Secure your business domains from cyberattacks

91% of cybercrimes start with an email, and phishing attacks reached a record high in 2023, with no signs of decreasing in 2025. This means your business must secure its email domains or risk the potentially irreparable damages of a successful cyberattack.

> 70% of businesses faced major disruption from breaches in 2024, with the healthcare & financial sectors experiencing the highest financial losses.

Source: IBM Cost of a Data Breach Report 2024

What is DMARC?

Domain-based Message Authentication, Reporting, and Conformance (DMARC) is a global email authentication standard that verifies the source of outbound emails and makes sure only real emails ever reach an inbox. It's backed by global email giants like Google, Yahoo, and Microsoft, as well as regulators and governments.

The email problem

In today's digital world, email remains essential to personal and professional communication. But it's also a prime target for cybercriminals due to its design flaw, which lets cybercriminals send emails impersonating trusted senders.

DMARC benefits

Increase security & trust

Verifies sender identity and email integrity, reducing the risk of a successful cyberattack

Maximize deliverability

Emails from domains with a strong DMARC policy are more likely to reach the inbox

Improve visibility & control

Provides reports on who's sending on your behalf so you can authorize legitimate senders and block malicious ones

Comply with global standards

DMARC's ability to verify email authenticity helps organizations meet multiple compliance standards

Why Sendmarc

People

A team of committed global DMARC experts who truly care about your success

Platform

A leading DMARC platform built to drive your success

Promise

A DMARC company that guarantees full protection within 90 days*

*For customers on Sendmarc's Premium Plan, subject to the number of domains.

ARMD digital
advance risk mitigation digital

Powered by SENDMARC