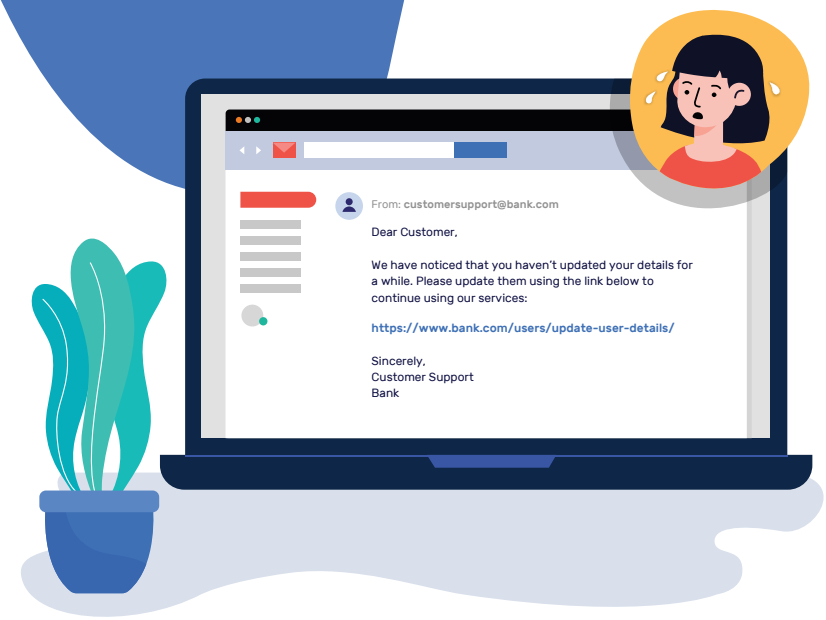
POWERDMARC

Datasheet

What is DMARC?

DMARC (Domain-based Message Authentication, Reporting and Conformance) is an email authentication system that protects your organization's domains from spoofing, phishing and other cyber attacks. It builds on the widely deployed email verification techniques: SPF (Sender Policy Framework) and DKIM (Domain Keys Identified Mail).

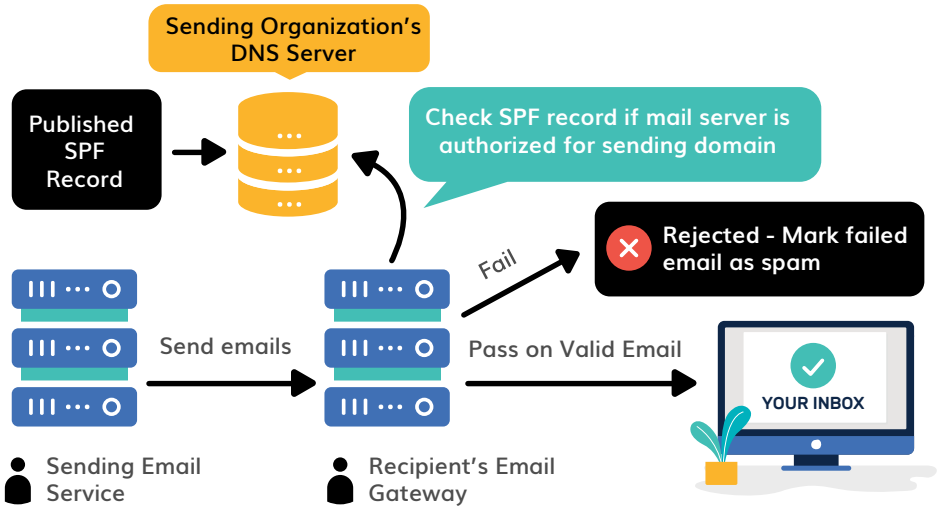


What kind of threats does it protect against?

DMARC protects against exact-domain attacks that spoof the header From: address, which is the one you see in the From: field. Without DMARC, emails that appear to originate from your domain can be used to steal personally identifiable information (PII).

What is SPF?

SPF (Sender Policy Framework) specifies the servers that are allowed to send emails on your domain's behalf.



What is DKIM?

DKIM, or **Domain Keys Identified Mail**, creates a digital signature, allowing senders to claim responsibility for messages and guarantee content has not been modified.

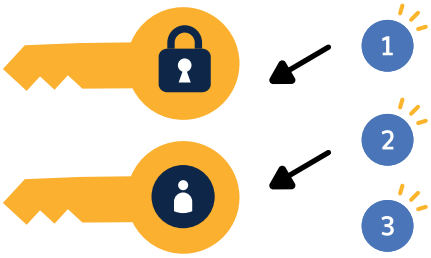
How does it work?

DKIM relies on **cryptography**, allowing senders to generate a pair of keys which are used to "sign" emails.

The **PUBLIC KEY** is published for internet service providers to access.

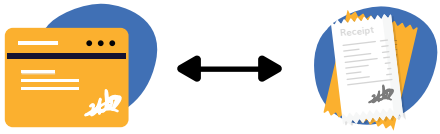
The **PRIVATE KEY** is kept on the outgoing mail server.

How are the keys used?



1. The PRIVATE KEY is used to create a signature for message content and key headers.
2. When the message is delivered, the destination server asks for a public key to verify the signature is right.
3. A matching signature means successful validation

Think of it this way: when you pay for something by credit card, the merchant checks your signature on both the **RECEIPT** and the **CARD** to confirm identity. DKIM operates on the same principle!



So, how does DMARC build on SPF and DKIM?

Unfortunately, SPF and DKIM cannot authenticate the header **From:** domain name on their own. DMARC addresses that by introducing the 'alignment' feature. This ties together either the **'Mail From/Return-Path'** domain or the domain in the **'d='** DKIM signature field to that displayed in the header **From:**, hence authenticating the email.

DMARC also introduces a reporting feature that allows you to gain insight on your email traffic and boost your deliverability. However, these DMARC reports are generated in a not so easy to read XML format. Not to worry, PowerDMARC takes care of that for you by fetching the data from these reports and displaying them in easy to read charts.