Case Study

mimecast

Loisirs ENCHERES

Online leisure and travel company protects their brand and email deliverability

Protects all 160 domains against spoofing and phishing attacks

Email marketing is the primary marketing channel for Loisirs Enchères, a leading French online leisure and travel company. In addition, all key transactions such as invoicing are done via email. It is therefore critical that customers can trust and rely on the email communications coming from them.

Legitimate emails were not being delivered and their brand was being damaged

Loisirs Enchères knew they were being targeted by cybercriminals who were spoofing their domains and sending emails targeting their customers. This also resulted in their legitimate emails being marked as spam. But with limited insight into their email channel and no SPF or DKIM set up, it was very difficult to investigate and put an end to the domain spoofing.

At a Glance

- Online leisure and travel company
- Based in France

The Problem:

- Attackers were spoofing their domains to target customers with phishing emails – damaging their brand.
- Legitimate email was being marked as spam – including email marketing and operational information like invoices.
- Limited visibility into their 160 domains meant it was difficult to investigate and resolve the domain spoofing problem.

The Solution:

Mimecast DMARC Analyzer

Benefits:

- All 160 domains are protected against spoofing and phishing attempts – protecting their brand and business.
- Full visibility of all email channels helps ensure ongoing DMARC compliance and optimum email deliverability.

They needed a solution to help effectively govern all their 160 domains by providing visibility into both legitimate email sources and fraudulent senders. This would then allow them to ensure deliverability of legitimate marketing and operational emails by enforcing DMARC compliance, while mitigating phishing, spoofing and other email attacks.

Rapid DMARC enforcement

To resolve these challenges, Loisirs Enchères needed to publish a custom DMARC record on all domains. With the DMARC record in place, Mimecast DMARC Analyzer could actively monitor and govern all the channels, providing full visibility of all senders, both legitimate and fraudulent. Since there was no SPF or DKIM in place, and a lot of emails were being forwarded, Mimecast advised to authenticate the email with a DKIM signature.

The DKIM signing on all sources ensured they reached near full DMARC compliance. This meant that they could move towards a DMARC enforcement policy to protect the domains against abuse such as phishing and spoofing attacks, and could optimize delivery of legitimate email.

> **“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.”**
>
> *IT security and infrastructure manager*