Phishing
AI POWERED PROTECTION

FONTE
ACN · Aprile 2026

ANALISI

Nuove Linee Guida ACN sulla Posta Elettronica: tutto quello che devi sapere su SPF, DKIM e DMARC

Spoofing, autenticazione del mittente e normativa NIS 2: analisi delle raccomandazioni operative per PA e aziende

A cura della redazione di gpiphishing.com
04 maggio 2026 www.gpiphishing.com

Gpi Cyberdefence.

ANALISI

L'Agenzia per la Cybersicurezza Nazionale (ACN) ha pubblicato ad aprile 2026 le **Linee Guida per la Configurazione del Servizio di Posta Elettronica per l'Autenticazione**, un documento tecnico che ogni amministratore di sistema, responsabile IT e professionista della sicurezza informatica dovrebbe leggere con attenzione.

Il tema è centrale per chiunque si occupi di phishing e sicurezza delle comunicazioni digitali: la posta elettronica rimane il vettore d'attacco preferito dai cybercriminali, e il protocollo su cui si basa, l'SMTP, è strutturalmente privo di meccanismi nativi di autenticazione del mittente.

Perché la posta elettronica è ancora così vulnerabile

Il protocollo SMTP nasce nel 1982 in un contesto accademico, progettato per la semplicità e non per la sicurezza. Ancora oggi, chiunque può tecnicamente configurare un client di posta per inviare un messaggio spacciandosi per qualsiasi mittente, che si tratti del proprio istituto bancario, del proprio capo o di un collega.

Questo è il cuore del problema. Il documento ACN individua tre categorie principali di minacce che sfruttano questa debolezza strutturale:

MINACCIA 1

Spoofing del mittente

Falsificazione dell'indirizzo email per far apparire il messaggio come proveniente da una fonte fidata. Può avvenire sia a livello di *envelope-from* sia di *message-from*. La distinzione tra questi due campi è cruciale per capire i limiti di ciascun protocollo di difesa.

MINACCIA 2

Phishing

Attacchi finalizzati al furto di credenziali, dati finanziari o informazioni sensibili tramite messaggi ingannevoli. Il phishing sfrutta spesso lo spoofing, ma può anche usare domini simili (*typosquatting*) o account compromessi. La variante *spear phishing* personalizza il messaggio sulla vittima specifica.

MINACCIA 3

Manomissione del messaggio

Modifica del contenuto durante il transito, possibile in assenza di crittografia end-to-end. Un attaccante in posizione di man-in-the-middle può alterare testo, allegati o link senza che mittente e destinatario se ne accorgano.

IL DATO

SMTP: un protocollo del 1982

L'assenza di meccanismi nativi di autenticazione del mittente nell'SMTP è la radice strutturale di tutte e tre le minacce. SPF, DKIM e DMARC sono stati aggiunti decenni dopo, come strati aggiuntivi sopra il protocollo originale.

I tre pilastri della difesa: SPF, DKIM e DMARC

Le linee guida illustrano in dettaglio i tre protocolli che, se implementati correttamente e **congiuntamente**, costituiscono la risposta tecnica più efficace a queste minacce.

SPF — Sender Policy Framework

SPF permette al proprietario di un dominio di dichiarare, tramite un record DNS di tipo TXT, quali indirizzi IP sono autorizzati a inviare email per suo conto. Quando il server di posta del destinatario riceve un messaggio, interroga il record SPF del dominio mittente e verifica se l'IP di provenienza è tra quelli autorizzati.

Il limite fondamentale di SPF, che le linee guida sottolineano esplicitamente, è che la verifica avviene sull'*envelope-from* e non sul *message-from*: un attaccante può quindi aggirarlo spoofando solo il campo visibile al destinatario. **SPF da solo non basta.**

> *Le linee guida raccomandano di pubblicare un record SPF con politica `-all` anche per i domini non usati per la posta, per impedire che vengano sfruttati in campagne di spoofing.*

DKIM — DomainKeys Identified Mail

DKIM agisce in modo diverso: invece di verificare l'IP mittente, appone una **firma digitale crittografica** al messaggio. Il server mittente firma il messaggio con la propria chiave privata; la chiave pubblica corrispondente è pubblicata nel DNS e permette al destinatario di verificare che il messaggio non sia stato alterato durante il transito.

La firma copre specifici header (From, To, Subject, Date) e il corpo del messaggio, calcolando un hash che viene incluso nelle intestazioni del messaggio stesso.

Sul piano crittografico, le linee guida raccomandano **RSA a 2048 bit** come standard attuale, avvertendo che la variante più moderna Ed25519, pur tecnicamente superiore, non è ancora supportata in modo affidabile dai principali provider. Né RSA né Ed25519 sono resistenti ai computer quantistici: sarà necessario seguire gli sviluppi della crittografia post-quantum.

> *Le linee guida dedicano attenzione alla gestione delle chiavi: rotazione periodica (almeno ogni sei mesi), permessi restrittivi, revoca immediata in caso di compromissione.*

DMARC — Domain-based Message Authentication, Reporting and Conformance

DMARC è il livello che orchestra SPF e DKIM, colmando le lacune di entrambi. Il suo contributo principale è il meccanismo di **allineamento**: verifica che il dominio autenticato da SPF e/o DKIM corrisponda al dominio del campo *message-from*, quello visibile all'utente finale. È proprio questa verifica che impedisce agli attaccanti di superare SPF o DKIM usando un *message-from* diverso.

DMARC definisce anche la **politica** da applicare ai messaggi che non superano la verifica: **none** (monitoraggio puro), **quarantine** (spostamento nello spam) e **reject** (rifiuto del messaggio). Il percorso consigliato è progressivo: partire da *none* per raccogliere dati tramite i report aggregati, identificare eventuali mittenti legittimi non coperti, poi inasprire verso *quarantine* e infine *reject*.

> *I report DMARC sono uno strumento prezioso anche dal punto di vista difensivo: consentono al titolare del dominio di monitorare se il proprio dominio viene usato in campagne di spoofing e in che misura.*

Il quadro normativo di riferimento

Le linee guida si inseriscono in un contesto normativo articolato. Le raccomandazioni sono valide per qualsiasi organizzazione, indipendentemente dall'assoggettamento alle normative specifiche:

- **Perimetro di Sicurezza Nazionale Cibernetica** (D.L. 105/2019) — per i soggetti che gestiscono funzioni o servizi essenziali per lo Stato.
- **Regolamento Cloud per la PA** (Decreto ACN n. 21007/24) — richiede a tutte le pubbliche amministrazioni di classificare dati e servizi e adottare misure adeguate al livello di rischio.
- **Decreto NIS 2** (D.Lgs. 138/2024) — stabilisce misure di sicurezza di base per soggetti essenziali e importanti, includendo esplicitamente i servizi di posta elettronica.

Cosa fare in pratica

- Pubblicare record **SPF, DKIM e DMARC** per tutti i domini, inclusi quelli non usati per la posta.
- Configurare il server mittente per **firmare i messaggi con DKIM**.
- Configurare il server destinatario per eseguire le verifiche SPF, DKIM e **applicare le politiche DMARC**.
- Proteggere la chiave privata DKIM con **permessi restrittivi** e monitoraggio costante.
- Ruotare le chiavi DKIM **almeno ogni sei mesi**.
- Monitorare i **report DMARC** per individuare abusi e problemi di configurazione.
- Considerare **DNSSEC** per proteggere i record DNS stessi da manipolazioni.

Perché questo documento è importante

Adottare SPF, DKIM e DMARC con politica *reject* non elimina il problema del phishing dato che gli attaccanti usano domini registrati appositamente, account compromessi e tecniche sempre più sofisticate, ma alza significativamente il costo e la complessità degli attacchi che sfruttano il domain spoofing diretto.

Il documento è disponibile sul portale dell'ACN e include esempi pratici di record DNS, schemi dei processi di verifica e riferimenti alle normative applicabili: https://www.acn.gov.it/portale/documents/d/guest/linee-guida-config-posta-elettronica-autenticazione_2604.

> *Adottare questi tre protocolli congiuntamente è oggi considerato un requisito di igiene digitale di base per qualsiasi organizzazione, pubblica o privata, che gestisca un dominio email.*

FONTE

Agenzia per la Cybersicurezza Nazionale — *Linee Guida per la Configurazione del Servizio di Posta Elettronica per l'Autenticazione*, versione 1.0.1, aprile 2026. Disponibile sul portale ufficiale ACN.

GPI PHISHING — CYBERSECURITY PLATFORM

Proteggi il tuo dominio. Insegna al tuo team a riconoscere le e-mail di phishing in tempo reale.

Simulazioni, feedback immediato e formazione continua per ridurre drasticamente i click su e-mail malevole.

Gpi Phishing
AI POWERED PROTECTION

www.gpiphishing.com