



SIM SWAP – LA TRUFFA CHE SVUOTA IL CONTO

Se la SIM del tuo smartphone ha improvvisamente smesso di funzionare forse potresti essere vittima di una truffa informatica.

FASE 1



Utilizzando mail di phishing, raccogliendo informazioni personali attraverso i social, agendo con tecniche di persuasione o di social engineering, il malintenzionato riesce a sottrarre le credenziali di accesso all'home banking della vittima. Ma non basta...

FASE 2



Raccolte le informazioni necessarie per il furto d'identità, il criminale può ora contattare il fornitore di telefonia mobile e, denunciando lo smarrimento della SIM, richiedere una nuova SIM e l'annullamento della vecchia... ovviamente mantenendo lo stesso numero di telefono.

FASE 3



Quando l'ignara vittima scopre di non avere più alcuna connessione, il criminale sta già ricevendo chiamate e messaggi sulla nuova SIM, tra cui anche la nuova password e i codici di sicurezza necessari per tutte le operazioni che richiedono un'autorizzazione, come quelle per muovere denaro.

COME PROTEGGERSI

- **Mantieni aggiornati** tutti i tuoi software, compresi i browser, gli antivirus e i sistemi operativi
- Fai **attenzione alle informazioni personali** che condividi sui social
- **Non cliccare mai su URL o allegati sospetti** o provenienti da fonti sconosciute
- Quando possibile, **non associare il tuo numero di telefono ad account che accedono a dati sensibili**