

# Smishing: cos'è e come difendersi

Lo smishing è una forma di phishing tramite sms o messaggi su app e social, che mira a rubare dati personali e bancari inducendo le vittime a cliccare link, scaricare file o rispondere con informazioni sensibili. Spesso i messaggi sfruttano toni intimidatori o fanno leva su inesistenti situazioni di urgenza per ingannare l'utente.

Come agiscono i truffatori:

invitando a cliccare su link o file allegati contenenti malware.

Chiedendo di inviare dati personali (PIN, codici OTP, ecc.).

Invitando a chiamare numeri falsi dove operatori fittizi estorcono informazioni.

Perché è pericoloso:

fa leva sulla paura e fretta della vittima.

Usa messaggi credibili, spesso imitando aspetti delle comunicazioni istituzionali di banche, enti pubblici o fornitori di servizi.

Consigli del Garante della privacy per proteggersi

Non condividere dati sensibili via SMS/messaggistica.

Non cliccare su link o allegati sospetti.

Verificare la credibilità del mittente (errori nel testo, numeri strani, ecc.).

Controllare periodicamente i movimenti bancari e attivare notifiche di sicurezza.

In caso di sospetto, contattare subito la banca o il gestore della carta attraverso canali ufficiali.

In caso di frode, segnalare alle competenti autorità di polizia.