April 2026

# TALKING TECH
*Helping your business*

## WHAT OUR CLIENTS SAY:

"Explained things easily, and was able to resolve my problem. He was very polite and friendly."

"Able to resolve the ongoing problem we had. He was very patient and incredibly helpful."

## DID YOU KNOW?

The first chocolate Easter eggs were made in the UK in 1873.


DSP IT Solutions
(03) 9001 0817
182C Sladen Street
Cranbourne VIC 3977
sales@dspit.com.au
www.dspit.com.au


## FROM DAMIEN'S DESK:

Hello, its April. The month of April fools, but we won't play any jokes on you.

But we will provide solid facts.
First, AI is not coming, it's already here. How is your business leveraging AI? There are some simple gains you can get in productivity using an AI platform like Microsoft Copilot. Reach out to us and we will walk you through how your business can get access to these productivity gains.

Second, A security framework will give you some certainty that your business is on the right track to being secure. Making sure your team understands why security is important in a business like yours. Do you have MFA (Multifactor authentication) on all your business-critical applications? You should and if you don't you are asking for trouble. Let us introduce you to SMB1001, a true SMB friendly framework that will help you embed a security baseline. Reach out we can help!

Stay Safe and don't get pranked

*Damien Pepper - Director*

#SuperResponsive #BuildRelationships #AlwaysLearning #MakeComplexSimple #NothingIsTooHard

# STOP RANSOMWARE IN ITS TRACKS:

# A 5 step proactive defence plan

Ransomware isn't a jump scare. It's a slow build.

In many cases, it begins days, or even weeks, before encryption, with something mundane, like a login that never should have succeeded. That's why an effective ransomware defence plan is about more than deploying antimalware. It's about preventing unauthorised access from gaining traction.

*Here's a five-step approach you can implement across small business environments without turning security into a daily obstacle course. Each step is practical, MSP friendly, and repeatable across small business enviroments.*

**Step 1: Phishing-Resistant Sign-Ins**

"Phishing-resistant" sign-ins are authentication methods that can't be easily compromised by fake login pages or intercepted onetime codes. It's the difference between "MFA is enabled" and "MFA still works when someone is specifically targeted."

- Enforce strong MFA across all accounts, with priority given to admin and remote accounts
- Eliminate legacy authentication methods that weaken your security baseline
- Implement conditional access rules, such as step-up verification for high-risk sign-ins, new devices, or unusual locations

**Step 2: Least Privilege + Separation**

"Least privilege" means each account gets only the access it needs to do its job, and nothing more.

"Separation" means keeping administrative privileges distinct from everyday user activity, so a single compromised login doesn't hand over control of the entire business.

- Keep administrative accounts separate from everyday user accounts
- Eliminate shared logins and minimise broad "everyone has access" groups
- Limit administrative tools to only the specific people and devices that genuinely require them

**Step 3: Close known holes**

"Known holes" are vulnerabilities attackers already know how to exploit, typically because systems are unpatched, exposed to the internet or running outdated software.

- Set clear patch guidelines: critical vulnerabilities addressed immediately, high-risk issues next, and all others on a defined schedule
- Prioritise internet-facing systems and remote access infrastructure
- Cover third-party applications

**Step 4: Early detection**

Early detection means identifying ransomware warning signs before encryption spreads across the environment. Think alerts for unusual behaviour that enable rapid containment.

A strong baseline includes:

- Endpoint monitoring that can flag suspicious behaviour quickly
- Rules for what gets escalated immediately vs what gets reviewed

**Step 5: Secure, Tested Backups**

"Secure, tested backups" are backups that attackers can't easily access or encrypt, and that you've verified you can restore successfully when it matters most.

Ransomware guidance emphasize that backups must be protected and restorable. Specifically, the need to "secure and isolate backups."

- Keep at least one backup copy isolated from the main environment.
- Run restore drills on a schedule
- Define recovery priorities ahead of time, what needs to be restored first, and in what sequence

*If you'd like help assessing your current defences and building a practical, repeatable ransomware protection plan, contact us today.*

# Your simple cyber hygiene checklist

**Unique passwords**
No re-use. Ever.

**Automatic updates**
Devices + apps.

**MFA everywhere**
Passwords alone aren't enough.

**Right access only**
Remove old logins.

**Daily backups**
Stored separately.

**Staff awareness**
Short reminders beat long training.

**Think before clicking**
Email is the #1 entry point.

**Incident plan**
Who to call. What to do.

**74%** of breaches involve human error.

**81%** involve stolen or weak passwords.

**We can help make sure your business's cyber hygiene is consistent, without being complicated.**
**Get in touch.**

dsp IT SOLUTIONS

# IS YOUR BUSINESS MISSING THESE 7 SECURITY LAYERS?

*If your security stack has grown organically over time, these are the gaps that often show up first.*

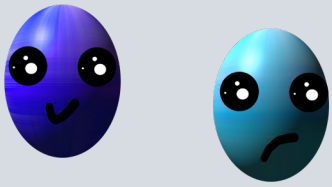
- Phishing-resistant authentication: enforce strong MFA everywhere, then tighten admin and remote access first.
- Device trust and usage policies: define what a compliant device is, and what happens when it isn't.
- Email and user risk controls: reduce exposure by default with filtering, warnings, and easy reporting.
- Continuous vulnerability and patch coverage: measure patch latency and include third-party apps.
- Detection and response readiness: define what gets escalated, document runbooks, and practice containment steps.
- Governance that sticks: publish clear "approved" standards and make exceptions time-bound and owned.
- Recovery that's proven: run restore drills and define recovery priorities before you need them.

*When you strengthen these seven layers, you turn your business' security into a repeatable, measurable baseline you can be confident in.*

## NEED A LAUGH

What did one Easter egg say to the other?

Heard any good yolks today?



## APRIL TRIVIA QUESTION

Test your knowledge!

The answer to last month's question was b) IBM. Do you know the answer to the question below? The answer will be in next month's Newsletter.

Before it was known as Adobe Photoshop, what was the original name of the software in 1987?

a) Image Pro
b) Display
c) DigitalPaint
d) Photocanvas