June 2026

TALKING TECH

Helping your business

WHAT OUR CLIENTS SAY:

Thank you so much! Super job as usual.

Melissa - Gracie's Lane

Very prompt service. Much appreciated.

Roxy - After-care Australasia

DID YOU KNOW?

Snails have teeth!

Their teeth can be found all over its file-like tongue.

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 June 2026 newsletter.

One of the biggest trends we continue to see is that most security incidents don't start with complex attacks — they start with everyday habits. Reused passwords, personal accounts on work devices, and quick decisions made under pressure remain some of the easiest ways for cyber risk to creep into a business.

This month's feature focuses on why human behaviour is such a critical part of modern security, and how smart controls can reduce risk without getting in the way of how people actually work. You'll also find practical reminders and checklists to help you review access, backups, and authentication before small gaps become bigger problems.

As always, our goal is to help you stay ahead of risk with clear, practical advice that fits real-world businesses.

Shane Rajasinghe
General Manager – DSP IT Solutions

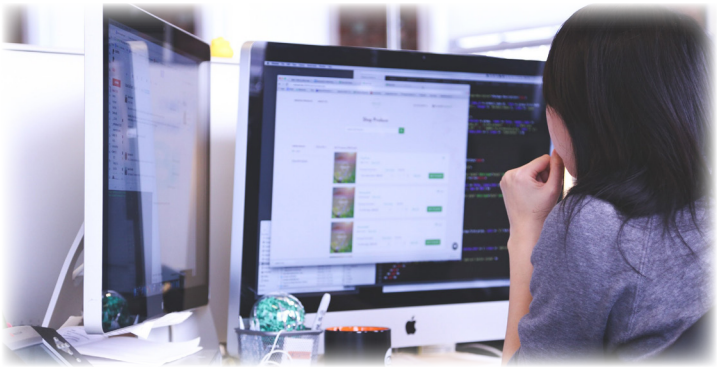
#SuperResponsive #BuildRelationships #AlwaysLearning #MakeComplexSimple #NothingIsTooHard

WHY HUMAN HABITS ARE YOUR BIGGEST SECURITY RISK

Most cyberattacks do not start with a sophisticated intrusion. They start with a click on a personal email, a reused password, or a file uploaded to a familiar cloud service because the approved option felt slower.
The Verizon Data Breach Investigations Report found that 68% of breaches involve the human element.
Not a zero-day exploit. Not a brute-force attack on a hardened system. Human behaviour, in the course of an ordinary working day.
For businesses running cloud-based workflows across multiple devices, the personal and professional overlap is now the rule.
Understanding where that overlap creates risk is no longer optional. It is a core part of modern security strategy.

How Personal Web Habits Create Business Exposure

Personal channels are phishing's preferred territory.
Personal inboxes, messaging platforms, and social media feeds are where phishing thrives. These environments are harder to filter, easier to spoof, and loaded with the emotional triggers that make people act before they think. When those channels share a device or browser with business systems, a single click can cross the boundary instantly.
Phishing is the most common entry method for attackers precisely because it exploits distraction rather than technical weakness. The target does not need to be
careless. They just need to be busy.
Password reuse is one of the most direct connections between personal and professional exposure.
When credentials from a personal account are compromised, attackers run them against business systems automatically. This technique, credential stuffing, is low-effort and highly effective because so many people use the same password across multiple accounts.
Unique credentials for every account, combined with multi-factor authentication, break that chain.
A personal breach has nowhere to go when the work account requires a second factor that the attacker cannot relay.



Why Blocking Behaviour Doesn't Work

The instinct is to lock things down: block personal apps, restrict browsing, enforce strict device policies.
In practice, blanket restrictions rarely stop the behaviour. They relocate it. Users find workarounds. Unapproved tools move to personal devices. IT teams lose visibility into exactly the activity they were trying to manage.
The risk does not disappear. It moves somewhere harder to see.
Security strategies that assume perfect compliance perform poorly in real workplaces.
The goal is not eliminating the overlap between personal and professional digital activity. It is managing it without breaking how people work.

What Actually Reduces Risk

The controls that work are the ones that match how people actually operate.

• Separate contexts, not people.

The simplest way to reduce crossover risk is to reduce crossover. Separate browser profiles for work and personal activity, clear guidance on where business accounts should be accessed, and identity boundaries that prevent accidental mixing all reduce exposure without restricting what people do with their time.

• Design for credential failure.

Assume passwords will eventually be exposed somewhere. Design for that outcome rather than hoping to prevent it. CISA reports that enabling multi-factor authentication makes accounts 99% less likely to be compromised, even when the underlying password has already been stolen.

Make secure behaviour easier than unsafe behaviour

Contact us or schedule a consultation to review current controls and identify where the most important gaps are.

When did you last...?

A quick check-in for any business owner

- ☐ **Test your backups?**
  Do you frequently check if they can be restored?
- ☐ **Review who has access to your systems?**
  Ex-staff, old contractors, accounts nobody uses any more.
- ☐ **Update your software and devices?**
  All of them, not just the ones that remind you.
- ☐ **Change your admin passwords?**
  Especially if anyone who knew them has left.
- ☐ **Check what devices are connected to your network?**
  Personal phones, old laptops, forgotten equipment.
- ☐ **Look at your cyber insurance policy?**
  Do you have one? Does it still reflect how your business operates?
- ☐ **Talk to your IT support partner about what's changed in your business?**
  New staff, new software, new ways of working all create new risks.

If you *can't remember* the last time you did any of these, it's time to get to work.

We can help you get on top of it (and stay on top of it).
Get in touch.

DSP IT SOLUTIONS

THE PASSKEY MIGRATION CHECKLIST

Transitioning to a passwordless environment doesn't have to happen overnight. Use this checklist to guide your team through a secure and efficient passkey migration.

Audit Your Platform Support
Identify which of your current tools already support passkeys natively.

Prioritise High-Risk Users
Begin your rollout with administrators and power users.

Implement a Parallel Authentication Phase
Allow users to authenticate with passkeys on enrolled devices while keeping passwords as fallback.

Bridge Gaps with Password Managers
For tools that do not yet support passkeys, utilise a password manager.

Establish Recovery & Sync Protocols
Ensure users understand how passkeys sync across their ecosystem (such as iCloud Keychain or Google Password Manager).

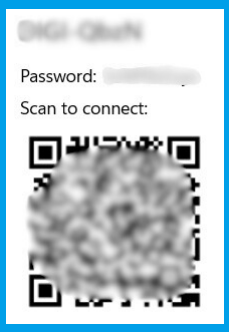
NEED A LAUGH

What do you call birds that stick together?

Vel-crows!

TALKING TECH TIP

Share Wi-Fi instantly with a QR Code



In Windows 11, navigate to Settings > Network & Internet > Wi-Fi, click your current network, and hit the Show button next to your password to instantly generate a QR code on your screen.

JUNE TRIVIA QUESTION

Test your knowledge!

The answer to last month's question was
d) World Server Throwing Championship.
Do you know the answer to the question below?
The answer will be in next month's Newsletter.

Which of these is the oldest web browser still in general use and development?

a) Internet Explorer
b) Lynx
c) Mosaic
d) Netscape

Love what we do?

Refer a friend and let us thank you!

Scan the QR code to go to our referral page. Your referral is the biggest compliment we can get.