Ogni viaggiatore moderno porta sempre con se un tablet o un laptop da utilizzare per il lavoro, per l'intrattenimento o per rimanere in contatto con casa. Il laptop diventa depositario di ricordi, di documenti importanti, della musica o delle foto dei propri cari... ma è tutto al sicuro?

Qualche giorno fa ho letto una notizia molto inquietante riportata online da diversi giornali di settore: un gruppo di hacker è riuscito a rubare un archivio da un computer di un agente del FBI contente gli identificativi dei dispositivi iOS (gli iPhone o simili per capirci) e dei relativi dati anagrafici dei rispettivi proprietari (link). La notizia è volata da sito a sito ed è stata seguita da diverse smentite da parte dell'FBI. Che sia vera o meno non ha importanza. Il punto è che i nostri portatili sono sempre esposti ad un possibile attacco, un furto o, più semplicemente, ad un malfunzionamento.

Vediamo 7 alcuni consigli per cercare di ridurre i rischi salvaguardando le nostre informazioni.

1. Sistema operativo, antivirus e firewall sempre aggiornati

Sembra un consiglio banale, ma capita molto spesso che per disattenzione non si effettui un aggiornamento costante dei propri sistemi. L'aggiornamento è fondamentale per gli utenti Windows, ma non ne sono esclusi gli utenti Mac (Apple): volete essere voi i primi ad inviare un virus al vostro vicino?

2. Fare periodicamente il backup

Non sapete quante volte ho sentito gli improperi di colleghi ed amici che avevano perso tutti i dati dopo un aggiornamento di una applicazione del proprio computer. E voi volete perdere le foto della vostra famiglia a causa di un malfunzionamento del proprio hard disk?

3. Bloccare il computer

E' importatissimo mettere sempre una password al vostro computer in modo che si blocchi dopo qualche minuto di inattività. E' altrettanto importante non lasciare mai incustodito il proprio portatile/tablet. Se lo dovete lasciare su un tavolo, usate un lucchetto con un cavo di acciaio per fissarlo. L'ufficio e l'albergo sono i primi due luoghi in cui viene rubato un laptop. Un lucchetto può fare la differenza.

4. Lasciate tutti i dati sensibili crittografati in un luogo sicuro

Abbiamo spesso parlato negli altri articoli di soluzioni per crittografare e proteggere i dati come TrueCrypt o AesCrypt (vedi 2010: Top Apps) e tali programmi sono la soluzione migliore nel caso in cui ci si debba portare con se dati sensibili (dati medici, conti bancari, etc). In ogni caso, è sempre consigliabile portare il minimo indispensabile e lasciare tutti i dati non necessari in una pendrive (o un harddisk) in un luogo sicuro (magari sottochiave). Le pendrive con dati sensibili non vanno mai lasciate incustodite (es: camere di albergo) ed i dati vanno sempre crittografati.

5. collegamento WiFi

Diffidate dei collegamenti senza protezione ed apparentemente "liberi". Utilizzateli solo per collegamenti che non trasmettano dati importanti (navigare su internet va bene, ma non utilizzateli per accedere al sito della banca o alla posta). Molto spesso le connessioni gratuite (in genere quelle offerte negli alberghi) non sono protette (cifrate) ed è meglio evitare di usarle per visitare siti Web con dati sensibili. Se necessario, utilizzate una collegamento via cavo o una WiFi con i sistemi di sicurezza attivati di tipo WEP o WPA.

Se vi collegate ad una rete aziendale, è buona norma utilizzate il collegamento VPN (Virtual Private Network
) od utilizzate un collegamento 3G o 4G.

In generale, evitate di fare acquisti od operazioni bancarie su rete non protette o sconosciute.

6. Diffidate dei servizi in Cloud (vedi Cloud or No Cloud?)

I servizi Cloud sono un nuovo modello a supporto degli utenti che, attraverso la rete, demanda tutte le problematiche di sicurezza ed affidabilità al fornitore del servizio (provider). Molti provider, per contratto, non garantiscono agli utenti la totale sicurezza dei loro sistemi e la completa affidabilità. Il livello di servizio, denominato SLA: Service Level Agreement, è spesso indicato nel contratto e solitamente protegge il Provider (a scapito dell'utente).

7. In generale: diffidare sempre

Richieste di aggiornamenti inaspettate, mail verosimili da utenti sconosciuti, allegati eseguibili ad email non voluti, programmi scaricati da fonti sconosciute sono solo alcune dei probabili rischi a cui sottoponete il vostro laptop. Fate sempre molta attenzione perché non si è mai troppo sicuri

Alla prossima.

(17/09/2012)