Navigare sicuri Come proteggersi dalle minacce informatiche

Amministratore delegato di Ne.W.S. - New Web Solutions srl

La sicurezza dei dati personali su Internet è un problema sempre più sentito dagli utenti comuni. Ecco alcune indicazioni per proteggere la propria privacy (e il portafoglio)

Ciascuno di noi, per il semplice fatto di essere connesso alla rete, è esposto quotidianamente a rischi di violazione della privacy, furto dei dati bancari, truffe.

La navigazione in Internet, l'utilizzo della posta elettronica, la frequentazione dei social network generano migliaia di informazioni sulle abitudini e sugli aspetti più sensibili delle nostre vite. Il rischio che terzi le utilizzino per scopi illeciti non è così remoto come può sembrare ed è pertanto necessario prendere una serie di precauzioni per proteggere i nostri dati personali, e la nostra stessa 'vita digitale'.

Il primo passo è porre la massima attenzione alle password che scegliamo per i nostri account. Non basta più scegliere password lunghe per tutelarci. È consigliabile inventarne di originali e non riconducibili alla nostra identità. Una soluzione è adottare **l'alfabeto 'Leet', nato ai tempi delle prime chat e che sostituisce alle lettere simboli e numeri** secondo un meccanismo di similitudini grafiche intuitive. Ecco che la A diventa 4 e la E 3, ed ecco che una password come Roberta1980 diventa R083RT41980. Un bel passo avanti!

Inoltre, è importante evitare di utilizzare la stessa password per più siti o servizi. **Diversificare le credenziali di accesso fa sì che, se un malintenzionato riesce a rubarci una password, può causarci un danno limitato.** Se invece ne usassimo una uguale per tutti gli abbonamenti, i servizi bancari e le caselle di posta, il furto potrebbe causare un vero disastro.

È evidente che adottare questi comportamenti ci espone alla facile eventualità di dimenticare le diverse combinazioni username-password. In questi casi, **ci vengono in aiuto dei veri e propri 'portachiavi virtuali', come 1Password e Lastpass**, in grado di custodire tutte le credenziali che desideriamo. Basterà ricordare una sola password, quella di accesso al portachiavi, per accedere a tutte le altre.

Una delle fonti di dati personali e sensibili di maggior valore per i malintenzionati sono i social network. Incuranti, pubblichiamo ogni giorno foto e status, comunicando al mondo dove siamo, cosa stiamo facendo e cosa ci piace. **Non è mai esistito un sistema più economico e semplice per prendere informazioni su una persona che guardare il suo profilo Facebook.**

Quindi il consiglio è di non accettare amicizie di cui non si è sicuri, oppure di relegarle in un raggruppamento di amici con forti restrizioni di condivisione, onde evitare che vengano a sapere quando siamo in vacanza, quali sono i nostri orientamenti politici o sessuali e tutto ciò di cui vogliamo rendere partecipi solo i nostri contatti più cari.

Da ultimo, è bene ricordare **l'importanza di mantenere i nostri strumenti di navigazione puliti e aggiornati.** Per ridurre la superficie attaccabile, infatti, è determinante conservare browser e sistemi operativi aggiornati all'ultima versione. Sono anche da evitare tutti quegli accessori, le cosiddette 'barre degli strumenti', forniti gratuitamente – guarda caso – e che si installano nei nostri browser: strumenti concepiti niente meno che per tracciare le nostre abitudini di navigazione.

SIMONE FOGGINI

Torinese, laureato in Economia e Commercio, dal 2000 è amministratore delegato di Ne.W.S. - New Web Solutions srl. Esperto di comunicazione online, si occupa di web marketing strategico e di progettazione di soluzioni e-business.

Ne.W.S. – Corso Alcide De Gasperi, 55 – Tel . 011.5806034 – www.ne-ws.it – info@ne-ws.it