

# TOSCANA TODAY

## ITALIA WEB MAGAZINE

 Italian

ATTUALITÀ

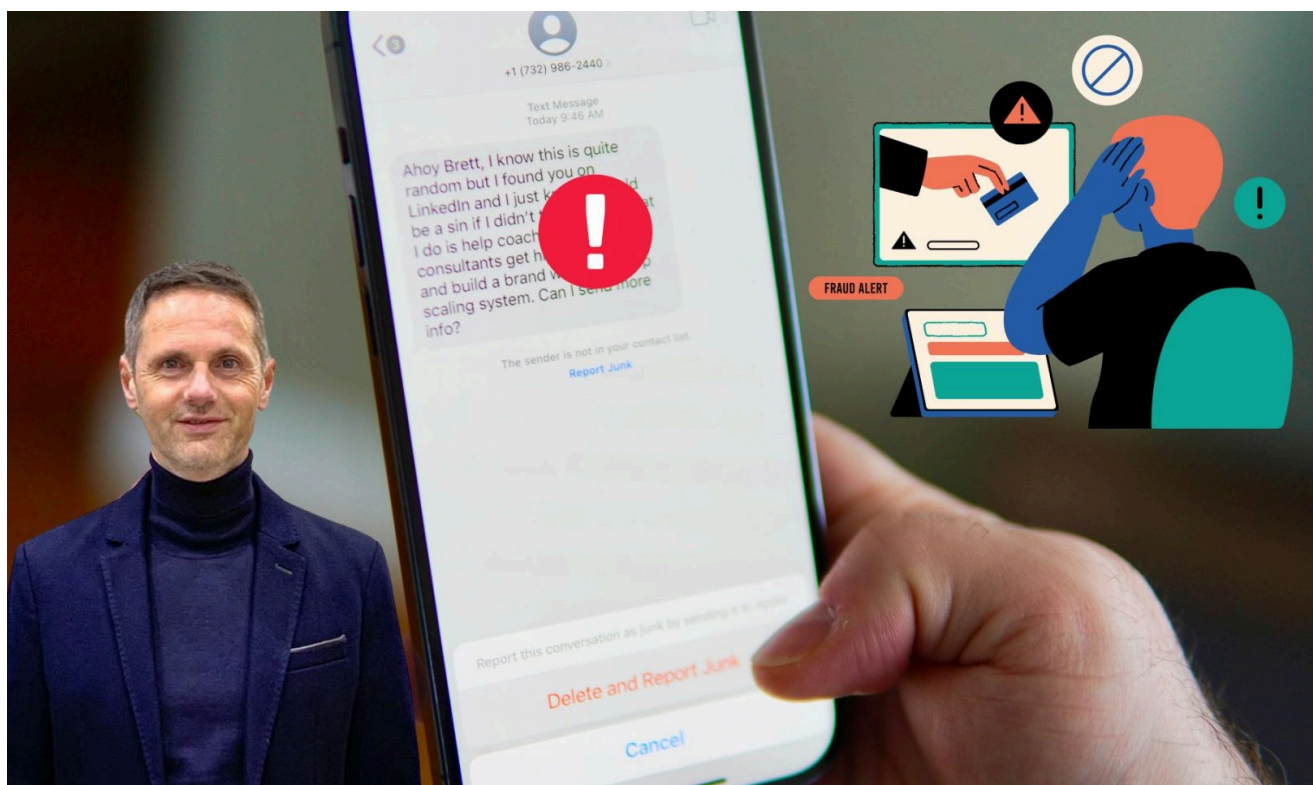
IN TOSCANA

GIURIDICA



LUOGHI E SAPORI

TERZA PAGINA



## Quando il truffatore ha la voce (e il numero) della tua banca

22/10/2026 17:54 · Alberto Foggia

[Preferenze privacy](#)

# di ALBERTO FOGGIA — Le truffe digitali più efficaci non “forzano” i sistemi informatici: ingannano le persone

**È** il principio dell'ingegneria sociale (*social engineering*): un insieme di tecniche di manipolazione psicologica che sfrutta fiducia, paura e urgenza per indurre la vittima a compiere, con le proprie mani, l'azione che consente al criminale di colpire.

Le vecchie e-mail sgrammaticate del *phishing* hanno lasciato il posto a schemi più sofisticati, che combinano:

- a) spoofing: la falsificazione del numero chiamante o del mittente dell'SMS, che appare identico a quello ufficiale della banca o delle forze dell'ordine;
- b) smishing e quishing: link malevoli inviati via SMS o WhatsApp, oppure nascosti in un QR code;
- c) trojan bancari e RAT (*Remote Access Tool*): applicazioni che, una volta installate, permettono al truffatore di vedere lo schermo, leggere i messaggi e comandare il telefono a distanza.

Il risultato è un attacco in cui la vittima è convinta di proteggere il proprio denaro proprio mentre lo sta consegnando.

## Il caso di Marco (storia inventata, ma verosimile)

Martedì, ore 18:40. Marco, 47 anni, impiegato, riceve una chiamata. Sul display compare il numero del servizio clienti della sua banca, lo stesso che ha in rubrica.

«Buonasera, sono dell'Ufficio Sicurezza. Rileviamo un accesso anomalo al suo conto da un dispositivo estero e un bonifico in uscita di 4.900 euro. Dobbiamo bloccarlo subito.»

L'operatore è cortese e preparato: conosce nome, cognome e la filiale di Marco. Poco dopo arriva un SMS, nella stessa conversazione dove Marco riceve i messaggi autentici della banca, con un link per scaricare la “nuova app di protezione del conto”. In alternativa, gli viene suggerito di inquadrare un QR code inviato su WhatsApp.

Marco installa l'app, concede le autorizzazioni richieste (“servono per la scansione antivirus”) e, su indicazione dell'operatore, apre l'app bancaria “per verificare che il

blocco sia attivo". Gli viene detto che riceverà alcuni codici "di annullamento" da confermare.

Il giorno dopo il conto è vuoto: tre bonifici istantanei e una ricarica su carta prepagata. Nessuna notifica è arrivata sul telefono.

### **Lo schema dell'attacco, passo dopo passo**

#### **a) Primo contatto e manipolazione psicologica**

Il criminale usa lo spoofing per far comparire un numero legittimo.

Crea un allarme (attacco in corso, bonifico sospetto) e un senso di urgenza che impedisce di riflettere.

Spesso dispone già di dati personali reperiti in precedenti violazioni o sui social, aumentando la credibilità.

#### **b) L'inganno dell'applicazione**

La vittima viene indotta a installare un'app presentata come "di sicurezza" o di "assistenza remota".

In realtà si tratta di un software di controllo remoto o di un trojan, cui la vittima stessa concede permessi estesi (accessibilità, lettura SMS, sovrapposizione allo schermo).

#### **c) Sottrazione delle credenziali e dei codici OTP/passkey**

L'app registra ciò che viene digitato e mostrato a schermo: username, password, PIN.

Intercetta i codici OTP (le password usa e getta inviate via SMS o generate dall'app) o induce la vittima ad approvare in buona fede le notifiche di autorizzazione, presentate come "annullamenti".

#### **d) Sottrazione dei fondi**

Con il controllo del dispositivo, il truffatore dispone bonifici istantanei, ricariche o pagamenti verso conti "di passaggio".

#### **e) Blocco delle notifiche e occultamento**

Le notifiche della banca vengono nascoste o cancellate; talvolta si modificano i recapiti associati al conto.

La vittima si accorge del danno solo ore o giorni dopo.

### **La banca deve rimborsare? Diligenza dell'istituto e colpa grave del cliente**

Sul piano civilistico, la disciplina di riferimento è il d.lgs. 27 gennaio 2010, n. 11, che recepisce la normativa europea sui servizi di pagamento.

La regola: rimborso immediato

In caso di operazione non autorizzata, la banca rimborsa l'importo immediatamente e in ogni caso al più tardi entro la fine della giornata operativa successiva a quella in cui ne prende atto o riceve la comunicazione. Può sospendere il rimborso solo in caso di motivato sospetto di frode.

Le tutele per il cliente

Nessuna perdita dopo la segnalazione: il cliente non sopporta perdite per gli utilizzi indebiti successivi alla comunicazione alla banca.

Autenticazione forte (SCA): se la banca non esige un'autenticazione forte del cliente – cioè la combinazione di almeno due fattori indipendenti, ad esempio password + dispositivo o impronta – il pagatore non sopporta alcuna perdita, salvo frode.

Perdita non percepibile: nessuna perdita se l'appropriazione dello strumento non poteva essere notata dal cliente prima del pagamento, o se è dovuta a dipendenti o fornitori della banca.

Franchigia massima di 50 euro negli altri casi.

### **Il punto critico: la colpa grave**

La tutela viene meno se il cliente non ha adempiuto ai propri obblighi «con dolo o colpa grave»: in tal caso sopporta tutte le perdite. Tra questi obblighi vi sono l'adozione di «tutte le ragionevoli misure idonee a proteggere le credenziali di sicurezza personalizzate» e la comunicazione «senza indugio» dell'uso non autorizzato.

### **Come si orientano Arbitro Bancario Finanziario e giudici**

La questione si gioca sul bilanciamento tra questi due poli:

a) da un lato, la diligenza della banca: aver richiesto la SCA, disporre di sistemi di monitoraggio delle operazioni anomale, aver informato il cliente sui rischi di frode;

b) dall'altro, la colpa grave dell'utente, che non può essere presunta dalla sola riuscita della frode, ma va valutata alla luce della sofisticazione dell'inganno. Lo spoofing di un numero ufficiale, che rende la chiamata indistinguibile da una autentica, è un elemento che incide in modo rilevante su questa valutazione.

L'esito dipende quindi molto dalle circostanze concrete: per questo è decisivo documentare tutto e – come vedremo – chiedere alla banca i dati tecnici dell'operazione.

### **Non limitarti a dire “non sono stato io”: chiedi i dati tecnici alla banca**

Nelle frodi con spoofing, app malevola e controllo remoto, la discussione non si gioca solo sul fatto che la vittima abbia ricevuto una chiamata ingannevole. Il punto centrale diventa spesso un altro: la banca aveva sistemi idonei a rilevare l'anomalia? Ha richiesto una SCA autentica e non solo apparente? I suoi alert hanno funzionato?

Senza queste informazioni, il cliente rischia di trovarsi in una posizione di debolezza probatoria nel reclamo o davanti all'ABF. Con questi dati, invece, un consulente tecnico può verificare se l'operazione sia stata davvero autenticata con procedure robuste, se il sistema abbia registrato accessi anomali, se vi siano stati cambi di dispositivo o IP poco prima delle disposizioni, e se gli alert antifrode siano stati generati, ignorati oppure mai attivati.

Nel reclamo – o in una successiva richiesta formale – è quindi opportuno chiedere alla banca, per iscritto e per ciascuna operazione contestata:

- a) Log di accessi e operazioni: data, ora, indirizzi IP, identificativi del dispositivo, geolocalizzazione tecnica disponibile, cronologia delle sessioni.
- b) Tracciato dell'autenticazione forte: quali fattori sono stati usati (SMS OTP, app, biometria, token), se tutti i passaggi siano stati completati correttamente, e soprattutto quali informazioni (importo, beneficiario) fossero mostrate al cliente nella schermata di autorizzazione. Il punto non è solo se “un codice è stato inserito”, ma se la procedura fosse realmente idonea a garantire un consenso informato.
- c) Alert antifrode e scoring di rischio: se l'operazione sia stata sottoposta a sistemi automatici di rilevazione anomalie, con quale esito, se siano stati generati alert interni e se vi sia stata o meno un'analisi di compatibilità con lo storico del cliente.
- d) Modifiche alle impostazioni di sicurezza: se, nelle ore o nei giorni precedenti i bonifici, siano stati registrati cambi di numero di telefono, nuovo dispositivo, modifica delle credenziali, variazione dei limiti dispositivi o disattivazione di notifiche. Nella frode con trojan o accesso remoto, il truffatore spesso prepara il terreno prima di agire.

e) Tracciato delle notifiche inviate: quali SMS, email o push siano stati inviati, a quale recapito, a che ora e con quale esito tecnico (consegnato, non consegnato). Questo consente di capire se la mancata ricezione da parte della vittima dipenda da un'interferenza malevola o da un malfunzionamento del sistema della banca.

f) Documentazione contrattuale e informativa: quali misure di sicurezza fossero previste nel contratto e quali avvisi antifrode la banca avesse fornito al cliente, per confrontare la prassi dichiarata con quanto realmente accaduto.

Una volta ottenuti questi elementi, l'esame di un esperto informatico può essere determinante. L'analisi tecnica consente di verificare se le operazioni fossero riconoscibili come atipiche, se l'autenticazione sia stata aggirata o resa inefficace dalla compromissione del telefono, e se i presidi della banca abbiano funzionato solo formalmente o anche nella sostanza. In altre parole: non è sufficiente sapere che cosa è successo; occorre capire come è tecnicamente successo. Ed è spesso lì che si decide la controversia.

In sintesi: nella truffa bancaria digitale la prova è anche tecnica. Pretendere trasparenza sui dati dell'operazione non è un capriccio: è il primo passo per far valere i propri diritti.

### **Le 5 regole d'oro per non cadere nella trappola**

a) La banca non ti chiede mai di installare app tramite link o QR code. Le app ufficiali si scaricano solo dagli store ufficiali, cercandole tu stesso.

b) Il numero sul display non è una garanzia. Con lo spoofing può essere falsificato. Riattacca e richiama tu il numero ufficiale riportato sul sito o sulla carta.

c) Mai condividere OTP, PIN o approvare notifiche che non hai avviato. Nessun operatore autentico te li chiederà, neppure per "annullare" un'operazione.

d) Diffida dell'urgenza. Pressione, toni allarmistici e richieste di agire "subito" sono il segnale tipico della manipolazione.

e) Non concedere permessi speciali alle app (accessibilità, controllo dello schermo, lettura SMS) se non sai esattamente perché servono. Nessuna "app di sicurezza bancaria" ne ha bisogno.

### **Sei già caduto nella truffa? Cosa fare subito**

Il fattore tempo è decisivo, anche giuridicamente: la legge impone di comunicare l'uso non autorizzato «senza indugio», e dalla segnalazione in poi le perdite non sono più a carico tuo.

#### a) Isola lo smartphone

Attiva la modalità aereo o spegni il telefono: il truffatore perde il controllo remoto.

Da un altro dispositivo, disinstalla in seguito l'app sospetta o fai verificare il telefono da un tecnico.

#### b) Blocca carte e accessi

Chiama il numero verde ufficiale della banca per il blocco di carte e home banking.

Da un dispositivo sicuro, cambia le password e disconnetti tutte le sessioni attive.

#### c) Disconosci le operazioni

Comunica formalmente alla banca che le operazioni non sono state autorizzate da te e chiedi il rimborso nei termini di legge.

#### d) Sporgi denuncia alla Polizia Postale o alla Guardia di Finanza

Riporta in modo dettagliato date, orari, numeri chiamanti, SMS, link e operazioni contestate.

Conserva screenshot, registro chiamate e messaggi: sono prove fondamentali sia nel procedimento penale sia nella richiesta di rimborso.

#### e) Invia un reclamo scritto alla banca

Allega copia della denuncia e ricostruisci i fatti, evidenziando gli elementi che rendevano l'inganno credibile (ad esempio, numero falsificato o SMS nel thread ufficiale).

Chiedi espressamente, già nel reclamo, i dati tecnici delle operazioni contestate (log, IP, dispositivi, tracciato SCA, alert antifrode, notifiche inviate), per farli esaminare da un consulente informatico.

Se il reclamo è respinto o rimane senza risposta, puoi presentare ricorso all'Arbitro Bancario Finanziario, possibilità che deve essere indicata nel tuo contratto.

Attenzione, quindi, la tecnologia dei truffatori evolve, ma la loro arma principale resta la manipolazione. Fermarsi, riattaccare e richiamare la banca dal numero ufficiale è spesso sufficiente a sventare l'attacco. E se il danno è già avvenuto, la legge offre tutele concrete: a condizione di agire subito, documentare ogni passaggio e pretendere trasparenza tecnica dall'intermediario.



## Alberto Foggia

Alberto Foggia è avvocato esperto di diritto bancario e di composizione delle crisi da sovraindebitamento.

### PRIVACY POLICY

---

[Cookie Policy](#)

[Termini e Condizioni](#)

# TOSCANA TODAY

Edito da Toscana Today News & Media con sede a Zurigo (Svizzera), Dolderstrasse 62  
(8031) VAT/P.IVA= CHE 219.143.708 - Impresa editoriale iscritta al Registro delle  
Imprese di Zurigo Designed by [WPZOOM](#)

[Privacy Policy](#) [Cookie Policy](#) [Termini e Condizioni](#)