DOSSIER TRUFFE AI CONSUMATORI IN ITALIA

Analisi delle principali frodi negli ultimi mesi (2025-2026)

A cura di: Consumerismo no profit
Data: Febbraio 2026
Periodo di riferimento: 2024-2026

INDICE

---

1. EXECUTIVE SUMMARY

Il fenomeno delle truffe ai danni dei consumatori italiani ha raggiunto dimensioni allarmanti negli ultimi mesi, con un'escalation significativa legata all'evoluzione tecnologica e all'utilizzo dell'intelligenza artificiale.

DATI CHIAVE:

- **559,4 milioni di euro** sottratti nel triennio 2022-2024
- **2,8 milioni di vittime** nel solo 2024
- **+30% di aumento** delle truffe nell'ultimo anno
- **+1000% di crescita** delle truffe legate al lavoro (maggio-luglio 2025)

---

2. QUADRO GENERALE E NUMERI DEL FENOMENO

2.1 Dimensione economica

Triennio 2022-2024: 559,4 milioni di euro sottratti

Anno	Truffe Online	Frodi Informatiche	Totale
2022	114,4 milioni €	38,5 milioni €	152,9 milioni €
2023	137,3 milioni €	46,5 milioni €	183,8 milioni €
2024	181,0 milioni €	48,1 milioni €	229,1 milioni €

Incrementi anno su anno:

- 2022-2023: +15,9% (+24,4 milioni €)
- 2023-2024: +29,2% (+51,7 milioni €)

2.2 Frodi creditizie

Primo semestre 2024:

- **17.200 casi** registrati
- **79 milioni di euro** di danni stimati
- Fenomeno trasversale a tutte le categorie di clienti bancari

2.3 Vittime

- **2,8 milioni di italiani** truffati nel 2024 (dato ANSA)
- **Oltre 7 milioni** hanno smesso di fare acquisti online dopo essere stati truffati
- **Il 95% delle truffe** avviene tramite canali digitali

---

3. TIPOLOGIE DI TRUFFE PIÙ DIFFUSE

3.1 SMISHING E PHISHING (35% dei casi)

Cos'è: Truffe tramite SMS e messaggi che imitano comunicazioni ufficiali

Varianti principali:

A) Falsi rimborsi fiscali

- **Pretesto:** Rimborsi IVA o crediti fiscali inesistenti
- **Importo esca:** 500-1.000 euro
- **Metodo:** Link a pagine clone dell'Agenzia delle Entrate
- **Periodo critico:** Gennaio-aprile (dichiarazioni fiscali)

Esempio di messaggio:

> "Gentile contribuente, hai diritto a un rimborso IVA di 500€. Clicca qui per verificare i tuoi dati e ricevere l'accredito."

B) Falsi problemi con spedizioni

- **Variante 1:** Pacco bloccato in dogana (pagamento 2,99-9,99€)
- **Variante 2:** Problemi con consegna Amazon/Poste
- **Vittimizzazione:** Anche chi non ha ordinato nulla (curiosità)

C) Falsi rimborsi sanitari

- **Target:** Over 60
- **Pretesto:** Rimborsi ticket o prestazioni sanitarie
- **Canale:** SMS con link a form fraudolenti
- **Rischio aggiuntivo:** Furto dati sanitari sensibili

3.2 TRUFFE BANCARIE E CARTE DI CREDITO (28% dei casi)

Modalità operative:

1. **False chiamate da operatori bancari**
    - Utilizzo di intelligenza artificiale per clonare voci
    - Richiesta di PIN/OTP con pretesto di "blocco conto"
    - Sofisticazione: caller ID falsificato con numero reale della banca
2. **Clonazione siti bancari**
    - Siti quasi identici agli originali
    - URL simili (es. intesasanpaolo.it con "I" maiuscola invece di "l")
    - Certificati SSL falsi per apparire sicuri
3. **Truffa Postepay**
    - Falsi rimborsi di 500€

- Link a pagine clone
- Richiesta dati carta + OTP

Danni: 48,1 milioni € nel 2024 (+25% vs 2022)

3.3 TRUFFE DEL LAVORO (crescita +1000%)

Esplosione del fenomeno: Maggio-luglio 2025

Tipologie:

1. **Falsi annunci su LinkedIn/Indeed**

    - Offerte di lavoro da remoto con stipendi irrealistici
    - Reindirizzamento a Telegram/WhatsApp
    - Richiesta dati personali per "contratto"
    - Richiesta pagamento per "corso di formazione"

2. **Schema del lavoro facile**

    - "Guadagna 3.000€ al mese da casa"
    - Richiesta investimento iniziale
    - Schema Ponzi mascherato da network marketing

3. **Falsi colloqui con IA**

    - Chiamate con voce artificiale
    - "Curriculum approvato, invia dati per procedere"
    - Furto identità per frodi creditizie successive

Target preferenziale: Giovani 18-35 anni e disoccupati

3.4 TRUFFE CON CRIPTOVALUTE (15% dei casi)

Varianti:

1. **Falsi investimenti**

    - Promesse di rendimenti del 100-500%
    - Piattaforme clone di exchange reali
    - Canali Telegram con "esperti" falsi

2. **Airdrop fraudolenti**

- "Ricevi 1 Bitcoin gratis"
- Richiesta piccolo pagamento per "sbloccare"
- Furto chiavi private wallet

3. **Pig Butchering 2.0**

    - Relazione sentimentale online costruita nel tempo
    - Introduzione graduale a "opportunità di investimento"
    - Piattaforme di trading completamente false
    - Perdite medie: 10.000-50.000€ per vittima

Piattaforme più utilizzate: Instagram, Telegram, dating app

3.5 TRUFFE MARKETPLACE (12% dei casi)

Settori colpiti:

- Facebook Marketplace
- Subito.it
- eBay (annunci esterni alla piattaforma)
- Vinted

Meccanismi:

1. **Prodotti inesistenti**

    - Prezzi irrealistici (AirPods a 30€)
    - Pagamento fuori piattaforma (bonifico)
    - Venditore sparisce dopo pagamento

2. **Bait and switch**

    - Prodotto mostrato diverso da quello inviato
    - Prodotti contraffatti/rotti

3. **Falsi acquirenti**

    - Link "per verifica identità venditore"
    - Phishing dati bancari

3.6 TRUFFE NELLE APP DI INCONTRI (8% dei casi)

Schema Romance Scam:

1. **Fase 1:** Costruzione relazione (settimane/mesi)
2. **Fase 2:** Emergenza improvvisa (medica, legale, viaggio)
3. **Fase 3:** Richiesta prestito/aiuto economico
4. **Fase 4:** Sparizione o richieste continue

Perdita media per vittima: 5.000-15.000€

Piattaforme: Tinder, Bumble, Facebook Dating, Meetic

3.7 FALSI PACCHI E PREMI (7% dei casi)

Periodo critico: Novembre-dicembre (festività)

Esempi:

- "Hai vinto un iPhone 15!"
- "Premio da Amazon per clienti fedeli"
- "Ultimo tentativo di consegna pacco"

Conseguenze:

- Installazione malware
- Sottoscrizioni non autorizzate
- Furto dati personali

---

4. ANALISI PER SETTORE

4.1 SETTORE ENERGETICO (Luce e Gas)

Fenomeni rilevati:

1. **Bollette in ritardo con costi nascosti**
    - Invio tardivo seguito da solleciti immediati
    - Applicazione interessi di mora esagerati
    - Sistema sospetto di profitto sui ritardi
2. **Cambio fornitore non autorizzato**
    - Contratti firmati a insaputa del cliente
    - Agenti porta a porta con tecniche aggressive

- Disdette non processate

Azione Consumerismo: Segnalazione sistematica alle Autorità competenti

4.2 SETTORE SANITARIO

Campagne malevole rilevate:

1. **SMS falsi rimborsi ticket**

    - Numeri 893 a sovrapprezzo
    - Compilazione form con dati sensibili
    - Rischio: furto identità sanitaria

2. **False prenotazioni CUP**

    - Chiamate da numeri fraudolenti
    - Richiesta di attendere in linea (costo elevato)
    - Prosciugamento credito telefonico

Invito Consumerismo: Massima prudenza e verifiche su gestione dati sanitari

4.3 SETTORE FISCALE

Campagne Agenzia Entrate (confermate dal Fisco):

2 gennaio 2026 - Falsi rimborsi IVA

- Target: Imprese e contribuenti
- Pretesto: Eccedenze versamento 2024
- Pagine clone portale AdE

Gennaio 2026 - Falsi rimborsi 730

- Importo esca: 500€
- Email/SMS con link e QR code
- Form raccolta dati fiscali e bancari

---

5. MODALITÀ OPERATIVE DEI TRUFFATORI

5.1 Evoluzione tecnologica

Utilizzo dell'Intelligenza Artificiale:

1. **Clonazione vocale**

    - Sintesi vocale realistica di operatori bancari
    - Imitazione voce familiari per truffe ai danni di anziani
    - Difficoltà crescente nel riconoscere la frode

2. **Deepfake**

    - Video falsi di personaggi pubblici che promuovono investimenti
    - Testimonianze false di "clienti soddisfatti"

3. **Chatbot sofisticati**

    - Conversazioni naturali su Telegram/WhatsApp
    - Risposte personalizzate basate su dati social

4. **Generazione automatica contenuti**

    - Siti web professionali creati in minuti
    - Email personalizzate su larga scala
    - Annunci di lavoro credibili

5.2 Ingegneria sociale

Tecniche psicologiche utilizzate:

1. **Urgenza artificiale**

    - "Agisci entro 24 ore o perderai l'opportunità"
    - "Conto bloccato: verifica immediata richiesta"

2. **Sfruttamento emozioni**

    - Paura (conto bloccato, problemi legali)
    - Avidità (guadagni facili, premi)
    - Speranza (lavoro, amore, investimenti)

3. **Autorità fittizia**

    - Logo enti ufficiali
    - Linguaggio burocratico
    - Riferimenti a normative (spesso inventate)

4. **Prova sociale**

    - Testimonianze false
    - Recensioni fabbricate
    - Gruppi Telegram con migliaia di membri (bot)

5.3 Canali di diffusione

Classifica per frequenza:

1. **SMS** (40%)
2. **Email** (25%)
3. **Chiamate** (15%)
4. **Social Media** (12%)
5. **Messaggistica istantanea** (8%)

---

6. IMPATTO TERRITORIALE

6.1 Regioni più colpite (dati 2024)

Top 5 per valore economico:

1. **Lombardia** - 98 milioni € (17,5%)
2. **Sicilia** - 67 milioni € (12%)
3. **Campania** - 61 milioni € (10,9%)
4. **Lazio** - 58 milioni € (10,4%)
5. **Veneto** - 42 milioni € (7,5%)

Analisi:

- Regioni più popolose proporzionalmente più colpite
- Sud Italia: maggiore incidenza su truffe telefoniche
- Nord: prevalenza truffe finanziarie/investimenti

6.2 Fasce d'età

Distribuzione vittime:

- **18-34 anni:** 28% (truffe lavoro, criptovalute, dating)
- **35-54 anni:** 35% (truffe finanziarie, marketplace)
- **55-74 anni:** 27% (truffe bancarie, phishing)
- **Over 75:** 10% (truffe telefoniche, falsi nipoti)

Perdita media per fascia:

- 18-34: 1.200€
- 35-54: 3.500€
- 55-74: 4.800€
- Over 75: 2.900€

---

7. SOLUZIONI E CONTROMISURE

7.1 Iniziative istituzionali

Provvedimenti 2025-2026:

1. **Blocco chiamate internazionali sospette** (19 novembre 2025)
    - Filtro automatico numeri esteri fraudolenti
    - Collaborazione operatori telefonici
2. **Registro Opposizioni potenziato**
    - Estensione a cellulari
    - Sanzioni inasprite per violatori
3. **Campagna Commissione Europea** (26 novembre 2025)
    - Sensibilizzazione truffe online periodo natalizio
    - Focus su meccanismo notice and action (DSA)
4. **Task force AGCOM-Polizia Postale**
    - Monitoraggio continuo campagne malevole

- Takedown rapido siti fraudolenti

7.2 Strumenti di protezione per i consumatori

TECNOLOGICI:

1. **Autenticazione multifattoriale**
    - Attivare su tutti gli account bancari/finanziari
    - Preferire app autenticatore vs SMS
2. **Antivirus e antimalware**
    - Aggiornamento costante
    - Scansione regolare dispositivi
3. **Password manager**
    - Password uniche e complesse
    - Non riutilizzare credenziali
4. **Carte prepagate per acquisti online**
    - Limitazione danni in caso di frode
    - Ricarica solo per importo necessario
5. **Notifiche transazioni in tempo reale**
    - Alert SMS/app per ogni movimento
    - Blocco immediato in caso di anomalie

COMPORTAMENTALI:

1. **Verifica sempre la fonte**
    - Non cliccare link in SMS/email sospette
    - Digitare manualmente URL siti bancari
    - Chiamare numero ufficiale per verifiche
2. **Non condividere MAI:**
    - PIN carte
    - OTP/codici di verifica

- Password
- Chiavi private criptovalute

3. **Diffidare di:**

    - Offerte troppo vantaggiose
    - Richieste urgenti
    - Errori grammaticali in comunicazioni ufficiali
    - Mittenti con email/numeri strani

4. **Verificare URL siti web**

    - Cercare errori (amaz0n invece di amazon)
    - Controllare certificato SSL
    - Verificare dominio ufficiale

5. **Per truffe lavoro:**

    - Ricercare azienda su Google
    - Leggere recensioni Glassdoor
    - Mai pagare per "corsi" o "materiali"
    - Verificare esistenza profilo LinkedIn aziendale

6. **Per marketplace:**

    - Pagare solo tramite piattaforma
    - Verificare recensioni venditore
    - Diffidare prezzi troppo bassi
    - Preferire ritiro persona o pagamento alla consegna

7.3 Cosa fare se si è vittima

IMMEDIATO (entro 1 ora):

1. **Blocco carte/conti**

    - Chiamare immediatamente la propria banca
    - Numero verde blocco carte (800.822.056 Visa, 800.110.847 Mastercard)

2. **Cambio password**

    - Tutti gli account potenzialmente compromessi
    - Particolare attenzione a email e home banking

3. **Contattare operatore telefonico**

    - Se credito prosciugato o SMS fraudolenti

ENTRO 24 ORE:

1. **Denuncia Polizia Postale**

    - Online: www.commissariatodips.it
    - Presso uffici territoriali
    - Portare tutta la documentazione (screenshot, email, SMS)

2. **Segnalazione a banca/ente coinvolto**

    - Contestazione operazioni non autorizzate
    - Richiesta storno (se possibile)

3. **Segnalazione ad associazioni consumatori**

    - Consumerismo no profit
    - Adiconsum, Codacons, Altroconsumo

FOLLOW-UP:

1. **Monitoraggio movimenti**

    - Controllo estratti conto per 6 mesi
    - Verifica assenza utilizzi fraudolenti identità

2. **Segnalazione CRIF**

    - Alert tentativi apertura crediti a proprio nome

3. **Supporto legale**

    - Valutare assistenza per recupero somme
    - Associazioni consumatori offrono supporto gratuito

7.4 Strumenti di verifica

Siti utili:

- **www.commissariatodips.it** - Verifica truffe note
- **www.agenziaentrate.gov.it** - Avvisi campagne phishing
- **www.poste.it/truffe-online** - Archivio truffe Postepay
- **www.bankitalia.it** - Verifica intermediari autorizzati
- **www.consob.it** - Verifica operatori finanziari

App:

- **TrueCaller** - Identificazione chiamate sospette
- **Kaspersky/Bitdefender** - Protezione mobile
- **Have I Been Pwned** - Verifica email compromesse

---

8. RACCOMANDAZIONI FINALI

8.1 Per i consumatori

GOLDEN RULES - Le 10 regole d'oro:

1. **Se sembra troppo bello, probabilmente è una truffa**
2. **Nessun ente serio chiede PIN/password per telefono**
3. **Verifica sempre indipendentemente prima di agire**
4. **Non cedere alla pressione dell'urgenza**
5. **Proteggi i tuoi dati come proteggeresti le chiavi di casa**
6. **Usa carte prepagate per acquisti online**
7. **Attiva notifiche per ogni transazione**
8. **Mantieni aggiornati dispositivi e antivirus**
9. **Diffida di contatti non sollecitati**
10. **In caso di dubbio, chiedi a qualcuno di fiducia**

8.2 Per le istituzioni

URGENZE:

1. **Educazione finanziaria nelle scuole**
    - Inserimento curricula su sicurezza digitale
    - Formazione riconoscimento truffe
2. **Campagne di sensibilizzazione mirate**
    - Particolare focus su anziani e giovani

- Utilizzo media tradizionali + social

3. **Rafforzamento cooperazione internazionale**

    - Truffe sempre più transnazionali
    - Server spesso all'estero

4. **Snellimento procedure rimborso**

    - Vittime spesso non recuperano nulla
    - Disincentivo alla denuncia

5. **Sanzioni più severe**

    - Pene attuali non deterrenti
    - Necessario inasprimento

8.3 Per le imprese

RESPONSABILITÀ:

1. **Sistemi di verifica identità robusti**
2. **Educazione clienti su propri canali ufficiali**
3. **Monitoraggio clonazioni brand**
4. **Collaborazione con autorità**
5. **Trasparenza su data breach**

8.4 Previsioni 2026

TREND ATTESI:

1. **Ulteriore sofisticazione IA**

    - Deepfake video in tempo reale
    - Truffe sempre più personalizzate

2. **Nuovi target**

    - Minori con carte prepagate
    - Anziani con smartphone

3. **Nuovi vettori**

    - Realtà virtuale/metaverso

- Assistenti vocali domestici

4. **Crescita settori**

    - Truffe green/ESG
    - Criptovalute e NFT

NECESSARIO: Vigilanza costante e aggiornamento continuo

CONCLUSIONI

Il fenomeno delle truffe ai consumatori italiani ha assunto proporzioni epidemiche, con **559,4 milioni di euro sottratti in tre anni** e **quasi 3 milioni di vittime** nel solo 2024. L'evoluzione tecnologica, in particolare l'intelligenza artificiale, ha reso le frodi sempre più sofisticate e difficili da riconoscere.

Le truffe non sono più un problema di "ingenuità" delle vittime, ma una minaccia sistemica che colpisce trasversalmente tutte le fasce d'età e sociali. L'aumento del **+1000% delle truffe legate al lavoro** dimostra come i criminali sappiano sfruttare le vulnerabilità socio-economiche.

LA PREVENZIONE È L'UNICA VERA DIFESA:

- Educazione continua dei consumatori
- Investimenti in sicurezza digitale
- Collaborazione tra istituzioni, imprese e associazioni
- Aggiornamento normativo costante

Consumerismo no profit continuerà a monitorare il fenomeno, segnalare alle autorità competenti le criticità rilevate e supportare i consumatori nella tutela dei propri diritti.

Per segnalazioni e supporto:

- Email: info@consumerismo.it
- Tel: [numero verde]
- Web: www.consumerismo.it

FONTI

- Federazione Autonoma Bancari Italiani (FABI) - Rapporto 2024-2025

- Agenzia delle Entrate - Alert truffe
- Ministero della Salute - Segnalazioni frodi sanitarie
- ANSA - Dati vittime 2024
- Associazione Italiana Consumatori - Report truffe online 2025
- Adiconsum - Monitoraggio truffe fiscali
- AGCOM - Osservatorio truffe digitali
- Polizia Postale - Statistiche denunce
- Commissione Europea - Campagna truffe online
- Visa - Ricerca comportamenti consumatori italiani
- Consumerismo no profit - Casi seguiti e segnalazioni

Documento a cura di: Consumerismo no profit APS/ETS

Data pubblicazione: Febbraio 2026 Ultimo aggiornamento: 09/02/2026