ATMA Soc. Cons. per Azioni
Via Alessandro Bocconi, 35
60125 Ancona

T. +39 071 2837 468
F. +39 071 2837 433
info@atmaancona.it
atma.pec@legalmail.it
www.atmaancona.it

azienda trasporti e mobilità di ancona e provincia

Oggetto: Comunicazione riservata agli utenti dell'APP ATMA registrati prima dell'attacco informatico avvenuto tra il 29 e il 30 marzo 2025

Gentile Utente,

su richiesta dell'Autorità Garante, siamo a meglio specificare e a fornire ulteriori informazioni rispetto a quanto già comunicatoLe con il precedente invio del 10/04/2025 e 10/07/2025 e con quanto già pubblicato nei siti https://www.atmaancona.it/ **relativamente all'attacco informatico avvenuto tra il 29 e il 30 marzo 2025**, nonché alla conseguente esfiltrazione di alcuni dati personali.

Le chiediamo di considerare questa comunicazione, integrante quelle già fornite sugli altri canali informativi messi a disposizione (APP, siti *web*), come completa descrizione dei fatti accaduti, così da garantire piena trasparenza.

Le scriviamo per fornire informazioni importanti relative alla sicurezza dei Suoi dati personali, ivi incluse le credenziali di accesso all'App Atma, in gestione a myCicero, e per indicare le azioni necessarie che deve mettere in atto qualora Lei non le avesse già intraprese.

La presente comunicazione è stata redatta in linguaggio semplice e chiaro, evitando tecnicismi, proprio per facilitare la lettura da parte di ogni utente.

Cosa è successo:

Tra il 29 e il 30 marzo 2025 si è verificato un attacco informatico che ha colpito i sistemi tecnologici, gestiti da myCicero S.r.l. e dai fornitori di servizi IT, sui quali risiede anche l'App Atma.

MyCicero, in collaborazione con l'Autorità Garante, ha attivato sin da subito tutte le necessarie procedure di sicurezza fin dall'immediatezza dei fatti, collaborando con le Autorità competenti, inclusa l'Agenzia per la Cybersicurezza Nazionale (ACN).

Quali informazioni sono state coinvolte:

La violazione aveva comportato l'esfiltrazione dei Suoi dati personali incluse le credenziali di autenticazione all'App Atma.

Nello specifico, gli autori dell'attacco hanno esfiltrato **dati personali**, propri del "**Profilo Utente**":

- Nome, cognome, indirizzo e-mail e numero di telefono;
- Eventuale Codice Fiscale o Partita IVA, se da Lei forniti;
- Le credenziali di autenticazione (username e password, sotto forma di stringa di testo «*hashed*», detta anche «*digest hashed*» della password).

Sono stati altresì esfiltrati, inoltre, i dati relativi ai Suoi **titoli di mobilità** eventualmente acquistati e i **dati personali ad essi correlati**. A seconda del titolo di mobilità, tali dati sono relativi al servizio:

- "**Biglietti TPL**": data acquisto, importo pagato, zona tariffaria, tipologia e data validità del titolo;
- "**Abbonamenti TPL**": data inizio e fine validità, zona tariffaria, importo pagato, tipologia titolo acquistato;

Non sono stati coinvolti i dati relativi a carte di credito o altri strumenti di pagamento.

Quali sono i potenziali rischi?

La divulgazione di queste informazioni potrebbe esporla a rischi quali la ricezione di e-mail o messaggi di *spam* e tentativi di truffa (*phishing*). Inoltre, se utilizzava o utilizza tuttora la stessa password o una simile per altri servizi online, esiste il rischio che soggetti non autorizzati possano tentare di accedere anche a tali servizi e alle informazioni ivi ospitate.

Più precisamente, la seguente tabella collega ogni tipo di dato sottratto a un esempio di rischio concreto. Questo Le permetterà di comprendere meglio la Sua personale esposizione e di agire di conseguenza.

Categoria di Dati	Dati Specifici Sottratti	Esempio di Rischio Concreto Associato
Dati del Profilo e Contatti	**Solo se registrati in APP prima del 29 marzo 2025.** **Nome, cognome, indirizzo e-mail, numero di telefono, ed eventuale Codice Fiscale o Partita IVA da Lei forniti.**	**Ricezione di e-mail o SMS di phishing molto credibili (truffe informatiche), tentativi di furto d'identità o di iscrizione a servizi non richiesti.**
Credenziali di Autenticazione	Solo se in uso prima del 29 marzo 2025. Username e password, sotto forma di stringa di testo «*hashed*», detta anche «*digest hashed*» della password.	Decifrazione della password e accesso non autorizzato. In caso di uso della stessa password per altri servizi (e-mail, social media, altro), anche quegli account sono a rischio di accesso non autorizzato.
Dati di Viaggio e Mobilità	Solo se utilizzato il servizio prima del 29 marzo 2025. Biglietti e abbonamenti per il trasporto pubblico (bus), includendo date, orari, luoghi di partenza e arrivo, importi pagati ed eventuali nomi di altri passeggeri.	Conoscenza degli spostamenti, che può rivelare informazioni sullo stile di vita.

Cosa è stato fatto?

A seguito dell'accaduto il fornitore ha dichiarato di aver implementato un articolato piano di rafforzamento di tutte le infrastrutture di sicurezza impiegate, anche dai subfornitori di tecnologia, per proteggere i dati. Sono state revisionate e rafforzate le misure tecniche, compreso il miglioramento degli algoritmi di crittografia e l'implementazione di sistemi di monitoraggio più avanzati per prevenire accessi non autorizzati in futuro.

Inoltre, **in data 01 ottobre 2025 sono state cancellate definitivamente le password di accesso all'App Atma, qualora la stessa non fosse da Lei stata già modificata dal 29 marzo 2025 in poi.**

Tale procedura si è resa necessaria per:

- facilitare la migrazione ad algoritmo più evoluto;
- forzare l'intera utenza dell'App Atma a modificare la password.

Cosa deve fare Lei ora per la sicurezza dei Suoi dati?

In considerazione delle informazioni sopra riportate, qualora Lei **utilizzasse la stessa password o una simile per altri servizi online**, La invitiamo a **provvedere immediatamente al suo aggiornamento su tali piattaforme qualora non avesse già provveduto**.

Cosa può fare Lei in futuro per migliorare la sicurezza dei Suoi dati?

La invitiamo a scegliere sempre password più complesse possibili, caratterizzate da simboli, numeri, lettere maiuscole e minuscole, di lunghezza particolarmente elevata. Tali password non dovrebbero coincidere con parole e termini noti, e non dovrebbero contenere elementi a Lei riconducibili (si pensi a password contenenti il suo nome e cognome associati alla sua data di nascita). Le suggeriamo altresì di modificare periodicamente le password utilizzate.

In termini generali, si raccomanda di attivare l'autenticazione a più fattori sull'account di posta elettronica collegato alla sua utenza, ove possibile. In presenza di comunicazioni che richiamano la presunta violazione, occorre mantenere la massima prudenza: verificare con cura l'identità del mittente di e-mail e SMS e non fornire mai dati personali in risposta a messaggi inattesi.

Per ridurre i rischi connessi ai dati di viaggio e spostamento potenzialmente esposti, Le suggeriamo di prestare particolare attenzione a possibili tentativi di phishing o ingegneria sociale. Ad esempio, un malintenzionato potrebbe contattarla citando tratte, orari o importi reali per apparire credibile e indurla a condividere informazioni. In tali casi, mantenga la massima diffidenza, non fornisca mai password, codici o dati di pagamento via e-mail o SMS e verifichi l'autenticità di qualsiasi richiesta solo attraverso canali ufficiali reperiti autonomamente (sito o numero dell'operatore).

La informiamo, inoltre, che la nostra Società non effettua contatti telefonici per richiedere o farLe confermare questo tipo di informazioni.

Cordiali saluti

Ancona, lì 21/01/2026

PAPAVERI
MUZIO
21.01.2026
10:40:39
GMT+01:00

Il Presidente ATMA S.c.p.A.

Dott. Muzio Papaveri

***

Per ogni ulteriore informazione in merito ad ogni aspetto di questa vicenda, può contattare il nostro servizio di assistenza specifica ai seguenti indirizzi:

info@atmaancona.it

Il nostro DPO può essere contattato all'indirizzo e-mail: dpo@atmaancona.it