



Posteitaliane
Area Territoriale Tutela
Aziendale Nord Ovest



REGIONE LIGURIA



COMUNE DI GENOVA



BANCA D'ITALIA



Difendersi dalle frodi

Guida pratica per riconoscere e prevenire truffe e frodi online

Le truffe più comuni

Riconosci i pericoli comuni e come avviene il furto dell'identità digitale.

Blocco del pagamento

La vittima riceve la segnalazione di un presunto blocco su un pagamento o su un conto corrente bancario. I truffatori, fingendosi operatori del servizio clienti o operatori di banca, inviano messaggi, sms, email, o chiamano le vittime per chiedere dati personali o finanziari con l'obiettivo di ripristinare il corretto funzionamento del sistema.

Attenzione! Se hai dubbi, contatta direttamente la tua banca tramite i numeri ufficiali.

Falso investimento o proposte di lavoro fasulle

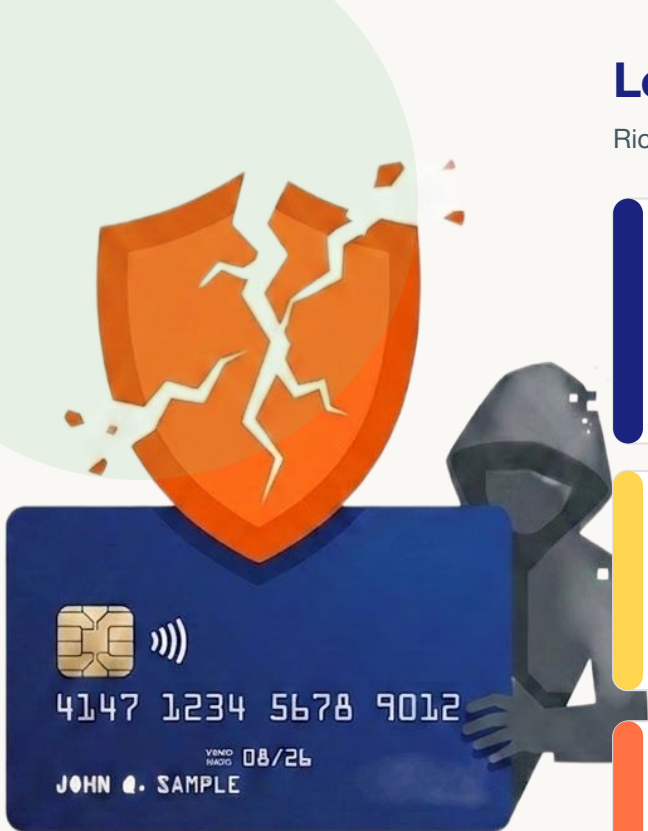
La truffa consiste nel promettere investimenti molto vantaggiosi, con rendimenti straordinari e senza rischi, attirando la vittima con l'inganno. Tuttavia, una volta effettuata l'operazione, il denaro scompare e i responsabili diventano irraggiungibili.

Diffida dai guadagni facili. Verifica sempre l'affidabilità della fonte.

Urgenza familiare

I truffatori fingono di voler aiutare un parente della vittima che versa in una situazione di pericolo. Sfruttando il panico del momento, chiedono di inviare urgentemente del denaro.

In questi casi, interrompi la chiamata e contatta il familiare!



Le richieste più comuni



Il bonifico

I truffatori, fingendosi appartenenti alle Forze dell'Ordine o operatori bancari, chiedono di effettuare dei bonifici istantanei o ordinari verso IBAN che vengono forniti alle vittime per tutelare i risparmi da frodi o indagini.

Attenzione! Se hai dubbi, contatta direttamente la tua banca tramite i numeri ufficiali.



Autorizzazione di un pagamento

La vittima riceve un SMS con il quale viene comunicata l'avvenuta autorizzazione di un pagamento su un conto corrente, bonifico o carta di credito. Il messaggio contiene poi la seguente dicitura: "Se non ha effettuato lei l'operazione, contatti il numero di telefono X per disconoscerla".

Diffida della comunicazione! Contatta direttamente la tua banca tramite i numeri ufficiali.

Quali sono gli strumenti di cui si avvale il truffatore?

Smishing

Tipo di phishing che usa SMS per invitare a cliccare su link malevoli, fingendo di essere una fonte affidabile come la banca.

Spoofing

Tecnica informatica che consente di falsificare l'identità del chiamante facendola apparire come un'utenza riconducibile a enti pubblici o Forze dell'Ordine.



Phishing

Truffa che mira ad ingannare gli utenti via email per ottenere informazioni sensibili come dati bancari, codici di accesso o credenziali personali, imitando comunicazioni ufficiali.

Vishing

Truffa telefonica vocale in cui i criminali si fingono operatori di banca, enti pubblici o aziende affidabili per ottenere informazioni sensibili e indurre a compiere azioni contro l'interesse della vittima.

SIM Swap: Il meccanismo

I truffatori ottengono, dal tuo operatore telefonico, una **nuova SIM**, disattivando la tua, per prendere il controllo del numero di telefono e dei codici di sicurezza inviati via SMS, così da poter accedere al tuo account bancario.

Segnali di allerta: come riconoscerli



Mittenti sconosciuti e link sospetti

Diffida da numeri sconosciuti e URL alterati. **Controlla l'URL:** "https" non garantisce l'affidabilità.



Linguaggio e tono

Errori grammaticali e toni eccessivamente urgenti o allarmistici sono segnali tipici di frode.



Richieste dati sensibili

Nessuna banca chiede **Password o OTP** via messaggio. Non condividere mai dati personali.



Pagamenti non tracciabili

I truffatori prediligono **canali non convenzionali**: criptovalute, ricariche, carte regalo o bonifici a terzi per evitare la tracciabilità.

Come fare per proteggersi?

Semplici regole da seguire per navigare in sicurezza online.



Dati personali

Non condividere mai info tramite SMS, email o chiamate vocali.



Password forti

Usa password uniche e attiva l'autenticazione a due fattori (2FA).



App e antivirus

Mantieni i dispositivi aggiornati e usa software antivirus affidabili.



Monitoraggio

Controlla regolarmente i movimenti bancari e segnala attività sospette.



Proteggi i tuoi dati

Evita di condividere documenti sensibili o info bancarie tramite WhatsApp e altri social.



Non cliccare link non verificati

Verifica sempre l'autenticità di un link prima di aprirlo per evitare furti di dati.



Attenzione all'Urgenza: Diffida da chi sollecita pagamenti immediati o segnala pericoli.

Cosa fare se sei vittima di truffa o frode

Azioni immediate

Se rilevi attività sospette, agisci subito: contatta la tua banca per bloccare carte e operatività online. Denuncia l'accaduto alle Forze dell'Ordine tramite il Numero Unico di Emergenza 112.

Controlla i movimenti bancari e, in caso di addebiti non autorizzati, comunica il disconoscimento richiedendo il rimborso.

Gestione del reclamo

Se l'interlocuzione con la banca non ti soddisfa, inoltra un reclamo formale. L'istituto ha l'obbligo di rispondere entro 15 giorni lavorativi.

In caso di mancato accoglimento o risposta non convincente, puoi procedere con ulteriori step di tutela istituzionale.

Tutela e ricorsi

È possibile presentare un esposto alla **Banca d'Italia** o ricorrere all'**Arbitro Bancario e Finanziario** se la risposta al reclamo non è soddisfacente.



Ricorda: la tua banca e le Forze dell'ordine non chiedono mai dati sensibili via SMS, e-mail o telefono, né chiedono di spostare i tuoi risparmi su conti correnti diversi dal tuo per tutelarli da frodi o indagini. **Verifica sempre prima di agire.**

Per qualsiasi informazione, puoi rivolgerti alle Associazioni dei Consumatori riconosciute dalla Regione Liguria.