Australian Government
Australian Taxation Office

Top cyber security tips for business

It is important you keep all your business and client information secure. If your data is lost or compromised, it can be very difficult or very costly to recover.

We developed these tips in consultation with the Cyber Security Working Group (CSWG), a group of tax practitioner industry groups and other industry partners, such as software developer associations, who are working with us to combat the growing threat of identity theft and cybercrime.

See also:

- How to protect your business (/General/Online-services/Identity-security/Protecting-your-information/How-to-protect-your-business/)

Ensure your passwords are strong and secure

Use multi-factor authentication where possible. Regularly change passwords, and do not share them.

Multi-factor authentication requires users to provide multiple pieces of information to authenticate themselves – for example, a text message sent to your phone when logging into a website.

As a business owner, remember:

- multi-factor authentication puts an additional layer of security on your accounts – it can make it harder for others to access your account
- strong passwords with a mix of upper and lower case letters, numbers, and symbols are harder to hack.

Remove system access from people who no longer need it

Immediately remove access for people who:

- no longer work for your business
- changed positions and no longer require access.

Unauthorised access to systems by past employees is a common cause of identity security or fraud issues for businesses.

Ensure all devices have the latest available security updates

Run weekly anti-virus and malware scans and have up to date security software.

Instances of malicious software (malware) are increasing. It can be easy to accidently click on an email or website link which can infect your computer.

In some instances, your device may be impacted by ransomware. Ransomware can:

- lock your computer until you pay a fee to criminals
- install software which provides access to your bank accounts, allowing criminals to steal your business's money.

Do not use USBs or external hard drives from an unfamiliar source

USBs and external hard drives may contain malware, which can infect your business computers without you noticing.

It can cost your business a lot of money to repair the damage.

Stolen information could be used to commit crimes, often in your business's name.

Use a spam filter on your email account

Do not open any unsolicited messages.

Be wary of downloading attachments or opening email links you receive, even if they are from a person or business you know. They can infect your computer with malware and lead to your business or client information being used to commit fraud.

Spam emails can be embedded with malware and can be used to trick you into:

- providing information
- paying fraudulent invoices
- buying non-legitimate goods

Secure your wireless network and be careful when using public wireless networks

Avoid making online transactions while using public or complimentary wi-fi.

Not all wi-fi access points are secure. By making online transactions (such as online banking) on an unsecure network, you can put your information and money at risk.

Be vigilant about what you share on social media

Keep your personal information private and be aware of who you are interacting with.

Many businesses now have a social media presence. Much like your personal profile, you should consider what information you share.

Scammers are able to take information you publicly display and impersonate you or your business. Impersonators may send emails to trick your staff into providing valuable information or releasing funds.

Monitor your accounts for unusual activity or transactions

Check your accounts (including bank accounts, digital portals and social media) for transactions or interactions you did not make, or content you did not post.

If an organisation you deal with sends you an email alerting you to unexpected changes on your account, do not:

- click on included hyperlinks
- log on to the organisation's website.

You should immediately:

- check those accounts
- contact the organisation by phone.

Use a PO Box, or ensure your mail is secure

Ensure your mail is secure and consider using a secure PO Box.

Mail theft is a leading cause of information security breaches.

Do not download programs or open attachments unless you know the program is legitimate

Some programs contain malware that can infect your computer (including ransomware which locks your files until you pay a criminal), or be used to harvest your sensitive personal and business information.

Be sure you are downloading authorised and legitimate programs.

Do not leave your information unattended – secure your electronic devices

Secure your electronic devices wherever you are.

Your information can be stolen in an instant. In some situations, you won't even know was stolen. Make sure you:

- do not leave your information unattended
- secure your electronic devices (such as phones or tablets) with passcodes.
- securely store portable storage devices (such as thumb and hard drives) when not in use.

Disclaimer

This publication was authored by the Cyber Security Working Group – a consultative forum comprising the ATO and professional associations.

It was published on [Date], for distribution by the professional associations to their members.

This publication is a general reference only. It is not a substitute for independent professional advice. You should obtain appropriate professional advice for your particular circumstances.

Links to external websites or publications are provided for your convenience. They do not constitute endorsement of material on those sites or in those publications.

The Cyber Security Working Group and its constituent associations do not accept responsibility or liability for any loss or damage incurred as a result or in connection with the use or distribution of this material or this publication.

Last modified: 23 Nov 2016 QC 50563

Our commitment to you

We are committed to providing you with accurate, consistent and clear information to help you understand your rights and entitlements and meet your obligations.

If you follow our information and it turns out to be incorrect, or it is misleading and you make a mistake as a result, we will take that into account when determining what action, if any, we should take.

Some of the information on this website applies to a specific financial year. This is clearly marked. Make sure you have the information for the right year before making decisions based on that information.

If you feel that our information does not fully cover your circumstances, or you are unsure how it applies to you, contact us or seek professional advice.

Copyright notice