September 2026

TALKING TECH

Helping your business

WHAT OUR CLIENTS SAY:

"DSP delivers the support and expertise we need."
Karen,
The Partner Leader Co.

"DSP consistently deliver reliable and tailored solutions."
Kevin,
Coastal Surveys

DID YOU KNOW?

A random computer glitch might actually be caused by outer space.
High energy cosmic rays constantly strike the Earth and can physically flip a single piece of data inside your memory chip, causing a spontaneous crash or reboot.

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

FROM SHANE'S DESK:

Cyber security is often viewed as a problem that only affects large organisations, but the reality is that small and medium-sized businesses are increasingly being targeted because attackers know many don't have dedicated security teams.

This month's newsletter highlights a few examples of how something seemingly simple, such as an unprotected Google Business Profile, a weak password, or a compromised device, can have a significant impact on your business. In many cases, cyber incidents don't begin with sophisticated attacks. They start with a single mistake, a missed update, or a convincing phishing email.

The good news is that protecting your business doesn't always require major investment. Simple measures such as enabling Multi-Factor Authentication, adopting passkeys where available, regularly reviewing who has access to your systems, and keeping devices updated can dramatically reduce your risk.

Technology continues to evolve, and so do the methods criminals use to exploit it. That's why we encourage our clients to take a proactive approach to security rather than waiting until something goes wrong.

As always, if you'd like help reviewing your security posture or implementing any of the recommendations discussed this month, our team is only a phone call away.

#SuperResponsive #BuildRelationships #AlwaysLearning #MakeComplexSimple #NothingIsTooHard

HOW SCAMMERS HIJACK GOOGLE LISTINGS

Most local businesses have a Google Business Profile. It's the listing that shows up on Google Search and Maps with your hours, phone number, website, and reviews. For a lot of owners, it brings in a good share of their calls and customers.

The problem is that someone who isn't you can take that listing over, and once they do, they control what your customers see.

There are three main ways they get in:

• **They ask Google for access.**
Google lets anyone request access to a listing, even one you already own. Google emails you and gives you three days to say yes or no. If you say yes by mistake, they get in right away. If you ignore it, after three days they may be able to claim the listing themselves.

• **They fake a Google login page.**
They send an email, text, or call pretending to be Google, then send you to a fake sign-in page and steal your password. AI makes these fakes very hard to spot now.

• **They "suggest an edit."**
Anyone can suggest changes to your listing, like a new phone number or website. Google is supposed to catch the bad ones, but some get through.

With access, they can change your phone number so your calls go to them, or send your website link somewhere else.

They can reply to reviews as if they're you, lock you out, or ask for money to give it back. Some just hide your listing so customers can't find you. You might not notice for weeks, because it all looks normal when you log in.

Do these three things so this doesn't happen to you:

• **Turn on 2-Step Verification** on the Google account that runs your listing. Go to myaccount.google.com/security and switch it on. Now even if someone steals your password, they can't log in without the code on your phone.

• **Go to Google yourself to manage your listing,** instead of using email links. The old Google My Business app is gone. If you have one location, sign in and search your business name on Google, or open it in Google Maps. If you have several, use business.google.com/manage.

• **Reply to access requests within three days,** and only say yes to people you know. If you ignore a real request, they may be able to claim your listing after three days. So log in, see who's asking, and say no unless you know them.

Google never charges for any of this, and it will never ask you for a code or PIN. Anyone who does is a scammer.

If you want a hand with this, reach out and we'll help you check who has access to your listing and get 2-Step Verification switched on.

How one insecure device puts your entire business at risk

Step 1:

One device gets compromised

- Phishing email
- Weak password
- Missed update
- Lost device

A single mistake can create an entry point.

Step 2:

Attackers gain access

They now have a foothold inside the business.

Step 3:

They move through the network

Connected systems can become connected risks.

Step 4:

Business data becomes exposed

- Customer records
- Financial data
- Company files
- Email inboxes

Sensitive information may be accessible.

Step 5:

The impact spreads

- Downtime
- Lost productivity
- Financial cost
- Reputation damage

The problem rarely stays on one device.

Protect every device

- Security updates
- Multi-factor authentication
- Device monitoring
- Strong passwords
- Staff training

Your security is only as strong as your weakest device.
Need help keeping your devices secure?

Get in touch.

DSP IT SOLUTIONS

PASSKEYS:
THE LOGIN THAT CAN'T BE PHISHED

Passwords are the weak point in most businesses People reuse them, write them down, and type them into fake login pages. Passkeys replace them: you sign in with the same fingerprint, face, or PIN you use to unlock your phone, and there's no password for anyone to steal, guess, or phish.

- Why they're safer: nothing to phish, nothing for a hacker to steal in a breach, and nothing to reus or forget.
- Where they work: Microsoft, Google, and Apple accounts, plus a growing list of banks and business tools.
- Included with Microsoft 365 at no extra cost.
- They're faster: Microsoft says a passkey sign-in takes about 3 seconds, against 69 for a password plus a code.
- Two types: a synced passkey is backed up to your account and works across your devices, while a device-bound passkey stays on one device or a physical security key.
- Start with your most sensitive accounts: administrators, finance, and anyone who can move money.
- Let everyone else add a passkey alongside their password at first.
- Give each person a backup, like a second device or a security key, so a lost phone doesn't lock anyone out.
- Keep passwords for the few systems that don't support passkeys yet.

Passwords won't disappear overnight, but passkeys are the strongest login upgrade most businesses can make.

NEED A LAUGH

How is the letter 'A' like a flower?

Because a bee comes after it!

SEPTEMBER TRIVIA QUESTION

Test your knowledge!

The answer to last month's question was b) 24, a horse's maximum output is about 18,000W which is equivalent to 24 horsepower. Do you know the answer to the question below? The answer will be in next month's Newsletter.

Do you know how tall Mount Everest actually is?

a) 6.9km
b) 10.2km
c) 7.5km
d) 8.8km

TALKING TECH TIP

Stop Spam Meetings from Auto-Filling Your Calendar

By default, Outlook adds every meeting invite to your calendar the moment it arrives, even before you've responded. Turn off "Auto-process invitations" in Outlook settings so nothing lands on your calendar until you accept it.