Polizia di Stato

La Polizia di Stato recupera 300mila euro sottratti dai conti correnti di ignari correntisti attraverso lo smishing

Sono numerosissimi i clienti di istituti di credito con operatività in home banking vittime di transazioni fraudolente, movimentate attraverso sofisticate tecniche di smishing; da dicembre ad oggi sono state moltissime le denunce ricevute dalla Polizia Postale da parte di cittadini che sono stati colpiti da questo fenomeno, per un importo complessivo di quasi 500.000 euro frodati. Il fenomeno, in continua evoluzione, si realizza generalmente in due passaggi. L'utente riceve un messaggio SMS, apparentemente inviato dalla propria Banca, contenente avvisi di movimentazioni sospette o problemi di accesso al servizio dell'home banking e viene invitato a cliccare su un link che rinvia, in realtà, ad un sito clone dell'istituto bancario, tramite il quale viene indotto a inserire le proprie credenziali (username, password, numero di telefono cellulare, nonché codice fiscale e indirizzo di posta elettronica). A tal fine, i criminali contattano telefonicamente o via SMS le vittime utilizzando un numero di telefono che viene rilevato dagli apparati cellulari come riferibile a quello della Banca (i sistemi operativi degli apparati cellulari individuano il solo mittente inserito dai truffatori e non il numero utilizzato); tale circostanza induce gli utenti a ritenere di essere in contatto con veri funzionari degli istituti di credito. Vengono, quindi, impartite disposizione ai clienti finalizzate a far rimuovere l'applicazione di accesso alle proprie posizioni di home banking che viene subito dopo reinstallata dai truffatori che prendono così il completo controllo dei conti correnti. Recentemente, si è verificata un'ulteriore evoluzione del fenomeno criminale che consiste nel movimentare le somme presenti nei conti correnti colpiti attraverso l'esecuzione di bollettini postali online. Questa modalità, a differenza dei bonifici bancari, presenta il vantaggio per i criminali di poter movimentare somme di denaro anche ingenti con operazioni non revocabili dall'utente. La destinazione di tali somme verso capitoli finanziari "speciali" sono state oggetto di specifiche indagini da parte degli inquirenti che hanno permesso di bloccare (e recuperare tempestivamente) in molte occasioni i flussi di denaro sottratti. Sono i casi di diversi utenti che, dopo essere stati contattati via SMS sulla rispettiva utenza telefonica e aver disinstallato, su invito dei truffatori, la APP della propria Banca, hanno subito la sottrazione di 43.000 euro, diretti, attraverso l'emissione di bollettini postali, su un conto postale sul quale risultavano giacenti più di 126.000 euro, provenienti da altre operazioni illecite. Le indagini, condotte dalla Polizia Postale di Bologna e coordinate dal Servizio Polizia Postale e delle Comunicazioni di Roma, sotto la direzione della Procura della Repubblica di Bologna, hanno consentito di bloccare il flusso di denaro e verificare che erano presenti rimesse sospette riconducibili ad analoghe truffe ai danni di numerosi correntisti residenti a Torino, Brescia, Milano, Teramo e Cagliari, che avevano subito lo svuotamento del proprio conto corrente per somme oscillanti tra i 10 ed i 50.000 euro. Molte delle vittime, turbate per l'accaduto, e nel timore di incorrere in altri episodi criminali non rispondevano alle chiamate alla loro utenza, neanche agli Operatori della Polizia Postale che volevano informarli che gli era stato recuperato il denaro sottratto. Per lo sviluppo delle indagini nei casi descritti è risultata indispensabile la collaborazione di diverse strutture di Poste Italiane S.p.A che hanno collaborato alle analisi finanziarie e alle procedure di restituzione delle somme alle vittime. ALCUNE SEMPLICI INFORMAZIONI PER NON CADERE IN ERRORE :

E' bene ricordare che le Banche non inviano MAI email, sms o chiamano al telefono per chiedere di fornire le credenziali di accesso all'home banking o all'app, i dati delle carte di credito o la variazione dei dati personali.

Se ricevi email, sms o telefonate che ti chiedono di fornire dati bancari, chiama immediatamente la Tua Banca e rivolgiti alla Polizia Postale:

- non aprire gli allegati o i link contenuti nelle e-mail o sms;

- tieni sempre aggiornato l'antivirus e il Sistema Operativo.

Per approfondimenti e segnalazioni su eventuali casi sospetti vai su: www.commissariatodips.it