JANUARY 2026

dsp IT SOLUTIONS

TALKING TECH

HELPING YOUR BUSINESS

FROM DAMIEN'S DESKTOP:

G'day and welcome to the start of 2026! We're excited to see what opportunities and challenges this year will bring, and we're eager to support you in making it a successful one for your business.

2025 was a year of rapid technological change and, as we step into 2026, the pace is only set to increase. Artificial Intelligence (AI) is no longer just a buzzword or a distant promise – it's now a driving force in how we work, communicate, and secure our digital lives. This means that businesses of all shapes and sizes need to be proactive in preparing for the new era of cybersecurity threats and solutions.

We're committed to helping you navigate the shifting landscape of cybersecurity. Throughout 2026, our newsletters will feature expert tips, case studies, and updates on the latest developments in AI and digital safety. Together, let's make this year one where your business not only survives, but thrives in the digital age.

Here's to a safe, successful, and exciting 2026!

Damien Pepper - Director
dSP IT Solutions

Clients' Words . . .

"We appreciate all that you do!"
Sandi
Grace Professional Services

"(The Tech) is very patient. He resolves very quickly. His service is always efficient."
Lili
After-care Australasia

DID YOU KNOW?

Studies have shown that an average keyboard has 400 times more bacteria than a rubbish bin!

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

#SuperResponsive #MakeTheComplexSimple #BuildRelationships #NothingIsTooHard #AlwaysLearning

ADVANCED STRATEGIES TO LOCK DOWN YOUR BUSINESS LOGINS

Good login security works in layers. The more hoops an attacker has to jump through, the less likely they are to make it to your sensitive data.

HERE ARE SOME PRACTICAL TIPS TO MAKE SURE YOUR EMPLOYEES ARE PROTECTED.

Strengthen Password and Authentication Policies.

If your company still allows short, predictable logins or reuses passwords, you've already given attackers a head start. Here's what works better:

- Require unique, complex passwords for every account.
- Swap out traditional passwords for passphrases; easier for humans to remember, harder for machines to guess.
- Roll out a password manager so staff can store and auto-generate strong credentials.

Enforce multi-factor authentication (MFA) everywhere possible.

- Check passwords against known breach lists and rotate them periodically.
- Apply the rules across the board. Leaving one "less important" account unprotected is like locking your front door but leaving the garage wide open.

Reduce Risk Through Access Control and Least Privilege.

- The fewer keys in circulation, the fewer chances there are for one to be stolen.
- Keep admin privileges limited to the smallest possible group.
- Separate super admin accounts from day-to-day logins and store them securely.
- Give third parties the bare minimum access they need.

Secure Devices, Networks, and Browsers.

Your login policies won't mean much if someone signs in from a compromised device or an open public network. Encrypt every company laptop and require strong passwords.

- *Use mobile security apps, especially for staff who connect on the go.*
- *Lock down your Wi-Fi.*
- *Keep firewalls active, both on-site and for remote workers.*
- *Turn on automatic updates for browsers, operating systems, and apps.*

Protect Email as a Common Attack Gateway.

One convincing message, and an employee clicks a link they shouldn't. To close that door:

- Enable advanced phishing and malware filtering.
- Set up SPF, DKIM, and DMARC to make your domain harder to spoof.
- Train your team to verify unexpected requests.

Plan for the Inevitable with Incident Response and Monitoring.

Even the best defences can be bypassed. The question is how fast you can respond.

- Incident Response Plan
- Vulnerability Scanning
- Credential Monitoring
- Regular Backups

Make Your Logins a Security Asset, not a Weak Spot

You don't have to do it all overnight. Start with the weakest link right now, maybe an old, shared admin password or a lack of MFA on your most sensitive systems and fix it. Then move to the next gap. Over time, those small improvements add up to a solid, layered defence.

HOW TO REDUCE WASTE IN MICROSOFT 365

Microsoft 365 is a powerful platform that helps a business in many ways. It boosts collaboration and streamlines operations, among other benefits. However, many companies waste money on unnecessary licences and features that are not fully used.

The good news is that much of this waste can be avoided. With discipline, proper tools, and regulation, you can redirect your budget to a smarter use of Microsoft 365. Below are some of the main strategies to adopt.

Downgrade Light Users

Not all users require an E3 or E5 licence. For example, why give your receptionist a complete E5 licence with enhanced compliance tools if they're only emailing and using Teams? By monitoring actual usage, you can downgrade such users to E1 or another lower-tiered plan without affecting productivity. Low-usage discovery utilities enable you to downgrade confidently without speculation.

Automate Offboarding of Ex-Employees

By automating onboarding processes, licences are unassigned automatically once you mark an employee as departed. Use workflow tools like Power Automate linked to HR systems or forms to revoke access, remove group memberships, convert mailboxes, and unassign licences in one automated process.

Consolidate Overlapping Features

Review your security, compliance, collaboration, and analytics tools to find overlaps. If your plan already offers advanced threat protection or endpoint detection, consider cancelling redundant third-party tools.

If Copilot addons duplicate other AI or automation tools you already use, streamline them under one system.

Review Group and Shared Mailboxes

Many organisations mistakenly assign premium licences to shared mailboxes, service accounts, or inactive mailboxes. This doesn't offer any functional benefits. Think about converting them to free shared mailboxes or archiving them to free up licence slots. That way, you ensure that your M365 budget is only spent on value-generating users.

Enable Licence Expiration Alerts and Governance Policies

Avoid wastage in the future by setting up policy checks and notifications and make sure you respond as needed. Note down renewal dates for contracts so you don't accidentally auto renew unused licences. Also, track levels of inactivity and flag for review licences that have passed the threshold.

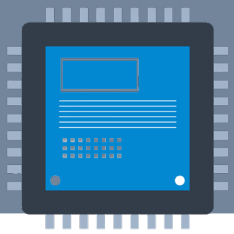
Make Microsoft 365 Work Smarter for You

Don't let Microsoft 365 licences and add-ons quietly drain your resources. Take control by reviewing how each licence is used. When you match your tools with actual business needs, you save money, simplify management, and improve productivity in your organisation.

Optimising your Microsoft 365 environment means getting full value from what you already have. When you use M365 security and Copilot add-ons responsibly, your business is likely to thrive.

NEED A LAUGH?

What is a computer's favourite snack to eat?



Microchips!

Love what we do?

Tell a friend and let us thank you! Scan the QR code to go our referral page.
Your referral is the biggest compliment we can get!

JANUARY TRIVIA QUESTION . . .

Test your knowledge!

The answer to last month's question was d) Merry Christmas. Can you guess the answer to the trivia question below? The answer will be revealed in next month's newsletter.

Which animal is depicted in the Firefox logo?

a) Red panda
b) Bear
c) Fox
d) Monkey