Small Business Security Guide

FOR AUSTRALIAN REAL ESTATE AGENTS

PRESENTED BY







Your business is your business

This short guide was developed to help you put in place some basic online security practices. It only takes a few minutes to read through the five easy steps, which will provide you with the basics on how to protect the information entrusted to you by your customers and suppliers.

Your business is *your* business — whether you're in business or managing someone else's business, you are responsible for its success. *Stay Smart Online* is the Australian Government's online safety and security information service, designed to help everyone understand the risks and simple steps that can be taken to protect personal and financial information when using the internet.

Additional information about the *Small Business Security Guide* can be found <u>here</u>.

This guide has been developed by the Australian Government's *Stay Smart Online* Initiative with the support of REA Group, Australia Post, Australia and New Zealand Banking Group Limited, Commonwealth Bank, National Australia Bank, Westpac and Telstra.

This guide has been adapted from the original Stay Smart Online to best explain the information to REA Group customers. In doing so, we have adapted the copy and creative assets originally provided by *Stay Smart Online*.





Introduction by Dan Tehan

The internet underpins so much of what we do in business – whether it's emailing meeting invites, purchasing goods online or processing customer sales.

The Turnbull Government understands the importance of a safe and secure internet which facilitates all of these activities and more.

In April 2016, the Prime Minister, the Hon Malcolm Turnbull MP, launched the Cyber Security Strategy and identified that the biggest challenge we face in the digital age is to both *advance* and *protect* our interests online. This means that we need to be empowered with an understanding of the potential risks and then take steps to protect ourselves and our entities.

This can be particularly challenging for the owners and operators of small-medium businesses.

We know that you don't have much time to spend on understanding the technical ins-and-outs of the internet or establishing complicated responses to potential risks. We also know that you are concerned about the loss of revenue, damage to equipment and reputational issues that can come from cybercrime and other malicious online activities.

That is why the *Stay Smart Online* program is so important. It provides easy to understand advice on a range of topics including securing your internet connection, backing up your data and Point of Sale (POS) security.

The Small Business Security Guide has been designed with all of this in mind. The information is relevant, to the point and simple to implement.

The Small Business Security Guide complements the Stay Smart Online Alert Service, which provides up-to-date information on the latest online threats and how to respond.

If any part of your business operates online – which is currently 84 per cent of Australian small-medium businesses – I encourage you to access the *Stay Smart Online* resources and start building your cyber resilience.

I want all Australian businesses to know first-hand that good cyber security is a key enabler of good business.

The Hon Dan Tehan MP

Minister Assisting the Prime Minister for Cyber Security



As Australia's largest property resource, we understand what a powerful tool the internet can be. While the internet offers us many benefits, there are also some security risks associated with its use.

We are committed to helping you protect your business and stay smart online. To help you with this, we have worked with staysmartonline.gov.au to develop a simple guide which highlights how you can protect your business. The guide covers everything from understanding the importance of privacy, to undertaking actions to protect your network and security devices. Customised to ensure it has the most impact for real estate agents in Australia, it relates specifically to the practices you undertake.

We want all Australian real estate agents to know that implementing strong cyber security is fundamental to doing good business.

Nigel Dalton

Chief Inventor, REA Group





Passphrases

AN ESSENTIAL ACTION TO PROTECT YOUR ONLINE ACCOUNTS

A passphrase is a series of words that are easier to remember, longer and harder to guess than traditional passwords. Passphrases can help prevent criminals from accessing critical information that can be used for fraudulent activity. They should be used for all fixed and mobile devices, and where possible, in combination with other security measures such as firewalls and antivirus software.

Please note that all websites are different and may enforce different password or passphrase standards; the following however, can be used as a guide.

Try not to use passphrases that might be expected or easy to guess. For example, we wouldn't recommend using 'Richmond 3121' as a secure passphrase.

These are examples of a passphrase:

- mirror meet lesson clock
- day above pipe purple
- free central myself clean

Employees should also use two-factor authentication (where available) to improve security. This means that instead of using just a username and password to log in to an account (a username and password are typically regarded as one factor), employees should always have to provide two factors — such as something they know (like a password) and something they have (like a one-time code sent to their mobile phone) — to gain access.

ACTION

Create passphrases for all online accounts, and enable two-factor authentication or verification for additional protection when it is available.

Learn more about Small Business Security





Privacy

YOUR INFORMATION IS VALUABLE, KEEP IT PRIVATE

It's important to keep you and your business safe online. Do not share passphrases or keep sensitive business or customer data on computers outside of your control.

Administrators need greater access privileges than most agents and property managers in the office so they can undertake activities that may impact several users or business processes. Avoid software that gives standard users the same access privileges as administrators. In addition, each employee should have individual access credentials for each business system (not shared credentials).

Your business information is a valuable commodity. Employees should only have access to the information they need to do their job. By limiting that access on a need-to-know basis, you reduce the risk of confidential information leaving the business.

ACTION

Each employee should understand the importance of information security.

Use the <u>Security Implementation Guide</u> for tips on training staff to keep your business information safe.

Learn more about Privacy





The more aware people are about online security, the more capable they are of applying that knowledge to protect the business.

It's important to be aware of what is happening in the online space and stay up-to-date with the latest scams, spam and internet threats.

Being aware also means knowing the right questions to ask. If you are a Principal or owner of your agency, make sure you have an informed discussion with your IT provider to ensure they can meet you and your team's needs. There are some questions at the end of this guide to help you.

Awareness also extends to being on the lookout for suspicious messages, including:

• Phishing emails or text messages (these messages try to lure you into providing your passwords/passphrases, online banking details, or other sensitive information).

• Spam (unsolicited advertising or promotional messages), and fake telemarketing calls requesting personal or financial information.

You should always be suspicious of unsolicited messages or phone calls requesting personal or financial information. If you have any doubt regarding the legitimacy of a phone call or message, contact the organisation to confirm it by using a phone number, address or form sourced from its legitimate website. If you have provided your details to a suspicious caller or sender, immediately change your passwords and associated information. You should also alert service providers such as your bank and ask them to monitor your accounts for unusual activity.

ACTION

To check that a website is legitimate, look for the padlock symbol in your browser address bar and 'https' at the start of the website address when visiting sites. Also, manually type website addresses into your browser's address bar and check that the address displays properly with no added letters, numbers or symbols.

Learn more about Awareness





Network and device security

It's essential to have antivirus software that is regularly updated, as well as setting your systems to automatically update software.

Did you know that mobile phones and tablets may provide access to your sensitive business information? Make sure you use a PIN in case of loss or theft and limit business information stored on them. Treat any network that is not controlled by the business as insecure, particularly public Wi-Fi.

Be aware of plugging unknown USB drives into your computers as these drives may contain viruses.

You can also improve the safety of the business by using separate computers at home for personal activities. In recent years, criminals and malicious individuals have turned to extortion as a way of obtaining money from businesses. Extortion techniques include tricking workers into infecting computers with software that encrypts files so the criminals can demand payment for the decryption key. This is known as ransomware.

ACTION

Keep your security software up to date and back up your data to devices or locations isolated from your corporate network.

Learn more about Network and Device Security





Backups

Business data includes accounting files, invoicing and quoting systems, letters and emails, information and resources, and even your website files. Regularly backing up your data or setting devices to automatically back up can help you quickly recover from a cyber-attack, hard disk failure or another disastrous event (such as becoming infected by ransomware).

Back up your data to a removable storage device such as a hard drive. Do not back up to your computer as it may become compromised too.

ACTION

Take your backup offsite or store it securely, like other important documents. Test your backup system regularly to ensure that it restores all information correctly.

Learn more about Backups



- information? If so, do they meet your business requirements? ☐ Who are the people that control the content and access to your site? Do you know exactly who can access your site? Access should be limited to individuals who need to perform administration or content deployment.
- ☐ Do you and your staff use unique credentials to access your information? How do you prevent unauthorised users from accessing your content?
- ☐ How do administrators access your site? Do you have rules and regulations about where and when the site can be accessed?

- infrastructure, and what happens if they are proven to be related to a security incident?
- How are security incidents managed? Once a security incident has been declared, what is the process to manage, resolve and learn from the incident?
- ☐ If you use an external hosting provider, do you know where your information is located i.e. which country?
- Who owns the IP on your site and how can you gain access to it? Will you have any data sovereignty issues in the event of an incident or trying to recover your information?

This information is not advice and is of a general nature only. If you rely on this guide, you do so entirely at your own risk and realestate.com.au Pty Ltd will not be liable for any direct or indirect loss, claim or damage arising from any errors or omissions contained in the content or your security being compromised. **Australian Government**



