MINACCE AI DATI 1.1

1.1.1 Distinguere tra dati e informazioni

In informatica, "dati" e "informazioni" sono termini ricorrenti. Quale significato occorre dare a ciascuno dei due termini?

Con il termine dati si indicano gli elementi che, se coordinati in modo opportuno, possono costituire un'informazione. Ad esempio: un nome di persona, un cognome, un nome di città, un nome di via o di piazza, un numero civico, sono, se presi singolarmente, dei dati. Raggruppati, in tutto o in parte, possono costituire un indirizzo anagrafico e cioè un'informazione.

Un altro esempio: il nome di una marca di elettrodomestici, la sigla di una lavastoviglie, un numero in formato valuta, un numero espresso in percentuale, se presi singolarmente sono dei dati, alcuni alfabetici, altri numerici. Raggruppati costituiscono un'informazione: il prezzo di un modello di lavastoviglie.

In informatica, spesso i dati sono elementi di ingresso nel processo del calcolo o della ricerca, mentre le informazioni sono il risultato del calcolo o della ricerca e cioè il risultato di un'elaborazione di dati.

1.1.2 Comprendere il termine crimine informatico

Per crimine informatico s'intende qualsiasi attività che, attraverso l'utilizzo di mezzi hardware o software, tende a recare danno a uno stato, un ente, un'istituzione, una società, un privato cittadino o alle loro rispettive strutture informatiche.

Il crimine informatico viene attuato attraverso:

- La duplicazione non autorizzata di programmi proprietari.
- L'accesso non autorizzato alle banche dati, ai contenuti di un disco.
- L'intercettazione dei dati in transito in una linea di trasmissione.
- La contraffazione e il furto di identità.
- Il phishing (pr. *fiscing*) e il pharming (pr. *fàrming*) cioè il tentativo di carpire i dati sensibili di un individuo, utilizzando in maniera fraudolenta il nome, il logo o il sito di un ente o di una società.
- Le frodi elettroniche, in genere.

Le legislazioni nazionali reprimono in vario modo le frodi informatiche, a seconda della maniera con cui vengono attuate.

1.1.3 Comprendere la differenza tra hacking, cracking e hacking etico

Il termine hacking (pr. *àkin*) deriva dall'inglese *to hack* = colpire, ferire. Nel linguaggio informatico il termine riguarda tutte le attività, lecite o non lecite, tese a neutralizzare le difese informatiche di banche dati, reti di dati, sistemi operativi, computer.

più

Anche se il termine hacker (pr. *àker*) tecnicamente indica colui che utilizza le proprie capacità per superare qualsiasi protezione o ostacolo informatico, al solo scopo di riuscirci e senza recare danno ad alcuno, nella coscienza collettiva l'hacker ha l'immagine negativa di colui che impiega il suo tempo a creare problemi, anziché a risolverli. In alcuni casi, hacker che sono stati individuati e condannati per aver violato le difese di importanti sistemi informativi, sono poi stati assunti alle dipendenze di aziende multinazionali, con il compito di migliorare la sicurezza informatica aziendale e di combattere i tentativi di intrusione esercitati da altri hacker.

I termini cracker (pr. *cràker*) e cracking (pr. *cràkin*) sono neologismi inventati da Richard Stallman, teorico del software libero, per distinguere gli hacker da chi utilizza la conoscenza informatica per trarne illegalmente profitto. I cracker, a differenza degli hacker, impegnano conoscenza e tempo per:

- Aggirare le difese software di sistemi operativi proprietari (ossia sistemi operativi coperti da licenze che ne impediscono il libero uso) e di programmi commerciali, allo scopo di rivenderne copie pirata.
- Decifrare illegalmente una trasmissione dati per carpire dati sensibili, come dati anagrafici, dati finanziari e simili.
- Entrare abusivamente nel contenuto di un disco o di una banca dati per copiare, modificare, distruggere dati, allo scopo di trarne profitto.
- Praticare il phishing e cioè utilizzare loghi o siti che simulano realtà conosciute, allo scopo di far digitare alla persona "presa all'amo" il proprio numero di conto corrente o numero di carta di credito e le relative password e successivamente utilizzarli per estorcere danaro.
- Scoprire i difetti di una rete sociale, come ad esempio *Facebook*, *Google+* e simili, per introdurvisi abusivamente, allo scopo di modificare i profili di un determinato partecipante o per postare falsi commenti.

Per hacking etico s'intende un esperto innanzitutto di reti informatiche che opera in maniera indipendente per rendere pubblici i difetti di un sistema operativo o di una rete sociale, difetti che potrebbero mettere in pericolo la sicurezza degli utenti e la riservatezza dei dati. Con il termine hacker etico si tende a identificare anche la figura professionale del tecnico che opera per prevenire e contrastare le varie forme di attacchi, rivolte ai sistemi informativi aziendali.

più

É noto il caso di un esperto informatico palestinese (Khalil Sherateh) che è riuscito a violare la pagina personale *Facebook* del suo ideatore Zuckerberg. Sherateh aveva in precedenza, senza essere stato preso sul serio, avvisato i progettisti di *Facebook* dell'esistenza della falla nella sicurezza della rete sociale. A seguito dell'azione di Sherateh, la rete sociale è stata rivista e resa più sicura.

Khalil Sherateh e Mark Zuckerberg

1.1.4

Riconoscere le minacce ai dati provocate da forza maggiore, quali fuoco, inondazione, guerra, terremoto

Le aziende pongono grande attenzione alla sicurezza dei dati, già in fase di progettazione del sito dove verranno installate le apparecchiature che tratteranno le informazioni aziendali. Tra gli altri compiti, il responsabile della sicurezza aziendale deve compilare un documento nel quale vengono riportate in dettaglio le norme di comportamento del personale che avrà accesso al centro di calcolo e gli accorgimenti che dovranno garantire il funzionamento ininterrotto dei computer e delle altre apparecchiature informatiche.

Alcune minacce alla sicurezza dei dati sono prevedibili:

- Furto dei dati.
- Contagio da malware, ossia dal software dannoso e non voluto, presente in rete.
- Blackout improvvisi (interruzione di alimentazione elettrica).
- Guasti hardware.
- Errori del personale.

Contro ciascuno di questi rischi, il responsabile della sicurezza prevede un piano che ha lo scopo innanzitutto di prevenire l'evento negativo e, solo in caso di fallimento della politica preventiva, di porvi rimedio:

- Controllo degli accessi al centro di calcolo.
- Installazione di apparecchiature firewall (pr. *fàir-uòl*) che, se opportunamente programmate, impediscono l'accesso alla rete dati da parte di malintenzionati e di malware.
- Installazione di gruppi di continuità elettrica che entrano in funzione automaticamente se l'alimentazione elettrica normale dovesse mancare, anche per pochi istanti.
- Programma di manutenzione tecnica adeguata, con tempi di risposta (tempo che corre tra la richiesta di intervento e l'arrivo del personale tecnico) inferiori, in genere, a quattro ore.
- Corsi di formazione a favore del personale addetto.

Esistono altre minacce definite "di forza maggiore" che difficilmente possono essere prevenute e contro le quali occorre adottare misure più drastiche:

- Incendio.
- Inondazione.
- Guerra/terrorismo.
- Terremoto.

Questi eventi sono considerati dei "disastri" proprio per la loro caratteristica di non prevedibilità e capacità distruttiva. Il responsabile per la sicurezza aziendale ha il compito di stendere un piano speciale denominato Disaster Recovery Plan (pr. *disàste ricàveri plan*) = piano di intervento in caso di disastro, in base al quale l'azienda deve poter disporre immediatamente di un secondo sistema informatico o, almeno, di una copia dei dati aziendali aggiornati, in modo da poter riprendere in breve tempo la propria attività.

Il Disaster Recovery Plan può essere progettato per due tipi di utilizzatori:

- Enti, grandi aziende di stato, banche, assicurazioni, compagnie telefoniche, reti televisive, ecc.: esistenza in un luogo, geograficamente distante da quello dove è installato il centro di calcolo aziendale, di un sistema informativo duplicato che lavora in parallelo con quello principale.
- Piccole e medie aziende, studi professionali: esistenza in un luogo, geograficamente distante da quello dove è installato il centro di calcolo, di una copia dei dati aziendali costantemente aggiornata (copia di backup, pr. *bekàp*).

1.1.5 Riconoscere le minacce ai dati provocate da impiegati, fornitori di servizi e persone esterne

Tra le minacce alla sicurezza dei dati aziendali, prevedibili e contro le quali occorre stabilire misure preventive, vanno ricordati i possibili comportamenti scorretti del personale interno ed esterno.

Il personale interno può inavvertitamente o astutamente venire a contatto con dati riservati, trattati dal sistema informativo aziendale. Per questo motivo, l'accesso al centro di calcolo deve essere riservato al personale strettamente indispensabile e qualificato. Tutti i programmi e le banche dati devono essere accessibili solo attraverso la digitazione di account (pr. *accàunt*) e password. Per le password deve esistere una politica aziendale di aggiornamento programmato.

Lo stesso personale aziendale abilitato all'accesso ai programmi e ai dati dell'azienda può costituire una minaccia ai dati se non è adeguatamente istruito e aggiornato sull'uso dei programmi. I fornitori di servizi possono a loro volta, attraverso le extranet (parte della rete aziendale, dedicata all'utenza esterna) tentare di violare la rete aziendale intranet (rete dati aziendale che lavora con il protocollo usato da Internet) se particolarmente pratici. A questo scopo, il ricorso a idonee apparecchiature di rete (firewall) opportunamente programmate e di software specifici, può ridurre il rischio di intrusione.

I visitatori che occasionalmente si trovano all'interno dell'azienda, possono costituire un rischio per la sicurezza dei dati aziendali anche solo prendendo occasionalmente visione di quanto riportato sullo schermo di un monitor o su un tabulato. Gli anglosassoni definiscono *shoulder surfing* (pr. *sciòulde sèefin*) la possibilità di un estraneo di "sbirciare alle spalle", allo scopo di carpire informazioni riservate. Per questo motivo, i visitatori devono essere registrati all'ingresso dell'azienda e possono circolare nell'area interna solo se accompagnati dalla persona di riferimento che è responsabile del corretto comportamento dell'ospite.

VALORE DELLE INFORMAZIONI 1.2

1.2.1

Comprendere i motivi per proteggere le informazioni personali, quali evitare il furto di identità o le frodi

I dati sensibili nei sistemi informativi sono protetti innanzitutto attraverso l'uso di account e password che qualificano e riconoscono l'utente come persona abilitata all'accesso. Se un estraneo s'impossessa in qualche modo di un account e della rispettiva password, la sicurezza dei dati non esiste più e il sistema informativo può diventare, ad opera dei malintenzionati, uno strumento per attuare frodi di qualsiasi tipo.

Il furto di identità è considerato uno dei maggiori rischi della sicurezza informatica e pertanto gli utenti devono porre particolare attenzione a mantenere riservato il proprio account e ricordarsi di cambiare periodicamente la propria password che deve rimanere sempre segreta.

1.2.2

Comprendere i motivi per proteggere informazioni commercialmente sensibili, quali prevenzione di furti, di uso improprio dei dati dei clienti o di informazioni finanziarie

Non tutti i dati che vengono trattati in un'azienda hanno lo stesso grado di importanza e meritano quindi lo stesso trattamento in fatto di sicurezza.

Le misure di protezione hanno un costo: se tutti i dati dovessero essere protetti allo stesso modo, i costi che ne deriverebbero sarebbero troppo alti o, dovendo abbassare il costo, il livello di protezione generale risulterebbe inadeguato. Per questo motivo le aziende adottano differenti livelli di protezione, a seconda del tipo di documenti trattato. Il livello di protezione più alto viene riservato per prevenire il furto di dati relativi ai clienti, ai progetti o alle trattative in corso, ai movimenti finanziari, in genere.

1.2.3

Identificare le misure per prevenire accessi non autorizzati ai dati, quali cifratura, password

Lo strumento principale per la protezione dei dati ritenuti "sensibili" e cioè che devono essere trattati con riservatezza, consiste nel permettere l'accesso ai dati esclusivamente a utenti abilitati attraverso opportuno account + password.

Si ricorda che se non si proteggono opportunamente i propri dati personali, come ad esempio: dati anagrafici, finanziari, bancari, commerciali, si corre il rischio di essere coinvolti in numerose possibili truffe che hanno come origine proprio il furto dei dati.

Le misure di base relative alla sicurezza dei dati sono, quindi, le seguenti:

- autenticazione e cioè uso di account + password per accedere ai personal computer;
- account + password per collegare i personal computer alla rete aziendale;

- password associata a file di particolare riservatezza, presenti nel disco dei personal computer;
- cifratura di file di particolare riservatezza, presenti nei dischi dei personal computer;
- cifratura dei dati ritenuti "sensibili" (dati che debbono restare riservati) che vengono trasmessi.

più

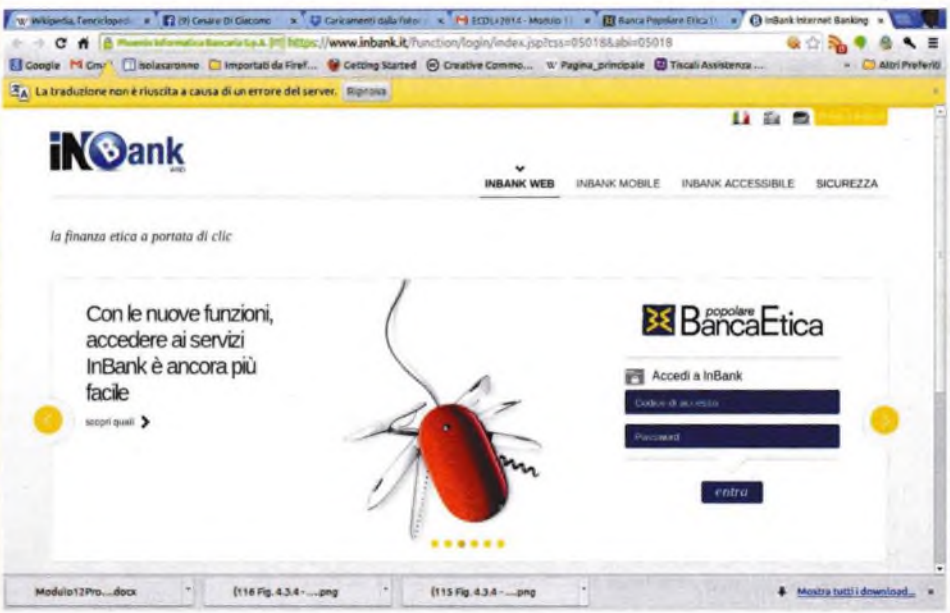
Cifrare (criptare, crittografare) i dati significa scambiare i caratteri del testo con altri caratteri, seguendo un criterio segreto, al fine di rendere il testo stesso non leggibile da chi non possiede la chiave (regola) per decifrarlo. La crittografia è quindi una potente precauzione tecnica contro l'accesso non autorizzato ai dati sensibili.

Per quanto riguarda l'autenticazione, occorre ricordare che, mentre l'account può essere liberamente conosciuto, la password deve rimanere assolutamente segreta, deve essere di difficile identificazione (a questo scopo, essa deve essere lunga almeno 8 caratteri, deve contenere lettere e numeri) e deve essere cambiata periodicamente.

Per quanto riguarda la cifratura, gli utenti devono accertarsi che i messaggi che richiedono segretezza o almeno discrezione, come pure le operazioni in linea che riguardano le attività finanziarie, vengano trattate attraverso programmi che utilizzano il protocollo di trasmissione *https* (Hyper Text Transfer Protocol Secure, al posto del normale protocollo *http*).

Come si fa a sapere se il programma di posta o il browser che si sta usando per la navigazione nel web sta utilizzando il protocollo https? È molto semplice: basta osservare la barra degli indirizzi e assicurarsi che, come primo parametro dell'indirizzo, appaia la dicitura https, affiancata da un lucchetto chiuso.

L'utilizzo di un programma basato su protocollo https obbliga l'utente che vuole entrare nel sito, a collegarsi attraverso un account riconosciuto e una password valida. Inoltre, il programma farà transitare in rete i dati solo dopo averli criptati.



▲ **Protocollo https**

1.2.4

Comprendere le caratteristiche fondamentali della sicurezza delle informazioni, quali confidenzialità, integrità, disponibilità

L'introduzione dell'elettronica nelle pratiche d'ufficio, nella pubblica amministrazione e nelle banche, ha obbligato i Parlamenti delle varie nazioni a emanare regolamenti più o meno eguali in tutti i paesi avanzati, allo scopo di regolamentare in modo omogeneo le operazioni effettuate attraverso i computer, in sostituzione di quelle che fino ad oggi vengono effettuate su carta, magari bollata.

Usando mezzi virtuali e non fisici, come evitare che un cliente che emette un ordine d'acquisto elettronico verso un'azienda, possa in un secondo momento negare di averlo inoltrato? Come evitare che l'azienda che riceve l'ordine via Internet, possa maggiorare il prezzo riportato dal cliente nell'ordine e trarne un vantaggio illecito?

Il problema viene risolto con l'adozione di protocolli "a chiavi asimmetriche", che prevedono l'uso di due chiavi (in questo caso per chiave s'intende un particolare file di testo, prodotto da un apposito programma): una prima chiave detta "pubblica" che tutti possono conoscere e usare e un'altra chiave corrispondente alla prima, detta "privata", che è in possesso del solo titolare. Per la conoscenza delle "chiavi pubbliche" esistono dei siti, che le aziende consultano e nei quali sono presenti tutte le chiavi pubbliche attive e usabili.

I messaggi crittografati con la chiave pubblica possono essere letti solo da chi ha la chiave privata corrispondente e questo impedisce che il messaggio sia letto da terze parti (caratteristica della riservatezza o confidenzialità), mentre i messaggi crittografati con la chiave privata possono essere letti solo con la chiave pubblica corrispondente e questo identifica il mittente del messaggio (caratteristica della affidabilità o autenticità). Il titolare della chiave privata, può usare la chiave per generare, insieme al messaggio che invia (ad esempio un ordine d'acquisto), una copia ristretta e crittografata (detta impronta) del messaggio. L'impronta diventa la "firma elettronica" del titolare della chiave.

Avendo il titolare abbinata la firma elettronica all'ordine d'acquisto, egli non potrà in un secondo momento negare di aver inoltrato l'ordine (caratteristica dell'autenticità).

L'azienda che riceve l'ordine d'acquisto, non potrà in nessun caso modificarlo perché non ci sarebbe più corrispondenza tra l'ordine d'acquisto e l'impronta (caratteristica dell'integrità).

L'insieme delle caratteristiche di confidenzialità, riservatezza, integrità e affidabilità consentono il non ripudio, ossia rendono non contestabile l'accordo avvenuto tra i due soggetti che l'hanno effettuato.

La disponibilità delle informazioni, ossia la certezza di poter disporre in qualsiasi momento dei dati aziendali, è assicurata dalle procedure di backup e di recovery descritte nel punto 1.1.4 (minacce di forza maggiore) e nei punti 6.1.3 e 6.1.4 (gestione sicura dei dati).

Esercizio 1.2.4 N. 1

Ricerca di una chiave pubblica

Come trovare una chiave pubblica? Esistono numerosi siti equivalenti, dove è possibile richiederle. Uno di questi è il sito: *MIT PGP Key Server*. Usando il sito *MIT PGP Key Server*, trova la chiave pubblica dell'azienda *HP Italiana*.

1. Digita nella casella di ricerca di un browser *MIT PGP Key Server*.
2. Entra nel sito.
3. Digita *hp italy* nella casella di ricerca.
4. Clicca sul pulsante *Fare la ricerca*.
5. La ricerca restituisce la chiave pubblica di *HP Italiana*.

Ricerca chiave pubblica di HP Italiana ▶

▼ Chiave pubblica *HP Italiana*

1.2.5

Identificare i requisiti principali per la protezione, conservazione e controllo di dati/privacy che si applicano in Italia

Il controllo dell'uso dei dati personali è illustrato in Italia dalla Legge 196 del 30 giugno 2003 "Testo unico sulla privacy" (pr. *pràivasi*). Questa legge si rifà alla direttiva europea conosciuta come "1995 European Data Protection Directive" (pr. *iuropìen dèit protécsion dairéctiv*, sign. "direttiva europea sulla protezione dei dati").

La legge 196 garantisce il diritto dei singoli a intervenire circa il trattamento dei propri dati, riguardo alla raccolta degli stessi, alla loro elaborazione, modifica e cancellazione.

Punti essenziali della legge sono:

- Nessuno può raccogliere e conservare dati personali altrui, senza il consenso scritto dell'interessato.

- L'ente, la società, il professionista che conserva i dati deve nominare un responsabile del trattamento dati che garantisca l'applicazione della legge.
- I soggetti interessati possono informarsi presso il responsabile, circa il trattamento dei loro dati (articolo 7 della legge 196) e, anche se hanno dato il consenso al trattamento, possono chiedere che gli stessi vengano cancellati, se ritengono violata la loro riservatezza.
- I dati personali devono essere cancellati non appena cessa il motivo del loro utilizzo.

1.2.6 Comprender l'importanza c creare e attenersi linee guida politiche per l'us dell'IC

La diffusione dell'uso degli strumenti informatici in ambito professionale e aziendale comporta la necessità di attuare misure che riguardano:

- sicurezza e disponibilità dei dati;
- ergonomia dei posti di lavoro;
- rispetto dell'ambiente.

È compito del Responsabile dell'ICT aziendale stendere un piano dettagliato che riguardi i tre punti appena elencati, dopo aver illustrato gli scopi del piano e aver ascoltato le proposte dei collaboratori e degli utenti dei servizi informatici. È importante, una volta diffuso il piano, che tutto il personale aziendale, compresi i collaboratori esterni, si attengano a quanto concordato.

SICUREZZA PERSONALE 1.3

1.3.1 Comprendere termine "ingegneri sociale" e le su implicazioni, qua raccolta d informazioni, frodi accesso a sisten informati

Nel punto 1.1.3 è stata illustrata la figura del *cracker*, cioè di colui che studia la maniera di introdursi nei programmi, nei sistemi operativi e nelle reti, allo scopo di trarne illeciti vantaggi economici, o per il gusto criminale di recare danno.
I moderni sistemi operativi, programmi commerciali e reti sociali, si sono specializzati nell'attuare difese energiche contro le intrusioni fraudolente. Per questo motivo, gli approfittatori della rete sono costretti a ricorrere a tecniche particolari, denominate "ingegneria sociale" che riguardano più il comportamento interpersonale che l'attività informatica, anche se lo scopo ultimo è quello di aggirare le difese dei sistemi, per ottenere illeciti guadagni. Chi ricorre ai mezzi fraudolenti dell'ingegneria sociale, attraverso colloqui amichevoli e supportati da riferimenti reali, riesce in genere ad ottenere da individui deboli come bambini ed anziani, informazioni personali che utilizzerà successivamente per commettere azioni criminose ai danni del malcapitato o dei suoi familiari.

1.3.2 Identificare i metod applica dall'ingegneri sociale, qua chiamate telefoniche phishing, shoulde surfing, al fine d carpire informazion persona

Fanno parte delle tecniche di ingegneria sociale:

- *Trashing* (pr. *tràscin*). Raccolta illecita di informazioni, ottenuta recuperando ricevute postali o bancarie o altro, nei cestini della spazzatura e nei cassonetti dei rifiuti.
- *Fishing* (pr. *fiscin*). Furto di identità attuato attraverso i programmi di posta elettronica, con l'utilizzo di falsi loghi e siti che riproducono l'immagine di banche, istituti, aziende, e altro, realmente esistenti.
- Chiamate telefoniche fatte simulando una banca o un istituto che fa richieste di identità e di numeri di carte di credito o di conti correnti bancari.

- Shoulder Surfing (pr. *sciòulde sèefin*). "Sbirciare" oltre la spalla di qualcuno, per sbirciare su una scrivania o su un video monitor.
- Pretexting (pr. *pritècstin*). Utilizzare riferimenti realmente esistenti per convincere la vittima ad abbassare le proprie difese e fornire informazioni personali o riservate.

Tutte queste tecniche hanno in comune la caratteristica di comportare un contatto abbastanza diretto del cracker con la vittima.

più Un caso assolutamente reale e attuale di ingegneria sociale è quello dei falsi siti tecnici dei quali il web è pieno:

- Vuoi aggiornare il tuo sistema operativo non più supportato? Scarica questo file, è gratis!
- Vuoi un antivirus? Sceglilo tra questi. È tutto gratis!
- Vuoi rendere più veloce il tuo PC? Scarica questo programma, è gratis!

Sembra che il mondo sia pieno di benefattori che ci vogliono aiutare. Non è così. Cercando di scaricare il file "gratuito" si entra in un labirinto di proposte "non gratuite". Quando, dopo aver perso tanto tempo, avremo individuato un file che sembra quello giusto, insieme al programma ci tireremo dentro il PC strane barre degli strumenti e purtroppo del malware che, nel migliore dei casi, metterà il nostro PC sotto controllo di un server nascosto, rendendolo un po' più lento e, nel caso peggiore, comincerà a farci visualizzare le pagine di centinaia di siti commerciali dai quali non ci libereremo più.

Morale: non abboccare all'amo. Chiedersi sempre: perché mi stanno offrendo una cosa gratis?

Per fortuna esiste anche il mondo del software libero (*open source*), ma quella è un'altra storia.

1.3.3 Comprendere il termine furto di identità e le sue implicazioni personali, finanziarie, lavorative, legali

Con l'espressione furto di identità si fa riferimento all'azione illegale che ha lo scopo di estorcere danaro o altri vantaggi, fingendo di essere una persona differente, ben definita.

Tipico è il caso delle clonazioni delle carte di credito contraffatte, con le quali i malviventi si presentano nei negozi a fare "shopping" a nome dell'ignaro titolare della carta. Purtroppo la vittima si accorge della truffa solo quando comincia a ricevere i primi segnali dal suo istituto di credito.

Chi è stato vittima del furto d'identità, non solo rischia di rimanere con il conto corrente bancario in rosso, ma può addirittura trovarsi coinvolto in fatti delittuosi quali furti, rapine, omicidi. Si sono verificati casi di dipendenti aziendali che hanno subito il licenziamento dal posto di lavoro, a causa di messaggi lesivi degli interessi aziendali, postati da ignoti a loro nome, su una certa rete sociale. Non è mai superfluo ricordare che per evitare il furto di identità occorre proteggere sempre e comunque i propri dati sensibili.

1.3.4 Identificare i metodi applicati per il furto d'identità, quali acquisire informazioni a partire da oggetti e informazioni scartati, fingendosi qualcun altro o mediante skimming

In tema d'ingegneria sociale, i tentativi di impadronirsi dell'identità altrui non conoscono limiti. Al punto 1.3.2 abbiamo già incontrato il termine *trashing*, con il quale s'individua la possibilità di collezionare informazioni a carico di un individuo, di una famiglia o di un'azienda, tenendo sotto controllo assiduo i documenti, le ricevute, le bollette, gli appunti che ogni giorno vengono scartati e cestinati. Un altro termine usato dagli anglosassoni per descrivere quest'attività è *diving information* (pr. *dàivin infomèscion*).

Un altro metodo d'indagine occulta è lo *skimming* (pr. *skìmin*). Lo skimming consiste nello scorrere un testo o un insieme di dati, a grande

velocità, non alla ricerca di un significato ma di una singola parola, una singola informazione.

Questa tecnica è spesso affidata a un programma che risiede in computer collegati alla rete telefonica. Il programma è stato istruito per registrare eventi come l'identificazione, nel traffico telefonico, o nei messaggi Internet, di determinate parole come, ad esempio: bomba, terrore, kamikaze, ecc. (attività antiterrorismo) ma anche: contratto, offerta, quotazione, sconto, ecc. (attività di spionaggio industriale).

più

È detto *skimming* anche il tentativo di copiare la banda magnetica delle carte di credito, attraverso apparecchi minuscoli ed estremamente sensibili, in grado di operare nel raggio di diversi centimetri, in prossimità quindi della vittima. Da notare che in Italia la rete Bancomat non utilizza la banda magnetica per il riconoscimento dell'utente ma il chip incorporato. Chi copia la banda magnetica e riesce a copiare anche il PIN (Personal Identification Number) lo fa allo scopo di inviare il tutto in un altro paese, dove la rete Bancomat utilizza ancora la banda magnetica.

▲ Echelon: la rete di spionaggio telefonico tramite skimming, in Inghilterra

SICUREZZA DEI FILE 1.4

1.4.1 Comprendere l'effetto di attivare/disattivare le impostazioni di sicurezza delle macro

Le macro sono dei segmenti di programma scritto con un linguaggio particolare, ideato da Microsoft: VBA, vale a dire Visual Basic for Applications (pr. *vìsual bèsik for aplichescions*). La loro caratteristica è di rendere ripetitive le operazioni che contengono. Purtroppo, il linguaggio VBA consente comandi che sono distruttivi per i file registrati sul disco e per lo stesso sistema operativo (*DOS* e *Windows*).

Se un malintenzionato produce un file di *Microsoft Office* (pr. *màicrosoft òffis)* contenente una macro distruttiva e riesce a installarlo in un computer, magari sotto forma di allegato di posta, può creare danni di tutti i tipi.

Per questo motivo, i sistemi operativi prevedono la possibilità di impedire l'esecuzione automatica delle macro contenute nei programmi di *Office: Word, Excel, PowerPoint, Access*, ecc.

Per lo stesso motivo, non è mai consigliabile aprire file allegati ai messaggi di posta che provengono da fonti non certificate e che potrebbero contenere delle macro malevole.

Se le macro sono disattivate dal sistema, è ovvio che quelle che sono presenti nei programmi non possono funzionare. È bene sempre aprire il file di *Office*, del quale si conosce la provenienza e che contiene delle macro, solo dopo averlo esaminato con un programma antivirus aggiornato.

La disattivazione delle macro può avvenire con diverse opzioni rispetto alle macro stesse:

- senza notifica;
- con notifica;
- tranne quelle con firma digitale;

Nel programma *Word*, ad esempio, la procedura per disattivare le macro senza notifica è la seguente: scheda *File* > *Opzioni* > *Centro protezione* > *Impostazioni Centro protezione* > *Disattiva tutte le macro senza notifica.*

1.4.2

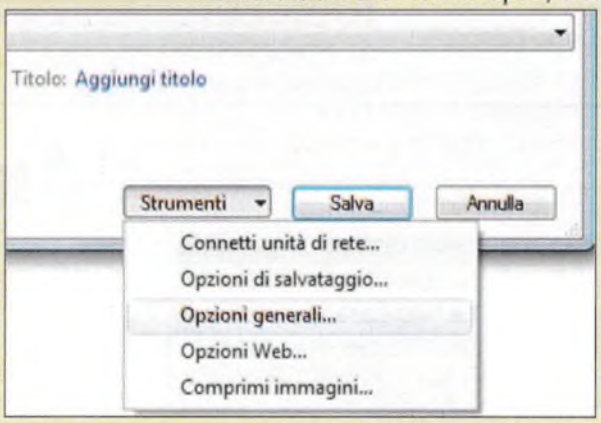
Impostare una password per file quali documenti, file compressi, fogli di calcolo

Non solo i computer, anche i programmi e le reti possono essere protetti da password. A volte è opportuno utilizzare una password anche per proteggere documenti, fogli elettronici e file compressi.
La password a un file compresso va impostata in fase di compressione, utilizzando un programma tipo *zip*, installato nel sistema.

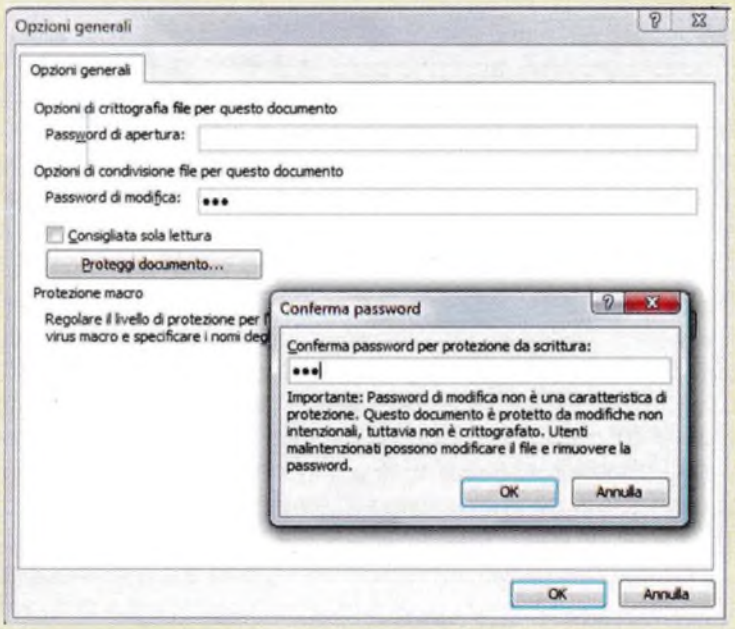
Esercizio 1.4.2 N.1

Impostare una password per sola lettura a un file di *Word 2010*

1. Apri *Microsoft Word 2010*.
2. Apri il documento da proteggere con password.
3. Clicca sulla scheda *File*.
4. Seleziona il comando *Salva con nome*.
5. Nella finestra che si apre, seleziona il pulsante *Strumenti*, in basso a destra.
6. Clicca sul triangolo delle scelte e seleziona *Opzioni generali*.
7. Nella finestra che si apre, scegli il tipo di protezione (password di apertura o password di modifica).
8. Digita la password.
9. Clicca sul pulsante *OK*.
10. Il programma chiede di reinserire la password per conferma.
11. Termina con il pulsante *Salva*.
12. Clicca sul pulsante *OK*.
13 Chiudi il file e riaprilo. Prova a modificarlo.
14 Il programma chiede di digitare la password.



▲ Inserire la password a un documento

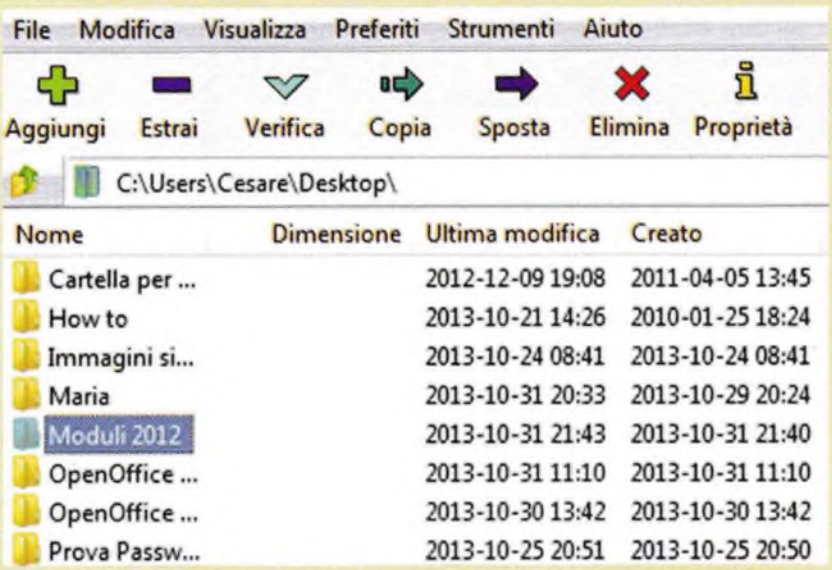


▲ Inserire la password di modifica a un documento

Esercizio 1.4.2 N.2

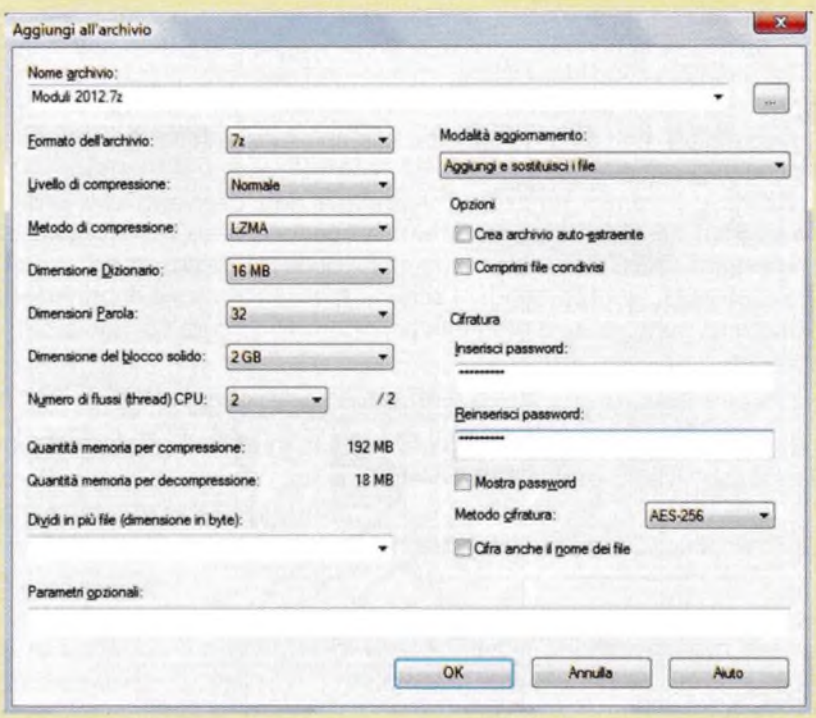
Impostare una password a una cartella compressa

1. Utilizza un programma di compressione (*7Zip file manager*).
2. Seleziona la cartella da comprimere e aggiungila all'archivio, usando il tasto *Aggiungi*.



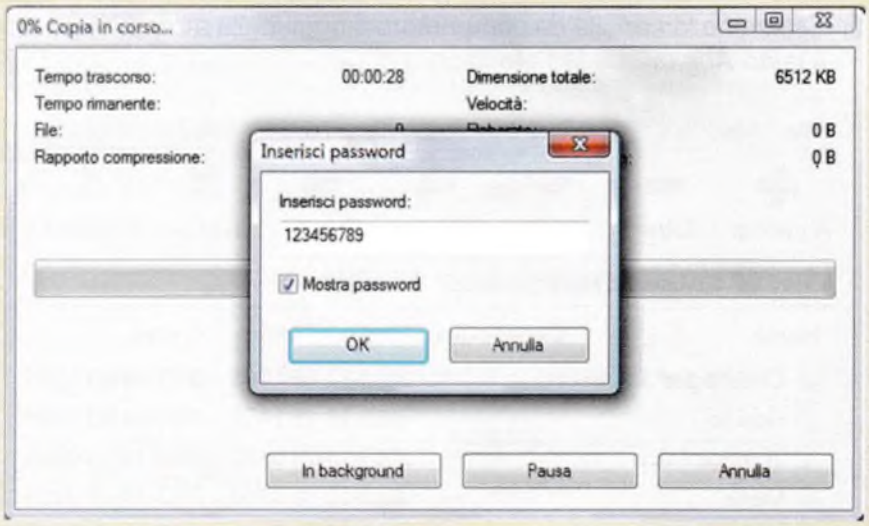
▲ Programma 7Zip

3. Nella cartella *Aggiungi all'archivio* che si apre, digita (due volte) la password.
4. Termina cliccando sul pulsante *OK*.



▲ Aggiungi all'archivio 7Zip

5. Se tenti di aprire (con lo stesso programma) la cartella compressa che è stata creata, devi digitare la password assegnata.



▲ password apertura

1.4.3 Comprendere i vantaggi e i limiti della cifratura

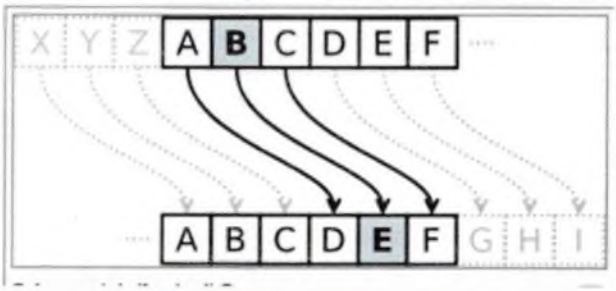
Rendere i messaggi scritti illeggibili è sempre stata una necessità innanzitutto militare. La storia racconta di un metodo di scrittura adottato dall'esercito di Giulio Cesare per impedire ai nemici di leggere il contenuto degli ordini trasportati dai messaggeri che venivano fatti prigionieri.

più

Si trattava di un metodo semplice ma ingegnoso. A ogni lettera che costituiva la parola originale, andava sostituita la lettera che si trova tre posizioni dopo, nell'alfabeto romano. Ad esempio: la parola DIFESA, veniva scritta GNIHVD. Chi riceveva l'ordine "cifrato" (detto anche "crittografato"), non doveva fare altro che riportare indietro di tre posizioni l'ordine di ciascuna lettera.

All'inizio i nemici rimasero interdetti e non capivano che ordini i messaggeri stessero trasportando. Poi, scoperto il trucco, resero inservibile la "crittografia" di Cesare. La crittografia è detta anche "cifratura".

Da allora i metodi per rendere segreti i messaggi si sono enormemente evoluti e la "crittografia" è diventata più sicura. Più sicura ma non sicura in assoluto.



▲ Cifrario di Cesare

I metodi di crittografia moderni sono, fondamentalmente, due:
- crittografia a chiavi simmetriche;
- crittografia a chiavi asimmetriche.

La sicurezza della crittografia è basata sulla segretezza delle "chiavi". Se si ha l'impressione che questa segretezza è compromessa, occorre subito disattivare le vecchie chiavi e produrne delle nuove.

Nel caso della crittografia a chiavi simmetriche esiste un'unica chiave per crittografare e per decrittografare. È un metodo debole, perché chi produce il messaggio crittografato deve, in qualche maniera, far conoscere alla persona che riceverà il messaggio qual è la chiave per interpretarlo e questa è la fase critica: qualcun altro può intercettare l'informazione e rendere inutile la crittografia.

Nel caso della crittografia a chiavi asimmetriche esiste una coppia di chiavi corrispondenti: una pubblica e una privata. Tutti possono conoscere la chiave pubblica, solo il proprietario conosce quella privata, corrispondente. I messaggi crittografati con la chiave "pubblica" possono essere decrittografati solo con la corrispondente chiave "privata". I messaggi crittografati con la chiave "privata" possono essere decrittografati solo con la corrispondente chiave "pubblica".

Attenzione: se la chiave di decodifica viene smarrita, i file crittografati diventano inutilizzabili!

Esercizio 1.4.3 N.1 - 2

Esercizio con le chiavi simmetriche

Antonio vuole spedire un messaggio a Bianca e vuole essere sicuro che Carlo, fratello di Bianca, non lo possa leggere.

1. Antonio, all'insaputa di Carlo, fa conoscere a Bianca la chiave di crittografia.
2. Antonio crittografa il messaggio e lo spedisce a Bianca.
3. Bianca riceve il messaggio e lo decifra con la chiave che le ha dato Antonio.
4. Carlo scopre il messaggio destinato a Bianca, ma non lo può leggere perché non conosce la chiave di crittografia utilizzata.

Il punto debole del sistema è la trasmissione della chiave di crittografia da Antonio a Bianca. Se Carlo intercetta la chiave, il gioco è scoperto.

Esercizio con le chiavi asimmetriche

Antonio vuole spedire un messaggio email a Bianca che possiede una coppia di chiavi asimmetriche e vuole essere sicuro che Carlo, fratello di Bianca, non lo possa leggere.

1. Antonio codifica un messaggio con la chiave pubblica di Bianca e glielo spedisce.
2. Bianca riceve il messaggio e lo decifra con la propria chiave privata.
3. Carlo accende il computer di Bianca, scopre il messaggio ma non può leggerlo perché non possiede la chiave privata di Bianca. Il sistema smette di essere sicuro solo se Bianca fa conoscere a Carlo la sua chiave privata.

Sezione 2

Malware

2.1 DEFINIZIONE E FUNZIONE

2.1.1 Comprendere il termine malware

Malware (pr. *màl-uèr*) è un termine che fa parte del linguaggio "computerese", come i più noti hardware (pr. *ard-uèr*), parte fisica del computer e software (pr. *soft-uèr*), parte concettuale del computer come programmi, cartelle e file dati, ma anche freeware (pr. *fri-uèr*), software liberamente installabile, courseware (pr. *cours-uèr*), materiale per un corso, ecc.

Il termine malware identifica tutta la famiglia di programmi e di sottoprogrammi (pezzi di programmi che si associano ad altri programmi), capaci di recare danno al contenuto di un computer o all'attività del suo utilizzatore.

Il tentativo dei malware di introdursi nei computer o nelle reti dei computer è definito con un termine, non a caso, militare: "attacco".

2.1.2 Riconoscere diversi modi con cui il malware si può nascondere, quali trojan, rootkit e backdoor

Il malware comprende numerose famiglie di software maligno, dalle quali occorre difendersi. Ne ricordiamo alcune:

- Trojan (pr. *tròjen* o più comunemente *tròian*). Il nome di questo tipo di malware deriva dalla mitologia greca e identifica un "attacco" che riesce a penetrare facilmente nel disco del computer perché si nasconde all'interno di un altro programma.
- Rootkit. I rootkit (pr. *rut-ket*) hanno lo scopo di "prendere possesso" del computer attaccato. La particolare pericolosità del rootkit deriva dal fatto che chi manovra questo tipo di malware può disporre di istruzioni capaci di aggirare le difese naturali del sistema operativo.
- Backdoor. I backdoor (pr. com'è scritto) sono programmi malevoli che s'insediano nel computer utilizzando una "porta sul retro" (da cui deriva il nome), già aperta da altri programmi (ad esempio *Emule* e *Skype*) e per questo sono difficilmente individuabili dai programmi antivirus. Anche i backdoor hanno lo scopo di creare un collegamento nascosto tra il computer attaccato e un computer attaccante. Dal computer attaccante può arrivare un gran numero di comandi che il computer attaccato esegue, senza che il proprietario se ne renda conto.

più

I computer possono essere rappresentati come l'edificio di un'azienda con una porta anteriore sorvegliata da un custode. Il custode impedisce l'ingresso alle persone sospette o indesiderate. Dalla porta anteriore transitano solo i dipendenti muniti di cartellino di riconoscimento, i clienti e i fornitori che hanno un appuntamento. Purtroppo, l'edificio ha anche delle porte posteriori che a volte rimangono aperte per molto tempo, ad esempio per scaricare o caricare le merci. In quei momenti, da quelle porte, può tentare l'ingresso chi è stato respinto dalla porta anteriore. Nei computer, le porte posteriori rimangono aperte quando si "scaricano" i file attraverso i programmi come *Emule*, quando si utilizzano collegamenti come *Skype* e così via.

2.2 TIPI

2.2.1

Riconoscere i tipi di malware infettivo e comprendere come funzionano, ad esempio virus e worm

Nel campo del malware s'incontrano altre due famiglie di software pericoloso:

- Worm (pr. *uòrm*). Appartengono alla categoria worm programmi malevoli che non hanno bisogno di associarsi a normali programmi per insediarsi in un computer. Non provocano danni diretti reali all'hardware o al software ma piuttosto determinano uno scadimento delle prestazioni del computer perché la loro attività consiste nel replicarsi all'infinito (fanno una copia continua di se stessi) e questo comporta un uso sproporzionato di spazio nel disco, di memoria RAM e di cicli di microprocessore.
- Virus. I virus informatici, al pari di quelli biologici, hanno la caratteristica di essere particolarmente infettivi, ossia sono in grado di passare da un computer a un altro, attraverso i collegamenti di rete. A differenza dei worm i virus, per manifestarsi e per contagiare hanno bisogno di un programma qualsiasi che li ospiti. Durante l'autoreplicazione, la CPU del computer può guastarsi per il calore, poiché i virus possono essere programmati per far funzionare la CPU in condizioni di overclocking (pr. *ove-clòkin* = velocità di esecuzione delle operazioni più alta del normale).

2.2.2

Riconoscere i tipi di malware usati per furto di dati, profitto/estorsione e comprendere come operano, ad esempio adware, spyware, botnet, keylogger e dialer

Oltre a quelle esaminate nei due punti precedenti, esistono altre categorie di malware che vanno sotto il nome di:

- Adware (pr. *ad-uèr*). Si tratta di programmi che includono al loro interno degli avvisi pubblicitari o banner (pr. *bane*). Questi software, oltre a rendere fastidioso l'uso del computer a causa dei continui messaggi pubblicitari che appaiono d'improvviso sullo schermo, violano la privacy dell'utente perché trasmettono a server remoti le scelte di navigazione Internet. In fase di installazione dei programmi, l'azione di un adware può risultare particolarmente fastidiosa, in quanto l'utente può essere indotto a scaricare software differente da quello voluto.
- Spyware (pr. *spai-uèr*). È un software progettato per raccogliere informazioni circa i siti visitati dall'utente e trasmetterle a un server remoto dove qualcuno le utilizzerà a scopi commerciali o di raggiro. Siccome gli spyware hanno bisogno di un programma ospite, la via di trasmissione nei computer degli ignari utenti sono i programmi in rete "gratuiti". Per questo motivo è sempre bene guardarsi dai siti del tipo: "scarica, è gratis!". Chi mai dovrebbe prendersi la pena di creare un sito, anche elaborato graficamente, per convincere gli utenti a scaricare gratuitamente del software? Diverso è il discorso del software "open source" presente sui siti specializzati e il software "contribuito" messo a disposizione dai produttori di sistemi operativi, sui propri siti.
- Botnet (pr. come si scrive). La botnet è una rete di computer infestati da software malevolo del tipo trojan, collegata a Internet. La rete diventata botnet è controllata remotamente da un server pirata. La via d'infezione principale della rete sono i collegamenti peer-to-peer (pr. *piir-to-piir* = da pari a pari), come, ad esempio Emule. Tutti i computer collegati alla botnet sono soggetti agli attacchi che provengono dal server pirata.

- Keylogger (pr. *chi-lògar*). Si tratta di malware che, una volta installato nel computer attraverso trojan, rimane sempre attivo e invia a un server remoto, le sequenze dei tasti premuti dall'operatore, compresa quella relativa alla digitazione di numeri di carte di credito e password. L'attività svolta dal keylogger è detta *keystroke logging*. L'infezione da keylogger può essere bloccata ricorrendo ad un'opportuna programmazione del firewall.
- Dialer (pr. *dàial-er*). Sono programmi in grado di fare autonomamente una chiamata telefonica a un numero di utenza, spesso estera, ad alti costi di utilizzo e di sostituire questa connessione telefonica a quella Internet, normalmente prevista nel computer che è stato infestato. Il risultato sono inaspettati costi delle bollette telefoniche. Il raggiro è possibile solo per collegamenti a Internet, fatti via modem analogico (collegamento dial up, pr. *dàial-ap*).

più

Con l'adozione dei collegamenti ADSL, i dialer non hanno più effetto. Chi è costretto a utilizzare ancora il modem analogico per il collegamento ad Internet, è bene che sappia che i dialer non hanno effetto con i sistemi operativi *Apple* e *Linux*.

2.3 PROTEZIONE

2.3.1 Comprendere come funziona il software anti-virus e quali limitazioni presenta

L'adozione di un firewall opportunamente programmato e un'attenta analisi, sia dei siti Internet che degli allegati di posta, prima di procedere alla loro apertura, mettono abbondantemente al riparo dall'infezione di malware. Ciononostante è bene che i computer siano sempre dotati di un buon programma antivirus, capace di riparare il danno, in caso di infezione avvenuta.

I programmi antivirus sono in grado di scandire le memorie del computer per ricercare del codice (righe di programma) sospetto che viene immediatamente comparato con modelli di codice malware conosciuti (definizioni o firme, impronte). Se il codice esaminato corrisponde a una definizione, viene qualificato come malware e messo in condizione di non nuocere. Se non esiste la certezza che il codice esaminato sia del malware, il programma antivirus lo isola in una zona virtuale denominata quarantena, come avveniva un tempo con l'equipaggio delle navi sospettate di portare la peste o il colera. È importante che il file delle definizioni, ossia delle "impronte" o "firme" dei virus, sia costantemente aggiornato via Internet, in modo che il programma sia messo a conoscenza anche del malware appena messo in circolazione e magari poter qualificare definitivamente come tale i file sospetti, messi in quarantena. È bene ricordarsi però che non sempre i programmi antivirus riescono a "scovare" il malware installato nel computer.

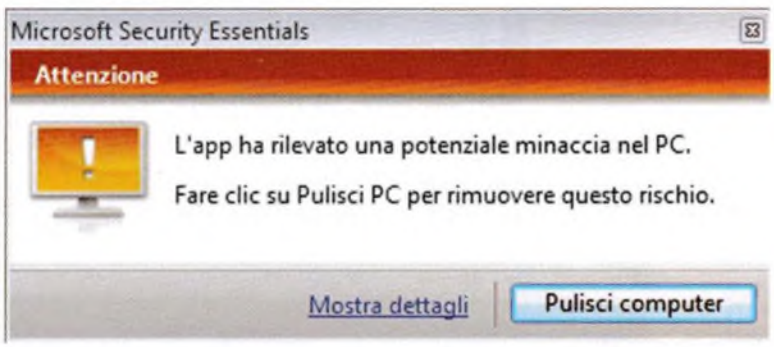
Modo di operare. Esistono due modi di operare, da parte dei programmi antivirus:

- Il programma risiede sul disco fisso e può essere richiamato per scandire un disco esterno (es. una chiavetta USB) o una cartella o un allegato di posta. In questo modo il programma normalmente non impegna risorse di sistema e non è quindi mai responsabile del decadimento delle prestazioni del computer. Per contro il computer è esposto a rischi se l'operatore non agisce in maniera accorta.
- Il programma è sempre attivo, già dall'accensione del computer e provvede autonomamente a eseguire scansioni programmate delle memorie, scandisce gli allegati di posta, interviene autonomamente

se s'inserisce una chiavetta USB o qualsiasi altro dispositivo di memoria. In questo modo il computer è al sicuro contro tutti i rischi. Per contro la super attività del programma antivirus può arrivare al punto da assorbire così tante risorse di sistema, da dare all'operatore l'impressione che tutto il computer sia a disposizione esclusiva del programma antivirus.

Evoluzione dei sistemi operativi. I moderni sistemi operativi tendono a incorporare determinate sicurezze: di base offrono un software firewall. I sistemi operativi *Windows* prevedono anche un software anti-spyware (*Microsoft Defender*). Quelli più recenti hanno incorporato il programma antivirus *Microsoft Security Essentials*.

Gli utilizzatori di *Windows* che non possedessero un sistema operativo già dotato di programma antivirus, possono ottenere scaricandola, a costo zero, l'applicazione *Microsoft Security Essentials* direttamente dal sito di *Microsoft*. Occorre però prima controllare che il sistema operativo utilizzato sia stato dichiarato compatibile.



▲ Microsoft Security Essentials

più

Programmi antivirus gratuiti. È bene confrontarsi con quest'argomento. Per quale motivo qualcuno, qualche azienda, dovrebbe impiegare delle proprie risorse per mettere in rete, magari attraverso siti graficamente accattivanti e quindi costosi, del software antivirus gratuito? Non esiste motivo plausibile, specie se a mettere in rete del software antivirus gratuito è un'azienda che vende programmi antivirus (casi di auto-concorrenza?). Di solito i programmi "gratuiti" installano insieme a se stessi anche "barre degli strumenti" particolari e applicazioni che consentono lo studio delle preferenze di navigazione in rete, con successivo invio di fastidiose pagine pubblicitarie.

Programmi antivirus commerciali. Esiste un buon numero di programmi antivirus commerciali. Occorre fare una giusta analisi dei rischi, delle risorse del computer, dell'importanza dei file che si vuole proteggere, prima di scegliere il software adeguato, tenendo conto anche del prezzo. Come è già stato detto, in molti casi, l'installazione di un corposo, prestigioso e costoso programma antivirus in un computer di modeste prestazioni, può portare alla completa paralisi dello stesso. Inoltre il programma antivirus non va installato se nel computer è già attivo un altro programma che ha la stessa funzione: due programmi antivirus concorrenti possono creare pericolosi conflitti.

Gli utilizzatori di sistemi operativi *Linux* sanno che questo sistema operativo, pur essendo meno soggetto di *Windows* alle insidie del malware, è corredato dal semplice ma efficiente software antivirus *Clamav* anch'esso facente parte della famiglia *opensource*.

2.3.2

Eseguire scansioni di specifiche unità, cartelle, file usando un software anti-virus. Pianificare scansioni, usando un software anti-virus

I programmi antivirus possono essere usati in modo automatico o non automatico, per scandire interi dischi, singole cartelle o file. È possibile impostarli perché propongano automaticamente la scansione ogni volta che un evento lo richiede (inserzione di una chiavetta USB o di un CD, ecc.) e perché scandiscano complete unità disco a orari programmati (in genere, di notte, fuori dall'orario di lavoro).

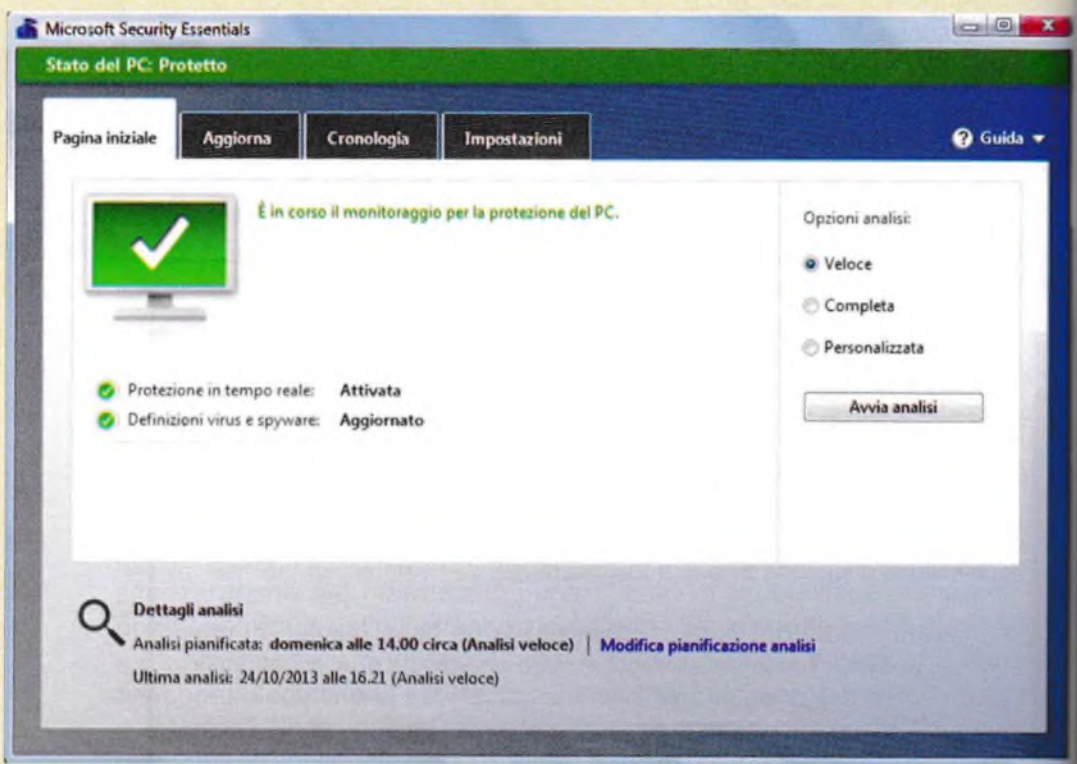
La scansione di una specifica unità di memoria (chiavetta USB, disco esterno) può essere avviata immediatamente attraverso il menu contestuale (clic con il tasto destro del mouse sull'icona dell'unità).

Per gli esercizi viene proposto il programma *Microsoft Security Essentials*, fornito insieme al sistema operativo *Microsoft*.

Esercizio 2.3.2 N.1

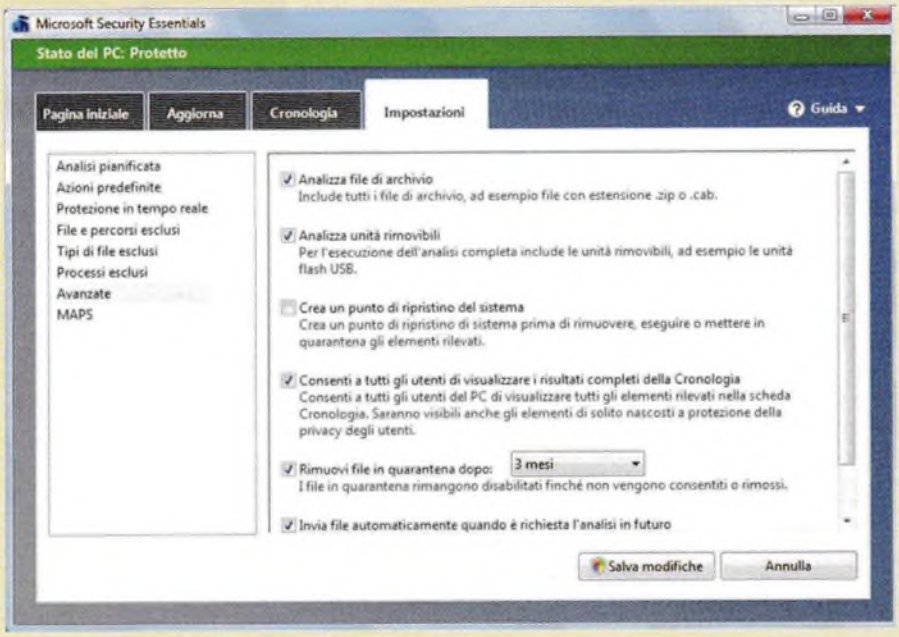
Impostare la scansione includendo un disco rimovibile, in un computer con sistema operativo *Windows*, usando *Microsoft Security Essentials*

1. Apri il programma *Microsoft Security Essentials*.



▲ *Microsoft Security Essentials*

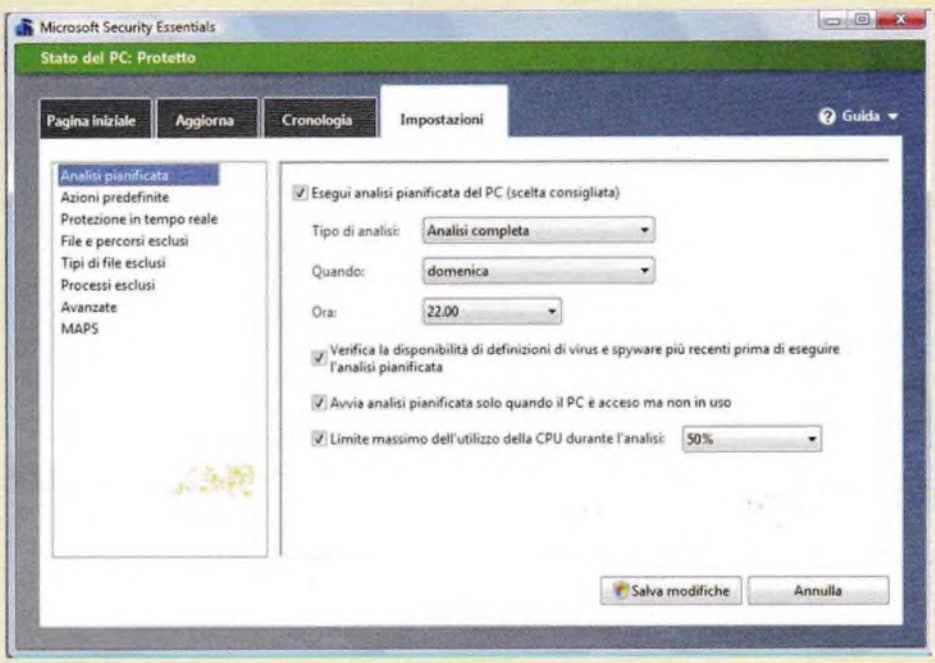
2. L'interfaccia grafica presenta quattro schede: *Pagina iniziale, Aggiorna, Cronologia e Impostazioni.*
3. Seleziona la scheda *Impostazioni* e poi l'opzione *Avanzate.*
4. Seleziona l'opzione *Analizza unità rimovibili.*
5. Clicca sul pulsante *Salva modifiche* e torna nella *Pagina iniziale.*



◀ Scheda *Impostazioni* di *Microsoft Security Essentials*

Usando *Microsoft Security Essentials* impostare l'orario per la scansione automatica completa del disco di un computer

1. Lancia il programma *Microsoft Security Essentials*.
2. Nella scheda *Impostazioni*, seleziona *Analisi pianificata*.
3. Definisci il giorno e l'orario.
4. Salva le modifiche e torna alla pagina iniziale.



▲ Programmazione scansioni *Microsoft Security Essentials*

Esercizio 2.3.2 N.2

2.3.3

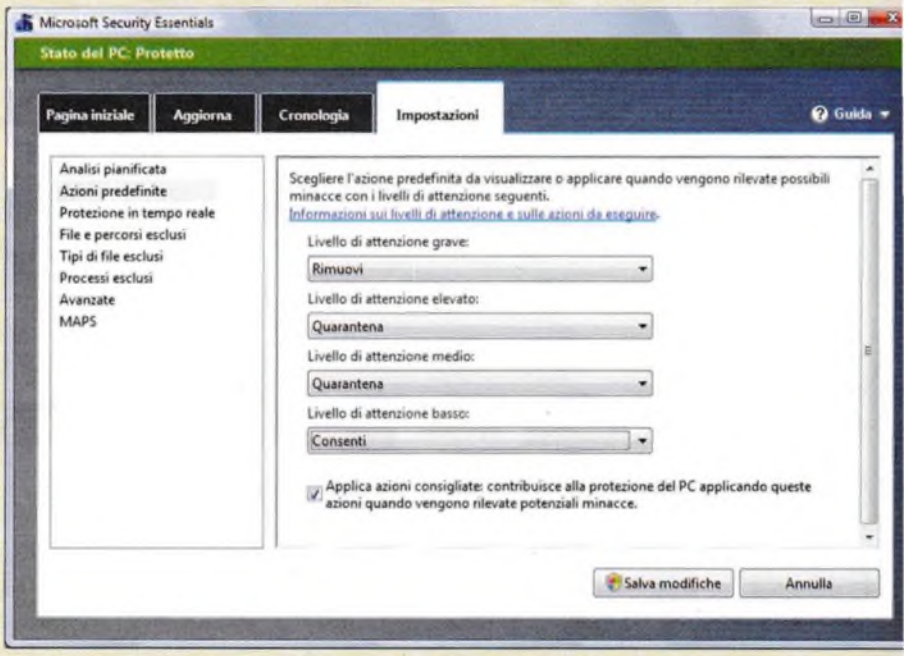
Comprendere il termine quarantena e l'operazione di mettere in quarantena file infetti/sospetti

Parlando di malware e di programmi antivirus, con il termine "quarantena" si definisce una zona virtuale di memoria dove il programma mette in isolamento i file sospetti, con l'intenzione di poterli riesaminare meglio successivamente, prima di chiedere se renderli ancora utilizzabili o destinarli all'eliminazione.

Esercizio 2.3.3 N.1

Usando *Microsoft Security Essentials*, programmare i livelli di attenzione Elevato e Medio, per mettere in quarantena i file sospetti

1. Lancia il programma *Microsoft Security Essentials*.
2. Nella scheda *Impostazioni*, seleziona *Azioni predefinite*.
3. Imposta le azioni, per i livelli di attenzione, nel seguente modo:
   Grave: Rimuovi
   Elevato: Quarantena
   Medio: Quarantena
   Basso: Consenti
4. Salva le modifiche.



▲ Azioni predefinite di *Microsoft Security Essentials*

2.3.4

Comprendere l'importanza di scaricare e installare aggiornamenti di software, file di definizione di antivirus

Tutti i programmi antivirus hanno la possibilità di scaricare periodicamente dalla rete i "file di definizione" e cioè le "impronte" o "firme" dei malware riconosciuti fino a quel momento. È possibile programmare in maniera fissa quest'operazione, in modo che il programma sia costantemente aggiornato e quindi operativo anche verso i malware più recenti.

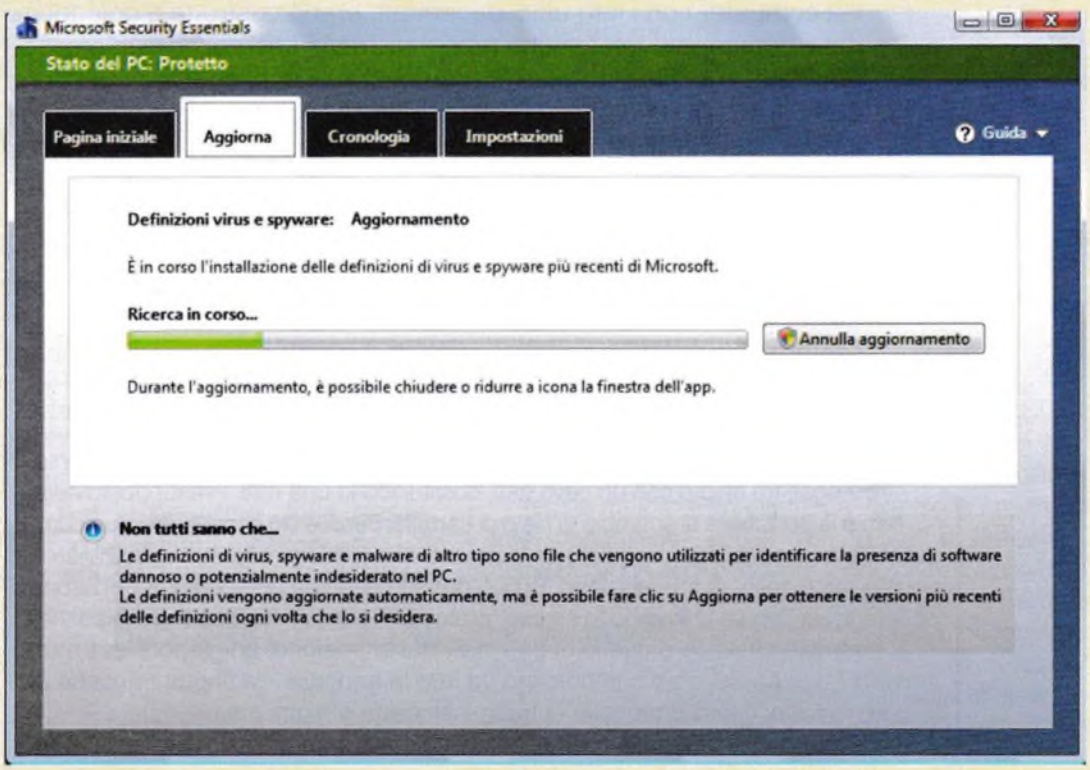
I sistemi operativi sono tenuti costantemente aggiornati dalle case produttrici, anche tra una "release" (pr. *rìlis*) e l'altra. Spesso questi aggiornamenti riguardano proprio la sicurezza e cioè la chiusura di "falle"

software attraverso le quali i crackers possono introdursi. Per questo motivo è bene lasciare che il sistema operativo si aggiorni o automaticamente, possibilmente in orari notturni, tenendo acceso il computer e collegata la rete, o al momento della segnalazione "aggiornamenti disponibili". Gli aggiornamenti in linea riguardano anche programmi di largo uso come *Java, Adobe Reader,* ecc. È bene consentire l'aggiornamento anche di questo software, ogni volta che la richiesta viene evidenziata sul video.

Esercizio 2.3.4 N.1

Usando *Microsoft Security Essentials*, aggiornare i file di definizione dei virus

1. Lancia il programma *Microsoft Security Essentials.*
2. Nella scheda *Aggiorna*, clicca sul tasto *Aggiorna.*



▲ Aggiorna file definizioni di *Microsoft Security Essentials*

Sezione 3 Sicurezza in rete

3.1 RETI

3.1.1

Comprendere il termine rete e riconoscere i più comuni tipi di rete, quali LAN (rete locale), WAN (rete geografica), VPN (rete privata virtuale)

- LAN. Quasi tutti i computer esistenti in una certa area, ad esempio un ufficio, una scuola, una fabbrica, sono collegati in rete tra loro, costituendo una LAN: *Local Area Network* e cioè una rete locale. Se la LAN è stata realizzata negli ultimi anni, il suo protocollo è quasi sicuramente TCP/IP, quello di Internet. Infatti il protocollo TCP/IP è molto sicuro, veloce e facilmente gestibile.
- WAN. Quando l'estensione fisica della rete comincia a comprendere un'area così vasta che per il trasporto dei dati tra i vari segmenti di rete occorre utilizzare, ad esempio, la rete telefonica, la rete prende il nome di WAN: *Wide Area Network*, diventa cioè una rete geografica. Il maggiore esempio di rete WAN è Internet.
- VPN. Nel recente passato, quando le aziende volevano comunicare via computer con i loro uffici decentrati, erano costrette a noleggiare dalle compagnie telefoniche nazionali, delle linee di comunicazione dedicate. I costi erano ovviamente molto elevati, specie in funzione delle distanze da coprire. Oggi, con l'avvento di Internet, sfruttando il protocollo TCP/IP, le aziende realizzano, attraverso una tecnica detta VPN: *Virtual Private Network*, una "rete privata virtuale" senza costi aggiuntivi, rispetto a quelli derivanti dal collegamento a Internet. La caratteristica della VPN è quella di essere a tutti gli effetti un pezzo di Internet che però si comporta come se fosse un'intranet, quindi una rete del tutto sicura, rispetto ai tentativi di accesso dall'esterno: le reti VPN sono protette da firewall e prevedono account + password conosciuti per consentire l'accesso.

più

Due computer dotati di opportuna scheda, del relativo software di collegamento, collegati tra di loro con un cavo dati, costituiscono una rete. Presupposto della rete è la possibilità di scambio di file e di cartelle. Perché ciò accada, nei due computer deve essere stato installato un software che fornisca alle due macchine un uguale "protocollo" di trasmissione. Si può dunque dire che due computer possono parlare tra di loro se utilizzano lo stesso "protocollo" e cioè lo stesso linguaggio.

L'esempio classico è quello di due individui al telefono: un giapponese e un italiano. I due personaggi comunicano tra loro in francese. La lingua francese è, in questo caso, il loro protocollo di trasmissione (o di comunicazione).

Punto fondamentale nella costruzione di una rete è il protocollo di trasmissione. Esistono infiniti tipi di rete, ognuno con il proprio protocollo. Questo è dovuto al fatto che, in passato, i metodi di trasmissione dei dati erano legati essenzialmente all'hardware del costruttore di computer. Il tipo di trasmissione era quasi sempre di tipo seriale, veniva cioè trasmesso un bit alla volta perché il flusso dei dati doveva transitare attraverso i modem (modulatore-demodulatore: apparecchiatura telefonica che adatta il computer alla rete del telefono). Con l'introduzione di Internet, il panorama delle reti si è rivoluzionato e la nuova tecnica è ora basata sulla trasmissione non di un bit per volta ma di un "pacchetto" fisso di bit per volta. Il protocollo adottato si chiama TCP/IP (Transport Control Protocol / Internet Protocol = Protocollo Internet con Controllo di Trasporto) e la sua caratteristica risiede nel fatto che con esso possono dialogare tutti gli altri protocolli delle reti esistenti. Per questo motivo Internet, che lo utilizza, è chiamata "la rete delle reti".

3.1.2

Comprendere il ruolo dell'amministratore di rete nella gestione delle operazioni di autenticazione, autorizzazione e assegnazione degli account all'interno di una rete

Si intuisce come, con la diffusione di Internet, gran parte degli aspetti tecnici che prima erano a carico degli esperti IT aziendali vengano ora risolti in altro modo, all'esterno dell'azienda. Di conseguenza la rete aziendale non è più riservata esclusivamente ai servizi interni ma è diventata molto più larga, includendo anche i servizi che vengono forniti dall'esterno. Anche per questo oggi ha assunto particolare rilievo la figura professionale dell'Amministratore di rete. L'Amministratore di rete ha, tra i compiti principali:

- garantire l'autenticazione degli ingressi alla rete;
- provvedere all'assegnazione degli account;
- provvedere e controllare l'autorizzazione degli account.

Per autenticazione s'intendono tutte le norme che servono a controllare la corretta identità di un utente (account), di un computer o di un software che chiedono di accedere ai servizi di rete. A questo scopo possono essere utilizzati:

- riconoscimento degli account, associati alle rispettive password;
- frasi di riconoscimento;
- tesserini identificativi letti da apposite apparecchiature;
- PIN = Personal Identification Number, numero di identificazione personale;
- riconoscimenti biometrici (voce, retina, impronte digitali, altro).

L'assegnazione degli account è un'attività particolarmente delicata poiché determina la possibilità o meno per un utente di accedere a determinati servizi di rete. L'amministratore di rete deve produrre uno schema nel quale vengono riportate:

- le norme per l'assegnazione dell'account (identificazione dell'utente, ruolo in azienda, procedure affidate, ecc.);
- le norme per la costruzione (lunghezza, tipo di caratteri) e per la gestione della password associata all'account;
- la metodologia per il suo recupero se la password viene dimenticata.

Per autorizzazione degli account s'intende la procedura attuata dall'Amministratore di rete, allo scopo di rendere i vari account realmente riconoscibili dalla rete stessa. È sempre e solo l'Amministratore di rete che può attuare la procedura inversa, cioè revocare l'accesso alla rete da parte di un determinato account.

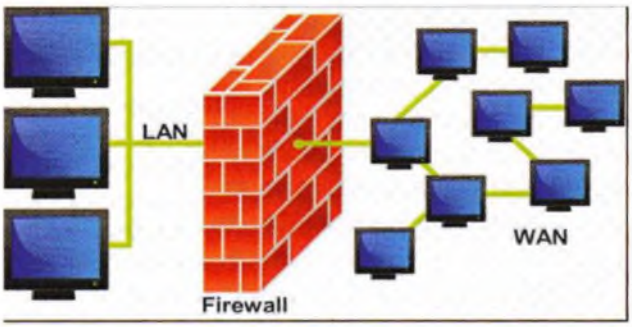
più

Le reti aziendali sono fisicamente costituite da parti di reti, ognuna dedicata ad un reparto specifico, collegate tra loro e ad Internet attraverso le apparecchiature denominate router (pr. *rùter*) e firewall. Con autorizzazione degli account s'identifica l'attività svolta dall'amministratore di rete nella programmazione dei router e dei firewall, volta a garantire che ciascun account possa liberamente accedere ai servizi di rete previsti dalle sue funzioni aziendali e che, contemporaneamente, gli sia impedito l'accesso casuale o malizioso alle funzioni per le quali non ha diritto d'accesso. Ad esempio, i firewall dovranno essere programmati affinché un account dell'area contabilità abbia accesso alle banche dati dei fornitori e dei clienti, ma non al file "paghe e contributi" dell'ufficio del personale.

3.1.3

Comprendere la funzione e i limiti di un firewall

Il firewall (pr. *fair-uòl*), dall'inglese "muro tagliafuoco" è un'apparecchiatura di rete che ha lo scopo di interporsi tra una rete locale e un'altra, generalmente: Internet. Nelle piccole applicazioni d'ufficio o in quelle casalinghe, il firewall è costituito da un software residente nel PC.



Nelle medie e grandi installazioni, il wall è costituito da un computer do di due schede di rete (una collegata a ternet e l'altra collegata alla rete loc e dell'opportuno software che, filtran pacchetti di dati in ingresso e in usc consente di abilitare o di disabilitare applicazioni e gli account che chied di interagire con la rete protetta, in b ad una programmazione preventiva.

Limiti del firewall. Il firewall può funzionare in due modi opposti:

- tutto ciò che non è vietato è permesso.
- tutto ciò che non è permesso è vietato.

Come s'intuisce, la mentalità rigida del firewall lo rende vulnerab

- primo caso: impossibilità di prevedere tutti i possibili espedienti c un cracker può mettere in atto per intrufolarsi nella rete;
- secondo caso: se l'amministratore di rete non ha previsto in dettag tutte le possibili necessità degli utenti, il firewall diventa un ostac nel normale flusso dell'attività d'ufficio. Una errata programmazio del firewall in senso assolutamente restrittivo, renderebbe del tu inutile il collegamento a Internet.

Inoltre, il firewall è inutile:
- contro gli attacchi di Ingegneria sociale (vedi punto 1.3.2);
- non controlla la presenza di virus nei pacchetti di dati;
- è impotente contro gli errori che può commettere il personale interr

3.2 CONNESSIONI DI RETE

3.2.1 Riconoscere le possibilità di connessione ad una rete mediante cavo o wireless

Al punto 3.1.1 abbiamo parlato di due computer dotati di opportu scheda e di software di collegamento che riconosce le due sched Perché i due computer costituiscano una rete LAN (*Local Ar Network)* grazie al protocollo di trasmissione, occorre che le due sche siano collegate tra loro attraverso un cavo dati, se il tipo di scheda usa prevede il collegamento via cavo (rete cablata). I computer posso ugualmente dialogare, senza essere fisicamente collegati, se il tipo scheda installata prevede il collegamento "wireless" (pr. *uàirless*) e ci "senza cavo" (Wireless LAN o WLAN).

Nelle reti moderne il protocollo usato è TCP/IP e il cavo dati cl collega i computer termina con due connettori denominati RJ45.

Se la connessione è di tipo wireless, è opportuno impostare p l'apertura della rete, la sicurezza WEP o WPA. La sicurezza compor la criptazione/decriptazione c messaggi in transito. Inoltre, richiesta di inserire la password rete impedisce l'ingresso ne stessa a chi non ne ha diritto.

▲ Icona wirless

◀ Connettori RJ45

3.2.2

Comprendere che la connessione ad una rete ha implicazioni di sicurezza, quali malware, accessi non autorizzati ai dati, mantenimento della privacy

L'utilizzo delle reti dati tra i computer comporta numerosi vantaggi che vanno crescendo con l'evoluzione della tecnologia complessiva. I moderni strumenti di collaborazione, di archiviazione, di calcolo in rete sono stati resi possibili proprio dallo sviluppo e dalla diffusione della rete Internet.

D'altra parte, quando ci si collega ad una rete per usufruire di qualsiasi servizio, bisogna essere consapevoli che ci si espone a diversi rischi quali:

- possibilità di importare malware;
- sono possibili accessi non autorizzati ai dati;
- la privacy può essere compromessa.

Contro questi rischi possono essere messi in atto degli strumenti preventivi quali:

- installazione di un firewall che limiti gli accessi non autorizzati;
- obbligo di digitare account e password riconosciuti, per collegarsi.

Inoltre nel computer deve essere presente del software antivirus costantemente aggiornato.

SICUREZZA SU RETI WIRELESS 3.3

3.3.1

Riconoscere l'importanza di richiedere una password per proteggere gli accessi a reti wireless

La necessità di proteggere le reti wireless con una password deriva da due necessità:

- limitare il numero degli accessi;
- impedire ingressi malevoli nella rete.

Accessi. La necessità di limitare il numero degli accessi risiede nel fatto che lo spazio virtuale nel quale transitano i pacchetti di dati di ogni singolo utente, può essere visto come un'autostrada a più corsie. In ogni corsia transitano, in un determinato istante, i pacchetti di un utente. Se gli utenti aumentano, il traffico rallenta e se aumenta troppo, si blocca.

Ingressi malevoli. Mentre sembra poco probabile che uno sconosciuto possa entrare in un ufficio privato, collegare con un cavo il proprio PC alla rete locale e mettersi tranquillamente a lavorare senza che nessuno se ne accorga e lo metta alla porta, il fatto che la rete wireless sia basata sulla trasmissione con onde radio rende la cosa perfettamente possibile, addirittura senza che l'intruso debba entrare nel locale che ospita il computer. Rimanendo fisicamente nei dintorni, una volta stabilito il collegamento e se ha la giusta preparazione tecnica, l'abusivo può introdursi arbitrariamente nei programmi e nei file dei regolari account, con risultati disastrosi.

3.3.2

Riconoscere diversi tipi di sicurezza per reti wireless, quali WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access), MAC (Media Access Control)

Una rete può dirsi sicura se rispetta tre principi:

- Riservatezza: i dati trasmessi non devono poter essere intercettati abusivamente.
- Integrità: i messaggi trasmessi non devono poter essere modificati.
- Accesso autorizzato: qualsiasi accesso alla rete deve avvenire solo attraverso account e password riconosciuti.

L'insieme di questi tre punti è previsto negli obiettivi di tre protocolli di sicurezza per le reti Wireless:

- WEP (*Wired Equivalent Privacy* = riservatezza equivalente a quella assicurata da un cavo LAN).
- WPA (*Wi-Fi Protected Access* = collegamento WiFi protetto)
- MAC (*Media Access Control* = controllo di accesso a livello hardware)

più

A questo proposito va ricordato che le schede di rete hanno ognuna un proprio indirizzo composto da un numero che identifica il costruttore (non possono esserci nel mondo due costruttori con lo stesso numero) seguito da un numero che identifica il modello di scheda, seguito da un numero progressivo di produzione. In questa maniera ogni scheda installata si distingue da tutte le altre esistenti. I computer collegati alla rete Internet possono essere identificati, con esattezza, in base al numero univoco della scheda di rete installata.

La sicurezza WEP si pone l'obiettivo di fornire, via onde radio, la stessa sicurezza che offrono le reti LAN cablate. Può avere una frase di sicurezza a 40 o a 128 bit (maggiore è il numero dei bit, maggiore è la sicurezza) + 24 bit di controllo.

La sicurezza WPA ha una frase di sicurezza più lunga (128 bit + 48 bit di controllo) e include un sistema più efficiente per garantire l'integrità del messaggio.

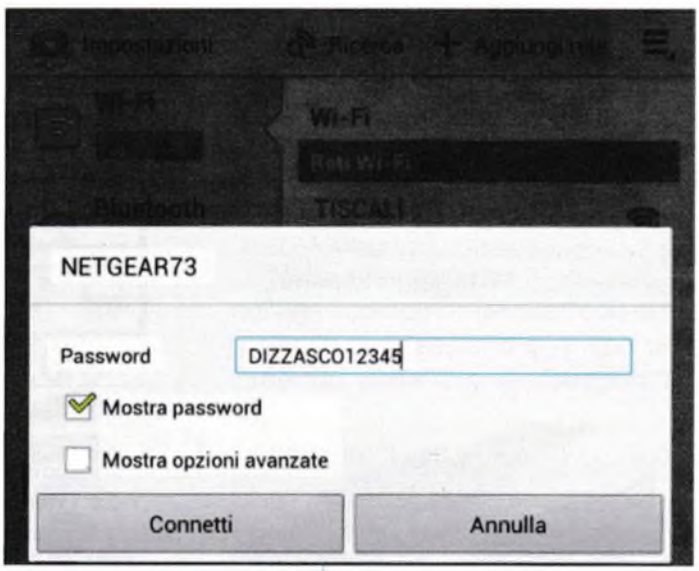
La sicurezza MAC prevede il collegamento tra computer, basato sull'indirizzo univoco delle rispettive schede di rete.

3.3.3

Essere consapevoli che usando una rete wireless non protetta si rischia che i propri dati vengano intercettati da "spie digitali"

Quando s'installa un router ADSL domestico, si tratta quasi sempre di un dispositivo wireless che magari include anche il VoIP: Voice Over Internet Protocol = telefonia basata sul protocollo Internet. Una delle semplici operazioni da compiere, è l'assegnazione (opzionale) della sicurezza WEP. Si tratta di decidere la lunghezza della frase di accesso (chiave o password) e inventarsi il testo che verrà richiesto ogni volta che si tenterà l'accesso alla rete. Di quanti caratteri deve essere composto il testo?

Nel caso di sicurezza a 128 bit, la lunghezza della chiave è di 13 caratteri. Infatti: 13 caratteri x 8bit/carattere = 104 bit + 24 bit/controllo = 128 bit totali.



▲ **Frase di sicurezza per WEP a 128 bit su un dispositivo mobile**

La rete protetta può essere utilizzata solo da chi conosce la password. Se invece si decide di lasciare la rete sprotetta, è bene sapere che si corrono dei rischi. Normalmente chi si collega ad una rete Wi-Fi sprotetta non riesce a entrare nei computer che fanno parte della rete wireless LAN, poiché non conosce i vari account e le rispettive password. L'unica cosa pratica che può fare, è collegarsi a Internet. Se però l'utente abusivo ha tempo e voglia a disposizione, può studiare vari trucchi per intrufolarsi nei computer collegati, aggirando account e password e questo rappresenta un notevole rischio per la sicurezza dei dati. Chi opera nascostamente per entrare in una rete di computer, è definito "spia digitale".

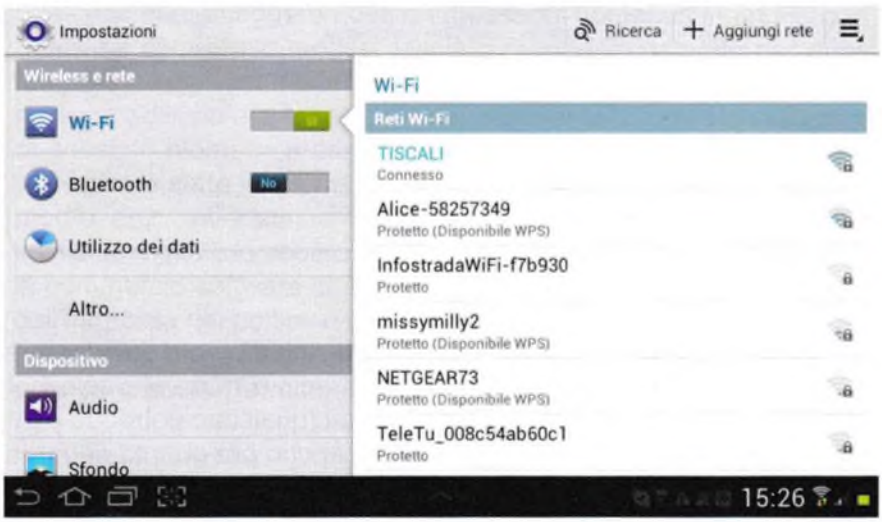
3.3.4 Connettersi ad una rete wireless protetta/non protetta

Quando si tenta la connessione ad una rete wireless protetta, viene richiesta la digitazione della chiave (password, passphrase). Viceversa, se la rete non è protetta, l'accesso è immediato. Una rete protetta si distingue per avere a fianco al nome il simbolo di un lucchetto chiuso.

Se ci si collega alla rete Internet da un Hot Spot (pr. come scritto) e cioè un luogo pubblico dotato di collegamento Wi-Fi a Internet e la rete non è protetta, è bene controllare se il protocollo che il programma usa per il collegamento sia *https*, come nel caso di utilizzo del servizio di posta *Gmail* (https://mail.google.com) o di *Facebook* (https://www.facebook.com).

Il protocollo https (http sicuro) provvede infatti a criptare la trasmissione dei dati, complicando il compito di intercettarla a chi volesse farlo, come invece non avviene se il protocollo di collegamento è il normale http.

Quando si tenta il collegamento ad una rete wireless con sicurezza WEP o WPA, appare una finestra di dialogo con la richiesta di inserimento di una frase di controllo detta *chiave*, in inglese: passphrase (pr. *pas-freis*).



Connettersi ad una rete Wireless

CONTROLLO DI ACCESSO 3.4

3.4.1 Comprendere lo scopo di un account di rete e come accedere alla rete usando un nome utente e una password

La procedura che si usa per collegarsi a un computer, una rete o un'applicazione è detta *login* (pr. *log-in*). Se il computer, la rete o l'applicazione sono protetti, il *login* consiste nella digitazione di un nome riconoscibile (account) e della relativa password.

Generalmente le reti sono protette da un firewall che ha lo scopo di consentire l'accesso solo a utenti che esibiscono un account, fornito dall'amministratore di rete e una password associata.

Le reti protette richiedono sempre la digitazione di account e password validi. L'esibizione di un account valido è condizione imprescindibile. Nel caso della password invece, generalmente sono previste delle procedure che consentono il recupero della password dimenticata o scaduta o la possibilità di produrne una nuova.

La procedura per connettere un PC ad una rete WiFi è la seguente: *Pannello di controllo* > *Rete e Internet* > *Centro connessioni di rete e condivisione* > *Gestisci reti wireless* > doppio clic sulla rete da attivare > *Scheda Sicurezza* > *Tipo di crittografia: WEP* > digitare la chiave nel riquadro *Chiave di sicurezza di rete*

più

L'accesso attraverso la digitazione di account e password riconosciuti dall'applicazione, costituisce il primo elemento della sicurezza in rete.

L'applicazione, ad esempio *Gmail* o *Facebook*, provvede sempre a creare un ambiente protetto per l'account, riservando i suoi dati in un'area personale nella quale gli altri account non possono penetrare, a meno di "falle" informatiche nel sistema. Se un account tenta di collegarsi con una password sbagliata, l'applicazione deve far partire un sistema di riconoscimento certo dell'utente, prima di consentirgli di dotarsi di una nuova password con la quale collegarsi. Uno dei metodi usati per riconoscere con buona certezza l'utente è costituito dalla digitazione di un codice di identificazione inviato dall'applicazione, attraverso un SMS, al telefono cellulare dell'utente. Il numero del telefono deve ovviamente essere stato fornito in precedenza e deve far parte degli elementi in base ai quali l'utente ha diritto di accesso.

3.4.2

Riconoscere buone politiche per la password, quali evitare di condividere le password, modificarle con regolarità, sceglierle di lunghezza adeguata e contenenti un numero accettabile di lettere, numeri e caratteri speciali

A differenza dell'account o nome dell'utente, la password deve essere sempre mantenuta segreta. Questo principio non vale solo per quanto riguarda la riservatezza dei propri dati (qualcuno potrebbe pensare: "Non m'importa di essere spiato") ma anche per quanto riguarda la riservatezza dei dati di tutti gli altri utenti della rete. Se infatti una "spia informatica" s'impossessa delle "credenziali" di un utente e cioè di account + password, entrando così tranquillamente nella rete, viene ovviamente favorito nella sua attività illegale. Nel privato ma soprattutto nel lavoro in azienda, esistono delle regole ormai consolidate nella gestione delle password.

La password:

- deve essere mantenuta segreta;
- non va scritta;
- deve essere lunga almeno 8 caratteri;
- non deve essere costituita da un nome facilmente riconducibile all'utente;
- deve contenere lettere e numeri;
- deve essere cambiata regolarmente e occasionalmente se si pensa che sia stata scoperta.

In alcuni casi, ad esempio nella sicurezza di una rete wireless, la password è costituita da un insieme di lettere e di numeri abbastanza lungo. In questi casi non si parla di password ma di passphrase (vedi punti: 3.3.2 e 3.3.3).

3.4.3

Identificare le comuni tecniche di sicurezza biometriche usate per il controllo degli accessi, quali impronte digitali, scansione dell'occhio

La segretezza della password, per quanto sia accurata, può in molti casi essere violata, utilizzando tecniche informatiche. Per questo motivo, i ricercatori in materia di sicurezza hanno realizzato dei metodi computerizzati per rendere l'accesso alle reti indipendente dalla digitazione di una password. Questi metodi comportano il riconoscimento dell'utente attraverso la lettura (scansione) di:

- voce;
- retina oculare;
- impronte digitali;
- altri parametri.

Ovviamente, questi parametri che vengono definiti biometrici e cioè basati sulla misura di elementi fisici, devono essere forniti al programma che provvede al loro riconoscimento, prima della richiesta di accesso alla rete.

Biometria. La sicurezza dei dati implica la necessità di impedire che qualcuno possa leggere i dati o i messaggi contenuti in un PC o in un qualsiasi dispositivo mobile, lasciato magari incustodito per qualche tempo. Una tecnica moderna che garantisce l'accesso ai dati alla sola persona abilitata è la tecnica di riconoscimento "biometrico". La tecnica di accesso biometrica consiste nell'associazione alla password (che può essere stata involontariamente diffusa o comunicata) il riconoscimento di caratteristiche fisiche assolutamente personali, come le impronte digitali, la voce o l'iride oculare e altro. A tale scopo esistono in commercio software che vanno associati ad un dispositivo di lettura dell'impronta del pollice o dell'indice e software che vanno associati al microfono, alla webcam del PC che bisogna fissare con lo sguardo, quando ci si vuol far riconoscere.

Sezione 4 Uso sicuro del web

4.1 NAVIGAZIONE IN RETE

4.1.1

Essere consapevoli che alcune attività in rete (acquisti, transazioni finanziarie) dovrebbero essere eseguite solo su pagine web sicure

L'attività di spionaggio informatico è particolarmente orientata sui siti attraverso i quali si effettuano attività commerciali o finanziarie. Obiettivo immediato del cracker è quello di praticare il "furto di identità" ottenendo illegalmente:

- "credenziali" dell'utente (account + password);
- numero della carta di credito;
- PIN della carta di credito;
- ente di emissione della carta di credito;
- numero di conto corrente.

Ottenute alcune di queste informazioni, il cracker è in grado di ripulire il conto corrente bancario della vittima.

Come mettersi al riparo dal rischio del "furto di identità"? Innanzitutto facendo riferimento solo a siti Internet ritenuti "sicuri" come i siti degli istituti bancari conosciuti, i siti commerciali di utilizzo diffuso o associati a marchi riconoscibili. Siti che esibiscono il certificato digitale controllabile direttamente in linea, oltre al simbolo del lucchetto chiuso, accanto all'indirizzo della pagina, con protocollo https.

4.1.2

Identificare un sito web sicuro, ad esempio associato ad https, simbolo del lucchetto

La maggior parte dei siti web utilizza il protocollo http che consente un accesso rapido, senza che debba essere adottata qualsiasi procedura per ottenere il collegamento. I siti che possono trattare dati "sensibili" adottano invece il protocollo https (http Sicuro) che associa al protocollo HTTP la *crittografia a chiavi asimmetriche* dei dati trasferiti (L'argomento *crittografia a chiavi asimmetriche* è trattato al punto 1.2.4). Quali sono i siti che tipicamente utilizzano il protocollo HTTPS? Generalmente sono i siti di origine finanziaria o assicurativa; i siti che praticano il commercio online ma anche quelli delle cliniche mediche e degli ospedali. Anche i programmi di posta e i browser web trattano dati che possono essere definiti "sensibili". Infatti *Gmail*, *Chrome*, *Google*, *Firefox*, ecc. usano il protocollo HTTPS.

Come poter identificare come sito "sicuro" un sito che richiede l'immissione di dati sensibili? Esistono tre parametri che possono fornire dati circa la sicurezza del sito:

- sulla barra degli indirizzi deve apparire il simbolo di un lucchetto chiuso;
- sulla barra degli indirizzi deve apparire il protocollo https;
- deve essere possibile la verifica del certificato del sito, cliccando due volte sul simbolo del lucchetto chiuso.

Esercizio 4.1.2 N.1

Verificare la presenza del protocollo https in un sito bancario

1. Apri il motore di ricerca *Google*.
2. Digita il nome di un istituto bancario (*Banca Etica iNBank*).
3. Clicca sull'indirizzo che appare (*Banca Popolare etica*).
4. Entra in un'area "sicura" cliccando sul link *Area clienti*.
5. Controlla che nella barra degli indirizzi sia presente il protocollo *https*, accompagnato dal simbolo del lucchetto chiuso.

▲ Protocollo https in sito bancario

4.1.3 Essere consapevoli del pharming

Attraverso il pharming (pr. *fàrmin*) il malintenzionato tenta di impossessarsi dell'identità della vittima: nome, indirizzo, numero di carta di credito, numero di conto corrente, ecc. indirizzandola verso un sito pirata, clone di un sito realmente operante.
L'attività criminosa è la stessa del phishing (vedi punto 1.1.2) con la differenza che mentre il phishing riguarda il rapporto del cracker con la vittima "da prendere all'amo", il pharming riguarda lo studio che il cracker fa dell'azienda e del suo sito, allo scopo di simularne un altro, quanto più possibile, simile all'originale. Nei siti clonati la barra degli indirizzi non ha il simbolo del lucchetto e il protocollo è http.

4.1.4 Comprendere il termine "certificato digitale". Convalidare un certificato digitale

I siti web che praticano attività finanziarie o commerciali, come pure i siti web che distribuiscono il software, attestano la loro identità attraverso un "certificato digitale", nello stesso modo che una persona, all'atto di effettuare un'operazione che lo richiede, esibisce la propria carta di identità. Il certificato digitale è basato sulla crittografia a chiavi asimmetriche, argomento descritto al punto 1.2.4 ed è costituito da un pacchetto di informazioni firmato da un'autorità riconosciuta. Il pacchetto deve contenere:

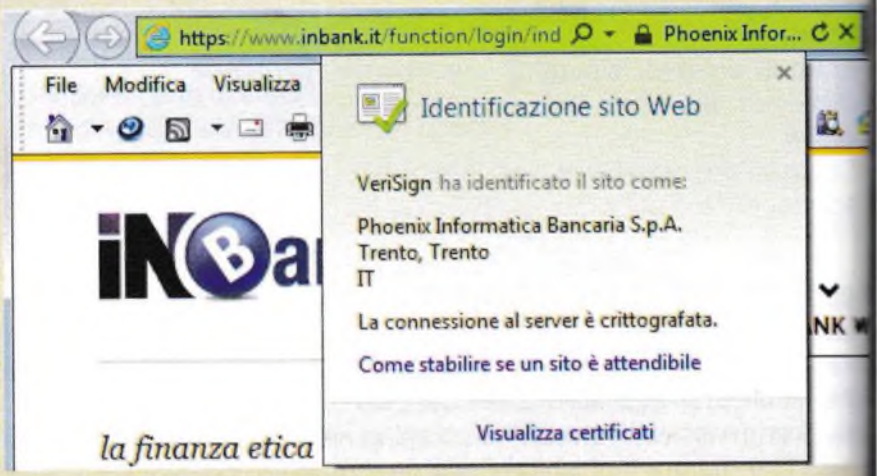
- generalità di un sito web o di computer o di un'organizzazione, ai quali il certificato si riferisce;
- chiave pubblica del titolare del certificato;
- periodo di validità attestato dall'autorità riconosciuta.

I siti delle banche o delle aziende che praticano il commercio online, utilizzano il protocollo di trasmissione https e mostrano accanto all'indirizzo il simbolo di un lucchetto chiuso. Se si clicca (due volte) sul lucchetto, parte la procedura di convalida del certificato digitale. Viene automaticamente inviato all'indirizzo del sito un testo crittografato con la chiave pubblica riportata nel certificato e, se il sito è quello reale, esso deve poter rispondere con l'uso della corrispondente chiave privata, generando accanto al simbolo del lucchetto, il messaggio: Sito sicuro o Sito verificato.

Esercizio 4.1.4 N.1

Verificare il certificato di un sito bancario

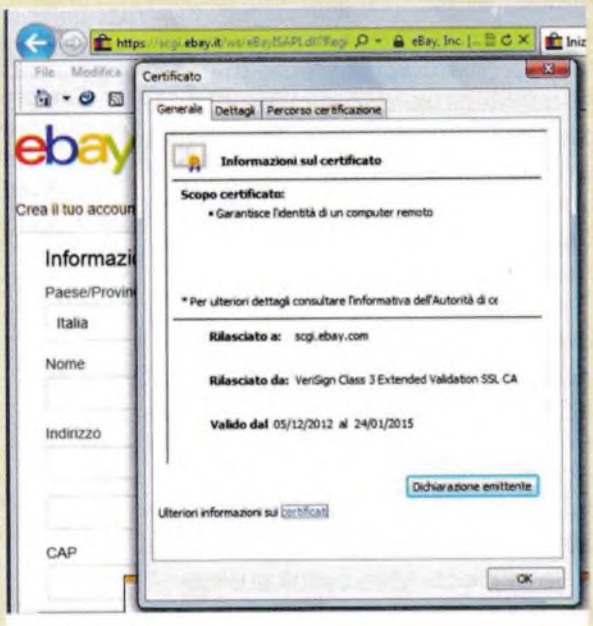
1. Apri il motore di ricerca *Google*.
2. Digita il nome di un istituto bancario (*Banca Etica iNBank*).
3. Clicca sull'indirizzo che appare (*Banca Popolare Etica*).
4. Entra in un'area "sicura" cliccando sul link *Apri un conto*.
5. Nella finestra che appare, clicca due volte sul simbolo del lucchet chiuso.
6. Controlla che sia avvenuta la verifica del certificato del sito.



▲ Verifica certificato del sito

Esercizio 4.1.4 N.2

Convalidare il certificato di un sito commerciale



▲ Certificato di *eBay*

1. Apri il motore di ricerca *Google*.
2. Digita il nome del sito di commercio pravendita *eBay*.
3. Clicca sull'indirizzo che appare (*eBay Annunci*.
4. Entra in un'area "sicura" cliccando sul bottone *Inserisci Annuncio*.
5. Nella finestra che appare, clicca due volte sul simbolo del lucchetto chiuso.
6. Controlla che sia avvenuta la verifica del certificato del sito.

4.1.5 Comprendere il termine "one-time password"

Uno dei maggiori rischi per la sicurezza delle reti aziendali (VPN = Virtual Private Network, vedi punto 3.1.1) deriva dagli accessi effettuati dai dipendenti che lavorano fuori sede, tipicamente i venditori e i tecnici d'assistenza.

Costoro, attraverso i normali dispositivi mobili (palmari, laptop, tablet, smartphone) o (ancora più rischioso) attraverso un computer del cliente, si collegano alla rete aziendale, per leggere la posta o per cercare notizie specifiche. Ogni volta che essi digitano i propri account e password, mettono un estraneo in condizione di apprendere la maniera di entrare abusivamente nella rete aziendale.

Per evitare che questo rischio duri nel tempo, gli esperti di sicurezza informatica hanno inventato il metodo della *one time password* (pr. *uan tàim pàss-uòrd*) che vuol dire: password valida una sola volta. Le tecniche di realizzazione sono varie. La più usata si basa sulla richiesta di accesso alla rete; la rete risponde inviando al computer chiamante o al cellulare della persona che chiama, un codice d'accesso valido per una sola volta, dopo aver verificate le credenziali dell'utente che chiede l'accesso. Il codice d'accesso è generato da un complesso algoritmo, ovviamente segreto.

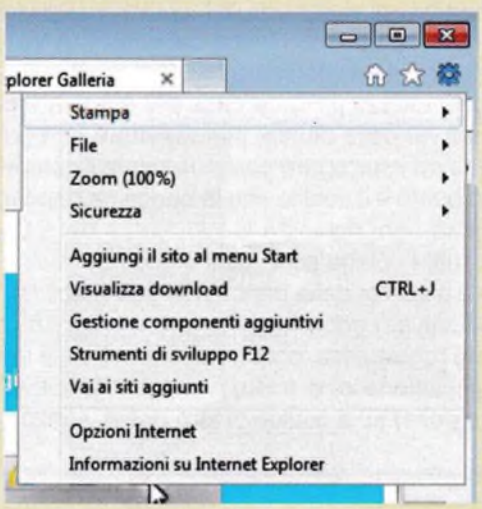
4.1.6 Selezionare impostazioni adeguate per attivare, disattivare il completamento automatico, il salvataggio automatico quando si compila un modulo

La compilazione dei moduli online è un'operazione che richiede sempre una buona dose di attenzione e di pazienza. Spesso, per accelerare si ricorre all'attivazione del completamento automatico dei campi (i campi sono le caselle che compongono il modulo).
Attenzione però: il completamento automatico potrebbe facilitare il compito della solita "spia informatica" che si aggira tra le scrivanie. Particolarmente rischioso è, sotto questo aspetto, il completamento automatico della password che può essere attivato solo sul PC domestico, avendo la certezza di essere l'unica persona che usa quel PC.
L'attivazione e la disattivazione del completamento automatico sono operazioni che vanno eseguite sul browser Internet utilizzato. La disattivazione del completamento automatico non comporta automaticamente la cancellazione dei dati conservati in precedenza. Questi vanno quindi cancellati a parte.

Esercizio 4.1.6 N.1

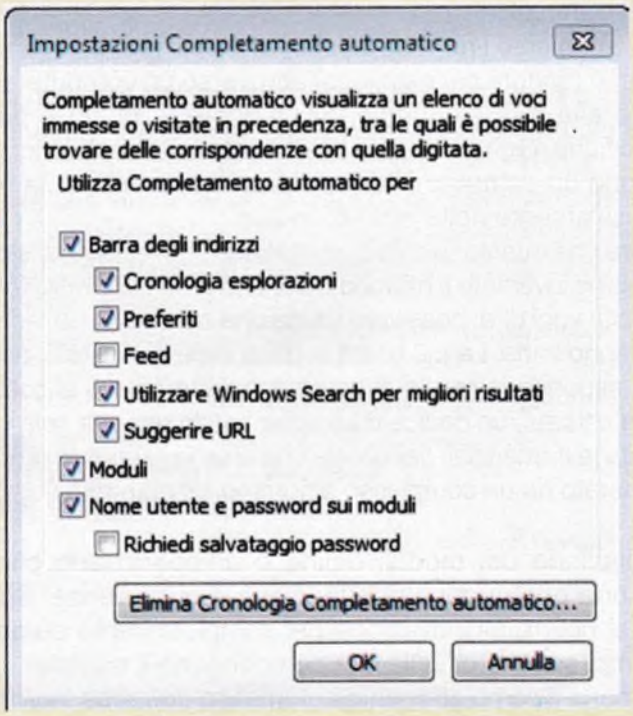
Utilizzando il browser *Internet Explorer 10*, disattivare il completamento automatico dei moduli e la possibilità che le password possano essere salvate automaticamente

1. Apri il browser *Internet Explorer*.
2. In alto a destra, seleziona il pulsante a forma di ruota dentata.
3. Viene visualizzato il menu a discesa.
   - Seleziona *Opzioni Internet*.
   - Seleziona la scheda *Contenuto*.
4. Clicca sul primo pulsante *Impostazioni* (memorizza i dati immessi in precedenza)
5. Disabilita l'opzione di completamento automatico per i moduli.



6. Disabilita l'opzione *Richiedi salvataggio password*.
7. Termina con il pulsante *OK*.

Disattivazione completamento moduli e password, con *Internet Explorer*



4.1.7 Comprendere il termine "cookie"

Quando si consultano delle pagine web, può accadere che il sito v visitato invii un cookie, ossia un file che si deposita nel disco d calcolatore dal quale è partita la richiesta di visualizzazione. Quan l'utilizzatore del computer ritorna a visitare lo stesso sito, il cookie pas al sito, insieme ai dati che identificano il computer, anche una serie dati di tipo commerciale e statistico. I cookie sono usati particolarmen dalle aziende che praticano il commercio online. Infatti, attraverso sistema dei cookie, è possibile costruire il "profilo" degli utenti della re e, di conseguenza, offrire a utenti pubblicità "mira ossia pubblicità che può e sere ben accolta e favorire vendita del prodotto o s servizio. È ovvio che, a d petto di quanto sperano i del commercio online, q mai chi utilizza la gradisce la pubblicità richiesta e infatti, i bro prevedono la possibilità bloccare tutti o in par cookie.

più

Dal momento che i siti che inviano i cookie possono essere sospettati di violazione della privacy, i browser provvedono a fornire l'opzione di blocco dei cookie. A volte però è indispensabile che il meccanismo dei cookie sia attivo. Quando, per esempio, si utilizza il PC da casa per effettuare operazioni bancarie, il server della banca, per rispettare le regole di sicurezza è costretto ad interrogare continuamente il computer chiamante. A questo punto è il cookie che la banca ha depositato in quel PC a fornire ad ogni richiesta le generalità del PC stesso. Se nel browser tutti i cookie sono stati bloccati, il dialogo tra il PC domestico e il server della banca non può stabilirsi.

In definitiva, i cookie vanno tenuti o vanno cancellati? Non esiste una regola fissa, occorre definire di volta in volta cosa fare. Se l'applicazione che stiamo usando è sicura e lo richiede, lasciamo pure i suoi cookie al loro posto, senza paura.

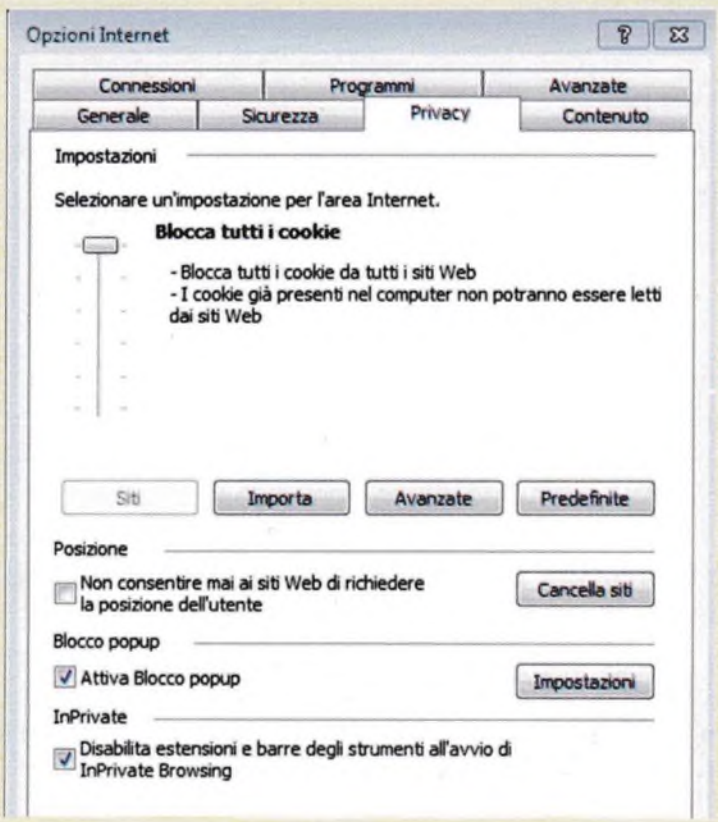
4.1.8 Selezionare impostazioni adeguate per consentire, bloccare i cookie

I browser consentono all'utente di impedire l'installazione incontrollata dei cookie. D'altra parte, alcuni cookie devono essere necessariamente installati se il sito con il quale si vuole dialogare (ad esempio un istituto bancario) lo richiede. In questi casi è possibile programmare il filtro dei cookie sul browser. L'operazione si svolge nella sezione *Impostazioni avanzate*.

Esercizio 4.1.8 N.1

Bloccare tutti i cookie nel browser *Internet Explorer*

1. Apri il browser *Internet Explorer*.
2. In alto a destra, seleziona il pulsante *Strumenti* a forma di *ruota dentata*. Viene visualizzato il menu a discesa.
3. Seleziona *Opzioni Internet*.
4. Seleziona la scheda *Privacy*.
5. Regola in alto il cursore verticale a sinistra che attiva gradualmente il blocco dei cookie.



Bloccare tutti i cookie con *Internet Explorer*

Esercizio N.2

Usando il browser *Internet Explorer*, consentire l'ingresso solo dei cookie provenienti da un sito specifico

1. Copia l'indirizzo (URL) di un sito che potrebbe richiedere l'abilitazione dei cookie.
2. Apri il browser *Internet Explorer*.
3. Clicca sul pulsante *Strumenti* a forma di ruota dentata, in alto a destra.
4. Nella finestra che appare, seleziona *Opzioni*.

5. Nella sezione *Privacy*, clicca sul primo pulsante: *Siti*.
6. Nella finestra *Gestione della privacy per sito*, copia l'indirizzo del s dal quale vuoi accettare i cookie, nella finestra *Indirizzo sito We*
7. Clicca sul pulsante *Consenti*.
8. Termina con il pulsante *OK*.

Consenso selettivo ai cookie con *InternetExplorer*

Esercizio 4.1.8 N.3

Usando il browser *Internet Explorer*, bloccare i cooki provenienti da un sito specifico

1. Apri il browser *Internet Explorer*.
2. Copia l'indirizzo del sito dal quale vuoi bloccare i cookie.
3. Clicca sul pulsante *Strumenti* a forma di ruota dentata, in a destra.
4. Nella finestra che appare, seleziona *Opzioni Internet*.
5. Seleziona la scheda *Privacy*.
6. Controlla che il cursore a sinistra si trovi in posizione centrale.
7. Clicca sul pulsante *Siti*.
8. Nella casella *Indirizzo sito Web* della finestra *Gestione della pri per sito* che appare, incolla l'indirizzo del sito dal quale vuoi bl care i cookie.
9. Clicca sul pulsante *Blocca*.
10. Termina con il pulsante *OK*.

4.1.9 Eliminare dati privati da un browser, quali cronologia di navigazione, file temporanei di Internet, password, cookie, dati per il completamento automatico

A volte capita di lavorare, anche in maniera sostenuta, utilizzando un computer di un amico, di un collega, di un fornitore. Al termine dell'attività, prima di lasciare il posto di lavoro occasionale, occorre tassativamente ricordarsi di non lasciare tracce di alcun tipo. Questa raccomandazione non è differente dall'altra, relativa alla scuola e sempre valida, di pulire accuratamente la lavagna, prima di lasciare l'aula.

Con il browser *Internet Explorer*, cancellare tutti i dati di navigazione in un computer

1. Apri il browser *Internet Explorer*.
2. In alto a destra, seleziona il pulsante *Strumenti* a forma di *ruota dentata*.
3. Viene visualizzato il menu a discesa.
4. Seleziona Opzioni *Internet*.
5. Seleziona la scheda *Privacy*.
6. Clicca sul pulsante *Cancella Siti*.

Eliminare tutti i dati di navigazione

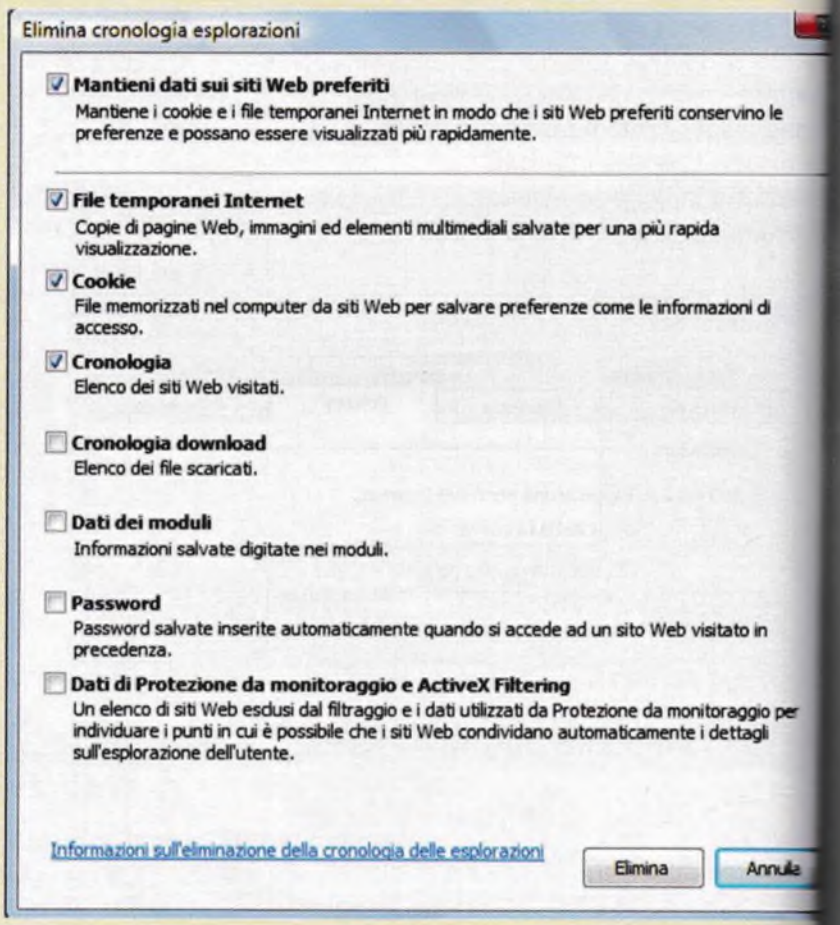
Esercizio 4.1.9 N.1

Esercizio 4.1.9 N.2

Con il browser *Internet Explorer*, eliminare la cronologia e i file temporanei

1. Apri il browser *Internet Explorer*.
2. In alto a destra, seleziona il pulsante *Strumenti* a forma di ruota den
3. Seleziona *Opzioni Internet*.
4. Seleziona la scheda *Generale*.
5. Clicca sul pulsante *Elimina*.
6. Nella finestra *Elimina cronologia esplorazioni* che si apre, selezi le opzioni *File temporanei Internet* e *Cronologia*.
7. Termina con il pulsante *Elimina*.

Elimina cronologia esplorazioni



4.1.10

Comprendere lo scopo, la funzione e i tipi di software per il controllo del contenuto, quali software per il filtraggio di Internet, software di controllo genitori

Se in casa c'è un bambino al quale piace curiosare, un PC coll ad Internet può essere di grande aiuto. Occorre però che i ge pongano particolare attenzione a non lasciare il bambino solo c computer. Il migliore utilizzo di questo potente mezzo di comunicaz consiste nel curiosare insieme: genitore e bambino.
Esistono rischi in cinque grandi aree di attività:

- durata dell'uso quotidiano del computer;
- siti visitati nel Web;
- messaggi di posta elettronica;
- chat line;
- reti sociali (*Facebook* e altre).

Per quanto riguarda l'ultimo punto (*Facebook* e altre reti sociali), un genitore attento può controllare l'attività del proprio minore anche da lontano, durante gli intervalli della giornata lavorativa.

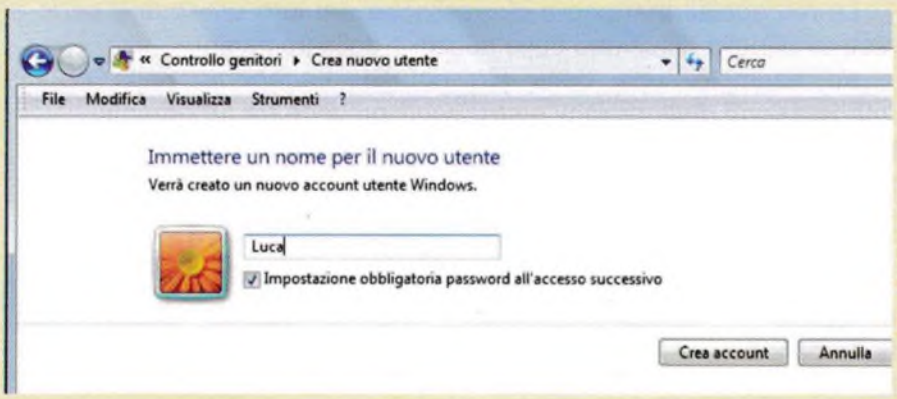
Per le altre aree, esistono programmi che possono anche impedire il funzionamento delle applicazioni specifiche o addirittura dello stesso computer, al di fuori degli orari decisi dal genitore, per ciascun giorno della settimana.

Software di controllo sono installati anche sui server web di alcune aziende dove la dirigenza ha riscontrato un eccessivo utilizzo delle reti sociali, durante l'orario di lavoro. Anche gli uffici pubblici dotati di PC a disposizione del pubblico utilizzano il software di controllo dei contenuti, per restringere le ricerche Internet alle sole funzioni di servizio. Ad esempio, presso molte biblioteche pubbliche è possibile cercare la biblioteca o la libreria che dispone di un certo titolo, ma non è possibile aprire *Facebook*.

Controllo genitoriale del PC (*Parental control*)

1. Da *Pannello di controllo*, seleziona *Controllo genitori*.
2. Scegli l'account che imposterà il controllo.
3. Selezionando l'account *Amministratore*, il programma chiede se vuoi creare un account specifico per il minore.
4. Digita il nome del minore e clicca sul tasto *Crea account*.
5. Nella scheda *Controlli utente* che si apre, puoi impostare una serie di restrizioni:
   - Orario di utilizzo del PC
   - Siti web
   - Materiale scaricato
   - Giochi
6. Inoltre, il programma può essere messo in grado di relazionare sulle specifiche attività svolte con il computer.
7. Imposta le restrizioni
8. Clicca sul pulsante *OK*.

▲ account per il Parental control



◀ Creazione account per minore

Esercizio 4.1.10 N.1

4.2 RETI SOCIALI

4.2.1

Comprendere l'importanza di non divulgare informazioni riservate su siti di reti sociali

Gli utilizzatori di reti sociali (*Facebook*, *Twitter*, *Google+*, ecc.) devono porre particolare attenzione nella divulgazione dei propri dati, immagini, riflessioni, perché, una volta messi in rete, questi elementi possono essere diffusi e di nuovo fatti circolare per anni, anche se sono stati immediatamente cancellati sul sito originale. Infatti, le reti sociali, con la tecnica della "condivisione", consentono una rapida divulgazione di qualsiasi elemento degno di nota, di curiosità o di scandalo, che sia stato posto in rete, anche per pochi attimi.

Recentemente si sono verificati in varie nazioni casi di politici che hanno visto rovinata una brillante carriera a causa di informazioni personali non proprio corrette, scioccamente affidate a *Facebook* o ad altre reti sociali.

4.2.2

Essere consapevoli della necessità di applicare impostazioni adeguate per la privacy del proprio account su una rete sociale

Quando si utilizza una rete sociale si possono avere due obiettivi:

- facilitare il lavoro di gruppo;
- giocare/passare del tempo.

Se l'obiettivo è quello di utilizzare i moderni mezzi di comunicazione di massa per rendere il lavoro più produttivo e anche più piacevole, allora ci si registra con il proprio nome e cognome, badando però a non fornire attraverso il proprio "profilo" più informazioni di quelle richieste per portare avanti con discrezione ed efficienza il lavoro di gruppo.

Le "cerchie" con le quali condividere immagini e documenti sono in genere riservate agli indirizzi di posta dei colleghi di lavoro. A nessuno verrebbe in mente di creare una "cerchia", ad esempio, di clienti o di fornitori.

Se invece l'obiettivo è quello di divertirsi e di vedere "cosa succede", allora è bene che chi frequenta la rete si registri con un nickname (pr. *nik-néim* = nome di fantasia) e di non dare, attraverso il proprio profilo, informazioni che possano far risalire alla propria identità. Questo specie nel caso in cui il profilo appartenga a una donna o a un minore. Particolare attenzione deve essere posta nella creazione delle "cerchie" di amici, di parenti e di conoscenti, per evitare la diffusione involontaria di immagini e di altro che, una volta diffuso, diventerebbe difficile eliminare.

Le reti sociali mettono a disposizione dei loro utenti una serie di restrizioni nella diffusione delle notizie e delle immagini.

Ad esempio, una delle più diffuse: *Facebook*, nella pagina *Impostazione della privacy e strumenti*, prevede tre argomenti:

- *Chi può vedere le mie cose?*
- *Chi può contattarmi?*
- *Chi può cercarmi?*

Per l'argomento "Chi può vedere le mie cose" è possibile scegli tra le opzioni:

- *Pubblica*
- *Amici, tranne conoscenti*
- *Solo io*

- *Personalizzata*
- *Amici più stretti*
- *Familiari*
- *Altre liste*

Solo l'opzione *Pubblica* prevede che "le mie cose" siano visualizzate da chiunque nella rete, senza alcuna restrizione.

4.2.3

Comprendere i rischi potenziali durante l'uso di siti di reti sociali, quali cyber bullismo, adescamento, informazioni fuorvianti/pericolose, false identità, link o messaggi fraudolenti

Come in tutti gli ambiti umani, anche "la Rete" è popolata da persone valide che è bello incontrare e personaggi poco raccomandabili, dai quali è meglio stare alla larga. Specie le donne e i minori devono frequentare la Rete con discrezione e interrompere i rapporti "virtuali" al primo sospetto di poca limpidezza. Infatti, la Rete è purtroppo mezzo di diffusione anche di atteggiamenti persecutori:

- Cyber bullismo. Cyber (pr. *sàiber*) è lo spazio virtuale messo a disposizione da Internet. Alcuni individui, forti anche del fatto che non possono essere facilmente individuati, si divertono a perseguitare altre persone attraverso email, SMS, post su reti sociali, ecc. (bullismo).
- Adescamento. L'adescamento (detto anche *grooming*, pr. *grùming*) è il mezzo attraverso il quale un frequentatore poco serio della rete induce una persona psicologicamente debole ad accettare un incontro fisico.
- Falsa identità. Falsa identità è quella che alcuni individui, poco raccomandabili, si costruiscono fingendo di essere una donna o un coetaneo per attirare ad un incontro fisico la propria vittima "conosciuta" in rete.
- Informazioni, link, messaggi fraudolenti. Nei punti 1.3.2 e 4.1.3 sono state illustrate le truffe messe in atto attraverso la rete, che vanno sotto il nome di *phishing* (prendere qualcuno all'amo come un pesce) e *pharming* (utilizzare in maniera illegale logo, sito e immagine di un'azienda), per trarre in inganno lo sprovveduto frequentatore di una rete sociale.

Sezione 5 Comunicazioni

5.1 POSTA ELETTRONICA

5.1.1
Comprendere lo scopo di cifrare, decifrare un messaggio di posta elettronica

I messaggi di posta elettronica, se usati per scopi professionali, pos sono contenere informazioni molto riservate. Ad esempio, una person che si trova in un ufficio periferico, trasmette al suo capo la copia un'offerta economica del valore di qualche migliaio di Euro. L'offer serve per partecipare ad una gara d'appalto. Una "spia informatica potrebbe intercettare il messaggio e "passarlo" ad un'azienda concor rente che, se poco corretta, ne potrebbe approfittare per produrre un'of ferta simile ma con prezzo più vantaggioso, aggiudicandosi la gara.

Per evitare queste disastrose eventualità, i messaggi commercia viaggiano in rete "criptati" cioè scritti con una "chiave pubblica" nota tutti e quindi rileggibili solo attraverso la corrispondente "chiave privata" in possesso esclusivo del destinatario del messaggio.

5.1.2
Comprendere il termine firma digitale

La firma digitale, detta anche firma elettronica, è basata sull sicurezza detta a "chiavi asimmetriche". Si tratta di due elementi dif "chiave", uno pubblico e cioè accessibile a tutti e uno, corrispondente privato, conservato dal solo proprietario della coppia di chiavi. Il princip della sicurezza a "chiavi asimmetriche" è il seguente: un messaggio testo se viene crittografato, ossia reso illeggibile, con la chiave privata può essere decrittografato, e cioè reso leggibile, solo utilizzando la chia ve pubblica corrispondente. Nella stessa maniera, un messaggio testo crittografato con la chiave pubblica può essere decrittografato sol con la chiave privata corrispondente.

In questa maniera un messaggio che può essere reso leggibile co la chiave pubblica di una determinata persona, azienda o ente, attest in maniera assoluta l'identità di chi ha inviato il messaggio stesso.

Osserva il caso di una gara di vendita all'asta alla quale si può parte cipare con un messaggio email certificato:

1. Più persone concorrenti inviano il proprio messaggio con l'offert d'acquisto di un certo prodotto messo all'asta. I messaggi devon includere la "firma digitale".
2. I concorrenti inviano la propria offerta firmata con la chiave privata
3. L'ente che ha indetto la gara legge le offerte con le rispettive chia pubbliche, ottenute dall'apposito sito che le custodisce.
4. La persona che ha proposto il prezzo più alto si aggiudica la gara.

In questo caso la "firma digitale" è costituita dal fatto che chi rice il messaggio con l'offerta lo può rileggere solo con la corrispondent "chiave pubblica" dell'offerente il quale non potrà mai negare di ave inviato l'offerta criptata con la sua "chiave privata".

5.1.3
Creare e aggiungere una firma digitale

La creazione di una firma digitale consiste nella procedura che gener una coppia di chiavi, una pubblica che deve essere a disposizione tutti ed una corrispondente privata che deve essere conservata gelosa mente dal titolare. È un'operazione che occorre fare una sola volta

La firma ha una scadenza temporale stabilita e, una volta generata, bisogna conservare con cura la "chiave privata" con la quale verranno firmati i messaggi. Occorre conservare con cura anche la "frase" usata nella procedura. Questa potrebbe servire, ad esempio, per annullare in qualsiasi momento la firma digitale generata.

La firma digitale va abbinata al programma di posta in uso, utilizzando un'apposita estensione che varia, a seconda del programma di posta e della procedura utilizzata per la generazione delle chiavi.

Nell'esercizio relativo a questo punto del Syllabus, è stato tenuto presente che la coppia di chiavi verrà generata con il programma *PGP* (Pretty Good Privacy = Buona riservatezza) il programma di posta è *Gmail* e l'estensione di PGP per *Gmail* è *WebPG*.

PGP Corporation

La PGP Corporation E L'Attuale Proprietaria del codice del software Pretty Good Privacy, sviluppato originariamente da Phil Zimmermann. La PGP Corporation Acquisto il codice El CD Diritti del nomo Dalla Network Associates Nel 2002. Wikipedia

Fondatore : Jon Callas

Anno di fondazione : 2002

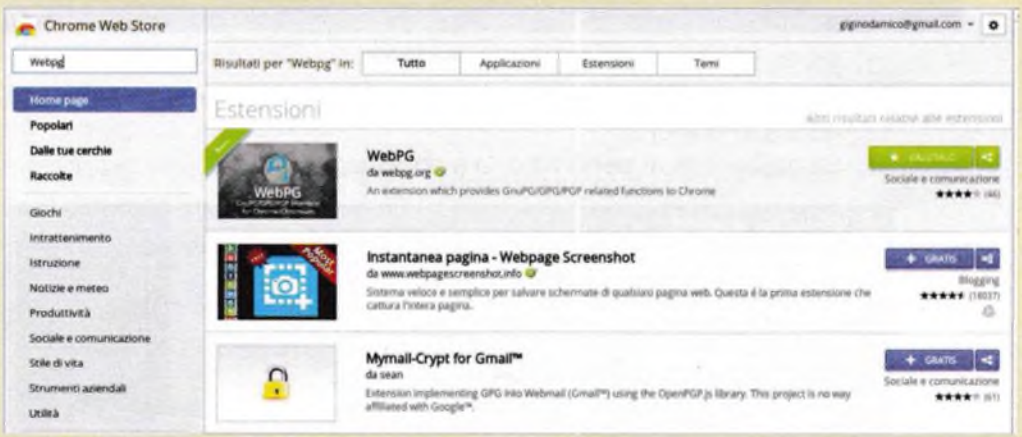
▲ PGP Corporation

Esercizio 5.1.3 N.1

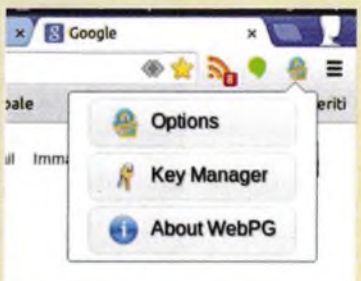
Creare una coppia di chiavi asimmetriche per alcuni utenti, usando l'estensione *WebPG* per *Gmail*

1. Apri *Gmail* con l'account per il quale vuoi generare la firma elettronica.
2. Clicca, in alto a destra, sul pulsante *Personalizza e controlla Google Chrome*.
3. Seleziona la voce *Strumenti*.
4. Nel riquadro Strumenti, seleziona la voce *Estensioni*.
5. Individua, attraverso "Prova altre estensioni" l'estensione *WebPG* ed abilitala.

▼ *WebPG*



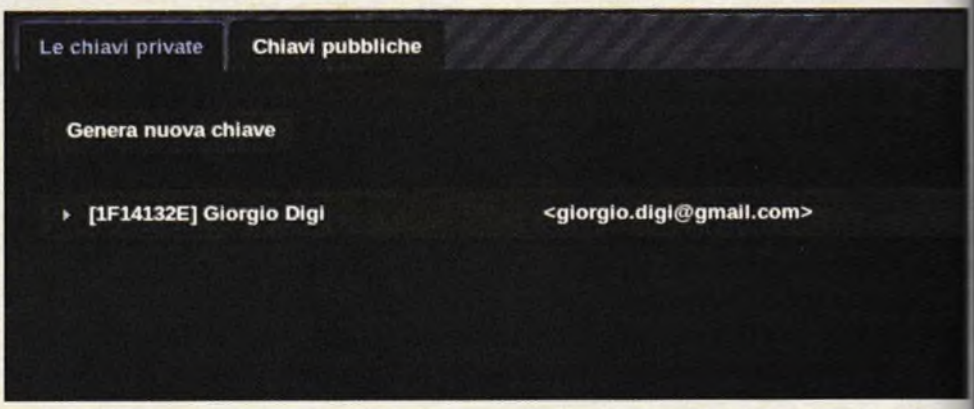
6. A questo punto, in alto a destra della pagina *Gmail* appare l'icona della firma digitale. Cliccando sull'icona appaiono le operazioni di inizializzazione.
7. Seleziona il pulsante *Key Manager*.



Icona *WebPG* ▶

8. Clicca sul tasto *Genera nuova chiave*.

Key Manager *WebPG*

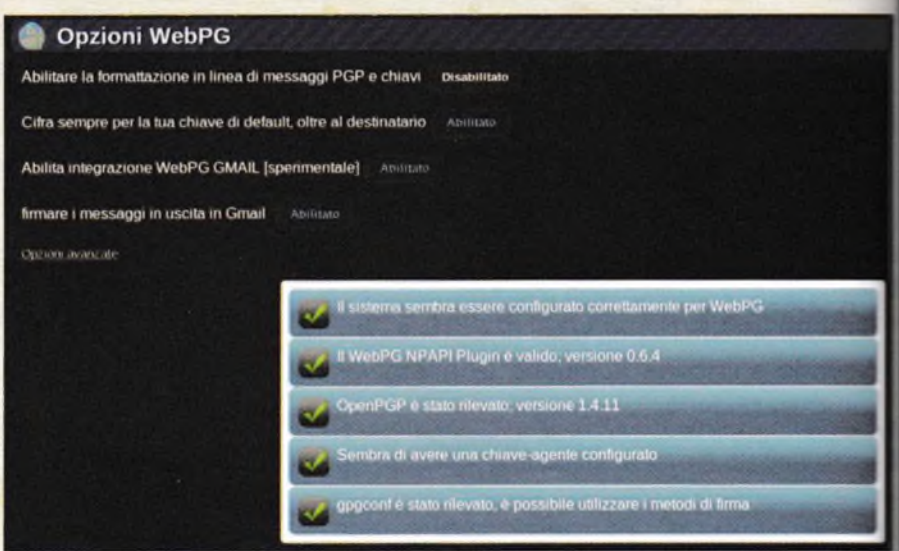


9. Inserisci nei campi i dettagli del nuovo account.
10. Conserva in un luogo nascosto la passphrase utilizzata.

Generazione chiave *WebPG*

11. Torna al menu principale.
12. Clicca sul pulsante *Options*.
13. Abilita le opzioni.
14. La procedura di generazione è conclusa.

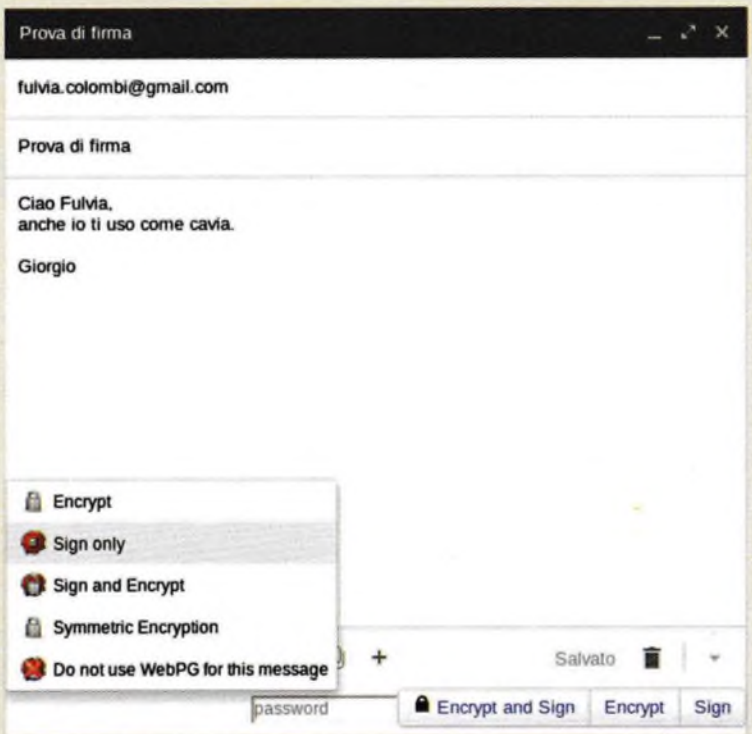
Opzioni *WebPG*



Esercizio 5.1.3 N.2

Inviare un messaggio di posta con firma digitale

1. Assicurati che tra le estensioni di *Google*, sia installato *WebPG*.
2. Invia al tuo amico un messaggio con firma digitale, usando *Gmail*.
3. Attiva l'opzione di sola firma (*Sign only*), in basso a sinistra.
4. Clicca sul tasto *Invia*.



Prova di firma con *WebPG*

5. Il tuo amico riceve il messaggio con la firma.

Messaggio firmato

Chiavi pubbliche

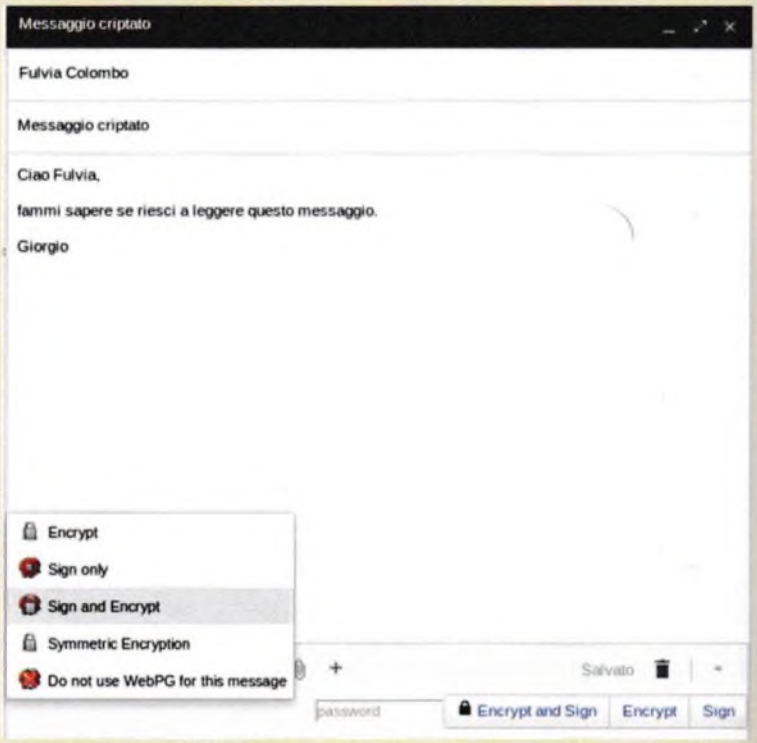
6. Cliccando sul pulsante *WebPG*, in alto a destra, è possibile esaminare l'elenco delle chiavi pubbliche dei corrispondenti.

Esercizio 5.1.3 N.3

Usare *Gmail* per inviare un messaggio di posta criptato e con firma digitale

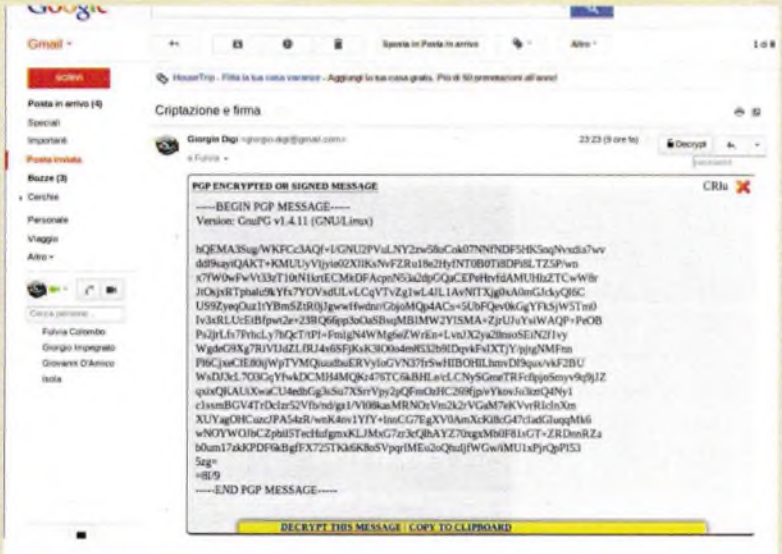
1. Apri *Gmail*.
2. Controlla che siano attive le estensioni *WebPG* (pulsante *Personalizza e controlla Google Chrome* > *Strumenti* > *Estensioni*).
3. Scrivi un messaggio da criptare.
4. Invia il messaggio al tuo amico, indicando (in basso a sinistra) l'opzione *Firma e Codifica* (*Sign and Encrypt*).
5. Il programma di posta invia il messaggio criptato.

Invio di un messaggio criptato



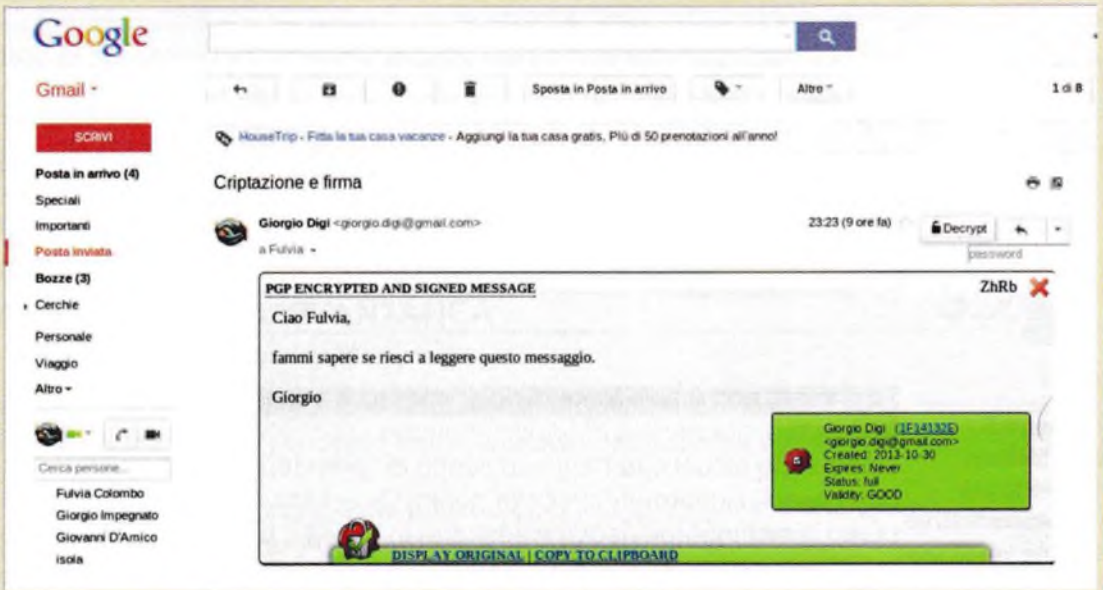
6. Il tuo amico riceve il messaggio criptato.

Ricezione di un messaggio criptato



7. Il tuo amico clicca sul pulsante *Decrypt this message*, in basso alla finestra.
8. Il programma di posta decifra il messaggio.
9. Appare il messaggio in chiaro.

▼ Decifrazione di un messaggio



Come inviare in rete un documento *Office 2010*, con firma digitale

1. Apri il documento da firmare.
2. Menu *File > Informazioni > Proteggi documento.*
3. Dalla finestra pop-up, seleziona *Aggiungi firma digitale.*
4. Seleziona l'opzione *Creare un proprio ID digitale* nella finestra di dialogo *Ottenere un ID digitale* e confermare con il pulsante *OK.*
5. Compila i campi della finestra di dialogo *Crea ID digitale* e conferma con il pulsante *Crea.*
6. Compila il riquadro nel quale si richiede lo scopo della firma e termina con il pulsante *Firma.*

Esercizio 5.1.3 N.4

5.1.4 Essere consapevoli della possibilità di ricevere messaggi fraudolenti e non richiesti

Quando si possiede una casella di posta elettronica (account di posta) si può essere bersagliati da numerosi annunci pubblicitari di qualsiasi tipo, non esclusi messaggi fraudolenti che, ad esempio, richiedono di digitare la propria password. Nessuno può impedire ai disturbatori di inviare i loro messaggi. Certo però, si può fare qualcosa per non essere vittime indifese.

Una prima linea di difesa è presso gli ISP, Internet Service Provider = Fornitore di servizi Internet. Gli ISP, insieme al servizio di posta gratuito, forniscono servizi aggiuntivi a pagamento, come appunto, l'antispam. Si tratta di programmi che utilizzano un sistema di riconoscimento e isolamento dello stesso messaggio, inviato ad una gran massa di utenti. In questo modo i messaggi indesiderati vengono bloccati, a livello del Server, prima dell'arrivo alla casella di posta.

Un'altra linea di difesa è presso l'utente. Chi utilizza un programm di posta può configurarlo per decidere all'arrivo quali messaggi n gradisce che gli vengano proposti. Si tratta di filtri in base ai quali, esempio, tutti i messaggi che hanno come mittente un certo indirizz o come oggetto un certo argomento, vanno a finire direttamente n cestino.

più

La massa dei messaggi non desiderati viene definita spam, in ricordo di una marca di carne in scatola americana i cui messaggi pubblicitari in TV erano così assillanti da rimanere per anni nella memoria dei poveri spettatori. Da spam è derivato "spammare", orribile parola che significa "riempire le caselle di posta con messaggi spazzatura".

5.1.5

Comprendere il termine phishing. Identificare le più comuni caratteristiche del phishing, quali uso del nome di aziende e persone autentiche, collegamenti a falsi siti web

Lo spam non è solo fonte di noia, spesso è anche origine di proble Infatti, nella massa dei messaggi che si ricevono quotidianament ce ne sono alcuni che hanno lo scopo di "prendere all'amo" come si con i pesci, l'ignaro utente della posta. Quest'attività viene definita a punto "phishing" (pr. *fiscin*) = pescare, in inglese. L'attività è ormai no a tutti: vengono spediti messaggi che simulano quelli dei siti banca delle assicurazioni, dell'INPS, delle Poste Italiane, ecc., nei quali chiede di inviare il numero del conto corrente bancario, il PIN de carta di credito, le password di qualsiasi tipo ed altro, con il pretesto "controllare" o di "risolvere" particolari situazioni. Nonostante conoscenza dell'imbroglio, ancora oggi qualche persona particola mente indifesa cade nella trappola.

Dello stesso tenore sono i messaggi che possono apparire quan si sta cercando in rete il sito di una certa azienda o le informazioni un professionista e che ci invitano a cliccare su un certo link, con pretesto che il sito è stato "spostato". Cliccando sul link proposto, l tente finisce a contatto con un server che cerca di carpirgli informazio riservate o che gli dà lo stimolo per acquistare merci e servizi, simi quelli per i quali stava effettuando la ricerca in rete.

5.1.6

Essere consapevoli del rischio di infettare il computer con malware attraverso l'apertura di un allegato contenente una macro o un file eseguibile

I computer sono spesso oggetto di attacchi da parte di agenti este che cercano di penetrare nella rete alla quale il computer è collega o nelle memorie del computer stesso. Per raggiungere il loro scopo, agenti esterni (spie informatiche), utilizzano del software "maligno" c nominato appunto "malware". Due tipi di file si prestano particolarmen ad essere manipolati per diventare "malware":

- allegati di posta;
- file eseguibili.

Gli allegati di posta possono contenere delle macro, cioè de istruzioni che si ripetono in maniera ciclica, cosa che aiuta molto c con questo mezzo, tenta e ritenta un'infinità di volte, incrementando m gari un numero o la posizione di una lettera all'interno di una parola, scoprire come sono confezionati una password o un PIN.

È bene quindi non aprire mai allegati di posta che non siano conosciuti, cioè allegati ad un messaggio spedito da una persona sicura, con le giuste motivazioni. Anche in questo caso è sempre bene eseguire una scansione dell'allegato con il programma antivirus, prima di procedere ad aprirlo.

I file eseguibili contengono programmi che una volta installati nel disco di un computer, possono essere eseguiti automaticamente, con esiti non prevedibili se l'origine del programma è sconosciuta.

Generalmente i programmi di posta non accettano per principio che un file eseguibile venga allegato ad un messaggio. Occorre comunque evitare di aprire file che terminano con *.bat* o con *.exe* (Ambiente *Windows*).

MESSAGGISTICA ISTANTANEA 5.2

5.2.1

Comprendere il termine messaggistica istantanea (IM) e i suoi usi

Al pari del servizio di posta elettronica (email), il servizio di messaggistica istantanea consente di trasmettere messaggi tra più utenti della rete.

Mentre però i messaggi della posta elettronica rimangono a disposizione del destinatario fin quando questo non li prende in considerazione (il servizio è quindi asincrono), il servizio di messaggistica istantanea (o Instant Messaging, pr. come è scritto) si basa sul principio che almeno due corrispondenti siano in rete nello stesso momento. Il servizio di messaggistica è infatti un servizio sincrono. A differenza del servizio email, il servizio di messaggistica istantanea è associato alla messaggistica in audio (i corrispondenti si parlano usando microfoni e altoparlanti) e in video (viene utilizzata anche la webcam), grazie alla tecnologia VoIP (Voice over Internet Protocol). Anche questo servizio consente il trasferimento di file.

5.2.2

Comprendere le vulnerabilità di sicurezza della messaggistica istantanea, quali malware, accesso da backdoor, accesso a file

I computer sono, sotto il profilo dei rischi che vengono dall'esterno, raffigurabili come delle case con una porta anteriore attraverso la quale lavora l'utente e tante porte posteriori, ognuna dedicata ad un servizio di ingresso/uscita verso la rete. Queste porte sono fatte per rimanere aperte solo per la durata del servizio specifico. I casi più rischiosi, in fatto di infezione da malware, sono quelli che riguardano il collegamento in rete prolungato. Ad esempio, quando si utilizza la messaggistica istantanea, si sta al computer per molto tempo e il collegamento a Internet prolungato consente a chi vuole introdursi furtivamente da una porta posteriore (spesso si tratta di programmi che girano in rete alla ricerca di "porte aperte") di farlo con più certezza di riuscita. Questi malware vanno sotto la voce di backdoor (pr. *bèk-door*) che, in inglese, significa appunto: porta posteriore.

5.2.3

Riconoscere metodi per assicurare la confidenzialità durante l'uso della messaggistica istantanea, quali cifratura, non divulgazione di informazioni importanti, limitazione di condivisione di file

Come detto nel punto 5.2.2, la messaggistica istantanea prevede lungo periodo durante il quale una "porta posteriore" del comp rimane aperta. Occorre essere consapevoli del fatto che in tutto que tempo possiamo essere spiati e quello che viene detto durante la c versazione può essere usato illegalmente o contro noi stessi. Occ quindi adottare delle misure che hanno lo scopo di ridurre il rischio c si corre:

- i messaggi scritti che vengono scambiati vanno "cifrati" se son particolare importanza;
- non discutere di cose che sono particolarmente rilevanti per l'azie o per una persona, se non strettamente richieste dal caso;
- ridurre allo stretto necessario la condivisione di file e provvede cancellarli, una volta terminato il lavoro in comune.

Gestione sicura dei dati

Sezione 6

MESSA IN SICUREZZA E SALVATAGGIO DI DATI 6.1

6.1.1

Riconoscere modi per assicurare la sicurezza fisica di dispositivi, quali registrare la collocazione e i dettagli degli apparati, usare cavi di sicurezza, controllare gli accessi

La sicurezza fisica dei dispositivi informatici (computer, periferiche, apparecchiature di rete, memorie di massa, ma anche tablet, smartphone, ecc.) è particolarmente importante non tanto per il valore economico dell'hardware, quanto per il valore del software installato e, ancora di più, per i dati aziendali che vi sono depositati. Riguardo all'apparecchiatura più piccola: lo smartphone, si pensi al danno che ne avrebbe una persona, in caso di smarrimento, se il malcapitato non avesse provveduto in tempo ad effettuare una copia della rubrica *Contatti*.

Non esiste un metodo certo per evitare che un'apparecchiatura venga danneggiata, sottratta o smarrita. Esistono delle precauzioni che però limitano i casi più gravi:

- Le apparecchiature elettroniche aziendali (tranne quelle personali) vanno installate in un unico locale soggetto a sorveglianza e con accesso strettamente limitato agli operatori. Nel caso di grandi aziende, come gruppi industriali, compagnie telefoniche, stazioni televisive, gruppi della grande distribuzione, istituti bancari e assicurativi, ospedali, ecc., normalmente esistono due siti distanti tra loro nei quali sono duplicate almeno le apparecchiature essenziali (unità centrali, unità di memorizzazione di massa), per rispondere ai casi più gravi di non più disponibilità delle stesse (vedi punto 1.1.4).
- Le apparecchiature presenti negli uffici (PC, stampanti, ecc.) vanno inventariate e controllate annualmente.
- Le apparecchiature installate in luoghi frequentati dal pubblico e non sufficientemente sorvegliati dal personale addetto, vanno bloccate al banco (consolle, tavolo, altro) dove sono in mostra, utilizzando l'opportuno cavo di sicurezza che, nel caso dei PC portatili, termina con un lucchetto che si blocca nel guscio del PC stesso.

▲ Cavo di sicurezza

6.1.2

Riconoscere l'importanza di avere una procedura di copie di sicurezza per ovviare alla perdita di dati, di informazioni finanziarie, di segnalibri/cronologia web

Mentre l'operazione di backup programmato viene effettuata in maniera professionale dal personale aziendale addetto, in modo da poter rispondere a qualsiasi richiesta di ripristino di dati persi, è ad esclusiva discrezione del singolo utilizzatore del PC effettuare copie di quanto riguarda la propria attività e che può andare smarrito o deteriorato, in modo da essere sempre pronto a ripartire con il lavoro, in maniera autonoma e professionale. Nella stessa maniera dovrebbe operare un utilizzatore casalingo del PC se questo non gli serve solo per "navigare" in Internet. Le copie di sicurezza (backup) più o meno periodiche riguardano, in genere:

- Dati finanziari frutto di elaborazioni proprie.
- Risultati di ricerche e progettazioni, anche temporanee.

Inoltre, sul browser utilizzato, va attivata l'opzione per la conservazione di *Segnalibri* e *Cronologia*, in modo da poter risalire con immediatezza ai siti già frequentati, dove si trovano le informazioni necessarie al lavoro in corso.

6.1.3

Identificare le caratteristiche di una procedura di copie di sicurezza, quali regolarità/frequenza, pianificazione, collocazione della memoria di massa

Nelle aziende, le copie di sicurezza dei dati sono organizzate in una procedura detta backup programmato. L'aggettivo "programmato" sottolinea l'importanza del fatto che le copie dei dati devono essere effettuate a precisi intervalli di tempo: in genere, ad ogni giorno lavorativo.

Tutte le grandi organizzazioni che sono soggette all'obbligo di legge della conservazione per lunghi periodi (cinque - dieci anni) dei dati trattati, ad esempio: banche, assicurazioni, ospedali, compagnie telefoniche, adottano per la procedura di backup i supporti a nastro magnetico. Le caratteristiche di questi supporti che li rendono idonei ai backup programmati, sono la compattezza, la velocità di scrittura, la capacità che negli ultimi modelli (DAT 4) arriva a 4 GB, la possibilità di riuso, il basso costo. Inoltre, quello che può sembrare un punto di debolezza delle "cassette" e cioè l'essere rimaste uguali da tanti anni, è invece il loro punto di forza, tenendo conto del fatto che solo una tecnologia stabile nel tempo può garantire il riuso di dati registrati cinque o dieci anni prima.

Le cartucce datate e numerate vanno conservate in un apposito contenitore ignifugo (protetto cioè contro il fuoco) che va depositato in un locale sufficientemente distante dal luogo dove è installato il computer in modo da non essere coinvolto dagli stessi probabili eventi negativi.

La moderna tendenza per le aziende che non hanno vincoli di conservazione dei dati a lunga scadenza è quella di utilizzare per il backup dischi in rete di grande capacità oppure di ricorrere al backup programmato presso gli appositi Service Provider che offrono il servizio di conservazione dei dati in rete (*storage network*).

I piccoli utenti e gli utilizzatori del PC domestico si affidano al programma di backup che ormai è presente in tutti i sistemi operativi per PC e utilizzano come supporto dati un DVD o un disco esterno USB. I sistemi operativi più moderni, pur lasciando la possibilità di utilizzare i DVD, consigliano l'uso di memorie di massa USB o l'archiviazione online. Un esempio appropriato alla piccola utenza è l'offerta di servizio di archiviazione online *MYPC backup* proposta da Norton *Secured.*

▼ **Backup in linea di *Norton Secured***

più

L'operazione di backup nelle aziende avviene quotidianamente, prima dell'orario di lavoro. L'attività è gestita da un software che identifica i file che sono stati creati o modificati dall'ultima operazione di backup e li invia ad un dispositivo che contiene una serie di cartucce per la registrazione. Questo significa che vengono copiati solo i nuovi dati. Quelli precedenti sono contenuti in una serie di cartucce, ciascuna identificata con la sua data di backup e un numero progressivo. La procedura calcola quante serie di salvataggi occorre conservare per disporre di tutti i dati che possono essere ricaricati, in caso o di richiesta di un singolo dipendente, o in caso di disastro totale.

▲ Cartuccia magnetica

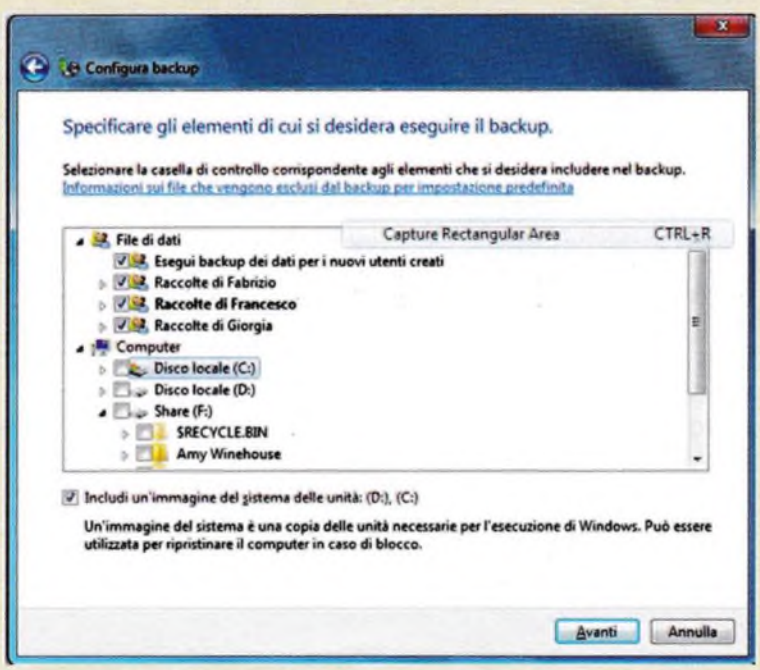
6.1.4 Effettuare la copia di sicurezza di dati

I file dati frutto di elaborazioni locali, vanno salvati con regolarità perché, una volta persi, non possono essere recuperati e occorre ripercorrere tutto il processo di elaborazione per ottenerne dei nuovi. Talvolta anche questo è impossibile perché magari i dati sono frutto dell'elaborazione di un evento irripetibile. Data l'importanza dell'operazione, tutti i sistemi operativi dispongono di un programma di backup (salvataggio) dei dati.

La versione *7* di *Windows* prevede il salvataggio in rete.

Eseguire il backup di un'unità disco *Windows 7*

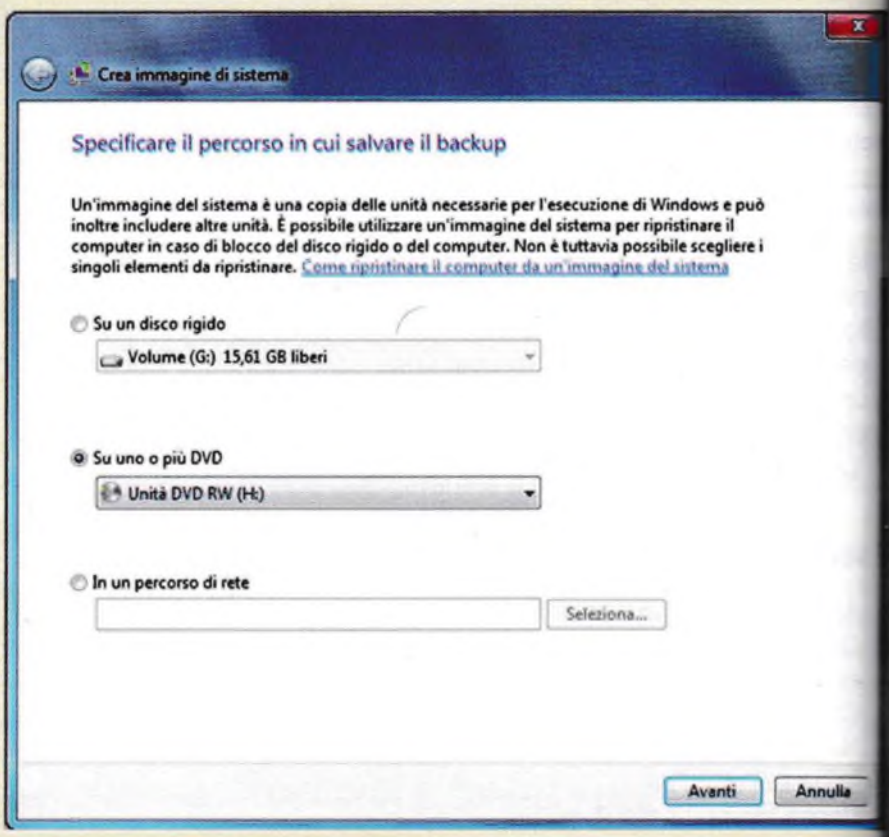
1. Apri il *Pannello di controllo*.
2. Clicca su *Tutti gli elementi del Pannello di controllo* > *backup e ripristino*.
3. Clicca su *Configura backup*.
4. Nella finestra "Configura backup" che si apre, seleziona l'unità di origine.
5. Clicca sul pulsante *Avanti*.
6. Scegli l'opzione *Manuale* e clicca sul pulsante *Avanti*.
7. Seleziona il disco "C:" e clicca sul pulsante *Avanti*.



◀ Scelta origine backup con *Windows 7*

Esercizio 6.1.4 N.1

8. Scegli l'unità di destinazione (unità DVD). Clicca sul pulsante *Avanti*.
9. Nella finestra di riepilogo che si apre, clicca sul pulsante *Salva impostazioni ed esegui il backup*.
10. Termina con il pulsante *Avanti*.



Scelta destinazione backup con *Windows 7*

11. Scegli l'opzione *Manuale* e clicca sul pulsante *Avanti*.
12. Seleziona il disco "C:" e clicca sul pulsante *Avanti*.
13. Nella finestra di riepilogo che si apre, clicca sul pulsante *Salva impostazioni ed esegui il backup*.
14. Termina con il pulsante *Avanti*.

Windows 8

Windows 8 dispone del programma di backup *Cronologia file*, che, oltre alle normali operazioni di backup/ripristino, s'incarica anche di salvare ad intervalli di tempo programmabili, i file sui quali si sta lavorando. Il programma è inoltre in grado di tentare il ripristino di file che risultano cancellati, danneggiati o persi.

Per quanto riguarda le operazioni di backup prestabilite, esse riguardano unicamente le cartelle di lavoro standard:

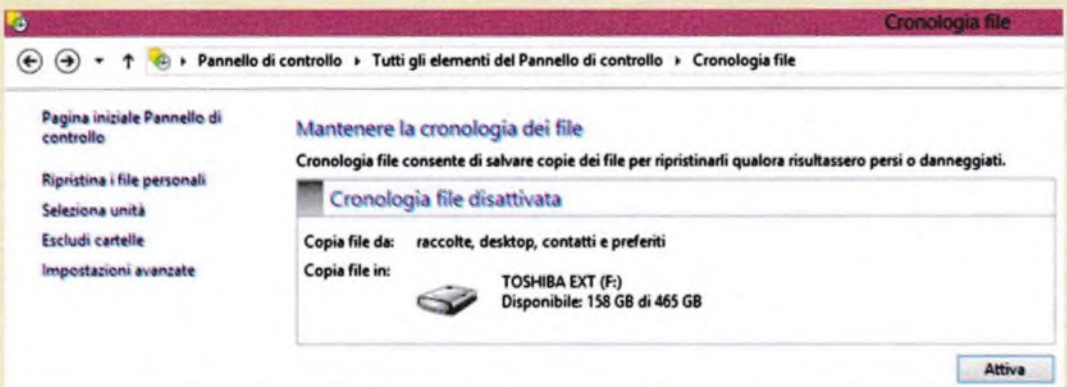
- *Documenti*
- *Musica*
- *Immagini*
- *Video*
- *Desktop*

Una o più di queste cartelle possono essere escluse dal salvataggio, attraverso il tasto *Escludi cartelle.* Altre cartelle possono invece essere aggiunte, in base alle necessità.
Prima di eseguire il backup, occorre definire l'unità di destinazione dei file. Benché il programma consenta qualsiasi possibilità, le unità consigliate sono le unità di massa USB e le unità di storage online.

Esercizio 6.1.4 N.2

Definire un disco USB, o un'unità online, come unità di backup, con il programma *Cronologia file* di *Windows 8*

Quando si collega un'unità esterna, il sistema operativo chiede cosa se ne vuol fare. È possibile, scegliendo l'opzione *Configura quest'unità …*, definire subito l'unità che conterrà i dati di backup.



▲ Configura unità di backup con *Windows 8*

1. Apri il programma *Cronologia file* da *Pannello di controllo.*
2. Scegli *Seleziona unità.*
3. Se l'unità di destinazione è un'unità in rete e non risulta nell'elenco, utilizza il tasto *Aggiunta guidata risorse di rete.*
4. Se premi il tasto *Avvia*, parte immediatamente il salvataggio di tutte le cartelle verso l'unità di backup. Anche per velocizzare l'operazione, puoi escludere le cartelle che ritieni non importanti per l'operazione di backup.
5. Usa il link *Escludi cartelle*, in alto al centro.
6. Seleziona le cartelle da escludere e termina con il pulsante *Salva modifiche.*
7. Si ritorna alla pagina iniziale. Inizia il salvataggio con il pulsante *Attiva.*

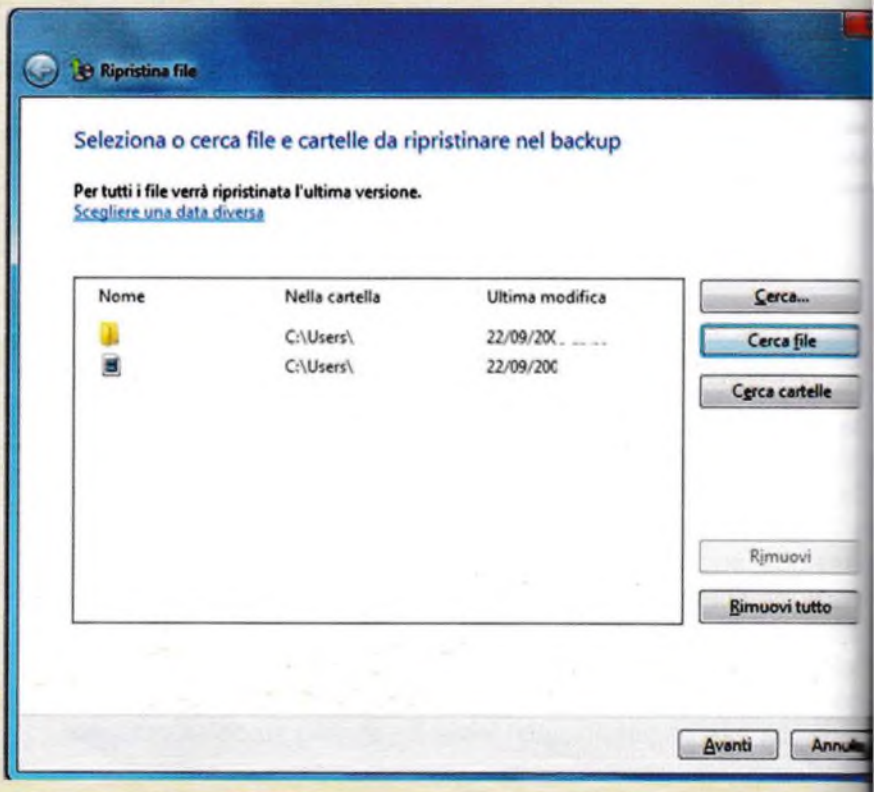
6.1.5
Ripristinare e validare i dati sottoposti a copia di sicurezza

L'operazione di ripristino può essere effettuata per ottenere di nu disponibili file e cartelle che per qualche motivo potrebbero ess andati persi.

Esercizio 6.1.5 N.1

Eseguire il ripristino del disco C: *Windows 7*

1. *Pannello di controllo > Backup e ripristino.*
2. Clicca sul pulsante *Ripristina file personali.* A destra nella fine che si apre, sono disponibili i pulsanti:
   - *Cerca*: ricerca un singolo file, attraverso il motore di ricerca.
   - *Cerca file*: consente di individuare i file da ripristinare, cercan tra le cartelle.
   - *Cerca cartelle*: consente di ripristinare intere cartelle di file.
3. Clicca sul pulsante *Avanti.*
4. Seleziona la destinazione del ripristino.
5. Termina con il pulsante *Avanti.*



Ripristino backup con *Windows 7*

Ripristinare i dati con *Cronologia file* di *Windows 8*

1. Apri il programma *Cronologia file* da *Pannello di controllo.*
2. Scegli *Ripristina i file personali.*
3. Seleziona i dati da ripristinare.
4. Termina con il pulsante *Attiva.*

DISTRUZIONE SICURA

Comprendere il motivo per eliminare in modo permanente i dati dalle memorie di massa o dai dispositivi

Se un dispositivo elettronico che contiene una memoria di massa costituita da un disco magnetico si guasta in maniera irreparabile o diventa non più utilizzabile, prima di smaltirlo come rifiuto, occorre, se possibile, formattare le memorie di massa eliminando qualsiasi dato aziendale o personale e qualsiasi programma commerciale. Questo perché i dati aziendali e personali potrebbero essere recuperati successivamente dalla solita "spia digitale" (vedi *trashing* al punto 1.3.2) e i programmi commerciali potrebbero essere riusati, commettendo una violazione al contratto di vendita (EULA= *End User License Agreement* pr. *end iùser làisens egrìment*) che lega il pacchetto software al soggetto che l'ha acquistato.

6.2.2

Distinguere tra cancellare i dati e distruggerli in modo permanente

Quando le aziende rinnovano i computer, tendono a donare a organizzazioni caritatevoli le apparecchiature funzionanti che sostituiscono. Prima di regalare l'hardware, cosa legalmente fattibile, anzi encomiabile, occorre eliminare dal disco fisso tutto il contenuto:

- sistema operativo proprietario;
- software d'ufficio proprietario;
- dati personali: vanno assolutamente eliminati.

Cosa s'intende per eliminare i dati? Non certo "cancellarli" o "spostarli nel cestino". Quasi sempre i dati registrati nel disco fisso, anche dopo aver "svuotato il cestino" possono essere recuperati, usando opportuni software ben conosciuti dalla "spia informatica".

Cosa fare allora? Un sistema è la "formattazione" completa del disco. La formattazione non cancella i dati: li distrugge, rendendoli irrecuperabili. Un sistema migliore è la riscrittura del disco eseguita più volte, attraverso particolari programmi di cancellazione.

più

Quando un computer diventa "sorpassato" si ha la tendenza a regalarlo ad un amico che ce lo chiede o ad un'organizzazione caritatevole. In genere questa non è una buona idea. Se l'organizzazione caritatevole non dispone al suo interno di una persona capace e se l'amico al quale abbiamo fatto il regalo non ha la giusta conoscenza e manualità il dono diventa una fonte di continue richieste di aiuto, anche perché spesso chi riceve il computer vorrebbe utilizzarlo per le stesse applicazioni che l'hanno reso "sorpassato" presso il proprietario originale. Inoltre bisogna ricordare che mentre l'hardware del PC è di nostra proprietà, il sistema operativo *Windows* e i programmi annessi (*Microsoft Office*) ci sono stati dati "in licenza", abbiamo cioè acquistato solo il loro uso. In teoria potremmo regalarli insieme al computer ma solo se corredati con le licenze cartacee originali, insieme ad un regolare contratto di vendita. La cosa migliore è regalare solo l'hardware, ma a cosa servirebbe?

Esiste una soluzione. Prima di regalare il PC, dopo aver "formattato il disco fisso" possiamo installare il software libero (libero dai legami EULA). Si tratta di software sviluppato e costantemente aggiornato da migliaia di volontari esperti nella programmazione. Questo software può essere liberamente installato, usato e perfino modificato. Non può essere rivenduto, solo regalato. Se s'incontrano dei "buchi", ossia dei difetti, ci si mette in contatto con i progettisti (il loro nome e indirizzo è sempre presente) e si comunica quanto riscontrato, in modo che alla prossima revisione il difetto sia corretto. Carichiamo e doniamo liberamente:

Sistema operativo: *Linux* (io uso con soddisfazione *Linux Ubuntu*).

Software d'ufficio: *Open Office* o *LibreOffice* (per gli usi domestici sostanzialmente uguali a *Microsoft Office* fino alla versione precedente all'introduzione della *barra multifunzione*).

Un'infinità di programmi liberi immediatamente installabili e usabili.

Se si pensa che quasi sempre i computer ricevuti in dono servono solo per "navigare" in Internet e per la posta elettronica, quale sia il sistema operativo installato, non interessa più di tanto. L'utilizzatore si limiterà a cliccare sull'icona di *Google Chrome* o di *Firefox* per raggiungere *Google*. Il fatto poi che *Google Chrome* abbia al suo interno anche il programma di videoscrittura e il foglio elettronico, completa brillantemente il quadro.

Qualche altra buona notizia: il sistema operativo *Linux* è estremamente elastico, deriva dal sistema operativo *UNIX* che gira sui grandi calcolatori (*mainframe*, pr. *mèin frèim*). Accetta i file prodotti con *Microsoft Office*, e può produrne con lo stesso formato, dialoga immediatamente con un numero incredibile di unità periferiche, molte delle quali sono rifiutate dal sistema operativo *Windows*. Inoltre *Linux* può coabitare egregiamente nello stesso computer, senza disturbare *Windows*.

6.2.3

Identificare i metodi più comuni per distruggere i dati in modo permanente, quali uso di trita documenti, distruzione di memorie di massa/dispositivi, smagnetizzazione, uso di utilità per la cancellazione definitiva dei dati

Quella della distruzione dei dati non più utili è un compito importante all'interno delle aziende, perché ha riflessi economici ed anche legali. Inoltre, il responsabile della sicurezza ha un autentico terrore della "spia informatica", sempre pronta a rovistare nel cassonetto dei rifiuti, pur di carpire segreti da rivendere.

Allo scopo vengono adottati diversi provvedimenti:

- I documenti cartacei, prima di essere gettati, vengono ridotti in striscioline o in coriandoli, facendoli passare dentro apparecchiature "distruggi documenti".
- Le memorie magnetiche vengono rese inservibili attraverso apparecchiature elettriche che generano un potente campo magnetico (*Degausser*) o vengono "martellate", dopo essere state estratte dall'involucro che le protegge.
- I CD e i DVD al corredo delle apparecchiature non più utilizzabili sono resi inservibili deformandoli meccanicamente.