

## Crimini informatici: estorsioni vere per finti hackeraggi

Molti utenti stanno ricevendo email a scopo estorsivo in cui vengono informati dell'hackeraggio del proprio account di posta elettronica ad opera di un gruppo internazionale di criminali.

### Come avviene

Nello specifico la 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. Ma nulla di tutto ciò è reale: la mail ha il solo scopo di gettarci nel panico ed indurci a pagare la somma illecitamente richiesta.

Infatti è tecnicamente impossibile che chiunque, pur se entrato abusivamente nella nostra casella di posta elettronica, abbia potuto installare un virus in grado di assumere il controllo del nostro dispositivo, attivando la webcam o rubando i nostri dati.

### Cosa fare

E allora come comportarsi? Mantenere la calma: Il criminale non dispone, in realtà, 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.

Inoltre, non pagare assolutamente: l'esperienza maturata in casi del genere come sextortion e ransomware dimostra che, persino quando il criminale dispone effettivamente di nostri dati informatici, pagare la somma richiesta determina, quale unico effetto, un accanimento nelle richieste estorsive con ulteriori pretese di denaro.

### Come proteggersi

Per proteggere adeguatamente la nostra email e in generale i nostri account virtuali bastano pochi semplici accorgimenti: cambiare - se non si è già provveduto a farlo - la password, impostando password complesse; non utilizzare mai la stessa password per più profili; abilitare, ove possibile, meccanismi di autenticazione "forte" ai nostri spazi virtuali, che associno, all'inserimento della password, l'immissione di un codice di sicurezza ricevuto sul nostro telefono cellulare.

Infine tenere presente che l'inoculazione, quella vera, di virus informatici capaci di assumere il controllo dei nostri dispositivi può avvenire soltanto se i criminali informatici hanno avuto la disponibilità materiale dei dispositivi stessi, oppure se sono riusciti a consumare, ai nostri danni, attività di phishing informatico. Quindi è buona norma non lasciare mai i nostri dispositivi incustoditi e non protetti e guardarsi dal cliccare su link o allegati di posta elettronica sospetti.

20/09/2018