Case Study

Achieving full DMARC ‘p=reject’ status within five weeks assures email security and deliverability for investment firm

KILLIK & Co

Save | Plan | Invest

Client Profile

Based in London’s Mayfair, Killik & Co is an independently-owned investment house that has been advising clients on how to save, plan and invest for over 30 years.

Their first branch opened in Chelsea in 1989 and they have since built a network of local branches across London and Surrey, managing assets for over 27,000 clients. They have sponsored the eponymous ‘Killik Cup’ annual rugby tournament since 2011.

Killik & Co’s 300 users are supported by their internal IT and development teams, both of which report into their CTO.

Client Testimonial

“I’m very pleased with the DMARC service Autodata recommended and how straightforward it was to install and implement. From an InfoSec perspective it’s important to have DMARC in place.

The offering from Red Sift met our needs well, our weekly onboarding communications together were very good and they successfully delivered our DMARC configuration into Reject mode within the timescales claimed at the outset.”

DAN YOUNG - HEAD OF IT SERVICE & SUPPORT, KILLIK & CO

Business Need

As an award-winning private-investment firm, Killik & Co prioritise cyber security and the safeguarding of their clients’ data. They already deploy a leading email-filtering solution for protection on incoming emails, but were keen to implement the email authentication, policy and reporting protocol known as DMARC (*Domain-Based Message Authentication, Reporting and Conformance*) to ensure a similar level of protection on outgoing email.

Once fully configured in a policy of p=reject, DMARC works in conjunction with existing SPF and DKIM protocols to ensure that all outgoing emails sent using the registered domain are legitimate. This prevents all direct email-based brand impersonation and spoofing which can be extremely damaging to a brand’s reputation. Although Killik & Co had no specific issues relating to email deliverability, DMARC has the additional benefit of helping to improve deliverability rates for marketing emails by automatically creating a record with metadata about the validation status of every email it receives from an organisation.

Killik & Co’s Head of IT Service & Support, Dan Young, was keen to get DMARC in place and fully-configured within a short timeframe so he could get on with other projects. However when he checked directly with an incumbent vendor who offered a DMARC service, they advised it would take around 12 months to get his DMARC into a policy of Reject (p=reject).

Solution

Autodata has been working with Killik & Co since 2013. DMARC had already come up in general conversation, so Dan subsequently asked for our opinion relating to indicative costs and timeframes for full DMARC implementation.

Autodata recommends **Red Sift’s ONDMARC** product for quick, cost-efficient and supported DMARC implementation. In order to provide a comparison with the other DMARC product, Dan ran a technical trial with both vendors and compared the costs and service offerings.

Instrumental to his decision to select Red Sift was their commitment to a drastically shorter timeframe (maximum two months) to achieve Reject mode, coupled with the fact their associated consultancy/managed service was included in the quoted price. The competing vendor, whose DMARC product had been acquired and not fully-integrated with their other solutions, quoted their support service separately and at a higher cost than Red Sift.

Killik & Co had weekly calls with Red Sift’s Customer Success Team to guide them through the DMARC process step-by-step, successfully ensuring they reached p=reject **within five weeks**. This timeframe was aided by the fact that Dan’s IT team exerts significant control over the business’ IPs and no new sending services are set up without their involvement.

Result

Dan is pleased to have another security tool fully implemented to enhance Killik & Co’s overall security posture. DMARC is also valuable for compliance purposes; Dan remarked that it is often cited on cyber security questionnaires that the business is required to complete in order to implement new services or take on new partners.

Outside of the regular weekly onboarding and getting-to-reject meetings, Dan found Red Sift very helpful and responsive whenever he or his team had additional questions. Red Sift also introduced him to BIMI (*Brand Indicators for Message Identification*), an additional authentication protocol enabling the use of brand-controlled logos within supporting email clients. BIMI is valuable for marketing efforts, but cannot be implemented until a Customer has first implemented DMARC in a policy of Quarantine or Reject.

256-260 Old Street, London, EC1V 9DD
t. +44 (0) 207 749 7949 | e. salesteam@autodata.co.uk