ADICONSUM
Associazione Difesa Consumatori APS
dal 1987
LAZIO, ROMA Capitale e RIETI

Difendersi dalle truffe

www.romaadiconsum.com

Finanziato con i fondi del 5X1000

Chi siamo

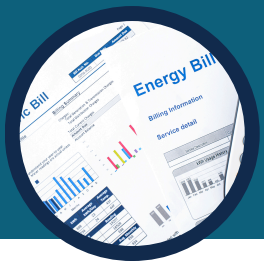
ADICONSUM
Associazione Difesa Consumatori APS
dal 1987
LAZIO, ROMA Capitale e RIETI

Adiconsum *è un'****associazione dei consumatori*** *riconosciuta dalla legge. Fa parte del* ***Consiglio Nazionale dei Consumatori e degli Utenti (CNCU)*** *presso il* ***Ministero dello sviluppo economico*** *ed è Associazione di* ***Promozione sociale****, approvata dal Ministero del lavoro e delle politiche sociali.*

Adiconsum Lazio, Roma capitale e Rieti *ne è la sua articolazione territoriale. Fa parte del* ***Consiglio Regionale dei Consumatori e degli Utenti (CRCU)*** *presso la Regione Lazio.*

Grazie alla sua rete di ***sportelli e al suo team di consulenti****, fornisce su tutto il territorio regionale* ***assistenza individuale e collettiva nei differenti ambiti del consumo.***

Servizi ai cittadini



Bollette luce e gas

Multe & tasse

Immobili

Sanità

Telefonia

Banche e Finanza

DIFENDERSI DALLE TRUFFE

Le truffe sono uno dei problemi più diffusi e **insidiosi nell'era digitale**, e ogni giorno **milioni di persone** in tutto il mondo ne diventano vittime. Che si tratti di **frodi telefoniche**, **email ingannevoli** o **siti web falsi**, i truffatori sono sempre più abili a manipolare le persone per ottenere denaro o informazioni sensibili.
In un'epoca in cui **la tecnologia e l'accesso a internet** sono parte integrante della nostra vita quotidiana, la consapevolezza è la **prima arma di difesa**. Le truffe possono assumere forme molto diverse: alcune sono veloci e di piccole entità, mentre altre sono complesse e possono portare a **gravi danni economici**. Inoltre, non solo le persone comuni **sono vulnerabili**, ma anche **aziende e istituzioni** possono essere bersagliate da attacchi mirati.

PERCHÉ LE TRUFFE SONO SEMPRE PIÙ COMUNI?

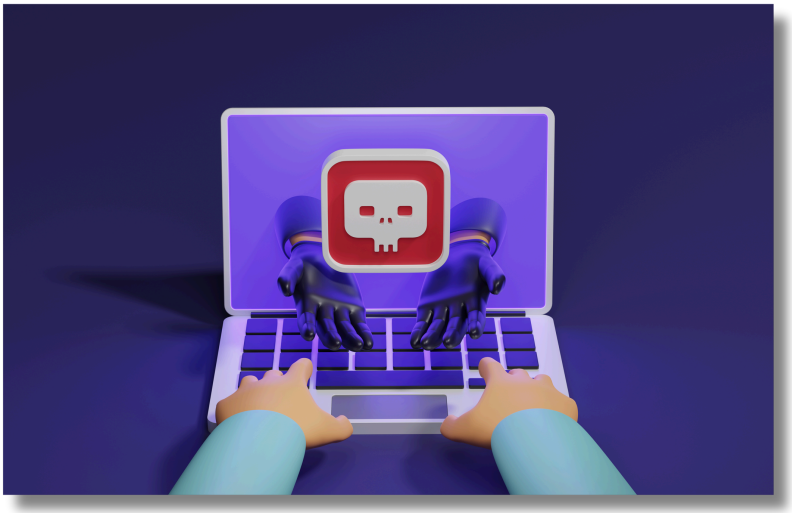
La digitalizzazione e **l'espansione delle comunicazioni** online hanno trasformato il mondo in un luogo in cui la truffa può avvenire in qualsiasi momento, da qualsiasi parte del globo. La facilità con cui le informazioni possono essere scambiate, unite alla crescente sofisticazione degli strumenti usati dai **truffatori**, ha reso **il crimine online più difficile** da individuare e da fermare. Inoltre, molte truffe sono costruite per **sfruttare emozioni forti** come la paura, l'urgenza o il desiderio di guadagno facile, mettendo le vittime in una **condizione di vulnerabilità psicologica**.
Oggi, chiunque può essere vittima di una truffa. Da una semplice **"phishing email"** che chiede di aggiornare i dettagli del proprio **conto bancario**, fino a **truffe più complesse** come il **"social engineering"** dove i truffatori si infilano nelle **vite digitali** delle persone per raccogliere informazioni personali e far leva su di esse.

COSA AFFRONTERAI IN QUESTA GUIDA?

Questa guida ha **l'obiettivo di fornirti gli strumenti** e le conoscenze per **proteggerti dalle truffe**. La tua sicurezza online è fondamentale, e con i giusti accorgimenti puoi ridurre notevolmente **il rischio di cadere vittima di inganni**. Imparerai a **riconoscere i segnali di allarme**, a gestire situazioni **sospette** e a **proteggere le tue informazioni sensibili.**

Nel corso di questa guida, tratteremo:

- Le **truffe più comuni**: dai **messaggi falsi alle frodi sui social media**, passando per le **truffe bancarie online**.
- Come riconoscere una truffa: i segnali di allarme a cui fare attenzione.
- Come **proteggere i tuoi dati personali e bancari:** suggerimenti pratici per **mettere in sicurezza i tuoi dispositivi e le tue informazioni**.
- Cosa fare se sei **vittima di una truffa:** cosa fare per cercare di **recuperare ciò che hai perso** e come segnalarlo alle autorità competenti.



Phishing: La Truffa via Email o SMS

*Il phishing è una delle **truffe più comuni e pericolose**. Consiste nell'invio di **email o messaggi SMS** (Smishing) che sembrano provenire da fonti affidabili (banche, aziende di e-commerce, social media), ma in realtà sono falsi. L'obiettivo dei truffatori è ottenere **informazioni sensibili**, come password, numeri di carta di credito o dati bancari.*

COME RICONOSCERLO:

- **Controlla l'indirizzo email** o il **numero del mittente**: spesso il truffatore utilizza un indirizzo mail leggermente diverso da quello ufficiale.
- **Diffida da messaggi urgenti che ti chiedono di fare clic su un link** o di fornire informazioni personali.

COME DIFENDERSI:

- Non rispondere mai a richieste di informazioni sensibili **via email o SMS**.
- Verifica sempre le comunicazioni attraverso i **canali ufficiali** (ad esempio, accedendo al sito web della banca).
- **Effettua periodicamente** una scansione antivirus del tuo dispositivo

ATTENZIONE!

Attraverso alcune tecniche (spoofing) il truffatore può copiare numero di enti riconosciuti.

Quindi, anche se ricevessi un sms da un numero conosciuto, invece di fare click sul link, accedi direttamente alla tua app di home banking o, in alternativa recati in filiale.

VISHING + SPOOFING

Pur trattandosi di una **variante del phishing** che utilizza la telefonata come strumento, è importante dedicare un capitolo a parte.
Si tratta di una truffa che può diventare **estremamente insidiosa** a causa di alcune **tecniche come quella dello spoofing** che consentono di manipolare il numero che appare sul display del nostro cellulare.

COME RICONOSCERLE:

- **Ricevi una chiamata da un numero che appare come quello della tua banca** e ti viene detto che **il tuo conto è stato bloccato**, per sbloccarlo dovrai effettuare dei **bonifici istantanei** verso alcuni conti.
- **L'atteggiamento** del **truffatore sarà insistente e allarmante**

COME DIFENDERSI:

- **Nessun operatore di banca** ti chiederà mai di fare bonifici o fornire dati riservati come il numero di carta di credito, quindi chiudi la chiamata
- Controlla **la tua app di home banking o recati in filiale**

TRUFFE SU SITI DI E-COMMERCE E MARKETPLACE

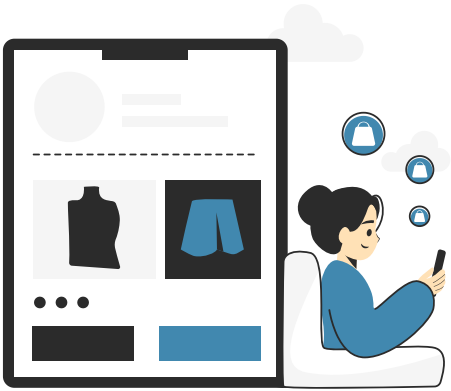
Un'altra **truffa** comune riguarda l'acquisto di beni e servizi su siti di **e-commerce** e **marketplace online**. I truffatori spesso vendono prodotti che non esistono o chiedono pagamenti anticipati utilizzando canali di pagamento esterni al marketplace per servizi mai forniti.

COME RICONOSCERLE:

- **Diffida da venditori** che ti chiedono di pagare tramite **metodi non tracciabili** (ad esempio, ricariche su carte prepagate o bonifici bancari).
- Leggi le **recensioni del venditore**
- **Controlla sempre che l'URL del sito web inizi con "https://"** e che ci sia un'icona di lucchetto accanto all'indirizzo nella barra del browser.

COME DIFENDERSI:

- Usa sempre **metodi di pagamento sicuri**, come carte di credito o piattaforme di pagamento protette (PayPal, ad esempio).
- Verifica che il **sito web sia sicuro** e abbia una buona reputazione.
- In caso di dubbio, cerca il **nome del venditore su internet** per vedere se ci sono segnalazioni di truffe.
- Se acquisti su un **marketplace** e il **venditore** ti dice di utilizzare canali di pagamento esterni , non fidarti. Perderesti automaticamente **tutte le tutele** offerte dal marketplace.



Truffe sui Prestiti e Investimenti

*Le truffe sui **prestiti e sugli investimenti** sfruttano il desiderio delle vittime di **ottenere rapidamente denaro** o rendimenti elevati. I truffatori promettono prestiti immediati, anche senza garanzie, oppure **investimenti con profitti certi e rischi nulli**. In realtà, l'obiettivo è **estorcere pagamenti anticipati**, carpire dati personali o far entrare la vittima in schemi fraudolenti.*
*Questa tipologia di truffa è **molto diffusa online, soprattutto su social network, siti-clone e messaggi privati.***

COME RICONOSCERLE:

- **Promesse irrealistiche:** prestiti immediati senza controlli, investimenti con guadagni garantiti o troppo elevati rispetto al mercato.
- **Richiesta di pagamenti anticipati:** "spese di istruttoria", "assicurazione del prestito", "sblocco fondi" o commissioni da versare prima di ricevere qualsiasi servizio.
- **Pressione e urgenza:** messaggi insistenti che invitano a decidere subito perché "l'offerta scade".
- **Assenza di controlli sulle garanzie o sulla solvibilità:** nessuna analisi della situazione finanziaria della vittima, cosa impossibile per un credito legittimo.
- **Documenti o siti non professionali:** contratti pieni di errori grammaticali, aziende sconosciute o non registrate, siti web molto simili a quelli di banche reali (clonati).
- **Pagamenti tramite metodi non tracciabili**: ricariche su carte prepagate, criptovalute o bonifici verso conti esteri sospetti.

COME DIFENDERSI:

- **Verifica sempre l'intermediario:** controlla se la società è autorizzata presso registri ufficiali
- **Diffida dai pagamenti anticipati:** nessun istituto serio chiede soldi prima di erogare un prestito o proporre un investimento.
- **Controlla il sito web:** assicurati che l'indirizzo sia corretto, con connessione sicura (https) e che l'azienda abbia contatti verificabili.
- **Non inviare documenti a sconosciuti**: condividi dati sensibili solo con operatori verificati e attraverso canali sicuri.
- **Fai attenzione alle proiezioni** soprattutto per gli investimenti in beni-rifugio, affidati solamente a indici riconosciuti a livello globale.
- **Chiedi una consulenza:** parla con un consulente finanziario autorizzato o con la tua banca prima di investire o richiedere prestiti online.
- Segnala e denuncia: se sospetti una truffa, contatta la Polizia Postale e segnala subito il profilo o il sito.

TRUFFE ASSICURATIVE

Le **truffe assicurative riguardano la vendita di polizze false o l'intermediazione da parte di soggetti non autorizzati**. I criminali sfruttano l'esigenza di ottenere **assicurazioni a basso costo** (soprattutto RC auto) e propongono offerte molto vantaggiose, spesso tramite **social network, siti web non ufficiali o messaggi privati.** Chi cade in queste trappole **paga per una polizza inesistente o non valida**: al momento del bisogno, scopre di **non avere alcuna copertura** e rischia sanzioni e problemi legali.

COME RICONOSCERLE:

- **Intermediari non autorizzati:** agenti o broker che non risultano iscritti ai registri ufficiali (es. RUI — Registro Unico degli Intermediari).
- **Siti web contraffatti o clone:** pagine molto simili a quelle delle compagnie reali, ma con URL diversi o dettagli incoerenti.
- **Richieste di pagamento rapide e non tracciabili:** bonifici verso conti esteri, ricariche su carte prepagate, link sospetti.
- **Contratti non conformi:** moduli con dati mancanti, marchi di compagnie non coerenti, errori grammaticali o informazioni poco chiare.

COME DIFENDERSI:

- **Verifica l'intermediario:** controlla sempre che l'agente o il broker sia iscritto al RUI (Registro Unico degli Intermediari) tramite i portali ufficiali.
- **Controlla la compagnia assicurativa:** usa i siti delle compagnie per verificare se il numero di polizza esiste davvero.
- **Usa solo canali ufficiali:** richiedi preventivi e acquista polizze tramite il sito della compagnia o presso agenzie certificate.
- **Evita pagamenti non tracciabili:** preferisci transazioni sicure come carta o bonifico verso conti italiani intestati alla compagnia o all'intermediario autorizzato.
- **Conserva tutta la documentazione:** contratto, quietanze, email e prova di pagamento.
- **Segnala i casi sospetti:** alla compagnia assicurativa, all'IVASS o alla Polizia Postale.

Le truffe offline

Le **truffe offline** sono quelle che si verificano al di fuori di internet, ma che non per questo sono meno pericolose.

Possono avvenire in qualsiasi situazione: **al telefono, durante una vendita porta a porta, in strada, etc..**
I truffatori spesso **sfruttano la distrazione, la buona fede o la pressione psicologica** per ingannare le persone e ottenere denaro o beni.

In questo contesto, è **fondamentale mantenere sempre un atteggiamento di cautela e sospetto** in caso di offerte troppo vantaggiose o situazioni che sembrano fuori dall'ordinario.

La **prevenzione è la chiave**: riconoscere **i segnali di allarme e sapere come comportarsi** può fare la differenza tra cadere in una truffa o evitarla.

ADICONSUM
Associazione Difesa Consumatori APS
dal 1987
LAZIO, ROMA Capitale e RIETI

Hai bisogno di maggiori informazioni?

EMAIL :
lazioadiconsum@gmail.com

SITO WEB:
www.romaadiconsum.com

INDIRIZZO:
Via Baldo degli Ubaldi 378, Roma
Via G.M. Crescimbeni 17/A, Roma

Finanziato con i fondi del 5X1000