POWERDMARC

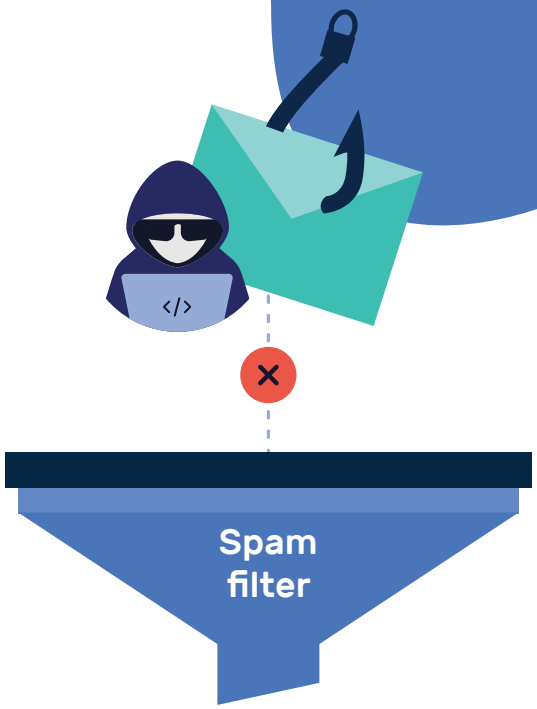
Datasheet

Is DMARC Just a Glorified Spam Filter?

Spam Filters Only Block Incoming Emails

Phishing emails are always changing, making it difficult for people to recognize them. Spam filters use algorithms to constantly monitor and detect email spam trends. When an email ticks enough boxes on their list to raise suspicion, the filter marks it as spam and blocks it.

While spam filters have gotten very good at their job, they're still only meant to do one thing. Reject incoming spam email. They don't do anything about emails **sent from your domain**, which means an attacker could still impersonate your brand to send phishing emails to the public.



Double Down on Brand Protection With DMARC

The biggest difference between DMARC and spam filters is that **DMARC keeps other people safe from fake emails** that use your domain name. When you use a spam filter, only your inbox is safe from phishing emails.

DMARC uses email authentication protocols to ensure that if an attacker tries to impersonate your brand and send emails, any receiving server blocks them.

This means that you're not just protecting your customers from phishing attacks, but you're **safeguarding your own brand image.** When you enforce DMARC, attackers won't be able to use your domain to send emails either internally in your organization or to the public.

If you thought spam filters were enough, think again. Find out how you can protect your brand from email spoofing now!