SMARTER EMAIL AUTHENTICATION
DMARC + BIMI > SPF + DKIM

THE PROBLEM

With email impersonation on the rise, how do you protect your brand and reputation from email fraud? There has been a significant rise in cases where cybercriminals spoof company email accounts and impersonate executives to try and fool an employee into executing unauthorised transfers or sending out confidential information to gather data for other criminal activities.

Even though many organisations are aware of Business Email Compromise (BEC), few recognise is not just a C-level issue - HR, IT and Finance also are prime targets. They continue to overlook the need to apply all necessary controls to protect their business and that of their customers. The right controls make it difficult for cybercriminals to impersonate emails and build confidence that an email originates from a legitimate source.

Over and above the risk management aspects, there are potentially huge cost and time implications dealing with the consequences of email fraud.

THE IMPACT

Impersonation drives the primary cybersecurity attack vector: Phishing, with BEC attacks alone causing at least $26 billion in losses in the past five years, according to the FBI. Other sources have noted that 83% of email attacks are brand impersonations and another 6% are impersonations of people, meaning nearly 90% of all email attacks rely on deceptive sender identity.

Businesses, and in particular financial institutions, are now being increasingly targeted due to their larger financial transactions and the greater potential profits for fraudsters. It is believed that nearly half a million SME businesses in the UK have been impacted by these scams. Aside from the financial costs, being a victim of fraud can cause serious reputational damage for businesses. In addition, one in five victims have had to make employees redundant due to the financial impact.

THE SOLUTION

DMARC and **BIMI** technologies are widely recommended by a variety of government agencies and industry organisations, including the UK's National Security Cyber Centre (NSCC), due to their effectiveness at curbing the most pernicious forms of phishing, and gaining control over the many email senders that organisations use.

ABOUT KA2

KA2 partners with companies in highly regulated sectors to achieve better business outcomes through security-driven IT transformation. Our bold, holistic approach is guided by the KA2 Smarter Framework which combines the KA2 Compliance Workflow Engine™ and domain expertise to help companies transcend silo-thinking and charter a transformation course guided by information security and compliance.

We specialise in delivering solutions that accelerate business transformation and provide an enhanced user experience for customers and employees. Our multi-dimensional perspective enables us to realise smarter and sustainable results for our clients, so they can deliver better outcomes and services for their clients and end users.

58%

increase in reported BEC attacks in 2019, according to Lloyds Bank

DMARC (Domain-based Message Authentication, Reporting and Conformance) is designed to give email domain owners the ability to protect their domain from unauthorised use. The purpose and primary outcome of implementing DMARC is to protect a domain from being used in phishing emails, email scams and business email compromise.

BIMI, (Brand Indicators for Message Identification) is a new standard created to make it easier to get your logo displayed next to your message in the inbox. It works alongside SPF, DKIM and DMARC to signal to email clients that you are you. Combined, all of these authentication methods will make for more reliable deliverability and a better reputation overall.

SMARTER EMAIL AUTHENTICATION
DMARC + BIMI > SPF + DKIM

KA2 has undertaken analysis of 1,000 random domains in the UK across multiple market sectors and have identified that only 90 domains have the full protection offered by DMARC and have BIMI enabled.

KA2's Smarter Email Authentication Assessment is an accelerated 30 day programme utilising our domain expertise to assess your existing email protocols, optimise where appropriate, and implement the recommended message authentication, including DMARC and BIMI. The **KA2 Compliance Workflow Engine™** will create, amend and approve the required corporate policies.

In addition to the core 30 day engagement, the KA2 Smarter Framework can deliver DMARC integration with your CRM, SaaS services and digital marketing strategy.

THE BENEFITS

- Significantly reduce email impersonation
- Improved message delivery rates and customer engagement
- Significantly reduce risk of financial fraud and data breaches
- Protect your brand reputation
- Increased confidence in email legitimacy
- Mitigate the message quarantine trap
- Provide enhanced customer security
- The KA2 Smarter Framework ensures an accelerated AND successful project delivery AND a rapid return on investment

Get in touch with our experts to discuss how secure your email and brand reputation from increasingly sophisticated security threats.

Andy Downs, Head of Digital Transformation

+44 (0) 203 978 1813
andy.downs@ka2.io

HOW DMARC WORKS