Sicurezza informatica: quali sono gli errori da evitare?

19 settembre 2011

Internet è funestato da cybercriminali sempre più abili e competenti. La CyberDefender Corporation ha stilato la classifica dei 10 comportamenti più a rischio, e ha scritto alcuni suggerimenti per navigare più tranquilli.

"I social network, le aste, i giochi multiplayer sono tra le applicazioni che devono la loro fortuna alla rete", afferma CyberDefender. Internet, tuttavia, è anche un luogo pericoloso "ed è opportuno rispettare dei semplici accorgimenti per limitare i possibili danni".

I dieci errori commessi più frequentemente dagli utenti sono:

1) "Mantieni la connessione" da un PC pubblico. Mai selezionare l'opzione "keep me signed in" (mantieni la connessione) se non si sta utilizzando il proprio PC. Quando ci si connette da una postazione pubblica, assicurarsi di aver deselezionato l'opzione per evitare di lasciare su un PC che viene utilizzato da più persone informazioni private come password e dati di accesso ai servizi, ai quali chiunque potrebbe risalire dalla cartella cookies. È opportuno procedere anche alla cancellazione delle cache e dei cookie.

2) Aggiornamenti. I sistemi operativi (come Windows) o i programmi come Java, Adobe Reader o Adobe Flash contengono dei punti deboli e sono perciò vulnerabili ad attacchi esterni. Lo diventano ancora di più se non vengono aggiornati periodicamente. Per evitare questi problemi, abilitare gli aggiornamenti automatici e installarli immediatamente.

3) Gossip. Le persone gravitano spesso e volentieri intorno alla vita privata delle celebrità, gli hacker progettano attacchi sempre nuovi rivolti a questo pubblico curioso. Un consiglio è quello di utilizzare l'indirizzo https://www.google.com invece del comune http://www.google.com. Il primo indirizzo, infatti, invia la ricerca su una connessione criptata e questo riduce i rischi di virus (SEO poisoning).

4) BitTorrent. È sempre un rischio utilizzare i cosiddetti "torrent" per scaricare contenuti protetti da diritto d'autore come film, software, programmi televisivi eccetera. Anche se sono siti sicuri, alcune fra le pubblicità presenti potrebbero comprometterne la sicurezza. Per non imbattersi in virus come trojan e spyware, per il download o lo streaming di contenuti, è meglio servirsi di iTunes, di Netflix o di Hulu/Hulu Plus.

5) Allegati. Allegati e link delle email andrebbero sempre trattati con prudenza. Se la email arriva da uno sconosciuto è meglio non aprirli. Anche nel caso in cui il mittente sia una persona a noi conosciuta, è importante fare attenzione perché il suo computer potrebbe essere infetto. Per evitare i virus è utile tenere sempre aggiornato e in funzione il software di sicurezza e avviare una scansione antivirus prima di aprire qualsiasi messaggio.

6) Giochi on line. I siti che offrono giochi gratuiti, social games o le applicazioni Facebook sono generalmente sicuri. Fare attenzione ai siti sconosciuti che chiedono di scaricare i loro programmi. Utilizzare soltanto siti conosciuti e fidati e assicurandosi prima che sia attivo l'anti-virus.

7) Social Network. Impostare le opzioni sulla privacy di Facebook per non consentire a chiunque di visualizzare informazioni private come l'indirizzo email, la data di nascita, il numero di telefono..., che possono essere usate per impossessarsi della nostra identità. Verificare sempre le impostazioni sulla privacy, assicurarsi che i dati privati siano tuttalpiù visibili ai soli amici. Essere sempre cauti non è mai esagerato: perciò evitare di fornire troppi dettagli sui viaggi, sui soggiorni all'estero, su attività durante le quali la casa resta disabitata, evitare assolutamente di dare informazioni bancarie o della carta di credito.

8) Reti wireless. Connettersi solo a reti ufficiali. Prestare attenzione alle reti wireless degli aeroporti, degli alberghi, dei

luoghi pubblici. Intercettare queste connessioni riproducendo una rete reale e sicura per avere pieno accesso ai computer che vi accedono è molto facile.

9) Password. Avere password diverse per i vari servizi utilizzati online è certamente più complesso, ma è decisamente sconsigliabile avere la stessa password. Una unica parola di accesso online può venire "rubata" più facilmente mettendo in pericolo i nostri dati. Per questo è importante usare più password e diversificare, in modo particolare, quella della posta elettronica da quella per i social network da quella usata per servizi online.

10) Vincite improbabili. Mai fornire informazioni personali a siti che sostengono di regalarti gadget come iPad o PlayStation o viaggi o, addirittura, soldi. Sono chiaramente delle truffe!

Fonte : Comunicatori & Comunicazione