

La telefonata della finta banca che svuota il conto corrente, la truffa online

Codici carpiri con il trucco dei falsi bonifici. A una delle vittime spariti 59mila euro

Come non fidarsi se la telefonata arriva dal numero del servizio clienti della tua banca? Sono decine le persone che si sono fidate (e purtroppo continuano a fidarsi) salvo ritrovarsi con il conto corrente prosciugato. Una nuova truffa online sta facendo strage dei risparmi degli italiani grazie alla incredibile possibilità di «copiare» impunemente i numeri di telefono.

Come ha denunciato alla Polizia una 55 enne di Milano assistita dall'avvocato Marcello Pistilli, la disavventura comincia con un sms, cioè con un'azione di phishing, il lancio di un «amo» digitale al quale c'è sempre qualcuno che abbocca, nonostante le banche invitino costantemente a non rispondere a sms e a email che chiedono di digitare le proprie credenziali.

Il messaggio, solitamente molto allarmante e altrettanto verosimile, nella vicenda della signora milanese sembra arrivare dall' Ufficio frodi della sua banca che, «in seguito a tentativi di accesso anomali», la invita a «confermare» i suoi dati collegandosi ad un determinato link.

Il numero di partenza del messaggio telefonico è esattamente quello del servizio clienti che la donna ha memorizzato sul cellulare sotto il nome della banca. Poco dopo, da quello stesso numero arriva una telefonata in cui una persona che si qualifica «come un operatore dell'ufficio antifrode», dichiara la vittima, chiede se è stata lei a fare una certa operazione e, dato che ovviamente non c'è stata alcuna operazione, si fa avanti per aiutarla chiedendole di confermare i messaggi che di lì a poco le arriveranno, probabilmente per carpirle i codici di autorizzazione delle operazioni. Qualche minuto dopo, sempre la stessa persona la invita ad andare immediatamente in un ufficio della banca per «riprogrammare» il conto. Guarda caso, però, quel giorno è un sabato e le banche sono chiuse. Ma la soluzione c'è: sarà l'operatore a mettere tutto a posto, basta che la cliente segua al telefono le sue istruzioni, che di solito vuol dire dare ancora i propri i codici.

Passano due giorni e la manfrina si ripete. Stavolta, però, il solito operatore gentile e premuroso, sempre dallo stesso numero, la invita a «stornare» un bonifico fraudolento di 16.900 euro che gli hacker che si erano impossessati del suo conto stavano per far partire, così come avverrà il giorno dopo, quando «mi riferiva — dichiara la vittima in questura — che ero di nuovo sotto attacco» e le fa «annullare» un bonifico da 19.100 euro, e il giorno dopo ancora, per altri 23.500 euro. Sembra tutto finito, ma i guai cominciano quando, trascorsa una settimana, la signora dà un'occhiata alle operazioni del suo conto corrente e si accorge che sono spariti 59.500 euro proprio con i tre bonifici fraudolenti che pensava fossero stati bloccati. Chiama il famoso numero del servizio clienti, al quale le rispondono invitandola ad andare in filiale per verificare cosa stesse succedendo, ma lì altro non possono fare che dirle di presentare una denuncia.

Ci sono moltissime storie come questa in tutta Italia fatte con i numeri di telefono delle banche. Com'è possibile? Un investigatore spiega che i truffatori usano servizi voip, la telefonia via internet, forniti da operatori che hanno sede in paesi stranieri nei quali la magistratura non può arrivare perché mancano convenzioni di assistenza giudiziaria con l'Italia. Questi operatori permettono ai loro clienti senza scrupoli di usare come proprio numero «chiamante» un qualsiasi numero telefonico, senza preoccuparsi se è usato e da chi. C'è poi da capire come fanno i truffatori ad essere in possesso dei numeri dei clienti.

Giuseppe Guastella

Corriere della Sera

16 Febbraio 2021