DMARC Compliance Service

SPF, DKIM, DMARC Management

Let's stop spoofed email - emails that appear genuine, but are actually sent by malicious senders trying to fool their targets.

Help fight the war on cyber crime. Step up to Flex IT's DMARC Compliance Service.

The service works by giving spam filters better details about your genuine email and how to handle fakes. With proper governance, email spam filters have enough information to detect real from fake and can report back on senders misusing your domain and your brand.

Features and Benefits

Key Features of DMARC Compliance are:

- Verify that the email came from an authorised source
- Verify that the email arrived as it was sent - i.e. not tampered with en route
- Whether to allow, quarantine or discard emails that fail verification
- How to report back on emails that fail verification

The service offers these benefits:

✓	Protect your brand reputation
✓	Insight into senders
✓	Prevents outbound email spoofing
✓	Management, control and reporting
✓	Increases email deliverability
✓	Part of a co-operative effort to stop email fraud

The Problem

Spoofing is a very common tactic to support phishing attacks because it helps make a malicious email look genuine and is more likely to fool the recipient.

Preventing spoofing will achieve two things:

- substantially reduce the general level of email fraud
- protect your brand from being spoofed and used by an attacker

The Solution - SPF, DKIM and DMARC

The latest tools in the armoury to distinguish genuine from spoofed emails are SPF, DKIM and DMARC. These tools are set up within your domain's DNS (Domain Name System) records. Once settings are applied and confirmed, they are used by email filters to validate emails you send. This is how they work:

- SPF details the servers allowed to send email from your domain
- DKIM 'fingerprint's the email content, so it cannot be tampered with en route
- DMARC sets governance policy for filtering results and performance reporting

Implementation

While these tools are very effective, they are tricky to set up correctly, misconfiguration can be highly disruptive, and DMARC reporting needs decoding. Email is an essential business tool, and wrong setup can result in emails you send being rejected.

Our Service

We do the heavy lifting and set up the right records in the right place. We offer a simple audit service to check your DMARC status and two service levels for setup, and an ongoing monitoring service for reporting on DMARC messages.

DMARC Audit
A simple report to review your email platforms and look at your existing DMARC configuration; report back with follow-up actions

DMARC Basic
For smaller businesses which use only a single email platform - we establish and deploy SPF, DKIM and DMARC records for your email platform; ongoing DMARC Monitoring is optional but recommended for full cover.

DMARC Comprehensive
For businesses with an extensive email footprint across several platforms - we register your domain on our management system; identify and configure deploy SPF and DKIM records for all email platforms, configure global policy for DMARC; ongoing DMARC Monitoring is required.

DMARC Monitoring
We monitor the DMARC reports, allowing onward management; supply regular reports to you; allowing validation of all platforms and visibility of your brand protection. Domain monitoring subscription term is 12 months