LA CATENA DI FIDUCIA

Chi può scrivere un'email a nome di un'istituzione

Roberto Pinna · 13 novembre 2026 robpinna.com/note/catena-di-fiducia-email-istituzioni/

Nota tecnica · 13 novembre 2026

La catena di fiducia: chi può scrivere un'email a nome di un'istituzione

di Roberto Pinna

Come una scuola può riconoscere se un'email che contiene un ordine è autentica, e quanti enti pubblici hanno attiva la protezione che indica ai sistemi di posta di fermare le email false inviate a loro nome. Censimento della posta elettronica dei Comuni dei 119 capoluoghi di provincia e di sette istituzioni nazionali, tra cui il Ministero dell'Interno e la Polizia di Stato, condotto per misurare il rischio prima che si verifichi.

Indice

Il rischio
I risultati principali
Gli allarmi di novembre
Che cosa è stato misurato
I Comuni capoluogo di provincia
Le istituzioni nazionali
Che cosa il dato non dimostra
Che cosa fare
Metodo
Glossario
Fonti

80 su 119
Comuni capoluogo di provincia che non chiedono di fermare le email inviate falsamente a loro nome (67,2%)

59
Comuni capoluogo con la regola su «nessuna azione»; in 35 casi manca anche l'indirizzo per i rapporti sulle email false

2 su 10
Comuni delle dieci città più popolose che risultano protetti

3 su 7
istituzioni nazionali esaminate che non chiedono di fermare le email false, tra cui la Polizia di Stato

Il rischio

Un'email che ordina la chiusura o l'evacuazione di una scuola, scritta a nome di un Comune, nella maggior parte dei casi non incontra alcuna difesa predisposta dal Comune stesso; che arrivi o venga fermata dipende allora soltanto dai filtri di posta elettronica di chi la riceve. È la condizione di due Comuni capoluogo di provincia su

tre.

La stessa condizione riguarda alcune istituzioni nazionali. I domini di posta elettronica della Polizia di Stato, dei Vigili del fuoco e della Protezione civile non chiedono ai sistemi di posta elettronica di fermare le email inviate falsamente a loro nome; quello della Polizia di Stato dichiara soltanto quali server possono spedire per suo conto, il che riduce l'esposizione senza eliminarla.

Il passaggio è in tre tempi. A novembre le minacce sono arrivate in massa da caselle straniere violate, e centinaia di scuole sono state evacuate. Il 12 novembre il Governo ha indicato che un'email inviata in massa non basta, da sola, a far evacuare una scuola, e che la decisione spetta al Prefetto. Da quel momento conta chi firma il messaggio più di ciò che dice; per chi volesse ripetere il disordine, scrivere a nome di un'autorità diventa una mossa più conveniente di prima. Questa nota misura, prima che accada, una delle vie per compierla.

Le conseguenze possibili sono tre.

- **Una scuola chiusa o evacuata su un ordine falso ricevuto per email**, con il disagio e l'apprensione che ne derivano per alunni, famiglie e personale.
- **Forze dell'ordine e soccorsi impegnati senza motivo**, in ore in cui potrebbero servire altrove.
- **La perdita di fiducia negli avvisi autentici**, che è il danno più durevole, perché un ordine vero rischia di essere accolto con lo stesso dubbio di uno falso.

Non risulta che un episodio di questo tipo sia già avvenuto. La nota misura un'esposizione, cioè una difesa della posta elettronica che manca, e non descrive un attacco in corso.

I risultati principali

Su 119 Comuni capoluogo di provincia, 39 hanno pubblicato una regola che chiede ai sistemi di posta elettronica di respingere o isolare le email inviate falsamente a loro nome; gli altri 80, pari al 67,2%, non lo chiedono.

- **59 Comuni capoluogo hanno pubblicato la regola e l'hanno lasciata su «nessuna azione».** In 35 casi manca anche l'indirizzo a cui ricevere i rapporti sulle email false, sicché la regola non serve nemmeno a osservare; gli altri 24 li ricevono, e potrebbero trovarsi nella fase di osservazione che precede una scelta più severa.
- **20 Comuni capoluogo non hanno pubblicato alcuna regola.** Due di essi non dichiarano neppure quali server siano autorizzati a spedire a loro nome.
- **Un Comune capoluogo applica il rifiuto a un decimo delle email false**, e lascia passare le altre.
- **Dei Comuni delle dieci città più popolose, due risultano protetti.**
- **La quota dei Comuni capoluogo protetti varia con l'area geografica e non con la dimensione.** I Comuni capoluogo protetti sono il 34,1% sopra i centomila abitanti e il 32,0% sotto; scendono dal 43,8% del Nord al 21,3% del Sud e delle isole.

- **Anche tre istituzioni nazionali, tra cui la Polizia di Stato, non chiedono di fermare le email false.** I domini della Presidenza del Consiglio, del Ministero dell'Interno e del Ministero dell'Istruzione rifiutano le email false; quelli della Polizia di Stato, dei Vigili del fuoco e della Protezione civile sono su «nessuna azione».

I dati completi, con l'elenco nominativo dei Comuni e il registro delle letture, sono a disposizione delle autorità competenti e degli enti interessati, che possono richiederli all'autore scrivendo a roberto@robpinna.com.

Gli allarmi di novembre

La mattina dell'11 novembre 2026 circa 6.300 scuole italiane hanno ricevuto un'email di allarme bomba (Il Post); il giorno seguente una seconda ondata ne ha raggiunte 1.803 (Fanpage).

Tre fatti, ricostruiti dalla stampa, definiscono il quadro.

- **Gli indirizzi erano pubblici.** Con ogni probabilità provengono dall'elenco delle scuole statali che il Ministero dell'Istruzione pubblica tra i propri dati aperti (Il Post).
- **Il mittente era una casella vera, violata.** Il messaggio dell'11 novembre è partito dall'account di un'università di Taiwan; gli allarmi delle settimane precedenti, da account violati di altri enti stranieri (Il Post).
- **Il Governo ha fissato un criterio.** Una nota di Palazzo Chigi del 12 novembre indica che, in assenza di elementi concreti, non si procede all'evacuazione, nemmeno quando si riceve soltanto un'email inviata in massa; resta al Prefetto la facoltà di disporla qualora abbia elementi specifici e concreti di rischio (Adnkronos).

Resta aperta la domanda da cui muove questa nota. Dalle fonti consultate non risulta con quale mezzo un ordine del Prefetto, o di un'altra autorità, debba raggiungere la scuola, né come la scuola possa accertarne l'autenticità.

Che cosa è stato misurato

La nota verifica se ciascun ente abbia chiesto, con una regola pubblica, di fermare le email che usano il suo nome senza provenire dai suoi sistemi.

Nella posta elettronica il mittente si dichiara, come sul retro di una busta, e chi spedisce può indicare qualunque nome. Per rimediare, il titolare di un dominio (la parte dell'indirizzo che segue la chiocciola) può pubblicare tre indicazioni, che i sistemi di posta consultano prima di consegnare un messaggio.

Le tre indicazioni che il titolare di un dominio può pubblicare

Indicazione	Che cosa dichiara	Misurata in questa nota
SPF	Quali server possono spedire a nome del dominio	Sì
DKIM	La firma che il dominio appone ai propri messaggi	No, perché richiede un messaggio autentico da esaminare
DMARC	Che cosa fare dei messaggi che non superano i controlli	Sì

La terza, il DMARC, è quella decisiva, perché è la sola a riguardare il mittente che il destinatario legge. Può assumere tre valori.

- **Nessuna azione.** L'ente non chiede di fermare il falso; la decisione resta al sistema di chi riceve.
- **Quarantena.** L'ente chiede che il falso sia trattato come sospetto, e di norma consegnato nella posta indesiderata.
- **Rifiuto.** L'ente chiede che il falso sia respinto.

In questa nota un ente è detto «protetto» quando ha scelto la quarantena o il rifiuto e li applica a tutti i messaggi.

I Comuni capoluogo di provincia

Un Comune capoluogo su tre è protetto contro le email false inviate a suo nome; la metà ha pubblicato una regola che non chiede di fermarle.

Comuni capoluogo di provincia per condizione del dominio di posta elettronica, 13 novembre 2026

Condizione del dominio di posta elettronica	Comuni capoluogo	Quota
Rifiuto delle email false, applicato a tutti i messaggi	23	19,3%
Quarantena delle email false, applicata a tutti i messaggi	16	13,4%
Rifiuto applicato a un decimo dei messaggi	1	0,8%
Regola pubblicata, su «nessuna azione»	59	49,6%
Nessuna regola pubblicata	20	16,8%

Le prime due righe formano i 39 Comuni capoluogo protetti; le altre tre, gli 80 Comuni capoluogo che non lo sono.

Comuni capoluogo protetti per area geografica

Area	Comuni capoluogo	Protetti	Quota
Nord	48	21	43,8%
Centro	24	8	33,3%
Sud e isole	47	10	21,3%

Tre osservazioni completano il quadro.

- **L'SPF non compensa.** Tra gli 80 Comuni capoluogo non protetti, 39 hanno un SPF rigido; esso però controlla un indirizzo tecnico che il destinatario non vede, e non impedisce di scrivere il nome del Comune nel campo visibile.
- **Molte regole non sono presidiate.** Dei 59 Comuni capoluogo con la regola su «nessuna azione», 35 non ricevono i rapporti sui falsi; in questi casi la regola ha l'aspetto di un'impostazione rimasta com'era al momento dell'attivazione.
- **Vi sono errori di scrittura.** Un Comune capoluogo pubblica un SPF non valido e un altro ne pubblica due; un terzo pubblica due regole DMARC, il che per lo standard equivale a non averne; un quarto indica per i rapporti un indirizzo privo di chiocciola.

Le istituzioni nazionali

Dei sette domini di posta elettronica delle istituzioni nazionali esaminate, tre rifiutano le email false, uno le mette in quarantena e tre non chiedono alcuna azione.

Istituzioni nazionali: che cosa chiede ciascun dominio per le email false

Istituzione	Dominio	Che cosa chiede per le email false
Presidenza del Consiglio	governo.it	Rifiuto
Ministero dell'Interno	interno.it	Rifiuto
Ministero dell'Istruzione	istruzione.it	Rifiuto
Arma dei Carabinieri	carabinieri.it	Quarantena
Polizia di Stato	poliziadistato.it	Nessuna azione
Vigili del fuoco	vigilfuoco.it	Nessuna azione
Protezione civile	protezionecivile.gov.it	Nessuna azione

L'anello da cui l'ordine dovrebbe partire è dunque protetto contro la falsificazione, poiché al dominio dell'Interno fa capo la posta delle prefetture. Il dominio della Polizia di Stato dichiara un SPF rigido, che riduce l'esposizione senza eliminarla.

Restano scoperti gli enti con cui una scuola ha i rapporti più frequenti, a cominciare dal Comune, che è proprietario degli edifici delle scuole del primo ciclo e ne dispone la chiusura in caso di emergenza. Un messaggio a suo nome è quello che una segreteria scolastica ha meno ragioni di mettere in dubbio.

Che cosa il dato non dimostra

Il dato descrive ciò che ogni ente ha chiesto ai sistemi di posta elettronica, e va letto entro cinque limiti.

- **Non dice quante email false arrivino a destinazione.** I sistemi di chi riceve applicano filtri propri; la posta delle scuole, sul dominio istruzione.it, è ospitata su Microsoft 365, come risulta dai record pubblici del dominio, e questa piattaforma ne ferma una parte. Un'email falsa finita nella posta indesiderata può tuttavia essere letta da una segreteria che attende comunicazioni.
- **Non riguarda le caselle vere violate.** Un messaggio spedito da una casella autentica, come quelli di novembre, supera i controlli di autenticità, e lo stesso vale per un dominio somigliante registrato apposta. Delle tre vie per fingersi un'autorità, la regola qui misurata chiude soltanto la falsificazione del nome, che è anche l'unica che l'ente può chiudere con una propria decisione.
- **Non equivale a un giudizio di sicurezza.** «Protetto» indica soltanto che la regola chiede di fermare i falsi. La firma DKIM non è stata verificata, e due Comuni capoluogo protetti lasciano scoperti i propri sottodomini.
- **Non si estende a tutti i Comuni.** I Comuni capoluogo sono stati letti tutti, ma non rappresentano i circa 7.900 Comuni italiani.
- **È una fotografia.** Le letture sono del 13 novembre 2026, e una regola si modifica in pochi minuti.

La posta certificata (PEC). La nota riguarda la posta elettronica ordinaria. La PEC offre una garanzia in più, perché il gestore certifica la casella da cui il messaggio parte, e un indirizzo PEC non si falsifica come uno ordinario. Non basta tuttavia a chiudere il problema, per due ragioni. Una casella PEC violata spedisce messaggi autentici, e campagne condotte da caselle PEC compromesse sono state segnalate dal CERT-AgID (Cybersecurity360). La PEC, inoltre, è di norma letta dagli uffici con i tempi del protocollo, e mal si presta a un ordine da eseguire in pochi minuti. Anche per un ordine ricevuto via PEC vale dunque la verifica a voce.

Che cosa fare

La misura più efficace è alla portata di ogni scuola, e consiste nel non eseguire alcun ordine di chiusura o di evacuazione ricevuto per posta elettronica prima di averlo verificato a voce. Essa vale anche contro le caselle violate, che nessuna regola tecnica può fermare.

Per le scuole

- Verificare l'ordine chiamando un numero già noto dell'ente che lo firma, e mai quello riportato nel messaggio.
- Tenere in segreteria un elenco aggiornato dei numeri di Prefettura, Questura, Comune e Carabinieri.

- Riservare la stessa cautela ai messaggi dall'aspetto regolare, perché una casella autentica può essere stata violata.

Per i Comuni

- Attivare la ricezione dei rapporti sui falsi, senza i quali non si può sapere quale posta legittima verrebbe scartata.
- Portare la regola DMARC alla quarantena e poi al rifiuto delle email false, entro un termine stabilito.
- Correggere i record non validi o duplicati.

Per le istituzioni

- Stabilire, e rendere noto alle scuole, il canale con cui un ordine le raggiunge e il modo di verificarlo.
- Portare al rifiuto delle email false i domini delle istituzioni nazionali ancora su «nessuna azione».
- Fissare un termine entro cui i Comuni devono adottare la regola DMARC di rifiuto.

Metodo

La nota si fonda sulla sola lettura di record DNS pubblici; nessun messaggio è stato inviato a nome di alcun ente, e nessun sistema degli enti è stato sollecitato.

- **Perimetro.** I 119 Comuni capoluogo di provincia, comprese le province con più capoluoghi (Tuttitalia, su dati Istat), e sette domini di istituzioni nazionali.
- **Dominio esaminato.** Quello usato per la posta ordinaria, con esclusione della posta certificata; la presenza di record MX conferma che il dominio riceve posta. Per quattro Comuni il dominio del sito non riceve posta, e quello corretto è stato individuato da documenti pubblici dell'ente.
- **Lettura principale.** Record DMARC, SPF e MX di 115 Comuni, letti il 13 novembre 2026 con lo strumento DNS di Windows attraverso un resolver pubblico. Di ogni interrogazione si conserva la risposta integrale, con data e ora.
- **Lettura secondaria.** I quattro domini corretti e i sette nazionali sono stati letti il 12 e il 13 novembre attraverso l'interfaccia web di un resolver pubblico.
- **Criterio.** È protetto il dominio che pubblica una sola regola DMARC, con quarantena o rifiuto applicati a tutti i messaggi.
- **Aree e popolazione.** Ripartizione Istat in Nord, Centro, Sud e isole; popolazione residente stimata al 1° gennaio 2026.
- **Margine.** Trattandosi di un censimento, il conteggio non richiede stima. A titolo indicativo, l'intervallo di Wilson al 95% sulla quota dei protetti va dal 25,0% al 41,6%.
- **Riservatezza.** L'elenco nominativo dei Comuni non è pubblicato.

Glossario

Dominio
La parte dell'indirizzo di posta che segue la chiocciola e identifica l'ente.

DNS
Il registro pubblico in cui ogni dominio dichiara i propri servizi e le proprie regole.

SPF
L'elenco dei server autorizzati a spedire a nome del dominio. È detto rigido quando chiede di scartare i messaggi provenienti da altri server.

DKIM
La firma digitale che il dominio appone ai messaggi in uscita.

DMARC
La regola che indica che cosa fare dei messaggi che usano il nome del dominio senza superare i controlli precedenti.

MX
L'indicazione dei server che ricevono la posta del dominio.

Resolver
Il servizio che interroga il DNS per conto di chi lo consulta.

Fonti

- Il Post, «Come ha fatto l'allarme bomba a raggiungere tutte le scuole», 12 novembre 2026
  https://www.ilpost.it/2026/11/12/allarme-bomba-mail-scuole/
- Adnkronos, «Allarmi bomba via mail, dal governo le regole da seguire», 12 novembre 2026
  https://www.adnkronos.com/politica/allarmi-bomba-mail-protocollo-regole-governo_3eoC4ioeCWJBGJ552wjL1I
- Fanpage, «Allarmi bomba nelle scuole, il Governo spiega il protocollo», 12 novembre 2026
  https://www.fanpage.it/politica/allarmi-bomba-nelle-scuole-il-governo-spiega-il-protocollo-no-allevacuazione-per-une-mail/
- Cybersecurity360, campagna Vidar attraverso caselle PEC compromesse, gennaio 2025
  https://www.cybersecurity360.it/news/vidar-il-malspam-prende-di-mira-le-pec-con-nuove-tecniche-di-offuscamento/
- Tuttitalia, elenco dei Comuni capoluogo di provincia su dati Istat
  https://www.tuttitalia.it/capoluoghi/per-provincia/
- Record DNS pubblici dei domini esaminati, letti il 12 e il 13 novembre 2026.

Come citare

> Pinna, R. (2026). La catena di fiducia: chi può scrivere un'email a nome di un'istituzione. Nota tecnica. 13 novembre 2026. robpinna.com. https://robpinna.com/note/catena-di-fiducia-email-istituzioni/

Versione online: https://robpinna.com/note/catena-di-fiducia-email-istituzioni/