

COMANDO STAZIONE CARABINIERI DI ARDESIO

Avviso pubblico a tutela della cittadinanza

ATTENZIONE ALLE TRUFFE!

PROTEGGI IL TUO DENARO E I TUOI DATI

I tentativi di truffa telefonica, tramite SMS o e-mail (Phishing) sono in continuo aumento. I malfattori si spacciano spesso per operatori della tua banca, delle Poste o persino per Forze dell'Ordine, usando toni urgenti o allarmanti per intimidirti e indurti in errore.

LA BANCA E LE FORZE DELL'ORDINE NON CHIEDONO MAI:

- I tuoi **codici di accesso** all'Home Banking (password, username o codici di sblocco).
- Il **PIN** del bancomat, della carta di credito o della carta postale.
- I **codici OTP** che ricevi via SMS o tramite App per autorizzare i pagamenti.
- I tuoi dati personali o copie dei documenti d'identità per telefono o tramite link.

COME DIFENDERSI E PREVENIRE:

1. **NON FORNIRE MAI DATI BANCARI O POSTALI:** Nessun istituto di credito ti chiederà mai queste informazioni per "sbloccare" un conto o verificare un pagamento sospetto a voce o via messaggio.
2. **NON CLICCARRE SUI LINK:** Se ricevi un SMS che afferma che il tuo conto è sospeso o bloccato, non aprire il link allegato. Accedi sempre ed esclusivamente dall'applicazione ufficiale della tua banca.
3. **NON TI FIDARE DEL NUMERO SUL DISPLAY:** I truffatori utilizzano tecniche digitali avanzate (spoofing) per camuffare il proprio numero di telefono, facendolo apparire come quello reale della banca o di una caserma.
4. **PRENDITI IL TUO TEMPO:** I ladri giocano sull'effetto sorpresa, sulla fretta e sulla paura. Se qualcuno ti mette pressione per compiere operazioni immediate, mantieni la calma e **attacca il telefono**.

IN CASO DI DUBBIO O SOSPETTO:

Sospendi immediatamente la conversazione. Chiama il numero ufficiale della tua banca (scritto sul retro della tessera) oppure contatta direttamente la Stazione Carabinieri o il **Numero Unico di Emergenza 112**.

La prevenzione è la tua miglior difesa. Condividi questo avviso con familiari, vicini di casa e persone anziane.