August 2026

TALKING TECH

Helping your business

WHAT OUR CLIENTS SAY:

I found DSP to be very professional and helpful. I would recommend their service without a doubt!

- Godfrey Agius P/L

As usual, DSP was excellent to deal with, very helpful and fast response times.

- Jeniffer, Erect A Rack

DID YOU KNOW?

Wi-Fi was nearly branded "Flankspeed" (*navel term for maximum speed*) before marketing chose the catchier name!

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

FROM SHANE'S DESK:

Welcome to our August issue of "Talking Tech - Helping your business."

This month is a good reminder that cyber risk doesn't always come from complex attacks — it often comes from small gaps.

SIM swapping shows how easily someone can take control of your phone number and, from there, access your accounts.

And without proper email protection, attackers can send messages that look like they've come straight from your business.

The fix isn't complicated — lock your number, move away from SMS codes, and make sure your email security (SPF, DKIM, DMARC) is fully set up, not just "monitoring."

The takeaway: getting the basics right makes the biggest difference.

If you'd like a hand tightening things up, we're here to help.

#SuperResponsive #BuildRelationships #AlwaysLearning #MakeComplexSimple #NothingIsTooHard

One morning your phone drops to "No Service" and stops receiving calls and texts. You assume it's a network glitch and you get on with your day.

But in the next suburb, someone has just convinced your mobile carrier that they're you. They've moved your number onto a SIM card sitting in their own phone.

Every call and text meant for you now goes to them, including the security codes that protect your email and your bank logins.

This is a SIM swap. The attacker never touches your password or breaks into a single system. They take over your phone number, then use it to reset everything attached to it.

They start by gathering a few details about you, often pulled from an old data breach or your social media.

Then they call your carrier, claim your phone was lost or damaged, and ask to activate your number on a new SIM. If the agent believes the story, your number is theirs in minutes.

From there, the SMS codes you rely on become their codes (SMS is the text-message system most accounts use to send those one-time login codes). Password reset links and login verifications all land on their device instead of yours.

Researchers at Princeton University tested five major US carriers by posing as customers and trying to move numbers they didn't own.

They succeeded on 80% of their first attempts, mostly because the carriers were leaning on security questions a motivated attacker could answer.

The losses reported to the FBI run into the tens of millions of dollars a year, and the true figure is almost certainly higher, because most victims report the end result, like a drained account, rather than the phone takeover that caused it.

Your personal mobile number is probably the recovery method for nearly everything you log into, from your Microsoft 365 account to your business bank.

If that one number falls into the wrong hands, a lot can fall with it. Don't panic though. This is very fixable, and the setup is quick and free:

1. Lock your number with your carrier.

Every major provider now offers a free toggle that blocks anyone from moving your SIM or porting your number without your say-so.

2. Move your important logins off text message codes.

For your email, banking, and admin accounts, switch from SMS codes to an authenticator app or a passkey.
Both keep working even if someone steals your number, because the approval happens on your device, not through your phone signal.

3. Add a separate passcode to your carrier account.

Most carriers let you set a PIN or passcode that's required before any change is made to your account. It's one more wall between an attacker and your number.

Many carriers now send a text or email alert when someone requests a SIM change on your account. If that alert shows up and it wasn't you, call your carrier right away.

If you'd like a hand checking which of your accounts still rely on text-message codes, or help locking down your team's numbers, reach out and we'll walk you through it.

HOW TO STOP SCAMMERS SENDING EMAILS IN YOUR ORGANISATION'S NAME

Right now, with no hacking at all, someone could send an email that looks like it came from your organisation. They put your domain in the "from" line and email your clients or suppliers, asking them to pay a fake invoice or move money to a new account. Because the message carries your name, the people who trust you are far more likely to act on it. It works because email was never built to check that senders are who they claim to be.

The three records that stop it

- **SPF** is a list of the mail servers allowed to send email for your domain.
- **DKIM** adds a tamper-proof signature that proves a message really came from you and wasn't changed on the way.
- **DMARC** ties the two together and tells receiving mail servers what to do with anything that fails the check.

The setting most businesses get wrong

Having the records isn't quite enough. DMARC has three settings, and most businesses stop at the wrong one. On "monitor only," it watches and reports but never blocks a fake. Real protection starts when it's set to "quarantine" or "reject." One thing these records don't stop: a lookalike domain (like yourorganisation-invoices.com.au), or a display name that shows your organisation over a random address. So, staff should still check the full email address before acting on any payment request.

How to switch it on without blocking your own email

DMARC is best turned up in stages. Start on "monitor only" and read the reports it sends, which show every source sending email as your domain, including the ones that shouldn't. Once you've confirmed your real email passes, move to "quarantine," then to "reject." Done gradually, you close the door on impersonation without sending your own invoices and quotes to the spam folder.

Worth having even if you barely send email

Beyond protecting your name, these records help your messages arrive. Since early 2024, Google and Yahoo have required bulk senders to use SPF, DKIM, and DMARC, and Microsoft began applying similar rules to Outlook.com in 2025. Even below those volumes, a properly set-up domain is more likely to land in the inbox than the spam folder. You can check what yours has in place with a free DMARC checker, or ask your IT provider to confirm it and walk the policy up to full protection safely.

The difference between monitoring and maintenance

MONITORING
(Watching for problems)

- Spots issues
- Sends alerts
- Tracks performance
- Detects unusual activity
- Watches systems 24/7

"Something might be wrong."

MAINTENANCE
(Preventing problems)

- Installs updates
- Fixes vulnerabilities
- Tests backups
- Removes old accounts
- Optimises systems

"Let's stop problems happening."

Good IT support needs both

Monitoring tells you when something needs attention.
Maintenance helps stop issues building up in the first place.

If your IT support only reacts to alerts,
you may be missing the bigger picture.
We can help you watch for and prevent problems.

Get in touch.

DSP IT SOLUTIONS

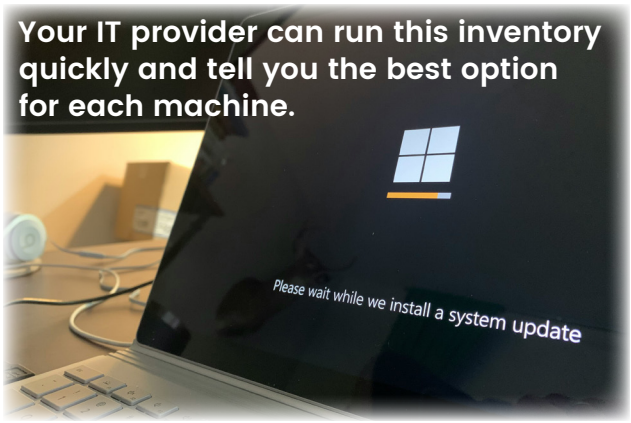
AI note-takers join your meetings, record every word, and store it on the vendor's servers. They're worth using, but before you let one into a client or staff meeting, run these quick checks.

- Pick one approved tool, and ask staff not to connect others to company meetings.
- Turn off auto-join, so it only records when someone chooses to.
- Announce the recording and get everyone's consent before it starts.
- Check whether the tool uses your conversations to train its AI.
- Prefer a tool that keeps recordings inside your own Microsoft or Google account.
- Check who the summary gets emailed to by default.
- Keep bots out of legal, HR, and confidential client meetings.

STILL ON WINDOWS 10? HERE'S WHY IT'S A RISK NOW

Windows 10 stopped getting security updates in October 2025. The computers still work, which is why it's easy to leave them, but every new flaw found now stays unpatched. That makes those machines easier to attack and can cause problems with compliance and your cyber insurance. Here's how to move off it:

1. List every computer still running Windows 10.
2. Check which ones can upgrade to Windows 11 (free if the hardware qualifies) using Microsoft's free PC Health Check app.
3. Upgrade the ones that qualify. The upgrade keeps your files and programs in place.
4. For the rest, choose between paid Extended Security Updates as a short-term bridge or replacing the PC.
5. Your IT provider can run this inventory quickly and tell you the best option for each machine.



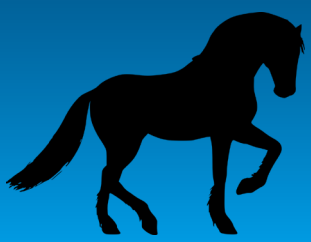
AUGUST TRIVIA QUESTION

Test your knowledge!

The answer to last month's question was a) 31cm, the wingspan of a butterfly found in Papua New Guinea. Do you know the answer to the question below? The answer will be in next month's Newsletter.

Approximately, how much horsepower does a horse actually have?

a) 1
b) 24
c) 8
d) 16



NEED A LAUGH

What did the baby corn say to the mama corn?

Where's popcorn!

TALKING TECH TIP

Lock Your PDFs

To prevent clients from accidentally editing your PDF contracts or invoices, you should "flatten" the file before sending. Open your document, select Print, choose Microsoft Print to PDF, and save it as a new file. This instantly converts editable fields into static text, locking the content.