Le truffe online più diffuse e i metodi per difendersi

In questa guida capiremo come evitare le truffe online più diffuse e quali sono gli strumenti e i comportamenti da adottare per prevenirle. Oggi è fondamentale comprendere come proteggere la propria identità e i propri conti, e la buona notizia è che non bisogna essere esperti informatici per massimizzare la sicurezza e limitare i rischi.
(Fonte: https://www.truffa.net/ 17/02/2025)

Quali sono le truffe informatiche più diffuse in Italia

Il tempo che quotidianamente trascorriamo online è sempre di più, così come sono più numerose le azioni che svolgiamo tramite Internet. Senza dubbio oggi siamo utenti più esperti e più avvezzi alle tecnologie informatiche. Questo però non ha portato un calo delle truffe online: al contrario dove ci sono più utenti, ci sono anche **più occasioni di effettuare frodi online**.
Gli hacker non sono equiparabili al borseggiatore che si nasconde dietro un angolo in attesa di una malcapitata vecchietta. Rispondono più al profilo di **criminali informatici molto esperti**, in grado di architettare raggiri in vari ambiti, molto ben congegnati e diretti a target specifici.
Ecco la lista delle truffe online più diffuse in Italia nel 2025:

1. Truffa del pacco
2. Truffe su Facebook Marketplace
3. Smishing
4. Truffe sentimentali
5. Truffa Postepay
6. Truffa Amazon
7. Truffa Instagram
8. Spoofing
9. Truffa conto corrente
10. Truffa donazioni fraudolente
11. Truffa nigeriana
12. Truffa Enel
13. Truffa Airbnb
14. Truffa criptovalute
15. Truffa schema Ponzi
16. Truffa annunci di lavoro falsi
17. Truffa WhatsApp
18. Truffa Telegram
19. Truffa Booking

Come si vede dalla lista, si tratta di truffe che corrispondono ad azioni che svolgiamo quasi quotidianamente. Dall'effettuare acquisti sui più popolari siti di e-commerce a prenotare una

vacanza online su Airbnb, dalla ricerca di un partner all'utilizzo delle proprie carte per pagare beni o servizi. Insomma **ogni ambito d'azione virtuale**, può essere oggetto di una truffa.

Come riconoscere truffe online

Il primo modo per evitare le truffe su Internet è quello di imparare a riconoscerle. Come vedremo nei vari approfondimenti dedicati a questo tema, spesso **gli hacker si dimostrano molto scaltri**, in grado di imbrogliare anche gli utenti più esperti. Il primo passo per tentare di smascherare un tentativo di raggiro è prestare attenzione a vari segnali. Spesso siamo abituati ad agire in modo molto rapido sul web, in modo particolare per le azioni che ripetiamo di continuo. Ma la fretta è un elemento su cui giocano i truffatori.

Dai siti truffa che imitano in tutto e per tutto quelli ufficiali, alle offerte di lavoro su Telegram o WhatsApp, troppo belle per essere vere, ma **che inducono alla risposta**. Altri strumenti sono le intimidazioni, ad esempio avvisi allarmanti sulla sicurezza, oppure messaggi, che ci propongono investimenti di nuove criptovalute pronte a esplodere, e così via.

Alcuni segnali possono essere colti **da chiunque si soffermi** qualche minuto sul messaggio ricevuto. Vanno considerati sospetti e degni di attenzione i messaggi caratterizzati da:

- Intestazione vaga
- Inviti all'azione immediata
- Carattere di urgenza
- Errori di ortografia o grammatica
- Presenza di link su cui cliccare
- Richieste di dati

Il meccanismo del phishing online

La maggior parte delle truffe in rete si basa sul meccanismo del phishing online. Con questo termine si indica un tipo di truffa online che induce gli utenti a fornire informazioni sensibili utilizzando un'esca. **Questa esca generalmente è un messaggio** inviato all'utente tramite e-mail, SMS, WhatsApp.

I messaggi di phishing online sono caratterizzati dalla presenza di un link e dalla richiesta di un'azione che l'utente deve effettuare. Il link porta a un sito web che appare **in tutto e per tutto simile** a quello ufficiale di un ente o un'azienda, che l'utente conosce. Qui viene richiesto di inserire informazioni personali, dati di accesso, password. In questo modo l'utente viene derubato dei propri dati.

Alcuni esempi di phishing online

Tra i casi più comuni vi sono quelli di **clone phishing**, che vengono effettuati tramite una mail che appare identica a quella di un mittente affidabile e che conduce tramite link a un sito clone. In

altri casi un'email avvisa l'utente che i propri dati di accesso e password stanno per scadere e che bisogna andare all'url indicato per aggiornarli.
Altro caso frequente è quello della mail di phishing che avvisa che il proprio conto, magari quello online di PayPal, è **stato disattivato perché compromesso** da un attacco o attività sospette. Ovviamente il messaggio invita a cliccare, portando su un falso sito web per riattivarlo.
Un'altra tecnica diffusa prevede l'invio di email o SMS che **imitano le comunicazioni** di piattaforme note, come Booking, subito dopo un acquisto. Questi messaggi contengono link a siti che riproducono fedelmente quello ufficiale, inducendo l'utente a credere di dover reinserire i dati della sua carta di credito per confermare l'ordine.

Come evitare truffe online

La prudenza **è la prima arma** da utilizzare per evitare o limitare il rischio di cadere in truffe online. Ecco alcuni suggerimenti per capire come difendersi dalle truffe, utili a chiunque sia attivo sul web o faccia acquisti via internet.
Per lo shopping in rete o per giocare sui **siti di gambling online**, rivolgersi a **siti noti o affidabili**. Scegliere portali conosciuti che hanno una buona reputazione è importante. Per i nuovi siti fare ricerche sulle recensioni di altri utenti, e cercare informazioni come indirizzo, numero di telefono, dati legali. Diffidare di quelli che pubblicano solo un indirizzo email.

- Usare solo **siti sicuri**. Questi cominceranno con "https" e avranno il simbolo di un lucchetto giallo che indica che il processo di pagamento è sicuro.
- Usare **metodi di pagamento** sicuri. Ad esempio preferire carte prepagate e E-wallet come PayPal, alle carte di credito e di debito collegate al conto bancario.
- **Mai cliccare sui link** proposti nei messaggi, sempre meglio digitare l'indirizzo del sito sul proprio browser e verificare se ci sono notifiche o richieste.
- Usare **password complesse** e non comunicarle a nessuno.
- Attivate l'autorizzazione **in due step** per ogni transazione con carte di credito.
- Controllare la lista movimenti del conto e attivare **le notifiche sulla app** della banca.
- Stampare sempre **una copia** degli ordini effettuati.

Come denunciare una truffa online

In Italia è possibile denunciare le truffe online rivolgendosi alla **polizia postale**, che è specializzata proprio nei reati telematici. Il sito ufficiale della polizia postale mette a disposizione un'area dedicata alle **segnalazioni online**. È possibile inserire gli elementi relativi alla truffa e i propri contatti. Il sito inoltre fornisce informazioni aggiornate sulle ultime truffe online, cosa fare e i comportamenti da evitare. Oltre a compilare il form online è possibile anche recarsi presso un posto di polizia fisicamente, per effettuare la denuncia.

Se si ricevono messaggi di phishing è anche possibile segnalarli ai diretti interessati. Pagine ufficiali infatti di banche, aziende, siti di e-commerce, mettono a disposizione link del tipo "**segnala phishing**" in cui è possibile indicare il tipo di messaggio ricevuto. In questo modo ci si potrà accertare che si tratta effettivamente di un tentativo di truffa e inoltre l'ente in questione potrà correre ai ripari e avvisare anche gli altri utenti.

Truffe più comuni del 2025

Come abbiamo accennato i cyber criminali sono sempre al lavoro. Tra le ultime truffe segnalate sul sito della polizia postale vi sono quelle effettuate **tramite messaggi WhatsApp**. In questo tipo di truffa si riceve un messaggio da un utente che finge di essere un proprio figlio o parente che ha smarrito il telefono e ha un nuovo numero. I primi messaggi saranno inoffensivi, ne seguiranno altri in cui si chiedono denaro, dati, credenziali d'accesso e così via.

Anche la seconda piattaforma di messaggistica al mondo, **Telegram, non è esente da truffe**, spesso legate a prodotti finanziari, a lavori pagati con criptovalute o ai classici schemi Ponzi che propongono notevoli guadagni in breve tempo.

Un'altra tendenza che sta prendendo piede, prende di mira chi vende sui marketplace più noti, per esempio Amazon o Facebook. Tra le offerte di acquisto si possono ricevere strane **proposte che si rivelano essere truffe**. Ad esempio il fantomatico cliente si offre di pagare tramite bonifico anziché con metodo indicato. Questo poi risulterà bloccato, seguiranno altre richieste che finiranno con danni al venditore.

FAQ

Quali sono le truffe online più diffuse in Italia?

Gli hacker si aggiornano di continuo, tra le ultime **truffe più diffuse in Italia** vi sono quelle del pacco bloccato, la truffa Postepay, la truffa su Amazon.

Si possono riconoscere le truffe sul web?

Sì, spesso basta prestare molta attenzione ai dettagli dei messaggi ricevuti e al modo in cui sono strutturati per riconoscere un tentativo di truffa. Alcuni segnali possono suggerire chiaramente che si tratta di **tentativi di phishing**.

Come evitare le truffe online?

Per evitare le truffe online è importante tenere gli occhi aperti e usare prudenza. Il primo passo è quello di **controllare che il sito web sia sicuro**. Inoltre è utile: usare password complesse, non comunicarle a nessuno, non cliccare su link all'interno di messaggi sospetti.

Cosa fare dopo essere stati truffati?

Nel caso vi rendiate conto di essere stati truffati dovete immediatamente **contattare la polizia postale** recandosi fisicamente a un posto di polizia, oppure tramite il sito ufficiale. Informare anche l'ente o azienda coinvolto nella truffa.