«In pochi minuti al telefono mi hanno rubato 28 mila euro (che non avevo) sul conto corrente»

La storia di Bianca M. Riceve una telefonata da un hacker che si spaccia per la sua banca, risponde, le segnala un tentativo di frode. Sapeva tutto di lei, si impossessa da remoto del suo smartphone e le effettua 10 transazioni (Fonte: https://www.corriere.it/ 23 dicembre 2025)

Quel che vi stiamo per raccontare può succedere a chiunque, per questo lo facciamo con dovizia di particolari. Affinché chi ci legge possa ricavarne una morale, evitando di rispondere al telefono anche se il numero fisso che ci sta chiamando sembra essere quello della nostra banca, segnatamente Unicredit. **Perché in pochi minuti si viene raggirati, l'hacker che abbiamo dall'altro lato del filo s'impossessa del nostro smartphone a distanza e con due codici è in grado di deviarci il telefono**, entrare sul nostro conto corrente attraverso la app di mobile banking, e sempre attraverso l'app, alzarci di sei volte i massimali mensili delle nostre carte di credito effettuando decine di transazioni a nostra insaputa verso un conto Revolut, oltre a disinvestire un fondo di investimento, il tutto senza che ne abbiamo alcuna consapevolezza. **Non contento, arriva persino a frodare, in tempo reale, un'azienda, dirottando il pagamento di una fattura sul nostro conto**, con il rischio che si possa addirittura venire indagati dall'autorità giudiziaria per un supposto tentativo di truffa. Formulazione fortunatamente sventata in questa vicenda, dopo l'immediata denuncia alla polizia, ma possiamo immaginare il panico di chi è stato coinvolto.

La storia

Benvenuti nella società digitale che abbiamo costruito. Con la capacità tecnologica di cui dispongono menti raffinatissime **possiamo venire derubati in pochi minuti di 28.010 euro senza che siamo in grado di capirlo.** Racconta Bianca M., professionista della comunicazione da diverso tempo a Milano, che il 27 novembre riceve una telefonata insolita sul suo numero privato alle ore 15.15. **La cronistoria è incalzante ed è la stessa che ha fatto pochi giorni dopo al Commissariato** denunciando una truffa sofisticatissima per le modalità in cui è avvenuta.

La telefonata

«Mi chiamano da un numero fisso di Milano 02 che appare riconducibile alla mia banca, Unicredit, rispondo - spiega Bianca M. -. **Dall'altro lato una voce non automatizzata, assolutamente naturale, che si qualifica come addetto responsabile anti-frode di Unicredit**. Mi segnala in tempo reale che gli risultano tre pagamenti a mio carico sulla piattaforma eBay da Taranto, luogo in cui non sono mai stata. **Pagamenti di 980, 970, 860 euro ciascuno». In quel preciso istante le arrivano gli sms** che segnalano queste transazioni.

Il presunto blocco della carta

«Leggo che avrei autorizzato queste tre operazioni Internet con la mia carta, compaiono anche i 6 numeri iniziali della mia carta. **Se non è stata lei, le dice la voce al telefono, dobbiamo procedere al blocco immediato** della carta, spedendole una nuova al suo indirizzo di residenza. «La voce con cui sto parlando sa persino dove è la mia residenza e conosce addirittura la domanda segreta per bloccare la mia carta. **Dunque, mi fido- racconta Bianca M. -. Procediamo al blocco, nel frattempo la voce al telefono, suppostamente di Unicredit**, mi dice che sta provando a stornare i tre importi». In tempo reale le arriva un sms del supposto ufficio AntiFrode di Unicredit con richiesta storno in corso. Gli storni vengono effettuati perché le arrivano altri due messaggi poco dopo, ma bisogna attendere 24 ore per l'aggiornamento del sistema.

Il raggiro

«Dobbiamo certificare il suo dispositivo affinché sia l'unico ad accedere all'app Unicredit di home banking - le spiega la voce al telefono -. Le manderemo dei codici che dovrà leggermi» e poco dopo le arriva un primo messaggio dove c'è scritto avvio certificazione dispositivo, e altri due sms con dei codici, il cui mittente risulta essere Unicredit. **«Gli sms compaiono nello storico dei messaggi che nel tempo ho ricevuto dalla banca», spiega Bianca M.** «Gli leggo i codici, così, ho ricostruito dopo, sono in grado di entrare nel telefono o nell'app di home banking. La voce al telefono mi dice cancellare l'app e poi lunedì la reinstalliamo», le spiega, lei è ignara che la stanno truffando. **Le dicono che non può usare il conto nel week end, e che ha a disposizione solo 150 euro per le spese di cui ha bisogno**, la telefonata si chiude.

Il week end

«Nel week end non faccio praticamente operazioni fino a lunedì mattina», dice Bianca M., in quei giorni le persone provano a chiamarla ma non c'è modo di parlare con lei. Le avevano impostato l'inoltro delle chiamate a sua insaputa, al loro numero. **La sua utenza di fatto è stata deviata. Quando il lunedì 1° dicembre Bianca M. prova a pagare le sigarette la transazione** viene rifiutata perché è stato superato il limite. Così scopre il raggiro. Il numero verde di Unicredit raggiungibile solo dal suo cellulare aziendale le dice che ha speso 28.010 euro in 2 giorni. **Soldi che sul conto non ha mai avuto, perché la sua giacenza era di appena 2.600 euro.**

Le operazioni

Le hanno fatto molteplici operazioni. 4 col bancomat, per un totale di 9.660 euro, trasferimenti fatti a distanza di pochi minuti, **nel giro di due giorni tra il 27 novembre- proprio nel giorno in cui aveva ricevuto lo stipendio- e il 1dicembre. Trasferimenti su carta Revolut intestata a Dublino.** Altre 6 operazioni, nello stesso intervallo di tempo, a favore del medesimo conto Revolut, fatte con la carta di credito, per un totale di 18.350 euro. **Hanno potuto farle modificando il plafond mensile della carta, da 1.500 a 9.500 euro mensili** e, quindi, hanno usato sia il fido di novembre che quello di dicembre.

La denuncia alla polizia

«Le richieste sono state fatte attraverso l'App e accolte dalla banca il giorno stesso. Come ennesima operazione, sempre il 1° dicembre, mi hanno disinvestito anche un fondo da 694 euro. Vado subito a fare denuncia alla polizia e la direttrice di banca mi attribuisce la responsabilità di quello che è successo». **Si tratta della direttrice della filiale storica dove avevano i conti anche i suoi nonni, ad Umbertide, in provincia di Perugia, si rammarica Bianca M. scopre persino che sono in corso degli accertamenti su di lei** «perché sul mio conto hanno fatto transitare un bonifico da 5mila euro operato da un'altra società truffata» racconta - **una Srl in provincia di Milano, che ha effettuato un bonifico riversato poi sul conto Revolut in Irlanda.**

Il reclamo

«Ho fatto evidentemente reclamo alla banca, secondo la quale, tuttavia, tutte queste operazioni sarebbero considerate autorizzate dal cliente», **legge Bianca M. nella lettera di risposta immediata di Unicredit. La loro giustificazione è che il cliente ha avuto «una custodia della carta non conforme a quanto previsto dal contratto»**, grazie «alla tecnologia 3 Ds dinamico, possiamo ravvisare la diretta responsabilità della signora...» e dunque la banca si solleva da qualunque responsabilità. **Bianca M. ora è seguita da un avvocato dello Studio Legale Crosta & C., che ha già richiesto gli indirizzi Ip da cui sono state fatte le transazioni.** Ma il legale si chiede

giustamente come può una banca avallare in pochi secondi operazioni per oltre 28mila euro attraverso l'aumento dei plafond se quel correntista ha solo 2.600 euro in giacenza? Misteri.