

Non farti hackerare: 5 suggerimenti per sentirti ed essere più sicuro online

Pubblicato: Lunedì 28 Novembre 2022



Sebbene Internet possa essere una grande fonte di informazioni e di contatti, è importante essere consapevoli dei **pericoli** che ne derivano.

Per esempio, uno studio compiuto da [Investigoal](#) ha evidenziato come in Italia tra il 2020 e il 2021 le truffe online abbiano portato a una “perdita” pro capite di oltre 2 mila euro.

Fortunatamente, ci sono alcuni semplici accorgimenti che puoi adottare per **proteggerti dal rischio di diventare vittima di una truffa online**.

5 suggerimenti per non farti hackerare

Ecco i nostri **5 suggerimenti per non farti hackerare** e per proteggere la tua sicurezza mentre navighi online.

#1 – Fai uso dell'autenticazione a due fattori

Nell'era digitale di oggi, è più importante che mai mantenere le proprie informazioni personali al sicuro e protette. Un modo per farlo è utilizzare la verifica in due passaggi, nota anche come **autenticazione a due fattori**.

Quando si utilizza la verifica in due passaggi, si accede prima con la propria password. Successivamente, ti verrà richiesto di verificare nuovamente la tua identità, di solito con un dato biometrico (impronta digitale o scansione del volto), una chiave di sicurezza o un codice univoco una tantum tramite un'applicazione sul tuo dispositivo mobile.

Molti siti web e aziende offrono la verifica in due passaggi e di solito è davvero facile da configurare. L'uso dell'autenticazione in due passaggi può aiutarti a sentirti più sicuro, soprattutto per i siti che contengono informazioni finanziarie.

#2 – Utilizza sempre una VPN

Una **VPN** è una rete privata virtuale che consente di nascondere il proprio indirizzo IP e di navigare su Internet in modo anonimo. Quando ti connetti a una VPN, il tuo traffico viene

crittografato e instradato attraverso un tunnel sicuro, rendendo difficile per chiunque spiare le tue attività o rubare i tuoi dati.

Inoltre, una [VPN online](#) può anche aiutarti a bypassare la censura e ad accedere ai siti web bloccati. Collegandoti a un server in un Paese diverso, puoi far credere al portale web che ti trovi effettivamente in quel Paese, consentendoti di accedere a siti web che altrimenti non sarebbero disponibili.

#3 – Crea password complesse

Non è un segreto che le password siano essenziali per la nostra sicurezza online. Eppure, molti di noi continuano a preferire la comodità alla sicurezza, utilizzando la stessa password per ogni account.

Sebbene possa sembrare una seccatura ricordare più password, la realtà è che semplicemente **non è sicuro riutilizzare le stesse parole d'accesso**. Se uno dei tuoi account venisse violato, il malintenzionato avrebbe accesso anche tutti gli altri. E spesso ci si accorge che la propria password è stata violata solo quando è troppo tardi.

Per garantire la sicurezza dei tuoi account, gli esperti consigliano di utilizzare una password diversa per ciascun profilo. Tuttavia, sappiamo che creare password uniche può essere difficile da ricordare. Ecco perché è importante creare parole d'accesso forti che siano anche facili da ricordare.

Una **password forte** è una parola lunga almeno 12 caratteri. Concentrati su parole positive o su frasi che ti piacciono e che sono facili da ricordare (ad esempio, "Amo la musica country"). Su molti siti è possibile utilizzare anche gli spazi!

#4 – Stai attento a chi dai la tua fiducia

Negli ultimi anni, il fenomeno del **catfishing** ha conquistato le prime pagine dei giornali ed è diventato sempre più comune. Il catfishing si verifica quando una persona crea un falso profilo online, spesso sui social media o sui siti di incontri, per colpire vittime ignare.

L'obiettivo è, di solito, quello di estorcere denaro a qualcuno, chiedendo donazioni o ingannando le vittime di turno per far loro inviare direttamente del denaro. Gli adescatori spesso prendono tempo per instaurare una relazione online, guadagnando la fiducia della vittima per un periodo di mesi prima di fare la loro mossa.

Le perdite possono essere significative, con una media di oltre 15.000 dollari per vittima.

Per evitare di cadere nella trappola del catfishing, è importante essere consapevoli dei rischi e sapere

come proteggersi. Innanzitutto, non accettare richieste di amicizia da persone che non conosci. In secondo luogo, non inviare mai denaro a qualcuno che non hai incontrato di persona. Infine, se una situazione ti sembra sospetta o troppo bella per essere vera, fidati del tuo istinto e interrompi immediatamente i contatti con quella persona.

#5 – Controlla la sicurezza dei siti web che visiti

Un altro consiglio molto importante per proteggere le tue informazioni personali mentre navighi online è **verificare la presenza della certificazione SSL** quando si inseriscono i dati della carta di credito o della banca in un sito web.

Questo processo sembra complicato, ma in realtà è molto semplice. Basta guardare l'URL del sito in cui ci si trova. Se inizia con "https://", la connessione è crittografata e sicura e tutti i dati immessi saranno inviati al sito in modo sicuro.

Non tutti i siti dispongono della certificazione SSL, quindi evita di condividere informazioni finanziarie o personali su siti privi di questo ulteriore livello di sicurezza.

Inizia a utilizzare alcuni di questi consigli già da oggi. Se prendi l'abitudine di seguire le giuste pratiche di sicurezza, potrai sentirti più protetto online e consapevole delle comuni truffe informatiche.

[Redazione VareseNews](#)

redazione@varesenews.it