

November 2026

TALKING TECH

Helping your business

WHAT OUR CLIENTS SAY:

> The service and professionalism provided to rectify my issue was fantastic, thank you very much.
> Paul,
> After-Care A'sia

> Professional, polite and knowledgeable. My problem was resolved very quickly. It is always a pleasure to speak with a DSP consultant.
> Emily,
> Unique Building Services

DID YOU KNOW?

The Moon is gradually drifting away from the Earth. The distance is around 3cm every year.



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



FROM SHANE'S DESK:

Strong security doesn't have to be complicated.

Small steps such as using individual logins, keeping devices up to date, and understanding how to respond to a data breach can make a significant difference to protecting your business.

Consistent attention to cybersecurity helps build resilience, protect customer trust, and keep your business running smoothly.

This month, I encourage you to take a few minutes to review your systems and ensure you're prepared before issues arise.

By taking action now, you can reduce risk and ensure your business is better prepared for whatever comes next.

A few simple steps today can help protect your business from costly disruptions tomorrow.

Have a great month!

Shane Rajasinghe
General Manager

#SuperResponsive #BuildRelationships #AlwaysLearning #MakeComplexSimple #NothingIsTooHard

WHAT TO ASK A SOFTWARE VENDOR

after they report a data breach

A breach notice from your payroll provider, accounting platform, CRM, or another software vendor may arrive before the company has finished its investigation. You still need enough information to decide what your business should do next.

First, confirm that the notice is genuine. Go to the vendor's website or customer portal using an address you already know. Criminals sometimes send fake password-reset or support messages after a public breach announcement.

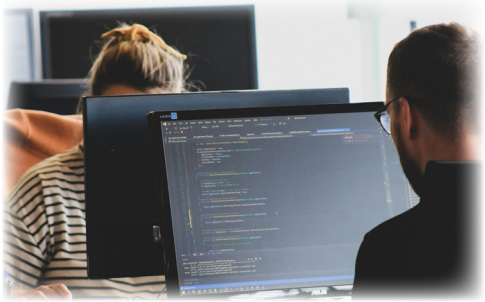
Once the notice is confirmed, ask whether your business was affected and what information was involved. Find out when the unauthorised access began, when the vendor detected it, and when the vendor contained it. Ask whether the person could view, copy, change, or delete information.

Also ask whether API keys, access tokens, single sign-on connections, or integrations with your email, accounting, payment, storage, or backup systems need to be reset or revoked.

If the vendor says there is no evidence that information was copied or misused, ask what logs support that statement and whether they cover the full period under investigation.

Get the vendor's instructions in writing. You may need to install an update, reset certain accounts, review transactions, disconnect an integration, or warn employees about related scams.

Keep the original notice, later updates, your questions, the vendor's answers, and a record of what your business did. Depending on the information involved and where your business operates, you may also need advice from your IT provider, insurer, privacy specialist, or legal adviser.





WHY SHARED LOGINS ARE A SECURITY RISK FOR YOUR BUSINESS

A shared login may seem convenient when several employees need the same software, mailbox, or website account. If a payment changes, customer information is downloaded, or the account signs in from an unfamiliar device, the account history may show every action under the same username.

Shared passwords also spread through messages, documents, browsers, and personal password stores. When an employee leaves, the password must be changed everywhere it is used or that person may keep access.

Give each employee their own account wherever the software allows it. Individual accounts let you remove one person's access, apply multifactor authentication properly, match permissions to the employee's work, and trace activity to a named user.

If an older system only provides one login, keep the password in a business password manager. Limit access to the employees who need it, name an owner for the account, and change the password whenever someone leaves the authorised group.

What happens during an **IT review?**

STEP 1

Review your devices

Are they secure, healthy and up to date?

STEP 2

Check your security

Could cyber criminals find an easy way in?

STEP 3

Review user access

Does everyone have the right access?

STEP 4

Protect your data

Could you recover if something went wrong?

STEP 5

Look for improvements

Where can technology save time?

STEP 6

Create an action plan

Prioritise the most important actions.

A good IT review means finding **opportunities**, *not faults.*

Ready to review your technology from top to bottom?

Get in touch.

dsp IT SOLUTIONS

dsp IT SOLUTIONS dsp IT SOLUTIONS dsp IT SOLUTIONS

HOW LONG BUSINESS COMPUTERS LAST

and when to replace them



Three to five years is a practical replacement range for many business computers, but age alone should not decide it. Start reviewing each device at three years, then check its security support, reliability, performance, warranty, and repair history.

Security comes first. Replace a computer if it cannot run an operating system that still receives security updates or the software your business requires. A computer that still runs well may need replacing if its operating system is no longer supported.

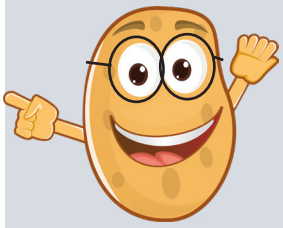
Have a slow computer checked before replacing it. Low storage, insufficient memory, overheating, malware, or an operating-system problem can all affect performance. An upgrade may be worthwhile if the computer remains supported and reliable.

Keep a replacement schedule with the purchase date, assigned user, warranty expiry, operating system, and review date for every computer. This lets you spread purchases across several budget periods.

Before an old computer is sold, donated, recycled, or returned, transfer the required data and have its storage properly erased. Deleting files or removing an account does not guarantee that the information is gone.

Ask your IT provider to review your computers at least once a year. If you do not have an IT provider, feel free to reach out to us and we'll help you plan the replacements.

NEED A LAUGH



What do you call a potato wearing glasses?

A Spec-Tater!

NOVEMBER TRIVIA QUESTION

Test your knowledge!

The answer to last month's question was a) 38 years. Quite a feat when you consider most domestic cats live for an average of 15 years.
Do you know the answer to the question below? It will be in next month's Newsletter.

How heavy was the first mobile phone developed by Motorola in 1973?

a) 2kg
b) 1kg
c) 1.5kg
d) 2.2kg



TALKING TECH TIP

Spot edits in a returned document

In Word for Windows, select Review > Compare > Compare and choose both versions. Word shows what changed, even without Track Changes.



DSP Communications

Delivering better.
Better service.
Better phones & Internet.

Need help with your communications?
www.dspcommunications.com.au