CORSO AVANZATO DI DIGITAL FORENSICS · EMAIL FORENSICS

Acquisizione forense di email

Vantaggi per la digital forensics e nel contrasto agli attacchi di tipo Man in the Mail o Business Email Compromise

Relatore: Vincenzo Calabrò

DKIM, DMARC ed SPF nella email forensics. Bibliografia aggiornata a novembre 2026.

Obiettivi della lezione

Al termine della mezza giornata lo studente è in grado di

1. leggere gli header di un messaggio e separare ciò che dichiara il mittente da ciò che annotano i server lungo il percorso;
2. spiegare che cosa autenticano SPF, DKIM e DMARC e che cosa lasciano scoperto;
3. verificare una firma DKIM e valutarne l’esito tenendo conto dei limiti documentati in letteratura;
4. impostare l’analisi di un caso di Man in the Mail e riferirne i risultati con le cautele richieste in sede giudiziaria.

Prerequisiti

Reti e DNS, crittografia a chiave pubblica, principi di acquisizione forense delle evidenze digitali.

Materiali

Kit di laboratorio con tre messaggi di prova. Bibliografia nelle slide finali, aggiornata a novembre 2026.

Programma della mezza giornata

Modulo	Contenuti	Minuti
1. Il fenomeno	Man in the Mail e BEC: fasi, varianti, numeri, quesiti	30
2. Anatomia di un messaggio	Envelope, header, Received, Authentication-Results	20
3. SPF, DKIM, DMARC	Funzionamento, limiti e valore probatorio di ciascun protocollo	55
Pausa		15
4. ARC e limiti dei protocolli	Forwarding, ARC, ricerca accademica, replay, deniability	25
5. Metodologia forense	Acquisizione, fonti, percorso di analisi, interpretazione	25
6. Laboratorio	Quattro esercizi su header, DNS e firme DKIM	40
7. Quadro giuridico italiano	Reati, acquisizione della prova, valore probatorio, responsabilità	20
8. Caso di studio e sintesi	Un caso ricostruito dalla segnalazione alla relazione	10

240 minuti complessivi, pausa compresa.

MODULO 1 · 30 MINUTI

Il fenomeno: Man in the Mail e Business Email Compromise

Che cos’è, come si svolge, quanto pesa e che cosa viene chiesto al consulente.

Una frode, molti nomi

Un terzo si inserisce in una corrispondenza commerciale e fa deviare un pagamento su un conto che controlla.

Denominazione	Che cosa mette in evidenza
Business Email Compromise (BEC)	Termine dell'FBI: caselle aziendali compromesse per ottenere trasferimenti di fondi
Email Account Compromise (EAC)	La stessa frode quando la casella violata è personale
Man in the Mail	La posizione dell'attaccante, fra le due parti della corrispondenza
Payment Redirection Fraud	L'effetto: il pagamento finisce su un altro conto
Account Takeover Fraud	Il mezzo: il controllo di un account altrui
CEO fraud	L'impersonificazione di un dirigente verso l'amministrazione interna
In italiano	Truffa dei bonifici, truffa dei falsi IBAN, frode delle false fatture

Fonte: FBI IC3, PSA I-091124-PSA, 11 settembre 2024.

Le fasi dell’attacco

Fase 1

Ricognizione

Chi paga chi, con quali importi e quali scadenze. Bastano il sito aziendale e i profili professionali.

Fase 2

Accesso o imitazione

Credenziali sottratte con phishing, oppure registrazione di un lookalike domain.

Fase 3

Osservazione

Lettura silenziosa della corrispondenza. Compaiono inbox rule che inoltrano o nascondono i messaggi.

Fase 4

Inserimento

Risposta dentro il thread reale, con le nuove coordinate bancarie e un pretesto plausibile.

Fase 5

Pagamento

Il debitore dispone il bonifico. Nessun sistema è stato forzato: l’ordine è autentico.

Fase 6

Dispersione

Il denaro transita su conti di money mule, spesso all’estero, e viene prelevato in poche ore.

Fra la fase 2 e la fase 4 possono passare settimane: la finestra di acquisizione va aperta ben prima della data del bonifico.

Tre varianti tecniche, tre impronte diverse

Variante	Che cosa fa l'attaccante	SPF	DKIM	DMARC	Dove cercare
A. Casella compromessa	Scrive dalla casella reale del fornitore	pass	pass, dominio reale	pass	Log di accesso, inbox rule, IP di invio
B. Lookalike domain	Registra un dominio simile e lo configura a regola d'arte	pass	pass, dominio simile	pass, se pubblicato	Dominio nel From, data di registrazione, Reply-To
C. Spoofing del dominio	Usa il dominio reale nel From da un server non autorizzato	fail o non allineato	assente o non allineata	fail	Authentication-Results, policy pubblicata all'epoca

Nelle varianti A e B i tre protocolli restituiscono pass: autenticano un dominio, non le intenzioni di chi scrive.

La distinzione fra le tre varianti è la prima risposta che il committente si aspetta, perché indica quale delle due parti ha subito la compromissione.

Le dimensioni del fenomeno

3,05 mld $

Perdite da BEC denunciate all'IC3 nel 2025, su 24.768 segnalazioni. Seconda voce per danno economico nel rapporto annuale.

55,5 mld $

Perdite esposte nel mondo fra ottobre 2013 e dicembre 2023, su 305.033 episodi censiti dall'FBI.

23%

Quota riconducibile alla BEC fra le tecniche di frode contro le imprese rilevate da CERTFin sui dati 2025.

In Italia la Polizia Postale ha trattato nel 2025 27.085 casi di truffe online e frodi informatiche, per oltre 269 milioni di euro sottratti. Il dato comprende tutte le tipologie, non la sola BEC.

Sono numeri costruiti sulle denunce: misurano ciò che viene segnalato e sottostimano il fenomeno reale.

Fonti: FBI IC3, Internet Crime Report 2025 e PSA I-091124-PSA; Polizia Postale, Report 2025; Clusit, ott. 2026.

Il contesto italiano: fattura elettronica e verifica del beneficiario

Dal 2019

Fattura elettronica e copia di cortesia

La fattura transita dal Sistema di Interscambio e arriva nel cassetto fiscale, dove alterarla è molto difficile.

Molte aziende però dispongono il bonifico dopo aver visto il PDF di cortesia ricevuto via email, senza confrontare l'IBAN con quello del file XML. Le fatture pro forma restano del tutto fuori dal circuito.

Dal 9 ottobre 2025

Verification of Payee

Il Regolamento (UE) 2024/886 obbliga i prestatori di servizi di pagamento dell'area euro a verificare, prima del bonifico, la corrispondenza fra IBAN e nome del beneficiario.

L'esito può essere di corrispondenza piena, parziale o assente. La decisione finale resta all'ordinante: l'esito mostrato e la scelta compiuta diventano elementi da acquisire.

I due presìdi riducono il rischio. Quando la frode riesce comunque, l'analisi dei messaggi resta il solo modo per ricostruire l'accaduto.

Fonti: Reg. (UE) 2024/886; Banca d'Italia, nota sulla VoP.

I quesiti posti al consulente

Quesito ricorrente	Evidenze che permettono di rispondere
Il messaggio con il nuovo IBAN proviene dalla casella del fornitore o da un altro mittente?	Header completi, Authentication-Results, firma DKIM
Il contenuto è stato modificato dopo l'invio?	Verifica DKIM sul formato nativo, confronto fra copia inviata e copia ricevuta
Quale delle due infrastrutture è stata compromessa, e da quando?	Log di accesso, inbox rule, indirizzi IP, record DNS dell'epoca
Le parti avevano adottato misure adeguate?	Record SPF, DKIM e DMARC pubblicati all'epoca, MFA, procedura di verifica degli IBAN
È possibile risalire all'autore?	IP e provider di origine, intestazione del conto beneficiario tramite l'autorità giudiziaria

Il consulente risponde sui fatti tecnici. La qualificazione giuridica e l'attribuzione delle responsabilità spettano al giudice.

MODULO 2 · 20 MINUTI

Anatomia di un messaggio

Envelope, header e artefatti: che cosa dichiara il mittente e che cosa annotano i server.

Envelope e header: le identità di un messaggio

DIALOGO SMTP (ENVELOPE)

```
EHLO mail.fornitore.example
MAIL FROM:<bounce@fornitore.example>
RCPT TO:<contabilita@cliente.example>
DATA
```

HEADER DEL MESSAGGIO

```
From: Amministrazione <amm@fornitore.example>
Reply-To: amm@fornitore.example
Subject: Fattura n. 118
```

Esempio illustrativo con domini riservati alla documentazione.

Identità	Chi la imposta	Chi la verifica
HELO / EHLO	Il server che si connette	SPF, in subordine
MAIL FROM, poi Return-Path	Il server o l'applicazione d'invio	SPF
From	L'autore o il suo client	DMARC, per alignment
d= in DKIM-Signature	Il server che firma	DKIM
Reply-To	L'autore o il suo client	Nessun protocollo

L'utente vede soltanto il From. SPF controlla il MAIL FROM, DKIM il dominio d=: DMARC nasce per legare queste identità a quella visibile.

Fonti: RFC 5321; RFC 5322; RFC 7208; RFC 6376; RFC 9989.

La catena dei Received e gli altri artefatti

- Ogni server che prende in carico il messaggio antepone un header Received: la catena si legge dal basso verso l'alto.
- Sono affidabili le righe scritte dai server del destinatario. Quelle sottostanti possono essere state costruite da chi invia.
- I timestamp, riportati a UTC, collocano gli eventi sulla linea del tempo e rivelano ritardi anomali.
- Message-ID, In-Reply-To e References permettono di ricostruire il thread e di capire in quale punto si è inserito l'attaccante.
- Date, X-Mailer e i boundary MIME dipendono dal client: sono indizi, non riscontri.

SCRITTO DAL SERVER DEL DESTINATARIO

```
Received: from mail.fornitore.example (203.0.113.25)
  by mx.cliente.example with ESMTPS;
  Thu, 12 Mar 2026 09:41:09 +0100
```

SCRITTO DAL SERVER DEL MITTENTE

```
Received: from [192.0.2.44] (helo=pc-amm)
  by mail.fornitore.example with ESMTPSA;
  Thu, 12 Mar 2026 09:41:07 +0100
```

```
Message-ID: <20260312084107.4F2A@fornitore.example>
In-Reply-To: <a81c77e0@cliente.example>
```

Esempio illustrativo.

Fonti: RFC 5321, § 4.4; RFC 5322, § 3.6.

L’header Authentication-Results

```
Authentication-Results: mx.cliente.example;
  spf=pass smtp.mailfrom=fornitore.example;
  dkim=pass header.d=fornitore.example
    header.s=s2026;
  dmarc=pass header.from=fornitore.example
```

Esempio illustrativo. In azzurro l’authserv-id, in arancione gli esiti.

- Lo scrive il server che riceve il messaggio, nel momento in cui lo riceve: documenta i controlli eseguiti allora.
- L’authserv-id dice chi ha eseguito i controlli. Conta soltanto l’header aggiunto dalla propria infrastruttura di ricezione; quelli omonimi arrivati dall’esterno vanno ignorati.
- Riporta gli esiti (pass, fail, softfail, none, temperror, permerror) e le identità valutate: smtp.mailfrom, header.d, header.s, header.from.
- Non è coperto da alcuna firma: in perizia è un riscontro da confrontare con la verifica indipendente della firma DKIM e con i record DNS dell’epoca.

Fonte: RFC 8601, Message Header Field for Indicating Message Authentication Status, 2019.

MODULO 3 · 55 MINUTI

SPF, DKIM, DMARC

Che cosa verifica ciascun protocollo, come lo fa e quale peso ha in un’analisi forense.

SPF: chi è autorizzato a inviare

SENDER POLICY FRAMEWORK

Il titolare del dominio pubblica in un record TXT l'elenco dei server che possono inviare posta usando quel dominio nel MAIL FROM.

Il server ricevente confronta l'indirizzo IP di chi si connette con l'elenco e annota un esito.

L'ultimo termine del record stabilisce la sorte di tutti gli altri mittenti.

```
$ dig +short TXT fornitore.example
"v=spf1 ip4:203.0.113.0/24
 include:_spf.provider.example
 mx -all"
```

Esempio illustrativo, spezzato su più righe. Sono autorizzati una rete, i server del provider e gli MX del dominio; tutti gli altri falliscono.

Qualificatore	Esito per chi corrisponde
+ (implicito)	pass
-	fail
~	softfail
?	neutral

Fonte: RFC 7208, Sender Policy Framework (SPF), 2014.

SPF: limiti e uso in perizia

Limiti

- Verifica il MAIL FROM e non il From visibile: da solo non impedisce di falsificare l'indirizzo che l'utente legge.
- Si rompe con il forwarding, perché il server che inoltra non compare fra quelli autorizzati.
- Ammette al massimo dieci termini che richiedono query DNS; oltre la soglia l'esito è permerror.
- Gli include verso infrastrutture condivise allargano l'insieme degli IP autorizzati. Lo studio BreakSPF ha trovato domini esposti anche fra i primi mille per popolarità.

In perizia

- L'IP del server che ha consegnato il messaggio si legge nel Received scritto dal destinatario e va confrontato con il record SPF.
- Il record di oggi può non essere quello dell'epoca: servono fonti storiche, come passive DNS, backup della zona, report DMARC.
- Un pass indica che il messaggio è partito da un server autorizzato dal dominio del MAIL FROM. Non dice chi lo ha scritto.
- Un fail su un messaggio che reca nel From il dominio del fornitore orienta verso lo spoofing del dominio.

Fonti: RFC 7208, § 4.6.4; RFC 7960; Wang et al., BreakSPF, NDSS 2024.

DKIM: firma e verifica

1 · Mittente

Firma

Il server d’invio calcola l’hash del body e degli header scelti e li firma con la chiave privata.

2 · Transito

Trasporto

La firma viaggia nell’header DKIM-Signature, insieme a dominio (d=) e selector (s=).

3 · Destinatario

Chiave pubblica

Il server ricevente chiede al DNS del dominio d= il record TXT indicato dal selector.

4 · Destinatario

Verifica

Ricalcola gli hash e controlla la firma. L’esito, pass o fail, finisce in Authentication-Results.

```
s2026._domainkey.fornitore.example. IN TXT "v=DKIM1; k=rsa; p=MIIBIjANBgkqhkiG9w0BAQEF[…]"
```

La chiave privata non lascia il server d’invio. La firma lega il messaggio a un dominio, non a una persona, e protegge il body e gli header elencati.

Fonte: RFC 6376, DomainKeys Identified Mail (DKIM) Signatures, 2011.

Anatomia di DKIM-Signature

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
 d=fornitore.example; s=s2026; t=1773304868;
 h=from:to:subject:date:message-id:
   mime-version:content-type;
 bh=zj9aAYmOtVncJxw5sZdqpGtYJ6qFrgKP6XoDq0ZqSsI=;
 b=QwVPMFOVfpZDVLFdSkRvaHnWSTvr8YLrmC07hNjHBO[…]
```

Firma generata per il laboratorio con dkimpy sul messaggio dell'esercizio 3. I tag i= e q= sono omessi, b= è abbreviato. Il valore di t= corrisponde al 12 marzo 2026, 08:41:08 UTC.

Tag	Significato
v, a	Versione e algoritmo di firma
d	Dominio che firma e ne risponde
s	Selector: individua la chiave nel DNS
h	Header coperti dalla firma, nell'ordine
bh	Hash del body dopo la canonicalization
b	Firma calcolata sugli header e su bh
c	Canonicalization di header e body
t, x	Istante della firma ed eventuale scadenza
l	Lunghezza del body firmata, se limitata

Fonte: RFC 6376, § 3.5.

Canonicalization e copertura della firma

	simple	relaxed
Header	Nessuna modifica tollerata	Nomi in minuscolo, righe ripiegate riunite, spazi multipli ridotti a uno
Body	Tollerate soltanto le righe vuote in coda	In più: spazi a fine riga ignorati, spazi multipli ridotti a uno

Con c=simple basta un gateway che ritocca gli spazi per rompere la firma. Una firma non valida non equivale a un messaggio contraffatto.

Che cosa è coperto

- Il body per intero, salvo che il tag l= ne limiti la lunghezza firmata.
- I soli header elencati in h=. Il From deve comparire sempre.
- Received e Return-Path restano fuori: cambiano lungo il percorso.
- Un header assente da h=, per esempio Reply-To, può essere aggiunto senza invalidare la firma.
- Ripetere un nome in h= più volte di quante compare nel messaggio impedisce di aggiungerne un altro (oversigning).

Fonte: RFC 6376, §§ 3.4, 3.5 e 5.4. I comportamenti indicati sono riprodotti nell’esercizio 3.

Chiavi, selector e verifica a distanza di tempo

Chiavi e selector

- RSA con chiavi di almeno 1024 bit, 2048 raccomandati. Dal 2018 è ammesso anche Ed25519; rsa-sha1 è dichiarato storico.
- Il selector permette più chiavi per lo stesso dominio e la loro rotazione periodica.
- Uno studio su cinque anni di dati ha rilevato difetti diffusi nella gestione delle chiavi e nell'implementazione delle firme, anche presso provider molto noti.

Il problema del tempo

- La verifica richiede la chiave pubblica in uso alla data della firma. Dopo la rotazione il record DNS viene rimosso o sovrascritto.
- Fonti per la chiave storica: passive DNS, archivi pubblici di chiavi DKIM, copie conservate dal gestore del dominio.
- All'acquisizione conviene interrogare subito il record del selector e conservarne l'esito con data, ora e hash.

Una chiave non più reperibile rende la firma non verificabile. Non la rende falsa.

Fonti: RFC 8301; RFC 8463; Wang et al., USENIX Security 2022; Vitale, tesi Politecnico di Torino, 2024.

Che cosa dimostra una firma DKIM valida

Dimostra

- Che il body e gli header elencati in h= non sono cambiati dopo la firma.
- Che la firma è stata apposta con la chiave privata del dominio d=, quindi da un sistema che ne aveva la disponibilità.
- Se la chiave è stata ritirata in una data nota, che la firma è anteriore a quella data, salvo divulgazione della chiave privata.

Non dimostra

- Chi ha materialmente scritto il messaggio: da una casella compromessa esce posta con firma valida.
- Che il destinatario lo abbia ricevuto, né quando: Date e t= sono dichiarati da chi invia.
- L'integrità degli header non firmati.
- Che quel messaggio fosse diretto a quel destinatario: una firma valida può essere riutilizzata.

In relazione si scrive «il messaggio risulta firmato dal dominio X e non alterato dopo la firma», non «il messaggio è stato scritto da Tizio».

DMARC: identifier alignment

Il controllo è superato quando almeno uno fra SPF e DKIM dà pass per un dominio allineato a quello del From.

From	MAIL FROM	d= della firma	SPF	DKIM	DMARC
fornitore.example	b.fornitore.example	fornitore.example	pass, allineato	pass, allineato	pass
fornitore.example	mailer.esp.example	esp.example	pass, non allineato	pass, non allineato	fail
fornitore.example	attaccante.example	assente	pass, non allineato	none	fail
fornitore.example	altro.example	fornitore.example	pass, non allineato	pass, allineato	pass

Relaxed, predefinito

Basta lo stesso Organizational Domain: b.fornitore.example è allineato a fornitore.example.

Strict

I due domini devono coincidere carattere per carattere.

Fonte: RFC 9989 (maggio 2026), che sostituisce RFC 7489. DMARC: Domain-based Message Authentication, Reporting and Conformance.

DMARC: record e policy

```
$ dig +short TXT _dmarc.fornitore.example
"v=DMARC1; p=reject; sp=reject;
 adkim=r; aspf=r;
 rua=mailto:dmarc@fornitore.example"
```

Esempio illustrativo, spezzato su più righe.

Con p=none il dominio riceve i report ma resta imitabile: un messaggio che ne falsifica il From può arrivare a destinazione.

Tag	Significato
p	Policy richiesta: none, quarantine, reject
sp	Policy per i sottodomini
np	Policy per i sottodomini inesistenti
adkim, aspf	Alignment relaxed (r) o strict (s)
rua	Destinatario dei report aggregate
ruf	Destinatario dei failure report
t	Modalità di test, al posto di pct

I tag np e t sono stati introdotti da RFC 9989.

Fonte: RFC 9989, Domain-Based Message Authentication, Reporting, and Conformance, 2026.

DMARCbis: RFC 9989, 9990 e 9991

Aggiornamento di maggio 2026	RFC 7489	RFC 9989 e documenti collegati
Stato	Informational, 2015	Proposed Standard, maggio 2026
Organizational Domain	Public Suffix List	DNS Tree Walk, al massimo otto query
Tag	pct, rf, ri presenti	Aggiunti np, psd, t. Storici pct, rf, ri
Report	Nello stesso documento	RFC 9990 per gli aggregate, RFC 9991 per i failure
Messaggi che falliscono	Il receiver può discostarsi dalla policy	Nessun rifiuto fondato sul solo p=reject (§ 7.4)

Continuità

Il record resta v=DMARC1 e quelli già pubblicati continuano a valere.

Mailing list

I domini i cui utenti scrivono a mailing list non dovrebbero pubblicare p=reject.

In relazione

Per fatti anteriori a maggio 2026 si indica la specifica allora in vigore. L'adeguamento dei provider è graduale.

Fonti: RFC 9989, RFC 9990, RFC 9991 (IETF, maggio 2026).

I report DMARC come fonte investigativa

RUA · Aggregate

Statistiche periodiche

File XML che i receiver inviano al dominio, di norma ogni giorno. Per ciascun IP di origine riportano numero di messaggi, esiti SPF e DKIM, domini valutati e trattamento applicato. Non contengono il testo dei messaggi.

RUF · Failure

Singoli messaggi

Copia o estratto del messaggio che non ha superato il controllo. Pochi provider li inviano, per ragioni di riservatezza.

In indagine

Che cosa se ne ricava

Date e IP dei tentativi di usare il dominio da server estranei. La policy effettivamente pubblicata all'epoca. Nulla sulle caselle compromesse e sui lookalike domain, che i report non vedono.

Un report aggregate può mostrare, per esempio, che in un certo giorno alcuni messaggi con il dominio nel From sono partiti da server sconosciuti e sono stati respinti in applicazione di p=reject.

Fonti: RFC 9990; RFC 9991; Ashiq et al., USENIX Security 2023.

Adozione: provider e linee guida ACN

Febbraio 2024

Google e Yahoo

Chi invia più di 5.000 messaggi al giorno deve autenticarli con SPF e DKIM e pubblicare un record DMARC, almeno con p=none.

5 maggio 2025

Microsoft

Requisiti analoghi per la posta diretta a Outlook.com, Hotmail e Live.

17 aprile 2026

ACN

Linee guida per la configurazione del servizio di posta elettronica per l'autenticazione del mittente.

Maggio 2026

IETF

Con RFC 9989 DMARC diventa Proposed Standard.

Nel 2015, sul primo milione di domini per popolarità, SPF era pubblicato dal 40% e DMARC dall'1%.

Queste date indicano che cosa era ragionevole attendersi da un'organizzazione in un dato momento: l'assenza di DMARC pesa diversamente nel 2021 e nel 2026.

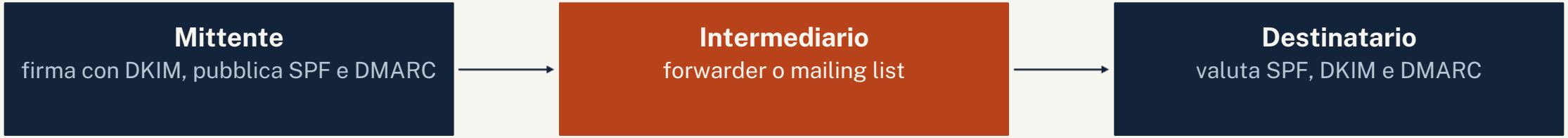
Fonti: requisiti per i mittenti di Google, Yahoo e Microsoft; ACN, Linee guida, 2026; Hu e Wang, 2018.

MODULO 4 · 25 MINUTI

ARC e limiti dei protocolli

Dove l’autenticazione si interrompe, che cosa ha mostrato la ricerca e quali casi restano fuori.

Forwarding e mailing list



Flusso	SPF	DKIM	DMARC
Invio diretto	pass	pass	pass
Forwarding senza modifiche	fail: l'IP è quello del forwarder	pass: la firma sopravvive	pass, grazie a DKIM
Mailing list che aggiunge un footer o un prefisso al Subject	fail	fail: body o header modificati	fail

Un fail su un messaggio passato da una lista o da un inoltro automatico ha una spiegazione fisiologica. Prima di parlare di contraffazione si legge la catena dei Received.

Fonti: RFC 7960; RFC 6377; RFC 9989, § 7.4.

ARC: Authenticated Received Chain

```
ARC-Seal: i=1; a=rsa-sha256; d=lista.example;
 s=arc1; cv=none; b=[…]
ARC-Message-Signature: i=1; a=rsa-sha256;
 d=lista.example; s=arc1; h=from:to:subject; […]
ARC-Authentication-Results: i=1; lista.example;
 dkim=pass header.d=fornitore.example;
 spf=pass smtp.mailfrom=fornitore.example
```

Esempio illustrativo di un primo passaggio (i=1).

L’intermediario che inoltra o modifica un messaggio annota gli esiti dei controlli che ha eseguito e sigilla l’annotazione.

Ogni passaggio aggiunge tre header con lo stesso numero d’ordine: gli esiti osservati, la firma sul messaggio com’era, il sigillo sulla catena.

Il destinatario può dare credito all’esito originario soltanto se si fida di chi ha sigillato.

Stato

RFC 8617, luglio 2019, Experimental.

Novembre 2026

Il working group DMARC dell’IETF ha in esame un documento che chiede di riclassificarlo Historic. La riclassificazione non è ancora avvenuta.

Dopo ARC

Le soluzioni utili confluiscono in DKIM2, tuttora Internet-Draft.

Fonti: RFC 8617; draft-ietf-dmarc-arc-to-historic-01; draft-ietf-dkim-dkim2-spec-09 (work in progress).

Che cosa dice la ricerca accademica

Studio	Che cosa ha mostrato	Ricaduta per l'analisi
Hu e Wang, USENIX Security 2018	Su 35 provider molti messaggi con mittente falsificato arrivavano in inbox e pochi client avvisavano l'utente	Un messaggio recapitato non è per questo autentico
Chen, Paxson e Jiang, USENIX Security 2020	18 attacchi che aggirano SPF, DKIM e DMARC sfruttando letture diverse dello stesso messaggio fra componenti	Il pass annotato dal server va riscontrato con una verifica indipendente
Shen et al., USENIX Security 2021	La catena di autenticazione cede nel punto più debole: server, relay o client	Si esaminano tutti i passaggi, non soltanto l'esito finale
Liu et al., IEEE EuroS&P 2023	Su 20 servizi di forwarding l'inoltro permette di far accettare messaggi falsificati	Un forwarder fra i Received impone cautela sull'esito
Wang et al., NDSS 2024	Record SPF troppo ampi su infrastrutture condivise mettono indirizzi IP autorizzati alla portata di terzi	Un SPF pass da IP di cloud condivisi non identifica il mittente

In tutti gli studi l'autenticazione regge quanto il componente più debole che il messaggio attraversa.

I riferimenti completi sono nella bibliografia finale.

DKIM replay

Come funziona

- Chi riceve un messaggio con firma valida può ritrasmetterlo identico ad altri destinatari.
- La firma continua a verificarsi, perché non copre l'envelope.
- Chi lo fa sfrutta la reputazione del dominio che ha firmato.

Che cosa cambia per l'analisi

- La firma valida non prova che il dominio abbia inviato il messaggio a quel destinatario.
- Indizi: Received estranei al dominio firmatario, destinatario assente da To e Cc, t= molto anteriore alla consegna.
- Una vecchia fattura firmata può essere ripresentata: si confrontano Message-ID e date con i messaggi già ricevuti.

Il problema è descritto già nella specifica del 2011. DKIM2 nasce anche per chiuderlo.

Fonti: RFC 6376, § 8.6; Chuang et al., DKIM Replay Problem Statement, IETF draft, 2023; DKIM2.

Non ripudio e deniability

Verificabilità

Ciò che serve a chi indaga

Finché la chiave pubblica è reperibile, chiunque può verificare la firma, anche a distanza di anni. È il meccanismo che dal 2016 ha permesso di confermare l'autenticità di messaggi trafugati e poi resi pubblici.

Deniability

Ciò che serve a chi è stato violato

Lo stesso meccanismo consegna a chi sottrae una casella la prova crittografica che il materiale è autentico. KeyForge e TimeForge propongono firme che proteggono dallo spoofing ma perdono valore dopo un intervallo.

In perizia si annota la data della verifica e si conserva la chiave pubblica usata. Se un provider divulgasse le chiavi private ritirate, le firme di quel periodo non proverebbero più nulla.

Fonti: Specter, Park e Green, KeyForge, USENIX Security 2021; Green, 2020.

Ciò che i protocolli non vedono

Casella compromessa

Il messaggio parte dall'infrastruttura legittima e supera ogni controllo. Le tracce stanno altrove: log di accesso, inbox rule, sessioni e token, indirizzi IP.

Lookalike domain

Il dominio è dell'attaccante, che lo configura con SPF, DKIM e DMARC corretti. Si confronta il nome carattere per carattere, omoglifi compresi, e si verifica la data di registrazione.

Display name e Reply-To

Il nome mostrato coincide con quello del fornitore, l'indirizzo no. Oppure il From è autentico e il Reply-To porta le risposte altrove. Nessun protocollo confronta questi campi.

Difetti di implementazione

Con lo SMTP smuggling, reso pubblico a dicembre 2023, server che interpretavano in modo diverso la fine dei dati lasciavano passare messaggi falsificati con SPF e DMARC superati.

In tutti e quattro i casi gli header riportano pass. L'esito va sempre letto insieme al contesto.

Fonti: RFC 9989, § 11.4; Longin, SMTP Smuggling, SEC Consult, 2023.

MODULO 5 · 25 MINUTI

Metodologia di analisi forense

Dall’acquisizione dei messaggi alla lettura degli esiti, con le cautele che la sede giudiziaria richiede.

Acquisizione dei messaggi

Da fare

- Acquisire i messaggi in formato nativo (EML, MSG, MBOX, PST) o, meglio, l'intera casella dal server.
- Raccogliere inviati e ricevuti di entrambe le parti, anche da indirizzi simili a quelli corretti, da prima della frode a qualche giorno dopo.
- Calcolare gli hash, verbalizzare strumenti, orari e operatori, lavorare su una copia.
- Interrogare subito i record SPF, DKIM e DMARC e conservarne l'esito.

Da evitare

- Stampe, PDF, screenshot e inoltri: perdono gli header e invalidano le firme.
- Aprire e risalvare i messaggi dal client: alcune esportazioni modificano i byte e la firma non si verifica più.
- Lavorare sulla copia di una sola delle parti.
- Rimandare: i log dei provider hanno tempi di conservazione brevi.

Per la PEC vale lo stesso principio: la firma del gestore si verifica sul file originale, non sulla stampa.

Fonte: ISO/IEC 27037:2012.

Le fonti oltre il messaggio

Fonte	Che cosa contiene	Chi la detiene
Log di accesso alla casella	IP, data e ora, client, esito dell'autenticazione, uso della MFA	Provider di posta, amministratore
Audit log del tenant	Accessi ai messaggi, creazione di inbox rule, deleghe, consensi OAuth	Microsoft 365, Google Workspace
Inbox rule e inoltri	Regole che spostano, cancellano o inoltrano i messaggi con parole come IBAN o fattura	Casella compromessa
Message trace e log SMTP	Percorso del messaggio, IP di consegna, esiti dei filtri	Provider del mittente e del destinatario
DNS storico	Record SPF, DKIM e DMARC alla data dei fatti	Passive DNS, archivi, gestore della zona
Dati bancari	Intestazione e movimenti del conto beneficiario, esito della verifica del beneficiario	Banche, tramite l'autorità giudiziaria

Nelle caselle compromesse la inbox rule è spesso la traccia più eloquente: indica che cosa l'attaccante voleva nascondere e da quando.

Il percorso di analisi

Passo 1

Cristallizzare

Acquisizione in formato nativo, hash, verbale.

Passo 2

Ordinare

Tutti i messaggi delle due parti su un’unica linea del tempo, in UTC.

Passo 3

Leggere

From, Reply-To, Return-Path, Received, Message-ID, Authentication-Results.

Passo 4

Verificare

Firma DKIM in modo indipendente. Record SPF e DMARC dell’epoca.

Passo 5

Confrontare

Copia inviata e copia ricevuta dello stesso messaggio: testo, IBAN, hash degli allegati.

Passo 6

Estendere

Log di accesso, inbox rule, DNS storico, report DMARC.

Passo 7

Concludere

Quale variante. Che cosa è accertato, che cosa è probabile, che cosa non è determinabile.

Sempre

Ogni passo lascia una traccia ripetibile: comandi, versioni degli strumenti, hash dei file prodotti.

Fonti: ISO/IEC 27037:2012; ISO/IEC 27042:2015.

Il sequence diagram degli eventi



Le frecce in arancione sono le azioni dell'attaccante. La richiesta di conferma del cliente (4) parte verso il fornitore, ma la inbox rule gliela nasconde.

Scenario didattico di fantasia, ripreso nel caso di studio.

Dagli esiti alle ipotesi

Che cosa si osserva nel messaggio con il nuovo IBAN	Ipotesi di lavoro	Verifica successiva
DKIM pass con d= del fornitore, DMARC pass, Received coerenti	Casella del fornitore compromessa	Log di accesso e inbox rule dal lato del fornitore
DKIM pass, ma d= e From appartengono a un dominio simile	Lookalike domain	Data di registrazione del dominio, Reply-To, thread
From del fornitore, SPF fail o non allineato, DKIM assente	Spoofing del dominio	Policy DMARC dell'epoca e ragione per cui il messaggio è stato recapitato
Body hash mismatch sulla copia del cliente, copia del fornitore integra	Modifica dopo la firma, in transito o dal lato del cliente	Confronto fra le due copie, gateway intermedi, log e regole del cliente

Sono ipotesi di lavoro. Ciascuna diventa una conclusione soltanto quando la conferma una fonte indipendente dal messaggio.

Errori ricorrenti e falsi allarmi

Falsi allarmi

- Footer, disclaimer o banner aggiunti da un gateway: la firma si rompe senza alcuna contraffazione.
- Messaggio risalvato dal client: byte diversi, firma non verificabile.
- Chiave ruotata: il record non esiste più.
- Mailing list o inoltro automatico: SPF fail fisiologico.

Errori di metodo

- Leggere Authentication-Results senza controllare chi lo ha scritto.
- Usare i record DNS di oggi per fatti di mesi prima.
- Concludere «autentico» da un pass, o «falso» da un fail, senza altre fonti.
- Trascurare la copia conservata dall'altra parte.

Un esito tecnico diventa elemento di prova quando è ripetibile, datato e accompagnato dai suoi limiti.

MODULO 6 · 40 MINUTI

Laboratorio

Quattro esercizi su messaggi di prova: leggere gli header, interrogare il DNS, verificare le firme.

Strumenti e ambiente

Strumento	A che cosa serve	Tipo
dig	Interrogare i record TXT di SPF, DKIM e DMARC	Riga di comando
dkimpy: dkimverify, arcverify	Verificare firme DKIM e catene ARC su file EML	Python, open source
Thunderbird con DKIM Verifier	Vedere l’esito della verifica durante la lettura	Estensione open source
Message Header Analyzer, Messageheader	Leggere gli header e i ritardi fra i Received	Servizi web di Microsoft e Google
parsedmarc	Leggere i report DMARC aggregate	Python, open source
Archivio pubblico di chiavi DKIM	Cercare chiavi pubbliche non più pubblicate nel DNS	Servizio web
Forensic Email Intelligence	Analisi di header, firme DKIM e catene ARC	Commerciale

Materiale

Tre file EML e il record della chiave pubblica, firmati per il dominio di prova fornitore.example.

Cautela

Gli header di un caso reale non si caricano su servizi online di terzi senza autorizzazione.

Esercizio 1: leggere gli header

messaggio-1.eml

Aprire il file con un editor di testo, senza client di posta, e rispondere.

1. Quale server ha consegnato il messaggio, e a che ora in UTC?
2. Quale dominio ha firmato, e con quale selector?
3. Quali header sono coperti dalla firma?
4. Un eventuale Reply-To sarebbe protetto?
5. A quale istante corrisponde il valore di t=?

```
Received: from mail.fornitore.example (203.0.113.25)
 by mx.cliente.example with ESMTPS;
 Thu, 12 Mar 2026 09:41:09 +0100
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
 d=fornitore.example; […] s=s2026; t=1773304868;
 h=from : to : subject : date : message-id :
 mime-version : content-type; bh=[…]; b=[…]
From: Amministrazione <amm@fornitore.example>
```

Risposte attese

1. mx.cliente.example, alle 08:41:09 UTC. 2. fornitore.example, selector s2026. 3. From, To, Subject, Date, Message-ID, MIME-Version, Content-Type. 4. No, perché non compare in h=. 5. 12 marzo 2026, 08:41:08 UTC.

Esercizio 2: interrogare il DNS

Un dominio a scelta

RECORD SPF

```
$ dig +short TXT dominio.example
```

RECORD DMARC

```
$ dig +short TXT _dmarc.dominio.example
```

CHIAVE DKIM

```
$ dig +short TXT selector._domainkey.dominio.example
```

Sostituire dominio.example con un dominio reale, per esempio quello dell'ateneo.

- Come termina il record SPF: -all, ~all o ?all? Quanti include contiene?
- Quale policy DMARC è pubblicata? Sono indicati gli indirizzi rua e ruf?
- Dove si ricava il nome del selector?
- Di quanti bit è la chiave RSA pubblicata?

Indicazioni

Il selector non si può elencare dal DNS: si legge nel tag s= di un messaggio ricevuto da quel dominio. In p= una chiave RSA a 2048 bit occupa 392 caratteri, una a 1024 bit 216.

Esercizio 3: verificare una firma DKIM

messaggio-1.eml e messaggio-2.eml

```
$ python3 verifica.py messaggio-1.eml
messaggio-1.eml: signature ok
```

```
$ python3 verifica.py messaggio-2.eml
messaggio-2.eml: signature verification failed
body hash mismatch
```

Lo script legge la chiave dal file del kit, perché il dominio di prova non esiste nel DNS. Su messaggi reali si usa dkimverify, che interroga il DNS.

Modificare una copia del messaggio-1 e ripetere la verifica.

Modifica	Esito
IBAN sostituito nel body	failed, body hash mismatch
Subject modificato	failed
Aggiunto un header Received	signature ok
Spazi in coda a una riga	signature ok
Riga aggiunta in fondo al body	failed, body hash mismatch

Perché

Received non è elencato in h=, quindi resta fuori dalla firma. Gli spazi a fine riga sono ignorati dalla canonicalization relaxed; con simple la stessa modifica fa fallire la verifica.

Esercizio 4: tre messaggi, una firma

I tre file del kit

I tre file recano la stessa DKIM-Signature. Per ciascuno indicare l'esito della verifica, che cosa è cambiato rispetto al messaggio-1 e che cosa si può affermare in una relazione.

File	Verifica	Che cosa è cambiato	Che cosa si può affermare
messaggio-1	signature ok	Nulla	Body e header firmati sono integri dalla firma in poi
messaggio-2	failed, body hash mismatch	L'IBAN nel body	Il body è stato modificato dopo la firma. Non si può dire da chi né dove
messaggio-3	signature ok	Aggiunto un Reply-To verso fornitore-example.example	La firma è valida, ma un header non coperto dirotta le risposte su un altro dominio

Il messaggio-3 è il più insidioso dei tre: la verifica dà esito positivo.

MODULO 7 · 20 MINUTI

Il quadro giuridico italiano

Reati configurabili, acquisizione della prova, valore probatorio dell’email e ripartizione della perdita.

Qualificazione penale

Condotta accertata sul piano tecnico	Ipotesi di reato ricorrente
Indurre il debitore a pagare su un altro conto con un messaggio ingannevole	Truffa, art. 640 c.p.
Entrare nella casella di posta altrui	Accesso abusivo, art. 615-ter c.p.
Presentarsi come il fornitore	Sostituzione di persona, art. 494 c.p.
Intercettare o alterare le comunicazioni	Artt. 617-quater e 617-sexies c.p.
Intervenire su dati o sistemi per trarne profitto	Frode informatica, art. 640-ter c.p.
Ricevere e trasferire le somme	Riciclaggio, art. 648-bis c.p.

Legge 90/2024

Ha inasprito le pene per diversi reati informatici ed esteso l'art. 24-bis del D.Lgs. 231/2001.

Ruolo del consulente

Descrive le condotte tecniche e le prove che le sorreggono. La qualificazione spetta al pubblico ministero e al giudice.

Fonti: codice penale; L. 28 giugno 2024, n. 90.

Acquisizione della prova nel processo penale

Legge 48/2008

Conservare senza alterare

Ispezioni, perquisizioni e sequestri informatici richiedono misure tecniche che conservino i dati originali e ne impediscano l'alterazione, con copie di cui sia assicurata la conformità.

Art. 254-bis c.p.p.

Dati presso i provider

Il sequestro di dati presso i fornitori di servizi informatici e telematici può avvenire mediante copia, con l'ordine di conservare e proteggere gli originali.

Corte cost. 170/2023

Email come corrispondenza

I messaggi già recapitati e conservati restano corrispondenza tutelata dall'art. 15 della Costituzione. La loro acquisizione richiede le garanzie del sequestro di corrispondenza.

Una copia forense eseguita correttamente consente a ogni parte di ripetere l'analisi sugli stessi dati. Quando l'operazione rischia di modificarli si procede nelle forme dell'art. 360 c.p.p.

Fonti: L. 48/2008; artt. 244, 247, 254-bis, 354, 359 e 360 c.p.p.; Corte cost., sent. n. 170/2023.

Valore probatorio dell’email nel processo civile

- L’email ordinaria è un documento informatico che la giurisprudenza riconduce alle riproduzioni dell’art. 2712 c.c.: fa piena prova se la parte contro cui è prodotta non ne disconosce la conformità.
- Il disconoscimento deve essere chiaro, circostanziato ed esplicito. Anche quando è rituale, il giudice può accertare la rispondenza con altri mezzi.
- Per l’art. 20, comma 1-bis, del CAD il valore del documento è liberamente valutabile in base a sicurezza, integrità e immodificabilità.

Dove entra la verifica tecnica

Di fronte a una contestazione, la verifica DKIM offre al giudice un dato misurabile sull’integrità del contenuto e sulla provenienza dal dominio.

Non risolve la questione dell’autore: la Cassazione ricorda che non è detto che a spedire il messaggio sia stato il titolare dell’account.

Fonti: art. 2712 c.c.; art. 20 CAD; Cass. civ., ordd. n. 11606/2018, n. 19155/2019 e n. 14046/2024.

Chi sopporta la perdita

La regola

- Chi paga a un soggetto diverso dal creditore non è liberato (art. 1188 c.c.).
- Fa eccezione il pagamento in buona fede al creditore apparente, in base a circostanze univoche (art. 1189 c.c.).
- Il fatto colposo del creditore può ridurre il risarcimento (art. 1227 c.c.).

Tribunale di Milano, 2024

- Sent. n. 6055 del 13 giugno: effetto liberatorio escluso. Hanno pesato l'IBAN diverso da quello abituale e l'inserimento manuale delle nuove coordinate.
- Sent. n. 9439 del 30 ottobre: art. 1189 non applicabile. Il messaggio veniva da un dominio diverso dal solito e il debitore non aveva svolto verifiche.

La relazione tecnica offre al giudice i fatti su cui misurare la diligenza: quale casella è stata compromessa, quali segnali erano visibili a chi ha pagato, quali misure erano attive.

Fonti: artt. 1188, 1189 e 1227 c.c.; Trib. Milano, sentt. n. 6055/2024 e n. 9439/2024.

Accountability e misure adeguate

Reg. (UE) 2016/679

GDPR

L’art. 32 chiede misure tecniche e organizzative adeguate al rischio. Una casella compromessa che contiene dati personali è una violazione da valutare ai fini della notifica.

D.Lgs. 231/2001

Responsabilità degli enti

L’art. 24-bis include i delitti informatici fra i reati presupposto. Il modello organizzativo deve prevedere la valutazione del rischio e i relativi presìdi.

D.Lgs. 138/2024

NIS2

Soggetti essenziali e importanti adottano misure di gestione del rischio e notificano gli incidenti. Le linee guida ACN del 2026 offrono un riferimento tecnico per l’autenticazione della posta.

Chi pubblica SPF, DKIM e DMARC protegge anzitutto le proprie controparti dall’uso abusivo del dominio, e mette entrambe le parti in condizione di ricostruire i fatti.

Fonti: Reg. (UE) 2016/679; D.Lgs. 231/2001; D.Lgs. 138/2024; ACN, Linee guida, 2026.

MODULO 8 · 10 MINUTI

Caso di studio e sintesi

Un caso ricostruito dalla segnalazione alla relazione, e ciò che conviene ricordare.

Caso di studio: la fattura n. 118

Data	Che cosa accade
12 marzo	Il fornitore invia al cliente la fattura n. 118, con l'IBAN italiano di sempre.
13 marzo	Nello stesso thread arriva un secondo messaggio: per verifiche sul conto abituale si chiede di pagare su un conto estero.
13 marzo	Il cliente chiede conferma via email e la riceve entro un'ora.
16 marzo	Il cliente dispone il bonifico sul nuovo conto.
27 marzo	Il fornitore sollecita il pagamento. Dichiara di non aver mai scritto il secondo messaggio né visto la richiesta di conferma.

Quesito

Da quale casella è partito il messaggio del 13 marzo, se è stato alterato e quale delle due infrastrutture è stata compromessa.

Materiale acquisito

Caselle delle due parti in formato nativo, log di accesso e audit log del fornitore, record DNS.

Scenario di fantasia: nomi, date e circostanze sono inventati a scopo didattico. Il thread è lo stesso del sequence diagram.

Caso di studio: evidenze e conclusioni

Evidenza	Che cosa mostra
Messaggio del 13 marzo, copia del cliente	DKIM pass con d=fornitore.example, DMARC pass, Received coerenti con il server del fornitore
Casella del fornitore	Il messaggio manca dagli inviati e si trova fra gli elementi eliminati ancora recuperabili
Log di accesso del fornitore	Dal 5 marzo accessi via webmail da un indirizzo IP estero mai comparso prima, senza MFA
Audit log del fornitore	Il 5 marzo viene creata una inbox rule che sposta in una cartella secondaria i messaggi del cliente contenenti la parola IBAN

Accertato

Il messaggio del 13 marzo è partito dalla casella del fornitore e non è stato alterato dopo la firma.

Altamente probabile

Dal 5 marzo la casella era nella disponibilità di un terzo, che ha scritto il messaggio e nascosto le risposte.

Non determinabile

Come siano state sottratte le credenziali e chi abbia operato. Servono atti dell'autorità giudiziaria.

Scenario di fantasia.

IN SINTESI

SPF, DKIM e DMARC autenticano un dominio. Stabilire chi ha scritto un messaggio resta compito dell'indagine.

Acquisire

In formato nativo, da entrambe le parti, salvando subito i record DNS.

Verificare

In modo indipendente da ciò che ha annotato il server, datando ogni verifica.

Riferire

Separando ciò che è accertato da ciò che è probabile e da ciò che non si può determinare.

Riferimenti: standard e documenti tecnici

IETF, Request for Comments

- RFC 5321, Simple Mail Transfer Protocol, 2008
- RFC 5322, Internet Message Format, 2008
- RFC 6376, DomainKeys Identified Mail (DKIM) Signatures, 2011
- RFC 6377, DKIM and Mailing Lists, 2011
- RFC 7208, Sender Policy Framework (SPF), 2014
- RFC 7489, DMARC, 2015, ora sostituito
- RFC 7960, Interoperability Issues between DMARC and Indirect Email Flows, 2016
- RFC 8301, Cryptographic Algorithm and Key Usage Update to DKIM, 2018
- RFC 8463, A New Cryptographic Signature Method for DKIM, 2018
- RFC 8601, Message Header Field for Indicating Message Authentication Status, 2019
- RFC 8617, The Authenticated Received Chain (ARC) Protocol, 2019
- RFC 9989, 9990 e 9991, DMARC e relativi report, 2026

Internet-Draft, work in progress

- draft-ietf-dkim-dkim2-spec-09, DomainKeys Identified Mail Signatures v2 (DKIM2), novembre 2026
- draft-ietf-dmarc-arc-to-historic-01, Reclassifying ARC as Historic, ottobre 2026
- draft-ietf-dkim-replay-problem-00, DKIM Replay Problem Statement, 2023, scaduto

Standard e linee guida

- NIST SP 800-177 Rev. 1, Trustworthy Email, 2019
- ISO/IEC 27037:2012 e ISO/IEC 27042:2015
- ACN, Linee guida per la configurazione del servizio di posta elettronica per l’autenticazione, aprile 2026

Riferimenti: letteratura accademica

- Hu H., Wang G., End-to-End Measurements of Email Spoofing Attacks, 27th USENIX Security Symposium, 2018
- Cidon A. et al., High Precision Detection of Business Email Compromise, 28th USENIX Security Symposium, 2019
- Chen J., Paxson V., Jiang J., Composition Kills: A Case Study of Email Sender Authentication, 29th USENIX Security Symposium, 2020
- Shen K. et al., Weak Links in Authentication Chains: A Large-scale Analysis of Email Sender Spoofing Attacks, 30th USENIX Security Symposium, 2021
- Specter M. A., Park S., Green M., KeyForge: Non-Attributable Email from Forward-Forgeable Signatures, 30th USENIX Security Symposium, 2021
- Tatang D. et al., The Evolution of DNS-based Email Authentication: Measuring Adoption and Finding Flaws, RAID 2021
- Wang C. et al., A Large-scale and Longitudinal Measurement Study of DKIM Deployment, 31st USENIX Security Symposium, 2022
- Liu E. et al., Forward Pass: On the Security Implications of Email Forwarding Mechanism and Policy, 8th IEEE EuroS&P, 2023
- Ashiq M. I. et al., You’ve Got Report: Measurement and Security Implications of DMARC Reporting, 32nd USENIX Security Symposium, 2023
- Wang C. et al., BreakSPF: How Shared Infrastructures Magnify SPF Vulnerabilities Across the Internet, NDSS 2024
- Vitale M., Enhancing Email Forensics: A DKIM archiving and re-verification tool for long-term Signature validation, tesi di laurea magistrale, Politecnico di Torino, 2024

Riferimenti: report, normativa e giurisprudenza

Report e fonti tecniche

- FBI IC3, Internet Crime Report 2025, aprile 2026
- FBI IC3, Business Email Compromise: The $55 Billion Scam, PSA I-091124-PSA, 11 settembre 2024
- Polizia Postale e per la Sicurezza Cibernetica, Report annuale 2025
- Clusit, Rapporto 2026, edizioni di marzo e di ottobre, con dati CERTFin
- Longin T., SMTP Smuggling: Spoofing E-Mails Worldwide, SEC Consult, dicembre 2023
- Green M., Ok Google: please publish your DKIM secret keys, 2020

Normativa

- Codice penale, artt. 494, 615-ter, 617-quater, 617-sexies, 640, 640-ter, 648-bis
- Codice di procedura penale, artt. 244, 247, 254-bis, 354, 359, 360; L. 48/2008
- Codice civile, artt. 1188, 1189, 1227, 2712; D.Lgs. 82/2005, art. 20
- Reg. (UE) 2016/679; Reg. (UE) 2024/886; D.Lgs. 231/2001; D.Lgs. 138/2024; L. 90/2024

Giurisprudenza

- Corte cost., sent. n. 170/2023
- Cass. civ., ordd. n. 11606/2018, n. 19155/2019, n. 14046/2024
- Trib. Milano, sentt. n. 6055/2024 e n. 9439/2024

CORSO AVANZATO DI DIGITAL FORENSICS · EMAIL FORENSICS

Grazie per l’attenzione

Vincenzo Calabrò

Domande e osservazioni sono benvenute.

www.vincenzocalabro.it



Inquadra per aprire il sito