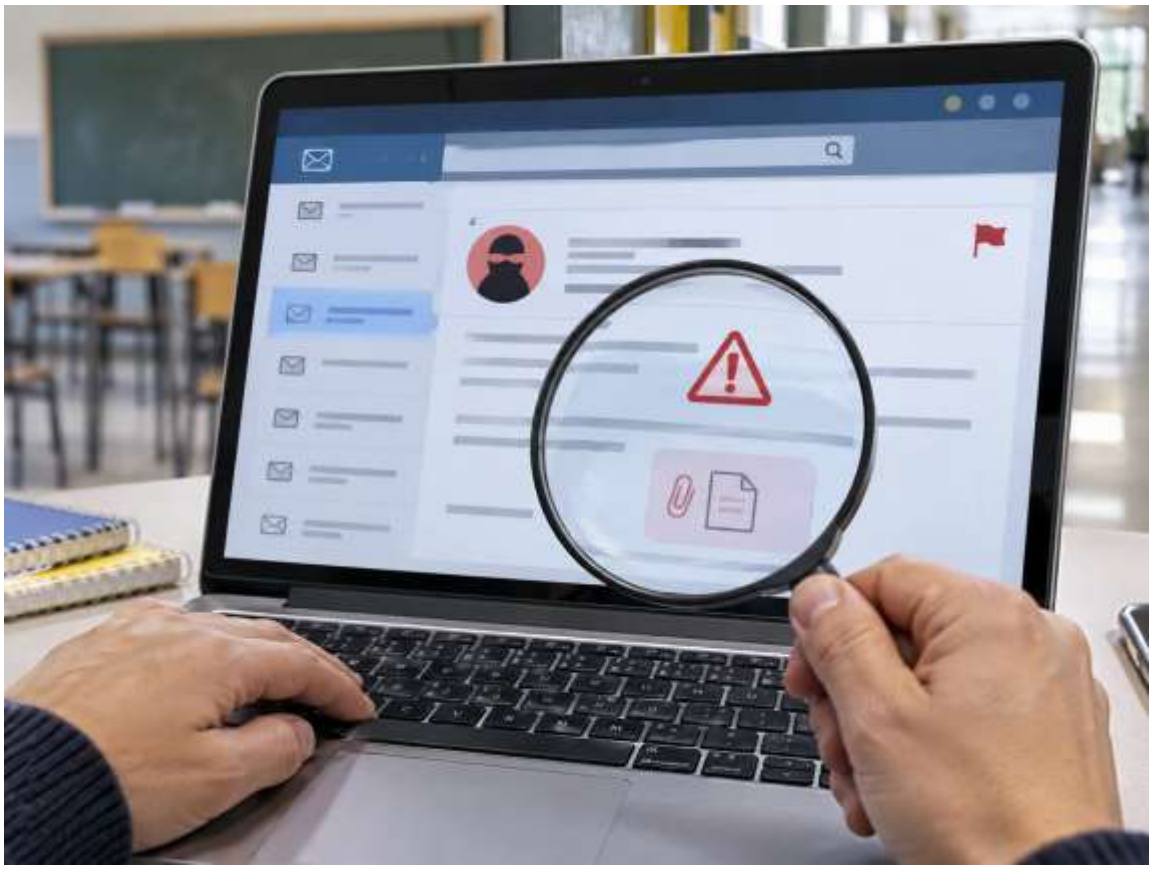
Come si fa a riconoscere una mail falsa? Una guida pratica, dopo gli allarmi bomba nelle scuole italiane di Saverio Alloggio

Le minacce recapitate a migliaia di istituti partivano da caselle autentiche, rubate a persone estranee ai fatti. Lo stesso trucco alimenta ogni giorno le truffe via posta elettronica. Dal mittente agli allegati, i controlli da fare prima di cliccare

(Fonte: https://www.corriere.it/ 12 novembre 2026)



Alle 9.39 di giovedì 12 novembre **una nuova mail firmata «Mikhail Andropov» è arrivata nelle segreterie di circa 1.800 scuole italiane**, secondo un primo bilancio, con l'oggetto «Messaggio dall'Italia. Siete in pericolo». Il giorno prima un testo simile, **che annunciava ordigni nascosti negli edifici**, aveva raggiunto circa seimila istituti, provocando evacuazioni da Nord a Sud e lasciando migliaia di studenti fuori dalle aule. Nei controlli non è stato trovato alcun ordigno. Giovedì la Presidenza del Consiglio, d'intesa con i ministri interessati, ha inviato alle scuole una circolare: senza elementi concreti ulteriori rispetto alla semplice ricezione di mail massive, gli edifici non vanno evacuati. Resta al prefetto la facoltà di ordinare l'evacuazione quando disponga di informazioni specifiche su un rischio effettivo. La vicenda, però, mostra un meccanismo che riguarda chiunque usi la **posta elettronica.**

Indice

- Un indirizzo autentico non basta
- Spam e phishing, la differenza
- Primo controllo: chi scrive davvero

- Secondo controllo: che cosa chiede
- Terzo controllo: link e allegati
- A scuola e in famiglia
- Se si è già cliccato

Un indirizzo autentico non basta

Le mail di mercoledì risultavano spedite dalla **casella reale di un'ex studentessa della Da-Yeh University**, a Taiwan, del tutto estranea alle minacce: l'ateneo ha fatto sapere che l'account era stato violato. Quelle di giovedì, secondo le prime verifiche, partivano dall'indirizzo di un insegnante di scienze delle Filippine, dipendente del ministero dell'Istruzione locale e anche lui estraneo ai fatti. Lo stesso pseudonimo era comparso all'inizio del mese nelle rivendicazioni dei falsi allarmi sui voli europei. Sull'origine dei messaggi lavora la Polizia Postale.

Per capire perché il dettaglio conta serve un passo indietro. Un indirizzo di posta ha due parti separate dalla chiocciola: prima c'è il nome della casella, dopo il dominio, cioè l'organizzazione che la gestisce (gmail.com, istruzione.it, un'università). Un messaggio falso può nascere in due modi. Il primo è lo spoofing, la falsificazione del mittente: l'equivalente di scrivere un indirizzo inventato sul retro di una busta. Il secondo è il furto della casella, che avviene quasi sempre rubando la password. Nel secondo caso la mail parte davvero da quell'indirizzo. I servizi di posta usano sistemi di verifica automatica che controllano se un messaggio arriva da un server autorizzato a spedire per quel dominio: funzionano bene contro lo spoofing, molto meno quando la casella è stata rubata e il messaggio risulta in regola. Il principio da ricordare è uno, ovvero che un mittente corretto è una condizione necessaria, non sufficiente.

Quanto ai destinatari, trovarli non richiede abilità particolari. Ogni scuola statale ha una casella istituzionale costruita sul proprio codice meccanografico e pubblicata sul sito dell'istituto, perché famiglie e uffici devono poterla raggiungere.

Spam e phishing, la differenza

Con spam si indica la posta indesiderata inviata in massa, quasi sempre pubblicità, in gran parte fermata dai filtri prima di arrivare nella casella principale. Il phishing è un'altra cosa. Un messaggio si spaccia per una banca, **un corriere**, un ente pubblico o un servizio conosciuto per convincere chi lo riceve a digitare una password, comunicare i dati della carta o aprire un file che installa un programma dannoso.

I falsi allarmi di questi giorni cercano il panico ma usano lo stesso strumento. E il phishing resta il pericolo di tutti i giorni. Nel 2025 il CERT-AGID, la struttura dell'Agenzia per l'Italia digitale che sorveglia le minacce informatiche, **ha censito in Italia 3.620 campagne malevole**, 1.922 delle quali di phishing, con 153 marchi imitati. La posta elettronica è il canale più sfruttato. Il solo **tema PagoPA**, con finte multe stradali da saldare, ha prodotto 328 campagne. Nemmeno la PEC, la posta

elettronica certificata, mette al riparo: gli abusi registrati sono stati 103, circa l'80% in più rispetto al 2024.

Primo controllo: chi scrive davvero

Il nome che compare in grassetto nella lista dei messaggi è un'etichetta scelta liberamente da chi invia: chiunque può presentarsi come **«Poste Italiane»** o **«Segreteria scolastica»**. Conta l'indirizzo completo. Sul computer appare aprendo il messaggio o passando il mouse sul nome, sullo smartphone bisogna toccare il nome del mittente. Il dominio va letto lettera per lettera, perché le imitazioni giocano sui dettagli: una «l» al posto di una «i», un trattino in più, parole aggiunte come «assistenza» o «verifica», estensioni insolite al posto di .it o .com. Una banca scrive dal proprio dominio, non da una casella gratuita né da un indirizzo che si limita a richiamarne il nome.

Anche il logo prova poco, perché copiarlo richiede pochi secondi. E un messaggio che riporta nome, cognome o altri dati personali non è per questo più affidabile, perché quelle informazioni circolano dopo i furti di dati subiti negli anni da aziende e servizi online.

Un ultimo accorgimento riguarda i contatti conosciuti. Se un collega, un amico o la segreteria della scuola scrivono qualcosa di insolito, come una richiesta di denaro o un file da scaricare con urgenza, conviene verificare con una telefonata. La loro casella potrebbe essere finita in mani altrui, come quelle usate per le minacce di questi giorni.

Secondo controllo: che cosa chiede

Le truffe fanno leva su tre sentimenti: la fretta («l'account verrà sospeso entro 24 ore»), la paura (una multa, un'azione legale, un accesso sospetto al conto) e l'interesse (un rimborso, un pacco in giacenza, una vincita). Quando un messaggio impone di agire subito, è bene sempre diffidare. Altri segnali sono i saluti generici come «Gentile cliente» e le richieste che nessun ente serio fa per posta: password, codici ricevuti via Sms, numeri della carta, foto dei documenti. Banche, Poste, Inps, Agenzia delle Entrate e scuole non li domandano in questo modo.

Un indizio, invece, ha perso valore. Per anni gli errori di ortografia e le traduzioni goffe hanno smascherato molte truffe. Oggi gli strumenti di intelligenza artificiale producono in pochi secondi testi corretti e credibili in qualunque lingua, e un italiano impeccabile non garantisce più nulla.

Terzo controllo: link e allegati

Il testo di un collegamento può mostrare un indirizzo e portare altrove. Prima di cliccare conviene verificare la destinazione reale: sul computer basta appoggiare il puntatore del mouse sul link, senza premere, e l'indirizzo compare in basso nella finestra; sullo smartphone una pressione prolungata apre un'anteprima. A identificare il sito sono le due parole, separate da un punto, che si trovano subito prima della prima barra singola «/». In un indirizzo come poste.it.verifica-conto.com/accesso il sito reale è verifica-conto.com, e Poste non c'entra. Lo stesso vale per i codici QR inseriti nelle mail: inquadrarli con il telefono equivale a cliccare un link di cui non si

vede l'indirizzo.
Gli allegati richiedono la stessa prudenza. Fatture inattese, archivi compressi come i file .zip, documenti che chiedono di «abilitare il contenuto» per essere letti sono i veicoli più comuni dei programmi dannosi. La regola più efficace è anche la più semplice: nel dubbio non si clicca. Si apre l'app ufficiale, oppure si digita a mano l'indirizzo del sito, e da lì si controlla se esiste davvero una comunicazione in sospeso.

A scuola e in famiglia

Il mondo della scuola ha un motivo in più per stare attento. Quest'estate un gruppo di criminali informatici ha rivendicato il **furto di 6,1 terabyte di dati** da oltre tremila istituti, attraverso una piattaforma del Gruppo Spaggiari Parma, il fornitore del **registro elettronico ClasseViva**. L'azienda ha ridimensionato l'episodio circoscrivendolo al servizio Modulistica Smart, ha precisato che il registro non è stato toccato e ha invitato gli utenti a cambiare la password e a diffidare dei messaggi non richiesti. Quando circolano dati reali il phishing diventa più credibile: una mail che cita il nome del figlio, la classe e la scuola abbassa le difese di qualunque genitore.
Le comunicazioni che sembrano arrivare dal registro elettronico e chiedono di «confermare i dati» o di pagare una quota vanno quindi verificate sull'app ufficiale o con una telefonata alla segreteria. I pagamenti verso la scuola passano dalle piattaforme pubbliche, a cui si accede digitando l'indirizzo, mai dal link ricevuto. Per chi lavora in segreteria, una minaccia di violenza si conserva e si segnala alle forze dell'ordine, che valutano il rischio insieme al prefetto.

Se si è già cliccato

Un errore può capitare, e a quel punto conta la rapidità. Chi ha inserito una password in una pagina sospetta **deve cambiarla subito**, possibilmente da un altro dispositivo, e sostituirla ovunque fosse usata la stessa. È anche il momento di attivare **l'autenticazione a due fattori**, che oltre alla password richiede un codice inviato al telefono: chi conosce soltanto la password non riesce a entrare. Se sono stati comunicati i dati della carta bisogna chiamare la banca e bloccarla. Se è stato aperto un allegato sospetto conviene scollegare il dispositivo da Internet, avviare una scansione con l'antivirus e, in ufficio, avvisare subito il tecnico.
Chi ha consegnato le credenziali della casella di lavoro o della scuola deve avvisare subito l'amministrazione, perché da quell'indirizzo possono partire nuovi messaggi verso colleghi e famiglie, con l'aspetto rassicurante di un mittente conosciuto.
Le mail truffaldine si possono inoltrare al CERT-AGID all'indirizzo malware@cert-agid.gov.it. Le denunce vanno presentate alla Polizia Postale, anche attraverso il portale commissariatodips.it. Davanti a minacce di attentati o di violenza il numero da chiamare è il 112, e il messaggio non va cancellato, perché per gli investigatori è una prova.