

## SOLUZIONI TECNOLOGICHE

---

### ***Sicurezza e privacy, due concetti indivisibili***

di [Teamsystem.com](http://Teamsystem.com)

Con l'uso sempre più frequente e intensivo di , l'attenzione da porre alla nostra è diventata un concetto sempre più importante. Interesse alla sicurezza per impedire a software maligni di infiltrarsi nei nostri computer, tablet o smartphone, ma anche alla , cioè alla protezione delle nostre abitudini che possono rappresentare un vero e proprio tallone di Achille.

Con questo concetto in mente, qualche settimana fa **Sophos**, una delle aziende più importanti a livello mondiale nel campo della sicurezza informatica ha deciso di proporre una "dieta" da seguire per proteggere la nostra privacy. I consigli di Sophos si articolano in realtà in tre semplici operazioni che hanno il compito di eliminare o perlomeno ridurre, alcune vulnerabilità a cui siamo sempre più esposti. Ecco di cosa si tratta.

#### **1. Disattivare la geolocalizzazione da tablet e telefoni**

Si tratta di spegnere quelle funzioni che spesso si attivano automaticamente quando lanciamo applicazioni come **Google Maps**, navigatori satellitari o ci colleghiamo a social network come **Facebook** o **Twitter**. Questi strumenti hanno il compito di tracciare la nostra posizione e quindi i nostri spostamenti. È spiacevole sapere che qualche malintenzionato possa controllare i nostri spostamenti anche quando pensiamo di non essere "seguiti" da nessuno.

#### **2. Disattivare il Wi-Fi quando non ci serve**

Collegarci a una rete senza fili per navigare è la cosa più normale da fare quando si controlla la posta da uno smartphone o da un tablet. Ma una volta usciti dall'ufficio o da una sala conferenze, quante volte ci ricordiamo di spegnere il Wi-Fi del dispositivo? Se lo facciamo sempre, vuol dire che siamo delle persone molto accorte, ma spesso la distrazione potrebbe avere il sopravvento. In questo caso ricordiamoci che normalmente uno **smartphone con Wi-Fi attivo cercherà costantemente delle reti alle quali collegarsi**. E non è in grado di sapere quali sono sicure e quali no. Cosa accadrebbe se, mentre ci troviamo in giro, il telefono o il tablet si collegassero a una rete aperta e qualcuno intercettasse le nostre mail? Inoltre, teniamo presente che passare da una rete all'altra fornisce, ancora una volta, una mappa completa dei nostri spostamenti: di nuovo **una minaccia per la nostra privacy**.

#### **3. Eseguire il log-out dopo il collegamento a un sito protetto**

Difficilmente ormai ci rechiamo in banca di persona per **eseguire un bonifico**, chiedere un estratto o controllare che il **pagamento di un cliente** sia arrivato sul nostro conto. Queste operazioni le eseguiamo sempre più spesso online inserendo il nostro account e codice di sicurezza sul sito della compagnia. Ma alla fine dell'operazione ci ricordiamo di uscire facendo clic sul tasto che nella maggior parte dei casi si chiama **"logout"** o **"esci"**? Stessa cosa dopo aver aggiornato il nostro **profilo Facebook**. Ricordiamo sempre di scollegarci o chiudiamo semplicemente la finestra del browser? Teniamo sempre presente che una volta completate le procedure di accesso a un sito protetto, abbiamo aperto le porte a quei contenuti. Un po' come succede con la porta di casa. Se giriamo la chiave per aprire, dovremmo fare la stessa cosa anche quando usciamo. In caso contrario, sarebbe come lasciare aperto un collegamento che un eventuale malintenzionato potrebbe sfruttare per intrufolarsi nei nostri affari.

Che quello della sicurezza sia un tema particolarmente sentito lo dimostra anche un recente studio condotto da **HP Security Research** che dal 2009, ogni anno realizza un report completo in tema di minacce informatiche. Proprio qualche giorno fa sono stati pubblicati i risultati dell'ultimo **Cyber Risk Report 2013** che mette in guardia le aziende in generale, ma anche gli sviluppatori di soluzioni software contro una rete di cybercriminali sempre più organizzata e insidiosa. Insomma, senza dover per forza diventare paranoici, ogni precauzione in grado di proteggere i nostri dati e la nostra sicurezza, va presa sul serio e adottata con la massima velocità.