OCTOBER 2025

dsp IT SOLUTIONS

TALKING TECH

HELPING YOUR BUSINESS

FROM DAMIEN'S DESKTOP:

This month, we have some exciting updates and initiatives that will enhance our operations and security.

Introducing SMB1001:
A New Standard in Cybersecurity
We are pleased to announce our adoption of the SMB1001 cybersecurity framework. Developed by Dynamic Standards International (DSI), SMB1001 is designed specifically for small and medium-sized businesses. This framework provides clear, actionable guidance to improve our cybersecurity practices, ensuring that we are well-protected against evolving cyber threats. Whether you are technical or non-technical staff, SMB1001 is designed to be accessible and practical for everyone.

Upgrading from Windows 10 to Windows 11
As Microsoft plans to end support for Windows 10 on October 14, 2025, we are preparing to upgrade all our systems to Windows 11. This upgrade is not just about new features; it's about ensuring our PCs remain secure, fast, and capable. Windows 11 offers enhanced performance, improved security, and a modern interface that will boost our productivity and user experience. It's essential to make this transition smoothly to avoid any security vulnerabilities and ensure our systems are up-to-date.

Let's embrace these changes and continue to work together towards a more secure and efficient future. If you have any questions or need further information, please do not hesitate to reach out.

Damien Pepper - Director
dSP IT Solutions

Clients' Words . . .

"Excellent service, as always. Friendly staff, extremely fast at actioning requests."
Michelle,
After-care Australasia

"Thank you 'Tech' for your amazing patience, my anxiety was through the roof and you just sailed me through each issue, professional and respectful."
Jennifer,
Community Kinders Plus

DID YOU KNOW?

The QWERTY keyboard was intentionally designed to slow people down:
The layout was created in the 1870s to prevent typewriter jams by spacing out commonly used letter pairings.

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

Is Your Smart Office a Security Risk?

What Businesses Need to Know About IoT

Your office thermostat, conference room speaker, and smart badge reader are convenient, but they're also doors into your network. With more devices than ever in play, keeping track can be tough, and it only takes one weak link to put your entire system at risk. That's why smart IT solutions matter now more than ever. A trusted IT partner can help you connect smart devices safely, keep data secure, and manage your whole setup without stress.

Here's a practical guide designed for small teams getting ready to work with connected tech.

WHAT IS IOT?

IoT, or the Internet of Things, is all about physical devices, like sensors, appliances, gadgets, or machines, being connected to the internet. These smart tools can collect and share data, and even act on their own, all without needing someone to constantly manage them. IoT helps boost efficiency, automate tasks, and provide useful data that leads to smarter decisions for both businesses and individuals. But it also comes with challenges, like keeping data secure, protecting privacy, and keeping track of all those connected devices.

Steps To Manage IoT Security Risks for Small Businesses

1. Know What You've Got

Begin with all of your network's smart devices, such as cameras, speakers, printers, and thermostats. If you are not aware of a gadget, you cannot keep it safe.

- Walk through the office and note each gadget
- Record model names and who uses them

With a clear inventory, you'll have the visibility you need to stay in control during updates or when responding to issues.

2. Change Default Passwords Immediately

Most smart devices come with weak, shared passwords. If you're still using the default password, you're inviting trouble.

- Change every password to something strong and unique
- Store passwords securely where your team can consistently access them

It takes just a minute, and it helps you avoid one of the most common rookie mistakes: weak passwords.

3. Segment Your Work

Let your smart printer talk, but don't let it talk to everything. Use network segmentation to give each IoT device space while keeping your main systems secure.

- Create separate Wi-Fi or VLAN sections for IoT gear
- Block IoT devices from accessing sensitive servers
- Use guest networks where possible

Segmented networks reduce risk and make monitoring easy.

4. Keep Firmware and Software Updated

Security flaws are found all the time, and updates fix them. If your devices are out of date, you're wide open to cyberattacks.

- Check for updates monthly
- Automate updates when possible
- Replace devices that are no longer supported

Even older gadgets can be secure if they keep receiving patches.

5. Monitor Traffic and Logs

Once your devices are in place, watch how they talk. Unexpected activity could signal trouble.

- Use basic network tools to track how often and where devices connect
- Set alerts for strange activity, like a badge reader suddenly reaching the internet
- Review logs regularly for odd patterns

You don't need an army of security experts, just something as simple as a nightly check-in.

6. Set Up a Response Plan

Incidents happen; devices can fail or malfunction. Without a plan, every problem turns into a major headache. Your response plan should include:

- Who to contact when devices act weird
- How you'll isolate a problematic device
- Available standby tools or firmware

A strong response plan lets you respond quickly and keep calm when things go wrong.

7. Limit What Each Device Can Do

Not every device needs full network access. The key is permission controls.

- Turn off unused features and remote access
- Block internet access where not needed
- Restrict device functions to exact roles only

Less access means less risk, yet your tools can still get the job done.

cont'd page 3

cont'd from page 2

8. Watch for Devices That Creep In
It's easy to bring in new devices without thinking of security risks, like smart coffee makers or guest speakers.
- Have a simple approval step for new devices
- Ask questions: "Does it need office Wi-Fi? Does it store data?"
- Reject or block any gear that can't be secured

Catching these risks early keeps your network strong.

9. Encrypt Sensitive Data
If your smart devices transmit data, ensure that data is encrypted both during transmission and while stored.
- Check device settings for encryption options
- Use encrypted storage systems on your network

Encryption adds a layer of protection without slowing things down.

10. Re-evaluate Regularly
It's easy to secure your office tech once and assume it stays that way. But tech changes fast, and so do threats.
- Do a full check-in every six months
- Reassess passwords, network segments, and firmware
- Replace devices that don't meet today's standards

With a regular schedule, you keep ahead without overthinking it.

WHY THIS ACTUALLY MATTERS
Smart devices simplify work but can pose risks if not properly secured. More businesses are experiencing cyberattacks through their IoT devices than ever before, and these attacks are rising rapidly.
Protecting your systems isn't about expensive high-tech solutions, it's about taking simple, smart steps like updating passwords, keeping devices up to date, and knowing what's connected.

If you need help training your team on the warning signs to look out for,
get in touch.

dsp IT SOLUTIONS

WE LOVE REFERRALS

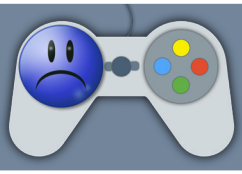
The greatest gift anyone can give us is a referral to your business friends.

Referrals help us keep costs down so we can pass on the savings to all our clients.

Simply introduce me via email damien@dspit.com.au or (03) 9001 0817 and I'll take it from there.

NEED A LAUGH?

What do you do when you encounter a sad Xbox?
You console it!



Strategic Ways to Plan Your Business's IT Expenses

STEP 1
Take some time to figure out what you are paying for and how it will benefit you.

STEP 2
Focus spending on investments that improve security, productivity, and training rather than just buying flashy gadgets.

STEP 3
Break down your expenses into clear categories such as: hardware, software, security, support, and training.

STEP 4
Trim what you don't need like old subscriptions, redundant tools, and overpriced vendors.

STEP 5
Allow for flexibility. Your budget should adapt to your needs without breaking under pressure.

STEP 6
Plan for the future. If growth is part of your plan, your IT budget should reflect that too.

STEP 7
Partner with experts who can help you stay organised, cut unnecessary costs, and keep everything running smoothly.

7 Ways to Boost Your WiFi Network's Performance

Upgrade Your Hardware: Invest in equipment that can handle today's demands and grow with you down the line.
Give Priority to What Matters Most: Prioritise important traffic like video and phone calls, ensuring they get the bandwidth they need first.
Divide Your Networks: By dividing your network into smaller segments, you reduce congestion and boost security.
Balance Server Load: Share workload across servers, keeps systems running smoothly during busy times and helps your team stay productive without delays.
Adjust Your Setup for Efficiency: Make sure to regularly check your router, switch, and firewall settings. Using network monitoring tools can help you quickly identify and fix any problems.
Watch for Threats Before They Slow You Down: An Intrusion Detection System (IDS) can keep an eye out for unusual activity that might be slowing down your network.
Build in a Backup Plan: Having a backup internet connection or extra equipment means your team can keep working, even if something goes down.

OCTOBER TRIVIA QUESTION . . .

Test your knowledge!

The answer to last month's question was a) Personal Identification Number. Can you guess the answer to the trivia question below? The answer will be revealed in next month's newsletter.

How much storage did the first commercially available USB flash drive provide?

a) 64MB
b) 8MB
c) 1.44MB
d) 256MB