

Mi hanno hackerato il conto! E adesso?

È l'incubo di tutti i clienti delle banche: qualcuno accede al conto e lo saccheggia. Se è già successo, bisogna contenere i danni – e imparare la lezione per il futuro.

Cosa fare in caso di accesso non autorizzato al proprio conto bancario:

- Se notate transazioni sospette o errori durante l'accesso all'e-banking, informate subito il vostro istituto finanziario e bloccate il contratto di e-banking in questione, i conti e le carte.
- Scollegate immediatamente da Internet tutti i dispositivi che potrebbero essere stati colpiti dagli hacker o da malware e spegneteli, oppure attivate la modalità aereo. Non effettuate subito un ripristino, però, perché potrebbero servire alla polizia per le analisi forensi.
- Modificate le password accedendo da un dispositivo diverso e non infetto. Se è possibile, impostate sempre l'autenticazione a doppio fattore.
- Se si tratta davvero di un atto criminale, presentate denuncia penale alla polizia. Prendete nota di tutte le informazioni che avete sulla frode o l'attacco.
- In futuro proteggetevi da accessi non autorizzati con le nostre «5 operazioni per la vostra sicurezza digitale» e i consigli per un e-banking sicuro.

Come si hackera un conto bancario?

I portali di e-banking degli istituti finanziari svizzeri godono di un'ottima protezione dagli attacchi informatici. A dire tutta la verità, oggi si può escludere la possibilità che qualche criminale riesca ad accedere direttamente ai sistemi informatici di una banca.

Un punto debole, tuttavia, è il cliente disattento: se gli hacker mettono le mani sui suoi dati d'accesso, possono accedere all'e-banking a suo nome senza che nessuno se ne accorga, ed eseguire transazioni o accedere a informazioni riservate. Ciò può avvenire, per esempio, a seguito di un [attacco di phishing \(https://www.ebas.ch/it/phishing/\)](https://www.ebas.ch/it/phishing/) o un'infezione di [malware \(https://www.ebas.ch/it/infezione-da-malware/\)](https://www.ebas.ch/it/infezione-da-malware/) specifico. A chi subisce il danno, poi, resta poco da fare se non cercare di limitare i danni.

Qual è il modo giusto di reagire di fronte a un danno?

Prima di tutto, la cosa più importante: se nutrite un sospetto, non c'è un minuto da perdere! Se poi constatate che è stata davvero commessa una frode, il contratto di e-banking interessato e i relativi conti vanno bloccati immediatamente, così da impedire ulteriori movimenti in uscita.

Ogni volta che sospettate una frode, per esempio se osservate transazioni sospette o messaggi di errore nell'e-banking, dovete informare immediatamente l'istituto finanziario per concordare il da farsi. Se la frode è confermata, denunciate il caso anche alla polizia.

Se, anche dopo aver parlato con la banca, non riuscite a ricostruire come i criminali abbiano potuto eseguire l'ac-

cesso, la prima ipotesi dev'essere che qualche sconosciuto conosce le vostre credenziali e sul dispositivo si è infiltrato un software dannoso, come un cavallo di Troia per l'e-banking.

Per prevenire ulteriori abusi dei vostri dati d'accesso (presumibilmente rubati), è consigliabile cambiare per precauzione la [password \(https://www.ebas.ch/it/4-proteggere-gli-accessi-online/\)](https://www.ebas.ch/it/4-proteggere-gli-accessi-online/) della casella di posta elettronica e quelle di tutti gli account online – senza usare il computer o dispositivo mobile che potrebbe essere infetto, ma uno strumento diverso. L'accesso all'e-banking è già stato bloccato: potrete cambiare quella password in un secondo momento, dopo aver chiarito la situazione con la banca.

Dove è disponibile, inoltre, attivate l'autenticazione a doppio fattore per godere di una protezione sostanzialmente più robusta degli accessi.

Scollegate il dispositivo dalla rete e spegnetelo, oppure attivate la modalità aereo; attendete però un eventuale esame da parte della polizia prima di [effettuare un ripristino \(https://www.ebas.ch/it/reinstallazione-di-windows-10/\)](https://www.ebas.ch/it/reinstallazione-di-windows-10/).

E, non da ultimo, mettete in atto per il futuro una protezione efficace contro altri tentativi di frode. Assicuratevi quindi di seguire le [«5 operazioni per la vostra sicurezza digitale» \(https://www.ebas.ch/it/5-operazioni-per-la-vostra-sicurezza-digitale/\)](https://www.ebas.ch/it/5-operazioni-per-la-vostra-sicurezza-digitale/) e i [consigli per un e-banking sicuro \(https://www.ebas.ch/it/consigli-per-un-e-banking-sicuro/\)](https://www.ebas.ch/it/consigli-per-un-e-banking-sicuro/) – con le giuste precauzioni non darete più nessuna chance agli hacker!

Misure immediate in caso di sospetto:

- *Informare l'istituto finanziario e far bloccare il conto*
- *Disconnettersi da Internet*
- *Cambiare le password*
- *Sporgere denuncia penale*

La banca è in grado di riconoscere e bloccare gli abusi?

Alcuni istituti finanziari dispongono di un sistema di rilevamento delle frodi che segnala le transazioni sospette o addirittura le interrompe automaticamente. Con il passare del tempo questi sistemi migliorano continuamente, ma non offrono una sicurezza al 100%. E i truffatori li aggirano con sempre maggiore abilità e discrezione.

Ciò significa che ognuno deve essere responsabile in prima persona: non aspettatevi che sia solo la banca, sempre e comunque, a proteggere i vostri conti da accessi non autorizzati – pensate al phishing, per esempio.

Chi risponde dei danni?

Sulla responsabilità non esiste una risposta generale, ed è necessaria una valutazione caso per caso. Oltre alla questione della colpa, infatti, svolge un ruolo determinante l'obbligo di diligenza.

Poiché in genere i colpevoli sono ignoti e operano dall'estero, spesso le indagini penali si scontrano con tutta una serie di ostacoli, tra cui il frequente coinvolgimento di intermediari che sono all'oscuro di tutto, i cosiddetti «[Money Mule](https://www.ebas.ch/it/money-mules-agenti-finanziari/)» (<https://www.ebas.ch/it/money-mules-agenti-finanziari/>), per dissimulare le operazioni. In molti casi, il denaro trasferito si può ritenere perduto per sempre.

Come regola generale, sia gli istituti finanziari che i loro clienti devono dare atto del proprio obbligo di diligenza nella gestione dei conti bancari e dei relativi fondi. Un tribunale valuterà quindi eventuali inadempienze e potrebbe anche imputare il problema al cliente, il quale per esempio potrebbe aver rivelato (consapevolmente o meno) i suoi dati d'accesso a uno sconosciuto.

Per non trovarvi costretti a studiare i rapporti di responsabilità, [proteggete il vostro conto adottando misure preventive](https://www.ebas.ch/it/consigli-per-un-e-banking-sicuro/) (<https://www.ebas.ch/it/consigli-per-un-e-banking-sicuro/>) !