

Agenti AI entrano nei conti bancari USA, c'è rischio di azioni fuori controllo

AI, le banche non distinguono più gli agenti dagli umani. Wall Street lancia l'allarme

Alcune delle principali banche statunitensi, tra cui **Morgan Stanley, Bank of America, JPMorgan e Wells Fargo**, stanno rilevando **agenti di intelligenza artificiale (AI)** che accedono ai conti dei clienti e, in certi casi, sembrano avviare attività non riconducibili alle istruzioni dell'utente. A riferirlo è *Axios*, citando persone informate. Il fenomeno è ancora difficile da misurare, ma ha già spinto diversi istituti a bloccare o limitare l'accesso degli strumenti di terze parti.

Il punto critico è che non tutti gli accessi sono uguali. **In molti casi il cliente autorizza un agente a entrare nel proprio conto usando le sue credenziali**, per esempio per controllare le spese o completare un'attività. Diversi istituti chiedono nei propri termini di servizio che sia la persona, non un programma, a effettuare l'accesso. Quando l'agente può anche disporre pagamenti o trasferire denaro, un'autorizzazione concessa con leggerezza può avere conseguenze concrete.

Il rischio vero è un agente AI con

accesso al denaro

Gli istituti temono soprattutto che un agente dotato di credenziali e di poteri operativi possa eseguire azioni dannose, **per errore** o perché ha ricevuto **istruzioni manipolate**. Un assistente progettato per svolgere compiti autonomamente può infatti interpretare una richiesta in modo imprevisto e agire prima che il cliente se ne accorga. **Il rischio aumenta se può spostare fondi, fare acquisti o interagire con il servizio clienti.**

Come raccontato da Madison Mills, alcune banche hanno osservato **agenti contattare i call center o compiere attività che sembravano non corrispondere alle istruzioni dell'utente**. Non significa che ogni accesso di un agente sia fraudolento, né che siano stati accertati ammanchi: Morgan Stanley ha dichiarato di non aver rilevato accessi di agenti "fuori controllo" alle proprie piattaforme. Ma **gli istituti faticano a distinguere un'azione automatizzata autorizzata da una non autorizzata**, o a capire se un agente abbia davvero agito per conto del cliente.

È questa ambiguità a rendere il problema urgente. I sistemi antifrode sono costruiti per riconoscere comportamenti sospetti, ma devono poter ricostruire chi ha impartito un ordine e chi lo ha eseguito. Se un agente usa le credenziali del cliente, la traccia può apparire legittima anche quando l'azione non lo è.

La risposta delle banche

Morgan Stanley ha iniziato a bloccare agenti di terze parti; JPMorgan, Bank of America e Citi stanno adottando restrizioni. Un portavoce di Chase ha **invitato i clienti a non condividere username e password**. Al tempo stesso, molti istituti valutano una via intermedia: consentire l'accesso in sola lettura, così che gli agenti possano consultare le informazioni finanziarie

senza disporre operazioni.

È un compromesso già noto nel settore: servizi come Quicken possono accedere ai dati per aiutare nella gestione del bilancio. Ma un agente capace di ragionare e agire introduce un livello diverso di rischio. Per questo la sola prudenza degli utenti non basta: servono autorizzazioni limitate, tracciabili e revocabili, con una distinzione chiara tra consultare un conto e muovere denaro.

Un rischio che supera il singolo conto

Se un agente compromesso o mal configurato potesse operare su molti conti, **l'impatto potrebbe estendersi oltre il singolo cliente**: frodi, trasferimenti indesiderati, investimenti azzardati e difficoltà nel ripristinare rapidamente l'accesso. Per le banche, la sfida è anche mantenere la fiducia in un'infrastruttura essenziale.

C'è poi una questione di responsabilità: **se l'agente sbaglia, chi risponde?** Il cliente che gli ha dato accesso, la società che lo ha sviluppato o la banca che ha accettato la transazione? Senza regole e registrazioni verificabili, ricostruire i fatti può diventare difficile. In prospettiva, **l'uso su larga scala di agenti finanziari potrebbe anche amplificare decisioni automatiche errate e vulnerabilità comuni**, con effetti sulla stabilità e sulla fiducia pubblica.

Le banche riconoscono che i clienti vorranno sempre più usare questi strumenti. Il problema è permetterlo senza consegnare loro un potere incontrollato sul denaro. Per ora, la risposta è limitare l'accesso e sperimentare modalità più sicure. La velocità con cui evolvono gli agenti, però, rende insufficiente affidarsi soltanto a blocchi e condizioni d'uso: occorre stabilire in modo verificabile quali azioni possono compiere, per conto di chi e con quali limiti.

The post Agenti AI entrano nei conti bancari USA, c'è rischio di azioni fuori controllo appeared first on Key4biz.

<https://www.key4biz.it/agenti-ai-entrano-nei-conti-bancari-usa-ce-rischio-di-azioni-fuori-controllo/591792/>