Australian Government

TAX PRACTITIONERS BOARD

Cyber security – back to basics

Presented by:
Craig Woodburn, Chief Technology Officer
Tax Practitioners Board

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

- ✓ Why cyber security matters
- ✓ Understanding cyber criminals
- ✓ Relevant Code of Professional Conduct items
- ✓ Types of cyber threats
- ✓ Tips to keep you safe
- ✓ Essential Eight
- ✓ Q&A

What is a cyber-attack?

'A deliberate act through cyberspace to manipulate, disrupt, deny, degrade or destroy computers or networks, or the information that resides on them, with the effect of seriously compromising national security, stability or economic prosperity'.

Why cyber security matters

- Cybersecurity is an important concern for every organisation – regardless of size.
- Cyber-attacks have increased now we're living more of our lives online.
- The average impact from a cyber-attack for a small business is $40,000/incident.
- A cybercrime is reported every 7 minutes.
- The finance industry has one of the highest number of data breaches reported.

Understanding cyber criminals

Motives behind cyber-attacks

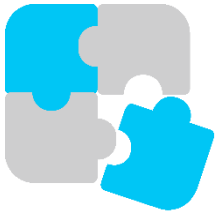
Most cyber-attacks are triggered by outsiders (70%) – organised crime makes up 55% of these outsider attacks.

Financial gain

Disruption

Spamming

Espionage

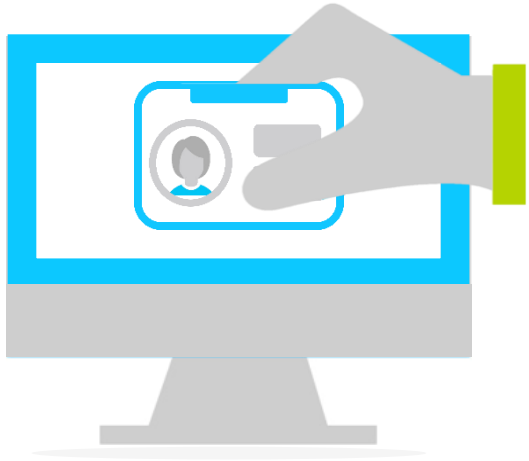


Fun

Cyber-crime

Types of cyber-crime reported in 2020-21:

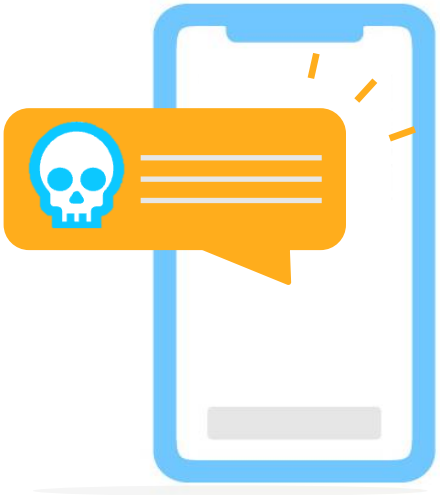
- Fraud related crime-crime – 23%.
- Online shopping scams – 17%.
- Online banking scams – 12%.
- The remaining 48% is spread between identity theft, business email compromise, investment, selling, bulk extortion and romance scams.
- Phishing is the greatest threat.



Financial loses to cyber-crime

Money lost to SMS scams:

- $3 million in 2020
- $8.6 million in 2021.



Code of Professional Conduct

Code item 6

You must not disclose any information relating to a client's affairs to a third party unless you have:

- *obtained the client's permission; or*
- *there is a legal duty to do so.*

Code item 7

You must ensure that a tax practitioner service that you provide, or that is provided on your behalf, is provided competently.

Cyber security threats

Cyber security threats

- Business email compromise
- Phishing Attacks
- Malware
- Ransomware
- Imposter Scams
- Identity theft
- Data breaches
- Hacking

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 a reputable source.
- Designed to gain access to systems or steal data.
- No single cyber security technology can prevent attacks. Take a layered approach such as 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 that cyber criminals use to harm your computer or network to steal your confidential information.
- It holds your computer to ransom or installs other 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.
- Malware includes a threat, often where you must 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 Australian Cyber Security Centre on 1300 CYBER1.

Imposter scams

- Someone ‘official’ calls or emails to report a crisis situation.
- They may say they represent the ATO, a bank, the lottery or technical support.
- There will be a sense of urgency and a penalty or loss if you don’t act
- **Example:** ATO scams – you receive a call claiming to be the ATO, reporting you owe money and need to pay or else get hit with a fine.

Identity theft

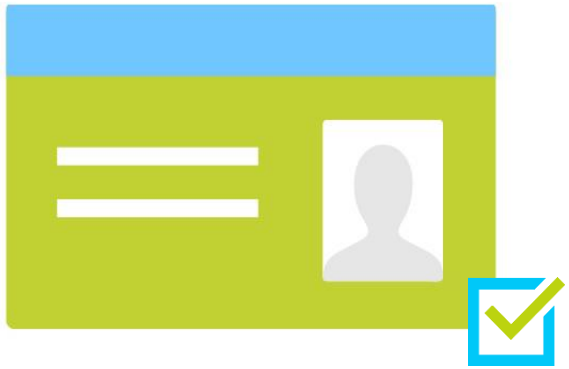
- Identity theft is when a cybercriminal gains access to your personal information to steal money or gain other benefits.
- They can create fake identity documents to get loans and benefits or apply for real identity documents in your name.
- Once your identity has been stolen it can be difficult to recover and you may have problems for years to come.
- A cybercriminal may look to steal a range of personal information.

Protect yourself and your clients

- Cybercriminals can learn a lot about you from your social media accounts.
- Limit what you share online.
- Set your privacy settings to 'private'.
- Don't accept 'friend' requests from strangers.
- Think twice before entering personal details into an unfamiliar website.
- Be careful about what you access over public or untrusted Wi-Fi.

Client verification

- We've developed POI guidelines to help you verify clients' identities and reduce the risk of identity theft.
- The guidelines help you meet your obligations to secure clients' personal and financial details.
- We strongly recommend you do not use email for communicating sensitive information, except where you use an encrypted or password protected attachment.

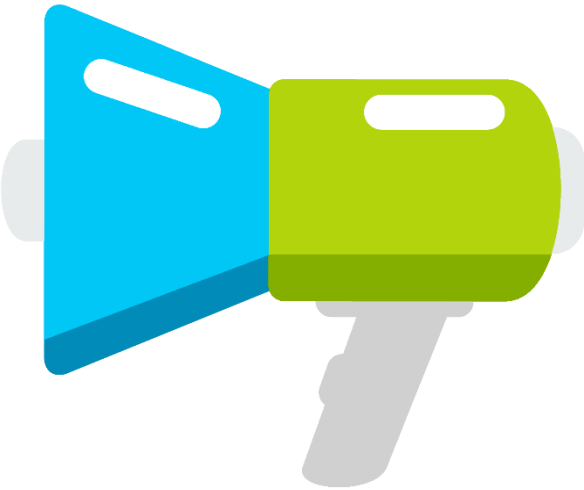


Data breaches

- A data breach is where sensitive or personal information is accessed, disclosed or exposed to unauthorised people.
- Information could also be used in targeted scams and to steal identities.
- **Example:** an email with personal information is sent to the wrong person, or a computer system is hacked and personal information is stolen.

The Notifiable Data Breaches scheme

- Organisations covered by the Privacy Act are legally required to quickly assess actual or suspected data breaches.
- If serious harm is likely to result, you must notify affected individuals.
- You must also notify the Office of the Australian Information Commissioner.



Hacking

- Hacking is an attack on your network or systems, often to exploit.
- Hacker's gain access via the internet or on your own network.
- Once in, a hacker can modify how a network works, steal data, obtain passwords, get credit card information, watch what you are doing or install malware to further the attack.

What should you do if you are hacked?

- Make a record of the key details of the incident – what happened, when it happened, if someone contacted you, and how you responded.
- Disconnect the internet.
- Scan for viruses and remove any malware.
- Change your passwords and passphrases.
- Notifying your clients and other networks to be on the alert for any strange links or email attachments.

Tips

Everyday tips

- Implement at least the Maturity Level One risk mitigations from the Essential Eight.
- Install and maintain anti-virus and antimalware software on your computers. For Windows users – Microsoft Defender detects over 99% of attacks.
- 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.
- Ensure people only have the access they need to do their jobs.

Everyday tips 

- Protect client records or files using encryption and back up at least once a day.
- Be careful of email attachments, web links and voice calls from unknown numbers.
- Do not click on a link or open an attachment that you were not expecting.
- Use separate personal and business computers, mobile devices, and accounts.
- Do not download software from an unknown web page.
- Never give out your username or password.
- Consider using a password management application to store your passwords for you.

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.

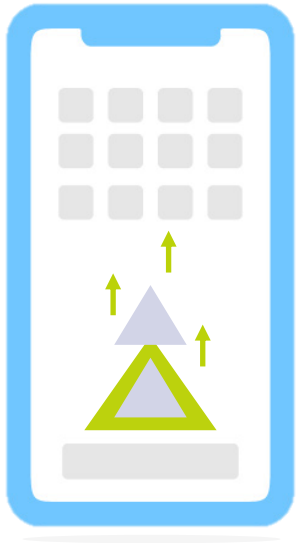
Maturity Levels

The Essential Eight consists of 4 maturity levels:

- **Maturity Level Zero** indicates there are weaknesses in the overall cyber security posture.
- **Maturity Level One** focuses on malicious actors who leverage commodity tradecraft that is widely available in order to gain access to a system.
- **Maturity Level Two** focuses on malicious actors operating more capability from the previous maturity level. These actors will invest more time in a target.
- **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.

Update your devices

- Updates are one of the strongest defences in your security toolkit.
- Updating your device and applications can fix issues and address new security concerns.
- It's important to check for updates regularly.
- Cyber criminals hack devices by using known weaknesses in systems or apps. Updates have security upgrades to fix these weaknesses.



Backup regularly

- If your data is damaged or stolen it can be expensive or even impossible to recover.
- That's why it's important to back-up regularly.
- A backup is a digital copy of information.
- Copies of your files are saved to an external storage device or to an online server, like the Cloud.
- Backing mean you can restore your files if something goes wrong.

Turn on multi-factor authentication

- Turn on MFA wherever possible.
- MFA provides extra checks to prove your identity and an extra layer of security by increasing confidence the person logging in is who they claim to be.
- MFA blocks 99.9% of automated cyber-attacks, 96% of bulk phishing attempts and 76% of targeted attacks.
- Some MFA authentication factors include a physical token, security key, biometrics, authenticator app and SMS, email or voice call.

Set secure passphrases

- Passphrases are more secure then passwords.
- They are made up of random words, making them longer and harder to guess, but easy to remember.
- Changing your passwords to a passphrase is a great way to improve your cyber security.
- When you choose your passphrase, make it long, unpredictable, unique and using a mix of random words.

Recognise and report scams

- Turn on MFA wherever possible.
- MFA provides extra checks to prove your identity and an extra layer of security by increasing confidence the person logging in is who they claim to be.
- MFA blocks 99.9% of automated cyber-attacks, 96% of bulk phishing attempts and 76% of targeted attacks.
- Some MFA authentication factors include a physical token, security key, biometrics, authenticator app and SMS, email or voice call.

Watch out for threats

Top tips to secure your business:

- Turn on multi-factor authentication.
- Use passphrases instead of passwords.
- Manage and limit the use of shared accounts.
- Only provide access to those who need it.
- Update your software.
- Backup for data.
- Use antivirus and ransomware protection.
- Consider additional PI insurance cover.

Questions

Stay in touch

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.