Le più comuni truffe online

1. In questa newsletter analizziamo le truffe più frequenti in cui possono imbattersi i consumatori che fanno *shopping online*

2. La frode informatica più classica è il *phishing*, che letteralmente significa "pescare". La tecnica consiste nel carpire dati personali importanti, soprattutto password di *home banking* e strumenti di pagamento, attraverso l'invio di e-mail false da parte di truffatori. I messaggi così spediti spesso recano il logo contraffatto dell'istituto di credito e invitano a fornire le credenziali bancarie personali motivando la richiesta con ragioni di tipo tecnico

3. Cosa fare se si è vittima di *phishing*? Non bisogna rispondere a queste e-mail, né aprire eventuali allegati, ma provvedere a cestinarle quanto prima

4. Come varianti del *phishing* esistono poi il *vishing* (voice phishing) e lo *smishing* (sms phishing). Si tratta di truffe nelle quali si cerca di carpire informazioni sulle credenziali bancarie attraverso, rispettivamente, una telefonata o un sms. Ovviamente anche in questi casi non bisogna rispondere in alcun modo alla comunicazione ed eliminare i messaggi fraudolenti quanto prima

5. Altra truffa diffusa è quella del *man in the middle* (letteralmente 'uomo nel mezzo'). Per mettere in atto questa frode, il malintenzionato intercetta le comunicazioni in rete che avvengono tra il cliente (ossia la vittima, il cittadino che esegue una transazione importante) e il server (per esempio, il server dell' istituto bancario). Mettendosi "nel mezzo" tra il cliente e il server della banca, l'*hacker* è in grado di carpire tutti i dati che vengono trasmessi, anche le credenziali bancarie. Ciò avviene quando il punto WiFi non è cifrato e la connessione non è privata, ossia, quando sulla barra degli indirizzi non compare il lucchetto e c'è la scritta "http", invece di "https"

6. Altro tipo di truffa è il *sim swapping*, una frode che colpisce la SIM del telefono e viola i sistemi di comunicazione su cui si basano alcuni servizi online, anche bancari. Oggetto di questa truffa sono i sistemi di autenticazione a doppia chiave (autenticazione forte), per i quali è necessaria sia la password personale che l'OTP (One Time Password), in genere veicolata attraverso un sms. Nella pratica, l'hacker riesce a introdursi nella SIM della persona che sta effettuando la transazione, in modo da intercettare il messaggio contenente l'OTP (il secondo fattore di autenticazione)

7. Come avviene il *sim swapping*? Il malintenzionato può trasferire il numero di telefono della vittima comunicando al gestore la volontà di assegnare il numero a un'altra SIM. Questa operazione, in sé legittima e anche piuttosto semplice dato che non è necessario presentare un documento di identità per inoltrare la richiesta, viene portata avanti in modo fraudolento, a volte anche con la complicità di chi lavora negli store del gestore

8. Come accorgersi che è avvenuto un *sim swapping* e come evitarlo? Dal fatto che il nostro telefono viene isolato e non è più in grado di comunicare con il *network* dell'operatore telefonico. In pratica "non ha campo". Se la situazione permane, occorre mettersi urgentemente in contatto con l'operatore per far presente il problema. Il suggerimento per evitare il *sim swapping*, è quello di scegliere altre vie per ottenere il secondo fattore di autenticazione: per esempio l'app o l'e-mail. Per cercare di prevenire le truffe, poi, è sempre opportuno avere sui propri dispositivi dei buoni software antivirus sempre aggiornati. Allo stesso modo, è utile evitare di connettersi a reti WiFi pubbliche (cioè quelle presenti in negozi, bar, aeroporti, ecc.), preferire la rete domestica e accertarsi sempre, quando si opera in rete, che ci siano il lucchetto e la scrittura "https" sulla barra dell'indirizzo internet del nostro intermediario bancario/finanziario

TEIC Transazioni Elettroniche Insicurezza&Consapevolezza

Realizzato/acquistato nell'ambito del Programma generale denominato Regione Lazio per il cittadino consumatore - VI, con i fondi del Ministero dello Sviluppo Economico - Ripartizione 2018

ADUSBEF

MOVIMENTO DIFESA DEL Cittadino LAZIO