Email Authentication Made Simple

DMARC is the trusted solution that brings together email authentication protocols, and adds reporting and compliance. In just a few steps, you can set up DMARC today to protect your organization from email fraud.

What is DMARC?

DMARC stands for Domain-Based Message Authentication, Reporting and Conformance. It’s like an identity check for your organization’s domain name. A DMARC policy allows a sender to indicate that their messages are protected and tells a receiver what to do if one of the authentication methods passes or fails – either send the message or reject the message to junk. DMARC will protect your brand by creating a high level of trust and integrity.

Business Impact

For organizations that use email to engage with customers, DMARC can be a major benefit for business. DMARC improves the delivery rate of the email you send to customers. It tells a recipient’s email server that your company’s message is authentic and safe, and helps prevent your company’s email from being flagged as spam.

DMARC helps prevent malware and phishing scams from being launched using your domain, and helps protect your internal network against inbound threats.

With DMARC, your company’s domain – and brand reputation – will be better protected.

SET UP DMARC NOW AT dmarc.globalcyberalliance.org

Volume of spam emails INCREASED 4 TIMES IN 2016

76% of organizations reported at least one PHISHING ATTACK

Average business user faces at least ONE RISKY EMAIL EACH DAY
How DMARC Works

GUESSING ISN’T WORTH THE RISK.

In 3 steps, DMARC ensures emails don’t come with any surprises. DMARC, SPF and DKIM work together to ensure stronger authentication.

GUESSING ISN’T WORTH THE RISK.

In 3 steps, DMARC ensures emails don’t come with any surprises. DMARC, SPF and DKIM work together to ensure stronger authentication.

DMARC Setup Guide

Now Available in Several Languages

Now, you can learn how to setup DMARC in many common languages, including French, Spanish, Japanese, Mandarin and more. Visit the website for a complete list of language options.

DMARC Setup Guide

Now Available in Several Languages

Now, you can learn how to setup DMARC in many common languages, including French, Spanish, Japanese, Mandarin and more. Visit the website for a complete list of language options.

Detect Fraud. Prevent Threats.

DMARC provides a way for participating senders and receivers to streamline the analysis process by coordinating their verification efforts. This prevents spammers and phishers from using valid organization names to conduct cyber attacks and provides insight into any attempts to spam, phish, or spearphish using your organization’s brand or name. Using DMARC, businesses can reduce the likelihood that their domain will be used in an attack, and they’ll be protected against incoming threats from other compromised domains. As a result, this increases customer confidence and builds trust in your brand.

DMARC Setup Guide

Now Available in Several Languages

Now, you can learn how to setup DMARC in many common languages, including French, Spanish, Japanese, Mandarin and more. Visit the website for a complete list of language options.

Detect Fraud. Prevent Threats.

DMARC provides a way for participating senders and receivers to streamline the analysis process by coordinating their verification efforts. This prevents spammers and phishers from using valid organization names to conduct cyber attacks and provides insight into any attempts to spam, phish, or spearphish using your organization’s brand or name. Using DMARC, businesses can reduce the likelihood that their domain will be used in an attack, and they’ll be protected against incoming threats from other compromised domains. As a result, this increases customer confidence and builds trust in your brand.

DMARC Setup Guide

Now Available in Several Languages

Now, you can learn how to setup DMARC in many common languages, including French, Spanish, Japanese, Mandarin and more. Visit the website for a complete list of language options.

Detect Fraud. Prevent Threats.

DMARC provides a way for participating senders and receivers to streamline the analysis process by coordinating their verification efforts. This prevents spammers and phishers from using valid organization names to conduct cyber attacks and provides insight into any attempts to spam, phish, or spearphish using your organization’s brand or name. Using DMARC, businesses can reduce the likelihood that their domain will be used in an attack, and they’ll be protected against incoming threats from other compromised domains. As a result, this increases customer confidence and builds trust in your brand.