ACCIUFFA LA TRUFFA

Un progetto delle associazioni consumatori ed utenti lombarde
CODICI, CASA DEL CONSUMATORE, ASSOUTENTI, CODACONS
Segnalazioni sul sito www. acciuffatruffe.com

ARTICOLO 6 - MARZO 2021 – "SIM SWAP: ACCIUFFA LA TRUFFA CHE TI SVUOTA IL CONTO CORRENTE"

Non tutti sanno che il reato di "phishing" molto spesso viene utilizzato come "cavallo di troia" per consentire la realizzazione di un'altra truffa quella dello c.d. "SIM SWAP".

Lo schema del Simswap funziona in questo modo: i criminali dapprima agiscono sottraendo le credenziali di accesso ai sistemi di *home banking*, attraverso attività di *phishing* e successivamente richiedono una nuova Sim card a nome della vittima e l'annullamento di quella in uso di chi deve essere raggirato per mantenere lo stesso numero.

I criminali in questione acquisiscono così il controllo del vostro numero cellulare riuscendo ad ingannare il gestore telefonico con una falsa identificazione attraverso il c.d. *Social Engineering* ovverouna tecnica che consiste nel"curiosare" nei vari profili *social media* della vittima in modo da raccogliere tutte le informazioni utili (data di nascita, città di residenza, nome dei familiari, nome dell'animale domestico, etc.) per poter effettuare il furto d'identità.

La duplicazione della SIM-card può essere conseguita molto semplicemente:il truffatore si rivolge al vostro gestore telefonico spacciandosi per voi con una scusa, ad esempio "ho perso la mia SIM-card". I gestori controllano l'identità dei loro clienti ma per assicurare al cliente semplicità nell'utilizzo del servizio mantengono un basso livello di controllo.

Infatti, gli Help Desk dei gestori telefonici controllano l'identità della persona in base alle risposte ad alcune domande personali mentre solo in negozio occorre mostrare la carta d'identità per richiedere una nuova SIM-card.

Così ottenuto il duplicato della SIM i criminali informatici sono in grado di ricevere gli sms con il codice OTP "One time password" inviati dalla banca al numero di cellulare ormai in pieno possesso dei truffatori.

Dopo qualche ora l'ignara vittima riceve una notifica sull'applicazione della propria Banca, relativa all'accesso sulla propria home banking, accorgendosi di lì a poco che senza alcuna autorizzazione, sono stati illecitamente impartiti ordini di bonifici a perfetti sconosciuti.

Successivamente le carte di pagamento e la *home banking* vengono bloccate a seguito del disconoscimento delle suddette operazioni. Spesso gli istituti di credito ritenendo la frode realizzata al di fuori degli ambiti controllati e controllabili dai propri sistemi di sicurezza, purtroppo, ri-addebitano le somme che, in un primo momento, avevano anticipato "salvo buon fine".

Nella truffa denominata "SIM SWAP" il ruolo della SIM è fondamentale. Infatti, è noto che tutti i sistemi di accesso a mezzo autenticazione tra cui Facebook, Instagram, Linkedin, fino a G-Mail

utilizzano il cellulare come sistema di verifica dell'identità del soggetto. Ciò vuol dire, che se si dimentica la password si può richiedere il recupero o il reset della password: Facebook ad esempio, invia un SMS con le istruzioni per il recupero o il reset. Nella truffa SIM Swap queste informazioni arrivano solo sulla SIM duplicata e non su quella della vittima che ormai è disconnessa dalla rete e quindi non riceverà più alcun avviso.

Questo allarmante scenario evidenzia gravi responsabilità a carico del **gestore telefonico,** che spesso con troppa facilità fornisce un duplicato della SIM, senza accertarsi della vera identità del soggetto richiedente (attraverso, per esempio, i dati di accesso e di login, un documento di identità oppure semplicemente copia della formale denuncia ai Carabinieri di smarrimento del cellulare); ma anche della **Banca,** che per censire un nuovo dispositivo non effettua alcun controllo antifrode: molto spesso sarebbe sufficiente usare le funzioni di geo-localizzazione e fare un *profiling* del tipo di operazioni svolte per accorgersi che i bonifici disposti con buona probabilità non erano "legittimi".

E' importante sapere che qualora l'utente neghi di aver autorizzato un'operazione di pagamento, l'onere di provare la genuinità della transazione ricade sul prestatore del servizio. E' dunque la Banca a dover provare di aver assicurato tutte le misure idonee a garantire la sicurezza dell'operazione via *home banking*, garantendo la sicurezza dei pagamenti on-line.

Per prevenire il furto di identità creditizia può essere utile attivare un servizio di verifica delle operazioni finanziarie fatte con il nostro nome nonché chiedere di ricevere avvisi relativi alle operazioni di conto corrente, anche tramite app ed email non solo, quindi, con sms cellulare.

E' tuttavia possibile cercare di non incappare in questa nuova truffa prestando attenzione ad alcuni segnali. Il telefono potrebbe smettere di funzionare, ovvero perdere inaspettatamente il segnale in maniera tale da non rendere possibile l'invio e/o la ricezione di SMS o chiamate.

Potresti essere chiamato da un presunto operatore telefonico che ti informa che ci potrebbero essere dei problemi di linea sul tuo smartphone rassicurandoti sulla temporaneità del disservizio, oppure potresti ricevere un SMS con la stessa informazione.

L'unico modo per mettersi realmente al riparo da questa tipologia di truffe è non utilizzare il numero di telefono cellulare per ricevere i codici di accesso o i codici dispositivi della banca. Dal luglio 2019, infatti, tutti gli istituti di credito europei si sono adeguati alla nuova direttiva europea PSD2 che prevede che l'accesso alle app di mobile banking o alle piattaforme di home banking, così come le operazioni dispositive, possano avvenire solo in seguito all'inserimento di un secondo codice, complementare alla password scelta dall'utente.

Dott. Davide Zanon

Segretario Regionale CODICI Lombardia

Progetto realizzato nell'ambito del Programma generale di intervento della Regione Lombardia con l'utilizzo dei fondi del Ministero dello sviluppo economico. Ripartizione 2018