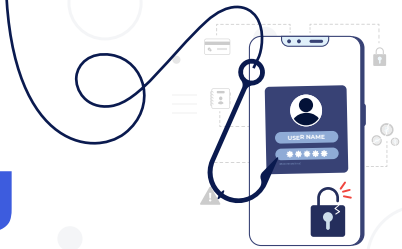

Smishing

Lo **smishing** è una truffa via SMS in cui gli aggressori si spacciano per rappresentanti di enti legittimi, cercando di convincerti a fornire informazioni sensibili come password, PIN e dati personali.

#1

MANTIENI LA CALMA E NON CEDERE ALLA FRETTA
Chiediti: è una truffa?

#2

NON CONDIVIDERE MAI INFORMAZIONI SENSIBILI VIA SMS
Le organizzazioni legittime non ti chiederanno mai password, PIN o altre informazioni riservate tramite SMS. Se ricevi un messaggio del genere, ignora e cancella.

#3

VERIFICA SEMPRE L'IDENTITÀ DEL MITTENTE
Se qualcosa ti sembra strano, cerca di contattare direttamente l'organizzazione tramite un numero ufficiale o il loro sito web. I truffatori possono falsificare i numeri di telefono per far sembrare che il messaggio provenga da una fonte affidabile.

#4

DIFFIDA DI MESSAGGI CHE RICHIEDONO AZIONI IMMEDIATE
Le richieste urgenti di pagamento o informazioni personali sono spesso segnali di una truffa. Le organizzazioni legittime non ti metteranno pressione per agire immediatamente.

Se hai ancora dubbi, **contatta direttamente la tua filiale** o il contact center al numero **800.755.866**.

CYBER -confusi-

Banco Desio