

DMARCADVISOR

HOW TO PREVENT PHISHING AND EMAIL ABUSE BY IMPLEMENTING DMARC

WHITEPAPER



Introduction

Phishing is one of the - if not the most - used types of cyber-attacks to date. Sensitive information like passwords, credit card numbers, or other personal information is stolen via phishing emails. For individuals, it can be devastating, but for businesses, the damage can sometimes even be detrimental.

A 2021 study from Verizon Data Breach Investigation Report showed that 36% of all data breaches involved phishing. Additionally, 85% of all breaches involving social engineering used phishing as the primary method.

The Anti-Phishing Working Group observed 1,350,037 total phishing attacks in Q4 2022. This was slightly up from the record third quarter when APWG recorded 1,270,883 total phishing attacks.

These studies show that phishing attacks are still very common and don't seem to be decreasing in actual numbers. At DMARC Advisor we help the biggest organizations in Europe to protect their domains from phishing attacks. As the title says it all, we do this by implementing DMARC. DMARC is built upon two other open standards, which are laws written by the internet that tell email servers what to do with authorized and unauthorized email flows. These open standards are SPF, DKIM, and DMARC.



”

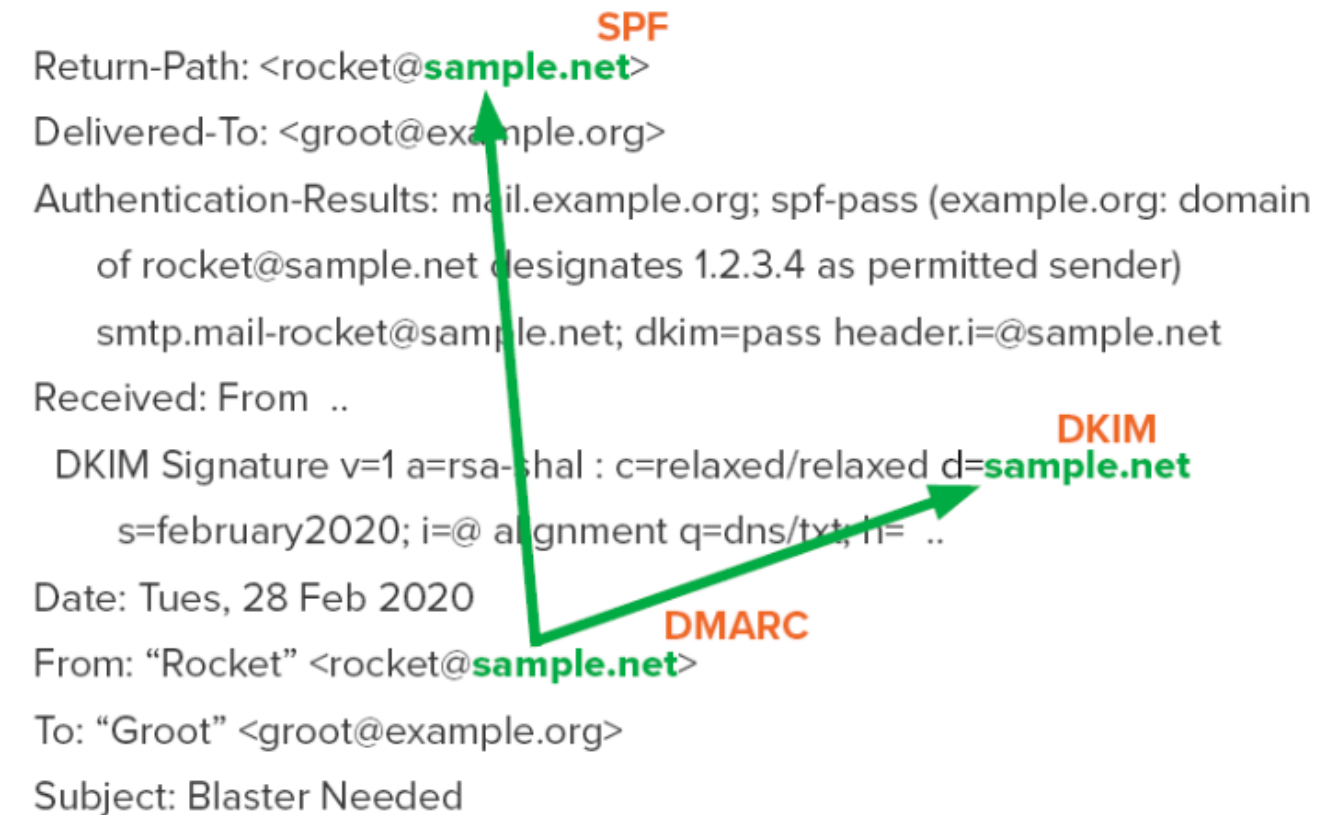
**36% of all data breaches
involved phishing**

What is SPF, DKIM, and DMARC?

SPF, DKIM, and DMARC are open standards that can be implemented by everyone on the internet, for free. The image on the right delivers a quick view of where to find each authentication method within an email.

The 'From:' domain, also known as the DMARC domain, is what is shown in an email. This is what everyone sees as being the 'sender'. But this is exactly the domain that is used in phishing campaigns. So even though SPF and DKIM can pass a validation check, that doesn't mean DMARC passes. The DMARC domain needs to be aligned with the SPF and DKIM domains to be protected from phishing or email abuse.

Perform a check for your domain to find out if your domain is protected with DMARC Advisor's [Domain Check](#). Completely free and without a catch.



Return-Path: <rocket@**sample.net**> **SPF**
Delivered-To: <groot@example.org>
Authentication-Results: mail.example.org; spf-pass (example.org: domain of rocket@sample.net designates 1.2.3.4 as permitted sender) smtp.mail-rocke@sample.net; dkim=pass header.i=@sample.net
Received: From ..
DKIM Signature v=1 a=rsa-sha : c=relaxed/relaxed d=**sample.net** **DKIM**
s=february2020; i=@ alignment q=dns/txt; h= ..
Date: Tues, 28 Feb 2020
From: "Rocket" <rocket@**sample.net**> **DMARC**
To: "Groot" <groot@example.org>
Subject: Blaster Needed

Fully aligned email (header examples)

SPF | Sender Policy Framework

'The Mailman'

SPF stands for Sender Policy Framework and allows the owner of a domain to specify which email servers are authorized to send email on behalf of that domain.

The easiest way to explain SPF is that you are sending a package to your friend and that you have authorized DHL to deliver your package. Any other postal service is not authorized.



DKIM | DomainKeys Identified Mail

'The Seal'

DKIM stands for DomainKeys Identified Mail and works by adding a digital signature to the header of an email message.

The easiest way to explain DKIM is that you add a seal to the package you sent, which should be intact upon arrival. If the seal is broken, you know the content can be tampered with.



DMARC | Domain-based Messaging Authentication Reporting & Conformance

DMARC stands for Domain-based Messaging Authentication Reporting & Conformance is an open standard that is built on top of SPF and DKIM. DMARC allows a domain owner to specify how their emails should be handled if they fail SPF or DKIM checks. The domain owner can choose to have the email rejected, marked as spam, or delivered as usual.

Without DMARC, the domain owner is not able to see who or what is sending emails on behalf of their domains. DMARC also provides feedback about how their emails are being handled by other email servers.



The Three DMARC Policies

DMARC allows a domain owner to choose a policy that tells the receiving email server what to do with an email if this email fails the DMARC verification check.

DMARC offers three policies to choose from, which are:

- **p=none**: monitors email flows. No further actions are taken.
- **p=quarantine**: handles email that doesn't pass the DMARC check as spam and sends it to the spam folder.
- **p=reject**: blocks email that doesn't pass the DMARC check. Emails simply don't arrive at the inbox. P=reject should always be the goal when implementing DMARC.

It is important to know that changing the DMARC policy can have a negative impact on your email flow if you haven't monitored your domains correctly in the p=none phase. A domain can be used to send a newsletter only once per three months. That means it takes three months to get all the data from that domain. So, take your time and monitor, don't make any hasty decisions.



How to get started with DMARC

Getting started involves a few steps, but it's not too complicated.

1 - Start with analyzing which domains you have, sending and non-sending domains. Even subdomains.

2 - Create an email authentication policy for each domain (hopefully you have this in place already). These are mentioned above, SPF and DKIM.

3 - Publish a DMARC policy in your domain's DNS record. This lets other mail servers know that you are using DMARC and how to handle any failed authentication checks.

4 - Monitor your DMARC reports to see how your email traffic is being handled by other mail servers. You can now identify any issues or vulnerabilities regarding your domains.

The only downside is that these DMARC reports, which are XML files, look like the image on the right.

That XML report is just from one single domain, and from one sender. So, if you're sending a lot of emails from a lot of domains, you will receive more than enough reports. Analyzing these reports can be time-consuming and hard to interpret correctly.

```
<?xml version="1.0" ?>
<feedback>
  <report_metadata>
    <org_name>google.com</org_name>
    <email>noreply-dmarc-support@google.com</email>
    <extra_contact_info>https://support.google.com/a/answer/2466580</extra_contact_info>
    <report_id>10662168003798883053</report_id>
    <date_range>
      <begin>1623110400</begin>
      <end>1623196799</end>
    </date_range>
  </report_metadata>
  <policy_published>
    <domain>dmarcadvisor.com</domain>
    <adkim>r</adkim>
    <aspf>r</aspf>
    <p>reject</p>
    <sp>reject</sp>
    <pct>100</pct>
  </policy_published>
  <record>
    <row>
      <source_ip>209.85.220.41</source_ip>
      <count>193</count>
      <policy_evaluated>
        <disposition>none</disposition>
        <dkim>pass</dkim>
        <spf>pass</spf>
      </policy_evaluated>
```

Raw DMARC XML data

Readable DMARC XML Reports

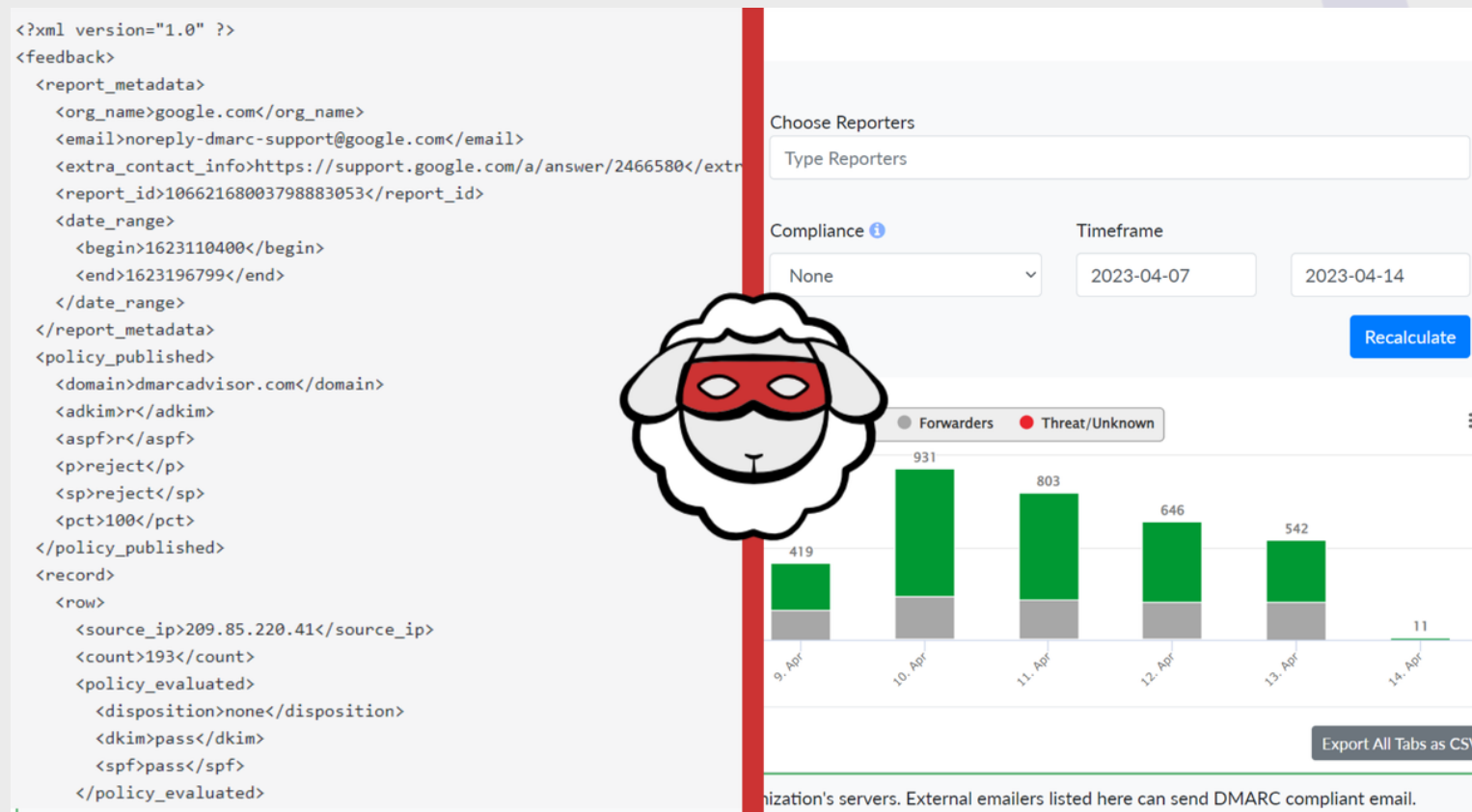
DMARC Advisor has been providing readable DMARC data since 2013 and continues to deliver the most detailed reports in the industry.

We understand that exploring DMARC data can be challenging. That's why we've created the Detail Viewer – a powerful tool that makes it easy to navigate. You can easily search through the data timeline and filter the results by specific search parameters like dates, domains, and data providers.

The filter option is especially useful, as it allows you to see what would have happened if a DMARC policy had been in place. With this information, you can stay ahead of any security breaches and take steps to improve your email security.

The Detail Viewer categorizes the DMARC data into four high-level tabs: DMARC-capable, Non-compliant, Forwarding, and Threat/Unknown. Each tab provides detailed information on DMARC compliance and highlights any infrastructure that requires attention. You can even drill down into each category to reveal more details and identify the sources of your domain's email.

Our platform also allows you to combine data from multiple providers across specific timelines. This gives you a comprehensive view of your domain's email security, making it easier to understand your DMARC data without any stress. At DMARC Advisor, we're committed to helping you get the insights you need quickly and easily, and the Detail Viewer is one way we're delivering on that promise



ABOUT DMARC ADVISOR

DMARC Advisor was founded in 2013 by real internet veterans. We were the first European DMARC provider. Nowadays we are also the #1 DMARC vendor in Europe. Our founders also established one of the first Email Service Providers in The Netherlands and already sent DMARC-compliant emails before DMARC was even invented. At their initiative, DMARC became a mandatory standard for governments in the Netherlands, which also led to a safe email initiative at a European scale.

DMARC Advisor is dedicated to inspiring people to implement open standards as a solid foundation to make the internet a safer place. With more than 20 years of experience in email deliverability and security, and more than 10 years of experience helping companies implement DMARC it's safe to say that DMARC Advisor is the new standard to implement DMARC!



www.dmarcadvisor.com



sales@dmardadvisor.com



[dmarc-advisor](https://www.linkedin.com/company/dmarc-advisor)

