

DECEMBER 2024 TALKING TECH HELPING YOUR BUSINESS



FROM DAMIEN'S DESK:

I'm dreaming of a white Christmas, for the USA and only sun here in Aus. I am sure the kids are counting down the days until the jolly man comes down the fictional chimney to deliver the goods under the tree.

Please remember that hackers and scammers don't take a break. In fact, they prey on you because of your festive spirit and the fact that you may not be taking as much notice as you normally would. Please stay vigilant and be on your "A" game, even when you may have indulged in too much egg nog!

Kids young and old will inevitably get new tech over Christmas, please treat it with the caution it deserves. Our federal government is likely implementing legislation that will ban under 16-year-olds from social media, please don't think this will solve all the issues. We as parents and employers still need to be super vigilant; know how technology is being used in both your homes and your workplaces.

Thank you all for your support this year. I also want to thank my team for ensuring your online safety and support.

May your days be merry and bright.

Merry Christmas and stay safe.

Damien Pepper - Director
dsp IT Solutions

DID YOU KN W?



Bing Crosby's White Christmas is the best selling Christmas song, with over 100 million sales worldwide.

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.



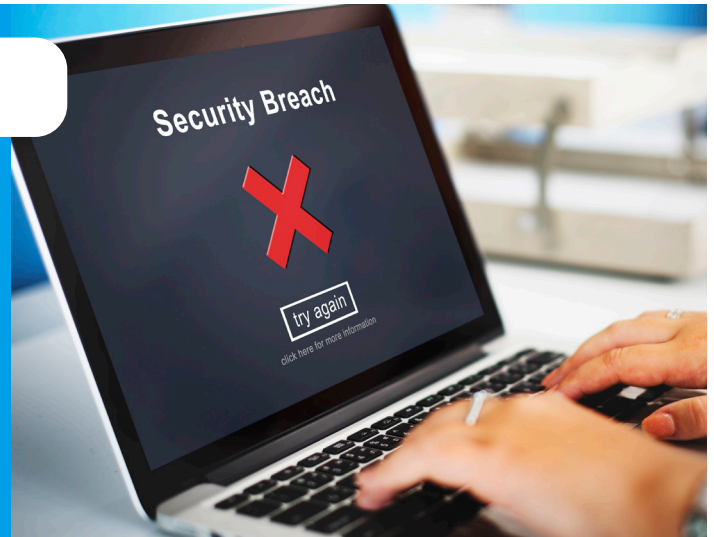
dSP IT Solutions
182C Sladen Street
Cranbourne VIC 3977
(03) 9001 0817
sales@dspit.com.au
www.dspit.com.au

WATCH OUT! "MALVERTISING" IS ON THE RISE

There are many types of malware. One of the most common is called "malvertising." It crops up everywhere. You can also see these malicious ads on Google searches.

Two things are making malvertising even more dangerous. One is that hackers use AI to make it very believable. The other is that it's on the rise, according to Malwarebytes. From September 2023, malvertising increased by 42% month over month.

Below, we'll help you understand malvertising and give you tips on identifying and avoiding it.



What Is "Malvertising?"

Malvertising is the use of online ads for malicious activities. One example is when the PlayStation 5 was first released. It was very hard to get, which created the perfect environment for hackers. Several malicious ads cropped up on Google searches. The ads made it look like someone was going to an official site. Instead, they went to copycat sites. Criminals design these sites to steal user credentials and credit card details. Google attempts to police its ads but hackers can have their ads running for hours or days before they're caught. These ads appear just as any other sponsored search ad. It can also appear on well-known sites that have been hacked or on social media feeds.

Tips for Protecting Yourself from Malicious Online Ads

Review URLs Carefully

You might see a slight misspelling in an online ad's URL. Just like phishing, malvertising often relies on copycat websites. Carefully review any links for things that look off.

Visit Websites Directly

A foolproof way to protect yourself is not to click any ads. Instead, go to the brand's website directly. If they truly are having a "big sale," you should see it there. Just don't click those links and go to the source directly.

Use a DNS Filter

A DNS filter protects you from mistaken clicks. It will redirect your browser to a warning page if it detects danger. DNS filters look for warning signs. This can keep you safe even if you accidentally click a malvertising link.

Do Not Log in After Clicking an Ad

Malvertising will often land you on a copycat site. The login page may look identical to the real thing. One of the things phishers are trying to steal is login credentials. If you click an ad, do not input your login credentials on the site, even if the site looks legitimate. Go to the brand's site in a different browser tab.

Don't Call Suspicious Ad Phone Numbers

Phishing can also happen offline. Some malicious ads include phone numbers to call. Unsuspecting victims may not realise fake representatives are part of these scams. Seniors are often targeted; they call and reveal personal information to the person on the other end of the line. Stay away from these ads. If you find yourself on a call, do not reveal any personal data.

Don't Download Directly from Ads

"Get a free copy of MS Word" or "Get a Free PC Cleaner."

These are common malvertising scams. They try to entice you into clicking a download link. It's often for a popular program or freebie. The link actually injects your system with malware to do further damage.

A direct download link is likely a scam. Only download from websites you trust.

Warn Others When You See Malvertising

If you see a suspicious ad, warn others. This helps keep your colleagues, friends, and family more secure. If unsure, do a Google search. You'll often run across scam alerts confirming your suspicion.

It's important to arm yourself and others with this kind of knowledge. Foster a culture of cyber-awareness to ensure safety and better online security.

DSP IT SOLUTIONS

How to choose the right new hardware for your business

71%

of organisations say their network assets are ageing or obsolete



It's time to upgrade when you notice:



Performance issues



Increased maintenance costs



Extra security concerns

Outdated hardware means you lose:



Time



Money



Productivity



80%

of businesses believe that outdated tech holds back progress and innovation

The right hardware:



Suits your team's needs



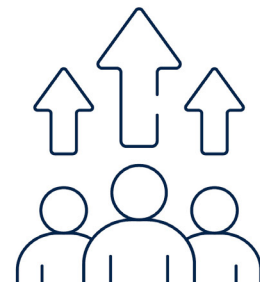
Improves security



Grows with your business



Boosts productivity

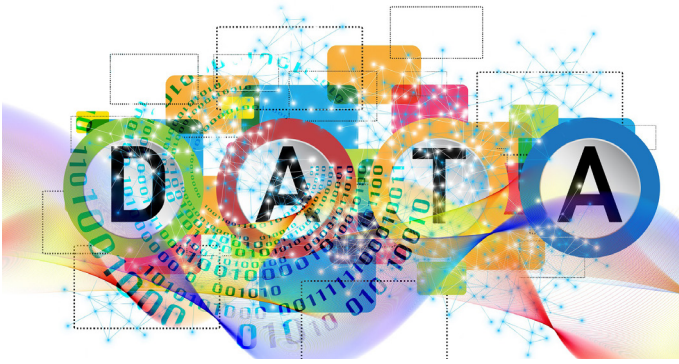


We can help you choose the right hardware to suit your needs, and your budget. Get in touch

(03) 9001 0817

sales@dspit.com.au

www.dspit.com.au




8 STEPS TO TAKE WHEN YOU GET A DATA BREACH NOTICE

When it happens, you feel powerless. You get an email or letter from a business saying someone breached your data. It happens all too often today. This leaves things like your address, SSN, and credit card details exposed to thieves.

A business getting hacked is something you have little control over, but you can take steps afterward. We've outlined the most important things to do. These steps can help you mitigate the financial losses.

1. Change your passwords
2. Enable multifactor authentication (MFA)
3. Check your bank accounts
4. Freeze your credit
5. Carefully review the breach notification
6. Get good cybersecurity protections
7. Be on the lookout for phishing scams
8. Make sure to update software & systems

Managed services can keep you protected at work. Let's improve your device security, we can help.



DSP Communications

**Delivering better.
Better telecommunications.
Better service.**

**VoIP Services
Business NBN
Business Mobile Phones
SIP**

Need help with your business telecommunications or internet?

(03) 9008 6900
sales@dspcommunications.com.au
www.dspcommunications.com.au

NEED A LAUGH?

How do Christmas trees get their email?



They log-on!

DECEMBER TRIVIA QUESTION . . .

Test your knowledge!

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

One for the maths people!

How many gifts are given in total in the song "The Twelve Days of Christmas"?

- a) 48
- b) 364
- c) 144
- d) 78

