**SPF, DKIM, and DMARC Email Authentication Protocols**

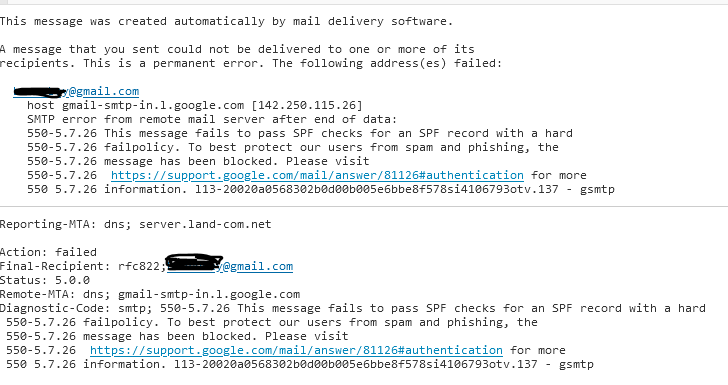
DMARC (Domain-based Message Authentication, Reporting, and Conformance) is an email protocol that uses the protocols DKIM (DomainKeys Identified Mail) and SPF (Sender Policy Framework) to prevent spoofing and validate email authenticity. If an email fails either SPF or DKIM, the email will be rejected or quarantined.

SPF first checks to see if the email came from a mail server that is authorized to send from your domain (google.com,outlook.com, etc). This can be updated in your DNS settings by altering the TXT records. The syntax of the record is:

v=spf1 ip4:’your ip address’ include:’domain name’ -all

(note: syntax can change depending on the domain server).

“V” indicates the version of SPF, “ip4” indicates the ip address of the mail server allowed to send emails, “include:” indicates a valid source of the email, and “-all” is a hard fail if SPF check fails.

Failed SPF with a hard fail policy.

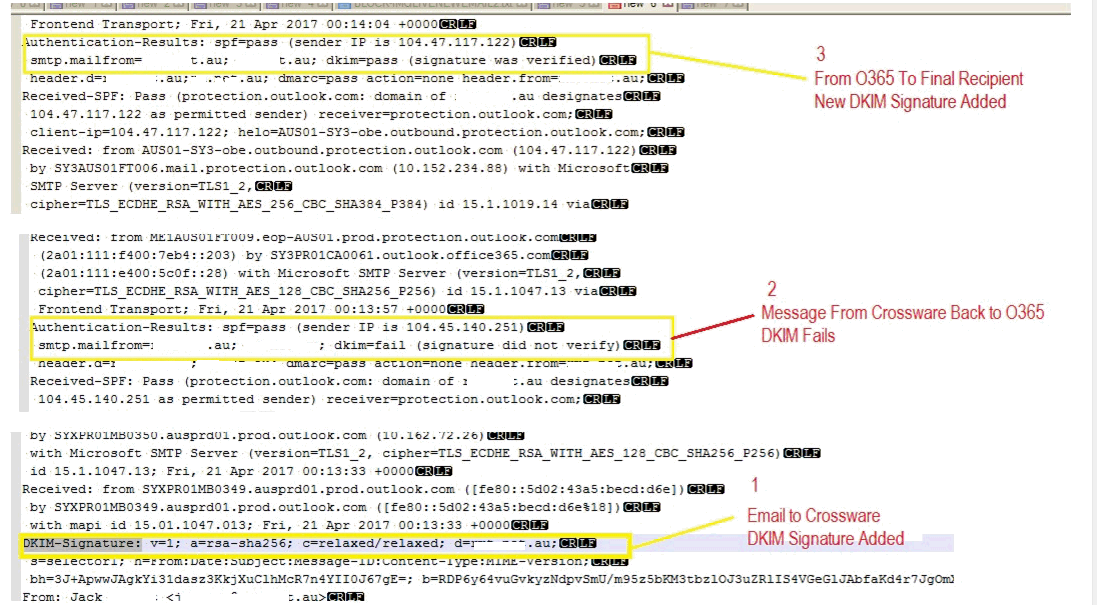
DKIM (DomainKeys Identified Mail) used digital signatures, a public key, and a private key to ensure the integrity of the contents of the email. Microsoft will generate keys for you, but you will have to create and add the Cname record to the domain.  The email is sent using the sender's private key in a digital signature included in the email header. The receiver of the email checks the email server of the sender to see if the keys match. The syntax of the Cname record is:

Hostname: selector1.\_domainkey

Points to address or value: selector1-<CustomDomain>. \_domainkey. <InitialDomain>

(note: selector1.\_domainkey is used for all Microsoft 365 organizations)

The “CustomDomain” field is where your domain is entered (ex. cybersafe.com). The “InitialDomain” field is where your domain is entered with your email service provider (ex. cybersafe.onmicrosoft.com)

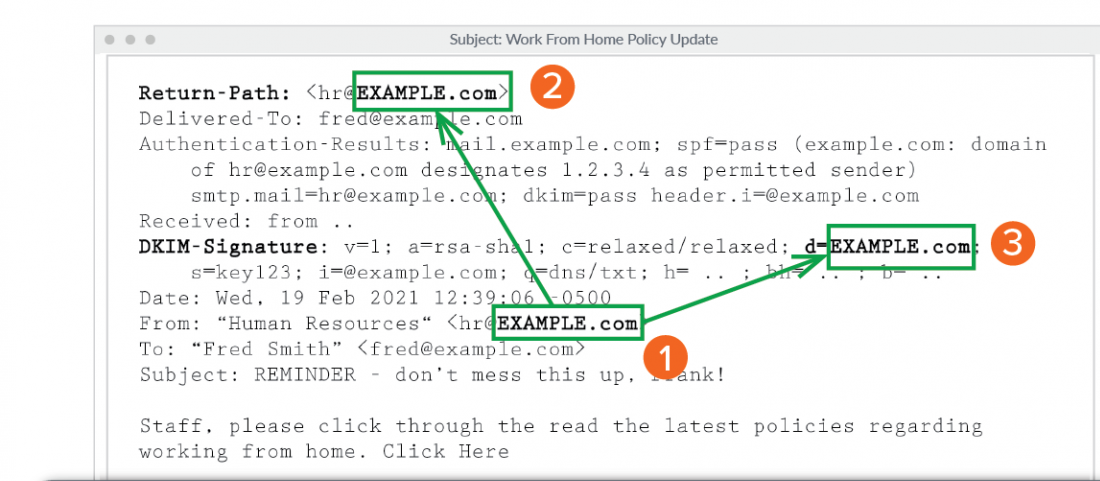
Here we have an SPF that passed, but failed DKIM.

It is best practice to rotate the keys generated every few months, or immediately after a cyber-attack.

DMARC tells your email server what to do if a received email passes or fails both SPF and DKIM. You can set the policy to do nothing, reject, or quarantine the email. The TXT record is set in the DNS settings. The syntax for the DMARC record is:

v=DMARC1; <DMARC policy>; <Percentage of DMARC failed mail subject to DMARC policy>; <DMARC reports>

“v” indicates the version and “policy” is what you decide to do to the email (reject, quarantine, or nothing). The percentage indicates what percentage of emails does the policy apply to, and reports lets you decide where to send reports to if needed. If both SPF and DKIM pass the email is accepted. If either fail, your DMARC policy determines what happens to the email.



Continuously keep SPF, DKIM, and DMARC records updated to keep your network, system and users safe.