PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 6 - numero 955 di lunedì 08 marzo 2004

Internet, posta elettronica e privacy: esigenze di sicurezza e comportamenti a rischio (2/2)

A cura del Dott. Gerardo Costabile - Iacis member. Vademecum per la sicurezza dei personal computer.

[Pubblichiamo oggi la seconda parte dell'estratto dell'intervento del dott. Gerardo Costabile ? Member of "The International Association of Computer Investigative Specialists" - durante la conferenza "Privacy e studi legali", svoltasi a Verona il 27 febbraio 2004.
La prima parte dell'articolo è stata pubblicata sul numero 954 di PuntoSicuro.]

Vademecum per la sicurezza dei personal computer

1) La sicurezza totale non esiste: informatevi, tenetevi aggiornati, prevenite.

2) Attivate la password di BIOS e la password dello screen saver, al fine di evitare che altre persone possano accedere al computer e carpirne i dati durante la vostra assenza.

3) Modificate periodicamente le password ed evitate di affidare a Windows la memorizzazione automatica delle stesse (posta elettronica, accesso remoto, etc.). Tutte le password gestite direttamente dal sistema operativo Windows sono altamente insicure. E' consigliabile digitare la password ogni volta che questi servizi vengono utilizzati.

4) Considerate il PC come un oggetto personale sia in azienda che in casa, alla stregua di carte di credito, carta d'identità, ecc. Non consentitene l'utilizzo a chiunque e, nel caso di problemi hardware o software che comportino la necessità di interventi, preferite sempre l'assistenza qualificata.

5) Attuate sempre una valida protezione hardware di base, ponendo una o più etichette adesive autografate sulle viti posteriori del cabinet (la stessa tecnica attuata da molte case produttrici per controllare l'invalidazione delle garanzie).

6) Evitate di usare la connessione internet con un PC contenente dati riservati e/o personali. Se è inevitabile la connessione, durante le navigazioni attivate sempre un firewall (locale o di rete) e mantenete attivo in background un antivirus costantemente aggiornato. Impostate i livelli di sensibilità e di protezione al massimo.

7) Eseguite la criptazione di tutti i files riservati o particolarmente delicati utilizzando chiavi non banali di lunghezza min. 8 caratteri alfanumerici e, normalmente, non presenti nei vocabolari in nessuna lingua (es. "32y47f_lvj"). Evitare assolutamente chiavi "brevi" e/o riferite a parole presenti nei vocabolari, come ad esempio "sole" o "computer", nomi propri, date di nascita, ecc. Eventualmente dotatevi di un programma di crittografia (es. PGP). Molti sono freeware, liberamente scaricabili da internet, e, spesso, si trovano anche nei CD delle riviste specializzate del settore. La maggior parte di essi permette anche funzioni di cifratura della posta elettronica e di firma digitale.

8) Evitate assolutamente comportamenti a rischio durante la navigazione in Internet; Internet è probabilmente la più potente risorsa multimediale a disposizione dell'umanità, ma l'approccio ad esso deve essere governato da conoscenza, moderazione e prudenza di fondo.
Sono comportamenti a rischio:
-la navigazione su siti di Hacking, cracking, ecc, senza apposite protezioni;
scaricare software da siti poco attendibili o non ufficiali;
-aprire messaggi di posta elettronica e eseguire files allegati ai messaggi senza preventiva scansione antivirus (anzi, prima si

dovrebbe effettuare l'aggiornamento e poi si dovrebbe aprire il programma di posta elettronica);
-installare programmi scaricati da siti non ufficiali o comunque di natura incerta;
-dar credito a un messaggio pubblicitario dalle caratteristiche sospette (spesso di natura erotica o che promette facili guadagni) che reindirizza ad un sito internet "per saperne di più";
-tenete sempre attivata l'opzione del browser "richiedi conferma" per l'installazione e il download di oggetti sulla vostra macchina. Disattivate sul browser l'esecuzione automatica degli script Java e ActiveX;
-mentre navigate prima di selezionare un link, posizionateci sopra il cursore del mouse e osservatene il percorso sulla apposita barra del browser: se è un file eseguibile probabilmente è un -trucco per scaricarvi un dialer o peggio;
-evitare di inviare posta elettronica in formato "html" che, seppure consente una forma più elegante e/o simpatica, è uno dei metodi più subdoli per veicolare contenuti virus, worm e frodi (senza necessità di allegati).

9) Eseguite periodicamente la pulizia del disco da cookies, file temporanei, etc. e, successivamente, cancellate gli stessi definitivamente con programmi specifici.

10) Ricorrete possibilmente alle versioni più recenti del sistema operativo e dei programmi maggiormente utilizzati, con particolare riferimento agli applicativi che consentono l'accesso ad internet.

11) Testate periodicamente il vostro PC per verificarne il livello di sicurezza, mediante importanti siti internet specializzati.

12) Non rispondete ai messaggi di posta "non sollecitati", chiedendo di essere cancellati da quella lista di invio: in tal modo rischiate di fare il gioco di chi li ha spediti, facendogli capire che la vostra casella di posta è attiva.

13) Non comunicate la vostra mail a siti ai quali non siete veramente interessati e/o sui quali avete anche il minimo dubbio.

14) Evitate i falsi allarmi e le catene di S. Antonio, controllando preventivamente la bontà delle informazioni prima di girarle (ad esempio grazie a siti specializzati come http://www.attivissimo.info/antibufala/elenco.htm).

(*) Firewall: Letteralmente significa "muro di fuoco". Meccanismo HW e/o SW che permette di impostare restrizioni all'accesso ad uno o più computer collegati in rete. In genere rappresenta l'insieme delle misure di sicurezza a protezione dei dati fra la Rete (aziendale o esterna) e un calcolatore. E' un sistema progettato per arginare l'accesso ai dati, impedendo, ad esempio, agli utenti provenienti da Internet, l'accesso non autorizzato ad una Intranet, cioè una rete privata.

---

www.puntosicuro.it