

TRUFFE SUL CELLULARE

Guida pratica per riconoscerle, evitarle e sapere cosa fare

FERMATI • VERIFICA • NON CONDIVIDERE CODICI

Se una richiesta arriva all'improvviso e ti mette fretta, prenditi un momento prima di agire.

1. La dinamica delle truffe

☐ TRUFFA SU WHATSAPP

Come funziona: arriva un messaggio, spesso camuffato da invito a votare per un concorso oppure da richiesta di aiuto proveniente da un contatto già in rubrica. Il messaggio invita a cliccare su un link e a inserire un codice ricevuto via SMS.

Cosa succede: il codice può consentire ai truffatori di prendere il controllo dell'account WhatsApp. Successivamente possono contattare amici e familiari della vittima per chiedere denaro.

Segnale d'allarme: richiesta improvvisa di cliccare su un link e, soprattutto, di comunicare o inserire un codice ricevuto via SMS.

☎ TRUFFA TELEFONICA — SPOOFING

Come funziona: i truffatori possono usare tecnologie che fanno apparire sul display un numero telefonico reale, ad esempio associato a una banca, alle forze dell'ordine o ad altra autorità.

Cosa dicono: sostengono che sia in corso un'indagine o che ci sia un problema sulla filiale bancaria e chiedono con urgenza un bonifico verso un presunto «conto sicuro», oppure credenziali e codici OTP.

Segnale d'allarme: pressione, urgenza, richiesta di denaro o di codici riservati.

2. Le regole d'oro e i consigli di sicurezza

1

☐ Non condividere mai dati sensibili

Nessun istituto di credito, forza dell'ordine o autorità chiederà di effettuare bonifici verso conti sconosciuti, trasferire denaro oppure comunicare password, codici OTP e credenziali di accesso.

2

☐ Verifica le richieste insolite

Se un contatto conosciuto chiede un pagamento urgente via messaggio, fermati e contatta direttamente la persona con un canale già conosciuto, per verificare che la richiesta sia autentica.

3

☐ Non dare seguito a richieste sospette

Non effettuare pagamenti o trasferimenti e non inviare codici ricevuti via SMS in risposta a telefonate o messaggi sospetti. In caso di dubbio, interrompi la conversazione e verifica autonomamente.

Mini-checklist: prima di cliccare o pagare

- ☐ Mi stanno mettendo fretta?
- ☐ Mi chiedono un codice ricevuto via SMS?
- ☐ Mi chiedono password, credenziali o OTP?
- ☐ Mi chiedono un bonifico verso un «conto sicuro»?
- ☐ Posso verificare la richiesta chiamando direttamente la persona o l'ente tramite un recapito già noto?

3. Come chiedere aiuto

1. Contatta la Polizia Postale oppure, in caso di emergenza, chiama il Numero Unico di Emergenza 112.
2. Conserva le prove: fai screenshot dei messaggi e annota il numero di telefono sospetto.
3. Puoi inoltre rivolgerti al supporto delle associazioni dei consumatori.

RICORDA

Una richiesta urgente non è una prova di autenticità. Fermati, verifica con un canale indipendente e non condividere codici o credenziali.