Australian Government

TAX PRACTITIONERS BOARD

Defend yourself against cyber threats

Presented by
Craig Woodburn, TPB Chief Technology Officer

Welcome

'In the spirit of reconciliation, I respectfully acknowledge the Traditional Owners and Custodians of Country throughout Australia and their continuing connection to land, waters and community. I would like to pay my respect to them and their cultures, and Elders past and present'.

Access the presentation slides : **tpb.gov.au/webinar-hub**

What we will cover today

- ✓ The cyber crime environment
- ✓ Top threats
- ✓ Safeguards
- ✓ Reporting an incident
- ✓ Where to get help
- ✓ Q&A

Be cyber aware

- Make cyber security a priority.
- Be aware of the cyber environment and current threats.
- Keep the conversation going.
- Spread the message to make a difference!

Cybercrime environment

$10.5T

Estimated global cost of cyber crime by 2025

(Cyber Security Ventures)

$46,000

Average reported loss for a small business – up 14%

(ASD Cyber Threat report 2022 - 2023)

A cyber report is made **every 6 minutes**

Costs of cybercrime

- Damage and destruction of data
- Stolen money
- Lost productivity and disruption to business
- Theft of intellectual property, personal and financial data
- Fraud
- Forensic investigation
- Restoration and deletion of hacked data and systems
- Reputational harm

! Tax practitioners hold valuable personal information – cyber criminals may target you to commit identity fraud.

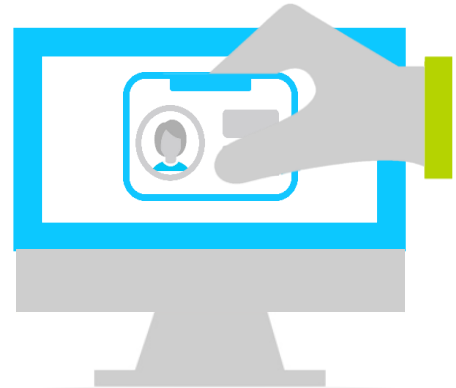
Top cybercrime threats

For individuals:

- Identity theft
- Online banking fraud
- Online shopping fraud

For businesses:

- Email compromise
- Business email compromise
- Online banking fraud



Who are cyber criminals?

Misconceptions about cyber criminals:

- They work alone.
- They're young.
- Are unorganized.
- Only target large corporations and government systems.

What cyber criminals look like:

- Run like a business – are profit driven.
- Can be any age.
- Have diverse methods and motives.
- Pose unique threats to individuals, businesses, and government.

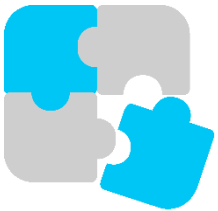
Motives behind cyber-attacks

Financial gain

Disruption

Spamming

Espionage



Fun

!

70% of cyber-attacks are triggered by outsiders and organised crime makes up 55% of these outsider attacks.

Business email compromise

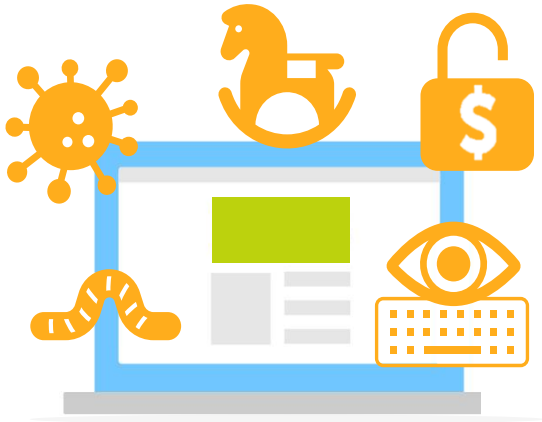
- BEC is where malicious actors compromise an organisation via email.
- Criminals target organisations and try to scam them out of money or goods.
- They also target employees and try to trick them into revealing important or confidential business information.
- Only a small fraction of BEC financial losses are ever recovered.

Phishing attacks

- Fraudulent communications that appear to come from reputable sources.
- Designed to gain access to systems or steal data.
- No single cyber security technology can prevent attacks. Take a layered approach – email and web security, malware protection, user behaviour monitoring, and access control.
- Example: An email pretending to be from your bank with instructions to share your login information.

Malware

- Malware is software cyber criminals use to harm your computer or network to steal information.
- It holds your computer to ransom or installs programs without your knowledge.
- Types of malware include, trojans, viruses and worms, keyloggers and ransomware.
- Example: A malicious program that displays unwanted or intrusive ads on your device or browser, often slowing down the system or redirecting you to malicious websites.

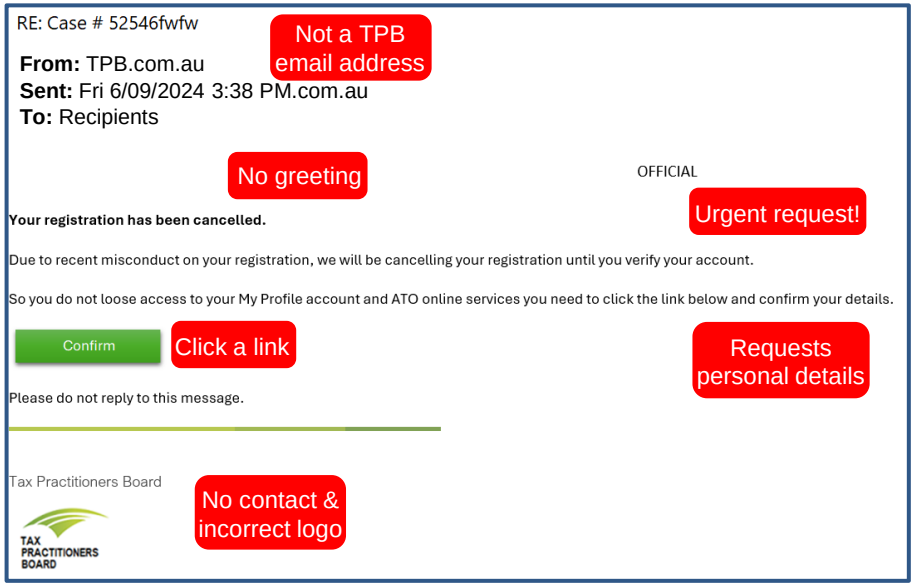


Ransomware

- Software that encrypts your data behind a secret key or passcode.
- Without that code, your data and network are inaccessible.
- Includes a threat, to pay a ransom to get your information unlocked.
- Failure to meet demands will cause them to lock or destroy your information.
- If you are a victim of ransomware contact the ASD on 1300 CYBER1.

How to spot a suspicious email

- Sender's email address does not match the organisation.
- Generically addressed and not personalised.
- Requests personal details.
- Offers a threat or reward.
- Link or button to click on that doesn't match the website.
- No official sign off.



QR codes

We’re sorry service is temporarily unavailable, and your package is on hold. We’re fixing the problem.

Scan the QR code to sign up for status alerts.

Thanks

Everyday tips

- Implement at least Maturity Level One from the Essential Eight.
- Install and maintain anti-virus and antimalware software on your computers.
- Deploy firewalls on your workplace computers and/or networks.
- Ensure your computer operating system and other programs always have the latest security updates. This is critical and so easy!
- Enable multifactor authentication.
- Use passphrases.
- Ensure people only have the access they need to do their jobs.

Everyday tips

- Protect client records or files using encryption.
- Be careful of email attachments, web links and unknown voice callers.
- Do not click on a link or open an attachment you weren’t expecting.
- Use separate personal and business computers, devices, and accounts.
- Don’t download software from an unknown web page.
- Never give out your username or password.
- Consider using a password management app.

The Essential Eight

The Essential Eight protects internet-connected IT networks. The mitigation strategies include:

- ✓ application control
- ✓ patch applications
- ✓ configure Microsoft Office macro settings
- ✓ user application hardening
- ✓ restrict administrative privileges
- ✓ patch operating systems
- ✓ multi-factor authentication
- ✓ regular backups.

Maturity Levels

- The Essential Eight consists of 4 maturity levels – Maturity Level Zero to Maturity Level Three.
- Maturity Level Zero – indicates weaknesses in an organisation's overall cyber security position.
- When exploited, the weaknesses could facilitate the compromise of the confidentiality of data, or the integrity or availability of systems and data.

Maturity Level One

- **Maturity Level One** focuses on malicious actors who leverage commodity tradecraft to gain access to a system.
- Malicious actors could access an internet-facing service using credentials that were stolen, reused, brute forced or guessed.
- They will opportunistically seek common weaknesses in many targets rather than investing in gaining access to a specific target.
- Malicious actors will employ common social engineering techniques to trick users into weakening the security of a system and launch malicious applications.

Maturity Level Two

- Maturity Level Two focuses on malicious actors operating more capability from the previous maturity level.
- These actors will invest more time in a target and in the effectiveness of their tools.
- They will likely employ well-known tradecraft to bypass controls implemented by a target and evade detection.
- They are likely to be more selective in targeting but are still conservative in the time, money and effort they may invest in a target.

Maturity Level Three

- Maturity Level Three focuses on malicious actors who are more adaptive and much less reliant on public tools and techniques.
- These actors exploit opportunities provided by weaknesses in cyber security to extend, evade detection and solidify their presence.
- These malicious actors may be more focused on targets and are willing and able to invest effort into circumventing the technical controls implemented by their targets.
- This includes social engineering a user to not only open a malicious document but also to unknowingly assist in bypassing controls.

Questions

Stay in touch with the TPB

tpb.gov.au

tpb.gov.au/**contact**

Australian enquiries
1300 362 829

Overseas enquiries
+61 2 6216 3443

Our enquiry lines are open
Monday to Friday 9 am to 5 pm
(Sydney time)

facebook.com/**TPB.gov**

linkedin.com/**tax-practitioners-board**

twitter.com/**TPB_gov_au**

youtube.com/**TPBgov**

Disclaimer

The information included in this webinar is intended as a general reference for users. The information does not constitute advice and should not be relied upon as such.

While the Tax Practitioners Board (TPB) makes every reasonable effort to ensure current and accurate information is included in this webinar, the TPB accepts no responsibility for the accuracy or completeness of any material contained in this webinar and recommends that users exercise their own skill and care with respect to its use.

Links to other websites may be referenced in this webinar for convenience and do not constitute endorsement of material on those sites, or any associated organisation, product or service.