

29.07.2020

Attenzione agli ordini di pagamento via e-mail

Una recente sentenza del Tribunale federale fa discutere: il conto di un cliente è stato saccheggiato dagli hacker, e la sua banca non è tenuta a risponderne. Ma da casi come questo ci si può proteggere.

A Jean-Claude Henchoz (*nome di fantasia*) è mancato il fiato quando ha letto la sentenza definitiva con cui il Tribunale federale stabilisce che è lui, cliente di una banca privata ginevrina, a doversi sobbarcare il danno provocatogli dagli hacker. In prima istanza, il Tribunale cantonale aveva imposto alla banca di rimborsargli buona parte della perdita, pari a diverse centinaia di migliaia di euro.

I criminali erano riusciti ad accedere al suo account e-mail e lo avevano utilizzato per ordinare alla banca diversi trasferimenti verso conti all'estero. Il problema è che il contratto esistente tra la banca e il cliente prevedeva la possibilità di inviare ordini di pagamento via e-mail, telefono e fax, senza richiedere la forma scritta, e di questo cavillo hanno approfittato gli hacker.

Il Tribunale cantonale di Ginevra aveva inizialmente stabilito che la banca avrebbe dovuto notare e bloccare i pagamenti illeciti per tempo. Il Tribunale federale non ha invece riscontrato alcun errore da parte della banca, la quale non sarebbe tenuta a presumere una potenziale origine fraudolenta, né a eseguire verifiche aggiuntive, quando riceve un mandato via e-mail a norma del contratto. Il rischio legato a errori di identificazione e trasmissione sarebbe quindi a carico del cliente.

Seguite queste raccomandazioni per proteggervi dalle perdite dovute a ordini di pagamento illeciti:

- Se possibile, conferite gli ordini di pagamento esclusivamente attraverso il portale di e-banking o l'app per il Mobile Banking della vostra banca, oppure di persona allo sportello, e chiedete il blocco contrattuale di canali diversi come e-mail, telefono e fax per l'esecuzione di pagamenti.
- Se non potete rinunciare all'e-mail per gli ordini di pagamento, utilizzate un provider di posta elettronica che offra l'autenticazione a due fattori e attivate questa protezione aggiuntiva.
- Utilizzate password diverse e complesse per tutti i vostri account di posta elettronica e per l'e-banking, conservatele in modo sicuro (p. es. con un password manager) e non rivelatele mai a nessuno.
- Impostate un indirizzo e-mail separato per comunicare con la vostra banca, non utilizzate quell'indirizzo per nessun altro scopo e non comunicatelo a nessun altro oltre alla banca.
- Se possibile, chiedete alla banca di prevedere un passaggio di autorizzazione delle transazioni, affinché tutti gli ordini di pagamento che superano un determinato importo possano essere eseguiti solo previa vostra conferma esplicita attraverso un secondo canale (p. es. al telefono).
- Controllate regolarmente i vostri estratti conto e le registrazioni recenti, e contattate immediatamente la banca se qualcosa non torna.