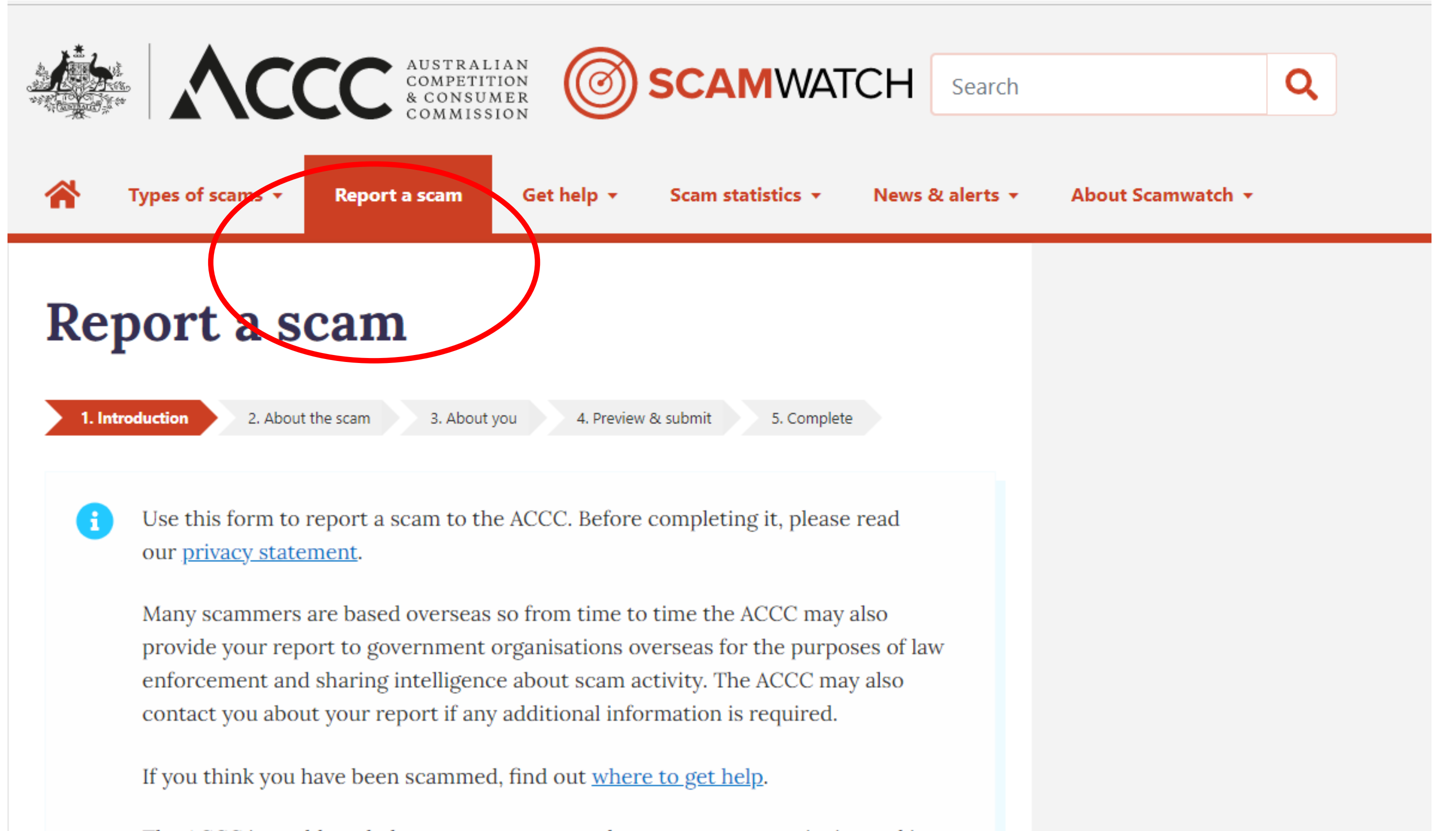


Phishing

Phishing is a type of email scam. The sender pretends to be a trustworthy organisation — like a bank or government agency — in an attempt to get you to provide them with personal information, particularly financial details.

Scan to visit CertNZ website!

Australia



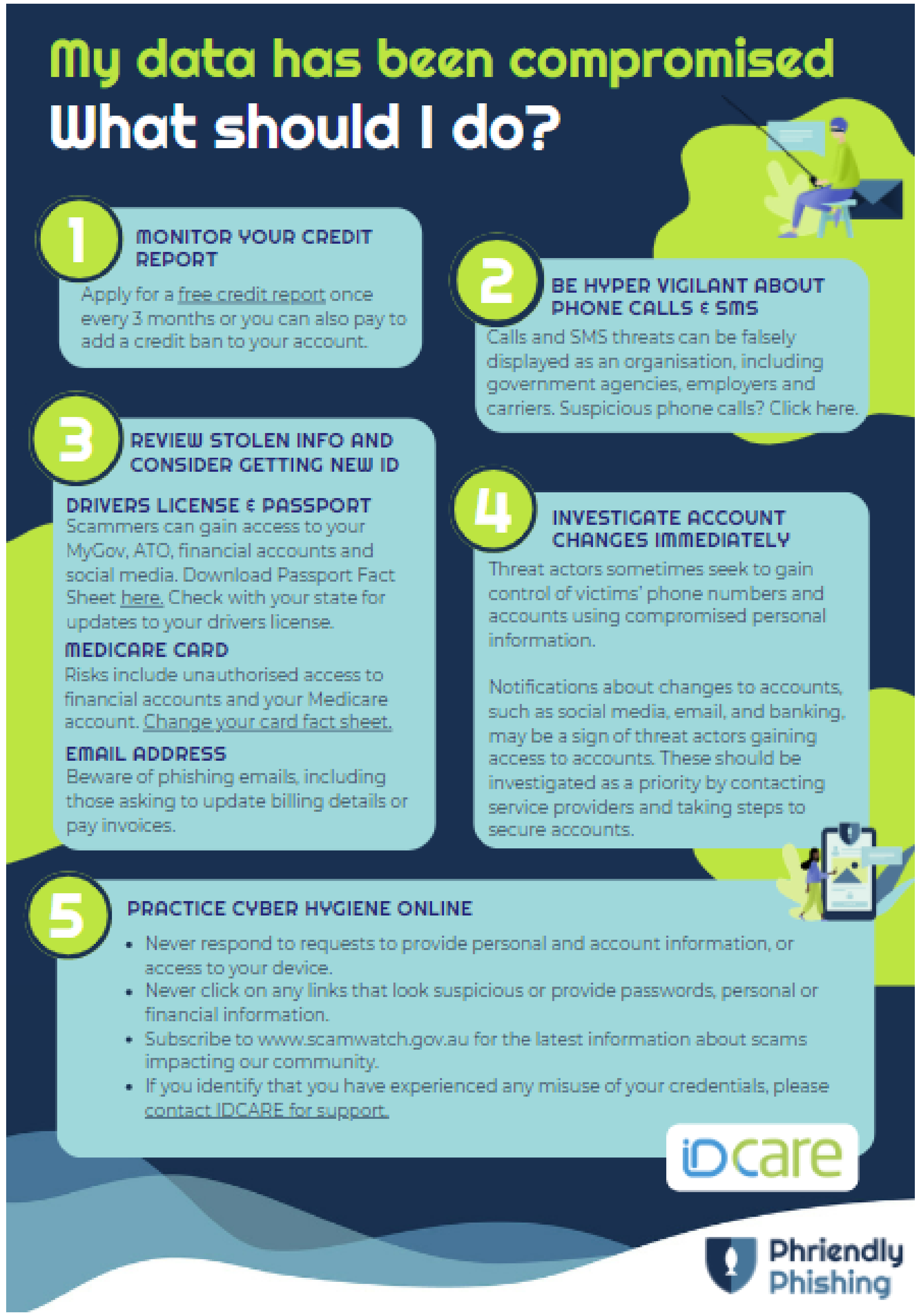
Report a scam

Use this form to report a scam to the ACCC. Before completing it, please read our privacy statement.

Many scammers are based overseas so from time to time the ACCC may also provide your report to government organisations overseas for the purposes of law enforcement and sharing intelligence about scam activity. The ACCC may also contact you about your report if any additional information is required.

If you think you have been scammed, find out where to get help.

Scan to visit Scam Watch website and complete the form



My data has been compromised

What should I do?

1 MONITOR YOUR CREDIT REPORT

Apply for a free credit report once every 3 months or you can also pay to add a credit ban to your account.

2 BE HYPER VIGILANT ABOUT PHONE CALLS & SMS

Calls and SMS threats can be falsely displayed as an organisation, including government agencies, employers and carriers. Suspicious phone calls? Click here.

3 REVIEW STOLEN INFO AND CONSIDER GETTING NEW ID

DRIVERS LICENSE & PASSPORT
Scammers can gain access to your MyGov, ATO, financial accounts and social media. Download Passport Fact Sheet here. Check with your state for updates to your drivers license.

MEDICARE CARD
Risks include unauthorised access to financial accounts and your Medicare account. Change your card fact sheet.

EMAIL ADDRESS
Beware of phishing emails, including those asking to update billing details or pay invoices.

4 INVESTIGATE ACCOUNT CHANGES IMMEDIATELY

Threat actors sometimes seek to gain control of victims' phone numbers and accounts using compromised personal information.

Notifications about changes to accounts, such as social media, email, and banking, may be a sign of threat actors gaining access to accounts. These should be investigated as a priority by contacting service providers and taking steps to secure accounts.

5 PRACTICE CYBER HYGIENE ONLINE

- Never respond to requests to provide personal and account information, or access to your device.
- Never click on any links that look suspicious or provide passwords, personal or financial information.
- Subscribe to www.scamwatch.gov.au for the latest information about scams impacting our community.
- If you identify that you have experienced any misuse of your credentials, please contact IDCARE for support.

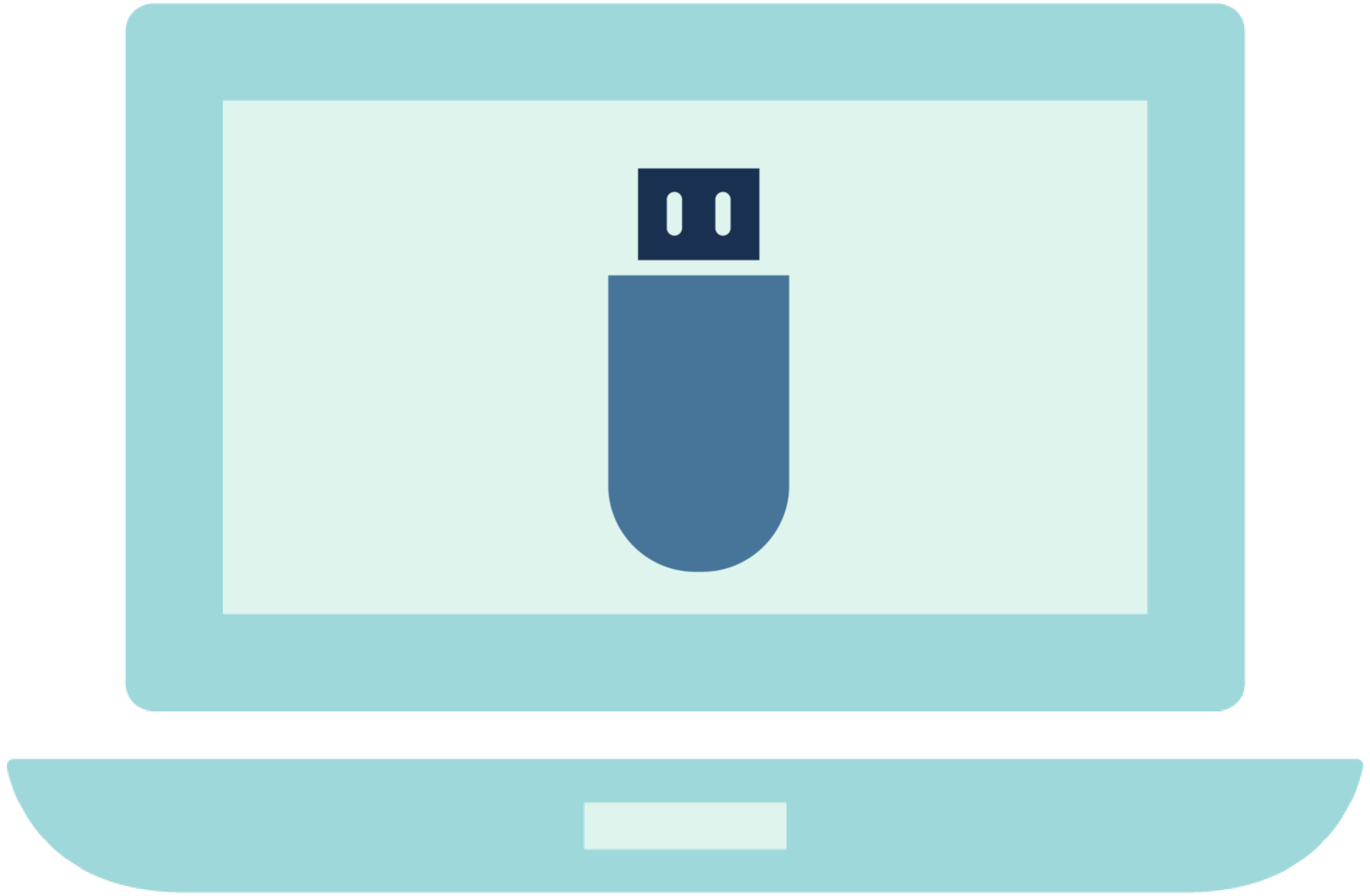
How to get your team talking? USB Drop

Key Features:

- Set up a file on a USB drive to test employees
- The file will be ‘armed’ to provide reporting to Phriendly Phishing

Why it matters:

- Refresh and test your security practices
- Test employees when they’re in the office or any physical work environment



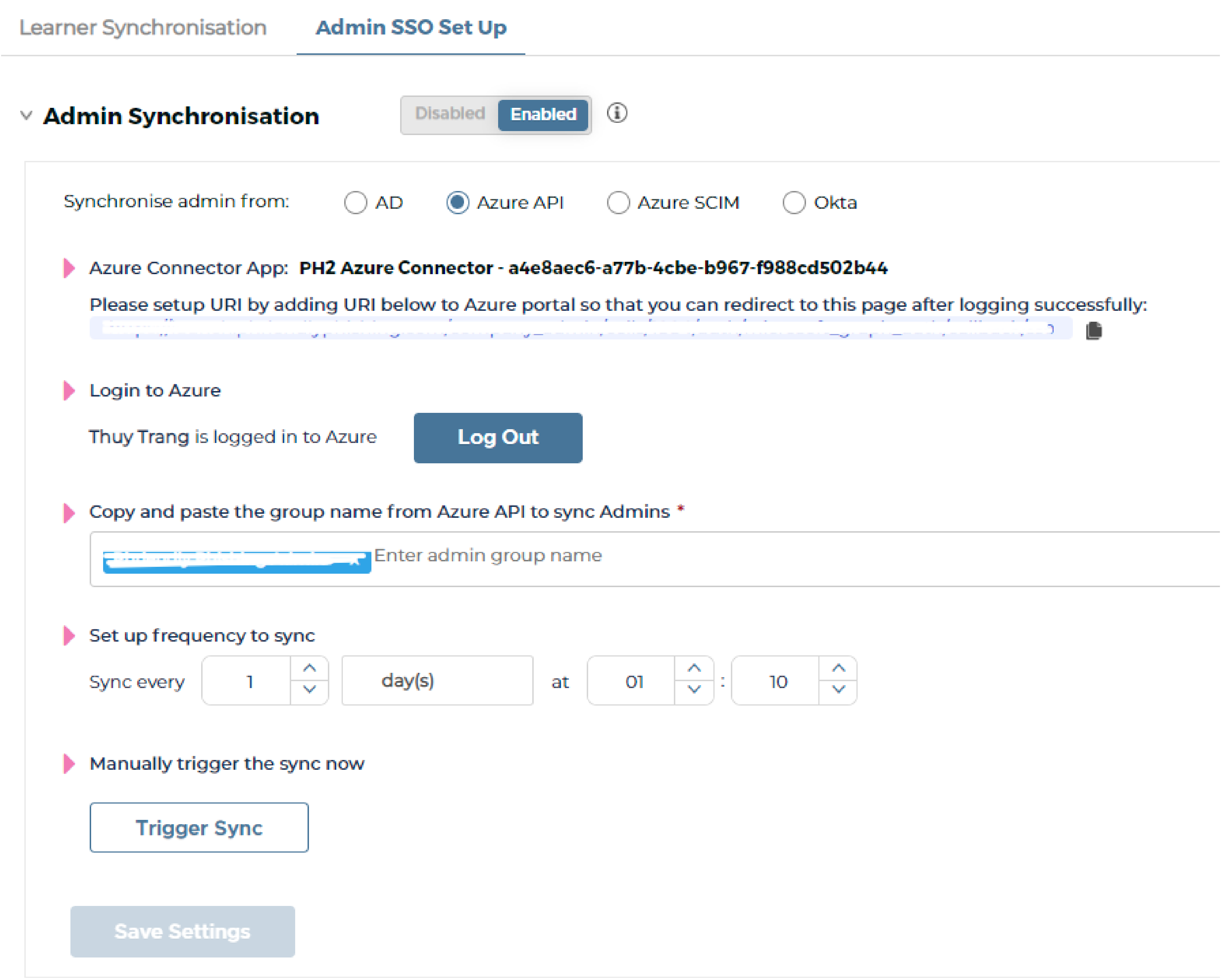
Additional security features

Key Features:

- Enable Single Sign On for admins
- Multi-factor Authentication (MFA)

Why it matters:

- Automate the process and maintain control of company administrators in your account
- Enable a second layer of verification for company admins to login



Admin Synchronisation Disabled **Enabled**

Synchronise admin from: ○ AD ● Azure API ○ Azure SCIM ○ Okta

Azure Connector App: **PH2 Azure Connector - a4e8aec6-a77b-4cbe-b967-f988cd502b44**

Please setup URI by adding URI below to Azure portal so that you can redirect to this page after logging successfully:

[redacted]

Login to Azure

Thuy Trang is logged in to Azure

Copy and paste the group name from Azure API to sync Admins *

[redacted] Enter admin group name

Set up frequency to sync

Sync every 1 day(s) at 01 : 10

Manually trigger the sync now

CONFIDENTIAL

Phriendly
Phishing

Questions?

support@phriendlyphishing.com
help.phriendlyphishing.com