

# Data breach Trenitalia: esposti dati di contatto e di viaggio dei passeggeri, alto il rischio phishing



Il data breach Trenitalia, comunicato il 26 giugno, espone i dati di contatto e di viaggio di una parte dei passeggeri. La principale compagnia ferroviaria italiana ha inviato ai clienti interessati una email con oggetto “Comunicazione di violazione dei dati personali ai sensi dell’art. 34 del Regolamento UE 679/2016”, attribuendo l’accesso non autorizzato ai database dei titoli di viaggio a “soggetti esterni non identificati”; al termine delle verifiche tecniche, spiega l’azienda nella comunicazione inviata agli interessati, sono state individuate le persone potenzialmente coinvolte. L’azienda, contattata dalla stampa, ha collocato l’origine dell’incidente nell’ottobre 2025: la ricostruzione tecnica degli accessi e l’identificazione degli interessati hanno richiesto mesi prima dell’invio delle comunicazioni.

Va detto subito ciò che, secondo la stessa Trenitalia, non è stato compromesso: i dati di accesso agli account, le credenziali personali e le informazioni di pagamento come numero della carta, data di scadenza o codice di sicurezza. Non risultano, al momento, rivendicazioni note né elementi che qualifichino l’evento come *ransomware*: la società parla di accesso non autorizzato ai database dei titoli di viaggio.

## Data breach Trenitalia: quali dati sono coinvolti

La violazione potrebbe aver interessato, qualora presenti nei

sistemi associati al titolo di viaggio, diverse categorie di dati personali: dati anagrafici e identificativi (nome, cognome, data e luogo di nascita del passeggero e dell'eventuale acquirente); recapiti di contatto come indirizzo email e numero di telefono; informazioni sul viaggio, tra cui tratta, data, orario e numero del titolo; codice della carta fedeltà associata al biglietto; società o ente datore di lavoro; tipologia di offerta o servizio associata al titolo di viaggio e i dati necessari per fruirne; estremi del documento d'identità; dati tecnici connessi alla generazione del titolo di viaggio. L'ampiezza esatta della platea coinvolta non è stata quantificata ufficialmente. Si tratta, nel complesso, di informazioni che descrivono chi viaggia, come raggiungerlo e quando: un profilo prezioso per chi voglia confezionare comunicazioni fraudolente credibili.

## **Notifica a Garante e CSIRT, denuncia alla Procura**

Trenitalia dichiara di aver adottato immediatamente le misure per contenere l'incidente, interrompendo l'intrusione e rafforzando i controlli sui sistemi. L'accaduto è stato notificato al Garante per la protezione dei dati personali e al CSIRT Italia, e una denuncia è stata presentata alla Procura della Repubblica presso il Tribunale di Roma per avviare le indagini. La società richiama l'articolo 34 del GDPR e le Linee guida EDPB n. 9/2022 (versione 2.0 del 28 marzo 2023) sulla notifica delle violazioni di dati personali, spiegando che la ricostruzione degli accessi e l'identificazione dei clienti hanno richiesto tempo: un passaggio che illustra bene le tempistiche e le valutazioni di rischio dietro la notifica al Garante e la comunicazione agli interessati.

# Il rischio vero: phishing su misura

Proprio perché non sono in gioco password o dati di pagamento, il pericolo più concreto si sposta sull'inganno. Recapiti e dettagli di viaggio sono il materiale ideale per costruire messaggi credibili: la stessa Trenitalia avverte i clienti della possibilità di ricevere email, SMS o telefonate che facciano riferimento a viaggi reali, invitando a non fornire dati personali o finanziari e a verificare sempre il mittente. È la logica dello spear phishing, la truffa personalizzata che usa informazioni autentiche della vittima per abbassarne la guardia. La società ricorda che non contatterà mai i clienti per chiedere password o dati di pagamento e ha attivato un servizio dedicato tramite il *webform* "Privacy – Gestione dei dati personali".

Per chi si occupa di sicurezza, il caso conferma che una violazione senza dati finanziari non è una violazione minore: l'esposizione di contatti e abitudini di viaggio alimenta campagne di frode mirata che possono colpire a distanza di settimane. Trenitalia rientra inoltre tra i soggetti essenziali per il Paese ai sensi della direttiva NIS2, e un episodio simile mostra quanto la superficie d'attacco di queste realtà comprenda ormai l'intera base clienti, non solo i sistemi operativi del trasporto. La difesa, lato utente, resta la verifica del canale e del mittente prima di cliccare; lato organizzazioni, il monitoraggio delle ondate di phishing che sfruttano il marchio Trenitalia nei prossimi giorni.

## Un contesto più ampio: la notifica parallela di Trenitalia Tper

L'episodio si inserisce in una sequenza che ha interessato l'ecosistema informatico del gruppo Ferrovie dello Stato. Nello stesso arco temporale dell'origine dichiarata dall'azienda, tra fine novembre e dicembre 2025 era emerso un

attacco ad Al maviva, fornitore IT del gruppo FS, con l'esfiltrazione di circa 2,3 terabyte di dati poi comparsi su un forum della rete Tor e riconducibili a numerose società del gruppo, Trenitalia inclusa.

Va tenuta distinta una seconda notifica, formalmente autonoma. Trenitalia Tper S.c.a.r.l., società che gestisce il servizio regionale in Emilia-Romagna, ha inviato nelle settimane precedenti una propria comunicazione ai sensi dell'art. 34 GDPR a clienti e dipendenti, con lo stesso impianto: accesso non autorizzato da parte di soggetti esterni non identificati, esclusione di credenziali e dati di pagamento, avviso sul rischio di phishing mirato. La comunicazione Tper differisce però da quella nazionale su punti verificabili: notifica al solo Garante con generico rimando alle Autorità competenti, assistenza tramite numero telefonico dedicato anziché *webform*, nessun richiamo alle Linee guida EDPB, invio via SMS anziché email. Si tratta quindi di due soggetti giuridici distinti e di due comunicazioni separate. Allo stato, le aziende non hanno dichiarato un nesso ufficiale tra le notifiche e l'attacco ad Al maviva: la coincidenza temporale è documentata, mentre l'attribuzione a un'unica matrice resta una ricostruzione non confermata.

Condividi sui Social Network:

<https://www.ictsecuritymagazine.com/notizie/data-breach-trenitalia-passeggeri-phishing/>