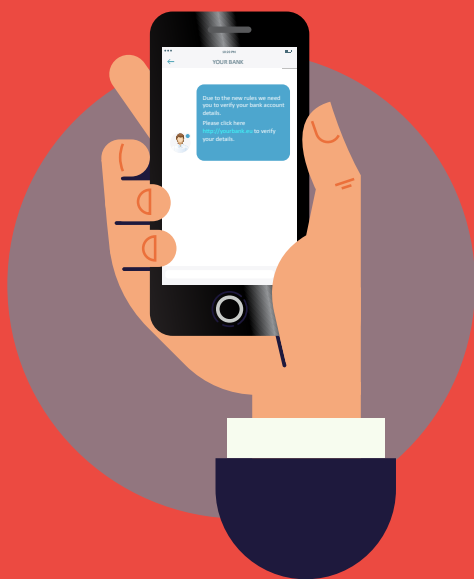


# SMS DI PHISHING BANCARIO

Lo smishing (dalla combinazione delle parole SMS e Phishing) è il tentativo da parte dei truffatori di acquisire informazioni personali, finanziarie o di sicurezza tramite SMS.



## COME FUNZIONA?

L'SMS ti chiederà in genere di fare clic su un link o di chiamare un numero di telefono per 'verificare', 'aggiornare' o 'riattivare' il tuo account. Ma... il link porta ad un sito web fasullo e il numero di telefono porta ad un truffatore che finge di essere la società legittima.

## COSA PUOI FARE?

- **Non cliccare su link, allegati o immagini** che ricevi da SMS indesiderati, senza prima verificare il mittente.
- **Non essere frettoloso.** Prenditi il tuo tempo e fai dei controlli appropriati prima di rispondere.
- **Non rispondere mai ad un SMS** che richiede il tuo PIN o la password del tuo conto online o qualsiasi altra credenziale di sicurezza.
- Se pensi che ci sia la possibilità che tu abbia risposto ad un testo smishing e fornito i tuoi dati bancari, **contatta immediatamente la tua banca.**