La sicurezza informatica dei PC domestici

Parte 2 – Come proteggersi dalle minacce

Note e avvertenze

Lo scopo di questa documento è quello di presentare a un pubblico di non specialisti i problemi della sicurezza informatica dei computer di casa e i possibili modi per affrontarli e risolverli. In questa seconda parte del documento vengono esaminati quali sono i comportamenti più adeguati per proteggersi dalle minacce.

Dove possibile sono stati indicati ulteriori riferimenti (in rosso) per gli approfondimenti, con collegamenti diretto a documenti presenti su Internet e cercando di sceglierli di preferenza in lingua italiana.

L'ACSI non si assume nessuna responsabilità per eventuali danni derivanti da prodotti o da indicazioni citati nella sezione.

Realizzazione

Testo a cura di Silvano Marioni,

Prima pubblicazione sul sito ACSI: Ottobre 2004
Revisione e adattamento in formato Acrobat/pdf: settembre 2009

Come difendersi

La sicurezza non è un prodotto ma un processo

In questa parte saranno elencate le buone abitudini e i comportamenti che ci faranno diventare gli strumenti attivi di protezione a complemento e integrazione degli strumenti tecnici presenti sul computer.

La sicurezza non è qualcosa che si può acquistare in blocco ma è un risultato che nasce dalla combinazione di comportamenti e tecnologie che riescono a fronteggiare in modo efficacie le minacce solo se sono utilizzate in modo combinato. La sicurezza non è qualcosa di definitivo ma è una soluzione intermedia che deve continuamente evolvere per fronteggiare nuovi rischi e nuove minacce.

Come nella vita reale anche nel mondo informatico la sicurezza è quindi un processo di adattamento delle soluzioni di sicurezza all'evoluzione dei rischi.

Le soluzioni di sicurezza devono essere proporzionali ai rischi, perché non vale la pena di spendere per le contromisure un importo superiore al valore dei bene da proteggere. Le corrette contromisure sono fondamentali in situazioni dove il rischio è alto ed è necessario proteggerci ma diventano meno importanti quando il rischio è basso e lo si può accettare. Ad esempio l'istallazione delle cinture di sicurezza su un'auto è giustificata dal rischio dei danni alle persone in caso di incidente. Non sarebbe invece giustificata l'istallazione di una seconda ruota di scorta perché il rischio di forare due volte di seguito è limitato, sia per probabilità che per gravità del danno.

Le contromisure per proteggerci da eventuali rischi informatici possono essere suddivise in tre categorie:

- **Contromisure di prevenzione**
  Queste contromisure sono finalizzate ad impedire che il rischio si manifesti o a ridurre i danni di un possibile rischio. Appartengono a queste contromisure la sensibilizzazione e l'informazione, l'uso della password o le procedure di salvataggio dei dati
- **Contromisure di scoperta**
  Queste contromisure servono per segnalare i danni al momento in cui si manifestano. Appartiene a questo tipo di contromisure l'uso di personal firewall per segnalare i tentativi di accesso non autorizzati.
- **Contromisure di reazione**
  Queste contromisure servono per ridurre gli eventuali danni e fare da correttivi in modo da evitare il peggioramento della situazione. Appartengono a queste contromisure i gruppi di continuità elettrica o gli .

La ricetta per una difesa efficace è quindi una giusta combinazione di contromisure che in momenti differenti sono in grado di contrastare i possibili attacchi e proteggerci dai rischi.

Bibliografia

Bruce Schneier, considerato uno dei maggiori esperti mondiali nel campo della sicurezza informatica, fa una presentazione non tecnica dei rischi e delle tecnologie di prevenzione mostrando come la sicurezza informatica non è solo un problema tecnico, ma dipende anche dai comportamenti delle persone.

Sicurezza digitale
Bruce Schneier
Tecniche Nuove, 2001
ISBN 12137

Protezione a strati

Quattro occhi vedono meglio di due

La protezione a strati è una tecnica che permette di combinare diversi strumenti di difesa per aumentare il livello di sicurezza. In questo modo anche se uno di questi strumenti fosse compromesso non viene messo in pericolo la sicurezza generale di tutto il sistema. Ne è un esempio il castello in cui sono presenti diversi livelli e tipologie di barriere per scoraggiare e contrastare gli attacchi.

La difesa dei beni informatici si basa su una serie di strumenti tecnici di protezione che coprono determinate aree e permettono di rendere più sicuri i nostri computer. Più strumenti utilizziamo, più aree copriamo e maggiore è la certezza di resistere agli eventuali attacchi. Ma gli strumenti tecnici non sono i soli elementi della protezione a strati.

È fondamentale la componente umana perché sempre più spesso gli attacchi non sono portati solo a livello tecnico ma combinati con la truffa e con l'inganno. Per questo oltre a rendere sicuri i sistemi, oggi è fondamentale migliorare la consapevolezza delle persone, informandole dei rischi e insegnando i giusti comportamenti per identificare e combattere gli eventuali attacchi.

Solo in questo modo, utilizzando in modo integrato gli strumenti tecnici e i comportamenti individuali, si può tenere alto il livello di sicurezza intorno ai nostri beni informatici.

Curiosità

Perché per accedere ai miei dati finanziari su Internet devo inserire tutti quei codici?

Nelle transazioni finanziarie su Internet oltre al nome utente e alla password si deve fornire un ulteriore codice che, utilizzando tecniche, diverse cambia a ogni accesso. Il sistema più diffuso è quello della lista di stralcio, una serie di numeri su carta o su una scheda che ci viene rinnovata a scadenze regolari. Questo è un esempio di protezione a strati che permette agli istituti bancari e finanziari di avere la certezza sull'autenticazione dei clienti perché il possesso di questo ulteriore codice assicura la loro identità garantendo che non sia un impostore, anche nel caso in cui sia stata sottratta la password.

L'importanza dell'autenticazione

Le password sono le chiavi per proteggere i nostri dati

Noi, come legittimi proprietari, non vogliamo che i nostri dati e le nostre applicazioni informatiche siano utilizzati da altre persone. L'autenticazione è il processo che ci identifica come legittimi proprietari fornendo una prova che solo noi conosciamo.

Questa prova è la password, una parola o una frase che permette solo a chi la conosce di accedere con un particolare servizio. (Esistono altri sistemi per identificarsi quali smart card o sistemi biometrici ma non sono usati in ambiente domestico perché più cari e complessi da gestire)

È importante impostare una password di accesso sul nostro computer per proteggere i nostri dati dagli attacchi da Internet o nel caso di furto del computer. Un computer su cui non è stata impostata una password di accesso è sicuramente più pratico da utilizzare ma il guaio è che diventa facilmente accessibile anche per un intruso che può entrare senza nessun controllo al nostro sistema e vedere i nostri dati.

La password si comporta come una vera e propria chiave elettronica che protegge i nostri beni informatici. Tutti custodiamo gelosamente la chiave di casa o dell'auto e siamo coscienti

dei rischi che corriamo se dovessimo perderle. Analogamente la password richiede alcune precauzioni sia nella scelta sia nel modo di utilizzo come vedremo in seguito.

Usare le password correttamente

Come scegliere e utilizzare la password

La scelta della password va fatta utilizzandole tutte precauzioni per evitare che possa essere scoperta da altri che potrebbero farne un uso improprio.

I rischi principali che possono compromettere la segretezza di una password sono i seguenti:

- La password può essere ricavata con calcoli matematici.
  Esistono programmi in grado di scoprire le password utilizzando tecniche combinatorie. Essi funzionano efficacemente solo fino a una certo lunghezza di parola e per questo si consiglia di scegliere la password con almeno 8 caratteri di lunghezza o superiori, usando combinazioni di caratteri (MAIUSCOLI e minuscoli), numeri e caratteri speciali.
- La password può essere indovinata.
  Dobbiamo evitare di usare come password parole ovvie quali il nome dei figli, la data di nascita, la targa dell'auto, sequenze di caratteri vicini sulla tastiera, ecc.
- La password può essere richiesta.
  Nessuna azienda o organizzazione ha la necessità di chiederci la password perchè è un'informazione che possiede gia. Essa potrebbe al limite fornirci una nuova password. Perciò diffidiamo di chi ci richiede la password. Solo un impostore ha interesse a conoscerla e qualora ci venisse richiesta, non dobbiamo mai comunicarla a nessuno !

Per scegliere una buona password bisogna conoscere quali caratteristiche importanti deve avere.

Deve essere difficile da indovinare. Infatti se una persona si appropria della nostra password può agire impunemente a nostro nome e nel caso di accessi e operazioni sul nostro computer o sul nostro conto bancario on-line, i risultati possono essere spiacevoli.

Deve essere facile da ricordare. Cerchiamo di ricordarla a memoria, evitiamo assolutamente di scriverla o di memorizzarla sul nostro computer in modo non protetto (ad esempio utilizzando le funzionalità del Browser Web "Memorizza password"). Per i più smemorati esistono delle tecniche che possono essere di aiuto. Le parole ovvie, che normalmente si consiglia di evitare, possono diventare il punto di partenza per l'applicazione di alcune regole, semplici - ma molto efficaci - che permettono di costruire password complesse ed aumentare il livello di sicurezza.

Partendo da parole facili da ricordare si può infatti:

- Sostituire un carattere con il numero della sua posizione corrispondente.
  Esempi: Attenzione può diventare 1tt5nzion5
- Combinare lettere e numeri in modo che risulti una parola pronunciabile.
  Esempi: 3mentina, 9vello, dove6stato, 3nta
- Utilizzare la medesima tecnica con parole composte.
  Esempi: Alta/lena, Ris8%giall0, 63mendo!, +ness1dorme
- Utilizzare frasi (ricavate da poesie, canzoni, ecc.) ed eventualmente applicare alle frasi le medesime regole.
  Esempi: questadiMarinellaèlastoriavera

Deve essere diversa a dipendenza del livello di criticità del sistema a cui ci si collega.

La password che comunichiamo a un sito Internet per scaricare gratuitamente un software o della musica non deve essere la stessa che usiamo per le transazioni finanziarie della nostra banca e nemmeno quella che usiamo per l'accesso al computer sul posto di lavoro. È utile avere password con almeno tre livelli differenti di criticità: quella per l'accesso ai dati

personali e finanziari, quella da utilizzare nell'ambiente di lavoro e quella per navigare sui siti Internet sconosciuti che richiedono una password.

Deve essere mantenuta segreta e non deve essere comunicata a nessun altro. Nel caso del computer utilizzato in famiglia è più prudente avere una password per ogni componente famigliare che condividere la medesima password.

Deve essere modificata regolarmente ogni due o tre mesi e in tutti i casi in cui si ha il dubbio che qualcuno possa avercela vista o rubata.

Nel caso fosse necessario memorizzare numerose password esistono comunque dei programmi per memorizzare in modo sicuro le password.

Curiosità

Che differenza c'è tra una password e un PIN?

Il PIN (Personal Identification Number) è un tipo particolare di password utilizzato in genere con le carte magnetiche (bancomat, carte di credito, ecc.) e con i cellulari. Il PIN ha delle limitazioni di tipo tecnico che lo rendono meno sicuro della password: è composto solo da numeri (in genere 6) e in alcuni casi non si può modificare. Ma i suoi rischi maggiori non sono di tipo tecnico ma comportamentale. Proprio perché il PIN è difficile da ricordare si è portati a scriverlo su un foglietto e a tenerlo nel portamonete insieme alla carta magnetica con il rischio che si perde il portamonete chiunque può utilizzare la nostra carta magnetica. Invece di scrivere i numeri del PIN sarebbe meglio sceglierli "facili da ricordare" e tenerli a mente.

Lavorare senza diritti

Meno poteri per una maggior sicurezza

I rischi maggiori per il PC domestico provengono da Internet ed è quindi utile sapere come proteggersi e per quale motivo bisogna comportarsi in un certo modo.
Normalmente quando si usa un computer domestico si lavora come amministratore del sistema. Questo significa che si hanno tutti i diritti per fare qualsiasi cosa a livello di utilizzo ma soprattutto a livello di istallazione e configurazione del computer.

Quando apriamo un messaggio di posta elettronica o accediamo a un sito Internet che contengono codice malefico, i nostri diritti sono ereditati da questi programmi che acquistano tutti i nostri poteri di accesso al PC e possono quindi anche danneggiarlo.

È buona cosa seguire le regole che normalmente vengono usate nelle aziende dove gli utenti comuni hanno diritti limitati e solo il personale tecnico ha il diritto di amministratore per istallare e configurare il computer. È necessario quindi cambiarsi di ruolo a secondo che si intenda usare semplicemente il PC o fare delle modifiche di configurazione.

Questo modo di operare può essere un po´ fastidioso da usare sul PC domestico. Per ovviare a questo problema, considerando che i rischi dei programmi malefici provengono per la maggior parte da Internet, una soluzione interessante sono i programmi che permettono di ridurre i diritti di amministratore solo quando si utilizza il browser Web o il programma di posta elettronica.

Mantenere aggiornato il software

Stiamo al passo con i rischi di sicurezza

Per capire perché si deve continuamente aggiornare il software dobbiamo considerare il livello di complessità di una moderna applicazione informatica. Se esaminiamo l'evoluzione del

sistema operativo Windows scopriamo che nel 1992 era composto da circa 3 milioni di righe di programma, nel 1995 Windows 95 era composto da circa 15 milioni di righe di programma e oggi Windows XP è composto da circa 45 milioni di righe di programma. È normale (e anche statisticamente provato) che all'interno di oggetti di tale complessità ci possano essere degli errori, che spesso si manifestano sotto forma di vulnerabilità di sicurezza, subito sfruttate dai malintenzionati.

Quindi quando qualcuno scopre una falla in un programma, il produttore deve subito intervenire con le correzioni e da parte nostra è importante istallarle subito. Le falle del sistema operativo (ad esempio Windows) sono quelle più critiche perché interessano il funzionamento di base del computer. E naturalmente se utilizziamo Internet diventano importanti anche le falle del Browser e del programma di posta elettronica.

È importante quindi verificare se esistono nuovi aggiornamenti al nostro software (ad esempio collegandovi al sito Windows Update per il sistema Windows) e istallarlo subito, almeno per le applicazione che utilizziamo.

Fare regolarmente il salvataggio dei dati

Prevedere i dati di riserva in caso di emergenza

Oggi che abbiamo sul nostro computer sempre più documenti - lettere, foto, brani musicali, documenti contabili e altro ancora - è veramente importante proteggerli nel caso in cui non fosse più possibile consultarli a causa del guasto del computer o per la rottura del disco.

Il salvataggio dei dati è l'operazione più importante per la sicurezza delle nostre informazioni ma è anche quella più trascurata a livello domestico.

Per definire il concetto del salvataggio dei dati dobbiamo decidere i seguenti punti:

Su quale media fare il salvataggio
Diversamente da una decina di anni fa quando l'unico media di salvataggio economico era il dischetto oggi abbiamo a disposizione una grande varieta di supporti. Si parte dall'economico - ma lento - CD o DVD monouso per arrivare al performante - ma più caro - disco rigido esterno. Ma possimo citare i dischi Zip, le chiavi USB ad alta capacità, i CD e i DVD riscrivibili, i DVD blu-ray.

- Che cosa salvare
  Non ci sono limiti al volume di dati da salvare e questo dipende solo dai costi che vogliamo sostenere. Oggi è possibile salvare solo i nostri dati su un CD o su una chiavetta USB a costi molto contenuti oppure l'intero contenuto del disco su un disco USB con costi sotto i 100.- franchi.
- Come fare il salvataggio dei dati
  Questo è il punto critico. Possiamo fare delle copie complete su CD o DVD monouso e archiviarle ma questo non è molto pratico da fare tutti i giorni. Oppure possiamo mantenere una copia dei nostri dati su un supporto riscrivibile (ad esempio un disco USB) e sincronizzarli con frequenza e regolarità con appositi programmi.
- Dove tenere il salvataggio dei dati
  Per maggior garanzia dovrebbe essere tenuto in un luogo diverso e lontano da dove abbiamo il computer. Ad esempio una copia di salvataggio dei dati su CD o DVD monouso potrebbe essere portata in un altro stabile .

Anche il salvataggio di un documento durante la sua stesura rientra nella filosofia del salvataggio dei dati. Una caduta di corrente o il blocco del programma potrebbero farci perdere ore di lavoro. Per questo è utile fare copie del documento a intervelli regolari o forse meglio farlo fare automaticamente dal computer impostando l'opzione di salvataggio automatico presente ad esempio in alcuni programmi come Word.

Essere prudenti utilizzando Internet

Pensare prima di cliccare

Quando navighiamo su Internet difficilmente riflettiamo sui possibili rischi a cui andiamo incontro. Quando però il nostro browser comincia a comportarsi in modo strano, aprendo automaticamente finestre e indirizzandoci su siti a noi sconosciuti ci rendiamo conto dei rischi che possiamo correre.

I problemi maggiori derivano dalle pagine Web con contenuti attivi. Questi programmi, inseriti nelle pagine per aumentare la funzionalità o l'estetica, possono essere alterati in versione malefica. Mentre nel caso di contenuti attivi in linguaggio Java Script i danni possono essere relativamente ridotti, nel caso di contenuti attivi ActiveX possiamo correre il rischio di farci istallare un programma sul nostro computer senza essere coscienti di cosa faccia. È il caso dei dialers, programmi per connettersi ad Internet che invece di fare una telefonata locale si connettono a numeri internazionali con costi esorbitanti. L'istallazione di un dialer avviene con un invito su una finestra pop-up che a volte, senza conoscenza dei rischi, si tende a seguire.

Se capitate in un sito che vi richiede l'istallazione di un programma ActiveX, procedete solo se siete ben sicuri di quello che state facendo. In tutti gli altri casi rifiutatelo e chiudete la finestra pop-up direttamente usando il bottone "chiudi" (bottone con la X in alto a destra) o con il tasto Alt+F4.

Un altro rischio è quello di accedere ad un sito che si spaccia per un'altro. Questo viene in genere fatto se ci sono in gioco transazioni finanziarie così come descritto riguardo al phishing. Oppure siti di dubbia onestà che offrono software di marca a prezzi irrisori con il solo scopo di catturare i numeri di carta di credito senza spedire mai la merce.

È possibile ottenere maggiori informazioni sulla pagina che state consultando premendo il bottone destro e selezionando proprietà. Diffidate dei siti che non vi permettono di visualizzare le proprietà perché hanno probabilmente qualcosa da nascondere.

Più buon senso con la posta elettronica

Riflettere prima di inviare o rispondere a un messaggio

Quando usiamo la posta elettronica la prima cosa da considerare riguarda la privacy dei dati che inviamo o riceviamo.

Tutti i testi inviati tramite posta elettronica potrebbero essere consultati e addirittura modificati da terzi. Per questo è importante che quando vogliamo inviare documenti riservati ci preoccupiamo di proteggerli, utilizzando un programma di cifratura, prima di inviarli.

Informiamo i nostri corrispondenti di questo fatto e chiediamo loro di cifrare i dati prima di inviarceli.

Un'altro punto importante è che non c'è garanzia sull'identità di chi ci invia il messaggio. Le intestazioni dei messaggi possono essere facilmente modificate, come lo dimostrano i messaggi che sono inviati dagli spammers, e non c'è la possibilità di risalire a chi li ha effettivamente inviati.

Nel caso di ricezioni di messaggi sospetti è utile adottare le seguenti precauzioni:

- Non rispondere al messaggio anche se il contenuto ci invita o ci stimola a farlo. Diffidate ad esempio delle lettere di richiesta di aiuto con ricompensa (Nigerian Scam) o delle vincite a lotterie a cui non avete mai partecipato.
- Non aprire gli allegati sconosciuti o sospetti perché possono contenere virus e codice malefico in grado di infettare il nostro computer.
- Non seguire i link proposti nel messaggio che ci potrebbero portare a pagine che, sfruttando eventuali falle del programma di posta, ci possono infettare il computer.

- In situazioni sospette verifichiamo con il mittente se è stato veramente lui a inviarci il messaggio.
- Non contribuire a diffondere messaggi su virus, attacchi o vulnerabilità dei programmi così come appelli medici, richieste di aiuto, ecc.(vedi Hoax). Se volete esaminare un campionario di questi messaggi consultate il sito di Paolo Attivissimo: http://attivissimo.blogspot.com/2004_06_01_archive.html

Che cosa è un Hoax?

Gli Hoax sono dei messaggi che fanno leva sulla buona fede e sulla solidarietà delle persone a diffondere notizie a proposito di presunti virus, attacchi, ecc. oppure richieste di aiuto a favore di persone bisognose o malate. Il loro scopo è spesso quello di raccogliere indirizzi di posta elettronica per poi usarli per fare spam oppure più semplicemente di creare problemi alla persone con poche conoscenze informatiche per disorientarli e poterli colpire in seguito con attacchi più mirati. Se ricevete messaggi di questo tipo potete fare una verifica nell'elenco degli Hoax sul sito http://www.symantec.com/avcenter/hoax.html oppure più semplicemente cercare i riferimenti del messaggio sul motore di ricerca Google verificando che cosa si dice sull'argomento.

Tutelare la nostra privacy

Proteggere i dati personali è un diritto di ogni cittadino

La protezione dei dati personali è tutelato per legge sia in Svizzera che nella maggioranza dei paesi occidentali. Per ogni dubbio riguardante la protezione dei dati personali potete consultare il sito dell'Incaricato Federale della Protezione dei Dati.

La protezione dei nostri dati personali dipende dall'identificazione della controparte che li richiede. Nel caso di una controparte conosciuta non dovremmo avere problemi a fornire i dati adeguati, ma attenzione a verificare che sia veramente chi dice di essere. Se la controparte è sconosciuta dovremmo evitare di fornire qualsiasi informazione personale.
È utile tenere sotto controllo i cookie. Questi file, indispensabili per il funzionamento delle applicazioni su Internet, possono essere anche utilizzati per raccogliere informazioni sui siti che visitiamo e tracciare quindi un nostro profilo. Con un programma di gestione dei cookies possiamo almeno vedere chi cerca controllarci ed eventualmente cancellare il cookie.

Verifichiamo che quando inviamo informazioni riservate e critiche come il numero della carta di credito, la comunicazione sia fatta automaticamente in modo cifrato. L'indirizzo deve iniziare con https (e non http) e sulla barra di stato in basso al Browser deve comparire un lucchetto chiuso che quando viene cliccato presenta le informazioni del sito con cui stiamo comunicando. La stessa cosa deve valere per la posta elettronica ma in questo caso dobbiamo essere noi a decidere manualmente di cifrare i dati.

Una categoria particolare di programmi che possono catturare i nostri dati personali sono gli spyware. Possono essere istallati se apriamo messaggi di posta inviatici da sconosciuti o accediamo a pagine Web che ci sono suggeriti sempre su messaggio di sconosciuti oppure li istalliamo noi senza saperlo, come programmi associati a programmi gratuiti. Con un programma antispyware siamo in grado di identificarli e di rimuoverli.
Un caso particolare di spyware sono i webbug, immagini di dimensioni minime, che sono inserite nelle pagine web (o nei messaggi di posta elettronica in formato HTML) per segnalare ad una terza parte la consultazione della pagina (o l'apertura del messaggio) senza che ce ne rendiamo conto e senza il nostro consenso.

Un altro caso di diffusione di dati personali riguarda i documenti Microsoft Office. Questi possono contenere informazioni nascoste che sono visibili se si apre il documento con un semplice programma di visualizzazione in formato testo. Microsoft stessa è al corrente del

problema e ha previsto un programma per cancellare le informazioni nascoste che si può trovare su Internet con il nome RHDTOOL.EXE

Un'importante precauzione riguarda la cancellazione dei dati. Mettere un documento nel cestino lo fa scomparire, ma tutte le informazioni rimangono ancora sul disco e possono essere visualizzate con opportuni programmi. Per cancellare definitivamente un documento è necessario utilizzare dei programmi che cancellano realmente il documento. Lo stesso vale per il disco del vostro computer. Se dovete venderlo o rottamarlo è importante cancellare i dati sul disco utilizzando dei programmi di pulizia del disco, per fare in modo che nessun altro possa accedere ai vostri dati.

Da ultimo dobbiamo citare i rischi di diffusione dei dati personali tramite i sistemi di comunicazione senza filo, le cosiddette reti wireless. Questa nuova tecnologia per comunicare con Internet o tra differenti PC, è molto pratica perché elimina il fastidio del cavi di collegamento alla rete, ha dei costi contenuti e per questo è sempre più utilizzata anche in ambiente domestico. Purtroppo, se l'apparecchiatura non è configurata in modo corretto, un intruso che si posiziona fuori da casa nostra può vedere tutte le informazioni che transitano via radio. Per proteggersi da questo rischio è importante configurare il sistema in modo che la trasmissione venga fatta in modo cifrato.

Ma è sicuro fare acquisti su Internet?
Chi avesse dubbi sul funzionamento del commercio elettronico può trovare spiegazioni tecniche sul funzionamento e sulla sicurezza all'indirizzo http://it.wikipedia.org/wiki/Commercio_elettronico.

Ulteriori informazioni possono essere consultate sul sito dell'Ufficio Federale del Consumo.

Proteggere gli apparecchi portatili

La comodità e i rischi di portarsi in giro tutti i propri dati

Oggi sempre più persone utilizzano apparecchi portatili. I computer portatili, le agende elettroniche ma anche i telefonini - sempre più simili a un computer – ci permettono di lavorare e accedere ai nostri dati anche fuori casa.
Il problema è che queste apparecchiature diventano il bersaglio ideale per i ladri.
Se qualcuno ci ruba un apparecchio portatile, il danno più appariscente è sicuramente il valore dell'apparecchio, ma se il ladro riesce ad accedere alle informazioni contenute, il danno diventa maggiore per le informazioni che possono essere rubate o più semplicemente per la violazione della nostra privacy.
È risaputo che il reale valore dei computer portatili aziendali sta nei dati contenuti e spesso i furti vengono perpetrati proprio per entrare in possesso di queste informazioni.
Quali sono le precauzioni che possiamo mettere in atto per proteggere i nostri apparecchi portatili e i dati in essi contenuti?

- Innanzitutto impostare una password di accesso al computer portatile e all'agenda elettronica e un PIN al telefonino.
- Nel caso dei computer portatili è possibile impostare un'ulteriore password al livello più tecnico (nel BIOS) che impedisce letteralmente di accendere il computer. Il solo modo di utilizzare un laptop senza conoscere la password a livello di BIOS è quello di formattare il disco – cancellando tutti i dati - e di conseguenza con questa precauzione impedite al ladro la visione dei vostri dati. (se non sapete come fare l'impostazione della password a livello di BIOS potete chiedere al vostro rivenditore).
- Non ostentate il vostro apparecchio portatile e non lasciatelo incustodito. Per trasportarlo utilizzate una borsa neutra che non faccia capire cosa contiene.
- Fate regolarmente il salvataggio dei dati contenuti sull'apparecchiature portatile o addirittura fate una copia immagine del disco per poter ricostruirlo velocemente con la medesima configurazione