

MAY 2024



TALKING TECH

HELPING YOUR BUSINESS



FROM DAMIEN'S DESK:

Email delivery is going to get harder! In February, Google and Yahoo introduced the need for businesses to have email authentication to deliver to their respective platforms. The method used to authenticate is called DMARC.

By using a valid DMARC record, the email system can prove the origin of the email, providing a secure and reliable communication channel. With today's constant barrage of email spoofing (where an email looks like it is coming from someone you know), DMARC will help ensure the email is legitimate and not a hacker trying to get you to click a link to give away your password. Whilst Google and Yahoo are the first to enforce this, it will only be a matter of time before all email platforms require this type of authentication.

DMARC is especially important if you use a line of business applications to deliver emails for your business. You may know the software as a CRM or something similar. A DMARC record needs to be set up for each application that you are using to deliver emails.

If you want more information on how this can be deployed in your organisation, please contact us, and we will point you in the right direction.

Stay Safe

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

Damien Pepper - Director
dsp IT Solutions

DID YOU KNOW?

The word technology was coined in 330 BC by the one and only Aristotle.



WE LOVE REFERRALS

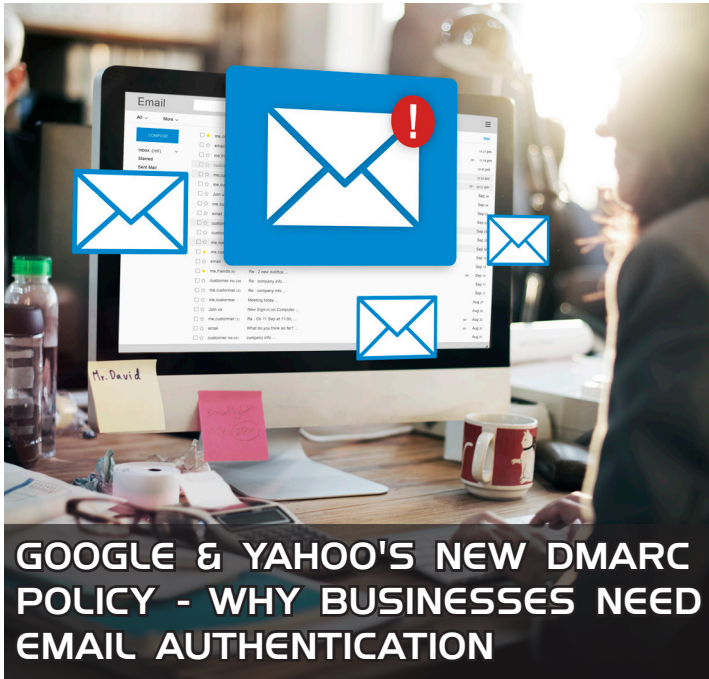
The greatest gift anyone can give us is a referral to your business friends.

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



Have you been hearing more about email authentication lately? There is a reason for that. It's the prevalence of phishing as a major security threat. Phishing continues as the main cause of data breaches and security incidents. This has been the case for many years. A major shift in the email landscape is happening. The reason is to combat phishing scams. Email authentication is becoming a requirement for email service providers. It's crucial to your online presence and communication to pay attention to this shift. Google and Yahoo are two of the world's largest email providers. They have implemented a new DMARC policy that took effect in February 2024. This policy essentially makes email authentication essential. It's targeted at businesses sending emails through Gmail and Yahoo Mail. But what's DMARC, and why is it suddenly important?

The Email Spoofing Problem

Imagine receiving an email seemingly from your bank. It requests urgent action. You click a link, enter your details, and boom – your information is compromised. The common name for this is email spoofing.

It's where scammers disguise their email addresses. They try to appear as legitimate individuals or organisations. Scammers spoof a business's email address. Then they email customers and vendors pretending to be that business.

These deceptive tactics can have devastating consequences on companies.

These include:

- Financial losses
- Reputational damage
- Data breaches
- Loss of future business

Unfortunately, email spoofing is a growing problem. It makes email authentication a critical defence measure.

What is Email Authentication?

Email authentication is a way of verifying that your email is legitimate. This includes verifying the server sending the email. It also includes reporting back unauthorised uses of a company domain.

Email authentication uses three key protocols, and each has a specific job:

- **SPF (Sender Policy Framework):** Records the IP addresses authorised to send email for a domain.
- **DKIM (DomainKeys Identified Mail):** Allows domain owners to digitally "sign" emails, verifying legitimacy.
- **DMARC (Domain-based Message Authentication, Reporting, and Conformance):** Gives instructions to a receiving email server including, what to do with the results of an SPF and DKIM check. It also alerts domain owners that their domain is being spoofed.

SPF and DKIM are protective steps. DMARC provides information critical to security enforcement. It helps keep scammers from using your domain name in spoofing attempts.

Why Google & Yahoo's New DMARC Policy Matters

Both Google and Yahoo have offered some level of spam filtering but didn't strictly enforce DMARC policies.

- Starting in February 2024, the new rule took place. Businesses sending over 5,000 emails daily must have DMARC implemented.
- Both companies also have policies for those sending fewer emails. These relate to SPF and DKIM authentication.

Look for email authentication requirements to continue. You need to pay attention to ensure the smooth delivery of your business email.

The Benefits of Implementing DMARC:

- Protects your brand reputation
- Improves email deliverability
- Provides valuable insights


EMAIL SECURITY



Phishing attacks are where cyber criminals pretend to be someone else (like your bank)



Scary stat 1



94%

of organisations have been a victim of phishing attacks



Scary stat 2



90%

of cyber security risks start in your email inbox



Scary stat 3



74%

of all breaches are caused by humans. Social engineering is where we're tricked into giving things away

You're not too small: They're targeting any business, any size

A breach can impact data, finances, and your reputation, as well as productivity



Three best ways to stay protected?

1 Educate your team on the risks



2 Use Multi-Factor Authentication (MFA) where you generate a login code on another device



3 Encryption makes your emails unreadable to the wrong people



5 DATA SECURITY TRENDS TO PREPARE FOR

With cyber threats evolving at an alarming pace, staying ahead of the curve is crucial. It's a must for safeguarding sensitive information.

Data security threats are becoming more sophisticated and prevalent. The landscape must change to keep up.

Here are some key areas to watch:


The Rise of the Machines:
AI and Machine Learning in Security

Battling the Ever-Evolving Threat:
Ransomware

Shifting Strategies:
Earlier Data Governance and Security Action

Building a Fortress:
Zero Trust Security and Multi-Factor Authentication

When Things Get Personal:
Biometric Data Protection



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

NEED A LAUGH?

Why are Microsoft employees
never relaxed?



Because they're always on Edge!



FREE!

For your FREE copy
of this book, go to:
[https://www.dspit.com.au/
cybersecurity-essentials/](https://www.dspit.com.au/cybersecurity-essentials/)

WIN A \$25 WISH GIFT CARD

There was no winner from last month's trivia question.
The answer was c) Confinity.

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!

The first 5MB hard drive weighed approximately . . .

- a) 12kgs
- b) 23kgs
- c) 118kgs
- d) 908kgs

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

