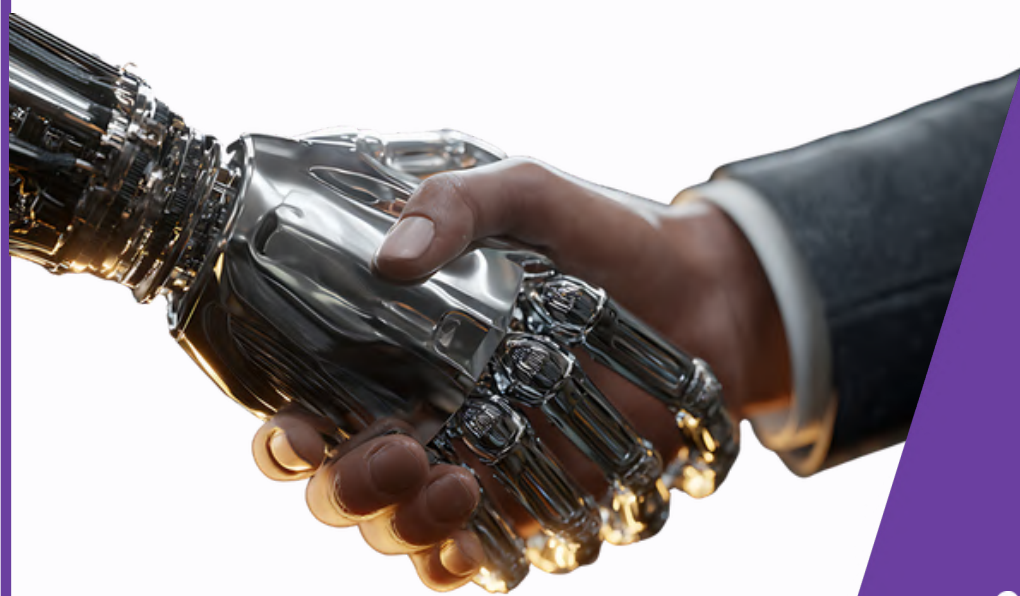


TRUFFE AI

Guida pratica per difendersi dalle
nuove frodi dell'Intelligenza Artificiale



UNC
CONSUMATORI.IT

INDICE

INTRODUZIONE..... 3

PERCHÉ OGGI È PIÙ DIFFICILE RICONOSCERE UN
IMBROGLIO..... 6

LE TRUFFE PIÙ FREQUENTI..... 10

LE 10 REGOLE D'ORO PER NON CADERE NELLE
TRUFFE..... 16

COSA FARE SE SEI STATO TRUFFATO..... 18

LE TRUFFE CHE STANNO ARRIVANDO..... 20

LA TRUFFA PIÙ ANTICA DEL MONDO..... 22

L'INTELLIGENZA ARTIFICIALE NON È IL NEMICO

Se stai leggendo queste pagine, probabilmente hai già sentito parlare di **deepfake, voci clonate, immagini false generate dall'Intelligenza Artificiale** o forse hai ricevuto un messaggio che ti ha fatto sorgere un dubbio: e se fosse una truffa?

Agli sportelli di Unione Nazionale Consumatori si moltiplicano le segnalazioni di consumatori preoccupati per le nuove tecnologie. **Alcuni raccontano di aver ricevuto telefonate apparentemente provenienti dalla propria banca**; altri hanno visto sui social video di personaggi famosi che promettevano guadagni facili; qualcuno si è trovato davanti a fotografie, documenti o conversazioni che sembravano autentici, ma che erano stati creati artificialmente.

La sensazione più diffusa è sempre la stessa: se non posso più fidarmi di ciò che vedo e sento, come faccio a difendermi? Prima di iniziare questo viaggio nelle truffe più frequenti che hanno a che fare con l'AI è bene fare una premessa: l'Intelligenza Artificiale non è il nemico, ma, come ogni tecnologia, **può essere utilizzata per migliorare la nostra vita oppure per danneggiare gli altri.**

È l'uso che se ne fa, dunque, a fare la differenza, ma anche come le persone vi si interfacciano.

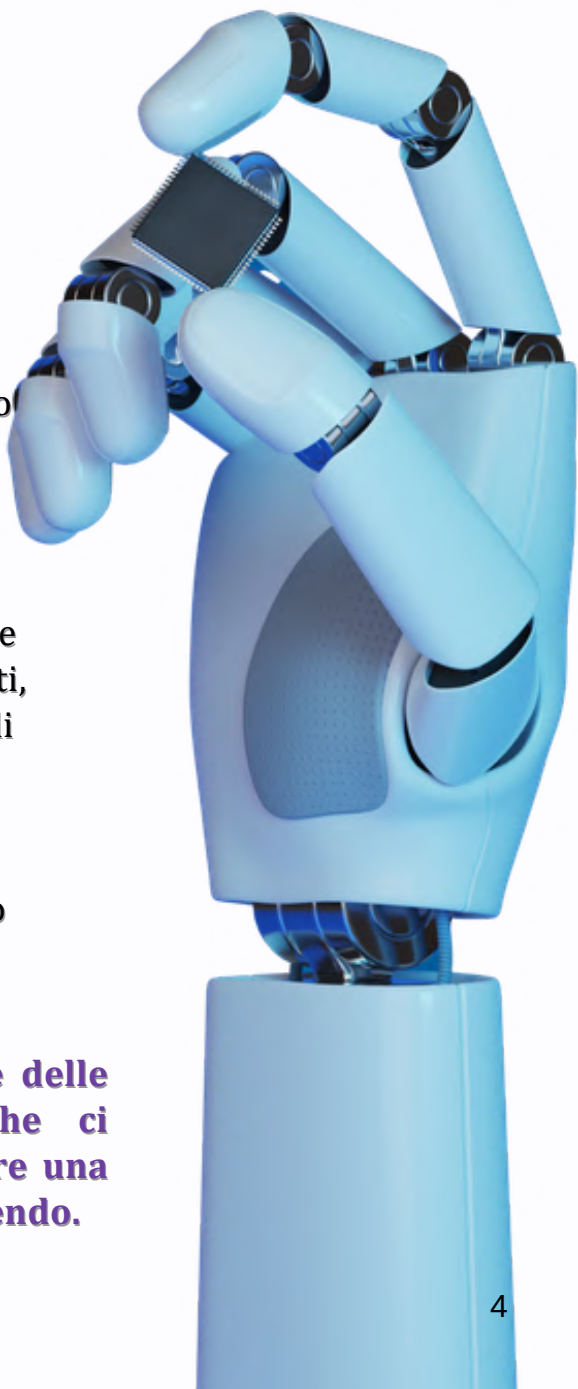
Perché le truffe stanno cambiando

Le truffe non sono una novità. Da sempre i criminali cercano di sfruttare la fiducia delle persone per ottenere denaro, dati personali o informazioni riservate.

Quello che sta cambiando è il **livello di credibilità** delle frodi.

Grazie all'Intelligenza Artificiale è oggi possibile scrivere messaggi perfetti, tradurre testi in decine di lingue senza errori, imitare una voce umana, generare fotografie realistiche e creare video estremamente convincenti.

Il risultato è che **molte delle tradizionali "spie" che ci aiutavano a riconoscere una truffa stanno scomparendo.**





Cosa rende l'AI così pericolosa

Quando si parla di truffe basate sull'Intelligenza Artificiale, spesso si pensa immediatamente ai deepfake o alle voci clonate.

In realtà il vero pericolo è un altro: **la scalabilità**.

Un tempo per preparare una truffa servivano tempo, competenze e risorse. Oggi alcuni strumenti consentono di creare **centinaia di messaggi personalizzati in pochi minuti**, ciascuno cucito su misura per la vittima designata.

È questa capacità industriale che rende l'AI così utile ai truffatori.

PERCHÉ OGGI È PIÙ DIFFICILE RICONOSCERE UN IMBROGLIO

Per anni ci siamo abituati a riconoscere le truffe online grazie a una serie di dettagli che tradivano i criminali: **messaggi scritti male, e-mail piene di errori, telefonate poco credibili, siti internet approssimativi**. Era fastidioso, ma era anche rassicurante: il truffatore si smascherava da solo.

Oggi molte di queste "spie" stanno scomparendo. **L'Intelligenza Artificiale consente di scrivere testi perfetti**, tradurre messaggi in qualsiasi lingua, creare immagini realistiche e persino imitare voci e volti di persone reali.

Dai vecchi phishing ai deepfake

Le tecniche utilizzate dai truffatori non sono cambiate molto: continuano a voler rubare soldi, dati personali o credenziali di accesso. Quello che è cambiato radicalmente è il livello di credibilità.

Un'**e-mail di phishing** di qualche anno fa era riconoscibile a colpo d'occhio. Oggi può essere indistinguibile da una comunicazione autentica della tua banca.



Le nuove armi dei truffatori

Ecco gli **strumenti** che l'Intelligenza Artificiale ha messo nelle mani dei criminali:

- **Voce clonata:** bastano pochi secondi di registrazione per riprodurre la voce di chiunque
- **Deepfake:** video falsi che mostrano persone reali dire cose che non hanno mai detto
- **Immagini artificiali:** fotografie di persone o documenti che non esistono
- **Chatbot intelligenti:** programmi capaci di sostenere conversazioni convincenti per ore
- **Messaggi perfetti:** testi senza errori grammaticali o stilistici, in qualsiasi lingua



Le tre leve dei truffatori: fretta, paura e fiducia

Nonostante tutte le innovazioni tecnologiche, c'è una cosa che non è cambiata. **Le truffe continuano a fare leva sulle stesse emozioni umane**: la fretta, la paura, la fiducia.

L'Intelligenza Artificiale rende queste strategie più efficaci, ma non le inventa ed è proprio per questo che possiamo ancora difenderci: conoscere il meccanismo è già metà della battaglia.

La **fretta** è la prima arma.

Quando qualcuno ci mette sotto pressione ("devi decidere adesso", "l'offerta scade tra un'ora", "tuo figlio ha bisogno di te subito") **il nostro cervello smette di ragionare** e comincia a reagire.

È un meccanismo evolutivo: in situazioni di pericolo, fermarsi a riflettere costa tempo prezioso. **I truffatori lo sanno** e costruiscono ogni messaggio per toglierti quel tempo. La tecnologia non ha inventato questa tecnica, ma oggi permette di confezionarla in modo molto più credibile e di consegnarla a milioni di persone contemporaneamente.



La **paura** funziona allo stesso modo, ma agisce su un piano ancora più profondo.

Non è la paura di perdere un'occasione, ma quella di **perdere qualcosa che già consideri tuo**: i risparmi sul conto, la sicurezza della famiglia, la reputazione. Un messaggio che ti avvisa di un accesso sospetto al tuo conto bancario non ti chiede di desiderare qualcosa, ma di proteggere ciò che hai. La risposta emotiva è immediata e potente, e lascia poco spazio al dubbio.

La **fiducia**, infine, è la leva più sofisticata.

Un truffatore che si presenta come sconosciuto ha poche possibilità di successo, ma se arriva indossando il volto di tua figlia, la voce del tuo direttore di banca o il logo di un'azienda che conosci da anni, le difese si abbassano prima ancora che tu te ne accorga. L'Intelligenza Artificiale ha reso questa impostura molto più accessibile: **clonare una voce, costruire un profilo credibile** o replicare graficamente una comunicazione ufficiale richiede oggi pochi minuti e nessuna competenza tecnica particolare.



LE TRUFFE PIÙ FREQUENTI

Conoscere le truffe più diffuse è il primo passo per non caderne vittima. Eccole una per una, con le caratteristiche che le rendono riconoscibili.

"Mamma, ho cambiato numero"

È una delle truffe più diffuse degli ultimi anni.

Il consumatore riceve un messaggio WhatsApp da un numero sconosciuto: **il presunto figlio o figlia racconta di aver perso il telefono e chiede di salvare il nuovo numero.**

Dopo qualche scambio di messaggi arriva puntuale la richiesta di denaro, giustificata dall'emergenza improvvisa.

La leva è sempre la stessa: l'affetto familiare e la paura che un figlio sia in difficoltà.



Il falso direttore di banca

Ricevi una telefonata apparentemente proveniente dalla tua banca. Una voce autorevole ti avvisa di un pagamento sospetto sul tuo conto e ti invita a trasferire il denaro su un conto "sicuro" per proteggerlo. In realtà stai parlando con un truffatore. Nessuna banca ti chiederà mai di spostare denaro per proteggertelo.

Il video del personaggio famoso

Sui social compaiono spesso video di imprenditori, giornalisti o personaggi famosi che sembrano promuovere investimenti miracolosi in criptovalute o piattaforme di trading. In molti casi si tratta di deepfake creati con l'Intelligenza Artificiale: il volto e la voce sono reali, le parole no.



Le false opportunità di guadagno

Siti professionali, recensioni false e chatbot vengono utilizzati per convincere le vittime a investire in criptovalute, trading automatico o piattaforme inesistenti. I guadagni iniziali (spesso reali, per costruire la fiducia) spariscono insieme al capitale nel momento cui si tenta un prelievo.

Il falso servizio clienti

Può capitare di cercare online il numero di assistenza di una banca, di un corriere o di una compagnia telefonica e trovare invece un contatto gestito dai truffatori. Numeri posizionati in cima ai risultati di ricerca grazie ad annunci a pagamento, indistinguibili dai contatti ufficiali.



Il QR Code trappola

Nei parcheggi, nei ristoranti, durante eventi o presso colonnine di ricarica possono essere applicati adesivi fraudolenti che rimandano a siti falsi. Prima di inquadrare un QR Code in un luogo pubblico, verifica che l'adesivo non sia stato applicato sopra quello originale.

La truffa del curriculum

Molti consumatori ricevono offerte di lavoro apparentemente interessanti tramite WhatsApp, Telegram o LinkedIn. Dopo una fase iniziale di colloquio, condotto talvolta da un chatbot AI, viene richiesto il pagamento di corsi obbligatori, software o depositi cauzionali. Il lavoro non esiste.¹³



L'amore artificiale

Le romance scam utilizzano fotografie generate artificialmente, profili social costruiti ad arte e conversazioni estremamente convincenti. La relazione si sviluppa per settimane o mesi, fino a quando arriva la richiesta di denaro per un'emergenza, un biglietto aereo o un investimento condiviso.



Influencer e profili inesistenti

Alcuni profili vengono creati interamente con strumenti AI: immagini generate, follower acquistati, contenuti artificiali. L'obiettivo può essere la promozione di prodotti falsi, la raccolta di dati personali o la costruzione di fiducia prima di una truffa.



La vacanza che non esiste

Case vacanza con foto perfette e prezzi irresistibili, annunci su piattaforme anche affidabili, proprietari disponibili e cordiali. Dopo il pagamento della caparra il proprietario sparisce. Prima di pagare, verifica sempre l'identità del locatore e usa metodi di pagamento tracciabili.

E-commerce e negozi fantasma

I siti fraudolenti sono sempre più professionali, con recensioni false, loghi di spedizionieri noti e politiche di reso dettagliate. Il consumatore acquista un prodotto che non verrà mai consegnato, oppure riceve un articolo completamente diverso da quello descritto



LE 10 REGOLE D'ORO PER NON CADERE NELLE TRUFFE

La tecnologia cambia, ma le regole per difendersi restano sorprendentemente semplici. Eccole.

1. Diffida dell'urgenza

"Devi farlo adesso, o perdi tutto." Questo è il segnale più affidabile che qualcosa non va. Prenditi sempre un momento prima di agire.

2. Verifica sempre con un secondo canale

Se ricevi una richiesta insolita da un familiare, una banca o un'azienda, richiama il numero ufficiale che conosci già. Non usare i recapiti forniti nel messaggio sospetto.

3. Non fidarti della voce

La clonazione vocale è oggi accessibile a chiunque. Se una voce familiare ti chiede denaro al telefono, interrompi la chiamata e richiama direttamente tu.

4. Non fidarti del video

I deepfake sono sempre più convincenti. Un volto noto che promuove un investimento sui social non è una garanzia di autenticità.

5. Controlla sempre l'IBAN

Prima di effettuare qualsiasi bonifico, verifica che il codice IBAN corrisponda a quello che ti aspetti. Chiama il beneficiario per conferma.

6. Non cliccare immediatamente

Un link in un messaggio urgente va trattato con sospetto. Vai direttamente al sito ufficiale digitando l'indirizzo nel browser.

7. Attenzione ai QR Code

Prima di inquadrare un codice in un luogo pubblico, controlla che non ci siano adesivi sovrapposti a quello originale.

8. Proteggi i tuoi account

Usa password diverse per ogni servizio e cambiale regolarmente. Un gestore di password può aiutarti.

9. Attiva l'autenticazione a due fattori

Aggiunge un secondo livello di protezione: anche se qualcuno ottiene la tua password, non potrà accedere senza il codice temporaneo.

10. Parla con qualcuno prima di pagare

Una persona di fiducia, un familiare, un amico. Il tempo di una telefonata può salvarti da un errore irreparabile.



La regola delle regole: nessuna emergenza reale peggiorerà perché ti sei preso cinque minuti per verificare. Molte truffe riescono proprio perché la vittima non si concede quei cinque minuti.

COSA FARE SE SEI STATO TRUFFATO

Scoprire di essere stati truffati è uno shock. Ma la velocità con cui reagisci può fare una grande differenza. Ecco cosa fare, nell'ordine giusto.

1. Blocca immediatamente i pagamenti

Contatta subito la tua banca, anche nel fine settimana, tramite i numeri di emergenza, e segnala l'operazione. In molti casi è possibile bloccare o stornare un bonifico se si agisce entro poche ore.

2. Cambia password e credenziali

Modifica immediatamente le password di tutti gli account coinvolti o potenzialmente compromessi. Inizia dall'e-mail, che spesso è la chiave di accesso agli altri servizi.



3. Conserva tutte le prove

Screenshot, ricevute, numeri di telefono, e-mail e conversazioni possono essere fondamentali sia per la denuncia sia per eventuali richieste di rimborso. Non cancellare nulla.

4. Presenta denuncia

Rivolgiti alle Forze dell'Ordine (Polizia Postale, Carabinieri o Polizia di Stato) con tutta la documentazione disponibile. Anche quando il recupero del denaro sembra improbabile, la denuncia contribuisce a costruire il quadro statistico e investigativo del fenomeno.

5. Avvisa amici e familiari

Se il truffatore ha avuto accesso ai tuoi contatti, potrebbe usare il tuo nome per colpire altre persone. Un avviso tempestivo può evitare che il danno si propaghi.

6. Controlla i movimenti successivi

Nei giorni e nelle settimane seguenti, monitora con attenzione conto corrente, carte e account digitali. Una truffa riuscita spesso viene seguita da ulteriori tentativi.



Non vergognarti di chiedere aiuto. Le truffe possono colpire chiunque, indipendentemente dall'età o dal livello di istruzione. L'importante è reagire rapidamente.

5. LE TRUFFE CHE STANNO ARRIVANDO

Il panorama delle frodi evolve velocemente. Alcune tecnologie ancora in fase di sviluppo potrebbero presto diventare strumenti nelle mani dei criminali. Conoscerle in anticipo è il modo migliore per prepararsi.

Deepfake in tempo reale

Le nuove tecnologie consentono già di modificare in tempo reale il volto e la voce di una persona durante una videochiamata. Quello che oggi richiede ancora tempo e potenza di calcolo diventerà presto accessibile a chiunque: una videochiamata non sarà più una prova sufficiente di identità.



La falsificazione dell'identità digitale

L'AI potrebbe rendere sempre più semplice la creazione di documenti falsi credibili (patenti, passaporti, bollette, estratti conto) e di identità digitali complete, con profili social, storico online e riferimenti incrociati. Verificare chi è davvero la persona con cui si sta trattando diventerà una competenza essenziale.

Gli agenti AI usati dai criminali

I cosiddetti agenti AI sono programmi capaci non solo di dialogare, ma di agire autonomamente: prenotare, pagare, inviare messaggi, adattarsi alle risposte ricevute. Se messi al servizio dei truffatori, potrebbero automatizzare completamente le frodi, gestendo centinaia di vittime in parallelo senza intervento umano.

La disinformazione sempre più sofisticata

Fotografie, audio, articoli e video possono essere utilizzati per diffondere notizie false, creare false emergenze o manipolare l'opinione pubblica. In questo contesto, la capacità di verificare le fonti prima di condividere qualsiasi contenuto diventa un atto di responsabilità civile, oltre che di autodifesa.



LA TRUFFA PIÙ ANTICA DEL MONDO



Le truffe esistono da quando esiste il linguaggio. Prima ancora che ci fosse internet, prima dei telefoni, prima della posta, c'era già qualcuno disposto a ingannare qualcun altro **facendo leva sulla sua buona fede, sulla sua paura** o sul suo desiderio di risolvere un problema in fretta.

L'Intelligenza Artificiale non ha cambiato questa storia, ma l'ha solo accelerata.

Oggi i criminali hanno a disposizione **strumenti che rendono le loro menzogne più credibili**, più scalabili e più difficili da smascherare.

Il meccanismo, però, è rimasto identico: trovare il momento in cui sei distratto, spaventato o di fretta, e approfittarne.



La buona notizia è che anche la difesa funziona allo stesso modo da sempre: non dipende dalla tecnologia che usi, dal telefono che hai in tasca o dal browser che preferisci. Dipende da un solo gesto: **fermarsi un momento prima di agire.**

Informarsi è la prima forma di difesa, verificare prima di agire è la seconda, **parlare con qualcuno** è la terza. Ma tutte e tre nascono dallo stesso istinto: non lasciare che qualcun altro decida per te sotto pressione.

Queste pagine non hanno la pretesa di essere esaustive. Il fenomeno è in continua evoluzione, e nuovi **strumenti di frode vengono sviluppati ogni giorno.** L'obiettivo è fornire una bussola che funziona indipendentemente da come cambia il paesaggio intorno.

Una persona informata sarà sempre più difficile da ingannare. E questo, almeno, non cambierà.



Realizzato nell'ambito del progetto "CARE – Conosci, Scegli, Proteggi" finanziato dal MIMIT. D.D. 12 maggio 2025



UNC
CONSUMATORI.IT

 [instagram](#)  [facebook](#)