



UNC
CONSUMATORI.IT

Le 10 truffe più segnalate negli ultimi mesi

20 Settembre 2021



Abbiamo messo insieme le **10 truffe più segnalate dai consumatori**. Negli ultimi tempi infatti il numero di tentativi di frode è in aumento, ecco allora un utile elenco per evitare di cadere vittima delle **truffe più comuni**.

Se siete stati truffati e avete bisogno della **CONSULENZA DEI NOSTRI ESPERTI NON ESITATE A CONTATTARCI TRAMITE IL NOSTRO SPORTELLO**.

1. Truffa della differenza

Lo schema di **questa truffa** è piuttosto ingegnoso: **arriva una mail** in cui una persona apparentemente affidabile chiede all'ignaro utente di **poter versare sul suo conto corrente** un'ingente somma di denaro. Per il disturbo si offre anche una ricompensa alla vittima. L'offerta sembra allettante dunque, se non fosse per il fatto che molto spesso questo denaro proviene da **attività di natura criminale**. Una volta **ricevuto il denaro** il rischio sarà di essere considerati dei **complici di queste attività criminose**. Il consiglio è quindi quello di non accettare questo genere di proposte per nessun motivo.

2. Phishing, non aprite quella mail

Il **phishing** rappresenta la nuova frontiera delle **frodi informatiche**. **Ai nostri sportelli arrivano numerose segnalazioni** di consumatori caduti vittima di questa truffa.

Si riceve una mail apparentemente proveniente da una **banca o da una società emittente carte di credito**. La comunicazione pare **ufficiale** poiché viene utilizzato il logo, il nome e il layout tipico dell'azienda imitata. Si invita quindi il destinatario a collegarsi **tramite un link** ad un sito internet del tutto simile a quello **della banca** e ad inserirvi, generalmente attraverso una finestra pop-up che si apre dallo stesso link, le **informazioni riservate**. **Una volta ottenuti i dati i truffatori effettuano operazioni bancarie ai danni dell'ignara vittima.**

La raccomandazione è di non inserire i propri dati su siti internet che vi sono stati inviati tramite messaggi. **Contattare la banca** è la cosa migliore per assicurarsi che la **comunicazione** arrivi veramente da loro.

3. Vishing: il pericolo viene dal telefono

Una telefonata da un numero che pare appartenere alla **propria banca**. Quando la vittima risponde gli vengono chiesti **i codici operativi** del proprio conto corrente. Una volta ottenuti, i truffatori sottraggono all'ignaro utente **migliaia di euro**. Nessun istituto di credito vi chiederà i vostri **codici operativi** (sono personali e alla banca non occorrono), tanto meno lo farà al telefono.

Per saperne di più sul vishing e come difendersi leggi l'articolo: **Vishing: la truffa del finto operatore bancario**

4. Truffa del sì

L'ennesima truffa che **passa dal telefono**. Lo schema è il seguente: una telefonata da parte dell'operatore di un call center domanda, ad esempio, se si tratti del Signor Rossi. **Una volta registrato il sì come risposta alla domanda apparentemente innocente, il file audio verrà montato** ed utilizzato per far sembrare che in realtà la vittima abbia dato il suo **consenso all'attivazione** di un contratto per la fornitura di luce e gas, ad esempio. State dunque ben attenti e, se proprio volete **confermare la vostra identità**, nel momento in cui al telefono vi si chiede se siete effettivamente il signor Rossi, un semplice "sono io" vi eviterà parecchie scocciature.

5. Truffa del catalogo

Alla porta della vittima si presenta una persona di bella presenza che, in cambio della **consegna di un catalogo** con non meglio specificati **"sconti speciali"**, chiede una **"firmeda"** sulla ricevuta di consegna. In realtà non si tratta affatto di una semplice ricevuta ma **quello firmato è un vero e proprio contratto capestro che impegna il consumatore** ad acquistare svariati oggetti al **costo di migliaia di euro**.

Controllate sempre con cura quello che firmate, in particolare diffidate da chi vi chiede **una semplice firma** senza dilungarsi troppo sul contenuto di quello che state per sottoscrivere.

6. Truffa dei buoni spesa

A chiunque farebbe piacere ricevere un **buono sconto del valore di 100€** da spendere su **Amazon, all'Esselunga o alla Coop**, ma realisticamente parlando è piuttosto difficile che questo genere di promozioni venga messa in atto e soprattutto che ci venga comunicato **su WhatsApp**.

Si tratta di una frode in cui l'intento dei truffatori è quello di rubare i dati degli utenti. Un messaggio sulla nota app di messaggistica informa la potenziale vittima che per poter riscuotere il fantomatico premio occorre inserire i riferimenti personali **comprese le coordinate bancarie**. Una volta fatto non si riceve nessun buono sconto. Attenzione dunque:

assicuratevi che il **link** sul quale state cliccando sia **realmente riconducibile al marchio indicato**;

visitate voi stessi il **sito internet ufficiale** per controllare se da qualche parte viene pubblicizzato questo genere di promozione.

7. Truffa del pacco sospeso

Il **commercio online** ha vissuto una vera e propria impennata in questi mesi. Alcuni **truffatori** hanno deciso di sfruttare questo momento per inviare degli sms alle vittime prescelte. In questo messaggio si legge che un **pacco in consegna** è stato bloccato e che per riceverlo sarebbe necessario pagare la cifra di 2€. L'inconsapevole consumatore, tratto in inganno dal fatto che l'SMS sembra davvero provenire dal **corriere** e in più che la cifra richiesta non sembra essere eccessiva, inserisce i dati della **carta di pagamento** sul sito truffa. Una volta effettuata quest'operazione i criminali rubano questi dati effettuando **operazioni fraudolente**. Non inserite **i vostri dati bancari, nessun corriere richiede il pagamento di alcuna cifra per sbloccare la vostra consegna**.

8. Sms dalla banca

Le tecniche per truffare i consumatori si stanno sempre più affinando. **È questo il caso dell'SMS Spoofing**: una tecnica che permette di modificare il **nome dell'utente** dal quale si sta ricevendo la comunicazione. Così molte segnalazioni parlano di **messaggi apparentemente ufficiali** provenienti dal **proprio istituto di credito** nel quale, con la scusa di dover bloccare alcune **operazioni sospette**, si richiede all'utente di inserire i propri dati per accedere al **conto online**. È una **truffa**, ricordiamo di nuovo che nessun istituto di credito vi richiederà i vostri **dati bancari** attraverso un sms.

9. Truffa case vacanze

La **vacanza rovinata** è purtroppo uno degli argomenti più ricorrenti tra le segnalazioni che giungono ai nostri sportelli al rientro dalle vacanze. Al momento di scegliere dove trascorrere le **vacanze**, tra i tanti annunci di **case vacanze veritieri**, ci sono **anche alcuni tentativi di truffa**. Le case che vengono mostrate nell'annuncio fraudolento in realtà non esistono.

I nostri esperti sono pronti a fornirvi tutta l'assistenza di cui avete bisogno. **In caso di vacanza rovinata contattateci attraverso lo sportello dedicato**.

10. Contachilometri alterato

Speravamo di non dover tornare a parlare di questo tema e invece, periodicamente, ai nostri sportelli giungono segnalazioni di utenti che acquistano **veicoli usati** salvo poi accorgersi che il **chilometraggio** fin lì effettuato sia molto più alto rispetto a quello indicato dal **contachilometri**.

Falsificare questo dato permette ai **truffatori** di vendere un veicolo con maggiore facilità facendolo passare come **“quasi nuovo”**. Qualora vi rendeste conto che il **contachilometri dell'auto** che avete comprato usata è stato **alterato** **qui diamo una serie di consigli utili per far valere i vostri diritti di consumatori**.

Autore: Lorenzo Cargnelutti

Data: 20 settembre 2021