

## SERVICE INFORMATION

# Smart DMARC - Protecting your Reputation

Smartdesc DMARC enables you to have confidence that only *you* are sending email as *your* organisation.

Our managed solution enables us to see who is trying to send emails on your behalf, whether legitimately or not, and therefore put controls in place to protect the reputation on the organisation, and those receiving emails from you

Domain-based Message Authentication, Reporting, and Conformance (DMARC) is not just another cybersecurity acronym but a crucial part of an overall email security strategy.

### What is DMARC?

DMARC is an authentication and reporting protocol that ensures that only authorized systems can send emails 'As' your organisation.

When a recipient receives an email from you, their email system will check 3 records to ensure that the email is legitimate.

- ▶ **SPF:** Specifies the servers and domains that are authorized to send email on behalf of your organization.
- ▶ **DKIM:** Adds a digital signature to every outgoing message, which lets receiving servers verify the message actually came from your organization.
- ▶ **DMARC:** Lets you tell receiving servers what to do with outgoing messages from your organization that don't pass SPF or DKIM.



### Why use SmartDMARC?

With DMARC, we can **block malware, protect against phishing attacks, and increase email deliverability** for your organisation. This drives **trust** in your brand and **protects your reputation**



Secure, Detect and Protect email spoofing of your domains



Reject emails sent by unauthorized senders



Comprehensive monitoring and analytics via regular, tailored reports



Increase Email Deliverability by addressing legitimate failures



Protect your digital brand, reputation and revenue – fewer bounce backs!



Report on who is sending as your domain and address discovered issues



Tailor your emails with your organization logo via [BIMI](#) to make them stand out