



Passepartout

per Consumatori Intelligenti

“DIFENDERSI DALLE FRODI”

Guida pratica per riconoscere
le truffe, proteggersi e
sapere cosa fare

*Truffe online,
telefoniche e
con intelligenza
artificiale*



Movimento Difesa del Cittadino
– Progetto “Passepartout, per
consumatori intelligenti”
Progetto finanziato dal MIMIT
– Art. 148 – L. 388/2000 – D.D.
12 maggio 2025

INTRODUZIONE

Perché questa guida ti riguarda



Caro lettore, cara lettrice,

le truffe non sono più quelle di una volta. Un tempo si riconoscevano da errori grossolani, grammatica sbagliata o toni poco credibili. **Oggi, grazie all'uso dell'intelligenza artificiale (IA)**, i truffatori possono clonare la voce di un familiare, creare un sito identico a quello della tua banca o inviare messaggi scritti in un italiano perfetto e personalizzato.

Questo non significa che sia diventato impossibile difendersi.

In concreto, significa imparare a riconoscere come operano oggi i truffatori e adottare alcune semplici abitudini di prudenza nella vita di tutti i giorni.

Non si tratta di diventare esperti di tecnologia. Basta adottare qualche semplice abitudine di prudenza, proprio come facciamo ogni giorno quando controlliamo di aver chiuso bene la porta prima di uscire.

Questa guida si rivolge a chi vuole usare internet e il telefono con più serenità, senza rinunciare ai benefici che offrono. I dati più recenti del Ministero dell'Interno mostrano che le persone over 65 sono spesso tra le più colpite da truffe online, telefoniche e porta a porta. Non per ingenuità, ma perché i truffatori le considerano interlocutori più disponibili alla fiducia o potenzialmente titolari di risparmi accumulati negli anni.

Non si tratta di essere ingenui o distratti. Molto spesso la differenza la fa semplicemente avere le informazioni giuste al momento giusto.

In queste pagine troverai spiegazioni chiare su come reagire se qualcosa ti sembra sospetto: cosa fare, a chi rivolgerti, quali passi compiere senza perdere tempo. Indicazioni concrete, pensate per essere applicate nella realtà, non solo lette.

Troverai anche un richiamo ai tuoi diritti e ai principali riferimenti istituzionali, così da sapere con precisione dove chiedere aiuto o come presentare una segnalazione.

L'idea è offrirti strumenti pratici, utili nella vita di tutti i giorni. Non formule complicate, ma punti fermi a cui fare riferimento quando serve.

Il mondo delle frodi è cambiato: L'inganno si fa sempre più sofisticato

Negli ultimi anni, i criminali hanno iniziato a usare strumenti di intelligenza artificiale facilmente accessibili. Questa tecnologia permette loro di creare inganni di qualità molto alta, difficili da riconoscere a prima vista.

PRIMA VS OGGI: UN ESEMPIO CHE FA RIFLETTERE

- **PRIMA:** arrivava una email piena di errori che fingeva di essere della tua banca.
- **OGGI:** arriva una telefonata con la voce identica a quella di tuo nipote, che ti dice di aver avuto un incidente e di aver bisogno di soldi subito. La voce è un **deepfake**, una copia artificiale creata partendo da brevi audio trovati online.

LE NUOVE MINACCE ABILITATE DALL'IA

1. DEEFAKE VOCALI

Clonazione della voce di una persona cara. Bastano pochi secondi di audio (presi da un video sui social o da una vecchia registrazione) per creare una voce molto convincente.

2. MESSAGGI IPER-PERSONALIZZATI

Email o SMS che sembrano scritti apposta per te, senza errori, con riferimenti alla tua città, alla tua banca o a servizi che usi davvero. L'IA analizza i dati che lasciamo in rete per costruire messaggi credibili.

3. CHATBOT TRUFFALDINI

Su siti web falsi, che imitano quelli di banche o di servizi pubblici, un assistente virtuale "gentile" dialoga con te e prova a farti rivelare le credenziali.

4. FRODI SENTIMENTALI "POTENZIATE"

Profili falsi sui social, con foto realistiche generate dall'IA, che avviano relazioni affettive per ottenere fiducia e, alla fine, denaro.

IL MESSAGGIO PIÙ IMPORTANTE È QUESTO:

Se un inganno ti sembra più credibile del solito, **non è colpa tua**. I truffatori hanno alzato l'asticella. Ma la buona notizia è che i **principi di difesa restano gli stessi**: diffidare delle urgenze, verificare sempre le informazioni e proteggere i propri dati personali. Vediamo come.

Impariamo a riconoscerle: Le truffe più diffuse



In questa sezione trovi delle **SCHEDE PRATICHE**.

Ogni scheda spiega:

- Come si presenta la truffa;
- I **CAMPANELLI D'ALLARME** a cui prestare attenzione;
- Le **AZIONI IMMEDIATE** da compiere.

2.1 LE TRUFFE "CLASSICHE" (sempre in azione)

PHISHING (email false) e **SMISHING** (SMS falsi)

COME SI PRESENTA

Ricevi un'email o un SMS che sembra provenire dalla tua banca, da Poste Italiane, dall'INPS o dall'Agenzia delle Entrate. Il messaggio parla di un problema urgente: un conto da sbloccare, un pacco fermo in giacenza, un rimborso fiscale da richiedere. Ti invita a cliccare su un link per "risolvere subito".

CAMPANELLI D'ALLARME

- Il tono è **ALLARMISTICO E URGENTE** ("il tuo account sarà sospeso entro 24 ore", "rispondi subito");
- Il mittente è sospetto (es. *supporto@posteitaliane-help.com* invece di un dominio ufficiale);
- Il link ti porta a una pagina che ti chiede di inserire **NOME UTENTE, PASSWORD, PIN O CODICI OTP**;
- Possono esserci errori di battitura o una grafica di bassa qualità, anche se oggi le truffe sono spesso molto ben fatte.



COSA FARE SUBITO

- 1. NON CLICCARE MAI** sul link presente nel messaggio;
- 2. NON RISPONDERE** e non chiamare eventuali numeri indicati nel testo;
- Se hai un dubbio, **ACCEDI AL SERVIZIO** (es. home banking) digitando tu stesso l'indirizzo nel browser o aprendo l'app ufficiale;
- 4. CANCELLA** il messaggio sospetto o segnalo come spam.

VISHING (truffe telefoniche)

COME SI PRESENTA

Ricevi una chiamata da qualcuno che si presenta come operatore della tua banca, delle forze dell'ordine, di un corriere o di un servizio tecnico (per il computer, lo smartphone, la TV). Ti dice che c'è un problema grave con il tuo conto o con il tuo dispositivo e che, per risolverlo, ha bisogno che tu gli dia dei dati o che installi un programma.

CAMPANELLI D'ALLARME

- Ti chiedono **CODICI DI SICUREZZA (OTP)**, password o di installare software di controllo remoto sul tuo dispositivo;
- Usano **PRESSIONI PSICOLOGICHE**: "se non lo fai adesso perdi tutti i soldi", "si tratta di un controllo urgente";
- A volte fingono di farti vincere un premio, ma ti chiedono prima il pagamento di "tasse" o "spese di gestione".

COSA FARE SUBITO

- 1. RIAGGANZIA CON CALMA.** Non devi nulla a chi ti chiama all'improvviso;
- 2. NON DARE MAI** informazioni personali, codici o permessi di accesso al tuo dispositivo;
- Se il problema può essere reale (es. banca), **CHIAMA TU** il numero ufficiale che trovi sul retro della carta o sul sito istituzionale.

CALL CENTER AGGRESSIVI E CONTRATTI NON RICHIESTI

COME SI PRESENTA

Ricevi telefonate insistenti per propositi offerte "imperdibili" su luce, gas,





telefono, internet, assicurazioni o servizi digitali. A volte dicono che stanno “migliorando” il tuo contratto esistente o che hai diritto a una promozione speciale.

CAMPANELLI D'ALLARME

- L'offerta sembra **TROPPO BELLA PER ESSERE VERA** (risparmi del 50%, costi azzerati, regali);
- L'operatore è molto **FRETTOLOSO**, ti fa domande complicate e ti spinge a dire “sì” più volte;
- Non ti inviano un preventivo scritto chiaro **PRIMA** dell'attivazione;
- Potrebbero usare spezzoni di registrazioni per far risultare un tuo consenso che non hai davvero dato.

COSA FARE SUBITO

- 1. NON DIRE “SÌ” ALLA LEGGERA** e non fornire dati del tuo documento o delle tue bollette se non vuoi cambiare contratto;
- 2.** Chiedi che ti mandino **TUTTA LA PROPOSTA PER ISCRITTO** (per email o posta) prima di prendere una decisione;
- 3.** Può capitare di accettare un'offerta al telefono o online e poi avere dei dubbi. In questi casi di contratti a distanza o sottoscritti fuori dai locali commerciali ricorda che il Codice del Consumo (Art. 52 e ss) riconosce un diritto di recesso/ripensamento entro 14 giorni, salvo specifiche eccezioni;
- 4.** Se invece ti accorgi che un contratto è stato attivato senza una tua volontà chiara e consapevole, non sei tenuto a pagare importi che non hai effettivamente accettato. In questi casi puoi chiedere chiarimenti al fornitore e, **SE NECESSARIO, SEGNALARE LA VICENDA ALLE AUTORITÀ COMPETENTI PERCHÉ VENGANO SVOLTE LE VERIFICHE DEL CASO.**

FALSO TECNICO/FALSO FUNZIONARIO (truffe porta a porta)

COME SI PRESENTA

Qualcuno suona al campanello e dice di essere un tecnico del gas, della luce, dell'acqua, o un addetto comunale. Sostiene che deve effettuare controlli obbligatori, sostituire contatori o verificare la sicurezza dell'impianto.

CAMPANELLI D'ALLARME

- Arriva **SENZA UN APPUNTAMENTO** che tu ricordi;
- Mostra tesserini di identificazione **POCO CHIARI O ILLEGGIBILI**;



- Insiste molto per entrare in casa, anche se sei solo;
- Chiede **PAGAMENTI IN CONTANTI** sul momento per “lavori urgenti”.

COSA FARE SUBITO

- 1. NON FAR ENTRARE NESSUNO** se non sei sicuro di chi sia;
2. Chiedi **NOME, COGNOME, AZIENDA E NUMERO DI MATRICOLA** del presunto tecnico;
- 3. CHIAMA IL NUMERO UFFICIALE** della società (reperito su bollette o sito ufficiale) per verificare se hanno davvero mandato qualcuno;
- 4.** Se qualcosa non ti convince o ti fa sentire in pericolo, non aprire la porta. Prenditi un momento, allontanati dall'ingresso **E CHIAMA IL 112 PER CHIEDERE AIUTO.**

2.2 LE NUOVE TRUFFE CHE SFRUTTANO L'INTELLIGENZA ARTIFICIALE

Qui le truffe diventano più sofisticate, ma i **SEGNALI DI ALLARME** restano riconoscibili.

SCHEDA 1 – LA TELEFONATA DEL FAMILIARE IN PERICOLO (DEEPPAKE VOCALE)

LO SCENARIO

Il telefono squilla. Rispondi e senti la voce, identica, di tuo figlio, tuo nipote o un parente stretto. Ti dice di essere in ospedale dopo un incidente, di aver rotto il telefono e di aver bisogno di soldi urgenti per una cauzione o per pagare cure mediche. Ti prega di non dirlo a nessuno per “non preoccupare gli altri”.

COME FUNZIONA

I truffatori clonano la voce del parente usando brevi audio trovati online o registrati.

Con l'IA, possono far dire a quella voce quasi qualunque cosa.

CAMPANELLI D'ALLARME

- **URGENZA E SEGRETEZZA:** “devi fare subito, non dirlo a nessuno”;
- **RICHIESTA DI PAGAMENTI POCO TRACCIABILI:** bonifici istantanei, ricariche di carte prepagate, metodi difficili da recuperare;
- **VOCE QUASI PERFETTA MA STORIA CONFUSA:** la voce può sembrare quella giusta, ma il racconto è poco chiaro o incoerente.



COSA FARE SUBITO

- 1. MANTIENI LA CALMA.** Il panico è il loro alleato;
- 2. NON INVIARE DENARO.** Nessun pagamento immediato;
- 3. CHIAMA TU** il familiare sul suo numero vero che hai in rubrica. Se non risponde, chiama un altro parente per verificare;
- 4.** Concorda in famiglia una **“PAROLA D’ORDINE”** da usare solo nelle vere emergenze, conosciuta solo dai familiari stretti.

SCHEDA 2 – L’ASSISTENTE VIRTUALE TROPPO “GENTILE” (CHATBOT IA SU SITI FALSI)

LO SCENARIO

Clicchi su un link ricevuto via email o SMS e arrivi su una pagina che sembra **IDENTICA AL SITO DELLA TUA BANCA O DELLE POSTE**. Si apre una chat: un assistente virtuale ti saluta, è molto cortese e ti dice che c’è un problema sul conto o su una spedizione.

Ti chiede di inserire i tuoi dati di accesso, il numero della carta e persino i codici OTP che ricevi via SMS per “bloccare la frode”.

COME FUNZIONA

Il sito è un clone del sito ufficiale. Il chatbot è un programma di IA che simula una conversazione umana e ti guida passo dopo passo a consegnare tutte le informazioni necessarie per svuotare il conto.

CAMPANELLI D’ALLARME

- **INDIRIZZO WEB (URL) SOSPETTO:** leggermente diverso dall’originale (es. aggiunta di parole, trattini, domini strani);
- **RICHIESTA DI OTP E PIN:** banca, Poste e altri servizi non chiedono mai codici OTP o PIN via chat, email o telefono;
- **PRESSIONE PER PROCEDERE SUBITO:** “il tempo sta per scadere”, “l’operazione è urgente”.

COSA FARE SUBITO

- 1. NON INSERIRE ALCUN DATO.** Non digitare username, password, PIN o codici;
- 2. CHIUDI IMMEDIATAMENTE** la pagina;



3. Accedi al servizio come fai di solito (digitando l'indirizzo o aprendo l'app ufficiale) per verificare se esista davvero un problema.

SCHEDA 3 – LA RELAZIONE ONLINE DIVENTATA PERICOLOSA (FRODE SENTIMENTALE EVOLUTA)

LO SCENARIO



Su un social network, su un sito di incontri o in una chat conosci una persona affidabile e affascinante. Inizia una relazione online fatta di messaggi premurosi, attenzioni, confidenze. Dopo qualche settimana o mese, emergono problemi: una malattia improvvisa, un viaggio per incontrarti che viene bloccato, un affare "sicuro" da concludere. La persona ti chiede aiuto economico, promettendo di restituire tutto.

COME FUNZIONA

I truffatori creano profili falsi con foto rubate o generate con l'IA. Possono usare messaggi predefiniti o strumenti automatici per portare avanti molte "relazioni" contemporaneamente (catfishing).

CAMPANELLI D'ALLARME

- **RELAZIONE TROPPO RAPIDA E INTENSA:** ti chiamano "amore", "anima gemella" in tempi brevissimi;
- **RIFIUTO COSTANTE DI INCONTRARSI DAL VIVO O IN VIDEOCHIAMATA:** ci sono sempre scuse perfette;
- **RICHIESTE DI DENARO:** prima piccole somme, poi importi più consistenti per emergenze, incidenti, problemi di lavoro;

COSA FARE

- 1. SII MOLTO PRUDENTE** con le relazioni nate solo online;
- Proponi una **VIDEOCHIAMATA:** se viene rifiutata sistematicamente, è un segnale forte;
- 3. NON INVIARE SOLDI** a persone che non hai mai incontrato di persona;
- Parla della situazione con un familiare o un amico di fiducia: uno sguardo esterno aiuta a vedere meglio i rischi;
- 5.** Blocca il contatto e segnala il profilo alla piattaforma.



La tua “CASSETTA DEGLI ATTREZZI” per la sicurezza quotidiana

Ora che conosci le principali truffe, vediamo le **REGOLE PRATICHE** da mettere in atto ogni giorno per proteggerti.

3.1 LE 4 REGOLE D'ORO (VALIDE PER TUTTO)

1. DIFFIDA SEMPRE DELLE URGENZE

La fretta è l'arma principale dei truffatori. Una banca o un ente pubblico non ti obbligano a decidere in due minuti. Se ti mettono pressione, fermati e verifica;

2. VERIFICA SEMPRE IN AUTONOMIA

Se ricevi un messaggio o una chiamata allarmante:

- Non usare i numeri o i link presenti nel messaggio;
- Cerca tu il numero ufficiale sul sito dell'ente, su una bolletta o sul retro della carta;
- Chiama tu per chiedere conferma.

3. I TUOI CODICI SONO COME LE CHIAVI DI CASA: NON DARLI MAI A NESSUNO

- Password, PIN, codici OTP vanno custoditi con grande attenzione;
- Nessun operatore legittimo (banca, Poste, forze dell'ordine, gestori di servizi) ti chiederà mai questi codici per telefono, chat o email.

4. CONTROLLA COSA CONDIVIDI ONLINE

- Limita la visibilità dei tuoi post sui social;
- Evita di pubblicare informazioni come indirizzo di casa, periodo in cui sei in vacanza, dettagli su familiari, documenti o tessere.

3.2 DIFESA SPECIFICA CONTRO LE TRUFFE CON IA

- **CONTRO I DEEFAKE VOCALI:** oltre alla “parola d'ordine”, ricorda che una vera emergenza non ti vieta di chiamare un altro familiare per verificare. Se ti dicono di non farlo, è un segnale di pericolo;

- **CONTRO IL PHISHING EVOLUTO:** attiva **L'AUTENTICAZIONE A DUE FATTORI (2FA)** sui servizi principali (email, home banking, SPID). Anche se qualcuno scopre la tua password, senza il secondo codice non potrà accedere;
- **CONTRO LE RELAZIONI ONLINE SOSPETTE:** fidati dei segnali di disagio. Se qualcosa non ti torna, parlane con qualcuno di cui ti fidi.

3.3 IMPOSTAZIONI DI SICUREZZA ESSENZIALI (SMARTPHONE E COMPUTER)

Prenditi un po' di tempo per verificare questi punti:

1. PASSWORD FORTI E DIVERSE TRA LORO

Usa frasi lunghe, facili da ricordare per te ma difficili da indovinare (es. "LaMiaGattaAdoraIlSole!"), evitando di usare sempre la stessa password ovunque;

2. AGGIORNAMENTI AUTOMATICI ATTIVI

Assicurati che il sistema operativo (Windows, Android, iOS) e le app, soprattutto quelle bancarie, si aggiornino automaticamente;

3. BACKUP REGOLARE DEI DATI

Salva foto e documenti importanti su un supporto esterno o su un servizio cloud affidabile. Così, anche in caso di attacco informatico, non perderai i tuoi ricordi;

4. BLOCCO SCHERMO SEMPRE ATTIVO

Usa PIN, password, impronta digitale o riconoscimento facciale per sbloccare il telefono e il computer.



Cosa fare se pensi di essere caduto in UNA TRUFFA



Non farti prendere dal panico e non sentirti in colpa. **LE TRUFFE SONO PROGETTATE DA PROFESSIONISTI.**

Quello che conta è **AGIRE SUBITO, CON ORDINE.**

4.1 HAI INVIATO DENARO O DATI SENSIBILI?

1. CHIAMA IMMEDIATAMENTE LA TUA BANCA O L'EMITTENTE DELLA CARTA.

Spiega cosa è successo e chiedi di:

- bloccare carte e operazioni sospette;
- verificare la possibilità di annullare bonifici o transazioni non autorizzate.

2. CAMBIA SUBITO LE PASSWORD.

Inizia dalla casella email principale, poi passa a home banking, social, altri servizi.

3. RACCOGLI E CONSERVA TUTTE LE PROVE.

- Screenshot di email, SMS, chat;
- Numeri di telefono dei chiamanti;
- Estratti conto con i movimenti sospetti;

4. PRESENTA DENUNCIA ALLA POLIZIA POSTALE O ALLE ALTRE FORZE DI POLIZIA.

Puoi farlo tramite il sito del **COMMISSARIATO DI PS ONLINE** oppure recandoti in commissariato o in questura. Portando le prove aiuti le indagini e tuteli meglio i tuoi diritti;

4.2 SOSPETTI UN FURTO DI IDENTITÀ DIGITALE (SPID, EMAIL, SOCIAL)?

1. BLOCCA L'ACCESSO.

- Per SPID: accedi al sito del tuo gestore di identità digitale (es. fornitori SPID) e usa le funzioni per sospendere o revocare le credenziali, poi contatta l'assistenza;

- Per email e social: usa la funzione “password dimenticata” e imposta una nuova password forte. Controlla anche i recapiti di recupero (telefono, email secondarie).

2. SEGNALA ALLE PIATTAFORME

Se ci sono profili falsi a tuo nome o se il tuo account è stato usato per truffare altre persone, segnala subito il problema ai gestori del servizio;

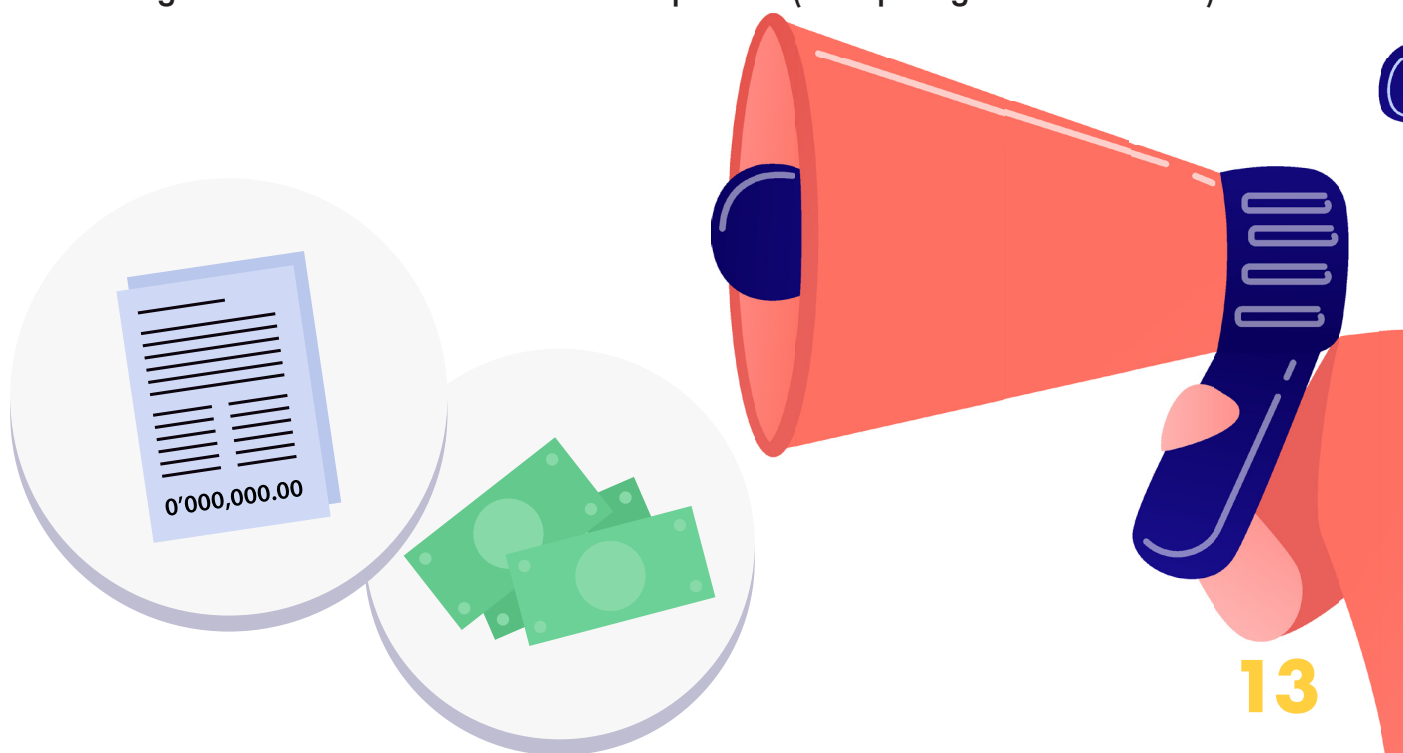
3. VALUTA UNA SEGNALAZIONE AL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI.

Se i tuoi dati personali sono stati usati o diffusi in modo grave, puoi presentare un reclamo tramite il sito del Garante Privacy;

4.3 HAI ATTIVATO PER SBAGLIO UN CONTRATTO (LUCE, GAS, TELEFONIA)?

Conoscere i tuoi diritti è fondamentale:

- Per **I CONTRATTI CONCLUSI A DISTANZA** (telefono, internet), il **CODICE DEL CONSUMO** prevede in generale un **DIRITTO DI RECESSO ENTRO 14 GIORNI** dall’adesione, salvo specifiche eccezioni previste dalla legge;
- In caso di **FORNITURE NON RICHIESTE** di beni o servizi, il Codice del Consumo stabilisce che il consumatore **NON È TENUTO AD ALCUNA PRESTAZIONE CORRISPETTIVA**: in pratica, **NON DEVE PAGARE** ciò che non ha richiesto in modo chiaro;
- Se ritieni di essere vittima di una pratica commerciale scorretta o di un contratto attivato in modo ingannevole, puoi:
 - Contestare per iscritto al fornitore (raccomandata o PEC);
 - Rivolgerti a un’associazione di consumatori come MDC - Movimento Difesa del Cittadino;
 - Segnalare il caso alle Autorità competenti (vedi paragrafo successivo).



Dove trovare aiuto: I tuoi alleati

Non devi affrontare tutto da solo. Esistono istituzioni e servizi nati proprio per aiutare i cittadini.

Oltre ai comandi delle Forze dell'ordine (*Polizia, Carabinieri, Guardia di Finanza*) più vicini, di seguito i dettagli di contatto delle principali Autorità a cui è possibile rivolgersi.

AUTORITÀ GARANTE DELLA CONCORRENZA E DEL MERCATO (AGCM)

Indirizzo Postale: Piazza G. Verdi 6/a, 00198 Roma,

Email: protocollo@agcm.it

Sito web: www.agcm.it

AUTORITÀ PER LE GARANZIE NELLE COMUNICAZIONI (AGCOM)

Indirizzo postale: Via Isonzo 21/B, 00198 Roma, Italia

Email: segreteria.generale@agcom.it

Sito web: www.agcom.it

AGENZIA PER L'ITALIA DIGITALE (AGID)

Indirizzo postale: Via Liszt, 21, 00144 Roma

Email: protocollo@agid.gov.it

Sito web: www.agid.gov.it

AGENZIA PER LA CYBERSICUREZZA NAZIONALE (Il DDL sulla IA del 23.04.24 ha delegato alla ACN funzioni in materia di tutela dei cittadini non ancora attive si consiglia il contatto solo per informazioni)

Indirizzo postale: Via di Santa Susanna n. 15 00198 Roma

Email: info@acn.gov.it

Sito web: www.acn.gov.it



COMMISSIONE NAZIONALE PER LE SOCIETÀ E LA BORSA (CONSOB)

Indirizzo postale: Via G. B. Martini, 3, 00198 Roma, Italia

Email: consob@pec.consob.it

Sito web: www.consob.it

BANCA D'ITALIA

Indirizzo postale: Via Nazionale, 91, 00184 Roma, Italia

Email: urp@bancaditalia.it

Sito web: www.bancaditalia.it

Effettuare una segnalazione è un processo semplice ma fondamentale.

Può essere fatto tramite email, utilizzando l'indirizzo PEC (*Posta Elettronica Certificata*) per una comunicazione sicura, o tramite posta tradizionale.

Ricordate di fornire tutte le informazioni pertinenti alla vostra segnalazione, inclusi eventuali dettagli sulla truffa, documentazione di supporto e le vostre informazioni di contatto per eventuali seguiti.

MOVIMENTO DIFESA DEL CITTADINO (MDC)

• **NUMERO VERDE NAZIONALE MDC:** 800.16.16.47

• **EMAIL:** reclami@mdc.it

• **SITO WEB:** www.mdc.it – qui puoi trovare informazioni e contatti degli sportelli territoriali.

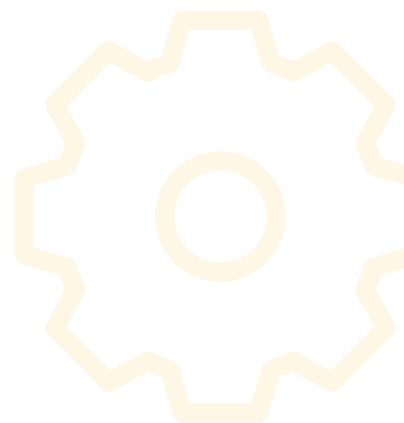
IL RUOLO DI MDC

MDC è un'associazione di consumatori che ti può:

- Aiutare a capire cosa è successo;
- Supportare nella scrittura di reclami verso aziende e gestori;
- Affiancare nella predisposizione di segnalazioni alle Autorità (Polizia Postale, AGCM, Garante Privacy).

MDC **NON SOSTITUISCE LE AUTORITÀ**, ma ti aiuta a usare al meglio i tuoi diritti e gli strumenti a tua disposizione.

APPENDICE – PICCOLO GLOSSARIO E DOMANDE FREQUENTI (FAQ)



GLOSSARIO (PER ORIENTARSI MEGLIO)

- **PHISHING:**

Truffa via email, con cui si cerca di “pescare” (to fish) i tuoi dati.

- **SMISHING:**

Truffa via SMS (SMS + phishing).

- **VISHING:**

Truffa via voce, cioè per telefono (voice + phishing).

- **DEEPFAKE:**

Contenuto (audio o video) falso ma molto realistico creato con l'intelligenza artificiale.

- **OTP (ONE TIME PASSWORD):**

Codice di sicurezza temporaneo che ricevi via SMS o app; serve a confermare un'operazione e deve restare segreto.

- **2FA / MFA (AUTENTICAZIONE A DUE/MULTI FATTORI):**

Sistema di sicurezza che richiede due o più prove di identità (es. password + codice OTP) per accedere a un servizio.

- **FRODE SENTIMENTALE:**

Truffa che sfrutta un finto rapporto affettivo per ottenere denaro o dati.



DOMANDE FREQUENTI

D: COME FACCIO A ESSERE SICURO AL 100% CHE UNA VOCE SIA UN DEEPPAKE?

R: Non devi essere un tecnico: ti basta seguire una regola semplice. Se c'è **URGENZA, PAURA E RICHIESTA DI SOLDI, VERIFICA SEMPRE CHIAMANDO TU** il numero vero del familiare o di un altro parente. Questa procedura di sicurezza è molto efficace.

D: LA MIA BANCA PUÒ CHIEDERMI IL CODICE OTP CHE MI ARRIVA VIA SMS?

R: NO. MAI. Il codice OTP serve solo a te per confermare operazioni che stai effettuando personalmente. Se qualcuno te lo chiede al telefono, via email o chat, è un segnale certo di truffa.

D: COSA DEVO PORTARE PER FARE UNA DENUNCIA ALLA POLIZIA POSTALE?

R: Porta:

- 1.** Documento di identità;
- 2.** Screenshot stampati o salvati su supporto digitale (email, chat, SMS);
- 3.** Numeri di telefono da cui sei stato contattato;
- 4.** Estratti conto con movimenti sospetti;
- 5.** Qualsiasi documento utile a ricostruire i fatti (ad esempio, contratti o comunicazioni aziendali).

D: MI SENTO TROPPO IN LÀ CON GLI ANNI PER IMPARARE COME FUNZIONA IL DIGITALE. HA SENSO PROVARCI?

R: La sicurezza non è una questione di età, ma di abitudini. Le regole principali di questa guida – non cliccare sui link sospetti, non dare codici per telefono, verificare facendo tu le chiamate – sono semplici e valgono anche per il telefono di casa. Puoi chiedere aiuto a un familiare o a uno sportello MDC per le impostazioni più tecniche.

OGNI PASSO IN PIÙ TI RENDE PIÙ PROTETTO.



UN ULTIMO MESSAGGIO PER TE

Leggere questa guida è già un passo importante per proteggerti.

Ricorda:

- **LA PRUDENZA NON È DIFFIDENZA, È SAGGEZZA;**
- **CHIEDERE AIUTO NON È UNA DEBOLEZZA, È UNA FORZA;**
- **LE ISTITUZIONI E LE ASSOCIAZIONI DI TUTELA,
COME IL MOVIMENTO DIFESA DEL CITTADINO, ESISTONO
PER ESSERE AL TUO FIANCO.**

Conserva questa guida, condividila con amici e familiari. La sicurezza è più forte
quando siamo **INFORMATI E UNITI**



Movimento Difesa del Cittadino – Progetto “Passepartout, per consumatori intelligenti”
Progetto finanziato dal MIMIT – Art. 148 – L. 388/2000 – D.D. 12 maggio 2025



Movimento Difesa del Cittadino
– Progetto “Passepartout, per
consumatori intelligenti”
Progetto finanziato dal MIMIT
– Art. 148 – L. 388/2000 – D.D.
12 maggio 2025