Greenhill

ONDMARC by RED SIFT

Highlights

- Greenhill used OnDMARC to block over a million spoof emails in just 90 days.
- OnDMARC uncovered 2,734 unauthorized email sources sending 671,000 fake emails from a parked domain, all of which were blocked.
- Greenhill's team gained essential visibility and guidance that enabled them to configure DKIM and SPF settings for Mimecast independently.
- Dynamic SPF meant breaking the lookup limit and managing 16 lookups directly from inside their account, increasing the pass rate from 79.70% to 100%.

www.ondmarc.redsift.com

contact@redsift.com

@redsift

Greenhill makes email trustworthy for financial matters by securing their domain

Greenhill is a leading independent investment bank focused on providing financial advisory services. The firm operates globally with 15 different offices and over 400 employees, sending over 7 million emails a year.

Financially-driven email matters make tasty phish bait

Chief Information Officer (CIO), John Shaffer, hired a third-party cybersecurity rating company to review the organization's cybersecurity. The audit flagged DMARC as failing and therefore a priority initiative to focus on. However, like most organizations introduced to DMARC by consultants, Greenhill were left with a sense of urgency to implement the email authentication protocol without any internal expertise or visibility of their email security landscape to know how.

Full visibility, clear direction, and ongoing guidance

Faced with choosing between taking the plunge themselves and risk blocking legitimate emails, or hiring an expensive consultant, CIO John Shaffer looked for a DIY DMARC solution. After comparing multiple vendors John found "OnDMARC was reasonably priced and very easy to use". With OnDMARC's tools John successfully tackled three key areas:

1) Visibility Greenhill uncovered 2,734 unauthorized email sources sending 671,000 fake emails from a parked domain, all of which were blocked using OnDMARC. OnDMARC also provided a clear visual of each legitimate email source's DKIM and SPF status which had once been a challenge for the firm.

2) Expertise With Mimecast already in place, DKIM and SPF settings were available, but it simply wasn't apparent to Greenhill's team where to begin. CIO John Shaffer explained, "We didn't know much about DMARC or how to configure it properly but OnDMARC gave us instructions on how to configure Mimecast".

3) Ongoing protection With their domains in reject, Greenhill still continues to have visibility of ongoing protection with OnDMARC which is actively blocking unauthorized email activity. As one example, over 640,000 spoof emails were blocked in just 3 months successfully protecting themselves, their clients and their prestige reputation.

> *"We used Mimecast for content filtering which did have DKIM settings in there and SPF to some extent but I didn't know how to put it all together. OnDMARC provided that link and connected the dots allowing me to configure Mimecast by myself."*
>
> *John Shaffer, Chief Information Officer, Greenhill*

Confidently transitioning to full protection

One of the common challenges, when dealing with email security, is the fear that changes may affect the entire organization by blocking legitimate emails which John Shaffer at Greenhill, admitted like most email security executives: " this can make it scary". Thanks to OnDMARC this wasn't the case as John found "We've been able to take a cautious approach to it which OnDMARC has enabled us to do by clearly seeing the extent of the issue and then making it relatively easy to transition into full protection. We know we can lean on the OnDMARC folks and their easy-to-use technology". Since using OnDMARC the financial institution has put all four domains into reject and observed from their reports after flicking the switch that large phishing campaigns being targeted at their domain weren't successful as they were blocked from being delivered.

Discovering limits and swift solutions with Dynamic SPF

As CIO, John took the lead and worked independently on implementing DMARC via OnDMARC's intuitive dashboard. After telling the OnDMARC team "It's rare we need to go in and check anything on the system, but shortly after deployment we discovered we were close to the 10 SPF lookup limit. By switching on OnDMARC's Dynamic SPF feature we were able to configure it all directly inside OnDMARC's portal versus going into our DNS manually and altering it". The team now manage 16 lookups inside OnDMARC which has allowed them to break the 10 lookup limit and remove the hassle of continual manual updates in their DNS. With ongoing insight into their SPF queries for all the authorized senders there is flawless automation at work and this, in turn, improves email deliverability. The firm has also seen its SPF pass rate increase from 79.70% to 100% since using OnDMARC.

> *"OnDMARC seemed like a very reasonable price and during our free trial the portal itself seemed very well thought out and easy to use"*
>
> *John Shaffer, Chief Information Officer, Greenhill*

Get in touch today to find out more about how you can use OnDMARC to secure your domain and protect both your reputation and clientele from email impersonation.

Member CyberExchange

Member of Microsoft Intelligent Security Association Microsoft

UK CLOUD AWARDS 2019 WINNER

2017 Computing Security Awards WINNER Anti Phishing Solution of the Year

bsi. ISO/IEC 27001 Information Security Management IS 672913

GLOBAL CYBER ALLIANCE

ONDMARC

The Red Sift Open Cloud is a data analysis platform that is purpose-built for the challenges of cybersecurity. By harnessing the power of AI we can securely collate, compute & visualize data from thousands of individual signals to help organizations to optimize their cybersecurity.

Our first product on the Red Sift platform is OnDMARC, a SaaS product that helps to implement and maintain DMARC. This email authentication protocol effectively blocks phishing attacks and increases the deliverability of genuine emails.

www.ondmarc.redsift.com
contact@redsift.com
@redsift