DIRITTI AL CENTRO

MANUALE COMPLETO PER RICONOSCERE, PREVENIRE E AFFRONTARE LE FRODI DIGITALI

GUIDA ANTITRUFFE ONLINE

A CURA DELL'AVV. FRANCESCO LUONGO - ESPERTO IN DIRITTO DEI CONSUMATORI

"FINANZIATO NELL'AMBITO DEL PROGRAMMA DELLA REGIONE UMBRIA CON FONDI MIMIT — DM 31/07/2024 E DD 14/2/2025"

Premessa e obiettivi

Questa Guida Anti truffe Online rappresenta un'opera di informazione pubblica realizzata dal Movimento Difesa del Cittadino di Perugia APS (MDC Umbria) . L'iniziativa si inserisce nel più ampio Programma Generale di Intervento della Regione Umbria - Rete degli Sportelli del Consumatore 2025/2026 , "finanziato nell'ambito del Programma della Regione UMBRIA, con fondi MIMIT - DM 31/07/2024 e DD 14/02/2025.

Negli ultimi anni, i nostri sportelli hanno registrato un notevole aumento delle segnalazioni relative a frodi digitali. Questa guida nasce quindi da un'esperienza concreta e diretta, maturata attraverso plurimi casi trattati. Non si tratta di teoria, ma di conoscenza pratica derivata da situazioni reali vissute dai nostri concittadini.

I nostri obiettivi :

1. Fornire una mappatura completa delle truffe digitali più diffuse

2. Offrire strumenti pratici per il riconoscimento preventivo

3. Indicare procedure chiare da seguire in caso di vittimizzazione

4. Creare una cultura della prevenzione digitale

Il panorama delle frodi digitali: dati e tendenze

L'EVOLUZIONE DELLA MINACCIA

Il fenomeno delle truffe online non è statico, ma in continua evoluzione. Se fino a cinque anni fa le frodi erano relativamente semplici da individuare, oggi i criminali informatici utilizzano tecniche sofisticate che sfruttano:

- Intelligenza Artificiale per creare messaggi sempre più convincenti
- Dati personali già compromessi in precedenti violazioni (data breach)
- Analisi comportamentali per personalizzare gli attacchi
- Tecnologie di spoofing avanzate che rendono quasi indistinguibili le comunicazioni false

DATI ALLARMANTI DALLA NOSTRA ESPERIENZA DIRETTA

Dall'analisi dei casi gestiti:

- 62% delle vittime aveva un'età superiore ai 55 anni
- 78% delle truffe avveniva tramite smartphone
- 43% dei casi riguardava perdite superiori a 1.000€
- Solo 22% delle vittime era riuscito a recuperare parzialmente il denaro
- 91% dei casi avrebbe potuto essere prevenuto con maggiore informazione

La psicologia della truffa: come i truffatori ci ingannano

INGEGNERIA SOCIALE: L'ARTE DELLA MANIPOLAZIONE

I criminali informatici non sono solo tecnici, ma psicologi pratici. Studiano le nostre reazioni e sfruttano:

1. IL PRINCIPIO DELL'URGENZA

Creano falsi deadline: "Devi agire entro 2 ore o il tuo account sarà bloccato". Il tempo limitato impedisce la riflessione critica.

2. L'AUTORITÀ PERCEPITA

Si presentano come: poliziotti, bancari, tecnici di società note, rappresentanti di enti pubblici, rappresentanti della tutela consumatori. L'uniforme (anche digitale) crea fiducia automatica.

3. LA PAURA E L'ANSIA

"Ci sono stati accessi anomali al tuo conto", "Il tuo computer è infetto", "Devi pagare una multa evitabile". "Devi agire subito per impedire operazioni fraudolente sul tuo conto". La paura spegne il pensiero razionale.

4. L'ECCITAZIONE E L'AVARIZIA

"Vinci un premio!", "Opportunità di investimento unica!", "Prodotto a prezzo irripetibile!". L'emozione positiva annebbia la cautela.

5. LA RECIPROCITÀ

Ti offrono "aiuto gratuito" (falso) per poi chiederti qualcosa in cambio. Il senso di obbligo morale ci spinge a corrispondere.

Le truffe digitali piu' diffuse

SEZIONE 1: TRUFFE BASATE SU COMUNICAZIONE (PHISHING, SMISHING, VISHING)

1.1 PHISHING CLASSICO VIA EMAIL

Descrizione: Email fraudolente che imitano istituzioni finanziarie, servizi pubblici, piattaforme di e-commerce.

Varianti evolute :

- Spear Phishing : Attacco personalizzato con i tuoi dati reali (nome, cognome, riferimenti)
- Whaling : Targeting di dirigenti o figure professionali di alto livello
- Clone Phishing : Duplicazione di email legittime ricevute in precedenza

Esempi concreti dai nostri casi:

> *"Il Signor Bianchi ha ricevuto un'email perfettamente identica a quelle dell'Agenzia delle Entrate, con il suo codice fiscale e riferimento alla dichiarazione dei redditi dell'anno precedente. Il link portava a un portale clone dove ha inserito le sue credenziali SPID."*

Indicatori di phishing:

1. ✅ Indirizzo mittente sospetto (es: `supporto@agenzia-entrate-italia.com` invece di `@agenziaentrate.it`)
2. ✅ Saluto generico ("Egregio Cliente" invece del tuo nome)
3. ✅ Errori di grammatica o sintassi insolite
4. ✅ Link che mostrano un testo ma puntano a URL diversi (passa il mouse sopra SENZA cliccare)
5. ✅ Richiesta di azione urgente e minacciosa

Attacchi "Man-in-the-Middle" e "Man-in-the-Browser"

Oltre alle tecniche di phishing, esistono attacchi più avanzati in cui il truffatore non si limita a ingannare la vittima, ma si inserisce direttamente nella comunicazione tra l'utente e il servizio utilizzato (ad esempio la banca).

Nel cosiddetto Man-in-the-Middle, l'aggressore intercetta o modifica i dati scambiati, spesso sfruttando reti Wi-Fi pubbliche o non protette.

Nel Man-in-the-Browser, invece, un malware infetta il browser dell'utente e consente di manipolare operazioni e transazioni anche su siti legittimi e protetti.

Questi attacchi sono spesso la fase successiva a un phishing riuscito e rendono ancora più importante mantenere dispositivi aggiornati, evitare reti non sicure e diffidare di comunicazioni inattese.

1.2 SMISHING (SMS PHISHING)

Descrizione: Messaggi SMS che sfruttano situazioni quotidiane: pacchi, multe, problemi bancari, codici di sicurezza.

Nuove tendenze:
- Falsi codici di sicurezza OTP : "Il tuo codice Amazon è 548921" (ma non hai richiesto nulla)
- Alert di sicurezza falsi : "Accesso anomalo al tuo account Google da Roma"
- Promozioni ingannevoli : "Hai vinto un buono da 50€. Clicca qui per ritirarlo"
- Caso reale :

"Una ragazza ha ricevuto un SMS apparentemente dal corriere: 'Il tuo pacco non è stato consegnato. Per programmare nuova consegna: [link].' Cliccando, hanno installato un malware che ha monitorato le loro operazioni bancarie online."*

1.3 VISHING (PHISHING VOCALE)

Descrizione: Chiamate telefoniche fraudolente che spesso utilizzano spoofing del numero (il chiamante sembra un numero ufficiale).

Scenari comuni:
1. Falso tecnico informatico: "Sono il supporto Microsoft/Apple. Il tuo computer ha un virus"
2. Falso operatore bancario: "Siamo della sicurezza della banca. Ci sono movimenti sospetti"
3. Falso agente di Polizia: "Sono della Polizia Postale. Abbiamo intercettato un pacco a tuo nome con documenti falsi"

Tecnica della "conferma passiva" : "Per verificare che sia lei, mi dica se ha una carta che termina con 1234" (in realtà stanno chiedendo conferma dei dati che già hanno)

SEZIONE 2: TRUFFE COMMERCIALI E D'ACQUISTO

2.1 FALSI E-COMMERCE

Come riconoscere un sito truffaldino :

Analisi URL e dominio :

- Controlla l'età del dominio (tools gratuiti: whois.domaintools.com)
- Diffida dei domini con trattini multipli: `miglior-prezzo-iphone14.it`
- Attenzione alle estensioni sospette: `.shop`, `.best`, `.deals` (non sono automaticamente truffe, ma richiedono verifica)

Indicatori di affidabilità:

- ✅ P.IVA italiana verificabile
- ✅ Indirizzo fisico reale (verifica su Google Maps)
- ✅ Recensioni su piattaforme terze (Trustpilot, Google My Business)
- ✅ Condizioni di vendita, reso e privacy chiare e complete
- ✅ Certificati SSL validi (lucchetto verde nella barra degli indirizzi)

Caso studio:

"Il sito 'TechDiscount24' offriva iPhone 15 Pro a 599€ (prezzo di listino: 1.199€). Il sito sembrava professionale, ma: P.IVA inesistente, indirizzo corrispondeva a un garage abbandonato, recensioni copiate da altri siti."

2.2 ANNUNCI FALSI SU MARKETPLACE

Piattaforme a rischio: Subito.it, Facebook Marketplace, eBay, Vinted

Tecniche comuni:

1. Prezzo troppo vantaggioso
2. Venditore che spinge per concludere fuori piattaforma
3. Richiesta di pagamento anticipato totale o parziale
4. Scuse per non fare incontri di persona ("sono fuori città", "malato", "lavoro turni")

Regola d'oro : Pagamento solo tramite metodi protetti della piattaforma e ritiro di persona quando possibile.

2.3 ABBONAMENTI TRAPPOLA E VENDITE AGGIUNTE

Descrizione: Offerte “gratuite” che si trasformano in abbonamenti costosi, spesso con condizioni nascoste.

Esempi:

- “30 giorni gratis” che richiedono carta di credito e si rinnovano automaticamente
- Servizi a “costo simbolico” che nascondono costi ricorrenti elevati
- Spunte pre-selezionate per servizi aggiuntivi durante gli acquisti online

Come difendersi :

1. Leggere SEMPRE le condizioni, soprattutto in piccolo
2. Usare carte prepagate con importo limitato per le prove gratuite
3. Impostare promemoria prima della scadenza del periodo gratuito
4. Controllare regolarmente gli estratti conto per individuare addebiti non autorizzati

SEZIONE 3: TRUFFE FINANZIARIE E SUGLI INVESTIMENTI

3.1 INVESTIMENTI FRAUDOLENTI

Caratteristiche comuni :

- Rendimenti garantiti e superiori al mercato (“20% mensile garantito”)
- Nessuna licenza CONSOB o autorità di vigilanza equivalente
- Piattaforme proprietarie non verificabili
- Pressure selling (“l’offerta scade tra 10 minuti”)

Criptovalute e Trading :

“Sig. Maurizio, 68 anni, ha investito 20.000€ in una ‘piattaforma di trading automatico su criptovalute’ promossa da un ‘consulente’ conosciuto su WhatsApp. Dopo apparenti guadagni iniziali, la piattaforma è scomparsa”.

Verifiche obbligatorie:

1. Controlla su CONSOB se l’intermediario è autorizzato
2. Cerca il nome della società + “truffa” o “recensioni”
3. Diffida delle piattaforme che non permettono prelievi facili
4. Ricorda: se sembra troppo bello per essere vero, probabilmente non è vero

3.2 FALSI PRESTITI E FINANZIAMENTI

Modus operandi:

1. Offerta di prestito “sicuro e immediato” senza garanzie
2. Richiesta di pagamento anticipato per “spese di pratica” o “assicurazione”
3. Utilizzo di documenti falsi o clonati
4. Minacce in caso di mancato pagamento delle “commissioni”

Legge fondamentale: In Italia, è vietato chiedere pagamenti anticipati per l’istruzione di pratiche di finanziamento .

SEZIONE 4: TRUFFE RELAZIONALI E SOCIALI

4.1 CATFISHING E TRUFFE SENTIMENTALI

Descrizione: Creazione di profili falsi su App di Dating o Social per stabilire relazioni sentimentali finalizzate a estorcere denaro.

Fasi tipiche:

1. Innamoramento rapido (love bombing)
2. Storie drammatiche (malattie, problemi finanziari, emergenze)
3. Richiesta di aiuto economico (spesso con promessa di rimborso)
4. Scomparsa dopo il trasferimento di denaro

Segnali d'allarme:

- Si rifiuta di fare videochiamate
- Ha sempre scuse per non incontrarsi
- La sua storia ha elementi inverosimili
- Chiede denaro, anche piccole somme iniziali

4.2 FALSI PROFILI SOCIAL E IMPERSONIFICAZIONE

Come avviene:

- Clonazione di profili esistenti (rubano foto e dati)
- Creazione di profili falsi di figure autorevoli
- Gruppi Facebook con offerte esclusive

La prevenzione attiva: strumenti e comportamenti

STRUMENTI TECNOLOGICI ESSENZIALI

1. SISTEMI DI PROTEZIONE BASE

- Antivirus aggiornato (anche su smartphone)
- Firewall attivo
- Aggiornamenti automatici di sistema operativo e applicazioni
- Backup automatici dei dati importanti (regola 3-2-1: 3 copie, 2 supporti diversi, 1 fuori sede)

2. GESTIONE DELLE PASSWORD

Cosa NON fare:

- Usare la stessa password per più servizi
- Usare password semplici (“123456”, “password”, “qwerty”)
- Conservare password in chiaro su file del computer
- Usare informazioni personali (date di nascita, nomi di figli)

Cosa FARE:

- Usare un password manager (Bitwarden, LastPass, 1Password)
- Creare password lunghe (minimo 12 caratteri) con mix di caratteri
- Attivare l’autenticazione a due fattori (2FA) ovunque possibile
- Cambiare password dopo notizie di data breach

3. CONFIGURAZIONI DI PRIVACY E SICUREZZA

Su Social Network:

- Limitare la visibilità dei profili
- Non condividere informazioni personali sensibili
- Verificare le impostazioni dei tag e delle menzioni
- Controllare periodicamente le app collegate all’account

Su Smartphone:

- Utilizzare blocchi schermo (PIN, impronta, riconoscimento facciale)
- Verificare i permessi delle app
- Disattivare Bluetooth e Wi-Fi quando non servono
- Utilizzare reti VPN su reti Wi-Fi pubbliche

COMPORTAMENTI PROATTIVI QUOTIDIANI

1. CULTURA DELLA VERIFICA

Prima di cliccare, inviare denaro o fornire dati:

1. FERMATI - Non reagire d'impulso
2. RIFLETTI - È plausibile? Perché mi contattano così?
3. VERIFICA - Contatta l'ente tramite canali ufficiali noti
4. CONFRONTA - Cerca esperienze simili online

2. GESTIONE DELLE COMUNICAZIONI

- Email : Non aprire allegati da mittenti sconosciuti
- SMS : Non rispondere a messaggi sospetti
- Telefono : In caso di dubbio, riattacca e richiama il numero ufficiale
- Social : Non accettare richieste di amicizia da sconosciuti con storie drammatiche

3. EDUCAZIONE CONTINUA

- Seguire siti istituzionali di cybersecurity (Cert-PA, Polizia Postale)
- Partecipare a webinar e incontri informativi
- Condividere esperienze (positive e negative) con familiari e amici
- Aggiornarsi sulle nuove tipologie di truffa

Protezione dei soggetti vulnerabili

PER ANZIANI E PERSONE MENO DIGITALI

1. Semplificare senza sostituire: Aiutarli a fare da soli, non fare al posto loro
2. Creare reti di supporto: Familiari, amici, volontari che possano aiutare
3. Strumenti semplificati: Configurare dispositivi con impostazioni di sicurezza massima
4. Comunicazione chiara: Spiegare i rischi con esempi concreti, non tecnicismi

PER GENITORI E MINORI

1. Controllo parentale equilibrato: Non solo blocchi, ma educazione
2. Dialogo aperto : Parlare di rischi senza creare panico
3. Esempi pratici : Mostrare casi reali adatti all'età
4. Regole familiari : Orari di utilizzo, dispositivi in spazi comuni

Cosa fare se si è vittima di una truffa

FASE 1: REAZIONE IMMEDIATA (PRIME 24 ORE)

1.1 BLOCCO DEGLI STRUMENTI FINANZIARI

Ordine di priorità :

1. Carte di credito/debito : Chiamare immediatamente il numero verde sul retro
2. Conti correnti : Contattare la banca per bloccare movimenti sospetti
3. Servizi di pagamento online (PayPal, Satispay, etc.): Segnalare la frode
4. Carte prepagate : Bloccarle se collegate a servizi o conti

Cosa comunicare alla banca :

- Data e ora della transazione fraudolenta
- Importo
- Descrizione di come è avvenuta la truffa
- Richiesta formale di blocco e contestazione
- Richiesta di storno e riaccredito delle somme

1.2 PROTEZIONE DELL'IDENTITÀ DIGITALE

Azioni immediate:

1. Cambiare tutte le password compromesse o potenzialmente compromesse
2. Attivare/disattivare 2FA su account importanti
3. Controllare attività sospette su Google Account, Facebook, etc.
4. Avvisare contatti se l'account è stato usato per inviare spam

1.3 RACCOLTA SISTEMATICA DELLE PROVE

Documentare tutto :

- Screenshot di conversazioni, pagine web, transazioni
- Copie di email, SMS, messaggi
- Registrazioni di chiamate (se consentito dalla legge)
- Ricevute di pagamento, bonifici, ricariche
- Note cronologiche di quanto accaduto

Organizzare le prove :

Creare una cartella con:
/Truffa_[Data]/

--- Documenti/

--- Screenshot/

--- Comunicazioni/

--- Ricevute/

--- Cronologia.txt

FASE 2: DENUNCIA E SEGNALAZIONI FORMALI

2.1 DENUNCIA ALLE FORZE DELL'ORDINE

Dove andare :

1. Polizia Postale e delle Comunicazioni (prioritaria per reati informatici)
2. Commissariato di Polizia più vicino
3. Stazione dei Carabinieri

Cosa portare :

- Documento di identità
- Tutte le prove raccolte
- Dettagli dei danni subiti
- Eventuali testimoni

Cosa aspettarsi :

- Ricevuta di denuncia/querela
- Numero di protocollo
- Possibile richiesta di ulteriori informazioni

2.2 SEGNALAZIONI A AUTORITÀ DI SETTORE

Nel caso in cui siate vittime di una truffa o sospettiate di essere stati oggetto di pratiche commerciali scorrette, è essenziale segnalarlo alle autorità competenti. Questo non solo aiuta a proteggere voi stessi, ma anche altri consumatori che potrebbero trovarsi in situazioni simili.

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**

2.3 SEGNALAZIONI A PIATTAFORME ONLINE

Importante: Segnalare profili falsi, siti truffaldini, annunci ingannevoli alle piattaforme che li ospitano:
- Google : Segnalazione siti di phishing
- Facebook/Instagram : Segnalazione profili falsi
- WhatsApp : Segnalazione numeri per truffe
- Siti di e-commerce : Segnalazione venditori truffaldini

FASE 3: RECUPERO E TUTELA

3.1 RECUPERO ECONOMICO

Possibilità di rimborso :

- Carte di credito : Chargeback entro termini (solitamente 120 giorni)
- Bonifici : Revoca possibile solo se ancora in lavorazione
- PayPal : Sistema di protezione acquirenti
- Assicurazioni : Alcune polizze coprono le frodi online

Tempi realistici :

- Blocco preventivo: Immediato
- Chargeback: 30-90 giorni
- Procedimenti legali: Mesi/anni

3.2 SUPPORTO PSICOLOGICO

Reazioni comuni dopo una truffa :

- Vergogna e imbarazzo
- Rabbia verso sé stessi o gli altri
- Ansia nell'utilizzo della tecnologia
- Difficoltà a fidarsi

Consigli :

- Parlare dell'accaduto con persone fidate
- Non colpevolizzarsi: i truffatori sono professionisti
- Considerare supporto psicologico se necessario
- Partecipare a gruppi di supporto per vittime

FASE 4: PREVENZIONE FUTURA

4.1 ANALISI DELL'ACCADUTO

Domande da porsi :

1. Quale segnale ho trascurato?
2. Cosa mi ha convinto a fidarmi?
3. Come posso riconoscere situazioni simili in futuro?
4. Quali strumenti di protezione mi mancavano?

4.2 IMPLEMENTAZIONE DI MISURE DI SICUREZZA

Basandosi sull'esperienza:

1. Rafforzare le password
2. Implementare 2FA ovunque possibile
3. Configurare alert di movimenti bancari
4. Istituire controlli familiari incrociati per transazioni importanti

Aspetti giuridici e tutele dalle truffe on line

QUADRO NORMATIVO DI RIFERIMENTO

REATI PRINCIPALI

1. Frode informatica (Art. 640-ter c.p.)
2. Accesso abusivo a sistema informatico (Art. 615-ter c.p.)
3. Detenzione e diffusione di codici di accesso (Art. 615-quater c.p.)
4. Falsificazione di siti web (Art. 491-bis c.p.)

TUTELE CIVILI

- Risarcimento del danno (patrimoniale e non patrimoniale)
- Restituzione dell'indebito
- Inibitoria (cessazione del comportamento illecito)

PROCEDURE CONCILIATIVE EXTRAGIUDIZIARIE

ARBITRATO BANCARIO FINANZIARIO (ABF)

Per controversie con banche e intermediari finanziari:

- Gratuito
- Decisione vincolante per la banca
- Tempi rapidi (circa 4 mesi)

CONCILIAZIONE PARITETICA

Per controversie con imprese:

- Mediata da organismi di conciliazione
- Possibilità di accordo vincolante
- Spesso gratuita o a costi contenuti

CLASS ACTION

Per danni derivanti da pratiche commerciali scorrette:

- Azione collettiva per gruppi di consumatori
- Maggiore forza negoziale
- Costi distribuiti

SPORTELLO DEL CONSUMATORE MDC DI BETTONA (PG)

La consulenza di primo contatto dell'esperto legale e/o del conciliatore dell'Associazione MDC Perugia APS è resa a titolo gratuito al consumatore, in quanto attività "Finanziata nell'ambito del programma della Regione UMBRIA con fondi MIMIT — DM 31/07/2024 e DD 14/2/2025"

Ubicazione:

Via Torgianese n. 19, Bettona (PG) - Presso Coworking Im.it

Contatti Multicanale :

- Telefono: 377 1251486
- WhatsApp : 371 4323964 (per messaggi, documenti, vocali)
- Email : mdc.perugia@libero.it
- Sito web: www.mdcumbria.it
- Facebook: www.facebook.com/movimentodifesacittadino.perugia

Orari di Ricevimento:

Lunedì: 11:00 – 15:00 (orario continuato)
Mercoledì: 15:00 – 19:00 (orario continuato)
Negli altri giorni, puoi contattarci telefonicamente, via email o WhatsApp

GUIDA ANTITRUFFE ONLINE

Movimento Difesa del Cittadino di Perugia APS • www.mdcumbria.it

“FINANZIATO NELL’AMBITO DEL PROGRAMMA DELLA REGIONE UMBRIA CON FONDI MIMIT — DM 31/07/2024 E DD 14/2/2025”