COS'È IL FURTO DI IDENTITÀ?

Furto d'identità è un **qualsiasi tipo di frode che porta alla perdita di dati personali**, come password, nomi utente, dati bancari o numeri di carte di credito. Su internet a volte il furto di identità online è detto *phishing*.

Il furto di identità non è una novità. I ladri hanno sempre trovato il modo di acquisire illegalmente informazioni personali altrui approfittando della buona fede (un comportamento noto anche come l'**ingegneria sociale**), rubando posta dalle cassette delle lettere o addirittura frugando in cassonetti e cestini della spazzatura. Adesso che il furto di identità ha raggiunto la rete, i criminali possono truffare un maggior numero di persone e quindi guadagnare molto di più.

Le frodi telematiche possono contenere i seguenti elementi:

- Messaggi allarmistici e minacce di chiusura dell'account.
- Promesse di denaro senza fatica.
- Offerte troppo belle per essere vere.
- Richieste di donazioni a enti benefici subito dopo che un disastro naturale ha fatto notizia.
- Pessima grammatica e ortografia.

COSA FARE SE RITIENI DI ESSERE VITTIMA DI UNA FRODE

Se temi di aver risposto a un tentativo di phishing fornendo informazioni personali o finanziarie, **attieniti ai seguenti passaggi** per ridurre al minimo eventuali conseguenze.

- Modifica password e/o PIN di tutti gli account online che temi possano essere compromessi.
- Inserisci un avviso di frode nelle tue relazioni creditizie. Consulta la banca o il tuo consulente finanziario se non sai come procedere.
- Contatta direttamente la banca o l'operatore online. Non seguire il link nel messaggio email fraudolento.
- Se sei a conoscenza dell'accesso o dell'apertura fraudolenta di tuoi account, chiudili.
- Esamina gli estratti conto bancari e delle carte di credito periodicamente e verifica l'eventuale presenza di spese immotivate o operazioni non richieste da te.

FURTO E FRODE DI IDENTITÀ

Il **furto di identità** si verifica quando qualcuno ottiene indebitamente i vostri dati personali. Si parla, invece, di **frode di identità** quando un criminale usa i vostri dati a vostra insaputa per ottenere credito, beni o altri servizi in modo fraudolento. Nel Regno Unito il costo complessivo è di oltre **£ 1,2 miliardi**, ma i danni per le vittime non sono solo finanziari; può essere un processo lungo e traumatico reclamare la propria identità.

Sia a casa che a lavoro abbiamo a che fare quotidianamente con informazioni che prese singolarmente possono sembrare innocue ma, messe insieme, possono essere molto preziose per i criminali che potrebbero utilizzarle per ottenere documenti di identità e patenti di guida a vostro nome, aprire conti bancari, ottenere carte di credito, prestiti e indennità statali.

COME AVVIENE IL FURTO DI IDENTITÀ?

Durante l'arco della giornata si può correre il rischio di subire un furto di identità a casa, quando si è in giro oonline. Se sapete dove guardare e come proteggervi, le possibilità che ciò si verifichi si riducono notevolmente.

In sostanza, i ladri di identità sono alla ricerca di informazioni personali su di voi, la vostra famiglia o anche la vostra attività, come il vostro nome completo, l'indirizzo attuale o precedente, la data di nascita e altre importanti informazioni come ad esempio i dati del vostro conto bancario o della vostra carta di credito.

Ecco alcuni dei modi più comuni attraverso cui i criminali recuperano le informazioni necessarie per rubare la vostra identità:

A CASA

Bin Raiding - I ladri di identità possono rovistare nella vostra immondizia. Bollette, estratti conto bancari e della carta di credito, lettere personali o curricula vitae contengono preziose informazioni personali che possono essere usate per rubare la vostra identità distruggete tutti i documenti che non volete che cadano nelle mani di un estraneo.

SUGGERIMENTO: Utilizzate un distruggidocumenti a frammento o microframmento per la massima sicurezza.

Cambiamento di indirizzo - I truffatori possono ricevere un'ingente quantità di informazioni sul vostro conto se a seguito di un trasferimento di residenza, ci si dimentica di comunicare la variazione dell'indirizzo alle Poste Italiane, alla Banca e a tutte le altre organizzazioni con cui si è in contatto.

In seguito a un cambiamento di residenza, fatevi reindirizzare la posta al nuovo indirizzo per almeno un anno.

Contatti indesiderati - Fate molta attenzione a chi vi contatta: spesso i truffatori si dichiarano incaricati di una banca e vi chiedono di aggiornare i vostri dati personali. Accade la stessa cosa con coloro che si presentano come ricercatori di mercato e vi richiedono informazioni personali. Le organizzazioni affidabili non faranno difficoltà davanti a una vostra richiesta di accertamento dell'autenticità prima di fornire tali informazioni.

IN GIRO

Furto o smarrimento del portafoglio - Generalmente i portafogli contengono , carte di redito e documenti di identità come la patente di guida e le tessere di iscrizione a determinate associazioni. Sebbene le vittime si accorgono molto presto che il loro portafoglio è stato rubato, spesso si rendono conto del valore delle informazioni in esso contenute quando è ormai troppo tardi.

Skimming - Si verifica in genere quando, ad esempio, una commessa o cameriere copiano i dati della carta di credito quando si effettua un acquisto. Queste informazioni vengono poi vendute a bande criminali. Come il phishing, lo skimming può essere utilizzato anche solo per raccogliere informazioni e utilizzare la carta di credito in modo fraudolento senza rubare la vostra dentità.

ONLINE

Informazioni personali online - A tutti coloro che usano internet viene chiesto regolarmente di fornire informazioni personali per poter accedere a determinati siti o per poter acquistare beni. Un crescente numero di utenti, inoltre, fornisce un'elevata quantità di dati personali a social network come **Facebook**, **Bebo**, **Twitter**, **Linkedin** e **MySpace**.