

# GLI STRUMENTI ELETTRONICI DI PAGAMENTO E LA BANCA ON-LINE Aspetti di attenzione

Ivrea, 16 marzo 2026



# Tecnologia e Pagamenti: dal sesterzio allo smart-phone



## IL CONTO CORRENTE

Il conto corrente semplifica la gestione del denaro.  
È una forma di deposito che consente di utilizzare la moneta bancaria per le transazioni.



Il cliente deposita in banca il denaro, la banca lo custodisce e offre una serie di servizi.

## I SERVIZI

- Pagamenti (es: domiciliazione delle utenze);
- Incassi (es: accredito di pensione o stipendio);
- Strumenti di pagamento (bonifici, assegni, carta di debito e di credito);
  
- Servizio di cassa (il cliente può versare e prelevare denaro dal conto corrente in qualsiasi momento);
- Servizi finanziari aggiuntivi agganciati al conto corrente:
  - Finanziamento (mutuo, fido..);
  - Investimento dei risparmi (gestione patrimoniale);
  
- Utilizzo a distanza (Home banking):
  - Phone banking;
  - Internet e Mobile banking.

## L'INDICATORE SINTETICO DI COSTO

Gli intermediari devono riportare nei fogli informativi e nei documenti di sintesi periodici dei conti correnti destinati ai consumatori l'ISC che

- Comprende tutte le spese e le commissioni che sarebbero addebitate al cliente nel corso dell'anno, al netto di oneri fiscali e interessi;
- Viene calcolato per uno o più «profili di operatività tipo» individuati dalla Banca d'Italia.

## IL CONTROLLO DEL CONTO CORRENTE

Controllare l'utilizzo del conto corrente è utile per:

- Gestire al meglio le proprie risorse;
- Verificare le spese effettuate;
- Verificare l'operato della banca.

In caso di errori, il cliente ha il diritto di segnalarli alla banca e ottenerne la correzione.

## Strumenti di pagamento alternativi al contante

### Le carte

- Carte di Debito
- Carte di Credito
- Carte Prepagate (le carte ibanizzate)
- Carte co-badge

### Strumenti legati al c/c

- Bonifico
- Addebito diretto

### Strumenti evoluti

- *mobile payments*
- *instant payments*
- *carte virtuali*
- ...

## Strumenti di pagamento alternativi al contante

### Pagamenti online

- Carte di pagamento
- Bonifico:
  - dal proprio internet banking
  - dal sito di e-commerce tramite un PISP diverso dalla propria banca
- Circuiti specializzati (es. paypal)

### Mobile payments

- Mobile banking
- Mobile WALLET (es. GooglePay, ApplePay, SamsungPay)
- Peer to peer e Instant Payment (es. paypal, satispay)
- Prelievi cardless

## Strumenti di pagamento alternativi al contante

### VANTAGGI

- comodi
- pagamenti online
- sicuri
- tracciabili

### RISCHI

#### CONTANTE:

Furto, smarrimento, banconote false, attività illegali

#### PAGAMENTI ELETTRONICI:

furto, smarrimento, clonazione, truffe



**Serve consapevolezza!**

## **Gli intermediari autorizzati sono soggetti a controlli**

La Banca d'Italia conduce la vigilanza sulle seguenti categorie di intermediari:

- ❖ **Banche e gruppi bancari**
- ❖ **SIM e gruppi di SIM**
- ❖ **SGR, SICAV e SICAF**
- ❖ **Istituti di moneta elettronica - IMEL**
- ❖ **Istituti di pagamento**
- ❖ **Conglomerati finanziari**
- ❖ **Intermediari finanziari**
- ❖ **Fornitori di crowdfunding per le imprese**
- ❖ **Soggetti MiCAR operanti in cripto-attività**
- ❖ **Gestori di crediti in sofferenza (c.d. *credit servicer*)**
- ❖ **Operatori del microcredito**

### **CONSOB - DIVISIONE VIGILANZA INTERMEDIARI E PROTEZIONE INVESTITORI**

Vigila sul rispetto delle norme in materia di prestazione di servizi e attività di investimento da parte dei soggetti abilitati, sui fornitori di servizi di *crowdfunding* e sui prestatori di servizi per cripto-attività (...)

## Dove posso informarmi?

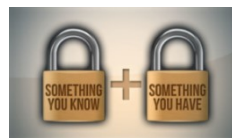
- <https://www.bancaditalia.it/servizi-cittadino/servizi/albi-elenchi/index.html>  
(<https://www.bancaditalia.it/compiti/vigilanza/albi-elenchi/index.html>)
- <https://www.consob.it/web/area-pubblica/impresediinvestimento1>  
(<https://www.consob.it/web/area-pubblica/impresediinvestimento-senza-succursale>)
- <https://euclid.eba.europa.eu/register/>
- <https://www.iosco.org/i-scan/>
- <https://www.esma.europa.eu/investor-corner/warning-and-publications-investors>

**e su altri siti istituzionali**

## LA NORMATIVA – I PRINCIPALI DIRITTI DEL CLIENTE

- Conto di base
- Portabilità
- I pagamenti in euro hanno tutti gli stessi costi (all'interno dell'area SEPA)
- **13 mesi di tempo per disconoscere operazioni di pagamento e chiederne il rimborso**
- **Diritto al rimborso di operazioni in assenza di:**
  - **SCA (*strong customer authentication*)**
  - **Colpa grave del cliente**

## I presidi di sicurezza



### STRONG CUSTOMER AUTHENTICATION (SCA)

- Richiesti almeno due elementi (indipendenti tra loro) per verificare l'identità dell'utilizzatore
- Necessaria per *i) accesso al conto; ii) operazioni di pagamento elettroniche; iii) operazioni a rischio frode*

### QUALI FATTORI?

- Qualcosa che solo l'utente **conosce** (pin, password)
- Qualcosa che solo l'utente **possiede** (token, device registrato - OTP)
- Qualcosa che **contraddistingue fisicamente** solo l'utente (impronta digitale, face ID)

### DYNAMIC LINKING

- operazioni di pagamento elettronico a distanza, comprende elementi che colleghino *in maniera dinamica* l'operazione a uno specifico importo e a un beneficiario specifico

# SERVIZI DI PAGAMENTO - OBBLIGHI DELL'INTERMEDIARIO

**DIMOSTRARE LA CORRETTA ESECUZIONE  
AUTORIZZAZIONE E CONTABILIZZAZIONE**

**SISTEMA DI AUTENTICAZIONE FORTE**

CON PWD DINAMICA PER PAGAMENTI ON LINE (art. 10-bis)

**SERVIZI BLOCCO CARTE** (art. 8)

**ESEGUIRE LE OPERAZIONI ALL'  
IDENTIFICATIVO UNICO INDICATO** (art. 24)

**VERIFICARE LA CORRISPONDENZA TRA NOME  
E IBAN DEL BENEFICIARIO DI BONIFICO**

(dal 9/10/25 Reg. UE 2024/886)



# SERVIZI DI PAGAMENTO - OBBLIGHI DELL'UTENTE

**UTILIZZO** CONFORME AI TERMINI  
CONTRATTUALI

**COMUNICAZIONE  
TEMPESTIVA**

UTILIZZO NON AUTORIZZATO E  
SMARRIMENTO/FURTO/APPR.IND.  
(13 mesi: art. 9)

**PROTEZIONE** CREDENZIALI



## In caso di problemi...



Presentare  
un reclamo  
alla banca

Inviare un  
esposto alla  
Banca d'Italia

Proporre  
ricorso  
all'ABF

## L'Arbitro Bancario Finanziario (ABF)

L'ABF è un sistema stragiudiziale di risoluzione delle controversie tra banche e clienti in materia di operazioni e servizi bancari e finanziari

E' indipendente ed autonomo dalla **Banca d'Italia** che ne supporta il funzionamento tramite le Segreterie Tecniche.



## IL RICORSO ALL'ARBITRO BANCARIO FINANZIARIO

<https://www.arbitrobancariofinanziario.it/presentare-ricorso/index.html>

**Organismo indipendente e imparziale**, sostenuto nel suo funzionamento dalla Banca d'Italia – ADR esternalizzato

Sistema attivabile solo dal cliente, con **costi contenuti** (€ 20)

**Sette Collegi**, che decidono secondo diritto sulla base della documentazione prodotta dalle parti

Decisioni non vincolanti ma **sanzione reputazionale** in caso di inadempimento

Impregiudicata la facoltà delle parti di adire **l'Autorità Giudiziaria**



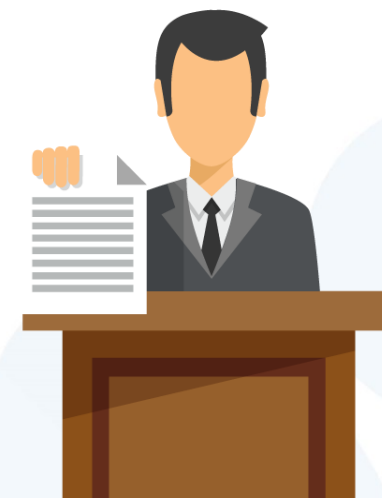
## L'ABF: CHI DECIDE I RICORSI



7 COLLEGI  
TERRITORIALI:  
Roma, Milano,  
Napoli, **Torino**,  
Bologna, Bari,  
Palermo

DOCENTI  
UNIVERSITARI;  
MAGISTRATI;  
PROFESSIONISTI

REQUISITI DI INTEGRITA'  
E INDIPENDENZA



sito web [www.arbitrobancariofinanziario.it](http://www.arbitrobancariofinanziario.it)

## Home Banking: andare in banca da casa

Tutti i servizi che le banche e gli intermediari finanziari offrono online e che, per questo, sono accessibili da casa.

Basta avere un pc, un tablet o uno smartphone; qualche volta potresti dover scaricare un'app.

...molti ne hanno scoperto utilità e praticità più generali.

- Costi inferiori
- Effetto positivo sull'ambiente
- Si risparmia tempo



## E' importante seguire le cautele per un corretto uso dell'home banking

Una regola importante è questa

- **Mai** inserire su pagine web o condividere, via e-mail o SMS, informazioni sensibili come credenziali di accesso all'home banking, Password, OTP (password temporanea), PIN, dati delle carte o altri codici personali.

**Sei sul sito...  
...giusto?**





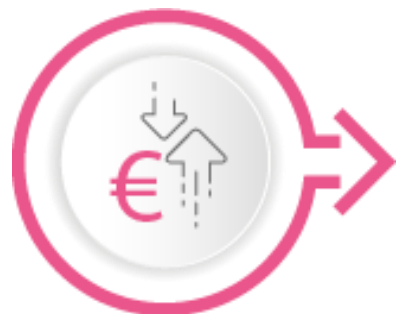
## SERVIZI INFORMATIVI

Puoi consultare **l'estratto conto**: visualizzare e verificare tutte le operazioni effettuate sul conto corrente e il saldo.



## GESTIONE DELLE CARTE DI PAGAMENTO

Puoi gestire le tue carte di pagamento, effettuare la **ricarica**, controllare **saldo** e **movimenti**.



## **DISPOSIZIONI DI OPERAZIONI BANCARIE**

Puoi svolgere **operazioni dispositive** quali:

- bonifici e giroconti
- addebiti diretti
- pagamento delle tasse
- ricariche telefoniche



## FINANZIAMENTI

Puoi verificare lo **stato dei finanziamenti attivi**, in particolare:

- le rate;
- il capitale residuo/erogato;
- gli altri finanziamenti attivi.

Puoi anche richiedere un prestito personale.



## INVESTIMENTI

Puoi **operare sui prodotti finanziari**, ad esempio compravendita titoli e monitoraggio del mercato, e **verificare i tuoi investimenti** (rendimenti e costi).



# I 5 principali consigli per rendere la tua casa una cyber fortezza contro gli attacchi informatici

1

**Cambia** sempre la **password** predefinita del modem/router, proteggi il tuo WiFi

2

Installa **software antivirus** su tutti i dispositivi

3

Scegli **password complesse** e diverse

4


Controlla le **autorizzazioni** delle tue app ed elimina quelle che non usi

5

Esegui il **backup** dei dati e gli aggiornamenti del software



# Sicurezza dei pagamenti elettronici in Italia: cosa ci dicono i dati

 Tempo di lettura **4 minuti**

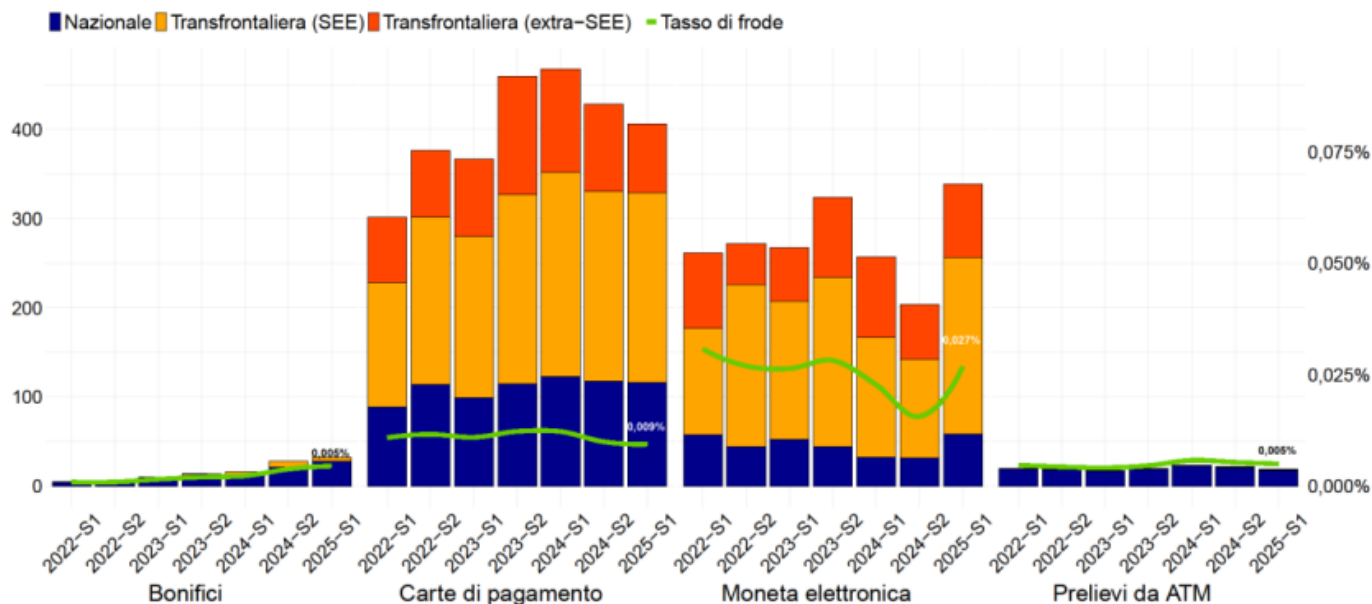
Publicato il **18/02/2026**

La Banca d'Italia ha pubblicato l'aggiornamento del [Rapporto sulle operazioni di pagamento fraudolente in Italia](#), che ci offre una fotografia aggiornata al primo semestre del 2025 sulla sicurezza dei [pagamenti elettronici](#) nel nostro Paese.

Nel complesso, il nostro sistema dei pagamenti è sicuro: se consideriamo tutti gli strumenti di pagamento elettronici vengono truffati **solo tre euro ogni 100.000 euro trasferiti**.

### Numero di operazioni fraudolente

(asse di sinistra: migliaia; asse di destra: in % del numero totale delle operazioni per strumento di pagamento)



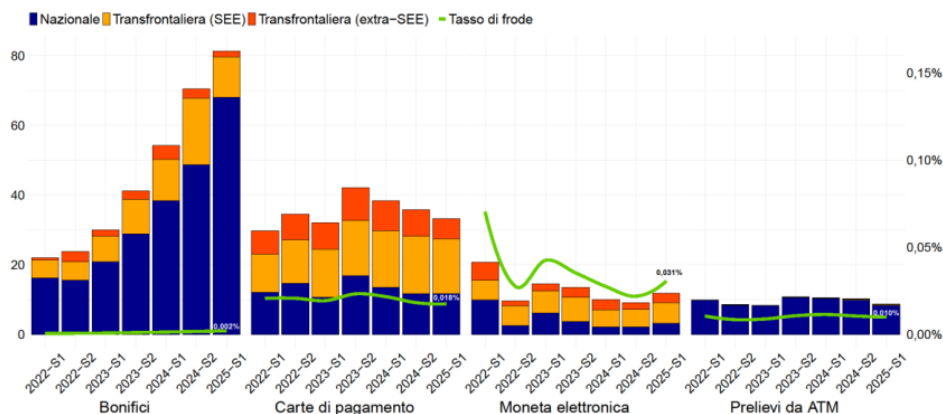
Fonte: Elaborazioni su dati di matrice dei conti forniti dai PSP italiani.

Il valore medio delle operazioni fraudolente si conferma più elevato per i bonifici

Il tasso di frode, misurato dal rapporto tra operazioni fraudolente e il totale delle transazioni di pagamento, è più elevato per la moneta elettronica e le carte di pagamento

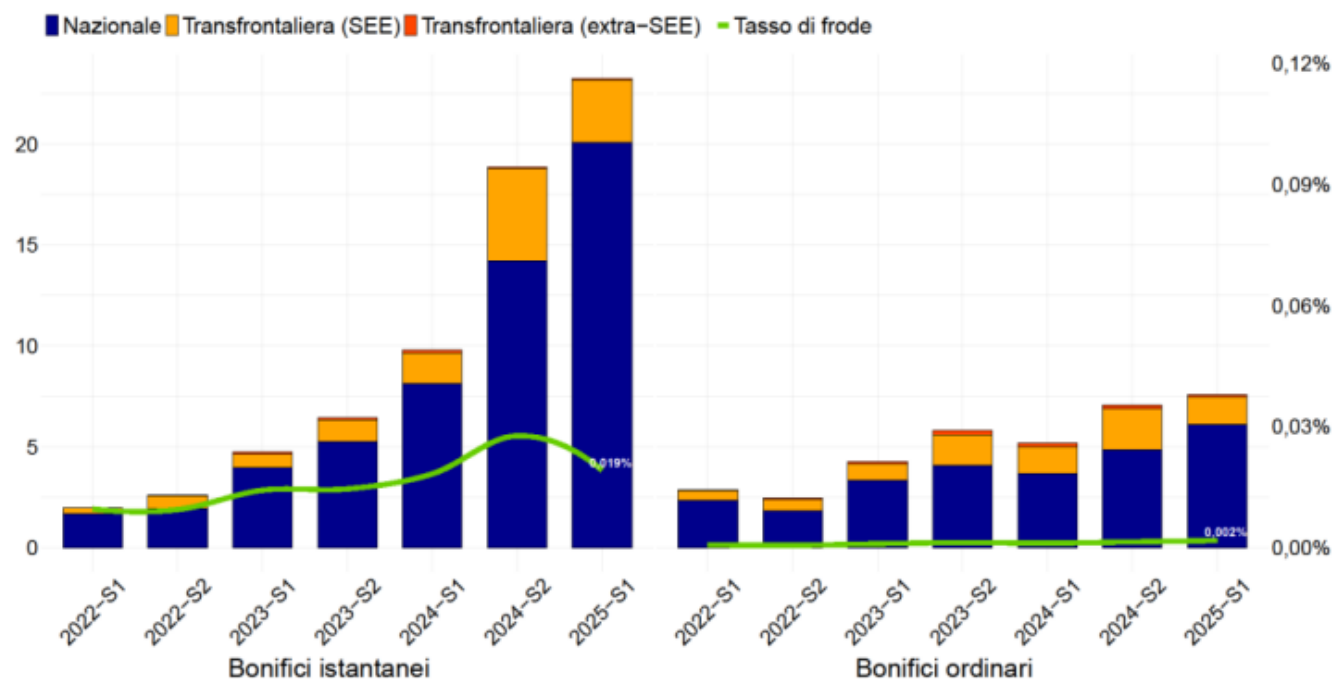
### Valore delle operazioni fraudolente

(asse di sinistra: milioni di euro; asse di destra: in % del valore totale delle operazioni per strumento di pagamento)



## Numero di operazioni fraudolente

(asse di sinistra: migliaia; asse di destra: in % del numero totale delle operazioni di pagamento)



I bonifici istantanei si confermano più rischiosi rispetto agli ordinari: **una volta disposti**, infatti, **i bonifici istantanei sono irrevocabili**, e questo li rende strumenti molto utili anche per i malintenzionati che hanno tutto l'interesse a ricevere il denaro truffato nel minor tempo possibile

Una buona notizia: **il tasso di frode si è ridotto** nel primo semestre 2025 (da 59 euro a 43 euro ogni 100.000 euro trasferiti). Alla riduzione del rischio potrebbe aver contribuito la **verifica della corrispondenza tra l'IBAN e il nome del beneficiario**, un servizio che le banche e gli altri intermediari mettono a disposizione quando effettuiamo un bonifico (sia istantaneo che ordinario)

## Le truffe più diffuse



### Phishing

Il truffatore ti manda un'email ingannevole per farti inviare denaro



### Smishing

Il truffatore ti invia un messaggio sul telefono per farti inviare denaro



### Vishing

Il truffatore ti telefona per farti inviare denaro



### Quishing



### Spoofing

Il truffatore camuffa l'origine dell'email, del messaggio o della telefonata. Potrebbe presentarsi come la tua banca



### Man in the browser

Il truffatore con un malware intercetta i dati con cui paghi online o usi l'home banking e li modifica in tempo reale



### Ingegneria sociale

Il truffatore tenta di persuaderti a dargli denaro o a comunicargli i dati con cui paghi via internet o usi l'home banking fingendo di essere qualcuno di cui ti fidi, creando un senso di urgenza per indurti ad agire senza riflettere



### Pharming

Il truffatore manipola il sito web per indirizzarti a un sito fasullo che danneggia il computer o preleva i tuoi dati

## Come funzionano le truffe nei pagamenti online

- 1) La **manipolazione del pagatore** consiste nell'indurre la vittima a fare un pagamento a favore del truffatore o altri complici con le motivazioni più varie, ad esempio fingendo di essere un figlio in difficoltà, un amico o persino un operatore della banca. In molti casi, il truffatore trasmette un senso di urgenza o paura per spingere la vittima ad agire rapidamente
- 2) L' **emissione del pagamento da parte del truffatore** consiste nell'esecuzione di un pagamento senza il consenso della vittima, ad esempio quando il truffatore entra in possesso di dati privati come numeri di carta di credito, PIN e credenziali d'accesso all'home banking
- 3) La **modifica di un ordine di pagamento da parte del frodatore** consiste nell'intercettare e modificare la comunicazione elettronica che contiene le informazioni di un pagamento legittimo. Un esempio è rappresentato dalla truffa nota come man in the browser, attraverso la quale il truffatore riesce a intercettare i dati inseriti durante pagamenti online o operazioni di home banking e a modificare ordini di pagamento legittimi, dirottandoli a proprio favore.

## Le truffe : come difendersi



**Informati sulle truffe più comuni**



**Non dare a nessuno le tue credenziali**



**Usa password diverse e non salvarle**



**Non cliccare su link o scansionare QR code in messaggi sospetti**



**Mantieni la calma e non farti prendere dalla fretta**



**Se hai dubbi, non agire subito e chiedi alla tua banca**



**Non usare l'home banking con reti wi-fi pubbliche**



**Controlla la sicurezza del sito**



**Installa un antivirus**



**Aggiorna il sistema operativo e l'antivirus**



**Controlla le tue operazioni periodicamente**



**Attiva l'alert che ti avvisa dei pagamenti**



# Alcuni esempi

(da ricorsi ABF)

**DISCIPLINA DI  
FAVOR PER  
L'UTENTE**

Art. 10  
d.lgs.  
11/2010

**Disconoscimento** di un'operazione di pagamento

1

Prova di **autenticazione**

2

Prova della **colpa grave**

un **comportamento abnorme** e,  
in quanto tale, **non scusabile**»



*Se non ha agito con frode o **colpa grave**, il cliente non sopporta alcuna perdita; al più il valore della franchigia*  
*(Recepimento italiano PSD II)*



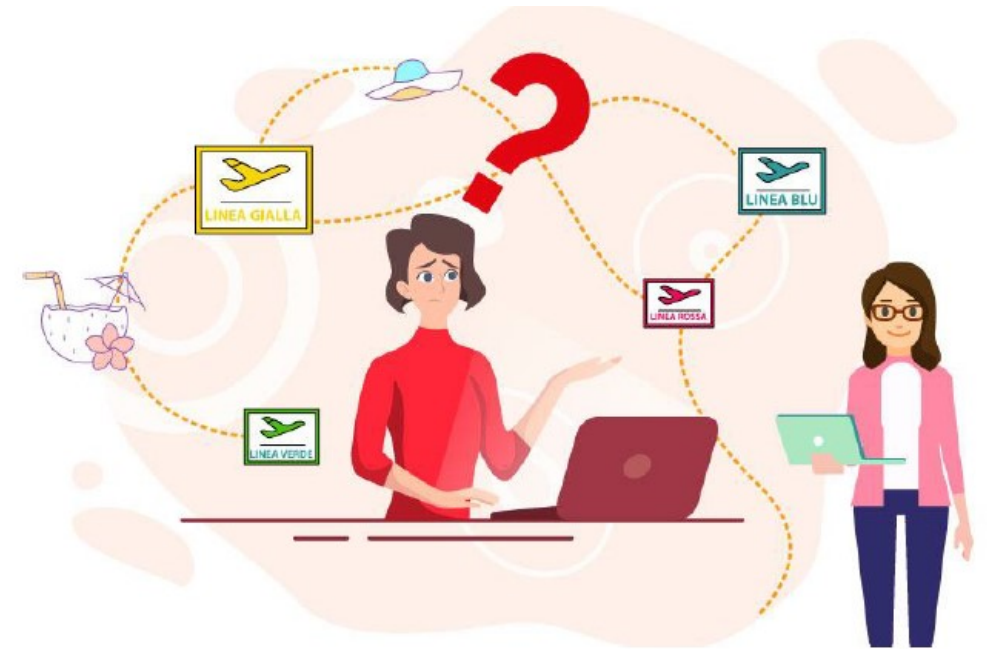
*E' in **colpa grave** chi opera con straordinaria e inescusabile imprudenza o negligenza, omettendo [...] quel grado minimo ed elementare di diligenza generalmente osservato da tutti" (Coord. ABF 5304/2013)*

# 1. Il caso del *phishing*

**Non abboccare!**

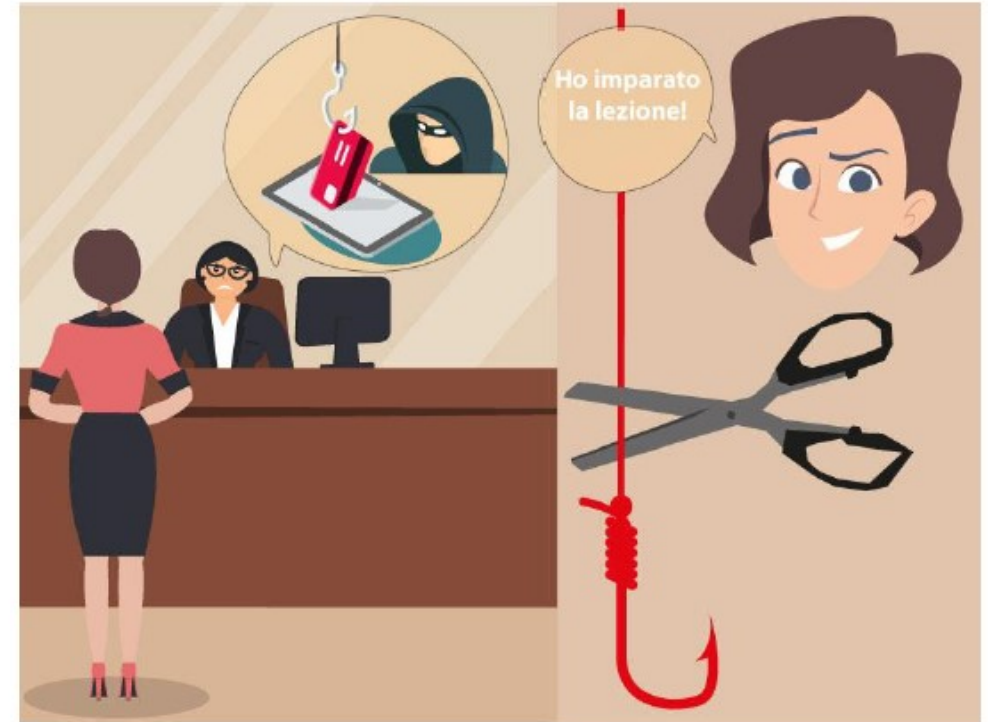
# Il caso del *phishing*

- ▶ La sig.ra Giuliana racconta di aver ricevuto un messaggio in cui le comunicavano il **blocco** del conto e, per **sbloccarlo**, chiedevano di «confermare la sua identità cliccando sul link *http:wwinfoconto.it* presente nel messaggio e inserendo i propri dati riservati sul sito di Banca Blu»



# Il caso del *phishing*

- ▷ Arriva una telefonata nel corso della quale le chiedono di comunicare i codici che riceve via SMS
- ▷ La sig. Giuliana riceve poi un SMS «Banca Blu, è stata richiesta un'autorizzazione di 120 euro per operazione internet su carta che termina con\*876»
- ▷ La sig.ra Giuliana grazie a sua figlia capisce di esser caduta vittima di una truffa e si rivolge alla sua banca che però **rifiuta** di rimborsare le operazioni
- ▷ La sig.ra Giuliana presenta ricorso all'ABF



**Il collegio ABF ha accolto la richiesta di rimborso?**



# 2. Il caso dello *spoofing*

**Non ti fidare!**

# Il caso dello *spoofing*

- ▷ Il sig. Martini riceve un SMS dal numero della propria banca con invito ad accedere al conto per evitare la sospensione
- ▷ Indirizzato a una pagina identica a quella del proprio *home banking*, appare un messaggio che preannuncia una telefonata da parte di un operatore



- ▷ Riceve una telefonata dal numero verde della banca in cui viene avvertito di n. 2 bonifici istantanei di € 14.900,00
- ▷ L'operatore dichiara che le operazioni sono state bloccate ma per completare la procedura occorre inserire il codice ricevuto via SMS

# Il caso dello *spoofing*

▷ Dalla documentazione allegata emerge che:

- L'sms truffaldino appare in coda a quelli genuini ricevuti dalla banca
- Il numero di telefono da cui ha ricevuto la chiamata corrisponde al numero verde della banca
- Il sig. Martini riceve SMS a conferma dell'avvenuto storno dei bonifici



**Il collegio ABF ha accolto la richiesta di rimborso?**



# 3. Il caso del *man in the browser*

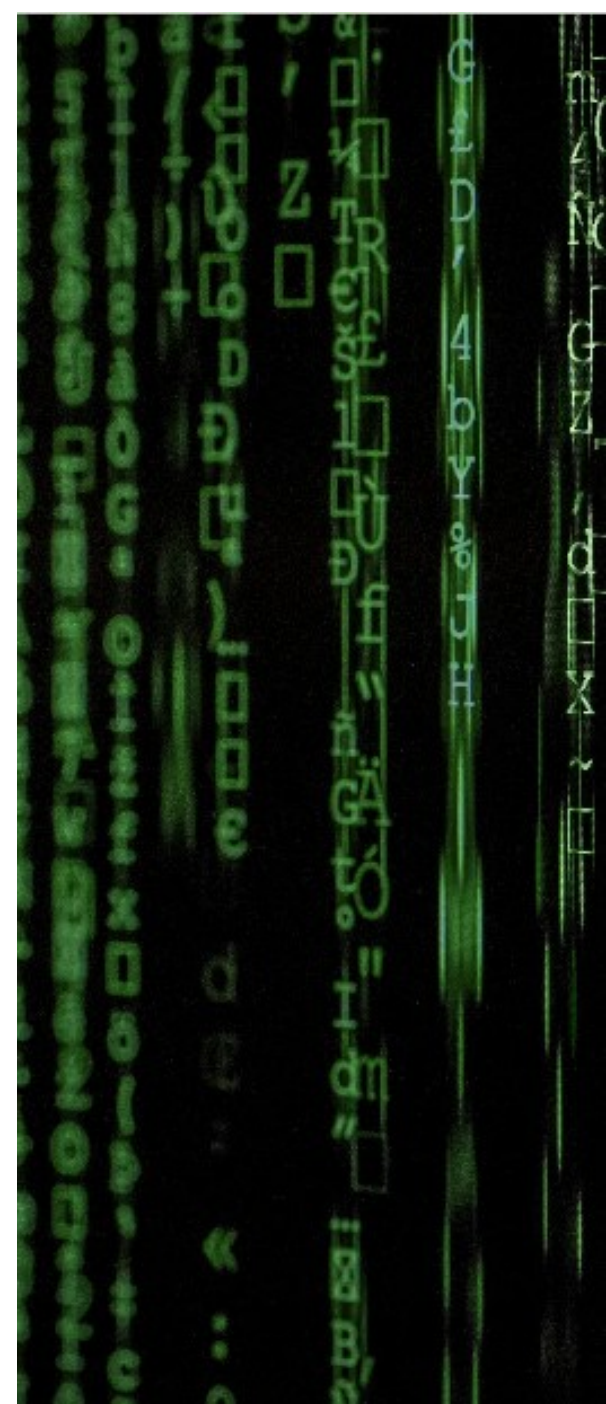
# Il caso del *man in the browser*

- ▷ Il sig. Favini, titolare di impresa, dispone un bonifico a saldo di fattura per oltre € 20.000
- ▷ Indirizza il bonifico alla società AUxxOS indicando l'IBAN adoperato per l'acconto (andato a buon fine)
- ▷ Dopo 10 giorni il fornitore lamenta il mancato pagamento
- ▷ A seguito di contestazione, la banca blocca il conto e lo sottopone a controlli, il bonifico risulta disposto a favore di soggetto sconosciuto





**Il collegio ABF ha accolto la richiesta di rimborso?**



# Decisioni ABF sui casi esaminati

- ▷ Phishing – E' in colpa grave il cliente che cade vittima di colpevole credulità «abboccando» a una mail o SMS o telefonata truffaldina e rivelando le proprie credenziali e codici
- ▷ Spoofing – Truffa insidiosa: se è allegato il messaggio «civetta» e questo risulta «verosimile» (es. privo di errori ortografici) è normalmente esclusa la colpa grave. Attenzione ai casi in cui l'invio dell'OTP avviene con «messaggio parlante»
- ▷ Man in the browser – Il carattere particolarmente insidioso della truffa, realizzata tramite *malware* che si frappone tra utente e intermediario esclude la colpa grave



<https://economieapertutti.bancaditalia.it/>

Cerca

Chi siamo ▾

Aree tematiche ▲

Notizie e rubriche ▾

Percorsi formativi ▾

Strumenti ▾

Media ed eventi ▾



Carta di credito



Carta co-badge



Conto corrente

Prestiti

Pagamenti

Diritti e tutele

Risparmio e investimenti

Finanza sostenibile

Trappole comportamentali



Carta prepagata



Truffe: come difendersi

Chi siamo ▾

Aree tematiche ▾

Notizie e rubriche ▾

Percorsi formativi ▾

Strumenti ▾

Home / Notizie e rubriche / Notizie / Le truffe nel mondo delle cryptoattività

TUTELA

## Le truffe nel mondo delle cryptoattività

Tempo di lettura **4 minuti**

Publicato il **22/12/2025**

La rapida crescita delle **cryptoattività** e le loro caratteristiche di ampia accessibilità, velocità, anonimato e spesso irreversibilità delle transazioni, hanno creato un terreno fertile per lo sviluppo di frodi, anche grazie all'innovazione tecnologica.

**Una nuova comunicazione** congiunta delle autorità europee ESMA, EBA ed EIOPA ci mette in guardia dal rischio di truffe connesse alle cryptoattività, ne descrive i principali tipi per aiutare le persone a riconoscerle, contiene alcuni consigli per evitarle.

**Grazie per l'attenzione**