



DMARC | SPF | DKIM | BIM | TLS

SMBsecure™

Managed DMARC & TLS

Cyber criminals can hijack and impersonate email domains to trick and defraud users, suppliers and customers.

Your Business's Email Could Be Next!

Overview of Service

SMBsecure™ Email Security Compliance is an easy to add-on vital email security service that protects your business's email domain(s) and safeguards against cyber threats such as phishing and Business Email Compromise (BEC) through impersonation attacks. This service enhances safety and credibility with users, clients and suppliers. It increases trusted delivery for your business emails, controls email sending sources, monitors for blacklisting and fortifies email security for your business email domain(s).

Protect Business Email & Improve Business Email Deliverability with **SMBsecure™**.

HOW IT WORKS

This **SMBsecure™** service add-on enhances safety for your Email domain(s) and DNS records. Fundamental security risks that could harm business integrity are assessed, remediated and fully monitored for you. **Can you read XML reports?** You don't have to! This service includes ongoing monitoring and tuning for the optimised use of email authentication & security protocols.

It's more than just record changes!

> It's a monthly managed service to do it right and ensure compliance & keep your business email domain(s) secure!

ESSENTIAL EMAIL SECURITY FOR YOUR BUSINESS



SMBsecure™ Email Security Compliance addresses vulnerabilities in your domain and business email security. It focuses on critical email authentication standards (protocols) for protecting the outbound email channel to defend against threats such as mailbox spoofing, phishing, C-Level fraud, and business email compromise (BEC).

ELEVATE YOUR EMAIL SECURITY STANDARDS



DMARC, DKIM, SPF, and BIM are powerful email authentication protocols that collectively establish sender legitimacy, prevent email impersonation, and safeguard the integrity of outbound email communications. With these protocols in place, you can ensure the authenticity and integrity of the emails sent by your business, bolstering your business' trustworthiness in the digital realm. **MTA-STS** on the other hand will ensure encryption of the email channel with **TLS** to provide secure inbound email communications.

MITIGATE RISKS AND IMPROVE REPUTATION



By implementing strong email authentication measures, your business can mitigate the risks associated with cyberattacks, phishing attempts, and fraudulent emails using your email domain. Maintaining a secure email ecosystem enhances your online reputation and delivery trust among your customers, suppliers, and stakeholders. The service includes ongoing monitoring for unknown email sources, email quarantine and rejections, and blacklisting of your domain(s).

DMARC AND TLS'S CRUCIAL ROLE



DMARC unifies SPF and DKIM protocols to prevent email phishing attempts that exploit domain spoofing. **TLS** mitigates Man-In-The-Middle (MITM) attacks by ensuring encryption of inbound emails. Despite its efficacy and relatively low cost, DMARC and TLS adoption remains low due to its complexity and misconfiguration. Attackers and scammers take advantage of this fact! **SMBsecure™** helps bridge this gap with this service by simplifying the implementation, ongoing monitoring, auditing and optimisation of DMARC and MTA-STS (TLS).

EASY IMPLEMENTATION



SMBsecure™ streamlines the implementation process of SPF, DKIM, DMARC, and MTA-STS (TLS) records. With direct assistance and guidance, we effortlessly enhance your email security posture. **SMBsecure™** reduces the risk of phishing, BEC and improves deliverability of business emails.