# Truffe online in aumento. Ecco le più comuni

22 Luglio 2020

Dopo che negli ultimi mesi ci siamo occupati spesso di **truffe ai danni dei consumatori** dobbiamo, purtroppo, tornare a parlarne. Infatti, a lanciare l'allarme è anche la **Polizia Postale** che segnala un aumento preoccupante delle **frodi online.**

Ecco quali sono le più comuni e come difendersi.

## Shopping con false identità

In crescita le **frodi creditizie** realizzate tramite **furto d'identità.** Come funziona? La truffa consiste, inizialmente, nel trafugare dati personali e finanziari (magari acquistandoli nel dark web); poi utilizzare le informazioni ottenute per **richiedere prestiti o acquistare oggetti** on line. Il tutto a danno delle sfortunate vittime che, molto spesso, si rendono conto della truffa solo tempo dopo quando, per esempio, provano a richiedere un finanziamento ma gli viene negato per non aver pagato le rate di quello attivato dai truffatori. In tal caso è necessario denunciare alle autorità e procedere con la richiesta di

**disconoscimento dell'operazione.**

## Bec Fraud e Ceo Fraud

*Business e-mail compromise o Chief executive officer,* sono questi alcuni dei nuovi tipi di **truffa** che vano a colpire in particolar modo le imprese. Infatti, attraverso di esse, i malviventi si inseriscono nelle comunicazioni commerciali tra aziende, o in quelle dei dirigenti di una stessa società e, con messaggi fasulli ma ritenuti credibili dai malcapitati, **dirottano somme ingenti** su conti corrente intestati ai truffatori.

## Vishing

Spesso ci siamo trovati a **parlarvi del phishing**, oggi però gli orizzonti di questo genere di illecito si sono allargati arrivando al **vishing**, nato dall'unione tra i concetti di *voice e phishing.*

Questa **nuova truffa** punta ad unire la conoscenza dei dati personali degli utenti con l'utilizzo di telefonate volte ad ingannarli.

Sul cellulare o sulla casella di posta elettronica delle vittime arriva una notifica, apparentemente dalla propria banca, che segnala operazioni sospette relative al proprio conto.

L'utente preoccupato dall'avviso clicca sull'indirizzo internet di un sito clone.

Una volta lì riceve una telefonata (apparentemente credibile grazie all'uso di **un finto numero verde** della banca) in cui i truffatori si spacciano per solerti impiegati dell'istituto di credito che vogliono bloccare il furto quando in realtà, una volta ottenuti i codici di accesso, **autorizzano bonifici o pagamenti** alle spalle dell'ignara vittima.

## Truffe sul bonus mobilità

Il Ministero dell'Ambiente ha denunciato come nei giorni scorsi siano arrivate diverse segnalazioni, da parte di chi intende avvalersi del **bonus mobilità**: sembra che vi siano diverse app che puntano ad ingannare gli utenti attraverso nomi accattivanti come "Bonus mobilità 2020".

In realtà il dicastero comunica che le modalità per richiedere il bonus saranno comunicate attraverso **i canali ufficiali** diversi giorni prima della data di invio delle richieste.

Le applicazioni ingannevoli sono state già segnalate puntualmente alle autorità competenti.

## Come difendersi

I consigli che gli esperti danno sono, oltre a prestare particolare attenzione:

- quando si inseriscono i dati della propria **carta di credito su internet**, verificare prima la sicurezza del sito;
- non inviare i propri codici di accesso al conto corrente. Gli istituti di credito ad esempio non richiedono mai via e-mail o per telefono le credenziali di accesso all'home-banking;
- prudenza e giudizio sono necessari nel momento in cui viene richiesto l'invio di copie di documenti;
- e infine, non scaricare mai allegati che arrivano tramite mail o sms se non si è sicuri circa l'identità del mittente.

**HAI BISOGNO DEL NOSTRO AIUTO? SCRIVICI ALLO SPORTELLO GENERICO**

**Autore**: Lorenzo Cargnelutti
**Data**: 22 luglio 2020