Falsi SMS Bancari e Smishing: Come Riconoscere le Truffe e Tutelarsi

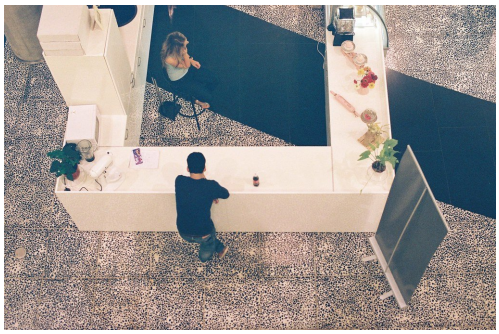

Foto di Tanel Teemusk (flickr) - NOTIZIARIO.NET

S SINTESI DELLA NOTIZIA

Aumentano i tentativi di truffa via SMS che simulano comunicazioni urgenti da parte degli istituti di credito. Scopri come identificare i messaggi malevoli, proteggere i tuoi dati personali e quali passi compiere per ottenere un eventuale rimborso.

R REGOLE D'ORO E SICUREZZA

- Non cliccare mai sui link contenuti in SMS di alert bancari.
- Verificare ogni comunicazione contattando direttamente il numero verde ufficiale.
- Nessun istituto chiede mai PIN o credenziali via telefono o messaggio.
- Attivare le notifiche push dall'app bancaria per monitorare ogni movimento.

P COSA C'E DA SAPERE IN SINTESI

- Le banche non inviano mai link via SMS per sbloccare conti o richiedere credenziali.
- In caso di errore, occorre bloccare subito le carte e contattare l'assistenza ufficiale.
- Il correntista ha diritto al rimborso se non si configura un'ipotesi di colpa grave.

C IL CONSIGLIO DELLA REDAZIONE

Salva nella rubrica dello smartphone il numero verde della tua banca presente sul retro della carta di credito e non rispondere mai a telefonate o messaggi ricevuti da numeri differenti.