

APP FINANZIARIE E SICUREZZA: L'ULTIMO CASO DI VIOLAZIONE DEI DATI

29 Aprile 2022



Tra i principali usi a cui le app vengono destinate c'è quello finanziario. Che si tratti di semplici app bancarie o di applicazioni più sofisticate e dedicate agli investimenti, nella finanza tradizionale o in quella decentralizzata, le app offrono una grande comodità. Basta un semplice tocco per visualizzare la situazione complessiva delle nostre finanze, senza dover ogni volta inserire password e codici. Effettivamente, le informazioni che immagazziniamo sono tante: potevano sfuggire ai malintenzionati della rete? Ovviamente no.

L'ultimo caso che ha riguardato una violazione massiccia dei dati e che ha destato preoccupazione in tutto il mondo è avvenuto con Cash App, l'applicazione creata per inviare e ricevere denaro (inclusa la crypto) e fare acquisti online. Come talvolta accade, "la talpa" era all'interno della società stessa: trattasi quindi di una minaccia interna, ovvero qualcuno che ha accesso legalmente ai dati e alle informazioni dell'azienda ma ne fa un uso illegale.

Il 10 dicembre 2021, un dipendente di Cash App ha scaricato dati in massa relativi ai clienti (magari con la prospettiva di arrotondare il suo budget per il Natale). Le informazioni sottratte includevano i nomi degli utenti dell'app, gran parte dello storico delle loro transazioni, gli asset presenti nei loro portafogli e tutte le attività di trading eseguite in giornata.

I responsabili della società si sono affrettati ad assicurare che alcuni tipi di informazioni sensibili non sono stati sottratti, ma rimane il dubbio anche in relazione a quanti utenti effettivi abbiano subito una violazione dei dati. Le stime parlano di almeno 8,2 milioni di utenti negli Stati Uniti, ma in realtà il numero potrebbe essere più elevato: in sostanza, tutti gli utenti sono rimasti con il dubbio di essere stati coinvolti dall'evento.

App finanziarie e sicurezza: due realtà non sempre in sintonia

Quando utilizziamo le app finanziarie, spesso ci sentiamo sicuri che il provider dei servizi adotti tutte le misure necessarie per proteggere il nostro account. Purtroppo però le precauzioni poste in essere dall'altra parte non sempre sono sufficienti a garantire la sicurezza del nostro conto. Come minimo, ogni volta che accediamo a un'applicazione, soprattutto se relativa a denaro e finanza, [dovremmo usare una VPN](#), oltre che un antivirus in grado di rilevare ogni tipo di minaccia e di tentativo malevolo (basti pensare al [phishing](#)).

La qualità è importante quando si tratta di sicurezza: i danni che possiamo subire purtroppo sono difficilmente recuperabili. Per avere una panoramica più ampia delle cattive esperienze vissute dagli utenti di servizi finanziari online, basti ricordare alcuni esempi:

- nell'agosto del 2020, la società di credito al consumo [Experian ha subito una violazione dei dati](#) che ha visto coinvolti circa 24 milioni di clienti. Tra le informazioni rubate, oltre al nome e ai recapiti telefonici, erano comprese anche quelle relative alla residenza, al luogo di lavoro e al tipo di posizione lavorativa svolta. Quanto basta quindi per integrare un furto d'identità.
- Nel 2017, i clienti di Equifax hanno vissuto un'esperienza ancora peggiore, dato che 147 milioni di utenti hanno visto sottrarsi, oltre alle informazioni personali, anche i numeri di carta di credito e i dati della patente di guida. Sicuramente un'esperienza da dimenticare!

- Nel gennaio 2008, Heartland, società leader nel sistema di pagamenti, ha assistito a una violazione dei dati dei propri clienti di portata enorme: sono stati rubati circa 100 milioni di numeri di carte di debito e credito, nonché le date di scadenza.

Quantificare i danni derivanti da questo tipo di violazioni è praticamente impossibile; prevenire però è una soluzione che di regola può essere applicata senza grandi difficoltà.