DECALOGO SICUREZZA E PRIVACY

In questa guida viene riportato un decalogo, semplice da seguire, con quelle che sono le regole basilari per poter godere l'utilizzo del nostro pc in piena sicurezza senza l'intrusione di "fattori disturbatori". Troppe volte si sottovaluta il fattore sicurezza ma in un'era dominata dalla trasmissione di informazioni, a volte anche sensibili, sulla rete internet curare la propria privacy e il salvataggio dei propri dati sono diventati una necessità non più trascurabile.

Introduzione:

1. Assicurate il vostro PC dal punto di vista fisico;
2. Utilizzate un antivirus aggiornato;
3. Eseguite regolari backup del PC;
4. Utilizzate password forti e cambiatele regolarmente;
5. Adottate il sistema di cifratura per le informazioni più importanti;
6. Navigate in Rete in modo prudente;
7. Installate un firewall;
8. Usate la posta elettronica in maniera sicura;
9. Aggiornate il sistema periodicamente;
10. Proteggete le vostre connessioni.

1. La sicurezza fisica:

Primo: assicurate il vostro PC dal punto di vista fisico. Potrà sembrare scontato, ma anche la protezione da pericoli reali o dalla possibilità di furti e danni esterni è un aspetto da non sottovalutare. In particolare, occorre prestare attenzione agli allarmi, alle chiusure dei cabinet o dei luoghi in cui si conservano i PC. Questa lista di 10 promemoria può aiutare ad assicurare meglio i propri computer:

1.1 posizionate i computer in aree che possano essere chiuse a chiave o in cui si possano installare allarmi;
1.2 assicuratevi che l'accesso alla stanza con i PC sia controllato visivamente da qualcuno;
1.3 per computer di maggior valore o server dedicati, restringete l'accesso o mettete un sistema di identificazione;
1.4 considerate sempre anche il rischio di un incendio: adottate i sistemi di prevenzione;
1.5 fate in modo che un responsabile chiuda a chiave i locali quando non c'è nessuno;
1.6 controllate gli allarmi regolarmente;
1.7 marchiate i computer dell'impresa con informazioni per identificare il proprietario, la scuola, il luogo;
1.8 conservate i numeri seriali dei PC nel caso di furto;
1.9 stabilite regole chiare per gli utenti che utilizzano dispositivi mobili o apparecchiature di valore e rendeteli responsabili della restituzione;
1.10 fate installare gruppi di continuità utili nel caso di black out, in particolare per portare corrente ai server o ai computer che non devono subire interruzioni o fermi macchina.

2. Antivirus su misura:

Seconda regola: utilizzate un antivirus aggiornato.
Non ci sono altre precauzioni così importanti come l'adozione di un software antivirus. La sua azione è preventiva, lavorando a monte delle infezioni. Permette la scansione dei file che vengono trasferiti sul PC via e-mail, via rete o semplicemente come copia da memorie esterne (floppy, ecc.) e pulisce quelli che presentano programmi maligni. Gli antivirus più evoluti mettono anche in quarantena i file incriminati, permettendo agli utenti di analizzare anche contenuti infetti e capire di quale pericolo si tratta. Per un uso corretto di questi applicativi è consigliabile seguire questi principi:

A. occorre installare un antivirus su ogni macchina di una rete;
B. l'antivirus deve essere adeguato alle proprie esigenze e all'esposizione al pericolo;
C. il software va aggiornato frequentemente, anche più volte al giorno, in caso di notizia di attacchi particolarmente virulenti sulla rete Internet, ricevendo informazioni e aggiornamenti dai produttori del software;
D. è necessario adottare qualsiasi meccanismo di autoprotezione disponibile, in particolare l'avvio automatico dell'antivirus;
E. non disattivare mai le protezioni antivirus sulla posta in entrata, in uscita, sugli script e sulle macro, se disponibili;
F. lanciare periodicamente un controllo completo del proprio PC, come se fosse un malato su cui fare un check up per valutare lo stato di salute. Per questa analisi è possibile utilizzare gli strumenti di pianificazione dell'antivirus, che permettono di eseguire in automatico, secondo un periodo prefissato, la scansione dei dischi e delle periferiche;
G. per i più esperti, è consigliabile anche tenere dei dischi di installazione del sistema a portata di mano e un set di dischetti di emergenza, di sola lettura, con i file di base per il ripristino di un sistema compromesso.

L'elenco riportato vale come guida per un comportamento responsabile, ma è ovvio che a monte di un antivirus deve esserci la precisa consapevolezza che ogni file, la cui provenienza non è accertata, è potenzialmente pericoloso e che non si devono aprire tutti i file ricevuti. Di questo devono essere consapevoli tutti gli utenti di PC. Allo stesso modo è assolutamente indispensabile mantenere aggiornato l'antivirus. Avere un software che non è al passo con il database dei virus in circolazione è sinonimo di esposizione alla contaminazione. Nella scelta di un antivirus, dunque, è preferibile adottare quelli che permettono il downolad da Internet degli aggiornamenti rilasciati in tempo reale.

3. Archiviare le informazioni utili:

Si chiama "back up", tecnicamente. Più semplicemente significa creare un "archivio delle informazioni che potrebbero tornare utili nel tempo". Un po' come fare delle fotocopie da inserire in un faldone distinto da quello originale per evitare, in caso di incendio, di perdere preziosi documenti. Anche con il PC è necessario predisporre copie da archiviare per prevenire gravi danni ai sistemi o alle apparecchiature hardware. È una prassi necessaria, soprattutto per salvaguardare la propria attività didattica o la conservazione di informazioni privilegiate, magari di tipo amministrativo. La stessa nuova legge sulla privacy, impone di fare la copia settimanale dei database che contengono le informazioni.

In generale dunque, come terza regola della sicurezza eseguite regolarmente il back up della macchina su cui è svolta un'attività. In pratica come si fa? Tenuto conto che fare un back up significa spostare determinati dati da un supporto informatico a uno differente, esistono back up completi e parziali, in base alla volontà di conservare tutto o solo una parte delle informazioni. Sta all'utente scegliere che cosa è più utile ai fini della conservazione dei dati, quanti ne vuole conservare e con quale frequenza desidera aggiornare il proprio archivio. Allo stesso modo esistono

sistemi per eseguire copie una tantum o in maniera pianificata. Il primo fa capo al semplice trasferimento di dati su floppy, Cd-Rom, Dvd. Il secondo all'impiego di sistemi software e hardware per regolarizzare la copia di dati sui supporti esterni o rendere più facile un eventuale ripristino delle informazioni perse.

4. Questione di password:

La password è il modo più comune per autenticare un'identità. È la chiave da inserire nella "serratura digitale" di un PC per accedere ogni giorno ai programmi e alle risorse utili. Come tutte le serrature, però, deve funzionare e la chiave deve avere determinate caratteristiche che rendono difficile ogni tentativo di scasso. In primo luogo, perché questo si verifichi, è necessario impiegare termini difficilmente indovinabili. Un esempio classico di parole da evitare, per esempio, è la login uguale al nome e la password al cognome, oppure al nome dell'istituto e alla città che lo ospita. Oppure al luogo di nascita o di residenza, oppure informazioni e dati facilmente riconducibili agli utenti o agli amministratori.

La regola più indicata è: utilizzate password forti e cambiatele regolarmente.

Ma che cosa significa in concreto una password "forte"? Partiamo, inizialmente, da alcuni esempi di segno opposto, ovvero dalle password deboli, per focalizzare la questione:

A. l'assenza di password è un grave errore. Così come la login uguale alla password. Permettono un accesso nel sistema senza alcuna difficoltà;
B. il nome reale del proprietario del PC, come già accennato, o il nome dell'istituto di appartenenza è sconsigliabile. Troppo immediato;
C. parole dal significato compiuto, sebbene meno immediate, sono comunque facilmente attaccabili attraverso sistemi automatici di scasso basati sui dizionari;
D. vanno evitate, inoltre, parole comuni, come "password" o formule del tipo "1234", tipica per esempio delle segreterie telefoniche.

Al contrario, invece, si possono definire queste regole per aumentare la forza di una password:

1. ogni password deve avere almeno 8 caratteri. Ma più è lunga meglio è.
2. è utile inserire una combinazione di maiuscole e minuscole, lettere, numeri e simboli (compreso lo spazio), come potrebbe essere a titolo di esempio questa stringa: "JFk7!e02". Ovviamente la difficoltà è quella di ricordarla;
3. rende forte una password la sua durata limitata nel tempo. Buona norma sarebbe quella di cambiarla ogni 3 mesi, meglio ancora ogni 45 giorni. Nel momento in cui si cambia, è necessario anche produrre significative variazioni dalle password precedenti.

Come ricordare le password? È possibile per esempio affidarsi a piccoli trucchi, anche se è meglio stare attenti che non rendano riconoscibile le parole nascoste.
In ultimo, si possono usare acronimi, come per esempio"Su1inM" che sta per "sono un asso in matematica". Attenzione, però, a non usare formule che abbiano un senso noto, perché se lo hanno per voi, potrebbero averlo anche per chi cerca di scassinare la vostra autenticazione. Infine, è giusto ricordare che esistono programmi e meccanismi automatici per trovare un password. Talvolta è soltanto una questione di tempo, per cui ogni password va custodita come la chiave di casa. Non va mai ceduta a nessuno. Se qualcuno viene a conoscenza della vostra password, il PC è potenzialmente vulnerabile.

5. File cifrati:

Così come le password proteggono l'accesso all'intero sistema, anche a livello più basso, per i singoli file che contengono informazioni riservate, esistono sistemi di difesa che impediscono l'accesso indesiderato da parte di persone indiscrete, ladri o hacker. In entrambi i casi se rubano il PC avete la certezza che hacker e curiosi faranno veramente fatica a trovare una via di accesso ai vostri dati. Per proteggerli, dunque, potete applicare la quinta regola: adottate il sistema di cifratura per le informazioni più importanti. Come fare? Sul mercato esistono software dedicati per crittografare le informazioni, ma spesso si tratta di applicativi complessi, che vincolano in maniera troppo forte l'uso e lo scambio di informazioni cifrate. Windows XP, invece, permette di cifrare i dati in modo davvero semplice.

6. Sul Web senza paura:

Internet è una minaccia o una risorsa? Certamente la seconda, ma non si deve dimenticare, in chiave di sicurezza informatica, che un canale così vasto è anche fonte di numerosi quanto sofisticati pericoli in cui spesso incappano studenti o docenti poco esperti. Come sesta regola si può dunque dire: navigate in modo prudente. In sostanza significa ancora una volta stabilire alcune regole e attenervisi. Sia per quanto riguarda la navigazione individuale sia se si consulta Internet in un contesto di gruppo, per cercare informazioni, svolgere ricerche o approfondire temi legati ai propri interessi. Ecco alcuni principi chiave, ovviamente da interpretare secondo le esigenze individuali:

1. non accedete a siti che non considerate affidabili;
2. non eseguite transazioni, acquisti di materiale didattico o pagamenti di servizi utilizzando circuiti bancari sconosciuti;
3. non navigate sul Web direttamente dal server di una rete. Questo perché nel caso si incappasse in un elemento compromettente per la sicurezza, il danno sarebbe ovviamente più elevato;
4. accedete a Internet con un firewall (di questo parleremo tra breve in dettaglio);
5. stabilite una politica condivisa per la navigazione e rendetela nota a chi usa i PC (Disciplinare per l'utilizzo di internet). In particolare, stabilite quali comportamenti sono considerati illeciti (per esempio, la navigazione su siti pornografici, violenti, illegali ecc.). È ovvio che non riguarda soltanto la sicurezza, ma l'etica del navigatore Web.

7. Una barriera chiamata firewall:

Settima regola: installate un firewall. Questo principio non ha deroghe. Il firewall, infatti, è uno degli strumenti più utili per contrastare i tentativi di intrusione su un PC e in una rete. Di che cosa si tratta? Un firewall, con buona approssimazione, è un sistema in grado di decidere quali informazioni e dati far passare e quali fermare in una rete. Ispeziona, cioè, il flusso di dati che passa sulla rete locale, intervenendo nel momento in cui identificasse qualcosa di non permesso dalle regole che l'amministratore del firewall ha deciso. Un firewall può essere sia un dispositivo fisico esterno al PC sia una componente software che collabora con il sistema operativo e i programmi installati. Microsoft Windows XP, per esempio, ha in dotazione un firewall, denominato Windows Firewall, a protezione dei dati personali e contro le intrusioni non autorizzate. Semplice e flessibile, permette di bloccare le connessione alla rete da parte di programmi. Due ultimi dettagli prima di passare alla posta elettronica. Tra i vantaggi di un firewall è giusto annoverare anche la capacità di nascondere i singoli PC di una rete all'esterno. In altre parole un firewall rende la vita difficile agli hacker che desiderano raggiungere una determinata macchina, poiché le identità sono coperte e protette in maniera specifica. Infine, è necessario ricordare ciò che un firewall non può fare. È giusto sapere anche questo, per evitare spiacevoli sorprese. Per esempio, non protegge da attacchi iniziati quando una rete è già stata compromessa, oppure da alcuni virus che non transitano dalla rete (per esempio presenti in file su floppy disk). Non protegge, in ultimo, da intrusioni interne, cioè da hacker che hanno iniziato a danneggiare la rete dall'interno di un istituto.

8. Posta elettronica sotto controllo:

Ottavo: usate la posta elettronica in maniera sicura. Possedere un sistema di posta elettronica sicuro non è più un optional, ma un reale vantaggio. Considerato il crescente bisogno di utilizzare la rete per comunicare e condurre attività amministrative, tenere sotto controllo i sistemi di e-mail è infatti fondamentale per dare continuità, sicurezza e protezione al lavoro e alle attività didattiche. La posta elettronica tuttavia, essendo il più usato servizio basato su Internet, è anche il più sfruttato sistema per portare attacchi alla sicurezza dei PC. Virus, spam, script maligni, macro: le minacce più sofisticate oggi arrivano proprio via e-mail. Per questo motivo è opportuno adottare le dovute cautele, seguendo regole di comportamento semplici quanto efficaci.
Eccone alcune di base:

1. tenete aggiornato il software per la posta elettronica. Per questo visitate spesso il sito dei produttori del vostro software, scaricate e installate le patch indicate;
2. installate un antivirus che controlli la posta in entrata e quella in uscita;
3. filtrate lo spamming, creando regole o scegliendo i produttori che permettono di impostare filtri automatici;
4. non aprite gli attachment (allegati) considerati pericolosi;
5. non rispondete allo spamming, perché confermereste di avere un account di posta attivo. Semplicemente cancellate le e-mail indesiderate;
6. non fornite mai dati sensibili via e-mail. Per esempio non trasmettete mai password, numeri di carta di credito, informazioni personali.

Anche in questo caso si tratta di regole di comportamento. Esistono poi software che agevolano l'esecuzione di tutto ciò in maniera automatica.

9. Aggiornare il sistema:

Nona regola: aggiornate il sistema periodicamente. Ogni accorgimento rischia di non essere sufficiente per una protezione completa se i sistemi operativi o le applicazioni non sono aggiornate con regolarità ed efficacia. Microsoft rilascia gratuitamente una volta al mese aggiornamenti e patch proprio per proteggere e migliorare i propri prodotti nel corso del tempo. Per chi dispone di un PC con sistema operativo Microsoft o di prodotti della famiglia Office esistono due semplici sistemi per verificare i livelli di sicurezza e di aggiornamento del software impiegato. Il primo è Microsoft Windows update. Un meccanismo immediato che grazie al collegamento Internet al sito effettua una scansione del sistema e suggerisce quali componenti aggiuntive scaricare gratuitamente e installare. Il secondo, invece, è specifico per chi usa il software per la produttività individuale Microsoft Office 2000, Microsoft Office XP e prodotti della piattaforma Office System. Anche in questo caso, collegandosi al sito microsoft vengono suggerite agli utenti le ultime migliorie realizzate da Microsoft per rendere più efficiente e sicuro il software. Con un download e l'installazione delle componenti aggiuntive si eliminano rischi e nuove minacce.

10. Connessioni protette:

Decima regola: proteggete le vostre connessioni. Lavorare da casa, collegarsi alla rete dell'Università in viaggio, connettersi dall'esterno alla rete di un’impresa sono situazioni sempre più frequenti. Consentire i collegamenti da remoto e mettere a disposizione l'e-mail anche a distanza permettono una flessibilità mai conosciuta in precedenza. Sono soluzioni che rappresentano una risorsa importante per flessibilizzare le attività, la collaborazione e lo scambio di informazioni. Al tempo stesso, però, sono elementi di grande esposizione al rischio. Lo stesso deve valere per il sistema di trasmissione dei dati o i dispositivi mobili. Se la connessione avviene sulla rete pubblica

di Internet, chiunque potrebbe insinuarsi e utilizzarla per i più disparati scopi. Allora è bene ricorrere alle contromisure adeguate. Crittazione dei dati e severe procedure d'autenticazione sono tra gli strumenti a disposizione per re-impossessarsi del nostro bene. A questi requisiti corrisponde la descrizione della Virtual Private Network (VPN), che rappresenta un canale di comunicazione sicuro in mezzo al mare magnum di Internet: una specie di tunnel nel quale i dati trasmessi sono al riparo dalle possibili interferenze esterne.
Anche per i collegamenti wireless il discorso è analogo. Altrettanto diffusi sono, infatti, i collegamenti, da notebook o palmari: è il cosiddetto wireless networking, di cui regina indiscussa è la tecnologia Wi-Fi.

Il pericolo è evidente: chiunque, senza bisogno di un collegamento fisico, è potenzialmente in grado di intromettersi nella comunicazione, se questa non è adeguatamente protetta. L'intruso potrebbe intercettare e "ascoltare" le comunicazioni, entrare e sottrarre parte dei dati. Per questo è bene assicurarsi di volta in volta, eventualmente ricorrendo a dei consulenti esperti, perché siano attivate tutte le caratteristiche di sicurezza per le reti wireless: limitazioni d'uso negli orari d'ufficio e di lezione, utilizzo di card certificate e di password a combinazione alfanumerica, restrizioni sul numero di utenti e degli accessi, accesso tramite server dedicati.