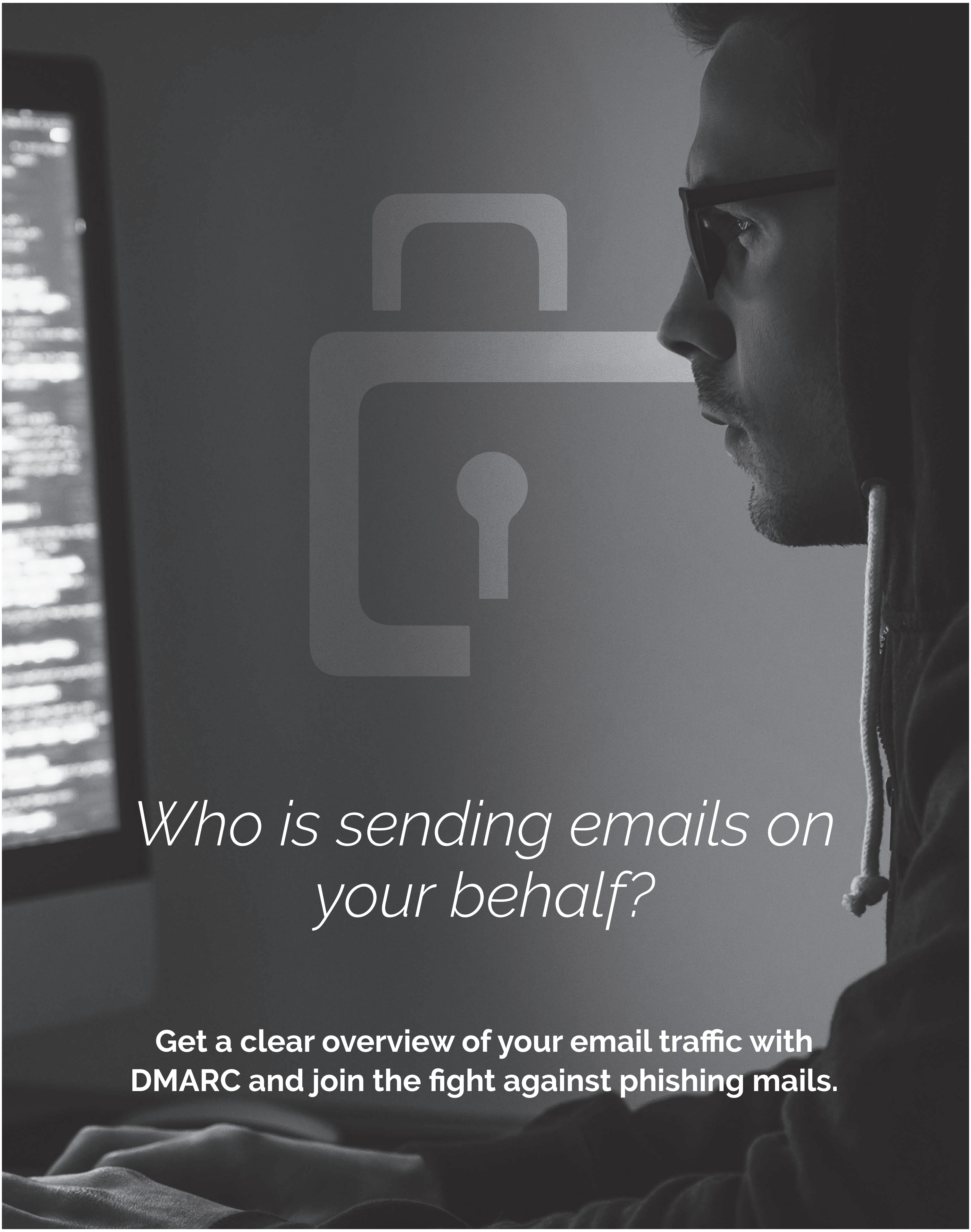


Who is sending emails on your behalf?

Get a clear overview of your email traffic with DMARC and join the fight against phishing mails.

MENA Info Security

Your data-driven **solution** that helps **to secure** your **e-mail**

Who is sending emails on your behalf?

Phishing is a hot topic and it’s in the news a lot. *‘The government has issued a warning for a circulating phishing email’*, *‘Fake emails in circulation to replace your bank card’*, *‘The latest research from Global Cyber Alliance said that it is now high priority to implement DMARC’* and there are many more examples. When you implement DMARC it offers you a simple solution to protect your domains. Next to protecting your domain it also gives you a clear view of who is using your domain to send email.

What is phishing?

Phishing email messages, websites and phone calls are developed to steal money. Most of the consumers are making online purchases on a regular basis and arrange their financial administration online. Important and confidential information like bank account numbers and private information can easily fall into the wrong hands.

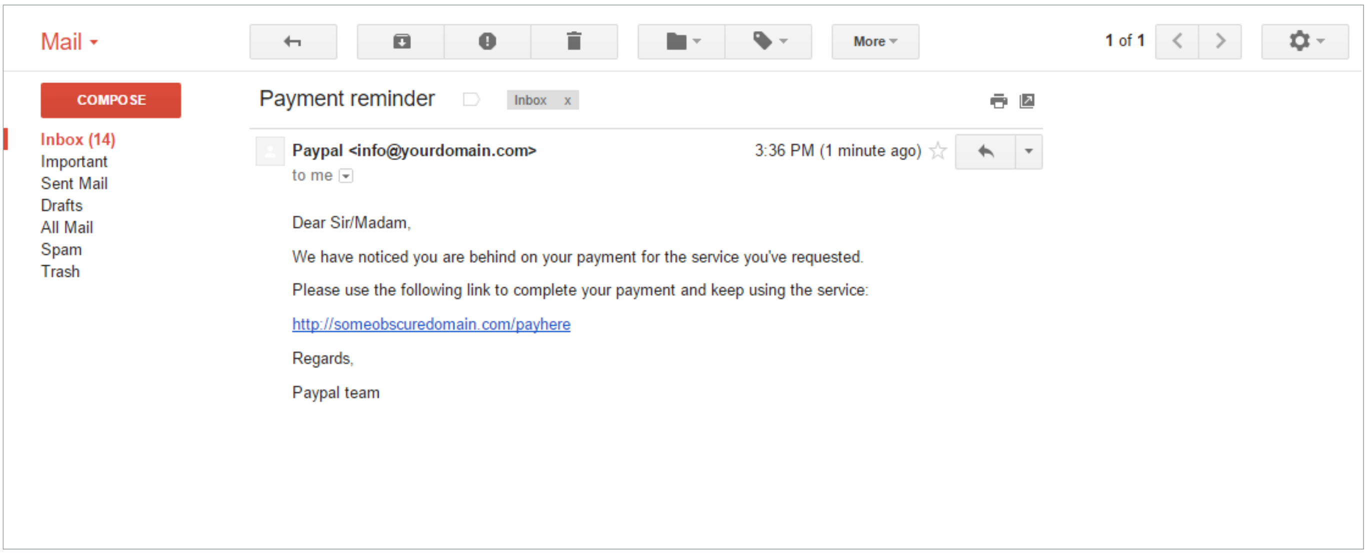
An email is easy to copy and easy to send out. Within some clicks private information becomes public.
A recognizable logo and the right corporate identity can create the illusion that an email is valid. It is (almost) impossible to see whether an email is fake or real. The receiver trusts the email and exposes private information. This is harmful to both the receiver and the organization which domain was abused.

Definition phishing email

An email which was sent to retrieve confidential information and is used for fraudulent purposes, where the actual sender is pretending to be someone else.

What would you do?

Have you ever received phishing emails? You probably have. Did you - before you gave any confidential information - find out that the email did not originate from the actual sender? But imagine a situation like this: What would you do if someone is pretending to be your supervisor and ask you to do something for him? Do you take the risk to ignore this email? Or do you dutifully fulfil your task?



Payment reminder

Paypal <info@yourdomain.com>
to me
3:36 PM (1 minute ago)

Dear Sir/Madam,

We have noticed you are behind on your payment for the service you've requested.

Please use the following link to complete your payment and keep using the service:

http://someobscuredomain.com/payhere

Regards,

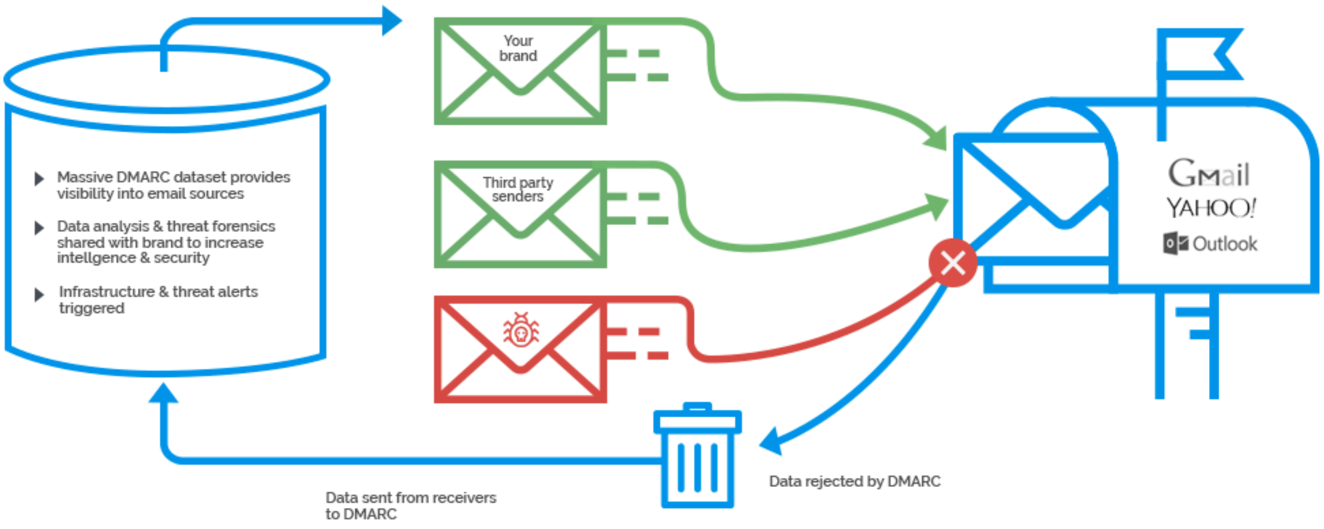
Paypal team

Who is sending email on your behalf?

Do you know who is sending emails by using your domain? The answer: *'Yes, that is me'* is the most given answer. Unfortunately - in most cases - this is not right.

Third party senders and phishers

You may be using a tool for your e-mailmarketing (e.g. MailChimp), you may have set up a help desk which can send emails (e.g. like Freshdesk or Zendesk) or you are using a CRM tool to send emails (e.g. Salesforce). These are a few examples of legitimate *'third party senders'*. However there are also parties that are not legitimate - like phishers - and these are risky!



- Massive DMARC dataset provides visibility into email sources
- Data analysis & threat forensics shared with brand to increase intellgence & security
- Infrastructure & threat alerts triggered

The implementation of DMARC gives a clear overview of the senders of the email per domain. But what is DMARC exactly? Learn more about DMARC in the paragraph below.

What is DMARC?

DMARC is a technical specification which is developed to stop phishing. Its definition is: **D**omain-based **M**essage **A**uthentication, **R**eporting & **C**onformance. The technical policy requires that the sender of the email (the sender which is visible in the inbox) proves he is the actual sender. This is done by validation and safety techniques like SPF and DKIM. These techniques are necessary to deliver the emails correctly. DMARC adds several important aspects which simplifies the deployment.

What is the added value of DMARC?

DMARC has a couple of interesting characteristics which makes it an increasingly popular technique to use.

Alignment - It is possible to send an email correctly with DKIM and SPF but still use *'another'* sender. Perhaps you are using Gmail and you have noticed that in some cases you can see the text: *'via sender@domain.com'*. In this particular case the *'technical sender'* is not equal to the *'from'* domain. This causes this email to become invalid for DMARC. For DMARC compliant emails you can certainly see that the sender (the *'from'* domain) has actually sent the email.

Reporting – All ISP's who gets an email from your domain as *'from'* domain will send reports on a daily basis to an email address of your choice. This can be dozens of reports per day. Do you want a simple analysis of these reports? We offer you the software 'DMARC for MENAInfoSec'. This tool helps you to easily implement DMARC.

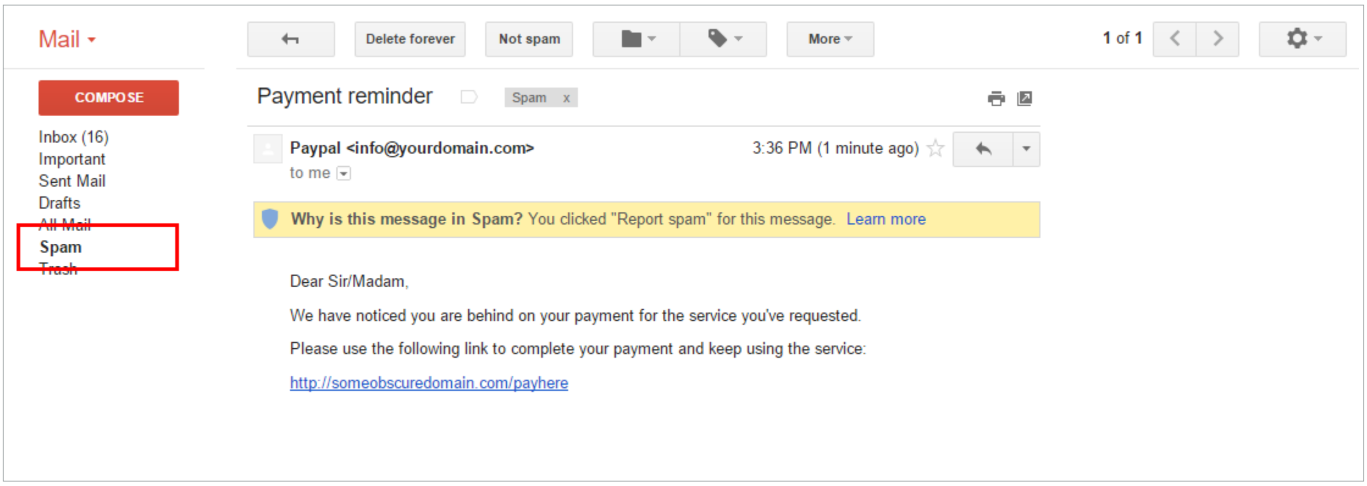
Policy – It is possible to configure a policy. With this policy you can indicate what an ISP should do with invalid emails. Furthermore it is possible to do a phased transition from one policy to another. The possible values are:

Policy values:

none – This policy has no influence on sent emails. Even though the reports are being sent to your email address.

quarantine – This policy instructs ISP's to place invalid emails in the *'spamfolder'*.

reject – This policy instructs ISP's to completely ignore invalid emails and reject them on SMTP level.



Payment reminder

Paypal <info@yourdomain.com>
to me
3:36 PM (1 minute ago)

Why is this message in Spam? You clicked "Report spam" for this message. Learn more

Dear Sir/Madam,

We have noticed you are behind on your payment for the service you've requested.

Please use the following link to complete your payment and keep using the service:

http://someobscuredomain.com/payhere

Use a good tool

If you plan to start with implementing DMARC you will receive many reports. You will need a good tool to help you analyse, read and understand these DMARC reports.

MENAInfoSec

We offer the tool DMARC for MENAInfoSec. Using this tool you can easily process the XML reports you receive to readable overviews. We will keep you up to date with the current status of your implementation on a daily basis.

A detailed insight is possible

Next to the grouped data that the ISP's are sending it is also possible to receive detailed messages from specific emails that are not 'DMARC compliant'. The 'forensic reports' can be very valuable while implementing DMARC.

Protect your domain and improve your reputation

The implementation of DMARC makes it possible to protect your domain from phishing. When you implement DMARC and will move to the reject policy over time, this will be a clear signal to the ISP's that you take email security seriously. This will increase the reliability of your domains, which is an important measurement for deliverability. Therefor implementing DMARC has a positive influence on your deliverability.

MENAInfoSec helps you to go to p=reject.

Our team of skilled DMARC consultants are there to help you to go to p=reject. Do you have any interest or questions? Don't hesitate to contact us!