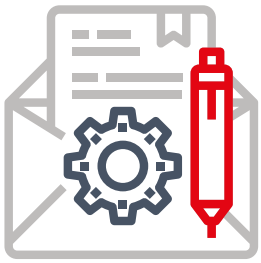
DMARC

DMARC is a technology for email authentication and domain protection. It protects not only against unauthorized sending of messages, but also against phishing attacks and especially spear-phishing attacks which often lead to massive damage.

Such attacks are usually precise and tailor-made by hackers usually to impersonate and authorize someone in a senior company position into making a payment,or sending confidential information that is subsequently misused to gain access to accounts to internal systems.Attackers typically spend a very long time often months or even a year in preparation. That time is spent using various methods to obtain information about internal processes, company structure, competencies of specific people, etc.

> "Simply put, DMARC will protect you from "fraud and other malicious email activities""

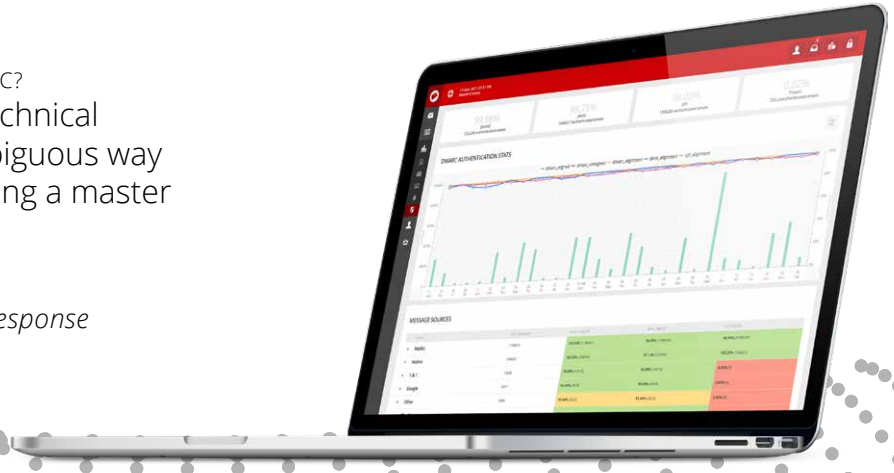


WHAT IS DMARC'S
ADDED VALUE

DMARC helps identify and properly configure the email infrastructure, including email authentication settings. Correct Email authentication setup is essential to securing against email attacks and ensuring maximum deliverability. As often happens companies organise development servers, test servers and other infrastructure elements to test a new product or service. But they are often not properly authenticated and greatly facilitate the possibility of abuse attack, thus leaving vulnerabilities in the network - gateways if you like for hackers to penetrate. Last but not least DMARC helps identify infrastructure to ensure compliance with GDPR.

According to statistics presented by Yahoo, the implementation of DMARC with strict enforcement policy yields an increase in open-rate by an average of 10% because of the increased trust. Essentially however DMARC is your protection against fraudulent e-mails that are sent on behalf of your company.

> WHY ENTRUST MAILKIT WITH DMARC?
> Your ability to present technical information in an unambiguous way is a real testament to being a master of your domain"
>
> *Richard Bewley,*
> *Head of Deliverability at GetResponse*



WHAT ARE OTHER DMARC

BENEFITS

Don't deal with the consequences, have the situation under control

The main benefit of DMARC is the ability to set strict rules for e-mail authentication and prevent abuse of the domain by third parties. Thanks to DMARC reports, you will find out if someone is impersonating you or abusing the name of your company, and with the help of clear policies you can prevent abuse. The motivations of the attackers are very different and the targets can be large, medium-sized, but small companies as well.

Enable deployment of new technologies

DMARC enforcement is a requirement for the deployment of new technologies such as AMP4email and BIMI. DMARC is an email security standard that is already required for sending emails over IPv6. In the future, we expect DMARC to be required by all major email services providers, just as DKIM signing is a requirement today.

Proper email infrastructure setup

DMARC reports fundamentally help to correctly set up the entire company email infrastructure from SPF, through DKIM to the mentioned DMARC. The company has everything under control, perfectly tuned, secured and ready for the best possible delivery.

WHAT ARE DMARC

REPORTS?

DMARC reports and their evaluation will show the authentication of email messages from the perspective of the receiving party. They provide information on how many messages and from which sources were correctly authenticated and how many were not. For example, how many fraudulent messages were prevented from being delivered. It is these reports that are used to set up the email infrastructure and to fulfill the goal of DMARC, which is to set strict rules - DMARC enforcement.

PRICING

The service is ordered for a min. 12 months and the complete package consists of several activities:

- We will process reports of your emails every month (the price will correspond to the volume of these messages)
- An initial detailed analysis will be performed - the scope and number of hours will depend on the volume of emails, see the previous point
- Over the period of 2-3 months we will gradually incorporate the results of our analysis and together with your IT implement all the necessary steps to correct the authentication and prepare for deployment of strict DMARC enforcement policy
- Subsequently, we provide regular monthly monitoring of your domain for a total of 2 hours/month

Do you want to deploy DMARC with us, are you interested in learning more details?

Do not hesitate to contact us and we will be happy to discuss everything with you.

Mailkit s.r.o. | Oranžová 225 | 252 19 Chrášťany Tel: +420 277 001 800 | E-mail: sales@mailkit.com