

# Truffe via SMS: Come Riconoscere lo Smishing e Proteggere i Propri Risparmi

LETTURA: 4 MINUTI | TARGET: CONSUMATORI E TITOLARI DI CONTO CORRENTE | FONTE: NOTIZIARIO.NET



Foto di Insights Unspoken (flickr) - NOTIZIARIO.NET

## S SINTESI DELLA NOTIZIA

L'allarme smishing continua a crescere in Italia, con SMS civetta che simulano comunicazioni bancarie o di corrieri espressi per rubare dati personali e bancari. Scopri le strategie chiave per individuare i messaggi trappola e difenderti efficacemente.

## R REGOLE D'ORO E SICUREZZA

- Non cliccare mai su collegamenti web presenti in SMS non sollecitati
- Verificare l'indirizzo URL prima di inserire credenziali riservate
- Contattare l'assistenza clienti tramite i canali ufficiali e non usando i numeri forniti nel testo dell'SMS
- Attivare le notifiche push dall'app della banca per monitorare ogni movimento finanziario

## P COSA C'E DA SAPERE IN SINTESI

- Banche ed enti ufficiali non richiedono mai credenziali di accesso o codice PIN tramite SMS.
- I link ingannevoli utilizzano la tecnica dello spoofing per apparire nella medesima chat dei messaggi autentici.
- In caso di truffa è indispensabile bloccare subito le carte di pagamento e sporgere denuncia alle autorità.

## C IL CONSIGLIO DELLA REDAZIONE

Verifica sempre la presenza di filtri anti-spam nelle impostazioni dell'app Messaggi del tuo smartphone ed evita di memorizzare password finanziarie nel browser.