Email Authentication

Criminals use domain spoofing in spear-phishing attacks to trick victims into disclosing sensitive information, transferring money, or downloading malware. A lot of these attacks are successful because many organizations do not have email authentication and DMARC policy set up properly.

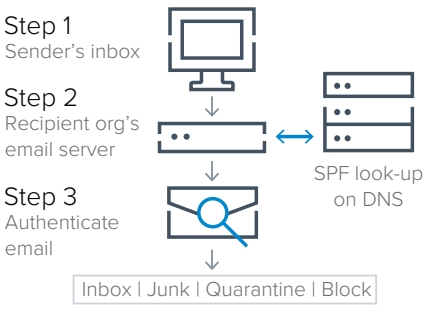
What is email authentication?

Email authentication helps recipients validate and verify that email comes from a legitimate source. It is relatively easy and inexpensive, and can prevent many impersonation attacks.

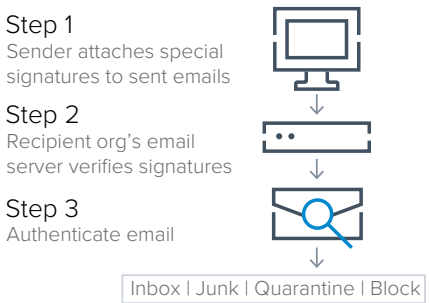
While email authentication should be part of every organization's email security strategy, many lack sufficient understanding of authentication standards and therefore find it difficult to properly configure them. As a result, they rely instead on inefficient and time-consuming manual processes—increasing risk from email-borne attacks.

What are the standards?

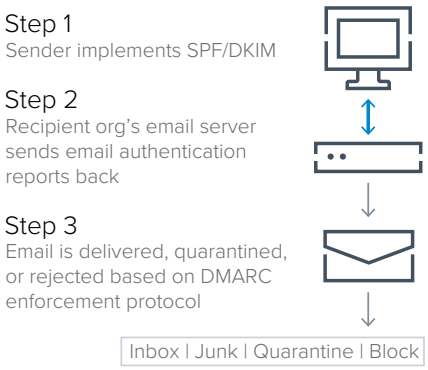
Sender Policy Framework (SPF) is essentially a reverse-DNS lookup. It checks if an email originates from a valid IP address or an IP range associated with email domain. Based on this information, the recipient of an email can determine whether they want to quarantine, block, or deliver the message.



Domain Keys Identified Mail (DKIM) is used to verify that the content of an email is trustworthy, meaning the content has not been changed from the time the email was transmitted by the sending mail server. The sender attaches special signatures to an email for authentication purposes. DKIM will link email back to the domain through these signatures attached to the message for the sender to verify that the email domain and the content of the message have not been changed. If email gets altered in-flight it changes the domain keys that are tied to an email.



Domain-based Message Authentication, Reporting and Conformance (DMARC) supports SPF and DKIM by presenting a clear policy. DMARC provides reports and insights into how an email domain is used, based on the data from SPF and DKIM implementation. The owner of the email domain can set up DMARC policy, based on interpretation of these reports, that will dictate what should be done with email that failed SPF and DKIM.



What are the benefits of SPF, DKIM, and DMARC?

Anti-spoofing and brand protection. Detect and prevent spammers, phishers, and fraudsters impersonating your brand and email domain. Properly set-up DMARC policies can help prevent all forms of domain spoofing.

Improve email deliverability. If recipients can verify and validate that the email is coming from a legitimate source, it enables them to accept the email as legitimate without questioning it. DMARC helps ensure that business-critical mail will reach recipients' inboxes.

How can Barracuda help?

Barracuda Email Protection provides complete protection from email domain fraud through DMARC reporting, analysis, and visibility into how your email domain is being used. It helps you to set up DMARC enforcement properly and reduce the potential of false-positive enforcements such as blocking legitimate email or misidentifying legitimate senders.

Barracuda
Your journey, secured.