Calder IT Info sheet-

DMARC-May 2024

DMARC (Domain-based Message Authentication, Reporting, and Conformance) is an email authentication protocol. It builds upon existing protocols like **DKIM** and **SPF**. **DMARC** verifies email senders, preventing domain spoofing (where attackers impersonate an organisation's domain).

Key points:

- **Authentication Protocols**: DMARC requires DKIM or SPF to be in place on an email domain.
- **Validation and Alignment**: After checking DKIM and SPF status, DMARC ensures the email domain's policy is shared and authenticated.
- **Blocking Spoofed Emails**: DMARC enforces authentication and alignment, allowing only authorised senders to use a domain.

Benefits:

- **Reputation**: Publishing a DMARC record protects a brand by preventing unauthorised users from sending emails using the domain.
- **Security**: Consistent policies handle unauthenticated messages, making the entire email ecosystem more secure.
- **Visibility**: DMARC reports provide insights into email traffic, allowing domain owners to monitor their email programs.

But why do you need to know about this? **Gmail** recently implemented new requirements to enhance email security and combat spam. Whether your email accounts are Microsoft/outlook or Gmail based you could be sending to Gmail users, so you need to ensure your emails are getting through. Here are the key changes:

- **Email Authentication**: from **February 2024**, Gmail required bulk senders (those who send more than 5,000 messages to Gmail addresses in one day) to **authenticate their emails** using well-established best practices. (DMARC) This authentication ensures that the sender is who they claim to be, closing loopholes exploited by attackers. Gmail has already seen a significant reduction in unauthenticated messages sent to Gmail addresses, which has helped declutter inboxes and block malicious messages with higher precision.
- **Easy Unsubscription**: Large senders must now provide Gmail recipients with the ability to **unsubscribe from commercial emails in one click**. Senders are required to process unsubscription requests within **two days**. This change aims to make it easier for users to stop receiving unwanted messages from specific senders.
- **Spam Rate Threshold**: Gmail will enforce a **clear spam rate threshold** that senders must stay under. This ensures that Gmail recipients are not bombarded with unwanted messages.

Gmail's AI-powered defences already block nearly 15 billion unwanted emails daily, but this additional protection further enhances user experience.
We expect all email accounts such as outlook to soon follow suit, and having DMARC in place means that you are demonstrating best practice.

The National Cyber Security Centre recommends that you have effective anti-spoofing controls and that your emails are secure in transit, you can read what they say here, and/or you can contact us to ensure that you have the maximum level of security on both your incoming and outgoing emails.