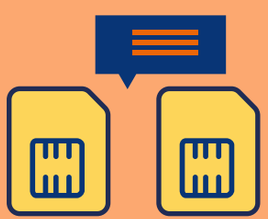
SIM SWAP - LA TRUFFA DEL CELLULARE

Il SIM swap avviene quando un frodatore, attraverso tecniche di social engineering, prende il controllo della tua SIM usando i dati personali che ti ha rubato.

COME FUNZIONA?

Il truffatore ottiene i dati personali della vittima ad esempio grazie a data breach, ricerche sui social, app fraudolente, shopping online, malware, etc.

Con le informazioni ottenute, il frodatore raggira l'operatore telefonico e lo convince a trasferire il numero telefonico della vittima su una SIM in suo possesso.



Il frodatore può ora ricevere telefonate e sms, inclusi i codici di accesso all'online banking della vittima.

il telefono ha perso il segnale, e potrebbe anche accorgersi di non poter più accedere al proprio conto online.

CHE COSA PUOI FARE?

- Tieni sempre aggiornati i software sul tuo smartphone, inclusi il browser, l'antivirus e il sistema operativo.
- Limita e fai attenzione alle informazioni che condividi sui social media.
- Non aprire mai link o documenti sospetti che ricevi via email o messaggio.
- Non ripondere a email sospette e non dare confidenza a chi ti chiama al telefono per chiederti informazioni personali.
- Aggiorna regolarmente le tue password.
- Scarica app solo dai fornitori ufficiali e leggi sempre le autorizzazioni richieste dall'app.
- Quando possibile, non collegare il tuo numero di telefono a profili online che contengono dati sensibili.
- Personalizza il PIN per limitare l'accesso alla tua SIM.
- Controlla spesso i movimenti sul tuo conto.

SEI UNA VITTIMA?

- Se il tuo cellulare perde il segnale senza motivo, segnalalo subito al tuo gestore telefonico.
- Se il tuo gestore telefonico conferma il SIM swap, denuncia alla Polizia.

EUROPOL EC3 European Cybercrime Centre

EBF European Banking Federation

#CyberScams