CYBERSECURUTY, LE NUOVE TRUFFE ONLINE: CONTI SVUOTATI A CAUSA DI UNA SCHEDA TELEFONICA

Sim swap fraud, le frodi di scambio di Sim card sono in aumento, gli esperti avvertono: "Non fidatevi delle reti wi-fi libere"

La lista delle truffe nel mondo "cyber risk" si aggiorna quotidianamente introducendo terminologie e configurazioni giuridiche sconosciute ai più. Truffe sempre più complicate da prevedere, ma non impossibili da contrastare per potersi difendere anche se effettuate con mezzi digitali di uso comune. Sta affinando tecniche sempre più argute la "sim swap" legata alla clonazione delle sim telefoniche che permettono ai truffatori di svuotare i conti in banca di ignari cittadini che si trovano improvvisamente in rosso. Come funziona? Presto fatto: una volta individuata la vittima 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. Negli ultimi mesi si stanno moltiplicando in maniera esponenziale i casi riscontrati dalla Polizia Postale che lancia l'allerta.

«Il fenomeno "*sim swap fraud*" è arrivato in Europa con una prima configurazione nel 2015 e si è gradatamente strutturato arrivando oggi ad assumere dimensioni preoccupanti- spiega Alessandro Rossetti, della Business Unit Digital Trust di Soft Strategy-. Non siamo ancora in possesso di dati precisi, ma ogni anno si ha notizia di un numero sempre crescente di questo tipo di frodi».

Rossetti chiarisce che, nella generalità dei casi, in un primo momento il criminale si procura i dati personali e le coordinate bancarie della vittima. Successivamente ha bisogno di ottenere una copia della scheda perché ha bisogno di superare l'autenticazione a due fattori utilizzata da molti enti finanziari nelle operazioni di home banking. Questi ultimi, infatti, in genere inviano un sms al telefono del cliente con il codice autorizzativo dell'operazione dispositiva che deve essere eseguita. «*L'operatore telefonico deve certamente avere un protocollo rigoroso sulla consegna di copie delle schede già rilasciate ai propri clienti*- avverte Rossetti-. *Ma purtroppo spesso i criminali utilizzano tecniche di ingegneria sociale, attacchi informatici o acquisti effettuati nel Dark Web per aggirare ogni misura di sicurezza ed avere accesso ai dati personali della vittima*».

Come riesce un hacker a rubare l'identità? «*Con molti diversi metodi*- afferma Francesco Faenzi, Direttore della Business Unit Digital Trust di Soft Strategy- *a partire dal cosiddetto "phishing", la più classica delle truffe online, o tramite la diffusione di un software malevolo tramite gli store dei vari produttori di telefoni, o ancora tramite reti wi-fi libere preparate ad hoc e collocate in punti strategici, come la lobby di un hotel o un bar particolarmente grande. Queste applicazioni, una volta installate, riescono ad estrarre dallo smartphone tutte le informazioni utili e spedirle su server appositamente predisposti*».

Come proteggersi: prestare sempre particolare attenzione a cosa si decide di installare sui propri dispositivi, esaminandone attentamente le condizioni d'uso, i dati ai quali si presta il consenso ad accedere e le relative licenze d'uso. «*Bisogna avere una certa cautela nell'utilizzare connessioni wi-fi aperte*- raccomanda Faenzi- *ed evitare di importare password troppo semplici od ovvie, anche se*- ammette- *sono misure che possono solo mitigare il rischio di essere compromessi*». Per intervenire concretamente sul rischio Faenzi ritiene che la conferma dell'identità dovrebbe passare attraverso sistemi più incisivi come l'utilizzo dei dati biometrici o di token fisici. 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.