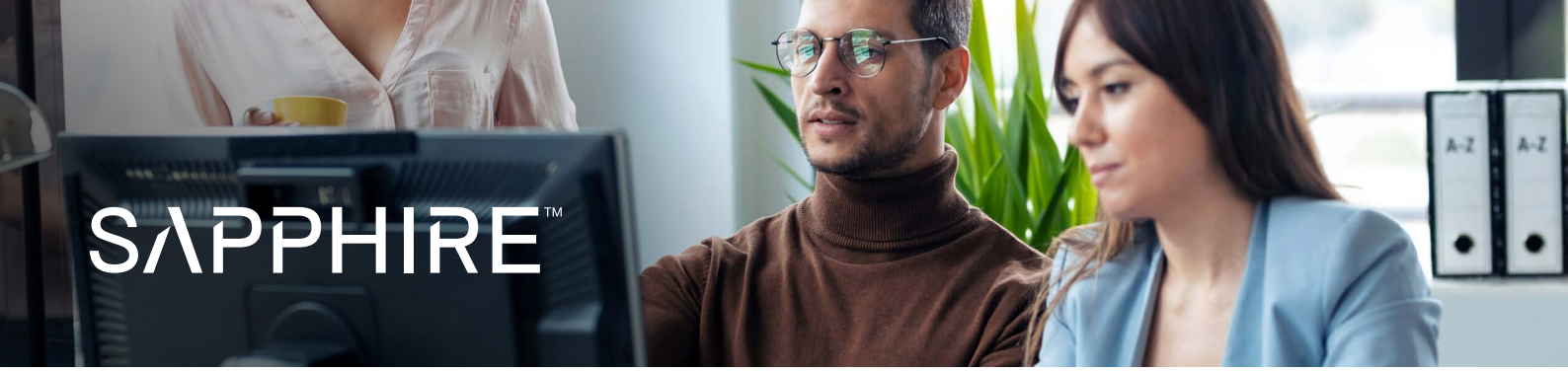


Protecting Your Brand's Reputation and Your Revenue

There is a myriad of ways in which a threat actor can attack your organisation, directly or indirectly. And technology solutions abound. We know that education also plays an important part in preventing successful attacks; people are part of the best security an organisation can have. But the increasing sophistication of scams can fool even the most attentive user.

Malicious emails are delivering malware or scamming individuals into making payments or passing on sensitive information. According to UK Finance data, in 2023 a total of £50.3 million was stolen from people in the UK through invoice and mandate scams. And 80% of those scam cases originated via an email. One UK based financial institution has stated that 40 of their clients are known to have been targeted in 2024 so far, with a total value attempted of more than £1.3 million.

The challenge is, email is easy to spoof and what's more, criminals have found spoofing to be an effective way to exploit user trust of well-known brands.

Emails being received aren't simply replicating the look and feel of a genuine one using either domain name spoofing (Company <person@yahoo.com>) or lookalike domain spoofing (Company <person@c0rnpany>) but the 'sender' is identical too (Company <person@company.com). This direct-domain spoofing is a real threat.

Benefits of DMARC

- Email Authentication and Spoofing Prevention
- Email Interception Prevention
- Improved Email Deliverability
- Brand Protection
- Compliance and Regulatory Requirements

A multi-layered approach to security is key but sometimes the more straightforward options are overlooked. One such option is DMARC.

If DMARC isn't configured or configured correctly, it is very easy for threat actors to intercept emails and alter document content. A common example is a change in banking details or payee information within an invoice.

DMARC – why it's important.

DMARC, or to use its full name, Domain-based Message Authentication, Reporting and Conformance, is a way to make it easier for email senders and receivers to determine whether or not a given message is legitimately from the sender. It doesn't require the purchase of any expensive technology but a configuration within DNS settings.

DMARC should be taken seriously. We're seeing moves around the world to enforce it and its being used by government agencies (Australia, Canada, Netherlands, New Zealand, U.K., U.S.A.). But most significantly, in October 2023 both Google and Yahoo, the world's largest mailbox providers, announced requirements

To find out more or to speak to an expert contact us today

CONTACT US TO FIND OUT MORE

Or call: 0845 58 27001

that bulk senders must have DMARC in place by the beginning February 2024. So, any organisation sending 5,000 messages a day or more to either of these, their email domain must have a DMARC policy in their DNS. If emails don't pass DMARC alignment, they will simply not be delivered. If you're trying to market your products and services, that will have a significant impact.

But DMARC is also playing a bigger part in compliance. It is now mandatory for any organisation requiring PCI DSS v4.0 compliance. And whilst not mandatory, DMARC plays a significant part in DORA compliance, complementing its objective of making the financial sector more digitally secure and resilient.

Dispelling a myth

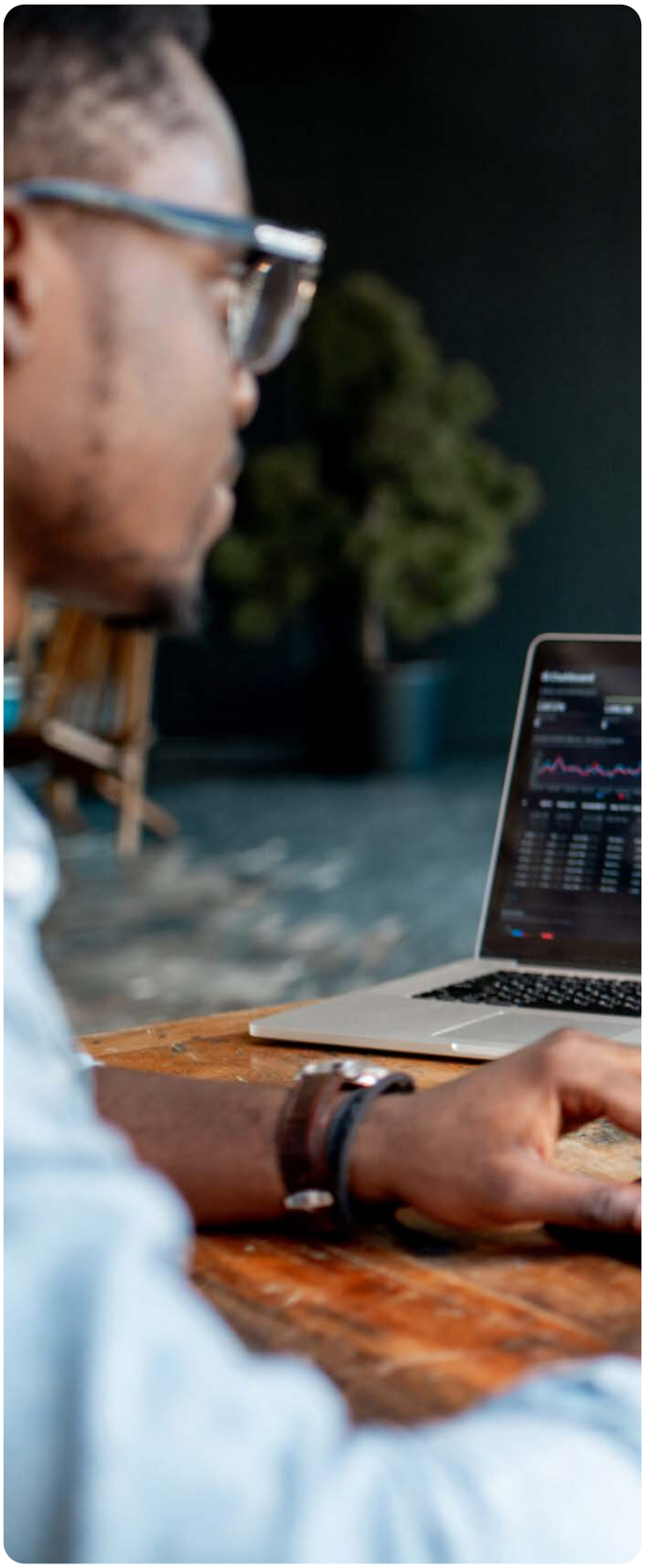
Some would say that DMARC doesn't protect the sender. Not true, it protects both sender and recipient. DMARC protects the brand and reputation of the sender by maintaining the trust and integrity of the email, and it protects the recipient by preventing malicious domains getting through.

How can Sapphire help?

To correctly configure DMARC takes knowledge and an investment of resource time. Let Sapphire help you and reduce that burden

Our experienced consultants will work with you using a DMARC tool to interpret the reports and identify who is sending emails in your name. With our guidance, you'll set up a DNS policy that will only allow legitimate emails to be sent from your domains.

Once at Reject, the job isn't done. Email is not simply a point-in-time configuration. But once we've taken you through that journey to the point of Reject, you'll be well placed to continue managing your DNS going forward. So should a colleague introduce the use of a new marketing tool and hasn't informed you, or the DKIM key isn't rotating properly, the visibility and knowledge you will have will enable you to deal with it efficiently.



To find out more or to speak to an expert contact us today

CONTACT US TO FIND OUT MORE

Or call: 0845 58 27001