**PHIL ALDRIDGE,** *Director for WA, Fuse Technology WA Pty Ltd.*
Linkedin: https://www.linkedin.com/in/philaldridge/
Website: https://fusetechnology.com
0450 382 270

## TIP 1. YOUR SERVICE PROVIDER

Do not assume that your IT Service Provider is doing a good job with your Cyber Security. Often they do not, because it highlights deficiencies in their service. At least once every 12 months get your Cyber Security Posture assessed by a 3rd Party Vendor and take action on the points raised. Ensure that your business complies with Essential Eight Level 1 or preferably 2.

## TIP 2. CYBER INSURANCE

Get Cyber Insurance for your business. It won’t protect you from being attacked, but it will assist you should you get hacked and just the process of getting cyber insurance will, in some way, demonstrate that you have got at least the basics of cyber security implemented in your business.

## TIP 3. ENSURE SECURITY

Microsoft and Google provide a platform that is extremely secure. They spend more on security than almost any other company on the planet. However, this does not mean your account with them is secure unless you configure it to be secure. This takes a lot of time and effort and skill. Ensure your IT Provider has secured your account.

## TIP 4. MULTI-FACTOR IDENTIFICATION

Do the basics and do them well. Most hacking comes through email so: ensure that your external email security is done properly. Ask your IT provider to confirm you have SPF, SKIM and DMARC setup. Also ask them to confirm that all accounts have some form of multi-factor authentication (MFA) applied.

## TIP 5. BACKUP

Don’t just backup. Of course backups are important; but, what is more important, is to ensure the backups can be restored. If you never do test restores you will have no idea if it will work when you need it - so do regular restores.

## TIP 6. BLOCK LEGACY SYSTEMS

Block access from Legacy computers / phones. If you have all new Windows 11 and Android/iPhones, then block legacy systems from being able to login to your systems.

## TIP 7. HOME VS. WORK COMPUTERS

Separate work computers from home use computers. Ensure all staff have dedicated use work computers if they work from home to eliminate any risk from hacking occurring when people use shared use computers.

## TIP 8. MANAGE EMAILS

If you allow staff to have work email on their phones, then ensure the email is managed centrally so it can be deleted if a user loses their phone or has it stolen.

## TIP 9. EDUCATE STAFF ABOUT HACKING

Hacking is almost always a result of human error. Training staff on the latest forms of risk is important but reducing the chance of them making a mistake is even more important.  Prevent users from being able to run new applications on their machines.

## TIP 10. LOG IN OPTIONS

If you and your staff normally only log in from Australia, then block people from attempting to log in from other countries - and then make exceptions when people go on holiday.