itnews FOR AUSTRALIAN BUSINESS

Supported by proofpoint.

The importance of DMARC for e-mail security

Security is always important, but in today's remote working world, stronger e-mail security is no longer a nice-to-have but a necessity to prevent many types of e-mail-related cyber-attacks.

There are many different e-mail products and services available today, but many do not support Domain-based Message Authentication, Reporting and Conformance, or DMARC. DMARC is designed to protect domains from falling to email-related compromise attacks, phishing, scams, and other cyber threats.

To understand how organisations are securing their e-mail with DMARC, iTnews and Proofpoint asked IT leaders about the importance of proper domain and e-mail security and how this is evolving in the era of cloud and remote work.

With nearly all organisations facing email security threats, and awareness of DMARC is high, IT managers believe a lack of expertise is holding back deployments.

With DMARC, business and IT leaders can transform their organisations with confidence and develop new products and services with e-mail security at the forefront.

78%

of IT leaders are aware of Domain-based Message Authentication, Reporting and Conformance (DMARC)

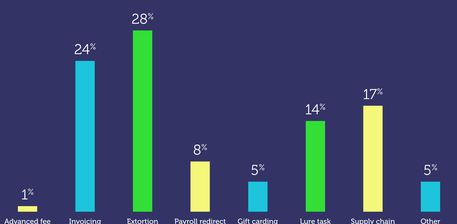
And an over-whelming **98%**

of survey respondents see their organisation exposed to at least one type of e-mail security threat

With more than **1 in 2**

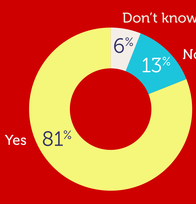
IT leaders saying e-mail fraud attacks involving invoicing and extortion are most concerning

What types of e-mail fraud attacks do you find most concerning?



Combatting e-mail fraud is a priority for nearly **81%** *of organisations*

Is addressing e-mail fraud a priority for your organisation?

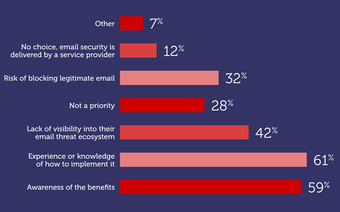


98%

are concerned about threats from impersonated or compromised suppliers

And building trust in the brand and preventing business email compromise (BEC) attacks the top reasons for implementing an e-mail fraud defence solution in **8 out of 10** *organisations*

Why do you think organisations have been slow to adopt DMARC?



Awareness of the benefits and experience or knowledge of how to implement it are the reasons

6 out of 10

IT leaders believe organisations have been slow to adopt DMARC.

***32%** believe there is a risk of blocking legitimate e-mail.*

About the survey

This survey was conducted in September, October and November 2021 by iTnews on behalf of Proofpoint, and attracted 127 respondents: 31.50% were managers or directors, 31.50% were professionals, including developers, analysts and engineers, and the rest included people in sales and marketing roles, CEOs, CFOs, GMs or MDs, those in analysis, consulting or education roles or similar, in addition to people in other roles. Looking at the size of their organisations, 23.62% worked for employers that have more than 2,500 staff members, 19.69% were at organisations with less than 10 people, while 7.87% worked for companies that employ 10-49 people.