Revolut, falsa richiesta da una PEC istituzionale espone i dati di 680 clienti

Data: Invalid Date | Autore: Redazione

Una casella di posta certificata riconducibile a un’istituzione italiana sarebbe stata utilizzata per ottenere informazioni riservate dalla fintech britannica. Avviate le indagini della Polizia postale mentre la società assicura che il denaro dei clienti non è stato sottratto

Una sofisticata operazione di **impersonificazione digitale**avrebbe consentito a un gruppo di hacker di ottenere da **Revolut** i dati personali e finanziari di circa **680 clienti**. Per rendere credibili le richieste, i criminali informatici avrebbero utilizzato un indirizzo e-mail istituzionale compromesso, appartenente al dominio legittimo di un’autorità italiana.

La corrispondenza appariva quindi collegata a una reale attività delle forze dell’ordine. Convinta di rispondere a richieste ufficiali formulate nell’ambito di un’indagine, la società avrebbe trasmesso una serie di informazioni riservate.

La **Polizia postale**ha avviato gli accertamenti ipotizzando i reati di accesso abusivo a un sistema informatico e frode informatica. Le indagini dovranno chiarire come sia stata compromessa la casella istituzionale e individuare i responsabili dell’operazione.

Quali dati sarebbero stati comunicati

Secondo quanto reso noto da Revolut, l'incidente avrebbe interessato un numero circoscritto di utenti. Tra le informazioni potenzialmente finite nelle mani di soggetti non autorizzati figurerebbero:

- dati contenuti nei **documenti di identità**
- numeri di passaporto
- indirizzi di residenza
- informazioni relative ai conti
- dettagli sulle operazioni e sui movimenti bancari

La società ha precisato che l'attacco non avrebbe comportato una violazione diretta dei propri sistemi informatici. Non risulterebbero compromessi neppure i fondi depositati dai clienti.

Il caso, dunque, non sarebbe riconducibile a un'intrusione nei server di Revolut, ma a una forma avanzata di **ingegneria sociale**basata sull'utilizzo fraudolento di credenziali e canali istituzionali autentici.

Come è stata realizzata la truffa contro Revolut

Gli autori dell'attacco avrebbero sfruttato un indirizzo appartenente a un dominio governativo legittimo per presentare delle richieste di informazioni apparentemente valide. Le comunicazioni sarebbero state formulate come atti necessari allo svolgimento di una presunta indagine internazionale.

La presenza di una corretta autenticazione tecnica del dominio avrebbe aumentato la credibilità dei messaggi. Per Revolut, le comunicazioni provenienti da indirizzi governativi verificati vengono normalmente gestite come **richieste legali obbligatorie**.

Proprio questo meccanismo di fiducia sarebbe stato trasformato dai criminali in uno strumento per ottenere i dati. Gli istituti finanziari, infatti, sono tenuti a collaborare con le autorità e a fornire determinate informazioni quando ricevono richieste formalmente valide.

I contatti sarebbero proseguiti per diversi mesi

La truffa non sarebbe stata realizzata attraverso una singola comunicazione. Gli hacker avrebbero intrattenuto per almeno due mesi uno scambio di messaggi con la società, presentandosi come appartenenti alle forze dell'ordine italiane.

Uno o più componenti del gruppo, identificati dallo pseudonimo **iamnotavillain**, avrebbero successivamente rivendicato l'operazione attraverso Telegram. Secondo il loro racconto, le richieste sarebbero state inviate più volte prima che l'inganno venisse scoperto.

Questa ricostruzione dovrà essere verificata dagli investigatori. La durata dello scambio, tuttavia, mostra quanto possa risultare difficile riconoscere una frode quando il mittente utilizza un dominio realmente riconducibile a un ente pubblico.

La risposta della società dopo la scoperta

Revolut ha dichiarato di essere intervenuta non appena individuata la truffa. L'indirizzo compromesso sarebbe stato immediatamente bloccato e la vicenda segnalata all'istituzione interessata.

La fintech ha inoltre informato:

- le autorità investigative
- gli organismi per la protezione dei dati
- le autorità di vigilanza finanziaria
- i clienti direttamente coinvolti

Agli utenti interessati sarebbe stata offerta assistenza specifica per ridurre il rischio di ulteriori abusi. Anche se i fondi non risultano sottratti, la disponibilità di **dati personali e bancari**potrebbe favorire nuovi tentativi di phishing, furti d'identità o comunicazioni fraudolente particolarmente credibili.

Codacons chiede chiarimenti sui clienti italiani

Sulla vicenda è intervenuto anche il **Codacons**, che ha chiesto di accertare se tra le persone coinvolte vi siano clienti residenti in Italia e quali categorie di dati siano state effettivamente comunicate.

L'associazione dei consumatori ha annunciato di valutare eventuali iniziative legali qualora venissero confermate violazioni della privacy degli utenti. Ha inoltre sollecitato verifiche sull'eventuale compromissione di altre caselle di posta appartenenti a istituzioni e forze dell'ordine italiane.

Il timore è che indirizzi istituzionali violati possano essere impiegati per rivolgere richieste analoghe ad altre banche, aziende o piattaforme digitali, esponendo una quantità più ampia di informazioni riservate.

Perché una PEC compromessa rappresenta un rischio elevato

La **PEC istituzionale**è normalmente considerata un canale affidabile perché permette di identificare il dominio del mittente e garantisce la tracciabilità delle comunicazioni. Tuttavia, queste caratteristiche non proteggono il destinatario quando è la casella autentica a essere stata compromessa.

L'incidente mette quindi in evidenza la necessità di affiancare ai controlli automatici ulteriori procedure di verifica. In presenza di richieste particolarmente estese o riguardanti informazioni finanziarie sensibili, può essere necessario confermare l'autenticità della comunicazione attraverso un secondo canale indipendente.

Cosa dovrebbero fare i clienti coinvolti

Gli utenti che hanno ricevuto una comunicazione ufficiale da Revolut dovrebbero controllare con attenzione il proprio account e diffidare di e-mail, telefonate o messaggi che facciano riferimento all'accaduto.

È consigliabile non comunicare codici di accesso o credenziali, attivare l'**autenticazione a due fattori** e verificare periodicamente i movimenti bancari. Qualsiasi operazione sospetta deve essere segnalata immediatamente alla società e alle autorità competenti.

L'episodio dimostra che la **sicurezza informatica bancaria**non dipende soltanto dalla protezione dei server. Anche l'affidabilità dei canali utilizzati per le comunicazioni ufficiali e la verifica delle richieste esterne rappresentano elementi essenziali per tutelare i dati dei clienti.