

FEBRUARY 2026



TALKING TECH

HELPING YOUR BUSINESS



FROM ~~DAMIEN'S~~ Clients' Words . . . JO'S DESK:

Hi and welcome to the February 2026 Newsletter.

I decided to write the welcome this month and give Damien a break! I hope everyone has settled into the new year and that things are going to plan.

Did you know, that SMS codes are no longer enough for an MFA? We have a great article this month that explores what to use instead. We also look at how to conduct a simple 15-minute daily cloud checkup. (Pssst: If you have a great IT partner, they will manage this for you!).

This newsletter also contains an Infographic clearly showing why your staff is your strongest cyber shield. If you need help in bringing your team up to speed, get in touch, we can help.

I hope my 'Dad' joke this month gives you a smile 😊

Have an excellent month and stay safe.

Jo

*Super quick and nailed it. Thanks!
Kevin,
Unique Building Services*

*Thanks for fixing my password so quickly - really appreciate the great support!
Mika,
Inclusion Melbourne*

DID YOU KNOW?

There are more computers than people in the world!



The human population is around 8 billion and there are over 10 billion connected devices!



Love what we do?

Tell a friend and let us thank you!
Scan the QR code, your referral is the biggest compliment we can get.

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

THE MFA LEVEL-UP:

SMS codes are no longer enough; we explore what to use instead.

For years, enabling Multi-Factor Authentication (MFA) has been a cornerstone of account and device security. While MFA remains essential, the threat landscape has evolved, making some older methods less effective.

The most common form of MFA, four or six digit codes sent via SMS, is convenient and familiar, and it's certainly better than relying on passwords alone. However, SMS is an outdated technology, and cybercriminals have developed reliable ways to bypass it. For organisations handling sensitive data, SMS based MFA is no longer sufficient. It's time to adopt the next generation of phishing resistant MFA to stay ahead of today's attackers.

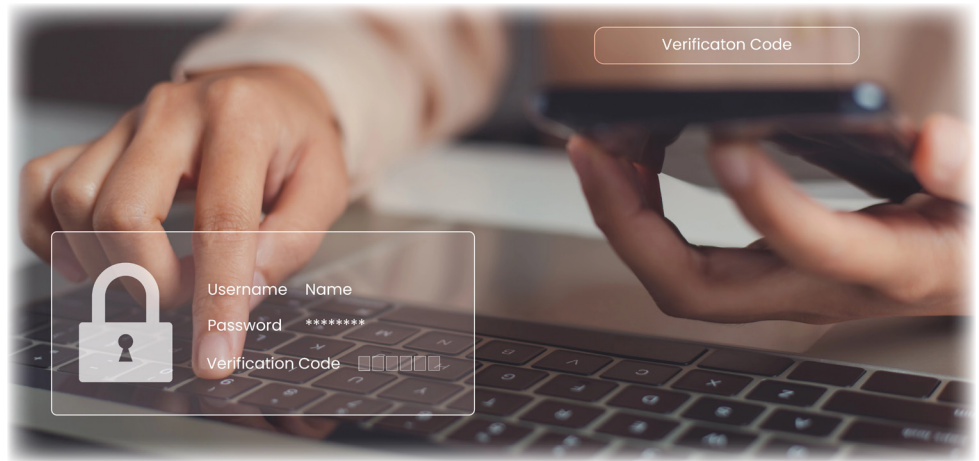
Why Phishing-Resistant MFA Is the New Gold Standard

To prevent these attacks, it's essential to remove the human element from authentication by using phishing resistant MFA. This approach relies on secure cryptographic protocols that tie login attempts to specific domains.

One of the more prominent standards used for such authentication is Fast Identity Online2 (FIDO2) open standard, that uses passkeys created using public key cryptography linking a specific device to a domain. Even if a user is tricked into clicking a phishing link, their authenticator application will not release the credentials because the domain does not match the specific record.

Implementing Hardware Security Keys

Hardware security keys are physical devices resembling a USB drive, which can be plugged into computer or tapped against a mobile device. You simply insert the key into the computer or touch a button, and the key



performs a cryptographic handshake with the service. This method is quite secure since there are no codes to type, and attackers can't steal your key over the internet. Unless they physically steal the key from you, they cannot access your account.

Mobile Authentication Apps and Push Notifications

If physical keys are not feasible, mobile authenticator apps such as Microsoft or Google Authenticator are a step up from SMS or MFA.

These apps generate codes locally on the device, eliminating the risk of SIM swapping or SMS interception since the codes are not sent over a cellular network.

There are still risks. For example, attackers may flood a user's phone with repeated login approval requests, causing a frustrated or confused user to "approve" just to stop the notifications. Modern authenticator apps address this with "number matching," requiring the user to enter a number shown on their login screen into the app. This ensures the person is physically present at their computer.

Passkeys: The Future of Authentication

Modern systems are embracing passkeys, digital credentials stored on a device and protected by biometrics. Passkeys are phishing resistant and can be synchronized across your ecosystem, such as iCloud Keychain or Google Password Manager. They offer the security of a hardware key with the convenience of a device that you already carry.

Your staff = your strongest cyber shield

(But only if they're trained right)



Suspicious emails

Train them to spot



Dangerous links



Fake login screens



Money or gift card requests



Weird attachments



Phoney password resets



"Act now!"
pressure tactics

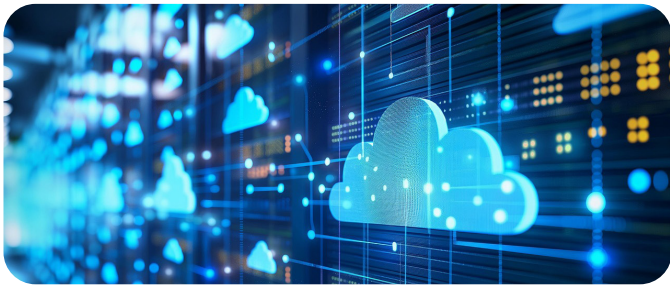


A trained team
blocks more
attacks than
any software

Empowered people
= safer business

We can help bring your team up to speed.
Get in touch.

dsp IT
SOLUTIONS



A SIMPLE 15-MINUTE DAILY CLOUD CHECKUP ROUTINE

Review Access Logs

Look for logins from unusual locations or at strange times.

Check for Storage Permissions

Review the permission settings on your storage buckets and ensure that your private data remains private.

Monitor for Resource Spikes

Check for any unexpected spikes in computing power and compare each day's metrics.

Examine Security Alerts and Notifications

These often contain critical information about vulnerabilities.

Verify Backup Integrity

Check the status of your overnight backup jobs.

Keep Software Patched and Updated

Make sure automated patching schedules are running correctly.

Note: If you have a great IT partner (managed support provider) they will look after all of this for you!

POLICIES FOR EMPLOYEES WORKING FROM PUBLIC PLACES

Mandate VPN Usage:

Employees must use VPN to encrypt all data and establish a secure tunnel over public Wi-Fi.

Prevent Visual Hacking:

Issue and require the use of privacy screens to prevent passersby from glancing and stealing sensitive information.

Maintain Physical Security:

Employees must keep their laptops and devices with them at all times.

Avoid Confidential Conversations:

Employees should not discuss sensitive business matters in public.

Create a Clear, Written Policy:

Publish a comprehensive remote work policy and set a regular review cadence.



NEED A LAUGH?

How do you throw a party in outer space?

You planet!

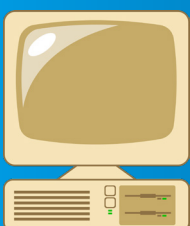


FEBRUARY TRIVIA QUESTION . . .

Test your knowledge!

The answer to last month's question was a) Red panda. Can you guess the answer to the trivia question below? The answer will be revealed in next month's newsletter.

Windows 1.0 was originally developed under what early project name?



- a) Interface Manager
- b) MS Panel System
- c) DOS Overlay
- d) GDOS