Allerta smishing: come riconoscere ed evitare le truffe SMS bancarie

LETTURA: 6 MINUTI | TARGET: CONSUMATORI E CORRENTISTI | FONTE: NOTIZIARIO.NET



Immagine generata con supporto AI - Trasparenza Reg. UE 2024/1689 (Fonte: NOTIZIARIO.NET)

S SINTESI DELLA NOTIZIA

Le truffe SMS bancarie sono un fenomeno in costante espansione in Italia. Scopri come funziona lo smishing, quali sono i rischi dello spoofing e come difendere i tuoi risparmi da attacchi informatici avanzati.

R REGOLE D'ORO E SICUREZZA

- Non cliccare su link sospetti contenuti nei messaggi di testo.
- Verificare qualsiasi notifica contattando il numero verde della banca.
- Non comunicare mai a terzi le password temporanee OTP ricevute sullo smartphone.
- Attivare gli alert di spesa e le notifiche push dall'app dell'istituto bancario.

P COSA C'E DA SAPERE IN SINTESI

- Le banche non chiedono mai inserimento di credenziali o PIN tramite link inviati via SMS.
- Il Sender ID Spoofing consente ai truffatori di posizionare i messaggi falsi all'interno delle chat SMS bancarie autentiche.
- In caso di truffa subita occorre tempestivamente bloccare il conto, cambiare le credenziali e sporgere denuncia.

C IL CONSIGLIO DELLA REDAZIONE

Non agire mai d'impulso di fronte a SMS che segnalano anomalie urgenti: prenditi un minuto, ignora il link e chiama direttamente la tua filiale bancaria per verificare la situazione.