Phishing
AI POWERED PROTECTION

TECNOLOGIE

SPF, DKIM e DMARC: le fondamenta tecniche che ogni azienda deve implementare

I tre standard di autenticazione e-mail che bloccano lo spoofing prima che l'utente veda il messaggio

A cura del team CENANT di GPI Cyberdefence

26 febbraio 2026 www.gpiphishing.com

TECNOLOGIE

I tre standard di autenticazione e-mail che bloccano lo spoofing prima che l'utente veda il messaggio

01 Il problema dello spoofing

Uno dei motivi per cui il phishing funziona così bene è che il protocollo SMTP, lo standard su cui si basa la posta elettronica, è stato progettato decenni fa senza meccanismi di autenticazione del mittente. Chiunque può inviare un'e-mail che sembra provenire da qualsiasi indirizzo: *support@vostra-banca.it*, *titolare@vostrostudio.it*, *noreply@poste.it*.

SPF, DKIM e DMARC sono tre standard complementari che colmano questa lacuna. Quando correttamente implementati, permettono al server di posta del destinatario di verificare se l'e-mail è davvero inviata da chi dichiara di essere, e di bloccarla o metterla in quarantena se non supera i controlli.

02 SPF: chi è autorizzato a inviare per il vostro dominio

SPF (Sender Policy Framework) è un record DNS che elenca i server autorizzati a inviare e-mail per conto del vostro dominio. Quando un mail server riceve un messaggio che dichiara di provenire da “vostra-azienda.com”, consulta il record SPF e verifica se l'IP mittente è nella lista autorizzata. Se non lo è, l'e-mail fallisce il controllo SPF.

Configurazione essenziale: pubblicare nel DNS un record TXT con la direttiva **-all** alla fine, che significa "qualsiasi mittente non in questa lista è non autorizzato".

03 DKIM: la firma digitale dell'e-mail

DKIM (DomainKeys Identified Mail) aggiunge una firma digitale crittografica a ogni e-mail inviata. Il server mittente firma il messaggio con una chiave privata; il server destinatario verifica la firma usando la chiave pubblica pubblicata nel DNS. Se il messaggio è stato modificato durante il transito, anche di un solo carattere, la firma non corrisponde e il controllo fallisce.

DKIM garantisce che il messaggio provenga realmente da chi afferma di inviarlo, e che non sia stato alterato. Entrambe sono proprietà fondamentali per difendersi dal phishing.

04 DMARC: la politica che governa il tutto

DMARC (Domain-based Message Authentication, Reporting & Conformance) è il livello che mette insieme SPF e DKIM, definendo cosa deve succedere quando un'e-mail fallisce uno o entrambi i controlli. Le opzioni sono tre: **none** (solo monitoraggio), **quarantine** (sposta in spam), **reject** (blocca completamente).

> *Un dominio senza SPF, DKIM e DMARC è come una busta senza mittente verificato: chiunque può imitarla.*

DMARC fornisce anche un meccanismo di reporting: il vostro dominio riceve periodicamente rapporti aggregati su chi sta cercando di inviare e-mail spacciandosi per voi, informazione preziosa per rilevare campagne di phishing attive a vostro danno.

05 Raccomandazione pratica

Iniziare con **p=none** su DMARC per raccogliere dati senza impatto operativo, analizzare i report per alcune settimane, poi progredire verso **p=quarantine** e infine **p=reject**. Monitorare regolarmente i record con strumenti come mxtoolbox.com e ruotare periodicamente le chiavi DKIM.

GPI PHISHING — CYBERSECURITY PLATFORM

Implementa SPF, DKIM e DMARC per proteggere il tuo dominio e-mail

Configurazione guidata, monitoraggio continuo
e protezione completa dallo spoofing del dominio.

Phishing
AI POWERED PROTECTION

www.gpiphishing.com