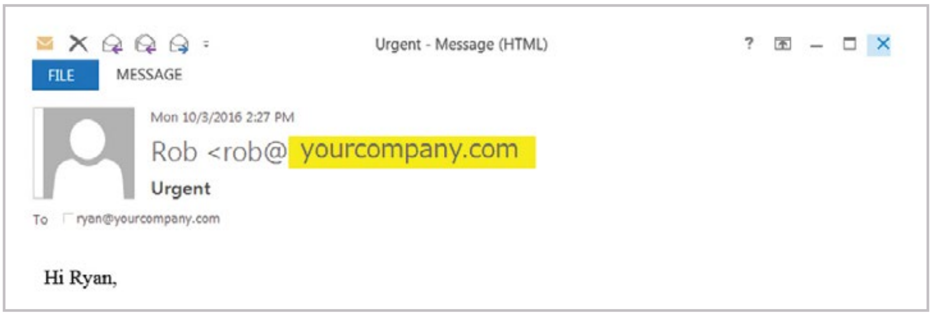
DATA SHEET

HOW TO IMPLEMENT DMARC

WHAT IS DMARC ?

DMARC (Domain-based Message Authentication Reporting and Conformance) is the first and only email authentication technology that can make the From address that users see in their email clients trustworthy.



Mon 10/3/2016 2:27 PM

Rob <rob@ yourcompany.com

Urgent

To ryan@yourcompany.com

Hi Ryan,

DMARC ensures that legitimate email is properly authenticating against established DKIM and SPF standards, and that fraudulent activity spoofing domains under your company's control is blocked.

HOW TO IMPLEMENT DMARC

STEP 1: Verify domain alignment (a.k.a. Identifier alignment)

Open the email headers from the emails you send. Identify the domain or subdomain listed in the following email places:

- The Envelope From (e.g., Return Path or Mail-From)
- The "Friendly" From (e.g., "Header" From)
- The d=domain in the DKIM-Signature (if present)

Are your domain names identical, or subdomains of the same top-level domain? If so, then your domains are aligned and you will be able to instruct mailbox providers to reject any malicious emails purporting to be from your brand. If not, you can still proceed to create your DMARC record and work with your messaging, IT, and/or security teams to get aligned.

STEP 2: Identify email accounts to receive DMARC reports

Through DMARC, you will receive aggregate and forensic (message level) reports daily. Designate the email account(s) where you want to receive these reports. You may want to use two separate accounts, as you could get inundated with the data.

DMARC reports are very difficult to parse because they are provided in raw format. Partnering with a company like Proofpoint can help you and your team make sense of them—fast.

STEP 3: Learn the DMARC tags DMARC tags are the language of the DMARC standard

They tell the email receiver (1) to check for DMARC and (2) what to do with messages that fail DMARC authentication. There are many DMARC tags available, but you do not have to use them all. In fact, we recommend keeping it simple. Focus on the v=, p=, fo=, rua, and ruf tags.

STEP 4: Generate your DMARC record with Proofpoint's DMARC Creation Wizard

Using our DMARC Creation Wizard, generate a DMARC text record in your DNS for each sending domain. Your mail receiver policy will automatically be set to "none," indicating DMARC's "monitor" mode (p=none).

Monitor allows us to gather information on your entire email ecosystem, including who is sending email on behalf of your brand (and who is pretending to do so, maliciously!), what emails are authenticating, and what emails are not.

Your record should look something like this:

v=DMARC1; p=none; fo=1;
rua=mailto:dmarc_rua@emaildefense.proofpoint.com;ruf=mailto:dmarc_ruf@emaildefense.proofpoint.com

Congratulations! You have created your DMARC record. The next step is implementation.

STEP 5: Implement your DMARC record into DNS

Work with your DNS server administrator to add your DMARC record to DNS and start monitoring your chosen domain, which might be your primary domain or a carefully selected other domain for testing. You will start receiving reports and see where email traffic using that domain is coming from.

Perhaps you will identify some vendors, partners or platforms you didn't realise were sending on your behalf. Perhaps you will be surprised to find that there is—or isn't—a significant volume of fraudulent messages using that domain and where those messages are coming from.

ABOUT PROOFPOINT
Proofpoint, Inc. (NASDAQ:PFPT), a next-generation cybersecurity company, enables organisations to protect the way their people work today from advanced threats and compliance risks. Proofpoint helps cybersecurity professionals protect their users from the advanced attacks that target them (via email, mobile apps, and social media), protect the critical information people create, and equip their teams with the right intelligence and tools to respond quickly when things go wrong. Leading organisations of all sizes, including over 50 percent of the Fortune 100, rely on Proofpoint solutions, which are built for today's mobile and social-enabled IT environments and leverage both the power of the cloud and a big-data-driven analytics platform to combat modern advanced threats.