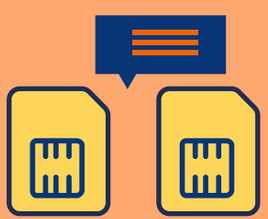
SIM SWAPPING – UNA TRUFFA AL CELLULARE

Il SIM swapping - o scambio di SIM - avviene quando un truffatore, usando tecniche di social engineering, prende il controllo della tua SIM usando i tuoi dati personali rubati.

COME FUNZIONA?

Un truffatore ottiene i dati personali della vittima per es. tramite: violazione dei dati, phishing, ricerche sui social media, app maligne, shopping online, malware, etc.

Con queste informazioni, il truffatore inganna l'operatore della rete mobile trasferendo il numero della vittima ad una SIM in suo possesso.



Il truffatore può ora ricevere le chiamate entranti ed i messaggi di testo, incluso l'accesso al banking online della vittima.

La vittima noterà che la rete non funziona, e infine scoprirà che non può collegarsi all'utenza della banca.

COSA PUOI FARE?

- Tieni il tuo software aggiornato, inclusi il browser, l'antivirus e il sistema operativo.
- Tieni l'informazione riservata e stai attento con i social media.
- Non aprire mai link sospetti o allegati ricevuti tramite email o messaggi di testo.
- Non rispondere alle email sospette e non impegolarti in conversazioni in cui vengono chiesti i tuoi dati personali.
- Aggiorna le tue password regolarmente.
- Acquista da fonti affidabili. Controlla il punteggio di ogni singolo venditore.
- Scarica le app solo da fornitori ufficiali e leggi sempre i loro permessi.
- Quando possibile, non associare il numero di telefono a utenze online sensibili.
- Inserisci un PIN per restringere l'accesso alla tua SIM card. Non condividere il PIN con nessuno.
- Controlla frequentemente il tuo estratto conto.

SEI UNA VITTIMA?

- Se il tuo cellulare perde la ricezione senza motivo, segnalalo immediatamente al tuo operatore mobile.
- Se il tuo operatore conferma che la tua SIM è stata scambiata, segnalalo alla polizia.

EUROPOL EC3 European Cybercrime Centre | EBF European Banking Federation | enisa European Union Agency for Cybersecurity | European Cyber Security Month

#CyberScams