

Truffa del SIM swapping: Guida Pratica per Difendersi

LETTURA: 7 MINUTI | TARGET: TUTTI I POSSESSORI DI SMARTPHONE E CONTI CORRENTI ONLINE | FONTE: NOTIZIARIO.NET



Immagine generata con Intelligenza Artificiale (Nano Banana Pro / Gemini) - Trasparenza AI Act (Regolamento UE 2024/1689) (Fonte: NOTIZIARIO.NET)

S SINTESI DELLA NOTIZIA

Il SIM swapping è una delle frodi digitali più pericolose del momento. I malintenzionati riescono a prendere il controllo del numero di telefono per svuotare i conti correnti bancari.

R REGOLE D'ORO E SICUREZZA

- Non condividere mai dati personali o il tuo numero di telefono su siti web poco affidabili o social network.
- Richiedi al tuo operatore telefonico di impostare una password o un PIN segreto per qualsiasi modifica alla SIM.
- Usa applicazioni di autenticazione (es. Google Authenticator) anziché gli SMS per i codici OTP.
- Controlla regolarmente l'estratto conto bancario per individuare tempestivamente eventuali transazioni anomale.

P COSA C'E DA SAPERE IN SINTESI

- Il SIM swapping avviene quando i truffatori clonano il tuo numero di telefono su una nuova SIM.
- La perdita improvvisa del segnale di rete è il primo campanello d'allarme da verificare subito.
- Abbandona gli SMS per l'autenticazione a due fattori e usa app di autenticazione sicure.

C IL CONSIGLIO DELLA REDAZIONE

La sicurezza digitale parte dalla consapevolezza: non sottovalutare mai i piccoli segnali di anomalie sul tuo smartphone e adotta subito l'autenticazione forte.