Sicurezza: Allerta Polizia Postale per maxi-estorsione online via e-mail ecco cosa fare

Redazione - 20/09/2018

ROMA, 20 SETTEMBRE - La Polizia Postale ha avvertito che e' in corso una massiva attivita' di spamming a scopo estorsivo con l'invio di email in cui gli utenti vengono informati dell'hackeraggio del proprio account di posta elettronica ad opera di un gruppo internazionale di criminali. Tale e-mail comunica che l'account sarebbe stato hackerato attraverso l'inoculamento di un virus mentre venivano visitati siti per adulti; da qui la minaccia di divulgare a tutti il tipo di sito visitato e la conseguente richiesta di denaro in criptovaluta. La Polizia postale ha avvertito che si tratta solo di un'invenzione per tentare di seminare il panico e indurre a pagare la somma illecita .

Le forze dell'ordine sottolineano che e' tecnicamente impossibile che chiunque, pur se entrato abusivamente nella nostra casella di posta elettronica, abbia potuto - per cio' solo - installare un virus in grado di assumere il controllo del nostro dispositivo, attivando la webcam o rubando i nostri dati.

Ecco dunque alcuni consigli su come comportarsi: Mantenere la calma: il criminale non dispone, in realta', di alcun filmato che ci ritrae in atteggiamenti intimi ne', con tutta probabilita', delle password dei profili social da cui ricavare la lista di nostri amici o parenti; Non pagare assolutamente alcun riscatto: lesperienza maturata con riguardo a precedenti fattispecie criminose (come #sextortion e #ransomware) dimostra che, persino quando il criminale dispone effettivamente di nostri dati informatici, pagare il riscatto determina quale unico effetto un accanimento nelle richieste estorsive, volte ad ottenere ulteriore denaro.

Proteggere adeguatamente la nostra email (ed in generale i nostri account virtuali): cambiare - se non si e' gia' provveduto a farlo - la password, impostando password complesse; non utilizzare mai la stessa password per piu' profili; abilitare, ove possibile, meccanismi di autenticazione "forte" ai nostri spazi virtuali, che associno allinserimento della password, limmissione di un codice di sicurezza ricevuto sul nostro telefono cellulare; Tenere presente che linoculazione (quella vera) di virus informatici capaci di assumere il controllo dei nostri dispositivi puo' avvenire soltanto se i criminali informatici abbiano avuto disponibilita' materiale dei dispositivi stessi, oppure qualora siano riusciti a consumare, ai nostri danni, episodi di phishing informatico: e' buona norma quindi non lasciare mai i nostri dispositivi incustoditi (e non protetti) e guardarsi dal cliccare su link o allegati di posta elettronica sospetti.