

NOVEMBER 2023



TALKING TECH

HELPING YOUR BUSINESS



FROM ~~DAMIEN'S~~ SHANE'S DESK:

While Damien is away I get to "put pen to paper" and I am delighted to share some exciting news with you this month. The Frankston & District Netball Association proudly unveiled the Jubilee Park Stadium to the public, and it's my pleasure to inform

you that DSP IT played an integral role in this endeavour. We were entrusted with the task of designing and implementing a robust customer network capable of accommodating over 3000 individuals. I must say, this project has been one of the most significant and rewarding undertakings in my career, and the final outcome speaks volumes about our commitment and expertise.

While we continue to celebrate this achievement, it's essential to acknowledge that the digital landscape is evolving, and with it, the threat of cyber-attacks and zero-day vulnerabilities is on the rise. In light of this, we strongly encourage all our valued clients, both current and prospective, to take proactive measures in safeguarding their businesses and infrastructure against such threats.

We suggest that every business takes the time to assess their current security posture, understanding what their security baseline entails. If you find yourself in need of guidance on comprehending and implementing a security baseline tailored to your unique business requirements, please don't hesitate to reach out. I would be delighted to assist you in ensuring your digital assets remain secure and resilient.

Your security and success are of utmost importance to us, and we are here to support you in every way possible. Feel free to contact us anytime with your inquiries or concerns.

Stay safe and take care,



Shane Rajasinghe - General Manager
DSP IT Solutions

DID YOU KN W?



The word "strengths" is the longest word in the English language with one vowel.



DSP COMMUNICATIONS



We have 5G and 4G mobile phone plans to suit your business needs

Call us on 03 9001 0817 or visit dspcommunications.com.au to find out how we can help you

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

WHAT IS SAAS RANSOMWARE? HOW CAN YOU DEFEND AGAINST IT?

Software-as-a-Service (SaaS) has revolutionised the way businesses operate. But alongside its benefits, SaaS brings with it potential threats. When software and data are online, they're more vulnerable to attacks. One of the latest threats to move from endpoint devices to the cloud is ransomware.

Between March and May of 2023, SaaS attacks increased by over 300%. A study in 2022 by Odaseva found that 51% of ransomware attacks targeted SaaS data.

What is SaaS Ransomware?

SaaS ransomware is also known as cloud ransomware. It's malicious code designed to target cloud-based applications and services. These include services like Google Workspace, Microsoft 365, and other cloud collaboration platforms.

Defending Against SaaS Ransomware

Educate Your Team

Start by educating your employees about the risks of SaaS ransomware. Include how it spreads through phishing emails, malicious links, or breached accounts. Teach them to recognise suspicious activities and report any unusual incidents immediately.

Enable Multi-Factor Authentication (MFA)

MFA is an essential layer of security. Enabling MFA reduces the risk of unauthorised access. This is true, even if a hacker compromises an account's login credentials.

Regular Backups

Frequently backing up your SaaS data is crucial. Having up-to-date backups ensures that you can restore your files. You won't need to pay the attacker's ransom demands.

Apply the Principle of Least Privilege

Limit user permissions to only the necessary functions. By doing this, you reduce the potential damage an attacker can do if they gain access.

Keep Software Up to Date

Ensure that you keep all software up to date. Regular updates close known vulnerabilities and strengthen your defence.

Deploy Advanced Security Solutions

Consider using third-party security solutions that specialise in protecting SaaS environments. These solutions can provide many benefits.

Including:

- Real-time threat detection
- Data loss prevention
- And other advanced security features

Track Account Activity

Put in place robust monitoring of user activity and network traffic. Suspicious behaviour can be early indicators of an attack. One example to watch for is several failed login attempts. Another is access from unusual locations.

Develop an Incident Response Plan

Prepare and practice an incident response plan. It should outline the steps to take in the event of a ransomware attack. A well-coordinated response can mitigate the impact of an incident. It can also aid in faster recovery. The sooner your team can respond, the faster business gets back to normal.

SUSTAINABLE TECH HABITS THAT ARE A WIN FOR YOUR BOTTOM LINE



Below are several sustainable tech habits you can adopt:

- Energy-efficient hardware and appliances
- Virtualisation and cloud computing
- Remote work and telecommuting
- Renewable energy sources
- E-waste recycling programs
- Optimise data centres
- Green web hosting
- Paperless office
- Eco-friendly office supplies
- Software optimisation
- Remote monitoring and control
- Green transportation policies
- Sustainable data practices
- Green IT certification
- Employee education and engagement
- Supply chain sustainability
- Lifecycle assessments
- Green marketing

WE LOVE REFERRALS . .

The greatest gift anyone can give us is a referral to your business colleagues/friends. Referrals help us keep costs down so we can pass the savings on to our clients. Simply introduce me via email to damien@dspit.com.au or (03) 9001 0817 and I'll take it from there.



FREE!

For your FREE copy of this book, go to:
<https://www.dspit.com.au/cybersecurity-essentials/>

10 BIGGEST CYBERSECURITY MISTAKES OF SMALL COMPANIES

Cybercriminals can launch very sophisticated attacks. But it's often lax cybersecurity practices that enable most breaches.

Small business owners often don't prioritise cybersecurity measures. They may be just fully focused on growing the company.

Below are some of the biggest reasons small businesses fall victim to cyberattacks:

- Underestimating the threat
- Neglecting employee training
- Using weak passwords
- Ignoring software updates
- Lacking a data backup plan
- No formal security policies
- Ignoring mobile security
- Failing to regularly watch networks
- No Incident Response Plan
- Thinking they don't need Managed IT Services

"SECURE-BY-DESIGN" CYBERSECURITY PRACTICES

Cybersecurity has become a critical foundation upon which many aspects of business rely. The frequency and sophistication of cyberattacks continue to increase. It's essential to shift from a reactive to a proactive cybersecurity approach, such as "Secure-by-Design."

"Secure-by-Design" integrates security measures into the very foundation of a system, app, or device. It does this from the start. It's about considering security as a fundamental aspect of the development process.

Key principles of "Secure-by-Design" include:

- Risk Assessment
- Standard Framework
- Least Privilege
- Defence in Depth
- Regular Updates
- User Education



The **TickTime Cube** is a digital countdown timer that's as easy to use as a light switch. It's a stylish, user-friendly gadget that helps you manage your time to help boost your efficiency and productivity. It's perfect for any tasks that needs a timer. It also comes in a variety of cool colors to match your style or mood. Get yours at <https://www.ticktime.store>

Why "Secure-by-Design" Matters

- Proactive Security
- Cost Savings
- Regulatory Compliance
- Reputation Management
- Future-Proofing
- Minimising Attack Surfaces

NEED A LAUGH?



How do scientists freshen their breath?

With experi-mints!

WIN A \$20 BUNNINGS GIFT CARD!



There was no winner from last month's trivia question. The answer was b) Made the computer run slower.

You could be the winner of this month's trivia question. Just contact us with the answer to the question below, (No Googling!) Good Luck!

What happens if a CD spins too fast?

- a) They're virtually indestructible by spinning
- b) It might separate the disc's layers
- c) It might explode
- d) It might melt

Call us with your answer
(03) 9001 0817 or email
jo@dspit.com.au