



Boost your cyber security

Help to build a culture of cyber
safety in the property sector

**Small business cyber security guide
for real estate agents, conveyancers
and the property sector**

An initiative of



cyberwardens.com.au

Cyber criminals are on the real estate sector

Australia's real estate and property sector is one of our largest industries and a growing target for cyber criminals.

With large financial transactions and substantial amounts of personal information collected, the real estate and property sector is a top target for cyber criminals, placing small agencies right in their target sights.

Data breaches and financial scams can wreak havoc on small business owners, their staff and clients. Reputational damage and financial loss are real possibilities, let alone the mental anguish and stress of managing a cyber attack.

With deep connections to local communities, 99 per cent of Australia's 47,000 real estate practitioners and agencies are small businesses. It's a common and dangerous misconception to consider your small agency too small for cyber criminals to target.

The average cyber attack will cost a small business \$56,600 according to the ACSC. The large transactions involved in real estate and property mean that figure could quickly escalate in the event of an attack.

This Cyber Wardens guide will help small businesses across the property sector learn about the threats and take the steps to protect themselves and their clients.

The guide includes:

- The most common small business cyber attacks
- Sensitive data and what to be mindful of
- Top 6 things to look out for and what to do
- Key research findings and a cyber security checklist

Most successful attacks will target your team, or involve human error. Our research shows businesses that regularly talk about cyber safety with their whole team are more cyber resilient.

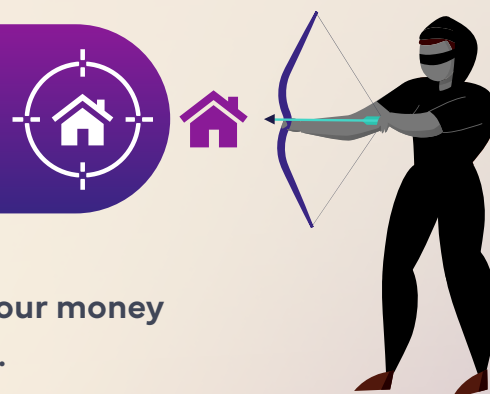
Encourage your team to start the financial year to improve their cyber security to ensure the digital doors to your business are closed. Distribute this guide to your team and encourage your team to start today by enrolling in the free and fast Cyber Wardens training.



Luke Achterstraat
COSBOA Chief Executive Officer



Real estate industry is a top target for crime



Scammers are usually after either your identity or your money - and the property sector can easily give them both.

1 in 6 (17.8%¹)

real estate professionals had been impacted by scams or fraud **equal 3rd of all industries**

1 in 4 (24.6%)

property professionals had suffered a cyber security attack **6th of all industries**

Top 3

business issue reported **for REIA Members²**

Recent attacks and scams on real estate businesses in Australia

Over the past few years, there have been numerous reports in the media and online of cyber attacks, data breaches and scams in the industry. Some have included branches of well-known companies, others have been caused by scams or hacks on staff, and others have included third-party suppliers. Here is a selection of them:



Phone phishing scam

Real estate agent fell victim to a phone scam, resulting in a staggering loss of over \$300,000.



Ransomware

Ransomware gang claimed to have taken employee and customer data, including passport scans, credit card details, and loan data.



Inbox break-in

Staff member's email was hacked, with months of data stolen and fake emails sent.



Mortgage deposit scam

Compromised broker emails, identity theft combined with fake invoices led to Qld couple transferring \$102,000 deposit to a scam trust account.



Tenancy scam

Tenancy application information collected via an agent's website was made public.



Data breach

Another data breach potentially exposed personal details such as photo identification, phone numbers, addresses, signatures and bank details to hackers.



The Real Estate Institute of Australia understands the need for a cultural shift to combat the growing risk to businesses, client data and the reputation of the industry.

“As an industry we recognise more needs to be done in relation to cyber security and that an ongoing way of working needs to be established within the real estate workforce, so cyber security is ‘everyone’s responsibility’.

REIA submission to the 2023 Cyber Security Strategy Discussion Paper

¹ ABS, Characteristics of Australian Business, 22/06/2023

² CYBER SECURITY AT FOREFRONT OF INDUSTRY CONCERNS, Real Estate Institute of Australia (REIA), 27/04/2023

Protecting sensitive data and knowing your obligations

The information normally required in real estate and property transactions to prove a person's identity and assess real estate applications is the same sensitive data targeted by cyber criminals.

Any information that would assist to reasonably identify a person is considered personal information or sensitive data.

Cyber criminals can use the sensitive data they collect to launch impersonation scams or socially engineered cyber attacks.

Businesses need to be aware of the aggregated value of many individual pieces of data, the regulatory obligations, as well as the financial and reputational risk of data theft and system hacks.



Types of sensitive data



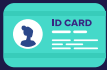
Personal Identification Information (PII)

- Name, email, phone number and current and former addresses;
- Proof of identity documents and bank statements collected by agents from potential buyers and tenants.



Financial Information

- Personal account details (Name, BSB, Account number)
- Previous income and bank statements and how you share your business bank or trust account details.

					
Medicare card	Passport	Licence	Income / Bank Statements	Identity documents	Address

How cyber criminals target the property sector



Data harvesting from
fake contact forms



Payment
redirections



Ransomware



Data breach and theft of personal
data from tenancy or purchases



Fake property
listings

Point of collection

All businesses and staff need to be vigilant around protecting data, including at the point of collection, whether via email, text message, your website or in person.

For example, PPI is collected at open viewings for a property sale or rental.

If you are collecting PPI on paper, you must ensure it is not visible to others looking at the property, who could easily take a photo of the information.

Everyone involved in the real estate sector should be asking themselves questions like:



- ? What data do we collect, and do we need to collect it all?
- ? How is it stored, and is the data backed up?
- ? Who can access it, and is it secure on all current and old devices?
- ? How is the data protected, and how responsive are we to new cyber threats?
- ? How long do we need to keep it, and are we safely deleting it once we no longer need it?
- ? Are we using the data for the initial purpose we collected it?
- ? What processes do we have when people leave the business?
- ? If there is an incident, who will report it promptly?



The Cyber Wardens free training helps identify and eradicate bad habits that make protecting important data less secure, and there is a suite of useful resources on cyberwardens.com.au

The Australian Signals Directorate also has great resources—such as [Ten Things to Know About Data Security](#).

Your legislative and regulatory obligations

Customer data that your organisation produces or collects is likely to be subject to archival, financial, privacy or taxation requirements, such as protection under the [Privacy Act 1988](#), including the Australian Privacy Principles. Please note that significant reform the Privacy Act is expected in late 2024.

In the event of a cyber security incident, regulatory obligations under the [Notifiable Data Breach Scheme](#) will also likely apply, which require you to notify the Office of the Australian Information Commissioner (OAIC) and affected individuals when an eligible data breach has occurred.

See the [OAIC small business checklist](#) and understand your requirements for utilising data for marketing purposes. The Real Estate Institute of Australia and their state and territory affiliates have good resources to help guide you.

Independent legal advice should be sought on any legislative and regulatory obligations that may apply.



Beware of secondary attacks!

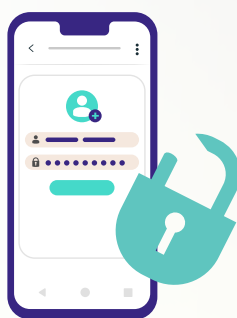
Have you or a staff or family member had their data stolen in a previous cyber-attack?

Information stolen in previous attacks can be used to launch secondary attacks that target your business, especially if passwords are being re-used. This type of attack is called credential stuffing. You can learn more about it, and other cyber safety tips in our [Resources Hub](#).

CREDENTIAL STUFFING SCAMS



Previously stolen
passwords
and user names



Tests your stolen
passwords on other
devices and systems,
including social media.



Report Cyber Crime

Every six minutes a cyber crime is reported in Australia.

If you have been the victim of a cyber attack, make sure you report it - cyber.gov.au/report-and-recover/report

This will help to protect other small businesses.

Top 6 things to look out for and what to do

While the online ecosystem presents opportunities for small businesses to innovate and grow, it also elevates the risk of a cyber hack or a scam.

Here are 6 things to look out for and what to do.

1.

Hackers will exploit poor processes and weak passwords

Your business email inbox and stored data give access to so much valuable business and client information. Unsafe cyber habits make you vulnerable to cyber attacks.

What to do:

- Protect your email and business accounts with multi-factor authentication.
- Set your apps, plug-ins and browsers to auto-update so you have the latest security updates.
- Shut down and restart regularly so your auto-updates are installed.
- Upgrade from passwords to longer passphrases on all logins, including cloud-based storage.
- Set a unique passphrase for every account (no double-ups and no shared passwords).
- Use a password manager to safely store passwords.

2.

Scammers will take advantage of how busy you are

It's harder to spot a scam, fake invoice or phishing attack when you're flat out. Scammers target busy times of the week and create a sense of urgency to manipulate you and your decisions.

What to do:

- Be careful whenever someone insists that you must act immediately, come back to it when you have more time.
- Stick to your usual banking and payment processes.
- Watch for red flags such as a strangely configured email address, unusual requests, unexpected invoices, "confidential" requests or unsophisticated language and typos.
- Be alert to urgent requests pressuring you to transfer funds.

3.

Cyber criminals will send you fake invoices or fake bank transfer details

Watch out for fake invoices, fake refund requests, and fake customer or supplier complaints.

What to do:

- Slow down and double-check every invoice and ensure they match previous ones.
- Ensure the business and bank details are legitimate.
- Check email links before clicking, and don't click links in text messages or on social media messages unless you are sure.
- Don't click on unusual file types and photos as the link may contain computer viruses or phishing attacks.

4.

Scammers will try to access your computer, phones and old devices

You lock your business and don't leave the keys in your vehicle, so don't leave your digital doors open. Be careful who accesses your computers, tablets, phones and operating systems. A breach could result in regulator fines or legal action if customers or employee personal information is accessed.

What to do:

- Ensure the refund request is legitimate. Only trust your regular supplier or a business you can verify.
- If you're contacted and offered technical support or if you put out a call for technical help, be aware that not everyone who offers you assistance will be genuine.
- Never give out sensitive details to unverified providers.
- Never allow remote access to your devices if you have been contacted unexpectedly.
- Be careful when disposing of your devices and old equipment. Ensure the protection of your data by performing a factory reset on your old devices.

5.

Scammers look for website weaknesses to access sensitive information

Your website is important to your business but it can also be an easy target to hack into your data.

What to do:

- Make sure your website starts with https:// (your domain). HTTPS is encrypted in order to increase security of data transfer.
- Set up auto-renewal for your website's domain name.
- Don't share password logins between staff, ensure strong passwords, use a password manager, and ensure all staff have activated multi-factor authentication.
- Regularly update your website's content management systems and plugins.
- Back up your website regularly so you can restore it if you are the victim of a cyber attack.
- If an external party manages or develops your website, speak with them about ways to improve your website security and make sure they are implementing the latest security updates.

6.

Scammers can target your staff and family to break into your business

Cyber security needs everyone pitching in — everyone involved with your business can be a target, and everyone has a role to play in spotting and stopping attacks.

What to do:

- Talk to your family and workers about the heightened risk of cyber attacks on small businesses.
- Remind them to double-check anything suspicious and confirm invoice details directly with suppliers using a trusted contact number.
- If workers are being pressured to pay an invoice they don't recognise or have assumed is for the business owner or another colleague, tell them it's okay to think twice and check with you.

In the market for real estate?

Securing suitable commercial real estate is an exciting step for any small business. As you navigate the search and move towards either renting or purchasing the property, be alert to the threat of cyber attacks.

3 real scams to watch out for



1.

Fake rental scams

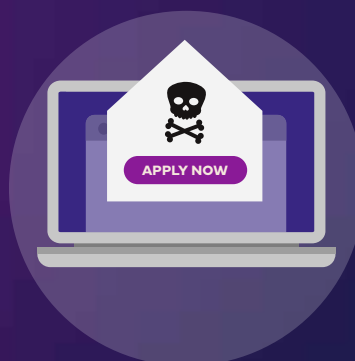
Fake rental property advertisements aiming to sign tenants without visiting the property.



2.

Sales listing scams

Scammers create a fake listing for a property that either doesn't exist or isn't for sale, aiming to collect contact details and personal information of interested buyers or to pressure them to hand over money.



3.

Fake invoices and payment redirection scams

Scammers break into the inbox of real estate agency, lawyers and conveyancers to provide fake invoices in order to redirect payments



Tips

- ✓ Always view property in person before signing an agreement or sending money no matter the competition.
- ✓ Beware of refusals or excuses as to why the property can't be viewed.
- ✓ Search the property on other real estate websites to verify details.
- ✓ Confirm the real estate agent is who they claim to be.
- ✓ Always use a verified trust account to make payments, not a personal bank account.
- ✓ Confirm trust account details with a known person.

Topline findings from the latest Cyber Wardens Research

Almost 2,100 small businesses participated in our latest research from late 2023 and early 2024. Here are some of the findings.

4 in 10 small businesses have little to no confidence in their ability to:



Prepare for a cyber incident



Get help when an incident occurs



Fight a cyber incident



Recover from a cyber incident

Small businesses need to talk more about cyber security

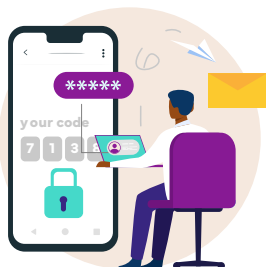
Cyber Wardens research found that small businesses that have a strong cyber security culture are more ready and resilient to cyber attacks. This includes having regular cyber safety conversations with staff.

However, most small businesses (61%) don't talk about cyber security regularly as part of their day-to-day operations, which further increases the risk they face.



Gaps in basic cyber safety create significant vulnerability

Simple cyber-safety strategies include; ensuring each account is protected with a virtual alarm via multi-factor authentication, up-to-date software, and strong password practices.



50%

of small businesses have turned on a **virtual alarm** using **multi-factor authentication**



52%

of small businesses are able to defend against digital break-ins with **up-to-date software**



53%

of small businesses are **backing up** daily and would be ready to recover from attack



30%

of small businesses have **strong password practices**

Bad habits can be the end of your business

Four in five small business owners (78%) have everyday habits which make them more vulnerable to cyber crime.



Common risky habits increasing cyber risk in small business



Keeping a password document



'Sleep mode' avoiding software updates



Re-using passwords



Snoozing software updates

From the Cyber Wardens [Bad Habits Research \(Jan 2024\)](#).

43% of cyber crime targets small business

Protect your small business with **FREE** and simple cyber security training.

The FREE Cyber Wardens program is a short online course for sole traders and small businesses.

You don't have to be tech savvy or an information technology (IT) wizard to boost your business's cyber safety.

What you'll learn in the free Cyber Wardens training:



Designed for small businesses



Enrol in just 2 minutes



FREE online training



Simple and practical wins

1 Identify and protect your **important business information**



2 Take simple and effective steps to **defend against digital break-ins**



3 **Spot common tricks and scams** hackers use to attack small businesses



4 **Promote cyber safety** in your team

