Email con ricatto: si tratta di una truffa

09 Dicembre 2020

Se ricevete una **email** in cui vi viene detto che siete stati **"scoperti"** a visitare **siti porno**, non apritela perché si tratta di una **truffa**. A lanciare l'allerta è stata diversi mesi fa la **Polizia Postale** dopo aver riscontrato una massiccia attività di **spamming** a scopo estorsivo. Allora è stato appurato che il tentativo di estorsione era opera di un gruppo internazionale di criminali che aveva inviato email in cui veniva comunicato agli utenti che il loro account di posta elettronica era stato **hackerato**. La Polizia Statale aveva però assicurato che si trattava di una falsa segnalazione, inviata per impaurire gli utenti e spingerli a pagare una somma di denaro richiesta. Nonostante questa rassicurazione, il rischio di ricevere sul proprio indirizzo di posta elettronica messaggi di questo tipo resta sempre vivo. Vediamo perché.

Cosa dice l'email

Nell'email i criminali dicono di avere 'beccato' l'utente mentre visitava un sito porno. Ma non solo. Dicono anche di aver scaricato tutte le **informazioni riservate** sul suo conto (compresa la cronologia di navigazione) e di aver installato un **virus** sul suo computer (un trojan) tramite il quale avrebbero avuto accesso alla webcam riuscendo a filmarlo in atti

intimi. Se l'utente non paga entro 48 ore un **riscatto di 300 dollari** in bitcoin (la moneta digitale), i criminali diffonderanno le immagini a tutti i suoi contatti, dunque amici, parenti e colleghi di lavoro.

Perché si tratta di una truffa

Sul suo sito la Polizia Postale spiega perché questo avvertimento è un tentativo di truffa. "È tecnicamente impossibile, infatti, – si legge sul sito – che chiunque, pur se entrato abusivamente nella nostra casella di posta elettronica, abbia potuto – per ciò solo – installare un virus in grado di assumere il controllo del nostro dispositivo, attivando la webcam o rubando i nostri dati".

Cosa fare se si riceve questa mail?

In caso abbiate ricevuto questo tipo di email sulla vostra casella di posta elettronica, i consigli da seguire indicati dalla Polizia Postale sono i seguenti. Chi invece vuole ulteriori chiarimenti, può rivolgersi direttamente alla Polizia Postale cliccando sul sito **www.commissariatodips.it**

1) **Mantenete la calma**: il criminale non dispone di alcun filmato che ci ritrae in atteggiamenti intimi né, con tutta probabilità, delle password dei profili social da cui ricavare la lista di nostri amici o parenti;

2) **Non pagate alcun riscatto**: pagarlo significherebbe ricevere altre minacce e altre richieste di denaro;

3) **Cambiate la password** della vostra email, sceglietene una particolarmente complessa e fate in modo che sia differente rispetto a quella che utilizzate per accedere ad altri vostri profili sul web (ad esempio Facebook);

4) Abilitate meccanismi di **autenticazione "forte"**: fate in modo che all'inserimento della password venga associata l'immissione di un codice di sicurezza ricevuto sul vostro telefono cellulare;

5) In generale, non lasciate mai i vostri **dispositivi incustoditi** e non cliccate su link o allegati di posta elettronica sospetti.

HAI BISOGNO DEL NOSTRO AIUTO? SCRIVICI ALLO SPORTELLO GENERICO

Autore: Rocco Bellantone
Data: 7 maggio 2019
Aggiornamento: 9 dicembre 2020