La truffa dei fondi da salvare

Come funziona?

1

Ricevi un **SMS**, apparentemente proveniente dalla Banca, con un link che rimanda **a un sito simile** all'internet banking originale e utilizzato dal malintenzionato per rubare le tue credenziali bancarie e ulteriori dati personali.

2

Il truffatore ti contatta per telefono, **fingendosi un operatore antifrode della Banca e/o della Polizia Postale** per acquisire la tua fiducia. Ti allerta circa **false «operazioni fraudolente momentaneamente bloccate»** sul tuo conto corrente.

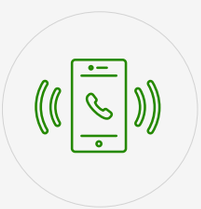
3

A questo punto, il truffatore cerca di convincerti a **recarti «con urgenza» in filiale** al fine di **«mettere in sicurezza»** i tuoi fondi, eseguendo da sportello operazioni di pagamento (tipicamente bonifici istantanei) verso un nuovo conto corrente appena aperto a tuo nome.

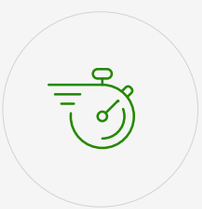
4

Se, convinto, vai in filiale, il truffatore ti persuade per telefono a eseguire un **bonifico** verso un **nuovo IBAN fraudolento**, da lui fornito. Convinto quindi di «mettere in sicurezza i tuoi risparmi», **li trasferisci invece nel suo conto**.

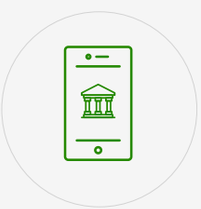
Impara a conoscere i segnali e a difenderti



Diffida da comunicazioni contenenti link o numeri di telefono sconosciuti



Presta attenzione a richieste urgenti



Chiudi la telefonata e contatta direttamente la Banca o una persona fidata per farti aiutare

INTESA SANPAOLO