La frode della Sim: a Sassari rubati 55mila euro con un sms. Gli esperti: ecco come difendersi

Data: Invalid Date | Autore: Redazione

SASSARI 14 SETT - Ancora un altro caso di frode telematica ai danni di un uomo di Sassari che si è visto prelevare dal conto 55mila euro semplicemente aprendo un sms in arrivo. Per fortuna questa volta gli agenti della Squadra Mobile della Questura di Sassari sono riusciti ad identificare e denunciare per truffa un 44enne e un 47enne, entrambi napoletani con precedenti di polizia. La vittima, però, non è ancora riuscita a recuperare per intero la somma sottratta.

Ma come funziona questa truffa?

«Una volta individuata la vittima- spiega Francesco Faenzi, direttore della Business Unit della Digital Trust di Soft Strategy- l'hacker procede all'acquisizione dei suoi dati e delle credenziali di accesso al servizio di home banking tramite la clonazione della scheda telefonica. In poco tempo l'utente riscontra il blackout della propria linea a seguito dell'annullamento della funzionalità. Dall'altra parte l'hacker, una volta sostituita la sim card della vittima, è in grado di avere accesso al conto e utilizzarlo per tutte le funzioni consentite. E questo anche perché il numero di telefono è quasi sempre utilizzato come secondo fattore nel processo di autenticazione in due fasi, specialmente ora che le banche stanno abbandonando il vecchio sistema delle chiavette dispositive».

«Il fenomeno "sim swap fraud" è iniziato negli Stati Uniti e già dal 2015 si è avuta notizia dei primi

casi in Italia - spiega Alessandro Rossetti, della Business Unit Digital Trust di Soft Strategy -. Un tipo di reato che si sta verificando sempre più spesso anche nel nostro Paese. Ricordo in particolare una frode informatica ai danni di una banca on line ai cui clienti, residenti in varie parti d'Italia, erano stati sottratti 300 mila euro. La raccolta illecita di dati personali e password può essere fatta in molti modi- prosegue Rossetti – a partire dal cosiddetto “web scraping” dei social network. Si raccoglie una grandissima quantità di dati personali pubblici tramite la diffusione di software malevolo negli store dei vari produttori di telefoni o tramite reti WiFi libere preparate ad hoc».

Rossetti raccomanda di prestare sempre particolare attenzione a ciò che decidiamo di diffondere online e di installare sui nostri smartphone, esaminandone attentamente le condizioni d’uso, i dati ai quali si presta il consenso ad accedere e le relative licenze d’uso. Se anche gli operatori telefonici cercano di tutelarsi nei confronti di queste truffe, a volte questi sforzi non bastano. «L’operatore telefonico deve certamente avere un protocollo rigoroso sulla consegna di copie delle schede già rilasciate ai propri clienti - avverte ancora Rossetti -. La richiesta di un documento d'identità, però, non basta. Soprattutto se si può disporre di un rivenditore telefonico che sia complice dei truffatori».

Per intervenire concretamente sul rischio Francesco Faenzi ritiene che « la conferma dell'identità dovrebbe passare attraverso sistemi più incisivi come l’utilizzo dei dati biometrici o di token fisici. Si raccomanda inoltre di curare particolarmente la sicurezza delle proprie password conservandole mediante l’utilizzo di appositi password manager o dispositivi di sicurezza a due fattori come le chiavi di sicurezza hardware. E nel caso in cui il telefono non riesca a connettersi per più di pochi minuti... contattare immediatamente la propria banca».

Claudia Tamiro