**Cyber Security for Accounting Technicians**

Cyber security is no longer negotiable for accounting professionals; it is something that you must take care of from day one in business. Whether you work as an employee, a solo practitioner or as part of a team, cyber security must be integral to your work.

Cyber attacks are any attempt to expose, alter, disable, destroy, steal or gain unauthorised access to a computer system or anything stored within that system.

Most cyber attacks against commercial entities are launched by cybercriminals for financial gain.

Small businesses are an easy target for cybercriminals as the people in the business are often uneducated about cyber security, and small business has limited financial resources to put towards cyber protection.

The biggest risk to your business, besides the massive financial impact, is the damage to your reputation. If identification details of staff, suppliers and customers are compromised, recovering from that violation can take months or years.

**Sources of Cyber-Attack**

Most cyber-attacks happen because of people – not systems. Educating yourself and your team is the best protection and risk minimisation strategy. Cybercriminals know that it is easier to trick people into giving information than to break through security technology.

For small businesses and accounting professionals, the most common cyber risks are from employees, associates of the business or others known to the business somehow.

Having strong internal controls will minimise or eliminate internal threats.

External sources may be individuals working alone, organised crime groups, hacktivists motivated by ideological reasons, corporate espionage or state-sponsored activity.

Proper cyber protections, hardware and technology will minimise external threats.

**Types of Cyber Incidents**

* Emails or calls from people pretending to be someone else wanting private information.
* Malicious emails or attachments.
* Compromised systems.
* Phishing and spear-phishing scams – tricks to get you to divulge personal information. Spear-phishing targets a specific individual rather than a general attempt.
* Smishing – a message pretending to inform you that you are locked out of an account and have to supply identification to re-access the account.
* Email harvesting, stripping or scanning.
* Software and password hacking.
* Unintentional data leakage because of poor practices.
* Ransomware or malware.
* Denial of service by making systems unavailable because of attack.
* Identity theft.
* Industrial espionage or theft of intellectual property of a business.
* Money laundering using unauthorised accounts to hide transactions.
* Lodging of fraudulent activity statements or tax returns from your login.

**TPB Guidance on Protecting Your Practice from Cyber-Attacks**

The Tax Practitioners Board also provides guidance for tax professionals, and it has a practice note specifically addressing online security: [TPB(PN) 1/2017 Cloud computing and the Code of Professional Conduct](https://www.tpb.gov.au/tpbpn-012017-cloud-computing-and-code-professional-conduct).

The TPB refers to cloud computing as the provision of information technology resources as a service through a network (including storing, managing and processing data), typically over the internet.

Information technology service includes data storage, software programs, applications, databases, email and file services provided as software as a service, platform as a service or infrastructure as a service.

Registered practitioners engage with cloud computing for various purposes, including information storage, lodgement of returns, digital signatures, client portals and practice management software. All of these applications must meet privacy and security guidelines.

The TPB recommends the following controls to assist in maintaining and protecting the confidentiality, integrity and availability of client data:

* An appropriate confidentiality agreement between the registered practitioner and the online service provider.
* Use of a secured website and encrypted network traffic
* Security credentials.
* User access controls ensuring unauthorised people do not have access to data.
* Standard business reporting.
* Audit trails.
* Appropriate segregation of duties.
* Review and approve data changes.

If a registered agent has inadequate cyber security arrangements, this could breach the Code of Professional Conduct.

Any information disclosed to a third party must have the client’s permission. This includes your practice management tools and applications if client data is disclosed.

Client permission must be obtained before sharing client data with a third party, either as general permission in the letter of engagement or specific permission if needed for new online service providers.

**ATO Security Advice for Tax Professionals**

The Australian Taxation Office recommends that you review your security systems and procedures regularly.

* Check the proof of identity for all new clients.
* Only lodge forms for clients whose identity you have verified.
* Ensure your computer systems are up to date and protected against cyber-attacks.
* Discuss the importance of cyber security with staff and provide training.
* Ensure staff understand what is appropriate to share on social media or via email.
* Immediately report unknown access to your myGovID.
* Immediately report data breaches.
* Report suspected fraud, identity theft or criminal activity.
* Secure your physical business premises and all identifiable information appropriately.
* Secure your computers, applications, passwords and any other devices and systems used to access client information.

**Data Breach Guidelines for Tax Professionals**

Data breaches occur when any unauthorised party has accessed confidential taxpayer information.

ATO examples of data breaches include:

* unauthorised removal of computers, data, or records in both paper and digital formats
* people with legitimate access to the data using it for fraudulent means
* accessing taxpayer files using a fraudulently obtained credential, such as myGovID
* criminals exploiting vulnerabilities in your IT security controls, hacking or phishing for information
* accidental disclosure of information – for example, records emailed to an unauthorised third party or hard copies left in a public place
* payroll information for your employees being unlawfully accessed
* unauthorised access to cloud-based accounting software you use to store information.

In the event of a breach:

* Contact the ATO.
* Inform staff and clients as soon as possible about a data breach.
* Contact relevant software providers if you suspect the breach has originated from them.
* Review what information was compromised.
* Take immediate steps to secure information, such as updating passwords, operating systems or software versions and increasing security settings.
* Review user access and remove or limit anyone who no longer requires it or has higher than necessary permissions.

**Steps to Cyber Security**

You can quickly implement many simple measures to increase your cyber security.

* Update your devices' operating systems and software whenever new updates are available. The most common reason for updates is security. Set all applications to update automatically. Legacy systems that are no longer supported or patched pose a more significant risk.
* As soon as you encounter an operating system update that cannot be performed on outdated hardware, upgrade your device.
* Use firewalls on workplace computers and networks.
* Perform both local physical backups of computers and secure online backups. Use a secure and trustworthy digital solution to schedule automatic backups.
* Back up your website. Cybercriminals attack websites to use them as fronts for communications. Either monitor comments before approving them on your website or disable them altogether.
* Electronic record keeping must follow the same principles as physical document security and be backed up in a separate location.
* Use a password protector. There is no excuse for not protecting passwords that allow access to clients' financial or personal data. Never reuse or share passwords. Instead, use complex or randomly generated passwords.
* Use anti-malware and anti-virus software on all devices.
* Use the highest security settings available for accessing your devices.
* Use a trusted Virtual Private Network (VPN) service to provide security while using public wi-fi connections.
* Use two-factor authentication on every application that supports it.
* Use authenticated digital signatures to avoid forgery.
* Use a secure email gateway provider to prevent spam and malicious emails from reaching you.
* Keep track of who has access to what systems and at what level of access. As soon as staff leave, remove access. Give staff the minimum level of access needed to do the job and not more.

**Password Hackability**

Having excellent passwords is still one of the essential protections in your cyber security plan.

But what constitutes an un-hackable password?

Brute force digital systems keep getting better and faster at cracking passwords.

Even long passwords that only contain letters or numbers can be hacked relatively quickly. It’s not until you use a mixture of upper and lower case letters, numbers and special characters that a password becomes really secure.

For example, hackers can crack a password of nine upper and lower case letters in an hour. If you add numbers and symbols, the password will take two days to hack.

A 12-character password of numbers only can be hacked instantly. But a password of 12 upper and lower case letters will take 24 years. If you include letters and symbols, that 24-character password would currently take 3,000 years to hack.

Passphrases made up of specific words in a phrase are also very secure if there are enough characters.

**Your Password Protocol**

* Review passwords for all systems that may access your own sensitive information or clients' data.
* Attend to any duplicated passwords immediately – never use the same password for multiple sites or accounts.
* Make your passwords long enough and complex enough to repel hackers.
* Use a password manager such as [LastPass](https://www.lastpass.com/) or [1Password](https://1password.com/), so you only have to remember one master password.

Check this article for a great chart on the hackability of different types of passwords: [TechRepublic – How an 8-character password could be cracked in less than an hour](https://www.techrepublic.com/article/how-an-8-character-password-could-be-cracked-in-less-than-an-hour/#:~:text=An%2018%2Dcharacter%20password%20with,2%20million%20years%20to%20crack.).

[AAT Tech Talks – Cyber Security for Accounting Technicians](https://www.aat.org.au/AAT/Member_Resources/Tech_Talk_Webinars/AAT/Member_Resources/Tech_Talks.aspx?hkey=ca4fbc21-bd92-434e-93ab-dd75ff74439c)