JULY 2022

dSP IT SOLUTIONS

TALKING TECH

HELPING YOUR BUSINESS

FROM DAMIEN'S DESK:

Happy New Financial Year! I truly hope you had a great year and that your business has been able to prosper.

When we talk about security, typically it's all about users clicking on things or back doors being left open by software developers. Well, nothing has changed on that front. Recently Wordpress came into the spotlight again in relation to an attack vector. One of the plugins with Wordpress had a serious security flaw which allowed a hacker to execute the code remotely.

So lets wind it back a little. Who knows what Wordpress is? On their website it states that 43% of the web is built on their platform. It is an application known as a content management system (CMS) that makes managing your website really simple. There is a fair chance that your website is running on this platform or something similar.

It is very important that all CMS applications get updated regularly along with all of the plugins that run along side them. Vulnerabilities are found regularly in the older versions of this application. To stay safe and update them on a regular basis.

Recently, I put together a book called **"CYBERSECURITY ESSENTIALS FOR BUSINESS OWNERS"** to which I am happy to send over a copy to you for **FREE**, no obligation, no hard sell, just plain old **FREE.** To get your hands on a copy please go to:

https://www.dspit.com.au/cybersecurity-essentials/

Damien Pepper - Managing Director
dSP IT Solutions

DID YOU KNOW?

The origin of the word "spam" in the context of an email is from a Monty Python skit from the 70s.

CARTOON for the MONTH

I didn't see any compliance issues.

dSP IT Solutions
182C Sladen Street
Cranbourne VIC 3977

TOP 5 CYBERSECURITY MISTAKES THAT LEAVE YOUR DATA AT RISK

The global damage of cybercrime has risen to an average of $11 million USD per minute, which is a cost of $190,000 each second. 60% of small and mid-sized companies that have a data breach end up closing their doors within six months because they can't afford the costs.

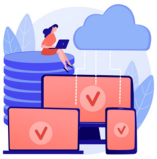
The costs of falling victim to a cyberattack can include loss of business, downtime and productivity losses, reparation costs for customers that have had data stolen, and more. Many of the most damaging breaches are due to common cybersecurity mistakes that companies and their employees make.

Here are several of the most common missteps when it comes to basic IT security best practices:

Not implementing Muti-Factor Authentication (MFA)

Credential theft has become the top cause of data breaches around the world, according to IBM Security. MFA reduces fraudulent sign-in attempts by a staggering 99.9%.

Ignoring the use of Shadow IT



Shadow IT is the use of cloud applications by employees for business data that haven't been approved and may not even be known about by a company.

Shadow IT use leaves companies at risk for several reasons:

· Data may be used in a non-secure application

· Data isn't included in company backup strategies

· If the employee leaves, the data could be lost

· The app being used might not meet company compliance requirements

It's important to have cloud use policies in place that spell out for employees the applications that can and cannot be used for work.

Thinking you're fine with only an Antivirus

No matter how small your business is, a simple antivirus application is not enough to keep you protected. In fact, many of today's threats don't use a malicious file at all.

Phishing emails will contain commands sent to legitimate PC systems that aren't flagged as a virus or malware. Phishing also overwhelmingly uses links these days rather than file attachments to send users to malicious sites. Those links won't get caught by simple antivirus solutions.

You need to have a multi-layered strategy in place that includes things like:
· Next-gen anti-malware (uses AI and machine learning)

· Next-gen firewall

· Email filtering

· DNS filtering

· Automated application and cloud security policies

· Cloud access monitoring

cont'd P3

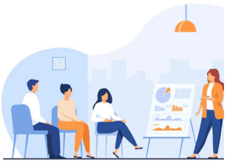
cont'd from P2

Not having Device Management in Place

A majority of companies around the world have had employees working remotely from home since the pandemic. However, device management for those remote employee devices as well as smartphones used for business hasn't always been put in place.

A device management application in place, like Intune in Microsoft 365 can help manage this.

Not providing adequate training to employees



An astonishing 95% of cybersecurity breaches are caused by human error.

Employee IT security awareness training should be done throughout the year, not just annually or during an onboarding process.

Some ways to infuse cybersecurity training into your company culture include:

- Short training videos
- IT security posters
- Webinars
- Team training sessions
- Cybersecurity tips in company newsletters

THE FUTURE OF LEADERSHIP

The pandemic completely changed the way many people view work. If there's one thing for certain, it's that remote work will continue once the pandemic ends. If your business has switched over to a remote or hybrid environment, you may need to reevaluate your leaders to ensure their skills align with the new work environment. Strong remote leaders possess traits that are essential for success.

In fact, if you want your business to prosper in the future, you must ensure your leaders are good communicators since they might not be working in the same location as their employees.

They also need to possess collaboration skills to ensure each facet of every project is covered. Additionally, your leaders should be able to align their values with those of your staff and customers.

Empathetic and understanding leaders are the future, and you need to have a leader who will look out for their team while also taking care of any customer needs. If you interview a candidate who possesses these great characteristics, they should be a top contender for your leadership positions.

dsp IT SOLUTIONS

CYBERSECURITY ESSENTIALS FOR BUSINESS OWNERS

OWN IT. SECURE IT. PROTECT IT.

If you would like a copy of our FREE, no obligation 40 page book that we have put together about Cybersecurity Essentials for Business Owners - please go to the website below, where you can leave your details and we will post one out to you.

https://www.dspit.com.au/cybersecurity-essentials/

CAMPAIGNS NEED LANDING PAGES!

Landing pages are a fantastic way to grasp the attention of multiple potential clients. With just one click of a link, they'll be met with an offer, fantastic information or a call to action that will help bring new customers to your business.

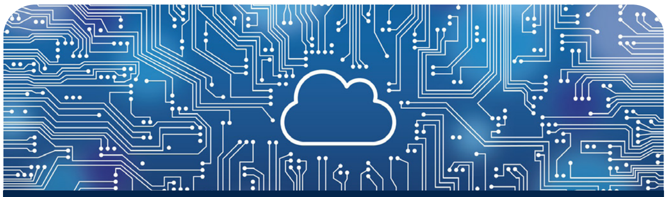
If you've been contemplating adding a landing page to your marketing campaign, check out these four great reasons to try it out.

· Landing pages operate as a tool to increase conversion rates for your business. Most businesses that utilise landing pages see higher conversions than those that don't.

· Landing pages allow you to showcase your offers. Your offers need somewhere to reside, and there's no better place than a landing page. You're able to highlight the greatest benefits of your offer this way.

· Your cost per acquisition will be lower with a landing page since they no longer cost an arm and a leg to set up. You can reallocate your resources to other avenues to truly boost your marketing campaign.

· You can test out new ideas on a landing page and judge how popular they will be with your entire customer base.



REASONS YOUR BUSINESS SHOULD BE USING A PRIVATE CLOUD

Gone are the days when everything was stored on a physical hard drive. Now, most businesses and private users utilise cloud computing to store their data. It's no secret that cloud storage is the present and future of data storage, but have you thought about using a private cloud that only allows your business and permitted users to access necessary information? There are many benefits that come with using a private cloud, such as the following:

· It offers better security since nobody besides authorised users can use the storage or servers.
· Your team will gain greater flexibility to continue their work without the fear of IT issues since backups are done automatically on private cloud servers.
· It's often cheaper to use a private cloud than to maintain physical servers.
· Private clouds usually come with managed IT services, so there's no need to hire an IT team to work on-site. This will save you time and money.

NEED A LAUGH?

Why did Wi-Fi and the laptop get married?
Because they had a connection!

WIN A $30 VILLAGE GIFT CARD!

The winner of last month's trivia question was Kevin from Coastal Surveys. The answer was d) ebay.

You could be the winner of this month's trivia, just contact us with the answer to the question below, Good Luck!

Which of these materials is the best conductor of heat?
a) Copper
b) Aluminum
c) Silver
d) Diamond

Contact us with your answer now! (03) 9001 0817 or jo@dspit.com.au