

# Cloudwize Tips

## Keeping Your Business Secure From Home

In a socially distanced world it is now more important than ever to ensure the integrity and confidentiality of your data.  
Here are 9 steps you can take to secure your organisation while working from home:

### Don't open suspicious emails.

Ensure that all staff know email security best practices - check the sender's address, and be wary if they ask you to share personal information or bank card details. Any attachments could contain malicious malware.



### Use strong passwords.

Use a password manager so you don't use the same password more than once. Have a complex password for accessing the password manager. Utilise smart phone integration so you can access your passwords on the go.



### Don't share your work devices with others.

Work laptops and other machines are for work. Do not share these with family or friends, as they may unknowingly access fraudulent websites or download malicious software.



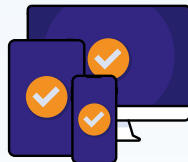
### Use a corporate VPN.

Always access corporate resources via VPN - this redirects your traffic via the corporate infrastructure, which is vastly more secure and can identify any security issues.



### Use Multi-Factor Authentication.

Multi-Factor Authentication asks users to verify their identity with multiple measures. It is a great way to combat credential and account compromise.



### Store information in backed up locations.

Save your files on company drives or company Sharepoint/Teams so that your data is in a location that is being backed up by company systems. This way, if your computer is compromised, you will not lose your data.



### Use only work devices when accessing corporate information.

Your work machines have the required security software needed to protect against a variety of malware, ransomware and other viruses.



### Avoid using insecure Wi-Fi networks.

Public networks such as airports and hotels can be easily hacked and attackers can use these networks to access ALL connected devices. If you plan on using a mobile device as a Wi-Fi hot spot, ensure it is configured with a strong password.



### Actively participate in Security Awareness Training.

Security Awareness Training can transform your people into a fortified last line of defence. Training should be implemented from senior managers to front line staff to ensure security is everyone's responsibility.



For more information, please do not hesitate to contact our expert advisers at:

[www.cloudwize.com.au](http://www.cloudwize.com.au)