Frode da parte di presunti dipendenti Microsoft

Oggetto: **Abuso e truffa** Numero del caso: **2022/13**

> Il cliente ha ricevuto una telefonata da presunti dipendenti Microsoft che sostenevano di voler risolvere i problemi del suo computer. Il cliente ha dato ai truffatori accesso al suo computer e poi ha fornito loro i dati della sua carta di credito per rinnovare quella ch'essi sostenevano essere una licenza Microsoft scaduta. In realtà, i truffatori si sono procurati l'accesso all'e-banking del cliente, hanno trasferito denaro dal suo conto alla sua carta di credito e successivamente hanno effettuato transazioni per ben 7'000 franchi. La banca si è rifiutata di risarcire il cliente, che ha quindi sottoposto il caso all'Ombudsman. Al termine della procedura di mediazione, la banca ha accettato di risarcire il cliente con 2'000 franchi come gesto commerciale. Il cliente ha accettato l'offerta.

Purtroppo, il metodo di frode, all'origine del presente caso, sembra essere ancora molto diffuso. I truffatori prendono di mira essenzialmente clienti di età avanzata. Facendosi passare per dipendenti Microsoft, essi contattano per telefono le persone e affermano che il loro computer ha numerosi problemi di sicurezza che devono essere risolti con urgenza. Le vittime, confidando in quanto detto loro, permettono ai malviventi di accedere al loro computer, di solito per il tramite di un programma di accesso remoto. I truffatori riescono quindi ad accedere all'e-banking del cliente e a effettuare delle transazioni in modo autonomo.

Nel caso di specie, non è stato possibile chiarire come i truffatori sono risusciti a ottenere i dati di accesso all'e-banking del cliente. La transazione fraudolenta consisteva nel trasferire del denaro sul conto della carta di credito del cliente. Dopo aver completato la transazione, i truffatori hanno indicato in modo deciso al client che la sua licenza Microsoft era scaduta e che avrebbe potuto rinnovarla per la modica somma di 12 franchi. Di conseguenza, il cliente ha fornito loro i dati della sua carta di credito. Con questi dati, i truffatori hanno effettuato transazioni per un totale di circa 7'000 franchi, che, come affermato dalla banca, il cliente ha confermato con i codici inviati al suo cellulare.

Dopo un po' di tempo, la transazione è sembrata sospetta al cliente. Egli ha spento il computer e ha telefonato alla banca. Essa ha immediatamente bloccato la sua carta di credito. Il cliente, che aveva quasi 80 anni, resosi conto del danno, si è vergognato molto per non essersi accorto prima di essere stato frodato.

Dopo aver esaminato i documenti e le relative condizioni contrattuali, l'Ombudsman ha contattato la banca. Essa si era ripetutamente rifiutata di risarcire il cliente. La banca, secondo quanto ampiamente riportato anche dalla stampa, aveva pubblicamente annunciato che avrebbe risarcito ai clienti vittime di attacchi informatici fino a un importo di 100.000 franchi. Nelle corrispondenti disposizioni relative alla sua offerta di servizi digitali, la banca prometteva di risarcire i clienti l'importo sottratto loro a seguito del furto da parte di terzi dei loro mezzi di identificazione o elementi di sicurezza, in particolare nel caso di attacchi di phishing o malware, a condizione che i clienti avessero rispettato pienamente le condizioni di partecipazione all'offerta di servizi digitali. L'Ombudsman ha chiesto alla banca di spiegare la portata di questa disposizione e il motivo per cui non intendeva risarcire il cliente nel caso in questione.

La banca considerava che non era evidente che il cliente fosse stato vittima di un reato di phishing,

poiché l’attacco era avvenuto per telefono e il cliente aveva deliberatamente e volontariamente messo a disposizione i suoi strumenti di legittimazione a terzi, nonostante egli non gli conoscesse e ch’essi non avessero alcun legame con la banca. Nelle condizioni di partecipazione, la banca rimandava a un sito web che trattava varie questioni di sicurezza e affermava, tra l’altro, che i dati personali, in particolare quelli relativi al conto, non dovevano essere trasmessi in nessun caso e che la banca non avrebbe mai contattato i propri clienti per richiedere i dati di accesso.

Secondo la banca, nel caso di specie, non era decisivo se si trattava di un caso di phishing o meno. Anche se fosse stato così, il cliente aveva violato una condizione decisiva per la promessa di indennizzo prevista dalla disposizione in questione. La promessa valeva infatti solo se le condizioni di partecipazione erano state integralmente rispettate, cosa che non era avvenuta nel caso in questione. La banca si è detta molto dispiaciuta dell’accaduto e ha dichiarato aver una grande stima per il cliente. Essa era quindi disposta a versargli 2’000 franchi come gesto commerciale.

L’Ombudsman non ha ritenuto questa argomentazione decisiva. A suo avviso, è notorio che il phishing può avvenire anche per telefono. Se il phishing per ottenere i dati relativi alla relazione bancaria o alla carta di credito va a buon fine, si tratta sempre di clienti che li trasmettono “volontariamente” a terzi non autorizzati, i quali successivamente utilizzano in modo improprio questi dati. Infatti, i truffatori fanno credere ai clienti che vi sia un motivo legittimo per trasmetterglieli e creano, talvolta in modo molto sofisticato, un contesto che lascia pensar loro che ciò lo sia effettivamente. Se le condizioni di partecipazione stabiliscono che la promessa d’indennizzo pubblicizzata non si applica nei casi in cui vi è stata trasmissione di dati, il suo ambito di applicazione appare vago.

Poiché l’Ombudsman ha ritenuto inutili ulteriori tentativi di mediazione a causa delle circostanze generali del caso, egli ha comunque presentato l’offerta di transazione al cliente fornendogli le necessarie spiegazioni. Il cliente ha deciso di accettare l’offerta della banca.