

Phishing bancario via WhatsApp: i passi immediati da compiere se si è cliccato un link sospetto

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

Il fenomeno del phishing bancario veicolato tramite l'applicazione WhatsApp rappresenta una minaccia costante per i correntisti italiani. In questa guida analizziamo nel dettaglio la dinamica della truffa e le azioni tempestive da intraprendere per mettere al sicuro il proprio conto corrente ed evitare ingenti perdite finanziarie.

R REGOLE D'ORO E SICUREZZA

- Non cliccare mai su link ricevuti via WhatsApp o SMS da numeri sconosciuti o da mittenti che simulano la banca.
- Attivare l'autenticazione a due fattori (2FA) e le notifiche push per ogni operazione sul conto.
- Ricordare che gli istituti bancari non chiedono mai password, PIN o codici OTP tramite chat o telefono.

P COSA C'E DA SAPERE IN SINTESI

- Bloccare immediatamente carte e credenziali bancarie contattando il servizio clienti della propria banca.
- Sporgere formale denuncia alla Polizia Postale e scansionare il dispositivo per rimuovere eventuali malware.
- Richiedere il rimborso delle transazioni disconosciute richiamando le tutele previste dalla normativa europea PSD2.

C IL CONSIGLIO DELLA REDAZIONE

In presenza di messaggi sospetti, non agire mai d'impulso: interrompi la comunicazione e verifica la situazione contattando direttamente la tua filiale bancaria tramite i canali ufficiali.