VareseNews

Sicurezza informatica: l’ABC per navigare sicuri, senza commettere errori

Pubblicato: Mercoledì 12 Marzo 2025

Viviamo in un’epoca in cui gran parte delle nostre attività quotidiane si svolgono online: pagamenti, comunicazioni, acquisti e persino lavoro. Questo significa che **proteggere i propri dati** personali è diventato più importante che mai.

Ciò nonostante, ancora tantissime persone sottovalutano i rischi della navigazione web, esponendosi a minacce come il phishing, i malware e gli attacchi informatici.

Per evitare problemi e proteggere la propria privacy, bisogna adottare alcune pratiche di sicurezza di base. Una delle prime cose da fare è **creare credenziali sicure e difficili da indovinare**. Ma come si mette in pratica tutto questo? Ecco alcuni consigli per una password efficace e per proteggere i propri account da accessi indesiderati.

Proteggere i propri account: la prima regola della sicurezza informatica

Una **password debole** è come lasciare la porta di casa aperta: rende facilissimo l’accesso a chiunque. L’ideale è utilizzare una combinazione di lettere maiuscole e minuscole, numeri e simboli speciali, in modo da renderle difficili da decifrare.

Ovviamente, non bisogna utilizzare **mai la stessa password per più account**, per quanto robusta e indecifrabile essa sia. Per verificare la robustezza delle credenziali, si possono utilizzare strumenti online come il **Password Checker**, utilissimo per capire se le password scelte sono realmente sicure. Anzi, lo strumento permette anche di **individuare eventuali debolezze** e migliorare la protezione dei vostri account.

Navigazione sicura: riconoscere e evitare le minacce

Uno dei pericoli più diffusi in rete è il **phishing**, tecnica utilizzata dai criminali informatici per ottenere informazioni personali fingendosi aziende o enti affidabili. Questi attacchi avvengono spesso **tramite email o messaggi**, nei quali si trovano **link ingannevoli** che portano a siti web falsi.

Per proteggervi da questi pericoli, evitate di inserire dati sensibili su siti web che non utilizzano il protocollo HTTPS, riconoscibile dall'icona del lucchetto accanto all'URL nella barra degli indirizzi. Se si utilizzano reti **Wi-Fi pubbliche**, è bene **evitare di effettuare operazioni sensibili**, come pagamenti o log-in ai vostri account personali.

E per finire, occorre mantenere **sempre aggiornati browser**, **sistemi operativi** e **software** di sicurezza; gli aggiornamenti, infatti, contengono spesso patch di sicurezza che correggono vulnerabilità sfruttabili dagli hacker. Ignorandoli si lasciano aperte delle porte d'accesso a potenziali malintenzionati.

Software e strumenti di protezione: quali scegliere e come usarli

Il kit di base di ogni navigante della rete contiene, quantomeno, un buon **antivirus** e un **firewall attivo**. L'antivirus aggiornato aiuta a rilevare e bloccare malware, spyware e altri tipi di minacce, mentre il firewall impedisce accessi non autorizzati sul dispositivo.

Un altro strumento utilissimo è l'**autenticazione a due fattori** (2FA), che aggiunge un ulteriore livello di sicurezza agli account online. Con questa tecnologia, oltre alla password, viene richiesto un secondo codice di verifica, generalmente inviato tramite SMS o generato da un'app dedicata.

Infine, si deve evitare di sottovalutare il rischio, perché le statistiche di attacchi andati a buon fine nel nostro Paese sono in continuo aumento. Per questo, è bene **salvare sempre copie dei file più importanti** su un hard disk esterno o su un servizio cloud: in questo modo si potrà recuperarli in caso di attacco e mitigare i danni.

Redazione VareseNews
redazione@varesenews.it