Mondo sempre più connesso? Occhio ai pericoli informatici!

Data: Invalid Date | Autore: Redazione



MILANO 17 LUGLIO -Il nostro mondo sta diventando sempre più *smart*, sempre più connesso alla rete, dove viaggiano milioni di dati ogni secondo, tra cui anche i nostri dati personali. E se da un alto questa iperconnessione ci aiuta nel lavoro, nella gestione della nostra vita e in molti altri campi, dall'altro bisogna stare sempre più attenti ai pericoli informatici. I cyber-attacchi infatti sono aumentati e si sono evoluti, costringendo il settore della cyber security a fare un balzo in avanti per fronteggiare questi pericoli. Ma quali sono gli attacchi informatici più frequenti? E un comune utente del web come può difendersi? Scopriamolo insieme in questa guida ai pericoli del web.

Tutti noi conosciamo i virus informatici per i quali abbiamo installato un antivirus nei nostri dispositivi, soprattutto computer. In realtà, la navigazione su internet avviene quasi sempre attraverso mobile ormai e dunque dobbiamo proteggere anche i nostri smartphone da possibili malware. I malware sono dei software – dunque dei programmi – malevoli che compromettono il funzionamento corretto del nostro dispositivo, fisso o mobile che sia. Tra i malware più frequenti troviamo:

• **Ransomware**: uno dei malware più pericolosi. Si infiltra nei computer e si finge l'amministratore tenendo in ostaggio il dispositivo e rubando i nostri dati. Tra i più famosi attacchi di questo tipo c'è WannaCry, che ha compromesso molte aziende nel mondo.

• **Spyware**: un malware che spia gli utenti, sia dal pc sia dallo smartphone, registrando dati sensibili e anche telefonate.

• **Phishing**: più che un programma, in questo caso si tratta di una truffa vera e propria, in cui un

hacker si finge qualcun altro per rubare le nostre informazioni personali.

• **Adware**: non tutte le pubblicità sono innocue. Oltre ad essere fastidiose infatti, possono nascondere dei programmi malevoli che vanno ad attaccare il nostro dispositivo.

Come possiamo proteggerci? Innanzitutto, come riportato all'inizio, installiamo un antivirus che comprenda le funzioni di anti spyware e anti phishing e che venga periodicamente aggiornato.

Dopodiché potete adottare alcune misure di sicurezza per proteggere i vostri dati e la vostra privacy:

• **Password sicure**: scegliete sempre con cura le vostre password per gli account. Ancor oggi la password più utilizzata è 123456 o la propria data di nascita: entrambe sono facilmente hackerabili, dunque scegliete una combinazione di numeri, lettere e simboli a cui difficilmente si può risalire.

• **Crittografia e verifica a due fattori**: molti servizi web ora mettono a disposizione, per gli account degli utenti, una crittografia avanzata e la verifica a due fattori, ovvero con due codici diversi. Quando è possibile adottate sempre questa misura di sicurezza.

• **Rete Tor**: un protocollo capace di mantenere l'anonimato, nascondere l'IP e crittografare le nostre ricerche? È possibile grazie a Tor, un browser per il web che mantiene al sicuro i vostri dati.

• **Virtual Private Network**: che cos'è una VPN? Si tratta di una connessione protetta, un tunnel virtuale in cui i nostri dati informatici viaggiano al riparo da possibili attacchi informatici.

Seguendo questi semplici consigli sarete già al sicuro dai cyber-attacchi più comuni e potrete navigare sul web senza problemi.

Articolo scaricato da www.infooggi.it
https://www.infooggi.it/articolo/mondo-sempre-piu-connesso-occhio-ai-pericoli-informatici/114999