Giornale del Piemonte [II]

PAESE :Italia
PAGINE :15
SUPERFICIE :24 %

AUTORE :N.D.

► 31 luglio 2019

TRA LE PRIME VITTIME ITALIANE UN IMPRENDITORE DI ALASSIO

La truffa della sim che svuota il conto

L'allarme degli esperti: i malviventi clonano la tessera del telefono

Si parte per le vacanze. Si chiude la porta a doppia mandata per evitare che i ladri entrino in casa. Eppure, molto spesso, la chiave che i delinquenti usano per arrivare ai nostri soldi è proprio nelle nostre tasche. Si tratta dello smartphone, strumento irrinunciabile anche quando siamo in vacanza. Può capitare mentre proviamo a caricare l'ultimo selfie fatto in spiaggia o a telefonare ai parenti rimasti in città. Il cellulare, improvvisamente, si scollega da internet e non ci consente di fare chiamate. Subito immaginiamo che il problema sia dovuto all'operatore telefonico, invece la situazione potrebbe essere molto più grave.Si chiamano «Sim Swap Fraud» e se il nome può sembrare ostico, la situazione è molto più chiara se pensiamo ad un imprenditore che, ad Alassio, sul mar Ligure, lo scorso ottobre, si è visto sottrarre 20 mila euro dal conto corrente dalla sera alla mattina, proprio a causa di questo tipo di truffa. «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».Ma come funziona questa truffa? 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. E questo anche perché «il numero di telefono è quasi sempre utilizzato come secondo fattore nel processo di autenticazione in due fasi – aggiunge Francesco Faenzi, direttore della Business Unit della Digital Trust di Soft Strategy - specialmente ora che le banche stanno abbandonando il vecchio sistema delle chiavette dispositive». «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». Come è puntualmente accaduto nel caso dell'imprenditore di Alassio.

Giornale del Piemonte [II]

PAESE : Italia
PAGINE : 15
SUPERFICIE : 24 %

AUTORE : N.D.

► **31 luglio 2019**

SIM CARD Lo smartphone è applicato anche nelle transazioni economiche