SMOKEBALL

TOP 5 TIPS

FOR PROTECTING YOUR BUSINESS AGAINST CYBERCRIME!

SMOKEBALL

TOP 5 TIPS FOR PROTECTING YOUR BUSINESS AGAINST CYBERCRIME

At Smokeball we now have over 2000 Australian Lawyers and Conveyancers using our eConveyancing software daily. We often receive queries from our clients seeking advice on how they can improve their cybersecurity and ultimately protect their business.

Conveyancers and Law Firms are an extremely attractive target for cybercriminals, considering they are typically small companies that deal with large financial transactions. In fact, small businesses make up 43% of all cybercrime victims.

Our increasingly interconnected environment means it is crucial to ensure cybersecurity is a priority. Fortunately, you can take key steps to improve cybersecurity efforts.

These are Smokeball's top 5 tips to assist you in protecting your business:

1. KEEP OPERATING SYSTEMS AND SOFTWARE UP-TO-DATE

Keeping your computers and applications up-to-date is one of the best ways to protect your business from being hacked. We know installing updates for your devices can at times be annoying, especially when the update wants to download in the middle of your work. However, failing to regularly update your Operating System and applications can leave you vulnerable to security risks.

Hackers, along with malicious programs and viruses, find vulnerabilities in software to access computers, smartphones and tablets. Installing updates limits these vulnerabilities and helps keep your devices secure. It is vital to install updates as soon as possible as this will limit the amount of time hackers have to exploit weaknesses in your Operating System or installed applications. The more out-of-date your programs are, the greater the risk of attack.

You must make installing updates a top priority for your business. Many software providers release patches and updates for their products to correct security concerns and improve functionality. Most modern software and applications update automatically, but make sure you agree to install updates when prompted.

SMOKEBALL

TOP 5 TIPS FOR PROTECTING YOUR BUSINESS AGAINST CYBERCRIME

The common software to keep updated are:

- Operating systems – (e.g. Microsoft Windows)
- Antivirus and security software
- Web browsers – Chrome, Internet Explorer, Firefox
- Web plugins – Adobe Flash, Reader, Skype, Java
- Other applications – Smokeball, Adobe Reader, Microsoft Office etc.

2. IMPLEMENT ROBUST PASSWORD SECURITY

Strong password security is the first line of defence for your conveyancing or legal business. 80% of hacking-related breaches leverage stolen, weak or guessable passwords. Hackers and malicious software can easily find ways into your accounts when you don't take extra measures to keep your passwords safe.

If a password is captured, guessed or stolen, an attacker can pretend to be you and potentially send emails from your accounts, withdraw money from your bank accounts or access files on your devices.

Take the following preventative measures to ramp up your password security:

Use Different Passwords: Don't reuse the same password across multiple programs, devices or accounts. When one account or application is compromised, a hacker may try accessing other accounts using the same credentials. Selecting a variety of passwords is a great way to limit access to your vital information and help your business contain any security breaches.

Change Passwords Regularly: As a rule of thumb, all passwords should be changed every few months. This way, if an old password has been compromised without your knowledge, the new password restores a measure of security to the affected account.

Use Strong Passwords: Create unique, lengthy, and obscure passwords that are not easily guessable. If you do this, you will be on the right track to keeping your business secure. Smokeball suggests you create passwords with a combination of upper and lowercase letters, numbers and punctuation. Ensure this password policy is well communicated and enforced.

SMOKEBALL

TOP 5 TIPS FOR PROTECTING YOUR BUSINESS AGAINST CYBERCRIME

Utilise a Password Manager: Remembering multiple complex passwords can be challenging and often why people use simple, guessable passwords. That's where password managers come to the rescue! Password managers will generate random, difficult to guess passwords and remember them for you. They can also synchronise passwords across all your devices. Your IT Professional can recommend the best password manager to suit your needs.

While it may seem inconvenient to change passwords often and to create complex ones, it's certainly worth it for the security of your business and data.

3. EMAIL MANAGEMENT

Anyone working in conveyancing knows the majority of communication is conducted via email. This is a primary reason why Conveyancers and Lawyers are constantly attacked by cybercriminals. It's much easier to disguise a malicious email and to convince someone it is genuine. Cybercriminals tend to work by exploiting the judgement of the end-user.

These threats tend to work as follows:

1. You receive an email that contains a call to action, an appeal or threat. The email attempts to influence you to do something.

2. You evaluate the email and determine it is legitimate and take the requested action.

3. Your action might be clicking a malicious link, opening a malicious file or provide sensitive information such as credit card details.

4. Once your email or computer is compromised, depending on the severity of the attack, sensitive information can potentially be obtained. This can range from your email address book, to important data on your computer.

At Smokeball, we receive emails each week from Lawyers and Conveyancers around the country who have had their emails or computers compromised. To the trained eye, these emails are clearly fake. So, how does one detect fake emails?

TOP 5 TIPS FOR PROTECTING YOUR BUSINESS AGAINST CYBER CRIME

To protect yourself and your clients, don't accept email requests at face value. Emails asking you to re-direct money may look legitimate but they could contain a malicious attachment or link. It is extremely vital that you pick up the phone and call the party to verify the authenticity of the email. Double-check any sensitive information, for example, before transferring funds.

You should also consider a professional email service provider for your business. Engaging with a company or IT Professional to set this up will allow you to focus on your clients and not worry about cyber threats. Free web email services from Gmail, Hotmail etc are not up to the task of supporting email for businesses.

Professional email providers can protect your business from threats with better email blocking capabilities. You significantly minimise the likelihood of infected or high-risk emails from reaching your inbox, thereby greatly reducing the risk of a cybercrime incident. They're far more effective thanks to their configuration of spam rules, handling of infected attachments and blacklisting known threats.

4. LEVERAGE A HYBRID CLOUD-BASED SOLUTION

There are many benefits of using a cloud-based solution for your conveyancing or legal business. Many software companies offer encrypted cloud storage for your sensitive data relieving some of the cybersecurity burdens, but there are also downfalls to only relying on 100% cloud-based software. For example, if you don't have internet access you unfortunately will not be able to access your files.

eConveyancing software like Smokeball uses a hybrid cloud system where you have the benefit of unlimited cloud storage while still allowing local computer access when you don't have an internet connection. This is especially beneficial if you are needing to obtain important data without an internet connection.

Your data is safer with a reputable cloud provider than on a server in your office. Most IT professionals would say it is easier for someone to steal information locally. All Smokeball data is housed in multiple secure locations around Australia, meaning data is not only more secure but there is minimal risk information can be lost – and data storage is unlimited. You also want to be prepared for disastrous situations, to minimise risk and avoid interruptions to your business. You will be using the same technology as those used by leading banks and large corporations to secure their data.

SMOKEBALL

TOP 5 TIPS FOR PROTECTING YOUR BUSINESS AGAINST CYBERCRIME

5. ENGAGE AN IT PROFESSIONAL

To help your business minimise uncertainty in a digital environment, we highly recommend engaging a professional IT service to give your business a thorough IT audit.

Conveyancers and Lawyers constantly talk about the importance of hiring an expert for legal/conveyancing work. The same rule applies to the IT infrastructure of your business. Investing in a good IT Professional can save you time and money should you encounter an issue.

Whether you're a solo or part of a larger business, IT professionals specialise in dealing with cybersecurity. They can help you understand the current threat environment and implement solutions to protect and secure your business. From threat detection and data security, they're able to design solutions to help safeguard your business by keeping malicious attacks from reaching you.

In doing so you will be able to focus your time and energy on your business and clients!

DON'T LEAVE YOUR CONVEYANCING OR LEGAL BUSINESS VULNERABLE TO HACKERS, IMPROVE YOUR CYBERSECURITY TODAY!

If you're interested in learning more about Smokeball eConveyancing software and the steps we take to protect your businesses and its data, schedule an obligation-free presentation today and see the Smokeball difference.

Call us on 1300 33 55 53
or visit www.smokeball.com.au/book-a-demo

SMOKEBALL

TOP 5 TIPS FOR PROTECTING YOUR BUSINESS AGAINST CYBERCRIME

Conveyancers and Law Firms are an extremely attractive target for cybercriminals, considering they are typically small companies that deal with large financial transactions.

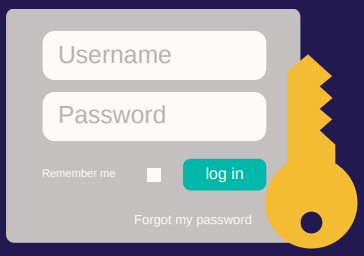
43%
of cybercrime victims are small businesses.

1. UPDATE OPERATING SYSTEMS & SOFTWARE

Hackers find vulnerabilities in software that they exploit to access devices. Installing updates mends vulnerabilities and keeps your devices secure.

- **Operating systems – Windows**
- **Antivirus /security software**
- **Web browsers – Chrome**
- **Other applications – Microsoft Office**

2. IMPLEMENT ROBUST PASSWORD SECURITY



of hacking related breaches leveraged stolen, weak or guessable passwords.

- **Change passwords regularly**
- **Use different/strong passwords**
- **Utilise a password manager**

3. EMAIL MANAGEMENT

Email is the number-one technique used to initiate malware delivery, impersonations and phishing attacks.

Be suspicious of email instructions. Call the party first to verify before taking any action e.g. transferring funds.

Professional email providers protect your business from threats with:

- **Effective email blocking**
- **Two-step verification**

4. LEVERAGE A HYBRID CLOUD-BASED SOLUTION

Software like Smokeball uses a hybrid cloud system where you have the benefits of unlimited cloud storage, while still allowing offline access. Your data is safer with a reputable cloud provider than on a server in your office - it's easier to steal information locally.

5. ENGAGE AN IT PROFESSIONAL

We highly recommend engaging a professional IT service to give your business a thorough IT audit. From threat detection and data security, they're able to design solutions to help safeguard your business by keeping malicious attacks from reaching you.