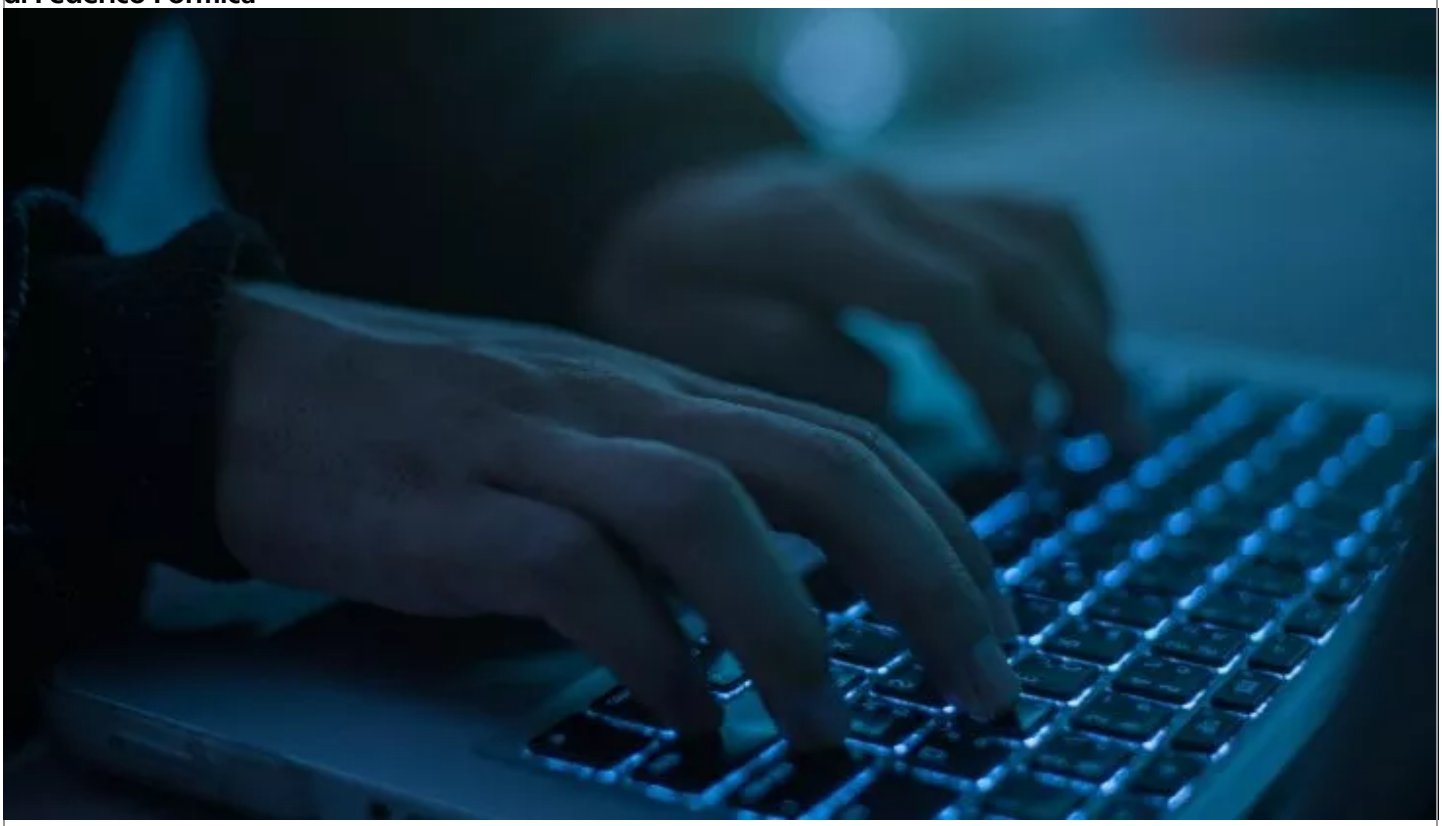
ESPERTO BANCHE E ASSICURAZIONI

Fai la tua domanda all'esperto:
esperto.banche-e-assicurazioni@repubblica.it
Leggi l'informativa

Vishing, con la "truffa al telefono" rubati 60 mila euro a un'azienda

di Federico Formica



Il caso di un una cliente di Intesa Sanpaolo. La truffa è iniziata poco dopo aver comunicato il numero allo sportello. Cherti, Abf: "La banca può fare di più per limitare i casi: abbassi i massimali". Dalla vigilanza di Bankitalia già due richieste di chiarimenti

16 FEBBRAIO 2022

4 MINUTI DI LETTURA

Una sfortunata coincidenza, oppure il segnale di un grosso problema di sicurezza. Il caso di vishing denunciato da Konsumer ha portato alla luce un fenomeno che preoccupa non solo le associazioni di consumatori ma anche la vigilanza di Bankitalia.

La vicenda riguarda un'azienda di famiglia di Roma, che a causa di una frode ha perso, dall'oggi al domani, quasi 60mila euro.

Il caso. Nei primi mesi del 2021 l'amministratrice della società è andata nella filiale della sua banca, Intesa Sanpaolo, per mandare in soffitta il vecchio token ed effettuare la procedura di autenticazione forte, prevista dalla direttiva europea Psd2; con l'occasione, l'operatore bancario fa scaricare alla cliente anche la app ufficiale per l'home banking. Solo che, anziché aumentare il livello di sicurezza bancaria, proprio da quel momento inizia il vortice.

L'amministratrice fornisce allo sportello il proprio numero di cellulare, che sarebbe servito per ricevere le password temporanee e autorizzare di volta in volta le operazioni. Insomma, quello che hanno dovuto fare tutti gli italiani dopo l'entrata in vigore della Psd2. Qui iniziano i problemi: "Pochissimi minuti dopo la signora riceve due sms, in cui come mittente appare Intesa Sanpaolo: uno con un 'codice di sicurezza', l'altro con un link per 'verificare i dati'. Poi riceve una telefonata in cui le viene chiesto di rilasciare un'intervista per la qualità del

servizio ricevuto in filiale" spiega Massimo Melpignano, legale della vittima e responsabile nazionale Banca e finanza per Konsumer. È tutto così lineare che l'imprenditrice non sospetta nulla.

Poi arrivano un altro sms e un'altra chiamata, sempre da numeri riconosciuti come quelli ufficiali, stavolta decisivi: "Il falso operatore dice alla vittima di scaricare una nuova applicazione e di cancellare quella installata in filiale. Un'operazione che, dice la voce, serve a 'metterla al riparo da frodi" continua Melpignano. La richiesta viene esaudita, la vittima installa la app e inserisce di nuovo le proprie credenziali.

Il giorno successivo, la vittima si accorge che mancano 59mila euro dal conto intestato alla società. Denaro che è stato versato, in un'unica tranche, a un conto corrente intestato a un'altra società, una srl. A quel punto scatta la denuncia alla Polizia postale e la segnalazione alla banca.

Per colpa di chi? Che però non ha alcuna intenzione di riaccreditare la cifra alla sua cliente, "vittima di una frode informatica di cui Intesa Sanpaolo non è in alcun modo responsabile, non essendo stati violati i sistemi di sicurezza della banca" spiegano a *Repubblica* dall'istituto di credito. La banca ha poi chiuso il conto della cliente, fornendole il preavviso previsto dalla legge. La tesi di Intesa - come di qualunque banca in casi simili - è semplice: il cliente ha fornito i dati al truffatore, non è stato attento e, dunque, non possiamo farci nulla.

La vittima e Melpignano sono di opinione opposta: "Il vishing è iniziato dal momento in cui la cliente ha comunicato il numero di telefono in filiale. Ci sono delle falle nei loro sistemi informatici? C'è qualcuno che dalla filiale comunica i numeri di telefono a terzi? Non vedo altre opzioni" ipotizza Melpignano, secondo il quale Intesa Sanpaolo "dice di non aver subito alcuna violazione ai sistemi, ma non ci fornisce alcuna prova. Abbiamo anche chiesto di vedere tutti i dettagli del pagamento da 59mila euro, ma anche qui nessuna risposta. In pratica, la banca ha emesso un giudizio di colpevolezza nei confronti della sua cliente e si rifiuta di mostrare le proprie carte". Melpignano spiega anche che l'azienda frodata non aveva mai effettuato pagamenti superiori ai 2/3mila euro. "Un'operazione da 60mila euro avrebbe dovuto quantomeno mettere in allarme la banca, far partire immediatamente una segnalazione all'ufficio antifrodi dell'istituto. Ma non è successo nulla di tutto questo".

Una falla, o è solo casualità? Il caso dell'imprenditrice non è isolato. Anzi. "Questa vicenda non mi sorprende: molti dei casi di vishing che arrivano alla nostra attenzione riguardano clienti di Intesa Sanpaolo" spiega Stefano Cherti, membro del collegio di Roma dell'Arbitro bancario finanziario e responsabile economico per Unione nazionale consumatori. "La banca - continua Cherti - dovrebbe ascoltare di più le associazioni di consumatori, perché se è vero che l'istituto ha molti clienti, ed è quindi più esposto, è vero anche che gli strumenti per risolvere i problemi ci sono. Uno su tutti: sensibilizzare i clienti ad abbassare al minimo i massimali per le operazioni via internet, perché i loro clienti sono oggi molto esposti a questi rischi".

Alcuni addetti ai lavori spiegano che la vigilanza di Bankitalia ha già inviato almeno due comunicazioni a Intesa Sanpaolo. Il tono delle missive era: considerato l'alto numero di casi di vishing, fate le opportune verifiche ai vostri sistemi informatici. C'è chi sostiene che la banca possa aver subito un furto massivo di dati, che poi vengono utilizzati per fare vishing.

"Spesso il vishing comporta delle operazioni sproporzionate rispetto alla storia del cliente. Le banche hanno tutti gli strumenti per far scattare allarmi in caso di operazioni sospette. Sono anni che imploriamo gli istituti a bloccare, nel dubbio, ogni pagamento di questo tipo" conclude l'esperto di Unc.

Intesa Sanpaolo non ha risposto alle nostre domande sul caso dell'imprenditrice "per motivi di riservatezza", ma neanche a domande di carattere più generale (ad esempio, avremmo voluto sapere quali sono i massimali applicati di default ai propri clienti per l'home banking) né ha confermato di aver ricevuto richieste di chiarimenti da Bankitalia ma ha fatto sapere di aver condotto, e di condurre, diverse campagne informative alla clientela "invitando a non fornire in alcuna circostanza informazioni o dati personali che potrebbero essere utilizzati in modo fraudolento" e che l'istituto non chiede mai dati già in suo possesso, "richieste di questo tipo sono sempre riconducibili ad azioni fraudolente".

Il gruppo, scrive ancora la banca, "supporta le principali istituzioni italiane e internazionali nel contrastare questo fenomeno anche attraverso il rafforzamento del quadro regolamentare e collabora costantemente con le forze dell'ordine per contribuire a ridurre e a mitigare gli impatti di questi reati". Ma serve la collaborazione di tutti: "I clienti stessi, custodendo con cura i propri codici e

prestando attenzione agli alert via sms; le banche, continuando a investire in sicurezza e prevenzione; gli operatori telefonici, verificando scrupolosamente l'identità dei clienti che chiedono un cambio sim e bloccando la manipolazione dei numeri mittenti di telefonate e sms; le istituzioni nazionali e comunitarie, semplificando la legislazione in materia e consentendo la velocizzazione dei tempi di reazione delle forze dell'ordine".

Nel frattempo il caso potrebbe presto finire sul tavolo dell'Abf. Che, in passato, in casi simili ha già dato alcune volte ragione al cliente.