AMET S.p.A.
Fondata nel 1908 già AEM

Oggetto: Importante comunicazione di sicurezza relativa ad una violazione di dati personali

Gentile Interessato/a,

con la presente comunicazione desideriamo informarLa di un incidente di sicurezza che ha coinvolto i sistemi informatici di AMET S.p.A. e che ha comportato una violazione di dati personali.

COSA È ACCADUTO E QUALI INIZIATIVE ABBIAMO INTRAPRESO

A seguito di un tentativo di truffa in danno di AMET S.p.A. abbiamo riscontrato accessi abusivi all'*account* di posta elettronica di un nostro dipendente, e l'impostazione di una regola di inoltro automatico dei messaggi verso un indirizzo *e-mail* esterno, non controllato dalla nostra Società.

Appena scoperto l'evento, abbiamo immediatamente disattivato la regola di inoltro, avviato un'indagine interna e notificato l'accaduto all'Autorità Garante per la Protezione dei Dati Personali. Sono tutt'ora in corso ulteriori indagini e nel frattempo stiamo adottando ulteriori misure, tecniche e organizzative, volte a evitare il ripetersi di simili incidenti e a garantire un adeguato livello di protezione dei dati personali trattati.

QUALI SOGGETTI E QUALI DATI PERSONALI HA RIGUARDATO L'INCIDENTE DI SICUREZZA

L'incidente, che ha riguardato un numero significativo di soggetti, tra cui dipendenti di AMET S.p.A., utenti, consulenti e personale dipendente di fornitori e/o altri soggetti con cui la Società intrattiene rapporti commerciali, ha comportato un potenziale accesso non autorizzato a dati personali, tra cui l'**indirizzo email** degli interessati e (ove presenti all'interno della singola comunicazione) alle seguenti ulteriori categorie di dati personali:

- **dati anagrafici** (come ad es. nome e cognome) **e/o altri dati identificativi** (come, ad es., codice fiscale, POD);
- **dati di contatto** (numeri di telefono, indirizzo di residenza e/o di fornitura);
- **dati di fatturazione e/o di pagamento**;
- **dati relativi a documenti di riconoscimento**.

QUALI SONO I POTENZIALI RISCHI:

In considerazione della natura dei dati coinvolti, i potenziali rischi sono da ricondursi a:

- tentativi di **phishing** (tipologia di truffa che mira, principalmente attraverso email, sms, altri messaggi di testo, telefonate e/o siti dal contenuto ingannevole, a carpire informazioni e/o dati personali, in particolare quelli di accesso a servizi, quali, ad esempio, quello di *internet banking*);

- tentativi di ***social engineering*** (insieme di tecniche utilizzate per indurre un soggetto a compiere determinate azioni e/o a comunicare informazioni riservate);

- possibili **furti di identità** (la combinazione di dati anagrafici e di contatto con altri dati identificativi può agevolare il furto d'identità e la conseguente sostituzione di persona);

- **altre forme di frode.**

COSA FARE PER TUTELARSI

Per difendersi dai suddetti rischi è consigliabile:

- **prestare la massima attenzione a e-mail, SMS o chiamate, inattese e/o sospette**, con cui vengono richiesti dati personali, in particolare credenziali di accesso o informazioni finanziarie, anche se provenienti da AMET S.p.A. Si raccomanda, inoltre, di non cliccare su *link* e di non aprire allegati provenienti da mittenti sconosciuti.

- **verificare sempre l'autenticità delle richieste:** in caso di dubbi su una comunicazione che sembra provenire da AMET S.p.A., ci contatti direttamente tramite i canali ufficiali ai recapiti indiati sul sito, evitando di rispondere alla comunicazione sospetta.

- **monitorare le attività sui propri account:** controlli regolarmente gli estratti conto bancari e le attività sui suoi *account online* per rilevare eventuali transazioni o accessi non autorizzati.

ULTERIORI INFORMAZIONI

Per qualsiasi chiarimento sulla presente comunicazione per sapere se la violazione riguarda la Sua persona o per ulteriori informazioni sulla violazione medesima, è possibile contattare il nostro Responsabile per la protezione dei dati (Polis Avvocati Sta Coop, nella persona dell'avv. Antonio Arzano) all'indirizzo e-mail **dpo@ametspa.it**

Trani, 16 giugno 2024

Il Presidente

dott.ssa Silvia Caputo