CASE STUDY DMARC ANALYZER

Governing the email channels of all 160 domains

This case study is based on a collaboration with a leading French eCommerce travel Enterprise, Loisir Encheres.

Challenge
The key domain of Loisirs Encheres was spoofed and used for phishing campaigns.

Solution
Gained insight in all sources that sent email on behalf of LE, implemented DKIM for all valid sources and enforced the policy.

Results
All 160 domains are protected against spoofing / phishing attempts.

Email marketing is the primary marketing channel for this client, all key transactions such as invoicing are done via email. Therefore the client wanted to be aware of the performance of her email channels to ensure that relations can rely on emails which origin from the client.

> " The support provided by the DMARC Analyzer team really helped us to achieve results, it has been a pleasure to work with them. Their profound knowledge and effective approach helped us to speed up the DMARC deployment for Loisirs Enchères. "
>
> **Jérémie Leca, CTO - Loisirs Enchères**

Challenges

The challenges that ensured DMARC Analyzer was needed as an executive party:

- Limited insight in email channels
- Ongoing spoofing attacks on brand
- No setup for SPF and DKIM
- Domains were abused
- Legitimate email was marked as spam

Project goals

The main project goals of this DMARC deployment project:
- Governing the email channels of all 160 domains and be aware of legitimate email streams as well as abuse
- Realize DMARC compliance for legitimate sources which are sending email on behalf of the customer domain(s)
- Mitigate the effect of phishing, spoofing and other attacks
- Optimize deliverability and the performance of email (marketing)

Company details

Company
Loisirs Encheres

Country
France

Company Size
Medium Enterprise

Industry
Online travel & leisure auctions

Project approach

In order to resolve the challenges above, the client had to publish a custom DMARC record on all domains. With DMARC Analyzer, the channels were actively monitored and governed. Since there was no SPF or DKIM in place and a lot of emails were being forwarded, DMARC Analyzer advised to authenticate the email with a DKIM signature. The DKIM signing on all sources ensured that the compliance rate nearly reached full DMARC compliance. This ensured that the client could move towards a DMARC enforcement policy. The DMARC enforcement policy protected the domains against abuse such as phishing and spoofing attacks and optimized delivery.

Achievements

Achievements realized for the client as a result of the DMARC Analyzer deployment:

- Gained full insight into the email channel
- Authenticated all email with a DKIM signature
- Moved towards an enforcement policy on all 160 domains
- Mitigated the effect of phishing, spoofing and other attacks
- Improved deliverability