

Promemoria per una maggior sicurezza:

- Attivo, se disponibile, la notifica via SMS o app per ogni operazione
- Non condivido mai OTP, PIN o password.
- Non faccio operazioni bancarie quando uso reti Wi-Fi pubbliche o non protette
- Chiamo la banca solo ai numeri ufficiali.
- Non clicco link sospetti.
- Parlo con un familiare prima di fare operazioni importanti.



La prudenza è il tuo scudo migliore. Non condividere mai codici o password e verifica sempre chi ti scrive o ti chiama.



Imparare a difendersi è facile
se sai come fare...

Più digitali. Più liberi. Più protetti.



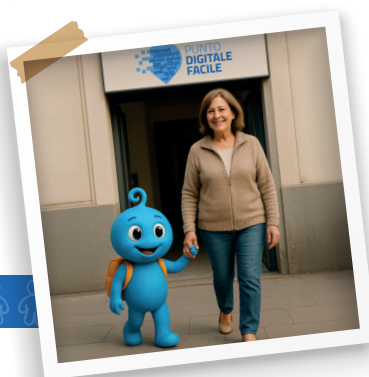
Per qualsiasi dubbio,
non esitare...

... vieni in un **Punto Digitale Facile** o contatta
una delle **Associazioni dei Consumatori**



Il progetto Digitalmentis è un'iniziativa per le competenze digitali finanziata dal Fondo MIMIT per i consumatori - DM 31/07/2024. In Piemonte è realizzato in collaborazione con le Associazioni dei Consumatori presenti sul territorio riconosciute dalla Regione Piemonte*, ed è correlato con la Misura 1.7.2 - "Rete di servizi di Facilitazione Digitale" del P.N.R.R."

 www.regione.piemonte.it/web/comunicazione/digitalmentis-piemonte



*Inquadra il QR code e scopri le associazioni dei consumatori che collaborano al progetto



Come difendersi dalle Frodi informatiche bancarie

Come riconoscerle e come evitarle,
passo dopo passo



Più digitali. Più liberi. Più protetti.

www.regione.piemonte.it/web/comunicazione/digitalmentis-piemonte

Cos'è una frode informatica bancaria informatica

Una truffa pensata per farti trasferire soldi o rivelare codici: può arrivare via SMS, email, telefono o tramite una pagina web falsa.

esempi comuni:

- **sms** che avvisano di "blocchi" o "problemi" e invitano a cliccare un link.
- **email** che sembrano dalla tua banca ma chiedono dati.
- **telefonate** da falsi "operatori" che chiedono codice OTP o password.



Le 4 regole d'oro per difenderti

1. Non condividere mai codici o password.

Nessuna banca seria ti chiede l'OTP, il PIN o la password al telefono o via email.

2. Verifica sempre il mittente.

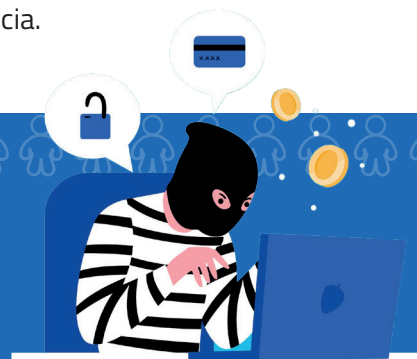
Se un messaggio ti sembra strano, non cliccare: chiama il numero ufficiale della tua banca.

3. Non aprire link sospetti.

Se ricevi un link, passa dal sito ufficiale della banca digitando l'indirizzo o usa l'app che usi sempre.

4. Fai controllare dai tuoi cari o dal Punto Digitale Facile.

Parlarne riduce il rischio: mostra il messaggio a una persona di fiducia.



Cosa fare se pensi di essere stato truffato

- ✓ Riattacca/chiudi la pagina e **non cliccare altro**.
- ✓ **chiama subito la tua banca** usando il numero sul retro della carta o sul sito ufficiale.
- ✓ **blocca la carta** e segnala le transazioni sospette.
- ✓ Segnala la truffa alla **polizia postale**, oppure vieni al **punto digitale facile** che ti aiuta a effettuare la segnalazione.

Se ti hanno chiesto un **codice OTP***, dillo subito alla banca: potrebbe essere l'ultima azione necessaria per bloccare il danno.