FROM DAMIEN'S DESK:

Well, here we are at the end of another financial year, I always joke once Christmas is over the end of the financial year is just around the corner. Once this happens, we are on the downhill run to Christmas. I think I am stuck in a loop!

As it is budget it time, it is worth reviewing unused software in your organisation. Unused software can be a financial drain on businesses, leading to unnecessary expenses. Companies often invest in tools that end up underutilised or forgotten, resulting in thousands of dollars wasted each year. Regular audits and careful planning can help mitigate this issue and optimise software spending.

Each year I take a look at DSP IT's licensing and make sure we are still getting bang for our buck.

Use the savings to invest in new technologies, like Microsoft CoPilot. Let us know if we can help.

Stay safe!

Damien Pepper - Director
dSP IT Solutions

WE LOVE REFERRALS

The greatest gift anyone can give us is a referral to your business friends.

Referrals help us keep costs down so we can pass on the savings to all our clients.

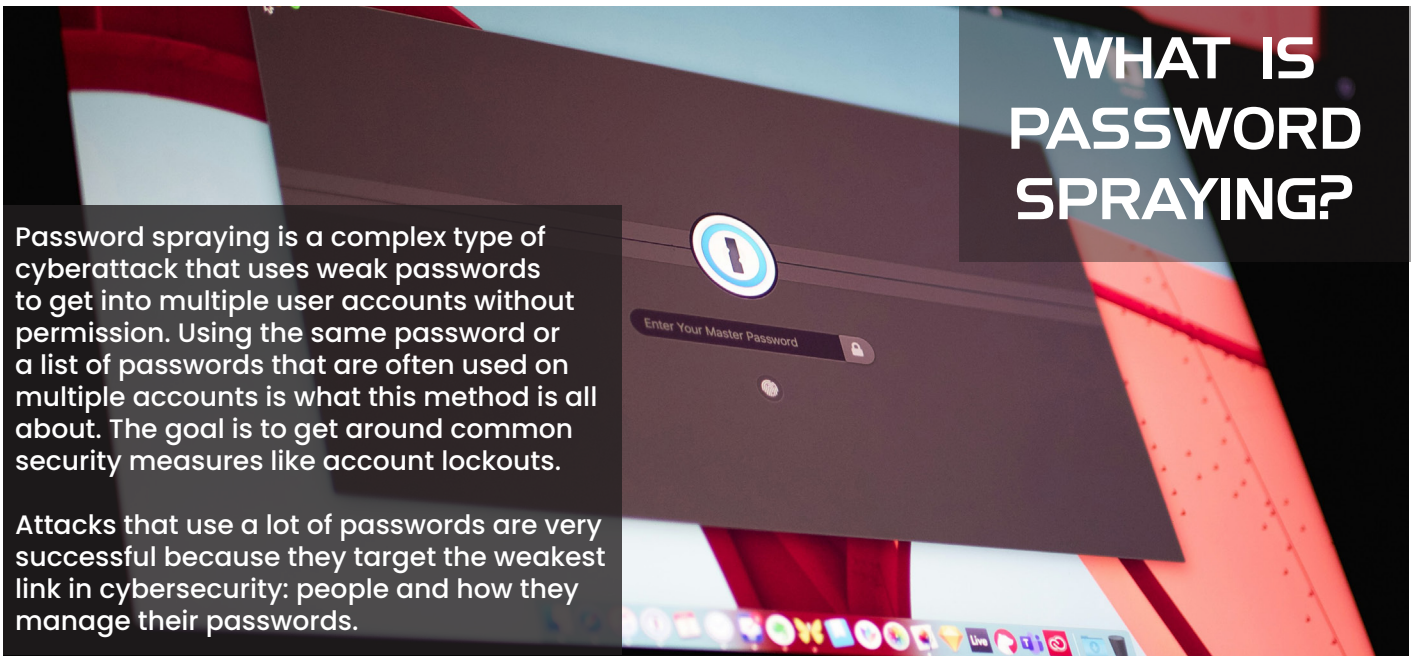
Simply introduce me via email damien@dspit.com.au or (03) 9001 0817 and I'll take it from there.

DID YOU KNOW?

In March 1984, the first commercial mobile phone, a motorola Dyna TAC 8000x, went on sale for $3,995.

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

#SuperResponsive #MakeTheComplexSimple #BuildRelationships #NothingIsTooHard #AlwaysLearning



WHAT IS PASSWORD SPRAYING?

Password spraying is a complex type of cyberattack that uses weak passwords to get into multiple user accounts without permission. Using the same password or a list of passwords that are often used on multiple accounts is what this method is all about. The goal is to get around common security measures like account lockouts.

Attacks that use a lot of passwords are very successful because they target the weakest link in cybersecurity: people and how they manage their passwords.

What Is Password Spraying and How Does It Work?

A brute-force attack called "password spraying" tries to get into multiple accounts with the same password. Attackers can avoid account shutdown policies with this method.

Attackers often get lists of usernames from public directories or data leaks that have already happened. They then use the same passwords to try to log in to all of these accounts. Usually, the process is automated so that it can quickly try all possible pairs of username and password.

Password spraying has become popular among hackers, even those working for the government, in recent years. Because it is so easy to do and works so well to get around security measures, it is a major threat to both personal and business data security. As cybersecurity improves, it will become more important to understand and stop password spraying threats.

How Does Password Spraying Differ from Other Cyberattacks?

Password spraying is distinct from other brute-force attacks in its approach and execution. While traditional brute-force attacks focus on trying multiple passwords against a single account, password spraying uses a single password across multiple accounts.

Understanding Brute-Force Attacks

Brute-force attacks involve systematically trying all possible combinations of passwords to gain access to an account. These attacks are often resource- intensive and can be easily detected due to the high volume of login attempts on a single account.

Comparing Credential Stuffing

Credential stuffing involves using lists of stolen username and password combinations to attempt logins.

How Can Organisations Detect and Prevent Password Spraying Attacks?

Detecting password spraying attacks requires a proactive approach to monitoring and analysis. Organisations must implement robust security measures to identify suspicious activities early on.

- **Implementing Strong Password Policies**

Organisations should adopt guidelines that ensure passwords are complex, lengthy, and regularly updated.

- **Deploying Multi-Factor Authentication**

Multi-factor authentication (MFA) significantly reduces the risk of unauthorised access by requiring additional verification steps beyond just a password.

- **Conducting Regular Security Audits**

Regular audits of authentication logs and security posture assessments can help identify vulnerabilities that could facilitate password spraying attacks.

- **Enhancing Login Detection**

Organisations should set up detection systems for login attempts to multiple accounts from a single host over a short period. Implementing stronger lockout policies that balance security with usability is also crucial.

- **Educating Users**

Users should be informed about the risks of weak passwords and the importance of MFA.

- **Incident Response Planning**

This plan should include procedures for alerting users, changing passwords, and conducting thorough security audits.

Taking Action Against Password Spraying

To enhance your organisation's cybersecurity and protect against password spraying attacks, contact us today to learn how we can assist you in securing your systems against evolving cyber threats.

Stop wasting money on unused software

Are you paying for software no one's using? Many businesses are.

53%
of software applications go unused or underutilised.

Enterprise businesses waste
$33 MILLION
a year on unused licenses.

Maybe you're not wasting millions... but a few hundred a month adds up fast.

How to cut the waste

Audit your software
Look at what you're using. Cancel what you're not.

Review subscriptions regularly
Set a reminder every 3–6 months to review license use.

Assign software properly
Make sure licenses go only to people who need them.

Check for overlap
Many tools do the same job - do you really need five project management apps?

Got a Microsoft 365 subscription?

You might already be paying for tools that Microsoft 365 does better, for no extra cost. Tools like:

- **Teams** (video calls & chat)
- **OneDrive** (cloud storage & file sharing)
- **Planner** (task management)
- **Forms** (surveys & feedback)
- **SharePoint** (intranet & collaboration)
- **Bookings** (online scheduling)

Need help reviewing your software?
Get in touch.

DSP IT SOLUTIONS

NEED A LAUGH?

What Dr. Seuss character likes to make side comments on Zoom?

The Cat in the Chat!

BEST PRACTICES FOR DATA MANAGEMENT

1. Transparency and Consent

Websites should clearly communicate how user data is collected and used. Users should have the option to opt-in or opt-out of data collection, and they should be able to access, modify, or delete their personal information.

2. Data Minimisation

Collecting only the data that is necessary for the website's functionality.

3. Secure Data Storage

Encrypting data both at rest and in transit ensures that it remains secure even if intercepted. Regular security audits and updates are also crucial to prevent vulnerabilities.

4. User Control

Providing users with tools to manage their data preferences fosters trust and accountability. This includes options to download, edit, or delete personal information.

JUNE TRIVIA QUESTION . . .

Test your knowledge!

The answer to last month's question was b) 2012. Can you guess the answer to June's trivia question below? The answer will be revealed in next month's newsletter.

What was the first search engine on the internet?

a) Archie
b) Google
c) Bliss
d) Emily