Truffa del finto operatore bancario: come riconoscerla e difendersi

LETTURA: 5 MINUTI | TARGET: CONSUMATORI E CORRENTISTI | 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

Negli ultimi mesi si registra un forte aumento degli attacchi informatici condotti da un finto operatore bancario. Ecco la dinamica della truffa, come proteggere il conto corrente e le azioni immediate da intraprendere per evitare perdite finanziarie.

R REGOLE D'ORO E SICUREZZA

- Non comunicare mai i codici OTP, PIN o credenziali d'accesso via telefono o messaggistica.
- Riagganciare immediatamente la telefonata e ricontattare la banca usando il numero presente sulla carta.
- Non cliccare mai sui link ricevuti via SMS che segnalano blocchi anomali del conto corrente.
- Attivare le notifiche in tempo reale e l'autenticazione a due fattori per tutte le transazioni bancarie.

P COSA C'E DA SAPERE IN SINTESI

- Le banche non richiedono mai codici personali OTP o password tramite chiamate telefoniche o messaggi SMS.
- Il Caller ID Spoofing consente ai truffatori di far apparire il numero reale della banca sul display del telefono della vittima.
- In caso di frode, occorre bloccare subito il conto, sporgere denuncia alle forze dell'ordine e chiedere il rimborso alla banca.

C IL CONSIGLIO DELLA REDAZIONE

In caso di telefonate d'emergenza dal tuo istituto bancario, mantieni la calma e riaggancia. Chiama personalmente il servizio clienti ufficiale usando solo i recapiti stampati sul retro della tua carta di pagamento.