InTech News

ISSUE 202646

Fortnight ending 8 November 2026

Five things worth two minutes of your time.

Four things worth knowing from the past fortnight, and one worth doing something about.

INTERESTING

Google's AI search answer will suggest a password, and hands many people the same one

Search Google for "generate a password" and the AI Overview at the top of the results can now suggest one. SEO consultant Natalia Witczyk pointed out that Google pre-computes these answers for common searches, so the same "random" password can be served to many people. PCMag tested it and saw the same password across different Google accounts and devices, in Incognito mode and over several days. It only appeared when signed in to a personal Google account, not a business account or when signed out.

> **What this means for you:** AI is a productivity tool, not a security tool. Use a password manager to generate and store passwords, and make sure every account has a unique one. Reused or predictable passwords remain one of the easiest ways for attackers to gain access.

Source: pcmag.com

CYBER SECURITY

SonicWall firewalls have a VPN sign-in flaw that attackers are already using

On 6 November SonicWall released updates for seven flaws in SonicOS, including one in its SSL-VPN that can let someone get around SAML sign-in, and potentially the multi-factor check attached to it. The US cyber agency CISA added it to its catalogue of vulnerabilities known to be exploited the same day. It only affects firewalls with SSL-VPN set up to use SAML, and SonicWall says there is no workaround, only the update.

> **What this means for you:** If your office has a SonicWall firewall that staff use for remote access, ask your IT provider one question: has it been updated since 6 November, and does it use SAML for VPN sign-in? If you have a different brand of firewall, nothing here applies to you. Treat it as a quick confirmation, not an emergency.

Source: cisa.gov

MICROSOFT WORLD

Fake prize invitations are tricking staff into approving attackers on Microsoft 365

Security firm Push Security spotted phishing pages in late October posing as events from OpenAI, SpaceX and Anthropic, promising rewards such as free ChatGPT Pro. Choosing "Continue with Microsoft" shows the victim a code to type into Microsoft's genuine sign-in page. That approves the attacker's device and can give them access to the account without needing to steal the user's password.

> **What this means for you:** Tell your team that nobody should enter a code from a web page they landed on unprompted, and that a prize reached by signing in with a work account is a trap. Then ask whoever manages your Microsoft 365 whether sign-in by device code can be switched off, since most small businesses never need it.

Source: bleepingcomputer.com

APPLE WORLD

iOS 27.2 fixed well over 150 security flaws on 26 October

Apple released iOS 27.2 and iPadOS 27.2 on 26 October, alongside macOS 27.2 and updates for the previous generation of its systems. Apple's security notes list well over 150 fixes across WebKit, the kernel and image handling. None is marked as exploited in attacks.

> **What this means for you:** Don't ignore phone updates. Your smartphone now holds business email, MFA apps, cloud files, passwords and client information. Keeping iOS up to date is one of the simplest and most effective ways to reduce cyber risk and protect business data. To check, go to Settings, then General, then Software Update, and turn on automatic updates.

Source: support.apple.com

BUSINESS SMARTS

Before the Christmas break, write down who is reachable and who can approve

Problems do not wait for the holidays, and the people who would normally deal with them are away. The Australian Cyber Security Centre's reporting page lists the Australian Cyber Security Hotline, 1300 CYBER1 (1300 292 371), for reporting a cybercrime or incident.

> **What this means for you:** By the end of November, put one page together: who is contactable each day of the break, who can approve a payment or a change to bank details, and the hours your IT provider and your bank are covering. Put the hotline number on it. Then send it to whoever might be left holding the phone, so nobody is working out who to call at 9pm on Boxing Day.

Source: cyber.gov.au

ALSO ON THE 1300 INTECH BLOG

Benefits of Managed IT Services for Melbourne Businesses

Our latest post sets out seven benefits of managed IT, from a forecastable monthly cost to cover when someone is away. Each comes with what it looks like in practice and a question you can put to your own provider, and it is honest about when managed IT does not pay, so it suits owners deciding whether it is worth it.

Read it at **1300intech.com.au/blog/benefits-of-managed-it-services**

Three ways to stay informed

Take the ones you want, leave the ones you don't. Free resources for your SMB.

- **The IT Essentials Digest** (monthly) A single business focus, four of our best articles, condensed into a four-minute read: the key insight from each, what you might be missing, and how to apply it to your own business.
- **InTech News** (every second Wednesday) **This one.** Five things worth two minutes of your time. Something interesting, something on security, Microsoft, Apple, and one practical thing a Melbourne business owner can act on.
- **Blog posts** (every 2-3 weeks) An email whenever we publish. Longer pieces, one subject at a time, written for owners rather than IT departments.

To start getting any of these, **sign up on the web edition**. It takes a few seconds.

InTech News is curated by the team at 1300 InTech.
Something here you want to talk through? Email **helpdesk@1300intech.com.au** or call 1300 468 324.

Read this issue online at 1300intech.com.au/blog/newsletters/2026-week-46
Every issue: 1300intech.com.au/blog/tag/intech-news