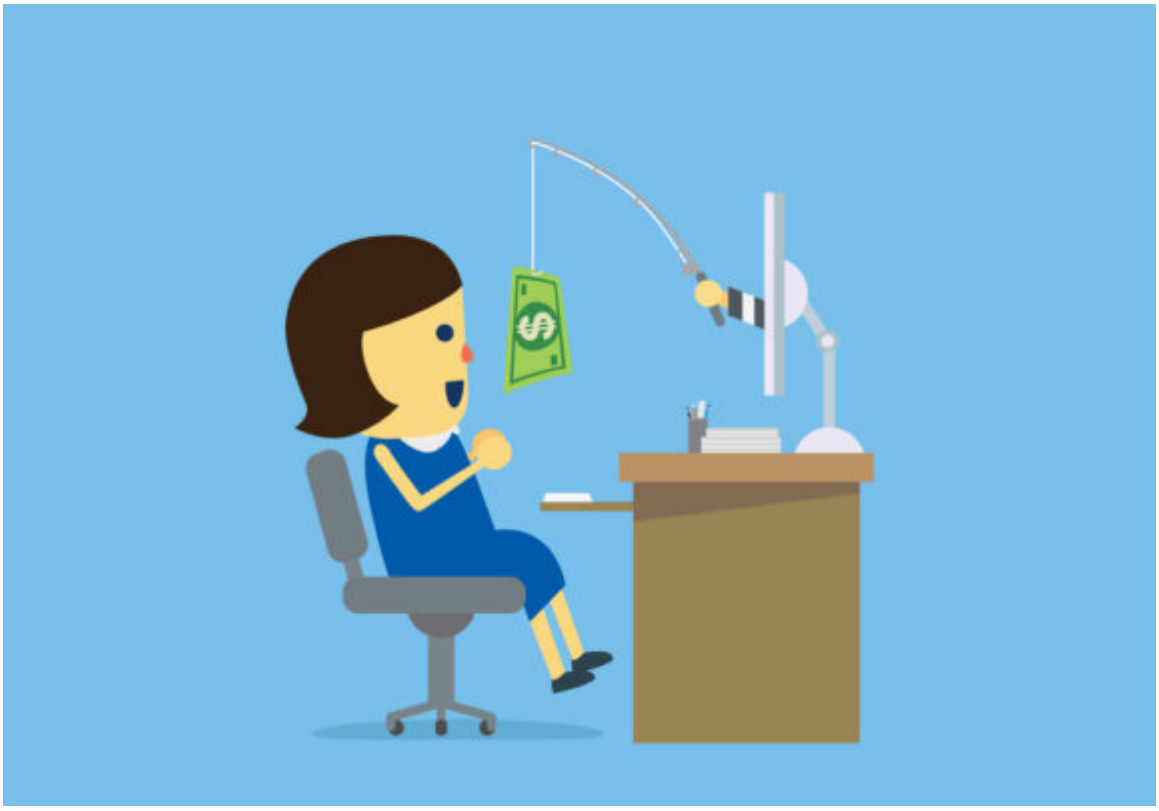
LA LEGGE PER TUTTI
INFORMAZIONE E CONSULENZA LEGALE

10 cose a cui fare attenzione per evitare una truffa

Autore: Mariano Acquaviva | 15/07/2020



Le truffe più diffuse e come riconoscerle: prezzi troppo vantaggiosi, phishing, promesse di facili guadagni, diete miracolose, ricatti per email.

Truffe e truffatori sono dietro l'angolo, soprattutto oggi che tutto passa per

internet: basta un passo falso in rete per poter cadere preda di subdoli figuri che, celandosi dietro email, messaggi, chat e download di dubbia provenienza, cercano di entrare nel portafogli (virtuale) delle persone. Ciò non significa che le frodi "classiche", cioè quelle architettate per strada, siano cadute in disuso. Insomma: per non fare la fine della pecora in mezzo ai lupi, ti consiglio vivamente di leggere questo articolo dedicato alle **10 cose a cui fare attenzione per evitare una truffa**.

La regola aurea da seguire è molto semplice: diffidare sempre, soprattutto se l'affare appare troppo conveniente oppure sospetto. Questo efficientissimo precetto potrebbe però essere insufficiente se il truffatore è particolarmente abile. Ecco allora che diventa opportuno seguire più di un precetto e, soprattutto, fare attenzione a tante piccole circostanze che, messe insieme, possono fornire il quadro completo della truffa da evitare. Se l'argomento suscita il tuo interesse, ti consiglio vivamente di proseguire nella lettura: vedremo insieme **a cosa fare attenzione per non incorrere in una truffa**.

Offerta troppo vantaggiosa

La prima cosa a cui fare attenzione per evitare di incappare in un raggiro bello e buono è il **tipo di offerta**: se essa si presenta incredibilmente **vantaggiosa**, allora occorre diffidare e aprire bene gli occhi.

Per offerta vantaggiosa possiamo intendere tanto il **prezzo d'acquisto** quanto qualsiasi altra condizione che renda inverosimile l'affare: pensa al nuovissimo cellulare di ultima generazione offerto a poche decine d'euro, oppure a un cimelio antico fatto giungere dall'estero solamente per te, o ancora al prezioso dipinto misteriosamente posseduto dal venditore.

Peraltro, tenere d'occhio le condizioni della vendita serve non solo a **evitare una truffa**, ma anche a non incappare in un reato: per questi aspetti, ti rimando alla lettura degli articoli dedicati all'incauto acquisto e alla ricettazione.

Luogo o venditori sospetti

Un altro indizio che deve metterti all'erta allorquando ti accingi a effettuare un acquisto è quello riguardante le **condizioni del luogo** ove avviene la transazione.

Se acquisti gioielli nel retro di un negozio per animali, renditi conto che probabilmente qualcosa non quadra e che quelli che ti stanno spacciando per diamanti sono probabilmente zirconi, mentre gli smeraldi sono fondi di bottiglia.

Allo stesso modo, presta attenzione alle condizioni in cui si presenta il **venditore**: l'abito non fa il monaco, ma spesso la prima impressione è quella esatta. Se colui che ti sta vendendo qualcosa non ti convince, ad esempio perché tratta beni di lusso mostrando una scarsissima cura per il suo vestiario e la sua igiene, allora lascia perdere: potrebbe trattarsi di un truffatore.

Pagamento in anticipo senza vedere la merce

Trucco vecchio come il mondo ma sempre efficace, molti truffatori si fanno **pagare prima di far vedere la merce** all'acquirente. In casi del genere, la truffa potrebbe essere dietro l'angolo. Evitarla è molto semplice: lo scambio deve avvenire immediatamente, sotto gli occhi di entrambe le parti. Insomma, il vecchio detto "pagare moneta e vedere cammello" è più che mai valido ancora ora.

Una truffa classica è quella di chi si fa mandare i soldi in anticipo con la scusa di dover sbloccare un pacco alla frontiera oppure di dover pagare dazi doganali per far arrivare la merce a destinazione.

Poiché oggi gran parte delle **transazioni** avviene a distanza, è difficile ottenere la simultaneità di pagamento e consegna del prodotto. Pertanto, se **acquisti online**, effettua il pagamento in maniera sicura e tracciabile. Ciò ci rimanda alla prossima cosa a cui fare attenzione per evitare una truffa.

Modalità di pagamento sospette

Oggi la moneta elettronica prevale sul vecchio contante. Pertanto, puoi tranquillamente pretendere che una transazione avvenga secondo **modalità di pagamento tracciabili**: bonifico, carta di credito, assegno, ecc.

Anche in questi casi, però, la truffa potrebbe essere dietro l'angolo. Ti spiego perché. Quando si effettuano acquisti a distanza, è praticamente inevitabile pagare con carte di credito o bonifici. Una modalità sospetta di pagamento potrebbe

essere la **ricarica della carta prepagata** (ad esempio, della Postepay).

Sebbene anche questo tipo di pagamento sia tracciabile, non va dimenticato che le **carte prepagate**, non poggiandosi su un conto, sono molto meno sicure per risalire al suo titolare, in quanto esse, una volta utilizzate per scopi illeciti, vengono poi gettate.

Oggi, peraltro, anche le carte prepagate sono munite di **codice Iban**: pertanto, anche un bonifico potrebbe essere diretto a una prepagata per poi sparire.

In casi del genere, per capire se il pagamento avviene su un conto corrente o su una prepagata, può essere utile effettuare un **controllo dell'Iban**, magari su questo sito o su tanti altri che ci sono in rete.

Le forze dell'ordine non vendono calendari

Una **truffa telefonica** molto in voga è quella del calendario di polizia. In pratica, una persona che si spaccia per poliziotto ti contatta dicendoti che puoi comprare, pagando direttamente al corriere, il calendario della Polizia di Stato italiana.

Ma non solo: oltre al calendario, il sedicente poliziotto aggiunge anche gagliardetti vari, adesivi per l'auto e codici utili per conoscere la legge.

Ciò che devi fare è solamente dare il tuo indirizzo e provvederanno loro (cioè i truffatori) a farti recapitare un pacco contenente i beni promessi. In cambio, è previsto il **pagamento** di qualche centinaio d'euro.

Ovviamente si tratta di una truffa: le forze dell'ordine non fanno vendite telefoniche o porta a porta.

Il pericolo che si cela dietro questa tipologia di **raggiro** è di soccombere alle insistenze di una persona che si qualifica come poliziotto e che, pertanto, si ammanta di autorità.

Email sospette: phishing

La **truffa online** per eccellenza ha un nome: **phising**. Il phishing consiste

nell'invio di una comunicazione contenente il logo contraffatto di un istituto di credito o di altra istituzione economica, e nella quale si invita il destinatario a fornire dati riservati (numero di carta di credito, password di accesso al servizio di home banking, ecc.), motivando tale richiesta con ragioni di ordine tecnico (tipo, disattivazione conto oppure *account*).

Solitamente nel messaggio, per rassicurare l'utente, è indicato un link che rimanda solo apparentemente al sito web dell'istituto di credito o del servizio a cui si è registrati. In realtà il sito a cui ci si collega è stato preparato in modo da assomigliare a quello originale. Qualora l'utente inserisca i propri dati riservati, questi saranno nella disponibilità dei **truffatori**.

Anche in questo caso, occhio all'email sospetta. Innanzitutto, la maggior parte delle email di questo tipo viene inserita automaticamente dalla casella di posta elettronica all'interno della cartella dedicato allo **spam**, cioè alle comunicazioni spazzatura inviate in serie a una molteplicità di destinatari.

In secondo luogo, se presterai bene attenzione, noterai tanti piccoli difetti all'interno dell'email: errori grammaticali, riferimenti a situazioni inesistenti (tipo conti correnti mai aperti), il logo dell'istituto di credito non perfettamente identico all'originale.

Ricatto per email

Un'altra forma di **truffa per email** è quella che consiste nel ricattare il destinatario, chiedendogli di pagare un determinato importo per mantenere segrete alcune sue informazioni riservate. Anche questa particolare **truffa per email** può assumere connotati diversi: a volte si minaccia la diffusione di un video scandaloso, altre volte invece quella delle **password** dei profili social.

Se dovesse arrivarvi qualcuna di queste comunicazioni, cercate di mantenere il sangue freddo e di denunciare subito l'accaduto, ovviamente senza assecondare il ricattatore: la maggior parte delle volte (quasi sempre) si tratta di un bluff, cioè di una richiesta fatta solamente per spaventare e ottenere i soldi senza in realtà essere in possesso di alcun dato riservato.

Nessuno ti regala soldi

Il funzionamento della truffa alla nigeriana riassume bene un concetto: nessuno è disposto a fare regali, di alcun tipo.

La truffa alla nigeriana è un particolare **raggiro a distanza** che consiste nell'ingannare la vittima spacciandosi per una **persona facoltosa** che, per problemi burocratici, non riesce a sbloccare un'ingente somma di denaro che gli deve essere resa ma che si trova momentaneamente presso un istituto di credito.

Per favorire l'operazione di trasferimento, il truffaldino chiede alla vittima di anticipare una (iniziale) modesta somma di denaro dietro la promessa che, al termine della vicenda, verrà restituita con lauti interessi. Altrettanto ovvio è, però, che nulla verrà reso e che si tratta di una truffa bella e buona. Le richieste di denaro, col tempo, si fanno sempre più cospicue, ogni volta sorrette da motivi pretestuosi.

Quanto appena detto per la truffa alla nigeriana vale ovviamente per qualsiasi tipo di raggiro simile, come ad esempio quello per cui devi **anticipare dei soldi per avere un'eredità**, oppure devi pagare per ottenere una somma molto più alta.

Le truffe dei broker online

Con l'avvento di internet in tanti hanno pensato di guadagnare soldi facili acquistando azioni in borsa per poi speculare sul prezzo di rivendita.

È così nato il **trading online**: attraverso una piattaforma internet, messa a disposizione da un **broker**, si acquistano e vendono **titoli finanziari** per mezzo del proprio computer con l'obiettivo di guadagnare sulla differenza di prezzo tra acquisto e vendita.

Per **difenderti dalle truffe** che avvengono sul trading online devi essere sicuro di affidarti a **broker sicuri**. I **broker truffaldini** non sono difficili da smascherare in quanto:

- promettono grandi guadagni senza che tu sappia nulla di finanza;
- vendono strumenti finanziari che consentono loro di avere un'enorme parte di vantaggio a scapito del trader;

- **offrono bonus di ingresso** molto allettanti con lo scopo di attirarti;
- non offrono alcuna formazione al futuro cliente/trader;
- hanno sede in **paradisi fiscali**.

Diete miracolose: non esistono

Internet ha diffuso un altro tipo di **truffa**: quella riguardante le diete che fanno miracoli. È abbastanza semplice rendersi conto che la dieta che circola sui social network è una fandonia: gli effetti sono troppo drastici e, soprattutto, sono ottenuti in un tempo incredibilmente breve.

Molte volte, per invogliare ancor più all'utilizzo della cura, la persona coinvolta nel "prima" e "dopo" trattamento è un volto noto dello spettacolo: pertanto, è ancor più facile constatare che la persona fuori forma non è la stessa che viene mostrata dopo con un fisico invidiabile.

Attenzione, quindi, ai **raffronti**: già da questi è possibile capire che si tratta di una falsa notizia o, peggio ancora, di una **truffa** vera e propria.

Inoltre, si tenga presente che al dimagrimento non corrisponde sempre un fisico tonico: in altre parole, anche se la massa grassa dovesse ridursi, quella muscolare dovrebbe essere rinforzata da costante esercizio fisico. La sola dieta, perciò, non basta.

Ancora, **attenzione alle fotografie**: molte di esse sono solo specchietti per le allodole. Alcune ritraggono improbabili dottori o dottoresse in tinelli poco rassicuranti, con in mano alambicchi e ampolle che dovrebbero conferire un tono rispettabile.

Le cure dimagranti che promettono miracoli sono, per lo più, false. Il problema è che, quando in cambio richiedono una controprestazione in denaro, esse possono diventare delle vere e proprie truffe.

Note

Autore immagine: Depositphotos.com