



Free Guide

Your Essential Guide To Staying Safe Online

Insights and practical tips to empower you with the knowledge and skills necessary to safeguard your online presence.

Reduce your vulnerability to cyber security threats

Protecting your data and identity online is of utmost importance in our connected world. Ransomware and phishing attacks dominate news cycles, and Australians lose billions of dollars annually to cyber security breaches.

In recent years cybersecurity attackers have shifted their focus from computers and network infrastructure to people in order to infiltrate company networks and gain access to critical business and personal information. No matter how well we manage IT infrastructure, we cannot patch against human-targeted attacks. Knowledge is your company's and people's best defence!



Be Aware and Alert

Make sure your team is made aware of and kept updated on emerging cybersecurity threats and attack methods. Use common sense and think twice before clicking links, opening attachments, visiting websites, or responding to emails or phone calls asking for sensitive information. Many cyberattacks can be prevented if you take a moment to consider what you are being asked and what the potential consequences will be if the information is provided. If in doubt don't click a link or attachment or provide sensitive information to unsolicited phone calls.

✓ **Know How to Identify Phishing Attempts**

Be wary of emails or calls that require “immediate action” or ask for personal information. Carefully inspect links to make sure they point to a reputable site before clicking and never respond to messages asking for your username and password. Often phishing emails use a manager’s full name, but the email address is not the correct email (e.g. “Joan Smith <js33554@gmail.com>”) which obviously is not a reputable email address if Joan was your manager. It’s important to not respond to any requests from suspicious emails. Always report suspicious emails to your manager or your IT support team as soon as possible, especially if you have inadvertently clicked on any links or attachments. It is better that your IT support team know about a potential issue so they can take steps before a breach occurs.

✓ **Use Multi Factor Authentication (MFA)**

Multi-factor authentication is a security measure which requires two or more pieces of evidence to prove your identity in order to grant access to a website or application. Access is only granted after successfully presenting two or more pieces of evidence to an authentication mechanism. This evidence can include a combination of username and password, plus a secondary method such as an SMS or email code, Authenticator application code, biometrics scan, or hardware token. Ensure your key systems and applications (e.g. email, storage services, accounting systems, etc) have MFA enabled. This extra layer of security requires you to provide additional information to verify your identity before accessing your account and can protect you from having your email or business critical applications hijacked or compromised.

Use Complex Passwords

Avoid simple password that are short, that have your name or initials as part of the password, that contain any personally associated information such as a birth date, and that do not have a combination of upper and lower-case letters, numbers, and special characters. Also, do not use the same password in more than one location. To make remembering your passwords easier store them in a reputable password vault and never write them down on a Post-it note stuck to your monitor or keep them as notes in your phone. There are a number of good password vaults on the market that Windstil can recommend, which are extremely secure, very simple to use, and can save you time and energy – and can even be faster to use than a Post-it note!

Use Antivirus and Antimalware Software

Ensure that your work and personal computers have a reputable antivirus and antimalware program installed on them, and that it is set to update at least daily. Windstil recommend BitDefender and Windows Defender, however there are several other good solutions to choose from.

Lock Your Devices

Never leave your devices unattended. Password protect your phone and computer and log off or lock your screen when you step away from your computer. On most devices this can be set to happen automatically after a defined period of inactivity, and Windstil can create a Company Policy to ensure compliance.

Keep Apps and Software up to Date

Always apply operating system and business application patches and updates when they are released by the vendor. Do this on your work and home computers and mobile devices, and regularly restart all devices to give them a chance to complete the update process.

Back up Your Computer & Data Often

Ensure your company data is being backed up at least daily, and ideally stored off-site or in a separate cloud storage location to your production data. Backups should include email accounts, storage accounts (such as OneDrive & SharePoint, DropBox etc) and business application data. Setting a regular backup schedule can prevent productivity loss in the event of a targeted ransomware attack.

Protect Personal Information

Do not store personally identifiable information such as credit card numbers or personal details on your computer unless it's in a reputable encrypted vault or e-wallet. Some of the password vaults Windstil recommends have the function to safely store this information.

Limit Activities on Public Wi-Fi

When traveling, either use your cellular network or a virtual private network (VPN) to ensure your internet access is secure. If you must use a public network, make sure it is reputable and refrain from accessing sensitive information, such as online banking.

Secure Staff Home Networks

With extended work from home practices, please encourage your teams to ensure their home network devices are updated with the latest security patches, and that their Wi-Fi networks are properly secured. Network devices that require regular patching include their home router and other computers which may be used to access work-related services. Keeping safe in an online world is challenging and requires you to be vigilant and take cybersecurity seriously. If your business is not sure how to navigate the online security space, please reach out to us. We are very passionate about the online security of your business and good at what we do.

Contact Windstil To Get Your Free IT Consultation

Call: 1300 019 988

Email: team@windstil.com.au

Website: <https://windstil.com.au/cyber-security/>

Address: 382 Middleborough Rd, Blackburn, VIC 3130

Your business' cyber security is in safe hands with Windstil.



WINDSTIL
TECHNOLOGY • PEOPLE • BUSINESS