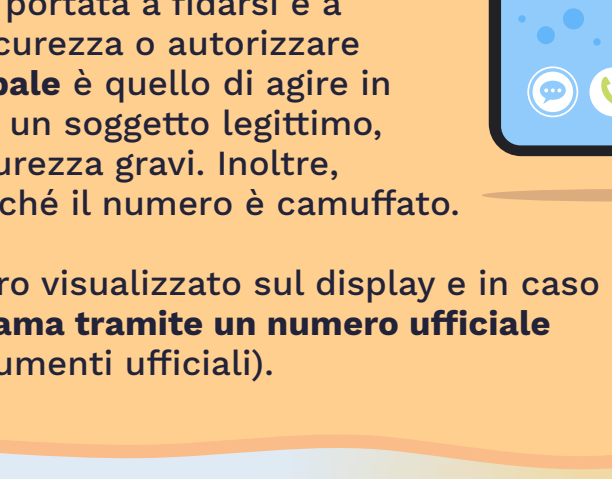


Esploriamo come possono avvenire, fornendo
r navigare online in sicurezza.

[illegible]

ing: attenzione al numero falsificato



Le truffe possono avere diverse forme.

Trovi di seguito le tipologie più comuni di truffa e alcuni



 La truffa dell'urgenza familiare (Family Emergency Scam):
quando la paura prende il sopravvento.

chiamano la vittima e si fingono in difficoltà o si spacciano per fittizi, costoro che di solito ci sono un tuo

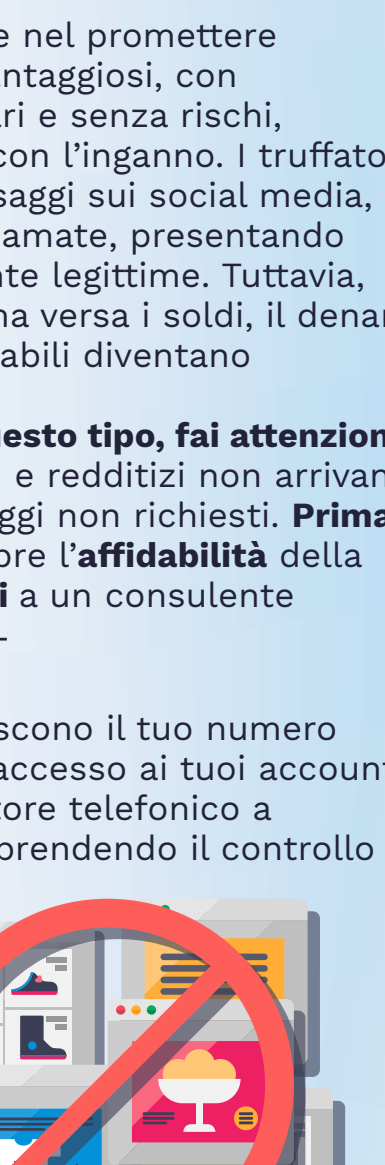
ioni sensibili. **Per evitare** di cadere in questa trappola, è
ntale non **cedere alla pressione emotiva e valutare con r**
la validità dei contenuti riportati dal manipolatore.



pagamento

**La truffa del falso investimento
(Fake Investment Scam):
il miraggio dei guadagni facili**

malintenzionati, che usano le informazioni che pubblici per personalizzare i loro attacchi.



oni sensibili, come dati
ziali personali.
esso fingendosi
ziende affidabili,
piere azioni contro il

emergency scam o il job scam (proporti offerte di lavoro fasulle per ottenere dati personali o denaro).

Il phishing è una truffa informatica che mira a ottenere dati sensibili, come password o informazioni bancarie, fingendosi un'entità affidabile tramite e-mail, messaggi o siti web fraudolenti.

Messaggi, email e chiamate sospette:
riconoscere phishing, smishing
e vishing su ogni canale -

 Mittenti sconosciuti: i truffatori spesso utilizzano numeri di

 Messaggi allarmistici: questi messaggi solitamente minacciano la chiusura di un account o richiedono azioni immediate per risolvere un problema falso

Richieste di informazioni personali: i truffatori chiedono spesso di condividere dati sensibili come password, OTP o informazioni finanziarie

URL inizia con https non significa che il sito sia legittimo, significa solo che c'è una connessione sicura. In caso di dubbi, verifica l'affidabilità del sito tramite recensioni online o app specifiche. Anche app come WhatsApp possono segnalare automaticamente i link sospetti. Meglio evitare di cliccare se

anziché tramite mezzi tracciabili come bonifici bancari o carte di credito. Tra i metodi preferiti figurano il prelievo di contanti, l'effettuazione di acquisti che non lasciano tracce evidenti, trasferimenti di denaro o bonifici verso conti terzi, dai quali è poi possibile prelevare fondi, effettuare ulteriori acquisti o

Ignora e blocca: non rispondere ai messaggi sospetti e **blocca immediatamente** i contatti sconosciuti

Non cliccare link non verificati:

correzioni per vulnerabilità note o informazioni bancarie tramite WhatsApp

alcune semplici regole da seguire:

- ✓ **non condividere mai** informazioni personali o finanziarie tramite SMS, e-mail

con cura le credenziali di accesso ai conti online e i codici delle carte di pagamento

sollecitano ad azioni immediate che comportano esborso di denaro e generano sensazioni di pericolo crescente, **diffida** di presunti operatori bancari che al telefono presentano come “amici” e segnalano situazioni di pericolo di familiari o conoscenti. **Verifica** sempre personalmente la situazione senza dar corso a

verifica i motivi contattando il tuo operatore telefonico.

Cosa fare se sei vittima di truffa o frode

Se sei stato vittima di un tentativo di phishing o rilevi attività sospette

Se l'interlocuzione con l'istituto finanziario non ti soddisfa, puoi inoltrare un reclamo allo stesso che deve rispondere nel termine di 15 giorni lavorativi.

Vuoi saperne di più?
Scopri di più sulla sicurezza online visitando il sito

Informazioni utili per affrontare le minacce informatiche in modo consapevole, proteggendo i tuoi dati e le tue transazioni.

