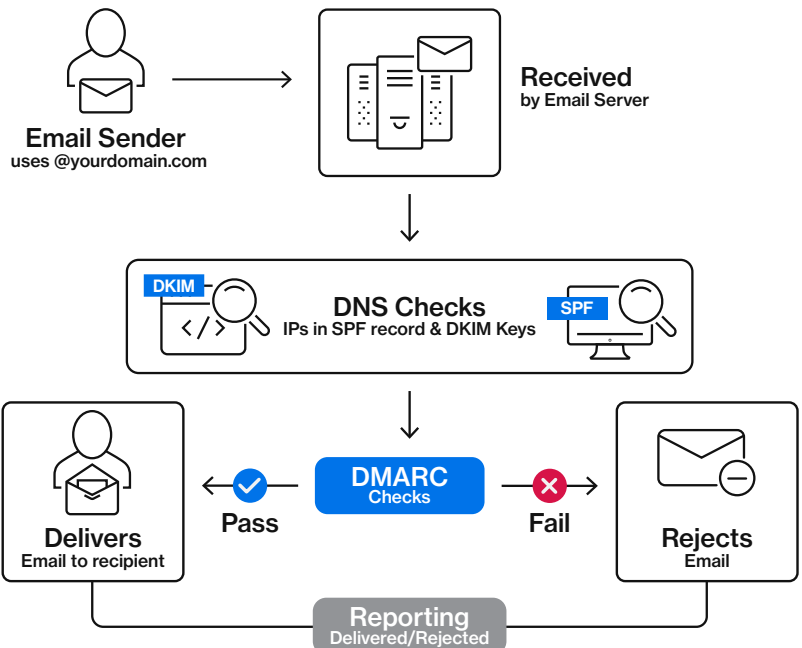# SENDMARC

Joining Forces to Make the Internet a Safer Place

Cybercrime is continuously surging, with attackers using increasingly sophisticated techniques and technologies to compromise data and breach security systems. This poses a significant threat to modern businesses. That's why we've Partnered with Sendmarc to arm organizations with the solutions to beat data breaches and email-based cyberattacks.

DMARC: What it is & how it works

Email is used in over 91% of network attacks, with cybercriminals becoming increasingly skilled at impersonating unprotected email domains.

Domain-based Message Authentication, Reporting and Conformance (DMARC) is a global email authentication standard that verifies the source of an email and makes sure only real emails ever reach an inbox. It provides full visibility and control over emails claiming to be from your business, ultimately securing your domain and improving email deliverability.

Email Sender uses @yourdomain.com

Received by Email Server

DKIM

DNS Checks IPs in SPF record & DKIM Keys

SPF

DMARC Checks

Delivers Email to recipient

Pass

Fail

Rejects Email

Reporting Delivered/Rejected

DMARC benefits
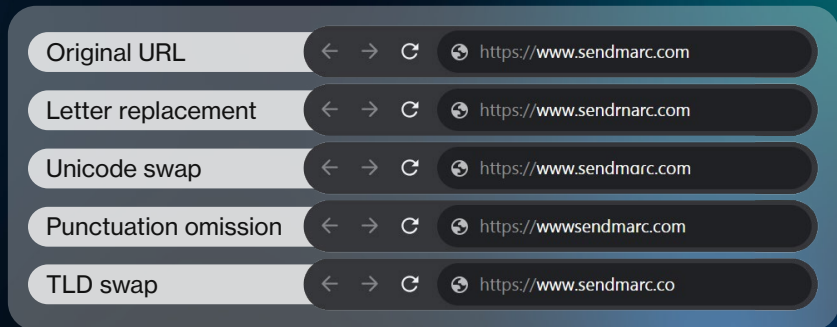
Maximize deliverability

Protect your brand

Avoid financial implications

Build customer trust

Gain visibility through reports

Comply with global standards

LOGICALIS
Architects of Change

In partnership with:

SENDMARC

Further protect your business
from cyberattacks

The digital nature of the Internet and cloud services in modern workspaces leaves your business vulnerable to various cyberthreats including credential breaches and lookalike domain attacks. Sendmarc can help your business gain visibility of its vulnerability to these threats.

Sendmarc Lookalike Domain Defense

Cybercriminals use lookalike domains (domains that look extremely similar to an organization's original domain/s) to perform convincing impersonation attacks, using fake emails or websites, to trick users into disclosing their data or credentials.

		https://www.sendmarc.com
Original URL	← → C ⊕	https://www.sendmarc.com
Letter replacement	← → C ⊕	https://www.sendrnarc.com
Unicode swap	← → C ⊕	https://www.sendmarc.com
Punctuation omission	← → C ⊕	https://wwwsendmarc.com
TLD swap	← → C ⊕	https://www.sendmarc.co

Example of lookalike domains

To combat this threat, Sendmarc Lookalike Domain Defense provides:

- Visibility of existing lookalike domains
- A watchlist of existing lookalike domains
- Notifications of new domain permutations (which will be added to the watchlist)
- Identification of web presence and email capability of lookalike domains

Sendmarc Breach Detection

Businesses don't know what data criminals have stolen from their employees and/or third parties that can cause damages such as an environment breach, operational disruption, decreased trust and financial loss.

To safeguard your business against this, Sendmarc Breach Detection monitors multiple sources, including the dark web, to:

- Detect any system breaches
- Reveal leaked user credentials
- Regularly check for breaches and leaked credentials
- Alert you about breaches (once notifications are set up)
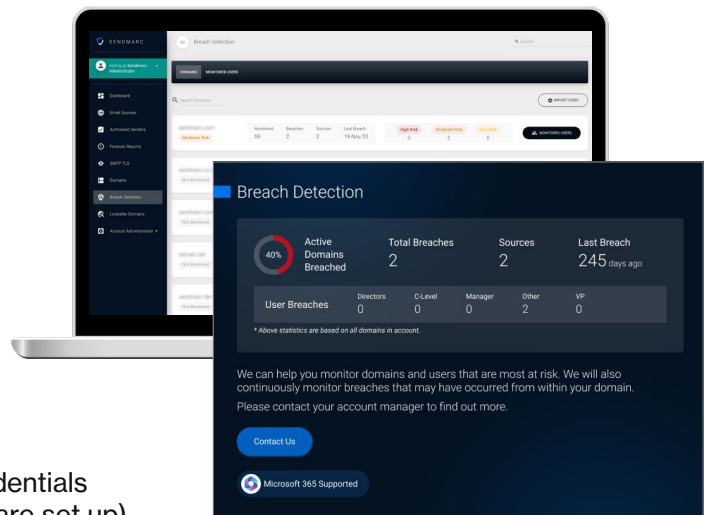
Using the data gathered from these products, your business can take the necessary steps to mitigate these risks, increase protection and avoid potential damages. **Contact us to start your journey to protection today.**

LOGICALIS
Architects of Change

In partnership with:

SENDMARC