

# CYBERCRIME IS BIG BUSINESS ARE YOU SAFE?

**Cybercriminals target businesses of all sizes, stealing information to commit identity theft, fraud and other crimes. The consequences of this can be devastating.**

## **Take these simple steps to protect your business from cybercrime.**

### **1. Know how to spot email scams**

Email scams cost Australian businesses more than \$60 million in lost revenue and time in 2018.

#### **Encourage staff to be aware of suspicious emails, including:**

- An email or invoice with new bank account details for a supplier
- Unexpected emails (e.g. an invoice from a supplier you haven't dealt with recently or for an unexpected amount)
- An email asking for urgent payment or threatening serious consequences
- An email from someone who wouldn't normally send payment requests
- An email address that doesn't look quite right (check previous emails)

If your staff see any of these signs, call the company using a phone number from the company's website (not the number listed in the suspicious email).

It's also worth setting up a process in your business to double-check requests for payment and sensitive information to help protect your business from scams.

## 2. Create strong password security

60% of hacking-related data breaches involve stolen or compromised credentials like passwords.

Weak passwords, like Password1, or names, are easy for cybercriminals to guess – there's even software that can guess billions of passwords a second. It's important not to use the same or very similar passwords across multiple business accounts, such as banking, email and social media, because if a cybercriminal cracks just one of them, they could get access to all these accounts.

To keep your accounts secure:

- **Create different passwords across all your online accounts.** This includes email, payroll, accounting software and admin accounts for your website and social channels.
- **Create strong passwords.** Develop a long passphrase made up of at least four words and at least 13 characters in length, such as 'horsecupstarshoe'. Pick words that are meaningful to you so you can remember the password
- **Turn on a second layer of security.** This is also known as two-factor authentication. It means you need to provide two things – your password and something else like a code sent to your mobile device, a physical token or a fingerprint – before you can access your accounts

Use the website [haveibeenpwned.com](http://haveibeenpwned.com) to see if your email addresses have been compromised. If so, take immediate action by changing your password (including on accounts using the same or similar password).

## 3. Keep business information private

59% of Australian organisations have their business interrupted by a cyber breach every month.

Do you know who has access to your business and customer information? It's important to limit access to only those who need it to do their jobs. This will reduce the risk of accidentally or maliciously releasing confidential information.

Also make sure your staff understand their role in keeping customer and employee information confidential. This includes not disclosing the information online, on social media or to people who don't need or shouldn't have it.

Visit the Office of the Australian Information Commissioner's website – [oaic.gov.au](http://oaic.gov.au) – for more information about how to train your staff on their privacy obligations.

Check out our interactive tools to help you and your staff reverse the threat of cybercrime to your business, by heading to:  
**[staysmartonline.gov.au/reversethethreat](http://staysmartonline.gov.au/reversethethreat)**



Follow us on  
Facebook  
**[fb.com/staysmartonline](https://fb.com/staysmartonline)**



Sign up to our free alerts  
**[staysmartonline.gov.au/alert-service](http://staysmartonline.gov.au/alert-service)**

# REVERSE THE THREAT

**Together we can reverse the threat of cybercrime.**  
**[staysmartonline.gov.au/reversethethreat](http://staysmartonline.gov.au/reversethethreat)**