How to read a DMARC report

1. Definitions:

- **DMARC record:** DMARC is an authentication protocol that protects and secures email domains against all forms of abuse by validating the SPF and DKIM policies published by the sender.
- **DMARC report:** A DMARC report provides a comprehensive set of data on the results of SPF/DKIM authentication of email for a specific domain. This report is generated by email recipients and sent to the email address specified in the DMARC record.

2. The importance of DMARC reports:

- The data in DMARC reports allows you to identify messages that pass or fail SPF and DKIM authentication and helps you to identify deliverability problems and improve email deliverability.
- Review your report data to quickly identify and detect any form of abuse. DMARC reports help you control your email authentication policies.

3. The role of a DMARC record:

- Fight against email or domain spoofing.
- Protect against phishing attacks, spoofing and spammers.
- Improve email deliverability and prevent emails from being marked as spam.
- Comply with new regulations from email providers.
- Protect the reputation of your domain name and your brand image.

4. How to read a DMARC report:

4.1. Method 1 (classic):

The DMARC report is sent in raw format. It is therefore important to be able to interpret and analyze this information. You will find the following data:

4.1.1 Your ISP, the name of your email service provider:

```
<feedback>
<report_metadata>
<org_name>emailsrvr.com</org_name>
<email>dmarc_reports@emailsrvr.com</email>
<extra_contact_info>http://emailsrvr.com</extra_contact_info>
```

4.1.2. The report identification number:

```
<report_id>ff2d7a69-d5a4-4caa-a69b-04814ac885e9</report_id>
```

4.1.3. The start and end date range (in seconds):

```
<date_range>
<begin>1705795200</begin>
<end>1705881600</end>
</date_range>
```

4.1.4. The specifications of your DMARC record as published in the DNS zone of your domain:

```
<policy_published>
<domain> yourdomain.com</domain>
<adkim>r</adkim>
<aspf>r</aspf>
<p>none</p>
<sp>none</sp>
<pct>100</pct>
</policy_published>
```

4.1.5. IP address of the sending source:

```
<source_ip>185.236.142.114</source_ip>
```

4.1.6. An overview of your authentication results (summary of SPF and DKIM pass/fail results):

```
<policy_evaluated>
<disposition>none</disposition>
<dkim>pass</dkim>
<spf>pass</spf>
</policy_evaluated>
```

4.1.7. From: domain:

```
<header_from> yourdomain.com </header_from>
```

4.1.8. SPF authentication results:

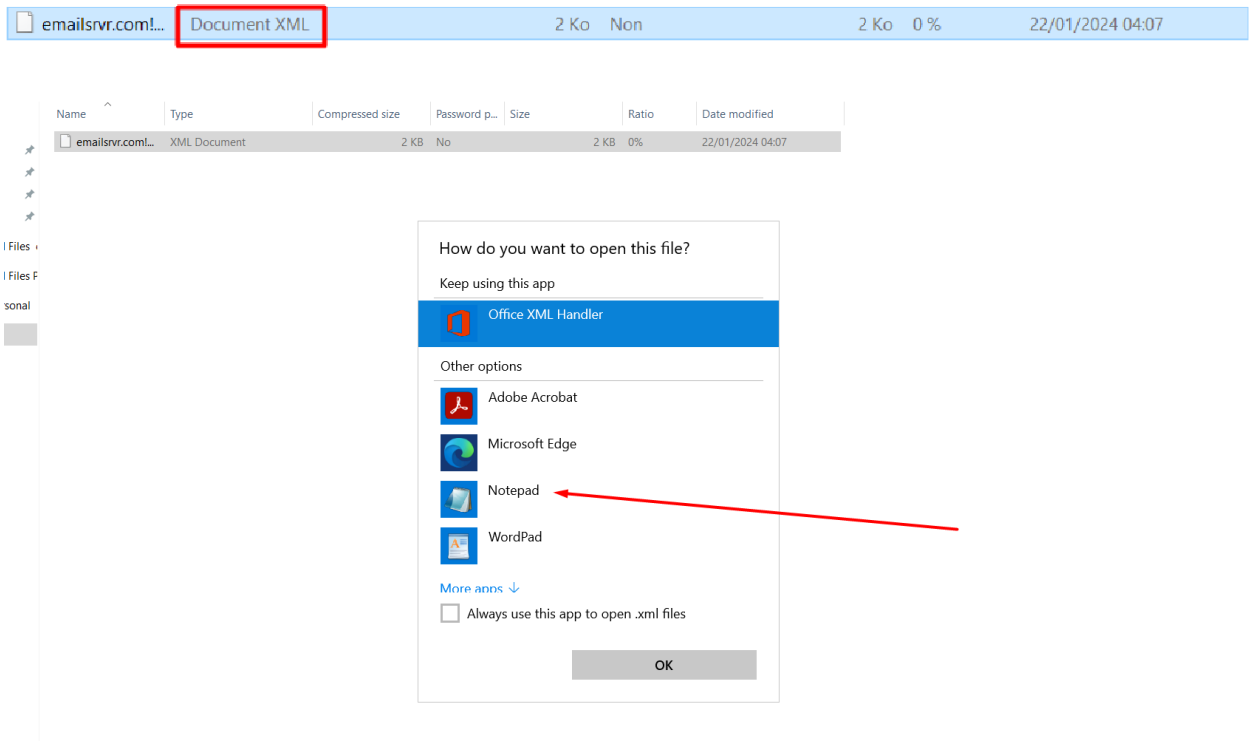
```
<spf>
<domain>si116382.yourdomain.com </domain>
<result>pass</result>
</spf>
```

4.2. Method 2 (ChatGPT):

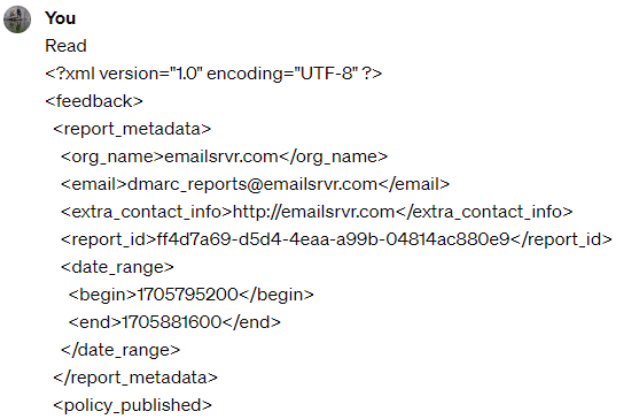
In this section, we will show you a simpler way to read a DMARC report using ChatGPT.

To get started, head to the email in question where the XML file containing the necessary information is located.

Once on the email, open the file using the "**Notepad**" application.



After opening the file with Notepad, you will see XML code. Copy this code, then paste it into the ChatGPT search bar and write "**Read**" at the beginning.



ChatGPT will provide you with both a summary and a detailed explanation of the DMARC report.

If you have any questions or require assistance, use the form below to contact us. Our support team is available 24/7.

https://systeme.io/en/support/contact-us