July 2026

TALKING TECH

Helping your business

WHAT OUR CLIENTS SAY:

> Fantastic service. Thanks for being so prompt in fixing my problem. GoldStar!!
> *Emmy*
> *Grace Professional Services*

> Very prompt service and rectified issue. Pleasant to work with.
> *Roxy*
> *After-care Australasia*

DID YOU KNOW?

There are over 455 million websites that use WordPress, meaning that the WordPress market share is 35% of all websites in the world!

FROM SHANE'S DESK:

Welcome to the new financil year. July already, it will be Christmas before we know it! I hope you find our July Newsletter relevant and insightful.

QR codes have quickly become part of everyday business — but they're also opening the door to a new wave of cyber threats known as "quishing." It's a simple tactic that bypasses traditional security and relies on us acting without thinking.

The takeaway is straightforward: treat every QR code with caution, especially in emails, invoices, or documents. A few small changes in behaviour can significantly reduce your risk.

If you're not sure whether your systems, or your team are protected against these newer threats, now's the time to act. Reach out to us for a quick security check and make sure your business isn't an easy target.

Have a great month.

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

#SuperResponsive #BuildRelationships #AlwaysLearning #MakeComplexSimple #NothingIsTooHard

QUISHING: The New Phishing Scam

A few years ago, scanning a QR code felt suspicious.

Today, you probably scan three or four a day without thinking about it... parking meters, restaurant menus, product instructions, charging stations, etc.

And because of that, there's now an entire category of attack called "quishing," which is just phishing delivered through a QR code instead of an email link.

Authorities started issuing public warnings about it in 2024. Since then, reported attacks have jumped over 600%, and small businesses are getting hit harder than anyone.

Think about what happens when a phishing email lands in your inbox.

Your email provider scans it for known threats, and your IT setup flags suspicious links.

But none of that exists with a QR code. You point your phone at a square of black-and-white dots, and you have no idea where it's about to send you until you're already there.

By the time the fake Microsoft 365 login page loads on your phone, you've also stepped outside your company's security stack.

And your personal phone isn't running the same protections as your work laptop.

So, these attacks usually arrive in one of three ways.

Someone prints a fake QR sticker and slaps it over the real one on a parking meter, EV charger, or restaurant menu.

An attacker embeds a QR code inside a PDF attachment. The code slips past email filters that only scan text links.

Or a flyer, business card, or conference poster sends you to a fake landing page that drops malware on your phone or steals your login.

Three habits will keep your team safer:

1. Treat every QR code like an unknown link.
If a code arrives in an email, a PDF, or a text message, don't scan it. Go to the company's real website yourself and find what you need from there.

2. Make accounts payable a QR-free zone.
Any invoice, payment portal, or "click here to verify" that arrives as a QR code is a hard no. Your team should only pay through known logins they type into the browser themselves, never through a code embedded in a document.

3. Look for tampering on physical codes.
Before you scan a QR in the wild, check if it's a sticker laid over another sticker. Run your fingernail along the edge. If it peels, walk away. Genuine QR codes are usually printed onto the surface, not stuck on top.

If you'd like us to check whether your team's phones and email gateway are set up to flag malicious QR codes, get in touch.

Still saving files to your desktop, a hard drive, or a USB stick?

Here's what that decision means for your business.

If a staff member leaves

Cloud: Access removed centrally in minutes
Local: Files may leave with them

Collaboration

Cloud: Multiple people can work on the same file simultaneously
Local: One person at a time. Version chaos is likely

Recovery

Cloud: Files backed up automatically and restorable quickly
Local: Gone if the device is lost, stolen, or damaged

Security

Cloud: Managed permissions, encryption, and access controls
Local: Anyone with physical access can take it

MANAGED CLOUD STORAGE

VS

LOCAL STORAGE

Version history

Cloud: Previous versions saved automatically
Local: Overwritten and gone

Access

Cloud: From any device, anywhere, any time
Local: Only on the device it's saved to

If a device fails

Cloud: Nothing lost
Local: Potentially everything lost

USB sticks get lost. Hard drives fail. Laptops get stolen. Managed cloud storage means your business keeps working regardless.

We can help you move to a setup that's secure, accessible, and built for how your team works.

Get in touch.

DSP IT SOLUTIONS

THE 5 MINUTE BROWSER EXTENSION SECURITY CHECK

Why Browser Extensions Deserve a Second Look
Browser extensions can boost productivity, block ads, and streamline workflows—but they also have access to nearly everything you do online. Many extensions can read your passwords, track your browsing history, and access sensitive business data. The good news? A quick five minute vetting process can help you separate legitimate tools from potential security risks.

What Makes Extensions Risky?

Extensions operate with elevated permissions inside your browser. Unlike regular websites, they can monitor your keystrokes, modify web pages, and transmit data to third parties. Kaspersky emphasizes that before installing any extension, you should always check the publisher's reputation, read user reviews, scrutinize the requested permissions, and review the privacy policy to understand how your data will be handled. For small businesses where employees access financial systems, customer databases, and proprietary information through their browsers, a compromised extension can become a gateway to your entire network.

The 5 Minute Vetting Checklist:

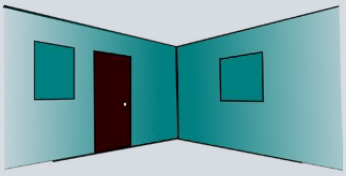
- Verify the publisher identity: Check if the extension comes from a known company or developer with a verifiable web presence and contact information.
- Review the permission requests: If a simple calculator extension asks to "read and change all your data on all websites," that's a red flag. Permissions should match functionality.
- Read recent user reviews: Sort by newest first and look for patterns of complaints about suspicious behaviour, performance issues, or recent changes after updates.
- Check the last update date: Extensions abandoned for over a year may contain unpatched security vulnerabilities. Active maintenance is a good sign.
- Search for the extension name plus "security" or "malware: A quick web search can reveal if security researchers have flagged the extension or if it's been removed from stores previously.
- Examine the privacy policy: Cloudflare recommends that users only install extensions from official stores and carefully review what data is collected and whether it's shared with third parties.

Take these five minutes before clicking "Add to Browser"—your business data is worth the wait.

NEED A LAUGH

What did one wall say to the other wall?

I'll meet you at the corner!



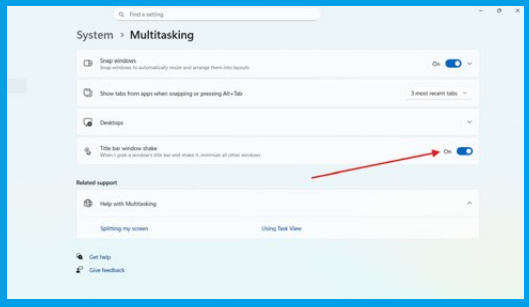
JULY TRIVIA QUESTION

Test your knowledge!
The answer to last month's question was b) Lynx. Originally developed in 1992, it remains one of the oldest actively maintained web browsers. Do you know the answer to the question below? The answer will be in next month's Newsletter.

The biggest butterfly in the world has a wingspan of:
a) 31cm
b) 35cm
c) 28cm
d) 25cm

TALKING TECH TIP

Shake to Minimise (Aero Shake)



If your screen is cluttered with too many open windows, click and hold the top bar of the one you want to focus on and give your mouse a quick "shake." This instantly minimises everything else in the background.
Shake it again to bring them all back!