Mail da Trenitalia sull’attacco hacker: cosa deve sapere chi ha ricevuto l’avviso

di Roberto Cosentino

Trenitalia ha avvisato i propri clienti di un accesso informatico non autorizzato e che ha potenzialmente compromesso i dati sensibili dei viaggiatori

(Fonte: https://roma.corriere.it/ 26 giugno 2026)

TRENITALIA

Gentile Cliente,

La informiamo che, a seguito di alcune verifiche, abbiamo rilevato un incidente di sicurezza informatica causato da soggetti esterni non identificati. Questo evento ha determinato un accesso non autorizzato ad alcuni dati personali legati ai titoli di viaggio.

Per individuare con precisione i soggetti interessati potenzialmente coinvolti è stato necessario svolgere approfondite analisi tecniche e di sicurezza da parte delle nostre strutture IT. Queste verifiche hanno richiesto tempo, perché si è trattato di ricostruire nel dettaglio eventuali accessi impropri ai dati. Solo al termine di queste attività siamo stati in grado di identificare i clienti interessati e inviare questa comunicazione, come previsto dall'art. 34 del Regolamento (UE) 2016/679 e in conformità con le Linee guida EDPB n. 9/2022 versione 2.0 del 28 marzo 2023 (punti 86 e ss.).

Ci teniamo a rassicurarla su un punto importante: non sono stati coinvolti dati di accesso agli account, credenziali personali o informazioni relative ai pagamenti (come il numero della carta, la scadenza o il codice di sicurezza).

Le informazioni che La riguardano e che potrebbero essere state oggetto di accesso non autorizzato, qualora presenti sui nostri sistemi informatici in relazione al titolo di viaggio, rientrano nelle seguenti categorie di dati personali:

Trenitalia nella giornata del **26 giugno** ha inoltrato ai propri utenti «potenzialmente coinvolti» una comunicazione relativa alla sicurezza dei rispettivi dati personali legati all’acquisto dei biglietti. Una violazione che ha coinvolto potenzialmente dati personali anche sensibili, sebbene non siano stati interessati dati di pagamento o credenziali degli account.

Trenitalia, l'attacco hacker: quali rischi si possono correre?

L'azienda nella comunicazione inoltrata per mail, rassicura innanzitutto che tra i dati violati **non si annoverano credenziali di accesso** o **informazioni di pagamento**. Tuttavia, i criminali informatici potrebbero aver messo le mani sui **dati anagrafici** quali cui nome, cognome, data di nascita e indirizzo; ma anche e-mail, numero di telefono, dati di viaggio, codici delle carte di fedeltà e dettagli sulla professione, oltre agli **estremi dei documenti di identità**. Insomma, dati di pagamento a parte, nel bottino di chi ha commesso l’accesso abusivo, vi sono parecchie informazioni sensibili.

Tra i rischi che possono correre gli utenti? Difficile prevederlo. I dati potenzialmente sottratti potrebbero essere usufruiti per campagne di phishing personalizzate, oppure tentativi di truffa o false comunicazioni riguardo ai viaggi acquistati per motivi simili. Ad ogni modo, che si sia

ricevuta o meno la comunicazione di Trenitalia, **è bene sempre fare attenzione alle comunicazioni che si ricevono e cosa richiedono**. Non bisogna **mai fornire dati personali, credenziali o di pagamento**, dal momento che tali richieste difficilmente provengono da enti legittimi. Inoltre, quando si riceve una comunicazione sospetta, **è sempre bene digitare nella barra degli indirizzi del browser l'indirizzo ufficiale** del **sito web che si intende raggiungere**, così da non correre il rischio di fare clic su collegamenti che portano a piattaforme compromesse. I più recenti software di sicurezza informatica, comunque, possiedono tool o strumenti che permettono di capire se la comunicazione ricevuta è legittima o se il sito che si sta visitando è compromesso.

I precedenti dell'attacco informatico a Trenitalia

La notifica agli enti come il Garante della Privacy, per legge, **dovrebbe avvenire entro le 72 ore**, ma l'evento risale allo scorso ottobre, come confermato dalla stessa compagnia. «A ottobre 2025 Trenitalia ha rilevato un tentativo di attacco informatico causato da soggetti esterni non identificati. L'evento ha determinato un accesso ad alcuni dati personali di una parte dei propri passeggeri».

Non è detto che i dati possano essere usati e come, ma sono nel **dark web da mesi**, per cui la possibilità è che siano anche già stati utilizzati per altri attacchi o ricatti. Il download era disponibile a chiunque, **non è noto dunque se la pubblicazione è dovuta al mancato pagamento di una richiesta di riscatto** (ransomware) o se l'azienda ha pagato ma è stato pubblicato comunque il file. Il gruppo hacker dietro la violazione è per ora ignoto. Nel forum in cui è stato inserito il link alla violazione **non vi sono riferimenti a riguardo** e nemmeno richieste di pagamento per consentire il download.

Da segnalare, inoltre, che nelle prime settimane di giugno, come riporta **BolognaToday**, il servizio di trasporto pubblico ferroviario regionale in Emilia-Romagna, **Trenitalia Tper S.c.a.r.l.**, ha pubblicato una comunicazione simile: «Trenitalia Tper informa che è stato rilevato un evento di sicurezza informatica, causato da un soggetto esterno, con accesso non autorizzato a dati personali connessi all'acquisto di titoli di viaggio. Non risultano coinvolti dati di pagamento, né credenziali di accesso. Sono state adottate misure di sicurezza e avviate verifiche tecniche per tutelare gli interessati». **Trenitalia conferma che i due eventi sono correlati.**