

APRIL 2024



# TALKING TECH

## HELPING YOUR BUSINESS



### FROM DAMIEN'S DESK:

Are you running Windows 11? If not, you should be working towards upgrading. Microsoft has announced that Windows 10 will reach end of support on October 14, 2025. So, it is time to start thinking about acting to upgrade.

Can all current Windows 10 machines upgrade to Windows 11? The simple answer is no, some of them cannot. Microsoft have a minimum system requirement for hardware for Windows 11 to be installed. More specifically the installer is looking for your hardware to have a Trusted Platform Module (TPM) that is at a minimum of 2.0. This module is used for Identity and Data protection in Windows 11.

I would highly recommend that you get your hardware audited today to confirm compatibility with Windows 11.

Reach out to us if you need help doing this.

Stay safe,

A handwritten signature in black ink, appearing to read 'Damien Pepper'.

Damien Pepper - Director  
dsp IT Solutions

### DID YOU KNOW?



The first product scanned was a packet of chewing gum fifty years ago in 1974.

### 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](mailto: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](mailto:sales@dspit.com.au)  
[www.dspit.com.au](http://www.dspit.com.au)

# BE CAREFUL WHEN SCANNING QR CODES

QR codes are everywhere these days. You can find them on restaurant menus, flyers and posters. They're used both offline and online. QR codes are convenient and easy to use. You just scan them with your smartphone camera. You're then directed to a link, a coupon, a video, or some other online content.

With the rise in popularity of QR codes comes an unfortunate dark-side. Cybercriminals are exploiting this technology for nefarious purposes. Scammers create fake QR codes. They can steal your personal information. They can also infect your device with malware or trick you into paying money.

It's crucial to exercise caution when scanning QR codes. This emerging scam highlights the potential dangers lurking behind those seemingly innocent squares.

## THE QR CODE RESURGENCE

QR codes were originally designed for tracking parts in the automotive industry. They have experienced a renaissance in recent years as a result, they're used as a form of marketing today.

They offer the convenience of instant access to information. You simply scan a code. Unfortunately, cybercriminals are quick to adapt. A new phishing scam has emerged, exploiting the trust we place in QR codes.

## How the Scam Works

The scammer prints out a fake QR code. They place it over a legitimate one. For example, they might stick it on a poster that advertises a product discount or a movie.

You come along and scan the fake QR code, thinking it's legitimate. The fake code may direct you to a phishing website. These sites may ask you to enter sensitive data such as your credit card details, login credentials, or other personal information.

Or scanning the QR code may prompt you to download a malicious app. One that contains malware that can do one or more of the following:

- Spy on your activity
- Access your copy/paste history
- Access your contacts
- Lock your device until you pay a ransom



The code could also direct you to a payment page. A page that charges you a fee for something supposedly free.

## Here are some tactics to watch out for:

### Malicious Codes Concealed

Cybercriminals tamper with legitimate QR codes. They often add a fake QR code sticker over a real one. They embed malicious content or redirect users to fraudulent websites.

### Fake Promotions and Contests

Scammers often use QR codes to lure users into fake promotions or contests. When users scan the code, it may direct them to a counterfeit website.

### Malware Distribution

Some malicious QR codes start downloads of malware onto the user's device.

## STAY VIGILANT:

### TIPS FOR SAFE QR CODE SCANNING

#### Verify the Source

Verify the legitimacy of the code and its source.

#### Use a QR Code Scanner App

Use a dedicated QR code scanner app rather than the default camera app on your device.

#### Inspect the URL Before Clicking

Before visiting a website prompted by a QR code, review the URL.

#### Avoid Scanning Suspicious Codes

Trust your instincts. If a QR code looks suspicious, refrain from scanning it.

#### Update Your Device and Apps

Keep your device's operating system and QR code scanning apps up to date.

#### Be Wary of Websites Accessed via QR Code

Don't enter any personal information on a website that you accessed through a QR code. This includes things like your address, credit card details, login information, etc. Don't pay any money or make any donations through a QR code.

# Contracted IT services vs break/fix



## Break/fix

When your provider fixes your broken tech . . . and that's it

### Break/fix benefit -

#### It's cheap

You only pay when you have a problem . . . but there's no ceiling to costs



### Break/fix benefit - There's no commitment

This works both ways. Your IT provider won't think about you in between problems



Umm . . . that's it . . .



## Contracted partnership

Where your IT partner proactively monitors and prevents problems affecting your tech

### Contract benefit -

#### Predictable costs

No unexpected bills with a contracted partnership



### Contract benefit -

#### Data is safer

Your data will be encrypted, backed up and verified



### Contract benefit -

#### Higher level of service

Your IT partner is always there for you



### Contract benefit -

#### Technology just works

Proactive monitoring means problems are fixed before they affect you



### Contract benefit -

#### Better communication & collaboration

Your staff will find it easier to work together, wherever they are working



### Contract benefit -

#### Happier, more productive staff

Fewer problems = less complaining!



(03) 9001 0817

sales@dspit.com.au

www.dspit.com.au

## CYBERSECURITY THREAT PREDICTIONS YOU SHOULD PLAN FOR

Cybersecurity is a constantly evolving field. There are new threats, technologies, and opportunities emerging every year.

Organisations need to be aware of current and future cyber threats. Businesses of all sizes and sectors should plan accordingly.

Staying ahead of the curve is paramount to safeguarding digital assets.

*5 current cybersecurity predictions you should consider:*

1. AI Will Be a double-edged sword
2. Hacking will rise in prominence
3. Ransomware will remain a persistent threat
4. Cyber Insurance will become more influential
5. Quantum computing will become a looming threat



# 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) 9001 0817  
sales@dspcommunications.com.au  
www.dspcommunications.com.au




# FREE!

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

## NEED A LAUGH?

Why was the computer cold? 



Because someone left it's Windows open!

## WIN A \$25 WISH GIFT CARD

The winner from last month's trivia question was Ann from Showtime Attractions. The answer was b) Wood.

You could be the winner of this month's trivia question. Just contact us with the answer to the question below, no googling and good luck!

Before being known as PayPal, the company went by what name?

- a) MoneyMate
- b) iCash.com
- c) Confinity
- d) The X-Change

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