FROM DAMIEN'S DESK:

Wow, can you believe it's already March? Time really does fly! Before we know it, the leaves will be changing colours and the cooler weather will be here.

I'm excited to share that we have a YouTube channel where I post a fun weekly video! It covers all the latest changes in software, along with handy hints and tips for security and the newest tech. I'd love for you to check it out here: https://www.youtube.com/@dsp-it

In this month's newsletter, we've put together a helpful 10-point plan to keep your data safe. And remember, if you have any questions or need assistance with this, feel free to reach out.

We're here to help!

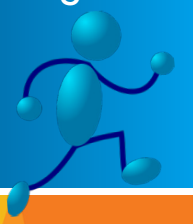
Looking forward to connecting next month!

Damien Pepper - Director
dSP IT Solutions

DID YOU KNOW?

There's a precise speed where jogging becomes running -

9.7 km hour!



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

GUIDE TO SECURE FILE STORAGE AND TRANSFERS

File storage and transferring is very important to most business owners. However, the safety of files is really tough to maintain. In this guide, we are going to help you protect your files. We will explore ways to store and send files securely.

What is secure file storage?

Secure file storage protects your files. It prevents others from accessing your files or altering them in any way. Good storage grants protection to your files using locks. You alone can unlock such files.

Types of secure storage

Files can be stored securely in various ways, as listed below.

- Cloud
- External hard drives
- Encrypted USB drives

Cloud storage saves files on the internet. External drives save files on a device you can hold. Encrypted drives use special codes to lock files.

Why is secure file storage important?

Secure storage keeps your information private. It stops thieves from stealing your data. It also helps you follow laws about data protection.

Risks of unsecured storage

Unsecured files can lead to huge troubles, including but not limited to the following:

- Identity theft
- Financial loss
- Privacy breaches

These risks give a reason why secure storage is important. You need to protect your personal and work files.

How Can I Make My File Storage Safer?

You can do so many things to make your storage safer, such as:

- Using strong passwords
- Enabling two-factor authentication
- Encrypting your files
- Keeping your software up to date frequently

Strong passwords are hard to guess. Two factor authentication adds an extra step to log in. Encryption scrambles your files so others can't read them. Updates fix security problems in your software.

Best practices for passwords

Good passwords are important in keeping your files safer. Here are some tips:

- Use long passwords
- Mix letters, numbers, and symbols
- Don't use personal info in passwords
- Use different passwords for each account

What is secure file transfer?

Secure file transfer is a way of sending files safely between individuals or devices. It prevents unauthorised access to files and prohibits modification of files while in transit. The better methods of transfer protect the files with encryption.

Common secure transfer methods

Here are several ways to securely transfer files:

- Secure FTP (SFTP)
- Virtual Private Networks (VPNs)
- Encrypted email attachments
- Secure file-sharing services

How to Transfer Files Safely?

These steps will keep your files safer while in transit:

- Select a secure method of transfer
- Encrypt the file before you send it
- Give strong passwords for file access
- Authenticate the recipient
- Send the access details separately

How to email attachments safely

- Encrypt important attachments
- Use a secure email service
- Avoid writing sensitive information in the body of an email
- Double-check the recipient's email address

Ready to Secure Your Files?

Protect your data from thieves and snoopers. Use strong passwords, encryption, and safe methods of transfer.

Need help with secure file storage? Feel free to reach out today and let us walk you through setting up safe systems for your files to take the next step in protecting critical data.

dsp IT SOLUTIONS

6 RELEVANT CYBER THREATS AND THEIR SOLUTIONS

Bolster your Cyber Shield and have threats bouncing right off!

1. Phishing / Spear Phishing

- Conduct **training sessions to** help employees recognise phishing / spear phishing attempts
- Implement **email filtering** to detect / block phishing emails **before they reach the inbox**

2. Distributed Denial of Service (DDOS)

- **Continuously monitor** traffic for unusual patterns that might indicate an attack
- Use **rate limiting** to restrict the # of requests a server can process from a single IP

3. Man In the Middle (MitM) Attacks

- Encourage the use of **VPNs** to encrypt data transmitted over public networks
- Use strong, two-factor authentication methods to **verify user identities**

4. Malware Attacks

- **Install** antivirus and anti-malware software on all devices
- Keep all software and systems **up to date** with the latest security patches

5. Drive-By Attacks

- Use **web filtering** to block access to malicious websites
- Ensure browsers are updated with the **latest security patches** and **configurations**

6. Password Attacks

- Encourage the use of **password managers** to store and generate secure passwords
- Implement **account lockout after** multiple failed attempts to prevent brute force attacks

We can help you navigate the complicated world of IT & Cybersecurity so you can better protect your Data and your Business!

dspit.com.au/cybershield

10 STEPS TO PREVENT A DATA BREACH

Data breaches can harm your business. They can cost you money and trust. Let's look at how to stop them from happening.

What is a data breach?

A data breach is when someone steals information. This can be names, emails, or credit card numbers. It's bad for your customers and your business.

Why should you care about data breaches?

Data breaches are terrible things. They will cost you money. Perhaps your customers will stop trusting you. You may even be fined. It is vital to try to prevent them from occurring in the first place.

How do you prevent a data breach?

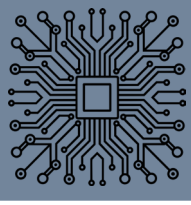
Here are 10 steps to help keep your data safe:

- Use strong passwords. Include letters, numbers, and symbols. Do not use the same password for all of your accounts.
- Update your software. Updates usually patches security holes. Have your computer set to update automatically.
- Train your employees. Teach them how to identify fake emails. Inform them to not click on suspicious links.
- Use encryption. Encryption scrambles your data.
- Limit access to data. Only give people access to what they need for their work.
- Create backups of your data. Keep these copies in a safe location.
- Use a firewall. A firewall acts like a guard for your computer.
- Be careful with emails. Almost every data breach starts with a trick email.
- Protect your Wi-Fi. Use a strong password on your Wi-Fi.
- Have a plan. Know whom to contact and what you should do. Do a practice drill so you are ready if there is an intrusion.

Even with good plans, data breaches can still happen. If one does, take action quickly. Fix the problem that led to the breach. Then, use what you learned from that mistake to make your security better.

NEED A LAUGH?

How do computers pay for things?



With cache!

MARCH TRIVIA QUESTION . . .

Test your knowledge!

The answer to last month's question was d) 1994. Can you guess the answer to March's trivia question below? The answer will be revealed in next month's newsletter.

What was the first item purchased using Bitcoin?

a) Xbox Game
b) Two Pizzas
c) Mobile Phone
d) Four Hamburgers