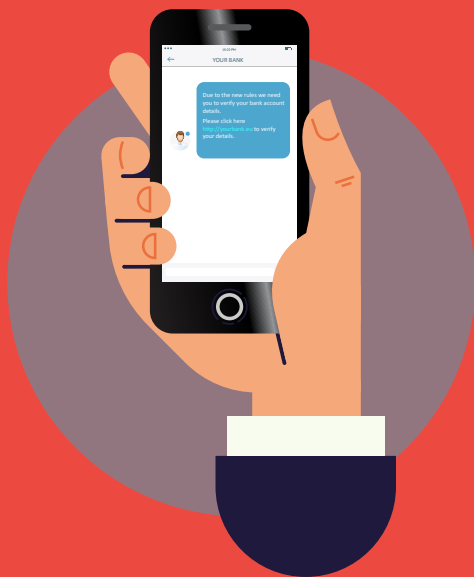


# PHISHING PRIN SMS

Smishing (combinație de cuvinte dintre SMS și Phishing) este încercarea de inducere în eroare prin mesaje text, pentru obținerea de date personale, bancare ori de securitate.



## CUM FUNCȚIONEAZĂ?

Prin mesajul text (SMS), autorii, de obicei, îți solicită să apelezi un număr de telefon sau să accesezi un link prin care "îți verifici, actualizezi, reactivezi" contul. Dar...în realitate ești direcționat către un site fals sau un operator-complice, pretins reprezentant al băncii.

## CE POȚI FACE?

- **Nu accesa link-uri, atașamente sau imagini nesolicitate**, primite prin SMS de la persoane necunoscute.
- **Nu acționa în grabă**. Ia-ți timp și verifică informațiile înainte de a trimite un eventual răspuns.
- **Niciodată nu răspunde unui SMS** prin care ți se solicită codul PIN, parole de acces la contul de online banking ori alte credențiale de siguranță.
- **Contactează imediat banca**, dacă știi că ai răspuns unui astfel de mesaj și ai furnizat detalii bancare în aceste condiții.