Sicurezza informatica

Programma analitico d'esame per il conseguimento della certificazione informatica per l'utente intermedio in linea con le indicazioni del CEN (Ente di standardizzazione Europeo) - eCF (e-Competence Framework)

Premessa

Questo modulo introduce le regole e le buone prassi che consentono di minimizzare la vulnerabilità dei sistemi informatici.

Di fatto, le nuove tecnologie informatiche consentono a un numero sempre più alto di persone di svolgere sempre più attività che hanno come oggetto anche dati e informazioni sensibili.

Il sistema informatico è la cassaforte delle nostre informazioni più preziose; ne deriva la necessità di garantirne la sicurezza.

Di seguito, analizzeremo tutti i metodi di prevenzione, i comportamenti che un utente *diligente* deve eseguire come ***netiquette*** e le tipologie più comuni di virus informatici.

netiquette

Nel linguaggio di Internet, insieme delle norme di comportamento, non scritte ma a volte imposte dai gestori, che regolano l'accesso dei singoli utenti alle reti telematiche, spec. alle *chat-lines*.
www.treccani.it

Acquisiremo, quindi, le competenze e le conoscenze necessarie per identificare e affrontare le principali minacce alla sicurezza informatica.

Certipass
Comitato Tecnico Scientifico

Disclaimer

Certipass ha predisposto questo documento per l'approfondimento delle materie relative alla Cultura Digitale e al migliore utilizzo del personal computer, in base agli standard e ai riferimenti Comunitari vigenti in materia; data la complessità e la vastità dell'argomento, peraltro, come editore, Certipass non fornisce garanzie riguardo la completezza delle informazioni contenute; non potrà, inoltre, essere considerata responsabile per eventuali errori, omissioni, perdite o danni eventualmente arrecati a causa di tali informazioni, ovvero istruzioni ovvero consigli contenuti nella pubblicazione ed eventualmente utilizzate anche da terzi.

Certipass si riserva di effettuare ogni modifica o correzione che a propria discrezione riterrà sia necessaria, in qualsiasi momento e senza dovere nessuna notifica.

L'Utenza destinataria è tenuta ad acquisire in merito periodiche informazioni visitando le aree del sito dedicate al Programma.

INDICE

1. IT SECURITY

L'IT Security rappresenta l'insieme delle tecnologie e dei processi progettati per garantire la protezione di reti, sistemi operativi, programmi e dati da attacchi, danni o accessi non autorizzati.

Il funzionamento delle applicazioni ICT e la riservatezza delle informazioni che sono immagazzinate sui computer e veicolate attraverso la Rete sono infatti continuamente esposti a differenti tipi di insidie.

L'IT Security si presenta dunque come una tematica complessa e delicata, soprattutto se posta in relazione all'importanza, anzi alla centralità, che le operazioni informatiche hanno assunto nella sfera privata e lavorativa.

Questa crescente importanza coincide con lo sviluppo dei rischi legati alla perdita dei dati e alla sottrazione fraudolenta delle informazioni sensibili.

1.1 Il problema della sicurezza informatica

Lo scopo principale dell'IT Security è quindi quello di:

- Minimizzare la **vulnerabilità** di sistemi, dati, informazioni e reti,
- Garantire la protezione dell'integrità fisica (*hardware*) e logico-funzionale (*software*) di un **sistema informatico** e dei dati in esso contenuti o scambiati nelle **comunicazione informatiche**.

1.1.1 Gli standard di sicurezza informatica

Gli standard di sicurezza informatica definiscono l'insieme delle misure minime richieste al fine di ridurre il più possibile la quantità e la pericolosità delle minacce esterne.

Le guide predisposte per l'applicazione degli standard di sicurezza definiscono, infatti, quelle regole che, se applicate adeguatamente, consentono di mettere in opera un sistema di sicurezza informatica efficace.

Nel caso di certi standard, è possibile ottenere anche delle **certificazioni** (le più note sono l'ISO27002-2007 e l'ISO27001-2005), rilasciate da istituzioni preposte.

1.1.2 Cosa proteggere?

Nell'ambito dell'IT Security, quindi, si protegge:

- L'insieme delle componenti essenziali del computer come sistemi operativi, programmi e dati,
- Le reti che mettono in connessione i singoli dispositivi informatici.

1.1.3 I diversi tipi di protezione

Le minacce a cui sono esposti sistemi operativi e dati sono soprattutto riconducibili a due ordini di fenomeni:

- Gli **eventi accidentali**. Si tratta delle conseguenze di eventi non ponderabili e legati a elementi casuali quali, ad esempio, gli eventi atmosferici che determinano l'interruzione dell'erogazione di energia elettrica e possono avere delle conseguenze sui sistemi operativi e sui dati.
- Gli **eventi indesiderati**. Sono le operazioni compiute da soggetti intenzionati a danneggiare il funzionamento dei dispostivi o a sottrarre informazioni e dati. In questo caso possiamo distinguere ulteriormente tra
  - Gli attacchi **malevoli**
  - L'**accesso ai dispositivi da parte di soggetti non autorizzati.**

1.1.4 I diversi livelli di protezione

A seconda del tipo di minaccia, è possibile attivare diversi livelli di protezione, attraverso differenti strumenti.

È possibile definire una prima distinzione tra:

- **Misure di protezione passive**, riconducibili agli accorgimenti da seguire a livello *fisico-materiale*, quale potrebbe essere, ad esempio, la localizzazione dei server in luoghi il più possibile sicuri, dotati di sorveglianza e/o di controllo degli accessi;
- **Misure di protezione attive**, disponibili sul PC per la sicurezza del sistema. In primo luogo, a protezione dell'hardware, è prescritta l'**autenticazione**, ossia la richiesta di un'autorizzazione (sotto forma di *password*) da parte dell'utente al fine di consentire l'avvio del sistema. Per fare un esempio concreto, così puoi evitare che al tuo PC acceda un'altra persona, soprattutto quando non l'hai autorizzata o di nascosto. L'autenticazione è la prima forma di protezione contro questo tipo di violazioni che, come è chiaro, non dipendono direttamente dall'utilizzo della Rete. Conseguenza logica è che devi scegliere le tue *password* utilizzando combinazioni non facili da

indovinare da terzi (come, ad esempio, il tuo nome o la tua data di nascita). Devi, inoltre, utilizzare *password* diverse per ognuno dei tuoi accessi (al PC, all'account di posta elettronica, a Skype e così via). È preferibile che siano composte da almeno 6 caratteri e siano ricomprese maiuscole, minuscole, numeri e segni speciali (ad esempio, ! / ? _).

La One-Time Password (OTP, *password usata solo una volta*) è una password valida solo per un accesso o una transazione. Se un hacker, quindi, riuscisse a intercettare una OTP appena utilizzata, non potrebbe più accedere ai dati protetti. D'altra parte, una OTP non può essere memorizzata e richiede di disporre di un dispositivo riconosciuto dal sistema di login in che genera *password* "usa e getta".
È un sistema molto utilizzato, ad esempio, per le transazioni bancarie.

Figura 1 | Generatori di OTP; sono sempre più usate apposite App per *smartphone*

Una volta che hai inserito correttamente *username* e *password* nella login (del tuo PC o della tua casella di posta elettronica, ad esempio), potrai **autenticarti** ed entrare nel sistema. Da questo momento, le tue attività sono tracciate e monitorate da parte di chi gestisce il sistema (si parla a tal proposito di *accountability*).

Cancellare la Cronologia

Facciamo un altro esempio pratico. Normalmente, quando navighi in Internet, il tuo **browser** conserva la cronologia dei siti visitati.

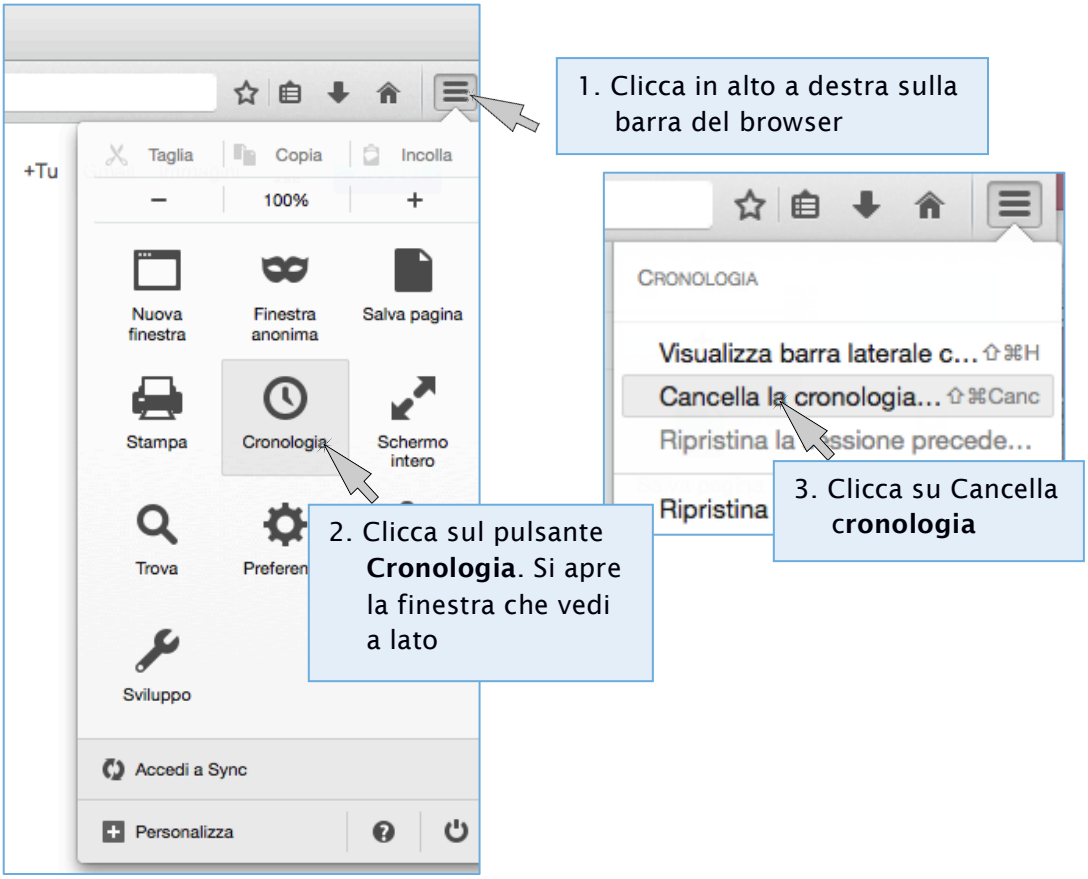
Questo strumento ti consente di tornare su un sito che ti è sembrato interessante o in cui ricordi ci siano informazioni utili, anche se, a distanza di tempo, ne hai dimenticato l'indirizzo (URL). Nella sezione dedicata alla cronologia, infatti, visualizzi gli indirizzi dei siti visitati, organizzati in maniera cronologica.

Questo utile strumento rappresenta, però, anche una minaccia alla tua privacy: chiunque abbia accesso al tuo computer, infatti, potrà conoscere le pagine che hai visto di recente.

Valutandone i pro ed i contro, potresti decidere di cancellare la cronologia ogni volta che navighi o, a seconda dei casi, ogni settimana, ogni mese e così via.

Ogni browser ha un apposito comando nella finestra delle opzioni. Parleremo approfonditamente del tema nel modulo dedicato alla navigazione online.

Figura 2 | Come cancellare la cronologia in Firefox



1.2 Gli attacchi informatici

Tra tutti gli eventi che possono minare la sicurezza del tuo computer o del tuo *smartphone*, i più pericolosi sono senza dubbio i cosiddetti **attacchi informatici**.

Per mezzo dei *dispositivi mobili di archiviazione* o attraverso i *collegamenti remoti della Rete*, un male intenzionato può compromettere, anche in maniera grave, il funzionamento di un PC (o di un altro dispositivo), compromettendone l'integrità, la riservatezza e la disponibilità dei dati e delle informazioni immagazzinate.

Differentemente dai rischi legati all'accesso da parte di utenti non autorizzati, questo tipo di infrazioni, per la natura immateriale della minaccia, sono più complesse da riconoscere e costituiscono, quindi, uno dei più importanti ambiti di studio dell'IT Security.

Le misure di **protezione attiva**, che agiscono in maniera dinamica contro le minacce, funzionano soprattutto a livello di *software* e si concentrano sulle insidie che derivano dalle innumerevoli comunicazioni tra utenti che navigano su internet.

1.2.1 L'hacker

Avrai sicuramente già sentito la parola inglese **hacker**. Si utilizza per identificare gli autori di attacchi informatici.

In realtà, la definizione non è proprio precisa, almeno rispetto alle origini: in effetti, quando negli anni Cinquanta è stata coniata questa parola negli USA, aveva un'accezione totalmente positiva, in quanto identificava gli studiosi che cercavano di superare creativamente le limitazioni imposte dai primi sistemi informatici.

Contrariamente alla maggioranza degli utenti, che impara solo lo stretto necessario, un *hacker* impara a programmare, quindi, con lo scopo di *estendere le applicazioni* per renderle più facilmente accessibili a tutti (da questo deriva la radice etimologica dell'espressione: il verbo *to hack* significa *tagliare*, *sfrondare*, *aprirsi un varco* fra le righe di codice che istruiscono i programmi *software*).

Con l'andar del tempo, è emersa la figura dell'esperto informatico che, abusando delle proprie abilità, sfrutta gli eventuali buchi nella sicurezza informatica del sistema attaccato per sottrarre dati e informazioni da utilizzare a proprio piacimento e, sicuramente, per fini diversi rispetto a quelli del soggetto che subisce la violazione.

Da qui è derivata la distinzione empirica tra l'*hacker etico*, il programmatore, e l'*hacker immorale* che attua pratiche di *violenza informatica*. Il tema è interessante e comporta notevoli implicazioni, anche politiche: è aperta la discussione circa la

moralità di azioni di *hackeraggio* mosse contro istituzioni di grandi dimensioni. Causando, a torto o a ragione, molti problemi nella nostra società (banche, multinazionali, enti governativi e non sovranazionali e così via).

In questo senso, molto famoso è il caso del movimento **Anonymous**. Abbiamo scelto per te un articolo che ne parla; se vuoi approfondire l'argomento, clicca qui.

Figura 3 | Attivitisti con la maschera simbolo di **Anonymous**

Categorie principali di criminali informatici

Aldilà delle riflessioni appena proposte, non ci sono dubbi circa l'illegalità di numerosi e specifici attacchi. Chi li identifica come coloro che sottraggono dati, li definisce, in maniera più precisa, **cracker**.

Ci sono ulteriori categorie o suddivisioni:

- I **phracher** sono specializzati nel furto di programmi che offrono servizi telefonici gratuiti o nella penetrazione in computer e database di società telefoniche;
- I **phreaker** sanno utilizzare numeri telefonici o carte telefoniche per accedere ad altri computer;
- I **black hat** agiscono con il chiaro fine di delinquere a differenza dei **white hat** che tengono alla loro moralità e alla legalità di tutte le azioni poste in essere.

2. MALWARE

2.1 Attacchi e minacce informatiche

2.1.1 I Malware

L'espressione **malware** (risultante dalla contrazione delle espressioni inglesi *malicious* e *software*) indica un qualsiasi *software* creato allo scopo di causare danni ad un dispositivo su cui viene eseguito e sui dati che vi sono immagazzinati. Ce ne sono di due tipi:

- **Di tipo parassitario**,
- **Del settore d'avvio**.

A differenza dei programmi malevoli di tipo *parassitario*, che vengono trasmessi mentre il dispositivo è in funzione, i virus del *settore d'avvio* si diffondono attraverso l'avvio, o il tentativo di avvio, da un disco esterno infettato.

Anche se il disco non contiene i file di sistema necessari per eseguire l'avvio, un *tentativo di avvio* da un disco infetto caricherà il virus in memoria. Il virus si aggancia in memoria come se fosse un *driver* di periferica ed è difficilissimo da rimuovere.

Di seguito elenchiamo alcuni dei più diffusi *malware* in circolazione.

Il virus

Il virus informatico (termine con cui generalmente, ma erroneamente, vengono indicati tutti i *malware*) è un piccolo programma o *software*, che contiene una sequenza di istruzioni in grado di attivare automaticamente azioni che danneggiano un computer.

Agisce in maniera simile ad un virus biologico: è pericoloso, quindi, per la sua tendenza a creare *epidemie*: parte delle istruzioni del programma infettivo sono deputate alla riproduzione di copie di sé stesso. Dopo la fase *riproduttiva*, i virus informatici iniziano a svolgere attività di diversa natura e, anche quando non sono direttamente dannosi per il sistema operativo che li ospita, comportano un certo spreco di risorse in termini di RAM, CPU e spazio sul disco fisso. In generale un virus danneggia direttamente solo il *software* della macchina che lo ospita, anche se può indirettamente provocare danni anche all'*hardware*, ad esempio causando il surriscaldamento della CPU, oppure fermando la ventola di raffreddamento.

Worm

I *malware worm* (letteralmente traducibile con la parola *verme*) modificano il Sistema Operativo del computer, facendo in modo di essere eseguiti automaticamente, rallentando il sistema con operazioni inutili e dannose.

Il Trojan horse

È un programma che l'utente scarica perché ha funzionalità utili e desiderate, ma che, se eseguito, avvia, a sua insaputa, (da qui il richiamo al *Cavallo di Troia*), istruzioni dannose per i file del sistema operativo.

Spyware

Sono *software* usati per spiare le informazioni del sistema sul quale sono installati (abitudini di navigazione, *password* e altri dati sensibili) che sono quindi acquisite da un terzo interessato ma non autorizzato.

Dialer

I *dialer* gestiscono la connessione a Internet tramite la vecchia linea telefonica. Possono essere utilizzati per modificare il numero telefonico digitato dall'utente, per chiamare, ad esempio, numeri a *tariffa speciale*, in modo da trarne illecitamente profitto.

Zip Bomb

La *zip bomb* è un programma che disattiva le difese del PC per consentire a un altro virus di infettarlo. È *un archivio compresso malevolo* che rende inutile il programma che lo legge: per eliminarlo, prima che *apra la strada* ad altri virus o *malware*, bisognerebbe cancellare il file senza aprirlo, eseguirlo o decomprimerlo.

2.1.2 Altre categorie di attacchi informatici: gli attacchi login

Sniffing

È il modo tramite cui un male intenzionato riesce ad intercettare passivamente i dati che transitano in una Rete telematica.

Questa attività è normalmente svolta per scopi legittimi (ad esempio, l'analisi e l'individuazione di problemi di comunicazione o di tentativi di intrusione).

I *software* utilizzati per eseguire queste attività vengono detti *sniffer* e, oltre ad intercettare e memorizzare il traffico, offrono funzionalità di analisi del traffico stesso.

Ma *software* dello stesso tipo possono essere utilizzati per scopi illeciti (intercettazione fraudolenta di *password* o altre informazioni sensibili).

Spoofing

È un attacco utilizzato tramite mail e consiste nel *camuffarsi*: il male intenzionato falsifica il proprio indirizzo in modo che, il destinatario, vedendosi arrivare una mail da un ente riconosciuto (Poste italiane, ad esempio), la apra immediatamente, pensando si tratti di una comunicazione importante.

Thiefing

Consiste nello sfruttare l'assenza di misure di protezione adeguate, per sottrarre servizi informatici: hai mai provato a connetterti alla Rete *wireless* del tuo vicino che non s'è curato di inserirvi una *password*? Stavi facendo *thiefing*!

Keylogger

È un sistema che consente di intercettare tutto quello che un utente digita su una tastiera. È molto usato per appropriarsi indebitamente dei dati digitati sulle tastiere degli sportelli bancomat.

Esistono due tipi di keylogger:

- *Hardware*: dispositivi che vengono collegati al cavo di comunicazione tra la tastiera ed il computer o all'interno della tastiera.
- *Software*: programmi che controllano e salvano la sequenza di tasti che viene digitata da un utente.

Phishing

È una *frode informatica* finalizzata a *rubare* l'identità di altre persone e, in concreto, carpire, attraverso le e-mail, i *dati di accesso* agli strumenti finanziari gestiti on-line (nome utente e *password* di conto corrente, carte di credito, carte prepagate, ecc.).

Il sistema funziona tramite l'invio di mail o l'apertura di *finestre a comparsa*. Il male intenzionato fa leva sul fatto che un utente inconsapevole o distratto possa cliccare su *allegati* o *pop-up*, senza prestare la necessaria attenzione.

2.2 Gli strumenti di difesa

L'unico computer totalmente sicuro e a prova di hacker è quello spento, non collegato a Internet e chiuso a chiave in una cassaforte!

I *software* maligni vengono diffusi principalmente tramite la Rete internet (e-mail, condivisione di file in reti P2P e per mezzo dei siti Web non attendibili), ma possono essere introdotti anche attraverso i *dispostivi di memoria esterni*, come chiavi USB.

Come abbiamo visto, la Rete è anche il principale veicolo di quelle particolari truffe informatiche finalizzate alla violazione dei *login di accesso*.

Il principale strumento per la difesa della sicurezza dei dati e delle ITC è costituito dal **buon senso** dell'utente.

Di fatto, la colpa dell'elevata diffusione di *malware* è da attribuire soprattutto a chi utilizza il PC, che troppo spesso non si cura delle basilari misure di sicurezza che comunque ha a disposizione e potrebbe facilmente impostare.

La protezione dei computer passa essenzialmente dalla presenza di dispostivi di difesa aggiornati e funzionanti come *firewall*, *antivirus* e altri *software* specifici per la protezione dei dati (DMS, IDS/NIDS).

2.2.1 Il firewall: una protezione contro i virus

Da quello che si è detto finora, abbiamo imparato che avere un *antivirus* aggiornato e perfettamente funzionante non ci assicura, in tutto e per tutto.

È bene, quindi, utilizzare tutti gli strumenti disponibili per la sicurezza del nostro sistema.

Il **firewall** (letteralmente *muro di fuoco*), se ben configurato e usato correttamente, permette di:

- Bloccare i virus, anche non conosciuti, prima che questi entrino nel computer,
- Bloccare, all'interno del PC, virus che siano già entrati, evitando così che possano infettare altri dispositivi eventualmente collegati.

Un *firewall* è uno strumento aggiuntivo che:

- Impedisce a un virus di infettare la macchina prima che venga individuato dall'antivirus (con possibile perdita del file infetto),
- Permette di nascondere parzialmente o totalmente il computer quando si naviga o si è collegati ad una Rete, diminuendo al minimo il rischio di attacchi informatici.

Approfondiremo tra breve il tema, per imparare a configurare il *firewall* sul tuo PC.

2.3 L'antivirus

L'*antivirus* è il più immediato sistema di protezione contro i *malware*. Si tratta di un *software* ideato appunto per

- Prevenire l'infezione,
- Rilevare ed eventualmente eliminare programmi malevoli che insidiano la sicurezza dei computer.

Figura 4 | Gli antivirus più diffusi

2.3.1 Il funzionamento di un software antivirus

L'*antivirus* identifica la minaccia attraverso l'analisi del database delle *firme del virus*.

Ciascun *malware* è composto da un numero preciso di **istruzioni**, un **codice** costituito da una stringa di **byte** che il programma antivirus cerca di rintracciare all'interno del computer, nei file o nella RAM.

Generalmente, con il termine *antivirus* si fa riferimento a diversi elementi del software:

- Il *file (o i file) delle firme*: file che contiene tutte le firme dei virus conosciuti. Questa parte è fondamentale ed essenziale per il funzionamento corretto di qualsiasi altro componente;
- Il *file binario* in grado di ricercare il virus all'interno dell'elaboratore. Questo componente è l'*antivirus* vero e proprio;
- Il *file binario* che rimane residente e richiama l'antivirus ogni qual volta viene creato/modificato un nuovo file o viene modificata una zona di memoria per controllare che il computer non sia stato infettato con questa operazione;
- Il *file binario* che effettua gli *update* (aggiornamento) del file delle firme e di tutti i binari dell'*antivirus*.

2.3.2 Scansione del sistema e analisi real-time

La scansione antivirus

La **scansione** è il processo di analisi di un PC effettuato dall'*antivirus*. Si può impostare la scansione all'avvio del computer o effettuarla in qualunque altro momento.

L'*antivirus* utilizza molte risorse del computer per funzionare: se viene avviato automaticamente ogni volta che il computer viene acceso, può comportare un forte rallentamento, soprattutto nelle fasi iniziali (perché controlla prima tutta la memoria e poi tutti i file, che rientrano nella ricerca selezionata durante la fase configurazione, su disco).

Attraverso i *software antivirus* è possibile programmare la scansione all'avvio del PC o ad un orario preciso.

Ci sono differenti modalità:

- **Scansione completa** di tutti i file e delle applicazioni in esecuzione in tutte le unità del computer. Questo tipo di scansione è più lento degli altri e richiede maggiori risorse del sistema operativo. Rallenta il funzionamento del computer ma consente di rilevare il maggior numero possibile di infezioni. È consigliabile eseguire la *scansione completa* una volta alla settimana, programmandola nel momento più idoneo, ad esempio, durante le ore notturne.
- **Scansione su misura o personalizzata**. Consente di selezionare le unità e le cartelle da sottoporre a scansione.
- I sistemi *antivirus* prevedono anche una **scansione rapida**, che consiste in una scansione limitata agli oggetti caricati all'avvio del sistema operativo, la memoria di sistema e i boot. La *scansione rapida* potrebbe non individuare alcuni *malware* ma, comunque, informa della presenza di un virus nel caso in cui il computer sia infetto.
- **Scansione intelligente**, effettuata soltanto nelle aree più soggette a infezione.

Avanzamento scansione

Durante l'esecuzione della scansione la *barra di avanzamento* indicherà la percentuale della scansione completata e stimerà il tempo rimanente. È possibile *interrompere* o *mettere in pausa* la scansione in ogni momento, usando le relative finestre di comando.

Risultati scansione

Completata la scansione, se sono state rilevate delle minacce, viene visualizzato *un elenco* delle infezioni e dei relativi livelli di rischio. A questo punto, è possibile selezionare le *opzioni di correzione*.

Riparazione delle infezioni al termine della scansione

È possibile:

- **Mettere in quarantena le infezioni**. I file selezionati vengono messi in condizioni di non nuocere al sistema e possono essere ripristinati in qualunque momento, se necessario;

- **Rimuovere** l'elemento in maniera permanente (senza metterlo in quarantena).

Creazione di un punto di ripristino Windows prima della rimozione delle infezioni

Nelle ultime versioni di Windows, è prevista la possibilità di creare un **punto di ripristino Windows**. In caso di malfunzionamento o errore del sistema generato da un'infezione grave, questo strumento consente di ripristinare *file di sistema*, *chiavi di registro*, *programmi installati*, etc.

Per creare un punto di ripristino

1. Fai clic sul pulsante **Start**.
2. Fai clic con il pulsante destro del mouse su **Computer** e seleziona **Proprietà**.
3. Nel riquadro sinistro, fai clic su **Protezione sistema**.
4. Seleziona la scheda **Protezione sistema** e fai clic su **Crea**.
5. Nella finestra di dialogo **Protezione sistema**, digita una descrizione e quindi fai clic su **Crea**.

Analisi antivirus Real-Time

Oltre il processo di scansione, in *antivirus* con tecnologie di analisi **Real-Time**, l'analisi del sistema viene effettuata su *ogni file* a cui l'utente o il sistema fanno accesso.

Attivando questa opzione di **analisi comportamentale**, si introduce un'*ultima linea di difesa* contro *malware* che potrebbero essere eseguiti sul sistema dopo aver eluso tutti gli altri tipi di rilevamento e scansione.

Di fatti, attraverso questa protezione, è possibile intercettare le operazioni eseguite dalle applicazioni installate nel computer in tempo reale, determinando, in base al loro comportamento, se i processi possono essere eseguiti o meno.

2.3.3 L'aggiornamento dell'antivirus

Il successo della scansione è tuttavia legato all'**aggiornamento** degli schemi che l'*antivirus* è in grado di riconoscere. L'aggiornamento dei *software antivirus* avviene, di solito, in base alle segnalazioni degli utenti o di gruppi specializzati che, per mestiere o per *hobby*, individuano nuovi virus.

Oltre ai produttori di *software antivirus*, infatti, sono diverse le organizzazioni che si occupano di raccogliere le segnalazioni di vulnerabilità o attacchi, e renderle pubblicamente disponibili, al fine di aggiornare continuamente i registri delle firme dei virus (tali organizzazioni sono normalmente note con l'acronimo di CERT,

Computer Emergency Response Team, *squadra di risposta alle emergenze informatiche*).

Anche in questo campo, la tecnologia sta facendo passi da gigante: il confronto tra chi crea virus e chi cerca di scovarne è sempre più serrata.

L'ultima frontiera è l'**euristica**. Gli *antivirus* programmati con tecnologia euristica sono in grado di riconoscere anche *firme parziali* di virus, per individuarne di nuovi o ancora non conosciuti, soprattutto del tipo dei **polimorfi**. I nuovi *antivirus* riescono ad analizzare il comportamento dei vari programmi, alla ricerca di istruzioni *sospette*. Ne riparleremo.

Il **virus polimorfo** è in grado di nascondere il proprio codice, utilizzando, quindi, una *chiave* diversa in ogni tentativo di infezione. È dotato pertanto di un *engine*, anch'esso cifrato, che modifica in maniera casuale la procedura di decrittazione (in chiaro) dopo ogni infezione.

Riassumendo, abbiamo imparato che

- L'*antivirus* è in grado di eliminare soltanto i virus che riconosce, ossia quelli presenti nel suo database,
- Tutti i *nuovi* virus (quelli non riconosciuti e quelli che non sono ancora stati scoperti) possono passare completamente inosservati e non essere rilevati.

L'aggiornamento del tuo *antivirus* serve proprio a rimpinguare il suo database, in modo tale che almeno tutti i *malware* già riconosciuti (cioè già immessi nella lista del database online del *software*) non diventino mai un problema serio per il tuo PC.

Da quando la *Symantec* ha introdotto il sistema automatico *Live-Update* per il suo *antivirus* **Norton**, è diventato davvero semplice aggiornare i programmi.

Oggi tutti gli *antivirus* si aggiornano automaticamente, non appena è disponibile una connessione online.

2.3.4 Antivirus, sistemi operativi e programmi

Antivirus e Sistemi Operativi

Se il tuo PC utilizza un sistema operativo Microsoft, devi sempre avere un *antivirus* perfettamente operativo, visto che, considerata la diffusione e la politica gestionale, questo sistema è il più vulnerabile.

Gli altri (Linux e Mac) sono molto meno esposti.

Ma il vero punto nodale della questione è quella relativa alla protezione dei **server**, (dei computer, cioè, che mettono in correlazione altri computer, scambiando quotidianamente una moltitudine di dati).

Se pensiamo ad un **server** che controlla i sistemi di posta elettronica, possiamo comprendere immediatamente la portata del problema.

Antivirus e programmi

Considerato quanto abbiamo appena detto, tra tutti i *software* che girano sui nostri PC, quelli più utilizzati per la diffusione dei virus sono:

- I **client di posta** elettronica,
- I **browser**.

Sono i programmi che ci consentono di sfruttare due tra gli strumenti più significativi dell'ICT: la *posta elettronica* e la *navigazione web*.

Anche i *file* prodotti dalle cosiddette **macro** di Microsoft Office sono molto vulnerabili. Parleremo approfonditamente delle *macro* nei moduli dedicati ai programmi di elaborazione testi e ai fogli di calcolo.

Per quello che serve qui, accenniamo al fatto che con i programmi di Microsoft Office è possibile impostare una serie di comandi (detti *macro*, appunto) per eseguire alcune funzionalità (quelle che utilizzi più di frequente) in maniera automatica o tramite una specifica *combinazione di tasti*.

Molti *cracker* sfruttano questo strumento per diffondere *macro* che sembrano poter facilitare la gestione di alcuni comandi ma che, in realtà, sono dei virus.

3. SICUREZZA DEI DATI

3.1 La gestione sicura dei dati

Come accennato, l'IT Security comprende tutte quelle attività finalizzate alla *protezione dei dati* attraverso misure di carattere tecnico-organizzativo e funzionali tese ad assicurare che:

- i dati conservati o trasmessi siano **integri**,
- qualora un terzo venga in possesso di dati trasmessi tra altri, questi siano per lui inutilizzabili (**confidenzialità dei dati**),
- qualora ci siano accessi privati, siano autorizzati solo gli aventi diritto (**autenticazione**),
- ogni utente usufruisca effettivamente di tutti i dati che gli competono e solo di quelli (**disponibilità**),
- ogni dispositivo *hardware* e *software* funzioni correttamente.

Terminata questa indispensabile parte introduttiva, vediamo adesso con maggiore attenzione alcune specifiche tecniche di prevenzione *fisico-materiali*.

3.1.2 Le tecniche di protezione dei dati

Lo storage

Se pensi alla mole di dati creati, disponibili e scambiati ogni giorno in Internet, comprendi facilmente quanto alta sia la necessità di *salvarli*, in modo sicuro.

Considerate queste necessità pratiche, la tecnologia si è evoluta fino ad aggregare *singole unità disco* per realizzare *infrastrutture* in cui, in pratica, non ci sono limiti fisici alla quantità di dati caricabili.

Nello stesso tempo, per ridurre i costi di gestione, queste risorse sono state sempre più centralizzate, fino ad essere conservate su *singoli dispositivi*.

Con il termine **storage** (che potremmo tradurre in *sistema di archiviazione dati*) si indicano tutti i supporti *hardware* e *software*:

- Organizzati con la specifica finalità di conservare enormi quantità di informazioni in formato elettronico,
- Capaci di garantire la sicurezza delle informazioni conservate.

Ce ne sono di diversi tipi.

NAS (*Network Attached Storage*). Il dispositivo è collegato a più computer messi in rete tra loro.

Questo sistema:

- Permette di centralizzare l'immagazzinamento dei dati in un'unità accessibile a tutti i nodi della rete e specializzata,
- Garantisce che i dati immagazzinati sia molto più al sicuro.

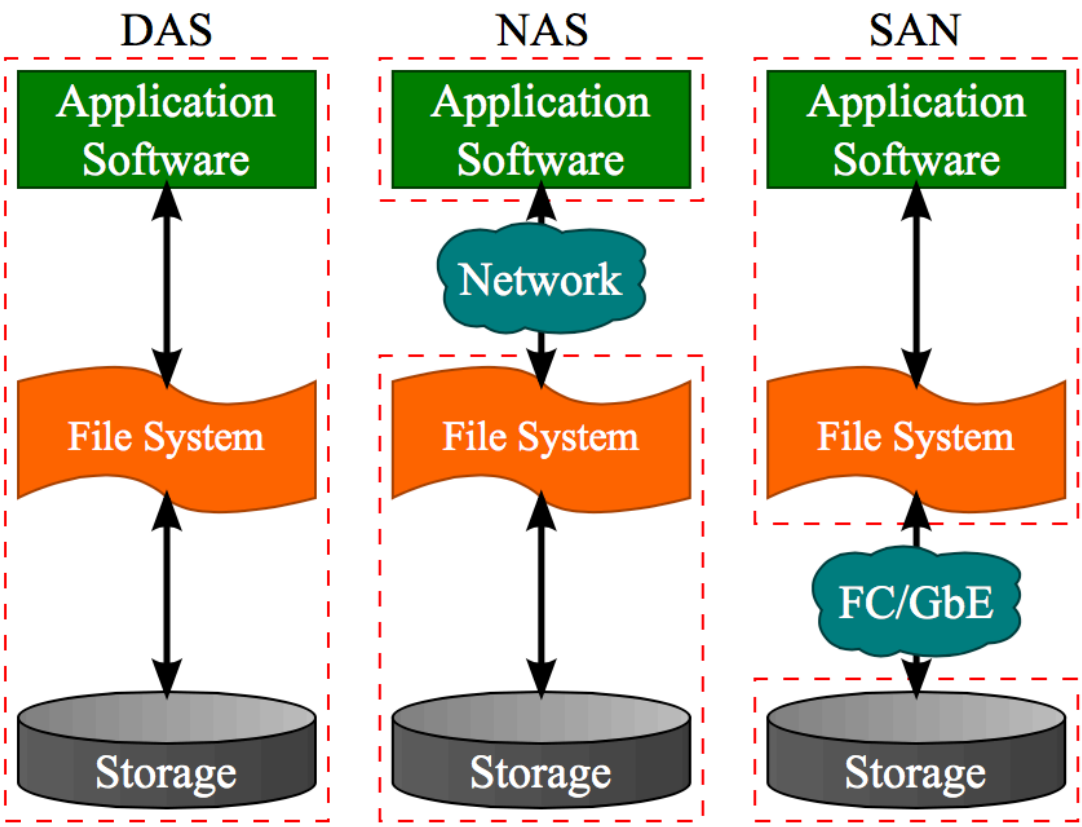
Lo svantaggio è che la grande quantità di dati in transito nella rete locale può determinare rallentamenti e malfunzionamenti del sistema.

DAS (*Direct Attached Storage*). Prima forma di **storage**, consiste in un dispositivo di immagazzinamento di dati che è collegato direttamente ad un **server** o ad un computer, non avendo alcuna connessione di Rete. Sono diverse le negatività, a confronto con i metodi più moderni: ad esempio,

- È difficile condividere i dati tra più computer,
- L'espansione dello spazio di immagazzinamento è complessa.

SAN (*Storage Area Network*). Sistema di immagazzinamento dati capace di renderli disponibili a computer connessi (normalmente ad Internet), ad altissima velocità, grazie all'utilizzo della *fibra ottica* (Gigabit/sec). I vantaggi rispetto ai sistemi DAS è evidente: consente ai **server** e ai **dispositivi di storage** di avere una connettività diretta, con un'ottimizzazione dell'efficienza dello spostamento di dati e processi (come, ad esempio, il *backup* o la *replica dei dati*).

Figura 5 | I diversi sistemi di storage



Il backup dei dati

Devi conoscere bene il concetto di *backup* (copia), perché si tratta di un aspetto davvero importante della *gestione* di un computer. Siamo tutti oramai abituati a creare *file*, in continuazione: scattare e caricare foto, scaricare musica e video, elaborare documenti di testo, di calcolo e così via.

Ciò detto, sai cosa potrebbe succedere al tuo computer in caso, ad esempio, di *sbalzo di tensione* o di una *momentanea interruzione della corrente*?

Figura 6 | Un gruppo di continuità

A meno che tu non utilizzi un *gruppo di continuità*, questi eventi possono corrompere i tuoi *file*, anche fino a renderli irrecuperabili!

Non è l'unico inconveniente, questo, che può farti perdere dati: potrebbe capitare, ad esempio, che l'*hard disk* del tuo computer si rompa (può succedere soprattutto se lo usi tutti i giorni) o che te lo rubino (soprattutto se è un portatile). Per evitare problemi di questo genere, è buona norma creare una *copia di sicurezza* dei propri dati che, in informatica, si definisce, appunto, *backup*.

È, in sostanza, una *copia di riserva* da cui puoi recuperare i tuoi dati in caso di perdite accidentali (che possono capitare molto più spesso di quanto si pensi). È possibile copiare dati su:

- Hard disk esterni,
- CD,
- DVD e Blu-Ray,
- Pen-drive USB,
- In generale, su supporti rimovibili,
- Internet, grazie ai *software* **Cloud**.

A prescindere dal metodo scelto, è buona norma fare almeno una copia al mese dei tuoi dati; sarebbe perfetto, inoltre, farla su più dispositivi (potresti perdere il DVD, ad esempio!). Come è facile intuire, la copia dei dati è un'attività fondamentale per aziende e lavoratori: i produttori di *software* dedicati a questa attività si impegnano per:

- Ottimizzare i processi, attraverso l'individuazione più veloce degli elementi da copiare,
- Ridurre il traffico necessario a copiare i dati,

In modo da aumentare la *frequenza* delle copie, tenendo in debita considerazione che questa attività non deve sovrapporsi alle attività quotidiane.

Ogni *backup*, infatti, impegna il sistema informatico, rallentando i tempi di risposta dei computer da cui sta copiando. Per questo motivo, vari sistemi di *backup* vengono ancora attivati di notte, quando normalmente gli utenti non lavorano.

Come fare il backup

Tutti i sistemi operativi dei computer di oggi hanno già integrato un *software di backup*: su Windows 7, c'è lo strumento *Backup e ripristino*, nel *pannello di controllo* ma, bada bene, in questo modo è possibile ripristinare il sistema operativo di Windows ma non ottieni una copia dei tuoi dati che, in ogni caso, andrebbero persi.

Windows 8 ha implementato questo sistema, prevedendo un secondo livello di *backup*, capace, questa volta, di salvare anche i tuoi dati: lo strumento si chiama *Cronologia file* e funziona sulla falsariga di *Time Machine*, il sistema di *backup* di Apple.

Dopo l'impostazione iniziale, il *backup* è veloce e automatico: sarà lo stesso sistema operativo ad aggiungere i nuovi *file* creati, di volta in volta, al *file copia*, utilizzando il metodo **incrementale**.

Ci sono tre tipi principali di backup: *completo*, *incrementale* e *differenziale*.

Il **backup completo** memorizza tutti i dati selezionati per il *backup*, costituendo la base per eventuali *backup incrementali* e *differenziali*. Consente di ripristinare i dati senza dover accedere ad altri *backup*. È utile soprattutto quando è necessario riportare il sistema allo stato iniziale.

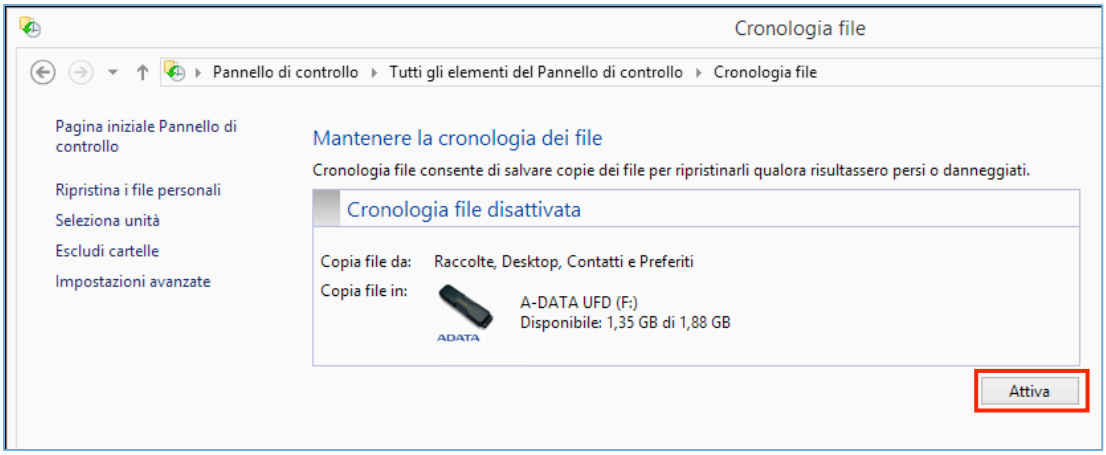
Il **backup incrementale** memorizza le modifiche apportate ai dati rispetto all'ultimo *backup*. Per ripristinare i dati, è necessario accedere agli altri *backup* dello stesso archivio. È utile quando si desidera avere la possibilità di riportare il sistema a uno dei diversi stati salvati a disposizione.

Il **backup differenziale** memorizza le modifiche apportate ai dati rispetto all'ultimo *backup completo*. Per ripristinare i dati da un *backup differenziale* è necessario accedere al *backup completo* corrispondente. È utile quando si vuole salvare solo lo stato più recente dei dati.

	Completo	Differenziale	Incrementale
Spazio di archiviazione	massimo	medio	minimo
Tempo di creazione	massimo	medio	minimo
Tempo di ripristino	minimo	medio	massimo

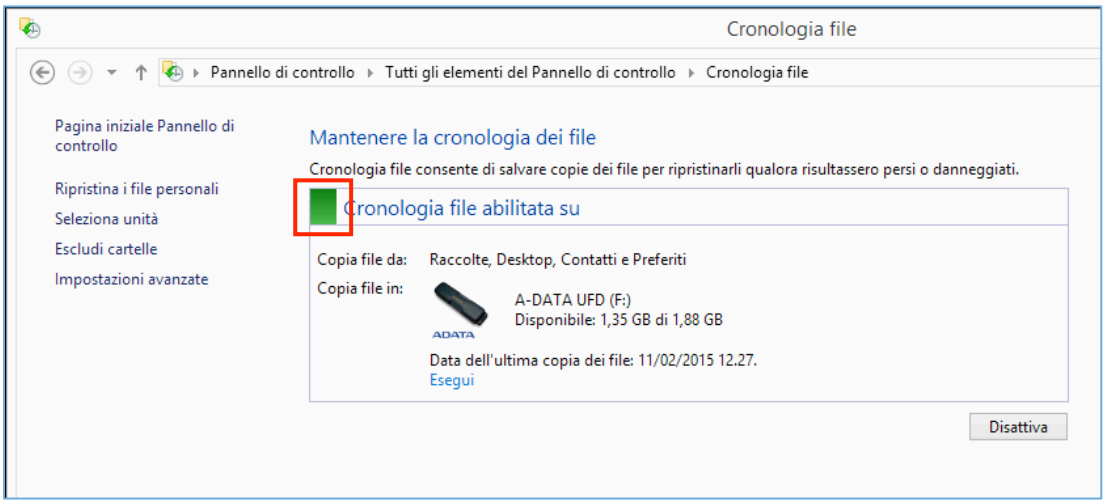
1. Accedi al **Pannello di controllo** e clicca su *Cronologia file*.
2. Se non hai ancora impostato il servizio, devi scegliere su quale dispositivo copiare i dati. Il sistema riconosce automaticamente quello che inserisci. Nell'esempio che segue, una Pen-drive USB denominata A-DATA UDF.

Figura 7 | Finestra *Cronologia file*



3. Clicca su attiva. Lo spazio a sinistra del titolo diventa verde.

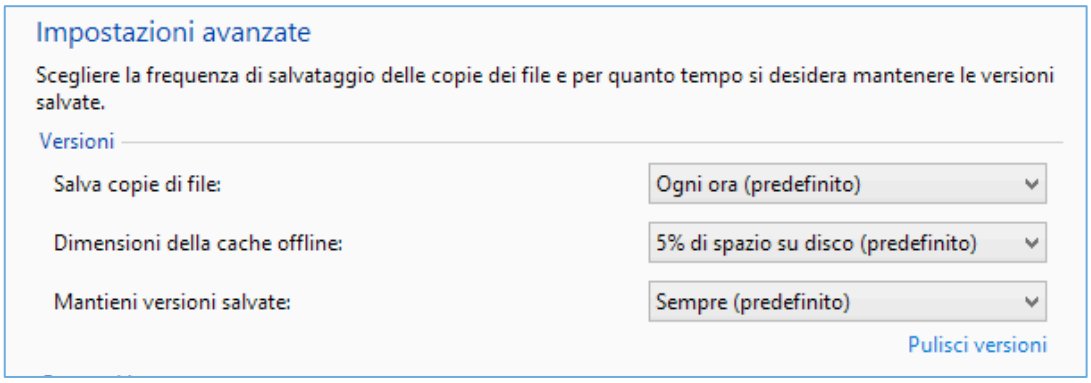
Figura 8 | Attivazione servizio



Per *ripristinare* (approfondiremo tra breve il tema), scegli la voce **Ripristina i file personali** dalla scheda principale di *Cronologia file* (oppure clicca sulla stessa voce nel menù a sinistra della sezione vista nella figura precedente) e scegli se ripristinare tutti o solamente una parte dei dati salvati.

Cliccando su *Impostazioni avanzate*, nel menù a sinistra, puoi settare altre opzioni, tra cui la frequenza dell'attività di *backup*.

Figura 9 | Attivazione servizio



Oltre alle funzioni integrate, puoi utilizzare *software* gratuiti molto performanti, come, ad esempio, *EaseUS Todo Backup Free* (compatibile anche con Windows Vista e Windows XP) o *fwbackups*, per chi utilizza Linux; ce ne sono, comunque, molti *altri*.

Il backup su smartphope e tablet

Se hai uno *smartphone* o un *tablet*, ti consigliamo di fare il *backup* direttamente su una memoria esterna (micro SD, ad esempio) utilizzando uno dei *software* che trovi, anche gratuitamente, in Internet. L'altra possibilità è quella di farlo sul PC o sul *Cloud* ma, in questi casi, è indispensabile avere una connessione ad Internet.

Focalizziamo l'attenzione su Windows *Phone*, specificando che quanto stiamo per dire riguarda la versione 8.1.

Capita spesso di voler importare i propri account, le proprie App e le proprie impostazioni da un telefono ad un altro; è sempre stata un'operazione abbastanza complessa, soprattutto quando il proprio cellulare è stato rubato, ad esempio. Il nuovo sistema Windows *Phone* consente di fare il *backup* dei dati salvati sul telefono e di importarli facilmente su altri telefoni o di ripristinarli. In questo caso sarà utilizzato il *Cloud*.

Nell'elenco delle app, vai a **Impostazioni** → **Backup** per scegliere il modo in cui il telefono deve eseguire il *backup.* Il telefono aspetta di collegarsi ad una rete Wi-Fi per avviare la copia. Puoi, però, avviarla manualmente:

1. Vai su **Impostazioni** → **Backup** → **App e impostazioni**
2. Attiva **Backup delle impostazioni**
3. Tocca **Esegui il Backup ora**.

È possibile attivare *Backup* diversi per App e impostazioni, SMS e foto e video.

Backup di App e impostazioni

1. Nell'elenco delle App, tocca **Impostazioni** → **Backup**.
2. Tocca **App e impostazioni**.
3. Attiva **Backup delle impostazioni**

Per fare il *Backup* delle App, assicurati che **Backup delle impostazioni** sia attivo e attiva **Backup delle App**

Backup degli SMS

1. Nell'elenco delle App, tocca **Impostazioni** → **Backup**.
2. Tocca **SMS**,
3. Attiva o disattiva **Backup degli SMS**.

Caricamento automatico di foto e video

1. Nell'elenco delle App, tocca **Impostazioni** → **Backup**.
2. Tocca **Foto e video**
3. Scegli una delle impostazioni disponibili (Non caricare, Qualità Buona, Qualità ottima).

Avrai sempre bisogno di una connessione per caricare video e foto sul *Cloud* e rivederle, successivamente, su ogni altro dispositivo collegato ad Internet.

3.1.3 Il ripristino

Con il termine *ripristino*, si fa riferimento a due diversi tipi di *recupero dati:*

- Quello relativo all'intero *sistema operativo* del computer.
- Quello di specifici *file*, che saranno semplicemente caricati su un nuovo dispositivo.

Il primo caso si riferisce alla circostanza in cui è necessario ripristinare l'**immagine di sistema**, perché il *disco rigido* o l'intero computer ha subito un danno tanto grave da smettere di funzionare.

L'**immagine del sistema** è una copia esatta di un'*unità*, che include tutto ciò che è necessario per il funzionamento di Windows, le impostazioni di sistema, i programmi e i *file*.

Quando si ripristina il computer da un'**immagine del sistema**, si esegue un *ripristino completo*; in sostanza, questo significa che tutti i programmi, le impostazioni e i *file* correnti verranno sostituiti dal contenuto dell'immagine stessa.

Prima di iniziare, devi verificare, inoltre, che il *disco* su cui stai ripristinando i dati abbia *dimensione* uguale o superiore al disco che intendi ripristinare (questo vale anche nel secondo caso).

In questa sede, ci soffermiamo sul secondo tipo di ripristino, riferendoci a quello dei soli *file*.

3.1.4 Eliminare in modo permanente i dati dalle memorie di massa o dai dispositivi

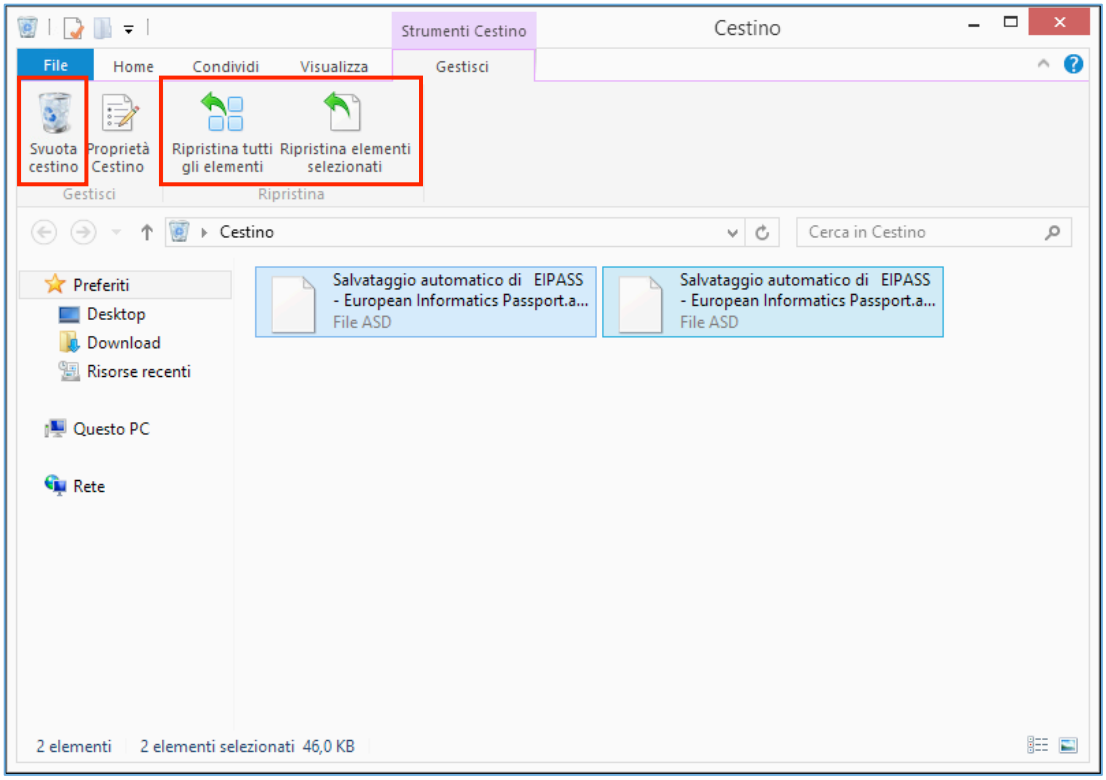
Quando un dato non ti serve più, è buona norma cancellarlo, piuttosto che intasare il tuo computer o il tuo *device* con *file* inutilizzati. Più sono i *file* sul tuo computer, infatti, minore sarà la sua velocità e peggiori le sue performance.

È molto facile cancellare *file*, spostandoli nel **cestino**.

Il *cestino* è una cartella speciale che contiene tutti i *file* eliminati. Bada bene, però: questi *file* sono tutti facilmente *recuperabili* (tecnicamente, si dice *ripristinabili*).

Se vuoi ripristinare file cancellati, apri la cartella *cestino*, seleziona i *file* e clicca su uno dei comandi indicati di seguito.

Figura 10 | La cartella cestino



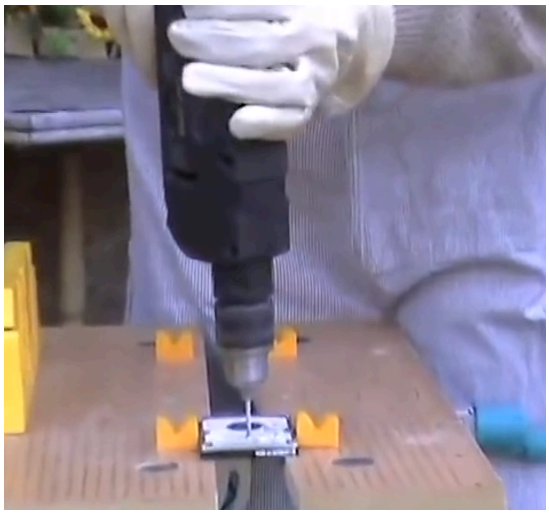
Per facilitare queste operazioni, ti consigliamo di visualizzare la *barra degli strumenti*, così come hai visto nella figura 10. Per farlo, clicca su **Gestisci** e, poi, sull'icona *freccetta in basso* , sulla destra della *barra dei menù*.

Se, invece, vuoi che i *file* nel cestino siano rimossi definitivamente, clicca sul comando **Svuota cestino**.

Devi sapere, però, che anche dopo aver svuotato questa cartella, sul disco rimangono delle tracce che *software* specifici (come **Glary Utilities**, e **Recuva**) possono acquisire per ricostruire integralmente o quasi i *file* rimossi, a seconda del tempo che passa dalla loro cancellazione e dai successivi utilizzi del computer.

Il modo più sicuro per eliminare definitivamente i *file* è quello che vedi raffigurato nell'immagine di fianco: forare con un *trapano* la memoria che li contiene!

Figura 11 | Distruggere la memoria di massa



Esistono, comunque, delle alternative meno cruente e invasive che assicurano una cancellazione sicura.

Glary Utilities, (lo stesso programma che può recuperare i *file*), ha uno strumento efficace per distruggerli in modo definitivo.

Il metodo usato (*American Dod 5220.22-M*) è sviluppato dal *Dipartimento Difesa USA* per rimuovere i dati in sicurezza.

CCleaner è un altro *software* che ti permette di cancellare (*ripulire*, come dice il nome) dal tuo computer tutti i *file* che non sono più utili.

Questo programma è in grado di cancellare anche tutti i *file* che registrano le tracce della tua navigazione in Internet e che vengono automaticamente salvati sul tuo PC.

Questo tipo di pulizia ha innegabili vantaggi:

- *libera spazio* di memoria dal tuo *hard disk*,
- difende la tua privacy,
- rende *più veloce* il sistema operativo.

3.2 La trasmissione dei dati tramite il *Bluetooth*

Ci sono diversi modi per far comunicare tra loro due o più dispositivi elettronici. Il più comune è sicuramente quello di utilizzare un *cavo*.

Se colleghi ancora tutti i tuoi dispositivi in questo modo, comprendiamo bene il disappunto che provi ogni volta che si tratta di risolvere il groviglio che si crea dietro il tuo *case*.

In realtà, sono sempre di più i dispositivi che si possono connettere tra loro *senza l'utilizzo di cavi*: la tecnologia **Bluetooth**, ormai molto diffusa, consente la comunicazione senza fili tra:

- Dispositivi di diversa natura (un computer e un *tablet*, ad esempio),
- Tra i dispositivi e i loro rispettivi accessori, come *mouse*, *tastiere*, *antenne satellitari*, ecc.

Il nome deriva da *Harald Bluetooth*, un re Vichingo del X Secolo che unificò i regni di Danimarca e Norvegia. Essendo questa la finalità dello *standard* (unificare), i tecnici scandinavi che lo hanno inventato hanno scelto di attribuire questo nome.

Si basa su *frequenze radio a corta portata*: i dispositivi che la utilizzano possono comunicare tra loro attraverso il dispositivo stesso.

Le caratteristiche principali sono:

- L'assenza completa di cavi e fili.
- Il costo limitato derivato dall'uso di una tecnologia semplice ed economica.
- La completa automazione: i dispositivi stabiliscono in modo automatico una connessione tra loro, senza che l'utente debba far nulla.

3.2.1 Il funzionamento del Bluetooth

È stata la **Ericcson** a sviluppare questa nuova tecnologia, introducendo l'uso delle *onde radio*, alla base della connessione definita **PAN** (*Personal Area network*) oppure **Piconet**: con questi termini ci si riferisce ad una Rete in cui l'utente ha la possibilità di spostarsi liberamente, senza l'ingombro dei cavi di connessione, e in cui ogni periferica può essere spostata senza perdere il collegamento alla Rete stessa.

Lo *standard Bluetooth* prevede l'utilizzo di una banda radio a 2.4Ghz con una velocità di traserimento dati, nell'ultima versione 4.0, di circa 24 mbps al secondo.

È interessante conoscere quale sia il raggio di azione di questo standard.

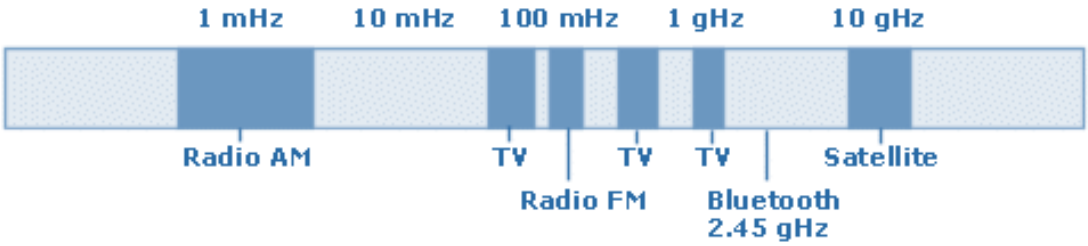
Varia, a seconda della potenza dell'*antenna radio* installata nei dispositivi:

- Fino a 10 metri con antenne di potenza 0dB.
- Fino a 50 metri con antenne di potenza 10dB.
- Fino a 100 metri con antenne di potenza 20dB.

Per quanto possa apparire conveniente utilizzare una potenza che assicuri contatto a grande distanza, in realtà, contemperando gli svantaggi (*maggior consumo* della batteria dei dispositivi e, soprattutto, maggiore probabilità di *interferenza* con altri dispositivi *Wireless*), molti produttori preferiscono produrre strumenti che si connettono entro i 10 metri di raggio.

Altro elemento importante: considerato che il *segnale radio* inviato da questo *standard* è molto debole (pari a circa un MilliWatt), non interferisce con altri apparecchi a frequenze radio, come i cellulari o la televisione. In ogni caso, il segnale *Bluetooth* si propaga attraverso i muri; puoi collegare, quindi, anche dispositivi che sono in stanze diverse (la funzionalità cambia, comuqnue, in base a diversi fattori: il segnale si propaga molto meglio tra muri di legno che tra muri di cemento, ad esempio).

Figura 12 | L'allocazione internazionale delle frequenze radio



Se, invece, stai pensando che un limite di questo *standard* possa essere l'*interferenza* tra i collegamenti di diversi dispositivi vicini tra loro, ti assicuriamo che questo non avviene… quasi mai!

In effetti, il sistema è tarato in modo che le interferenze siano davvero un accidente: il cosiddetto *Spread-Spectrum Frequency Hopping* consente ad ogni dispositivo:

- Di usare fino a *79 frequenze* (in modo casuale e all'interno di un range specifico),
- Cambiare la *frequenza* fino a *1600 volte al secondo*.

È davvero molto improbabile che due dispositivi trasmettano sulla stessa frequenza allo stesso tempo e, in ogni caso, l'*interferenza* durerebbe una frazione millesimale di secondo.

L'impiego di questa tecnologia teoricamente non ha limiti;

Vediamo alcune applicazioni:

- **Collagamento wireless** (*senza fili*) tra *mouse* e tastiera, tra computer e stampante e tra computer e cuffie.
- **Trasferimento file** tra computer e PDA (*Personal Digital Assistant*, da noi sono conosciuti come *palmari*), tra computer e *smartphone* e tra computer e fotocamera digitale
- **Condivisione** dei *file* tra due computer collegati.

Altre applicazioni, oltre che comode, sono molto utili anche per la nostra sicurezza (non solo informatica): molte auto, ad esempio, già offrono il servizio di connessione *Bluethoot* tramite cui puoi ascoltare la musica che hai scaricato sul tuo *smartphone* e, soprattutto, utilizzare il vivavoce per rispondere al telefono, senza preoccuparti di tirarlo fuori dalla giacca o dalla borsa. Di questi esempi, probabilmente, sai già.

Per darti il senso di quanto possa ancora svilupparsi l'applicazione di questo sistema di connessione, te ne facciamo un altro: con **Indoor Navigation**, potrai andare in giro per città ma anche, musei, stadi, ospedali, centri commerciali che, dopo essere stati mappati, potranno essere visitati come puoi vedere nell'immagine di fianco.

Figura 13 | Indoor Navigation

Dovrai solo inserire il posto in cui vuoi andare ed il tuo *smartphone* ti guiderà passo passo. Ma, visto che stiamo trattando questo argomento, questo tipo di strumenti danno vita a nuovi problemi di privacy e sicurezza: per funzionare, il tuo *smartphone* dovrà infatti condividere i tuoi dati.

I protocolli *Bluetooth* e *Wi-Fi* possono essere compromessi e intercettati dagli *hacker* che avrebbero la possibilità di acquisire davvero moltissimi dati! E non solo loro: ti invitiamo a riflettere sul fatto che, qualora strumenti come questi si diffondessero (come ci si può aspettare), una persona sarebbe sempre connessa a un sistema che potrebbe tracciare, senza soluzione di continuità, la sua posizione…

Nokia ha dichiarato di aver mappato circa 50.000 spazi interni per questo strumento che, oltre ad essere una fantastica risorsa per gli utenti, sarà, in ogni caso, un altro campo di sfida per gli esperti di sicurezza informatica.

Come attivare il bluetooth sul tuo PC

Prima di iniziare, devi accertarti che il tuo computer integri il supporto alla rete *Bluetooth*.

Se utilizzi Windows 7, clicca sul pulsante **Start** di Windows, seleziona con il pulsante destro del *mouse* la voce **Computer** (nella colonna di destra) e clicca sulla voce **Proprietà** nel menu che compare.

Se utilizzi una versione di Windows pari o superiore a Windows 8 (qui il *menù Start* non è più previsto),

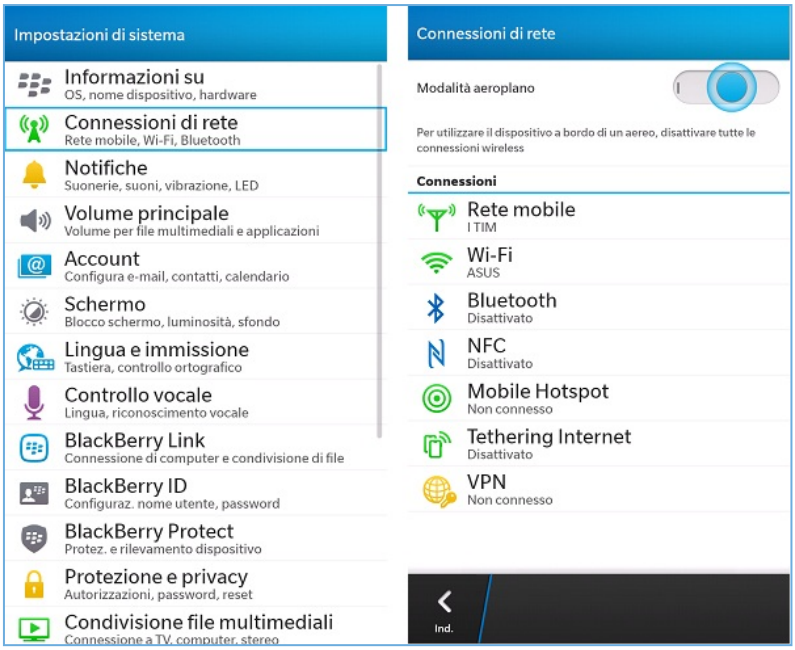
1. Passa con il *mouse* nella parte *in basso a destra* dell'interfaccia (non devi cliccare): si apre un menù;
2. Clicca su **Impostazioni**.
3. Seleziona **Modifica impostazioni del PC**.
4. Vai sul *menu Wireless*; di qui, se disponibili, potrai attivare o disattivare le opzioni *Wi-Fi* e *Bluetooth* (è possibile attivare anche la *modalità aereo* che consente di tenere il PC acceso anche durante i voli, evitando ogni possibile interferenza con i sistemi del veivolo).

Figura 14 | Modalità aereo

Attivare e disattivare il *Bluetooth* negli *smartphone* è molto semplice. A seconda delle piccole differenze tra i vari supporti:

1. Accedi a **Impostazioni di sistema**.
2. Digita su **Connessioni di rete**.
3. Digita su **Bluetooth** per attivarlo o disattivarlo.

Figura 15 | Attiva/disattiva *Bluetooth* sugli *smartphone*



Nel caso in cui il tuo PC non supporti la rete *Bluetooth*, puoi rimediare investendo pochi euro per acquistare un **adattatore Bluetooth USB**.

Si tratta di particolari *penne USB* acquistabili in qualsiasi negozio di elettronica a 15-20 euro che permettono di aggiungere il supporto *Bluetooth* ai PC che ne sono sprovvisti.

Figura 16 | un adattarore Bluetooth USB

Per abilitare il *Bluetooth* sul PC, collega l'adattatore ad una delle prese USB del computer. Quando colleghi la *pennetta* per la prima volta, aspetta qualche istante: l'*installazione dei driver* necessari per far funzionare il dispositivo partirà automaticamente.

Conclusa l'installazione, verifica che tutto sia andato come previsto:

1. Nell'area di notifica deve esservi l'icona del *Bluetooth*
2. In **visualizza connessioni di rete**, controlla che fra le connessioni disponibili ci sia anche la **Connessione di rete Bluetooth** attiva.

Se il tuo computer dispone del *Bluetooth integrato*, per **attivarlo** cerca e premi il tasto della tastiera del tuo PC su cui è stampato sopra il simbolo (una "B" stilizzata).

Figura 17
Icona *Bluetooth*

In alcuni casi, il tasto per **accendere il Bluetooth nel PC** è associato ad altre funzioni e quindi per usarlo devi tenere premuto il tasto **Fn** (dove supportato: sulle tastiere del Mac Apple, per esempio, questo tasto non è previsto).

Figura 18 | Tasto FN

È possibile che, al posto del tasto, soprattutto nei primi computer che supportavano il sistema, ci sia una *levetta* con scritto *Bluetooth* o *Wireless* che devi spostare su **ON** (di solito, c'è una piccola luce accanto alla levetta che segnala l'attivazione della

funzione). In ogni caso, le posizioni di tasti e levette variano da un computer all'altro.

Se utilizzi un portatile che non è collegato ad una fonte di elettricità, appena hai finito di scambiare i *file*, disattiva il *Bluetooth* (premendo il tasto sulla tastiera o spostando la levetta su **OFF**): consuma molta batteria!

Come comunicano i dispositivi Bluetooth

Impara questi termini:

- **Modalità di rilevamento**. Un dispositivo *Bluetooth* invia un *segnale* che consente ad altri dispositivi *Bluetooth* vicini di *vederlo*.
- **Ricerca**. Così si chiama il processo in base al quale un dispositivo *Bluetooth individua* un altro dispositivo *Bluetooth* che sta inviando un segnale in *modalità di rilevamento*.
- **Associazione**. È il processo in base al quale due dispositivi *Bluetooth* stabiliscono un collegamento tra loro per la prima volta, utilizzando una *passkey*.
- **Passkey** o *passcode* o *codice di associazione*, è costituita da una serie di numeri univoci (è una *password*, in sostanza) che consentono a due dispositivi *Bluetooth* di comunicare tra loro in modo sicuro.

Per avviare il trasferimento di un *file* dal computer allo *smartphone* o viceversa, si tratta di associare i due dispositivi, autorizzando il collegamento su uno di essi e scegliendo i documenti da scambiare: segui le indicazioni a video.

Ci sono altre tecnologie che si basano sullo scambio dei *file* senza fili: il sistema **NFC** (*Near Field Communication*) consente di scambiare molte informazioni, anche riservate (come un numero di conto bancario).

Con questo sistema, infatti, si sta cercando di trasformare uno *smartphone* in una *carta di credito* o in un *badge*, che possa funzionare solo avvicinandolo ad un lettore come quello in figura, per rendere le nostre transazioni ancora più comode e veloci.

Figura 19 | Il sistema NFC

4. LA SICUREZZA DELLE COMUNICAZIONI

4.1 La posta elettronica

L'e-mail (posta elettronica) è uno dei mezzi di comunicazione più diffuso. Pratica e veloce, la utilizziamo tutti i giorni, sia a lavoro che nella vita privata, per comunicare con tutti, ovunque.

Non è il caso di soffermarsi troppo sulle funzioni di base, essendo oramai uno strumento conosciutissimo; in breve accenniamo al fato che, attivando una casella di posta elettronica, puoi:

- **Inviare** e **ricevere messaggi** a tutte le persone che, a loro volta, ne hanno una, che tu conosci. La tua comunicazione sarà recapitata al o ai destinatari in qualche secondo, indipendentemente dal fatto che si tratti di vicini di casa o di una persona che vive dall'altra parte del mondo.
- **Inviare** e **ricevere file** di ogni tipo (documenti, immagini e musica). I file inviati per email si chiamano *allegati*.
- **Inoltrare messaggi**. Se vuoi girare una mail ricevuta da un tuo amico ad un altro, non deve riscriverla, ti basta utilizzare il comando **Inoltra**.

Non ci sono limiti temporali per l'invio (puoi scrivere a qualsiasi ora del giorno e della notte) e non ci sono spese per il singolo invio: l'unico costo da sostenere è quello per la connessione a *Internet* o per un programma di posta elettronica specifico che preveda un canone (considerato che, nella normalità dei casi, il servizio è offerto gratuitamente – anche se, a questo punto, dovrebbe essere molto chiaro che i tuoi dati personali hanno un valore molto stimato e utilizzabile per chi gestisce questi servizi online).

Requisiti per l'utilizzo della posta elettronica

Per utilizzare la posta elettronica, è necessario disporre di tre elementi:

- Una **connessione Internet**;
- Un **software di posta elettronica** o un **servizio equivalente disponibile online**. Nel primo caso, è necessario acquistare un programma (un **client di posta**, vedi di seguito) e configurarlo sul proprio PC. Nel secondo caso, si utilizzano particolari programmi online (**client web-mail**) eseguiti direttamente dai siti Web che offrono il servizio: sono i siti più popolari ed utilizzati (**Gmail, Windows Live Hotmail, Libero Mail** o **Yahoo! Mail**, per fare qualche esempio), grazie ai quali non devi configurare nulla sul tuo PC e, soprattutto, puoi accedere alla tua casella di posta elettronica da ogni PC connesso ad Internet (ecco perché è così importante chiudere la sessione quando finisci di controllare la tua posta elettronica su un PC pubblico: ci

vanno in moltissimi e, se la tua sessione è ancora aperta, la persona che viene dopo di te può accedere tranquillamente alla tua posta!).

- **Un indirizzo di posta elettronica**.

Affronteremo integralmente l'argomento nel modulo dedicato alla comunicazione online. Qui ci soffermiamo sull'incidenza che questo strumento può avere per la nostra privacy e la nostra sicurezza.

4.1.1 La vulnerabilità della posta elettronica

Essendo così diffuso, questo servizio è esposto a diverse minacce, che possiamo suddividere in due gruppi principali:

- Infiltrazioni *malware*: gli allegati sono lo strumento più utilizzato per diffonderli.
- Posta indesiderata: considerati i costi minimi, la email è molto utilizzata da chiunque voglia far conoscere, presentare e soprattutto vendere qualcosa; è molto facile, quindi, che giornalmente, tu riceva email da persone o aziende che non conosci e a cui non hai mai dato il tuo indirizzo né l'autorizzazione a inviarti comunicazioni.

Proteggere la propria casella di posta elettronica da questo tipo di comunicazioni è divenuta una necessità per tutti.

Sia i programmi che i servizi di posta elettronica online includono strumenti per *filtrare* messaggi di posta indesiderata: analizzano il contenuto dei messaggi ricevuti e spostano i messaggi sospetti in una speciale cartella **Posta indesiderata**, in cui è possibile visualizzarli o eliminarli in qualsiasi momento.

Nel caso in cui un messaggio di posta indesiderata dovesse oltrepassare il filtro e arrivare nella casella della posta in arrivo, i programmi di posta elettronica consentono di *segnalare* quel messaggio: i futuri messaggi provenienti dallo stesso mittente verranno automaticamente spostati nella cartella **Posta indesiderata**.

Si parla diffusamente di questo argomento nel modulo dedicato alla comunicazione online.

Ecco di seguito alcuni consigli utili per ridurre al minimo il problema di ricevere posta indesiderata:

- Comunica il tuo indirizzo di posta elettronica solo a persone fidate ed evita di pubblicarlo in aree pubbliche di Internet (come su un social, ad esempio).
- Quando usi un servizio online (fai un acquisto, ad esempio) leggi l'informativa sulla privacy per verificare che non sia prevista la divulgazione

del tuo indirizzo ad altre aziende partner: spesso puoi scegliere se lasciare questa libertà o meno al gestore del sito.

- Lo ripetiamo ancora: la prima causa di diffusione dei virus tramite email è l'esecuzione degli *allegati*.

Tra breve vedremo qualche altro consiglio pratico, parlando di *spam*.

4.1.2 Client di posta

Il termine **client** (cliente) viene utilizzato perché anche il servizio email, come molti altri in Internet, si basa su un'architettura **client-server**:

- Il **client** si occupa della composizione, lettura/ricezione e trasmissione,
- Il **server** si occupa della raccolta/smistamento dei messaggi verso altri *server* o i *destinatari finali*.

Come abbiamo accennato, a differenza dei servizi di posta online, i **client di posta** devono essere configurati su un PC, secondo le relative istruzioni.

C'è una funzione che può indurre a scegliere un **client** piuttosto che un servizio online: se scarichi un programma di posta, puoi impostare e, quindi, utilizzare più *account*, ognuno dei quali avrà il proprio indirizzo e le proprie credenziali. Ecco perché questo sistema è molto usato dalle aziende che, tramite lo stesso programma, possono far utilizzare a tutti i propri collaboratori email personali ma settate in maniera univoca e tutte controllabili.

Ogni **client** ha particolari funzioni e accessori.

Tra i più diffusi spiccano Outlook Express o Windows mail, preinstallati, nella versione base, su tutti i sistemi operativi Microsoft.

4.1.3 Lo spam

Tema discusso e articolato, lo spam è uno dei simboli (in negativo) dell'era della comunicazione digitale.

È molto curioso l'origine del termine: sembra sia stato preso da una delle cervellotiche scenette tipiche del *Flying Circus* dei *Monty Python*, un gruppo di comici davvero *British*, in voga negli anni settanta: due clienti chiedono cosa ci sia per colazione e l'originale cameriera fa un elenco di pietanze in cui c'è sempre *spam* (si tratta di una marca di carne in scatola); dice così tante volte *spam* che non si capisce nulla del menù!

Guarda il video

Con questo termine, ci si riferisce al **disturbo** arrecato da terzi alla nostra comunicazione, messo in atto mediante l'invio di grandi quantità di messaggi elettronici non richiesti, tramite Internet.

Lo *spammer* è colui che invia, tutte assieme, tantissime email a scopo pubblicitario, senza alcun consenso da parte del destinatario, anche per conto di terzi: ci sono molte aziende che fanno questo lavoro!

Quante sono le email spam?

Non è così semplice fare delle stime, peraltro in continuo aumento. Per darti un'idea, ti diamo comunque dei dati:

- più di 2 miliardi di persone scrivono 144 miliardi di email al giono. Il 70% sono spam!
- Il 50% di spam è inviato da o per conto di case farmaceutiche.
- Il 16% è relativo a prodotti sessuali.
- Il 15% tratta articoli da regalo.
- La restante percentuale è divisa tra mutui e prestiti e altri prodotti commerciali.

Quello che è importante comprendere è che non stiamo parlando solo di un fastidio più o meno sopportabile ma di un danno economico non di poco conto. Pensa, infatti a:

- il **tempo** perso dai destinatari per scaricare, verificare e cancellare il messaggio,
- i **costi** sostenuti dagli ISP per la gestione della banda e dai destinatari che pagano la bolletta per scaricare comunicazioni inutili, quando non dannose.

Ecco alcune semplici regole da seguire se non si vuole essere spammati:

- **Non pubblicare il tuo indirizzo e-mail in pagine web**. Un esempio pratico? Se lavori in un'azienda e tu ed i tuoi colleghi avete tutti una mail personale, conviene pubblicare solo mail generiche (*info@azienda.it*) piuttosto che tutte quelle effettivamente funzionanti. Se gestisci un blog o hai un profilo su un *social*, ti consigliamo di non pubblicare il tuo indirizzo email. Se proprio devi farlo, inseriscilo come *immagine*: i *software* degli *spammer* alla ricerca di indirizzi non lo vedranno, le persone interessate a scriverti si.

- Anche se partecipi a **forum, chat o newsproup**, non è necessario indicare il tuo indirizzo, a meno che tu non voglia essere contattato in privato dagli altri utenti.

- Uno dei trucchi più utilizzati dagli *spammer* per indurti a rispondere e verificare che, in effetti, il tuo indirizzo sia un valido bersaglio, è quello di

inserire nei messaggi false opzioni di cancellazioni (del tipo *Se non vuoi ricevere altre mail da noi, clicca qui*). **Non rispondere mai, non serve protestare**.

- **Non inserire l'indirizzo e-mail nel browser**. Nel modulo dedicato alla navigazione online, vedremo come i browser consentano di memorizzare i propri dati personali, per non doverli riscrivere ogni volta che, online, ne abbiamo bisogno per iscriverci da qualche parte o fare qualche acquisto. La funzione è molto *comoda* ma devi sapere che questo è uno degli strumenti più attaccabili da chi è alla ricerca di indirizzi da bersagliare.
- Ricordati di **usare e fare usare sempre la *copia carbone nascosta***. Quando devi inviare lo stesso messaggio a più persone, scegli sempre l'opzione di invio che ti consente di non far vedere tutti gli indirizzi dei destinatari.

Oltre a prendere le buone abitudini appena descritte, ci sono degli strumenti che possiamo utilizzare per bloccare lo spam o, meglio, per **filtrarlo**.

Esistono appositi programmi (denominati, appunto *antispam*) che utilizzano diversi metodi per riconoscere e bloccare le email indesiderate. Anche tutti i fornitori di servizi di posta elettronica offrono servizi specifici di filtraggio. Nel modulo dedicato alla comunicazione online, vedremo come impostare questi filtri.

Qui ci soffermiamo sul funzionamento teorico dei metodi impiegati. Sono tre:

- **Statico**. I programmi che utilizzano questo tipo di filtro confrontano il messaggio in arrivo con un *elenco di parole chiave*, impostate dall'utente. Se il messaggio contiene una di queste parole, viene classificato come spam e spostato automaticamente in un'apposita cartella. È facile comprendere quale sia il problema di questo sistema: un messaggio che non è spam può essere catagotato in questo modo se contiene una delle *parole chiave* impostate.
- **Euristico**. Questo sistema è, invece, a carico dell'amministratore del *software* antispam che, per tenere efficiente il prodotto, deve continuamente aggiornare il database delle *parole chiave*. Quando arriva un messaggio, il *software* verifica se, al suo interno, ci sono una o più delle *parole chiave* nel proprio database. Il risultato di questa analisi è un *valore numerico* che, se supera una certa soglia, classifica il messaggio come spam.
- **Bayesiano**. È il sistema più completo e, quindi, più complesso. In sostanza, il risultato dell'analisi è un calcolo probabilistico che va oltre il mero inserimento o meno di una *parola chiave*: anche se il messaggio contiene parole normalmente *segnalate* (come, ad esempio, *soldi* e *guadagno*),

potrebbe non essere filtrato come spam se l'incidenza di queste parole sul resto del testo non è significativa.

Lo spam è il metodo classico tramite cui maleintenzionati inondano le caselle di posta di messaggi che sono formattati e sembrano effettivamente inviati da Enti di una certa rilevanza, in modo tale indurre i destinatari a comunicare i propri dati. Nel modulo dedicato ai fondamenti dell'ICT abbiamo fatto l'esempio delle mail inviate *per conto* di Poste Italiane.

È il cosiddetto *phishing*. Abbiamo ripetuto la cosa porprio perché è uno dei maleware più pericolosi; la regola è sempre la stessa: attenzione e cautela!

4.1.4 Riconoscere Hoaxes e leggende metropolitane

Hoax sta, letteralmente, per *bufala*.

Sono così tante le informazioni che girano in Rete ed è così facile che diventino virali che è sempre bene verificare prima di… credere ai proprio occhi!

Potremmo fare una lunghissima lista di notizie false prese per vere da milioni di persone. Certo, non è una novità: tutti conosciamo lo straordinario caso (siamo nel 1938) di una trasmissione radiofonica prodotta e diretta da Orson Welles in cui si faceva una drammatica radiocronaca dell'invasione in atto di marziani distruttori che, da navi spaziali camuffate da meteore, seminavano morte con i loro raggi implacabili.

La trasmissione fu creduta autentica da moltissimi ascoltatori; ci furono scene di panico collettive, uno si suicidò!

Questo era il potere della radio; immagina, adesso, cosa si può fare con Internet e quante più persone possono essere raggiunte in un attimo, in tutto il mondo.

Si definiscono *leggende metropolitane*, poi, quelle informazioni che, per molti versi verosimili, non sono comunque fondate.

Bufale e *leggende metropolitane* sono diffuse soprattutto tramite email. Hai mai visto o sentito parlare di promesse di denaro in cambio dell'invio di dati personali o di inoltro della comunicazione ai propri contatti? Questo è un buon esempio.

Non c'è un *software* o un metodo che filtra questo tipo di email. Come succede spesso, per non cadere nelle truffe, devi essere accorto e comportarti in maniera diligente; su Internet, questo significa, cercare altre fonti e documentarsi, prima di condividere, rispondere, scrivere ecc.

Oltre alle promesse di denaro di cui abbiamo detto, ci sono, comunque, altri segnali che devono subito insospettirti:

- Si parla di conseguenze gravi o dannose se non si eseguono le istruzioni indicate nel messaggio.
- Si invita a cliccare sull'allegato, in cui si spiega come proteggersi da nuovi *maleware*, non ancora conosciuti dagli *antivirus*.
- Nel corpo del testo del messaggio è scritto a chiare lettere che... *non si tratta di una* bufala!
- Ci sono molti errori di grammatica o di logica nel testo.
- C'è un avviso che incita a rispondere con urgenza.
- L'email è stata inoltrata più volte; puoi verificarlo, vedendo nel corpo del testo, dove sono riportati tutti i dati di ogni invio.

4.1.5 La Pec

Strumento rivoluzionario per la Pubblica Amministrazione e le comunicazioni formali, la posta elettronica certificata (PEC) è lo strumento disciplinato dalla legge italiana che permette di dare a una email lo *stesso valore legale* di una **raccomandata** (garantendo il **non ripudio**).

Il mittente riceve sempre un *avviso di ricevimento* (quindi è sicuro che la comunicazione è andata a buon fine).

Il mittente, se ritiene, può, inoltre, **certificare** e **firmare elettronicamente** o **criptare** il testo e il contenuto della comunicazione.

Funzionamento

Per utilizzare la PEC devi disporre di un'apposita casella:

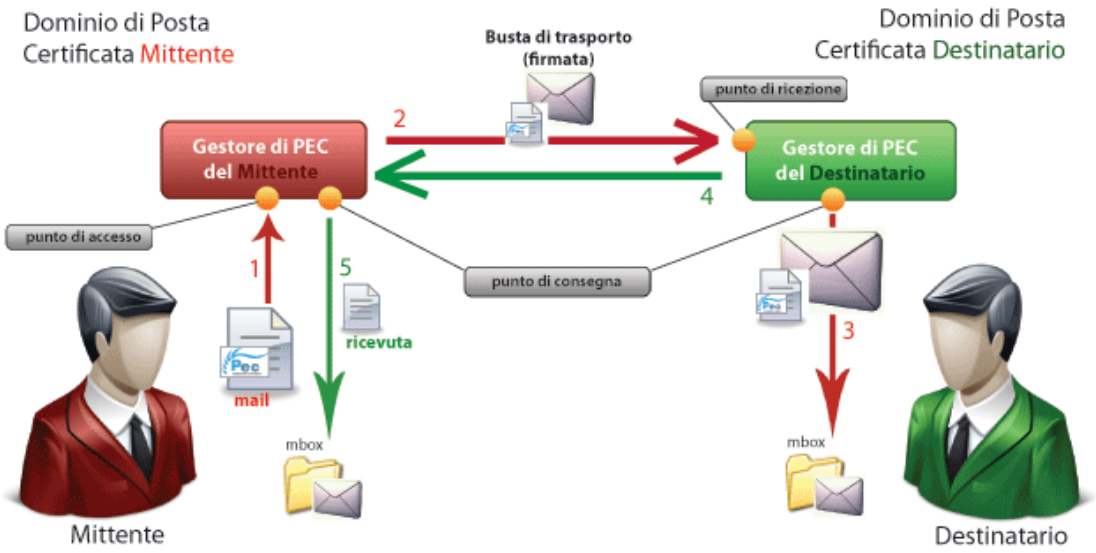
- Fornita dal Governo Italiano: la versione gratuita offre servizi base che ti consentono di dialogare in modo sicuro e certificato con la Pubblica Amministrazione; in questo caso si parla di **CEC-PAC**: è un canale di comunicazione chiuso ed esclusivo tra Pubblica Amministrazione e cittadino. Non sono, infatti, previste comunicazioni al di fuori di tale canale, per esempio tra cittadino e cittadino o nelle relazioni tra realtà aziendali, nei rapporti con banche, clienti e fornitori.
- Fornita a pagamento da gestori autorizzati; in questo caso, potrai comunicare con tutte le caselle di posta elettronica.

Tutto il sistema è gestito dall'*Agenzia per l'Italia Digitale*.

Il principio alla base del sistema è, quindi, la certezza legale dell'**invio** e della **ricezione** di un messaggio. Questa certezza è garantita da un meccanismo complesso solo a livello teorico:

1. Quando invii una PEC, il *gestore del mittente* ti fornisce una *ricevuta* che ha valore legale circa l'avvenuta (o mancata) trasmissione del messaggio, con l'indicazione del momento in cui la comunicazione è stata inviata.
2. Il *gestore della casella PEC del destinatario*, dopo aver depositato il messaggio nella casella di **posta arrivata** del destinatario, ti fornisce una *ricevuta di avvenuta consegna*, con l'indicazione del momento in cui tale consegna è avvenuta. Il destinatario non visualizza la tua comunicazione ma un *messaggio automatico* generato dal tuo gestore, che contiene due allegati: la tua email originale (con gli eventuali allegati) e un file di testo che contiene le stesse informazioni della *notifica di invio* che hai ricevuto tu (ID del messaggio, luogo data e ora di invio, email del destinatario, oggetto).

Figura 20 | Il funzionamento della PEC



L'attuale normativa prevede che i gestori conservino per trenta mesi tutte le ricevute di invio e ricezione. In caso di smarrimento, è possibile quindi richiederle direttamente a loro.

Come avrai compreso, la casella di posta funziona come quelle standard: ciò che cambia è il sistema di monitoraggio e registrazione delle comunicazioni e l'autorizzazione dei gestori: secondo la legge italiana (D.P.R. n. 68/2005 e dalle successive regole da esso previste, dal Codice dell'Amministrazione Digitale, Decreto legislativo n. 235/2010), infatti:

- I gestori che erogano il servizio devono essere accreditati;
- Devono essere usati *domini dedicati*;
- Ogni gestore deve sottoporsi a test d'*interoperabilità*.

Puoi inviare una PEC anche ad un destinatario che non abbia, a sua volta, una casella di posta certificata. In questo caso, anche se genererà gli avvisi di

avvenuta/mancata consegna (e lettura del messaggio), questi non avranno alcun valore legale.

Vantaggi della PEC

Questo servizio, quindi, sostituisce la *raccomandata* tradizionale, con evidenti vantaggi pratici. Oltre a quelli già visti, possiamo segnalare che:

- Si possono inviare *allegati* che hanno lo stesso *valore legale* della comunicazione stessa;
- I messaggi possono essere consultati da ogni dispositivo connesso a Internet;
- Le *ricevute di consegna* hanno piena *validità legale*, anche se il messaggio non è stato letto dal destinatario (su cui grava l'*onere della prova* di non aver ricevuto il messaggio). Il funzionamento è simile alla c.d. *compiuta giacenza* dell'atto giudiziario cartaceo, con la significativa differenza che la notifica *cartacea* si perfeziona dopo 10 giorni dal deposito presso l'ufficio postale, mentre la notifica elettronica è pressoché istantanea;
- I costi sono sicuramente inferiori;
- Sono garantiti qualità e continuità del servizio;
- Esiste una funzionalità che permette, a chi invia, di chiedere una ricevuta di consegna *completa* (che contiene anche una copia esatta, *firmata digitalmente* dal proprio gestore di posta, del messaggio spedito): la ricevuta *completa* fa piena prova del contenuto inviato.

4.2 Communication technologies

Quello che abbiamo visto fin qui ci conferma che, oltre all'*informatizzazione delle procedure*, ciò che maggiormente caratterizza l'ICT è la varietà e l'usabilità degli strumenti disponibili per comunicare online.

Strumenti di comunicazione online

1. Telefonate via Internet
2. Feed RSS
3. Servizi di posta elettronica
4. Utilizzo di blog e podcast
5. Messaggistica istantanea, chat e bots
6. Videochiamate
7. Comunità virtuali

4.2.1 I differenti strumenti di comunicazione istantanea

Il **VoIP** (*Voice over Internet Protocol*) è il sistema utilizzato per telefonare tramite Internet, risparmiando molto rispetto al metodo tradizionale. Gli abbonamenti VoiP assicurano, inoltre, servizi ulteriori: avendone uno, potrai vedere in video il tuo interlocutore, a patto che entrambi abbiate una *webcam* installata.

I **Feed RSS** ti consentono di rimanere sempre aggiornato su tutte le novità pubblicate sui siti o sui blog che visiti più spesso, facendo in modo che ti arrivi una notifica ogni volta che uno di questi siti o blog vengano aggiornati.

Non devi essere tu, quindi, a collegarti ogni volta a questi siti ma saranno loro che ti avviseranno degli aggiornamenti, con un risparmio significativo di tempo.

Figura 21 | Il simbolo dei Feed RSS

Guarda il video. È datato, ma spiega bene come funziona il sistema.

Della **posta elettronica** abbiamo parlato e parleremo ancora molto nei prossimi moduli.

Anche del **blog** parleremo ancora: qui lo presentiamo brevemente, dicendo che si tratta di un sito internet gestito da un utente privato che voglia tenere e condividere con gli *internauti* (si definiscono così tutti coloro che navigano in Internet) una sorta di *diario personale* in cui annota messaggi personali, commenti, idee e opinioni, materiale fotografico e multimediale. È uno strumento molto utilizzato dai più giovani.

Con il termine **podcast** si indica un archivio messo a disposizione dell'utenza abbonata a determinati servizi. Ogni utente può scaricare notizie in formato audio e video. La lettura dei documenti è assicurata da un apposito programma chiamato *feed reader*. È uno strumento molto utilizzato dalle testate giornalistiche online.

Con il sistema denominato **messaggistica istantanea** (*Immediate Message*, IM) due utenti, collegati ad appositi **server di rete**, possono scambiarsi, in tempo reale, *brevi messaggi di testo* che vengono visualizzati immediatamente sia sul dispositivo del mittente che su quello del destinatario. A differenza dell'IM, le **chat** (Internet Chat Relay, ICR), consentono di mettere in contatto più di due utenti, costituendo dunque un luogo di discussione aperto a diverse interazioni.

Abbiamo accennato alle **videochiamate** parlando di VoIP. Si può sfruttare questo servizio anche tramite appositi programmi disponibili online. **Skype** è l'esempio più celebre: che consente di chiamare, chattare e scambiare documenti anche con più utenti contemporaneamente.

Le **comunità virtuali** sono aggregazioni di utenti che utilizzano la Rete per comunicare per discutere, scambiare corrispondenza, condividere materiali multimediali. Attualmente, la più diffusa *comunità virtuale*, o **social network**, è costituita dagli iscritti a **Facebook**.

I materiali condivisi dalla comunità virtuale (foto, immagini, musica, testi), sono normalmente disponibili a tutti: chi pubblica si rende disponibile per contatti personali attraverso una chat oppure un indirizzo di posta elettronica.

Non sempre però la condivisione di contributi è finalizzata a scopi sociali: a volte capita che, su un sito o un social, vengano pubblicati documenti che, volontariamente o meno, danneggiano qualcuno, compromettendone l'immagine. La cronaca riporta molti casi di adolescenti *incastrati* da foto scattate da amici, quando non da se stessi, finite in Rete con conseguenze drammatiche e, purtroppo, non valutate prima.

La diffusione di materiali audio e video riferiti ad una persona è soggetta a specifiche autorizzazioni a tutela della privacy che sono normalmente descritte nei siti dei social e di cui si richiede, all'atto dell'iscrizione, di prenderne visione: il punto è che quasi mai gli utenti si soffermano a leggere queste norme, con la conseguenza che spesso ci si comporta in maniera non corretta.

Parleremo ancora di questi strumenti e del modo migliore per utilizzarli correttamente ed in modo intelligente: quello che ci interessa chiarire qui è che i nuovi modi di comunicare online hanno determinato un sostanziale cambiamento, a livello socioculturale, del modo di conoscere e farsi conoscere, introducendo modalità che, pur se molto efficaci, lasciano aperte molte falle e molti quesiti su temi determinanti come quelli che stiamo discutendo in questo modulo (privacy e sicurezza).

4.2.2 Vantaggi e svantaggi della comunicazione istantanea

L'uso di programmi di messaggistica istantanea, videochiamata o video chat e social networks ha innegabili *vantaggi*:

- Permette la comunicazione a distanza tra due o più utenti che possono trovarsi in diversi luoghi, come in due uffici, in due città o in due stati,
- La comunicazione è istantanea,
- Velocità di condivisione di dati (foto, *file* o documenti),
- Economicità, in quanto non prevedono una spesa o un costo ulteriore a quello di una normale connessione a Internet,
- Permettono di arricchire la comunicazione con *emoticon* e *animoticon*, che permettono di esprimere i propri stati d'animo,
- La videochiamata, oltre ad arricchire sostanzialmente la comunicazione, consente anche a non udenti di interagire a distanza.

Non possiamo sottacere, però, alcuni innegabili *svantaggi*:

- È molto facile fraintendere il tono del messaggio dell'interlocutore,
- La comunicazione istantanea permette di manipolare la comunicazione: in questa maniera si possono fare scherzi ma anche, mentire, truffare ecc.,
- Durante le videochiamate, non è possibile *nascondere* il luogo da cui viene effettuata o ricevuta la chiamata: questo elemento può essere utilizzato illecitamente, da chi avesse cattive intenzioni.

Oltre ai vantaggi e agli svantaggi pratici, è importante considerare anche l'impatto psicologico e sociale che questi esercitano su coloro che ne fanno uso.

L'uso di questi programmi consente una comunicazione *allargata* (che coinvolge, cioè, un gran numero di persone nello stesso momento); le persone coinvolte, molto spesso non si conoscono direttamente ma solo in maniera *virtuale*, potendo vivere a tantissima distanza.

È molto facile, così, non sentirsi mai *soli*. La modalità *a distanza*, inoltre, permette di esprimere con maggiore facilità sentimenti che potrebbero essere inibiti nella relazione diretta, specialmente in persone che sono particolarmente timide.

D'altro canto, l'uso massiccio di questi strumenti ha controindicazioni chiare, come la cosiddetta *dipendenza da internet* (IAD, *Internet addiction disorder*).

In un primo momento (*Fase Tossicofilica*) la *dipendenza* è caratterizzata dall'attenzione ossessiva verso temi e/o strumenti online (come il controllo continuo della posta elettronica, la ricerca di programmi di comunicazione sempre più efficaci e moderni, lunghissimi periodi passati in chat, l'accesso continuo ai social network.

In un secondo momento (*Fase Tossicomanica*) si assiste all'aumento del tempo trascorso online accompagnato da un crescente senso di malessere, agitazione, bassa attivazione quando si è scollegati (condizione paragonabile all'astinenza).

L'abuso di Internet può sfociare in un forte danneggiamento della sfera sociale, familiare, affettiva, scolastica e lavorativa. Tienilo sempre presente.

4.2.3 Poisoning

Tra le tantissime cose che è possibile fare sui social, c'è anche l'*inquinamento* dei contenuti. È il cosiddetto **Social Network Poisoning**, tramite cui un maleintenzionato introduce profili artefatti e relazioni inesistenti per contraffare e rendere inaffidabili le informazioni contenute sulle pagine Web del social network.

Non essendo possibile verificare sempre e in ogni momento la veridicità dei profili degli utenti dei social, è possibile imbattersi in utenti parzialmente o completamente falsi (si parla, in casi del genere, di *fake*).

I principali casi di **poisoning** attualmente praticati sono:

- La *sostituzione* e la *simulazione di identità*,
- L'introduzione volontaria di elementi falsi e/o non congrui nel proprio profilo (*profile fuzzing*),
- L'ingresso in gruppi che non hanno a che fare con i propri interessi e relazioni, con il solo intento di fare *rumore* (*social graph fuzzing*).

Soffermiamoci su uno dei fenomeni più gravi che riguardano l'IT Security: la *sostituzione* o *simulazione d'identità*.

In questo contesto, si parla di **ingegneria sociale** (*social engineering*) per riferirsi all'attività di chi si costruisce una identità fittizia al fine di ottenere risultati che non riuscirebbe mai ad ottenere utilizzando la sua identità reale.

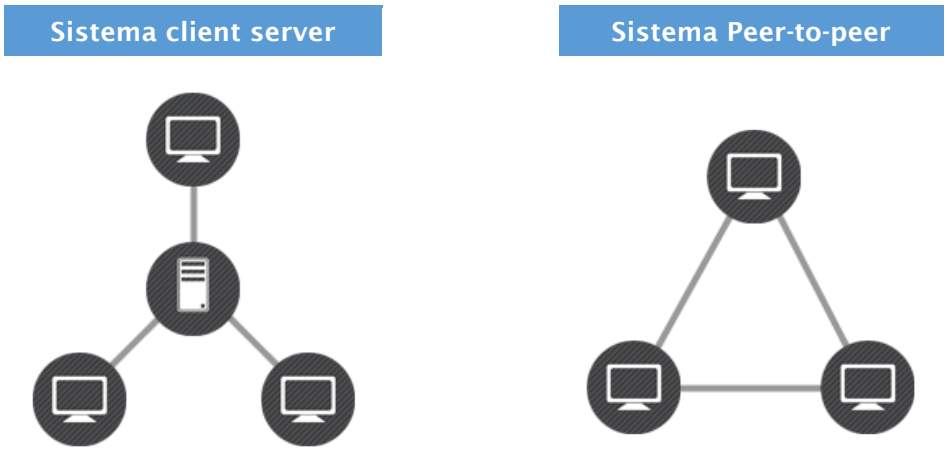
Lo strumento più utilizzato per mettere in atto questa attività è quello delle email contraffatte, tramite cui il maleintenzionato, fingendosi altri, tenta di carpire informazioni personali al destinatario.

Ne abbiamo parlato e ne parleremo ancora. È uno dei punti chiave della tua sicurezza online.

4.3 La tecnologia *peer to peer* (P2P)

Il **P2P** è la tecnologia tramite cui gli utenti connessi a Internet possono condividere i *file* archiviati sul proprio PC, come se fossero in una rete LAN.

Figura 22 | Sistema Client Server (a sinistra) e Sistema Peer-to-peer (a destra)



4.3.1 Che cosa è il P2P

Con il termine **Peer-to-peer** (**P2P**) o **rete paritaria** o **paritetica** si indica una Rete in cui i nodi non sono organizzati e suddivisi in **client** o **server fissi** (in *clienti* e *serventi*), ma sono **equivalenti** o **paritari** (in inglese, *peer*).

Questo significa che ogni nodo può essere, allo stesso tempo, *cliente* e *servente* degli altri nodi (detti *host*) connessi, scambiando con ognuno i *file* archiviati.

Le applicazioni possono essere molto varie (Microsoft e Google, ad esempio, consentono a piccoli gruppi di condividere e lavorare su *file* online) ma questa tecnologia è utilizzata soprattutto per condividere musica, film e tanti altri tipi di *file*, comportando rischi per la sicurezza degli utenti ed elementi di illegalità relativi alla violazione dei diritti di *copyright* dei dati scambiati.

Figura 23 | Le reti P2P più conosciute

4.3.2 I rischi della tecnologia P2P

Vediamo con attenzione quali sono i rischi di questo sistema, per altri versi davvero democratico e universale.

Indipendentemente dall'applicazione utilizzata (eMule, Napster, MIRC ecc.), è impossibile stabilire a priori l'*affidabilità* del nodo da cui stiamo scaricando i dati; in pratica, non sappiamo se il PC dell'utente da cui stiamo acquisendo un film, ad esempio, sia infettato con virus o se l'utente stesso non usi questo sistema per riempirci di *malware* tramite cui accedere, successivamente al nostro PC.

Bisogna tener conto del fatto che, per funzionare, questi programmi richiedono spesso, ad esempio, di disattivare il *firewall*.

I *file* disponibili sulle reti P2P, come accennato, possono includere *software piratato*, materiale sprovvisto di copyright o materiale pornografico. In casi del genere, potresti incorrere in multe o in serie azioni legali.

Infine, questa attività di *upload/download* (denominata *File Sharing*) incrementa la mole di traffico scambiato e il carico di lavoro del nostro computer, rallentandone le prestazioni.

Da quanto detto, deriva che la cosa migliore sarebbe non utilizzare le applicazioni P2P per scambiare *file*.

Nel caso non se ne possa fare a meno, si raccomanda almeno di mantenere aggiornati i programmi *antivirus* e di usare il *firewall*, quando consentito.

5. LA SICUREZZA DELLE RETI

5.1 Le connessioni di Rete

Abbiamo già introdotto il tema nel modulo dedicato ai fondamenti dell'ICT. Riprendiamo il discorso per valutare altri punti di vista.

Intanto, ricordiamo che con il termine generico **Rete** si indica un insieme di entità (oggetti, persone, ecc.) interconnesse le une alle altre.

In informatica, si definisce *Rete* un gruppo di computer collegati fra loro grazie a delle linee fisiche, capaci di scambiare informazioni sotto forma di dati numerici (sono i cosiddetti **valori binari**, cioè codificati sotto forma di segnali che possono assumere due valori: 0 e 1): è questo il sistema tramite cui, in una Rete informatica, è possibile condividere e far circolare elementi *immateriali* tra tutti i dispositivi connessi.

Rete (in inglese, *network*)	**Attuazione di una rete** (*networking*)
Insieme di computer e periferiche connesse le une alle altre: due computer connessi tra loro costituiscono una *rete minimale*.	Strumenti e compiti che permettono di collegare diversi computer tra loro, affinché possano condividere delle risorse, *in Rete*.

Già sappiamo che esistono differenti tipologie di Reti informatiche a seconda della tipologia dei computer connessi, del linguaggio utilizzato per comunicare, del tipo di collegamento, della modalità di trasferimento di dati (circolazione di dati sotto forma d'impulsi elettrici, di luce o di onde elettromagnetiche) e del tipo di supporto (cavo coassiale, coppie incrociate, fibra ottica, ecc.).

Ogni Rete, inoltre, può avere diverse finalità:

- *Condivisione* di risorse (*file*, applicazioni o hardware, connessione a Internet, ecc.),
- *Comunicazione* fra persone (posta elettronica, messaggeria, ecc),
- *Comunicazione* tra processi (fra computer industriali, ad esempio),
- *Garanzia* di unicità e universalità dell'accesso all'informazione (database in Rete),
- I videogiochi multi-giocatore.

I vantaggi del *networking* sono evidenti:

- Diminuzione dei costi, grazie alle condivisioni di dati e periferiche,
- Standardizzazione delle applicazioni,
- Accesso ai dati in tempo reale,
- Comunicazione e organizzazione più efficace.

Altri criteri di classificazione sono:

- *Tipologia dei protocolli* utilizzati (distinguiamo le Reti **peer to peer** da quelle organizzate sul sistema **client/server**),
- *Scala geografica* di riferimento (la LAN, *Limited area network*, ha estensione limitata mentre la WAN, *Wired Area Network*, si estende su un territorio che può essere davvero molto ampio; parlandone nel modulo dedicato ai fondamenti dell'ICT, abbiamo fatto riferimento anche alla MAN, di estensione intermedia).

È chiaro che si sceglie una tipologia piuttosto che un'altra, a seconda delle specifiche esigenze, come ad esempio:

- Dimensione dell'azienda,
- Livello di sicurezza necessario,
- Tipo di attività,
- Livello di competenza amministrativa disponibile,
- Volume di traffico,
- Bisogni degli utenti.

Ci sono, in ogni caso, elementi comuni:

- **Server**: sono i computer che forniscono delle risorse condivise agli utenti in Rete,
- **Client**: sono i computer degli utenti che accedono alle risorse condivise fornite da un server di rete,
- **Supporto di connessione**: ogni Rete ha bisogno di un sistema che colleghi i computer coinvolti,
- **Dati condivisi**: sono i *file* resi accessibili agli utenti collegati,
- **Stampanti e altre periferiche condivise** : file, stampanti o altri elementi utilizzati dagli utenti della rete.

5.1.1 LAN

Analizziamo meglio la Rete LAN, per verificare quanto sia utile connettere dispositivi utilizzati in uno stesso ambiente, lavorativo o ricreativo che sia.

Qualsiasi dispositivo infatti (server, computer, laptop, stampante, televisore, hard disk, NAS) può diventare **nodo** di una LAN e condividere tutte le proprie risorse con gli altri nodi/dispositivi. Se, ad esempio, nella nostra LAN è presente una stampante, tutti gli utenti connessi potranno utilizzarla dalla propria postazione.

Anche le LAN si differenziano tra loro per:

- **Tipologia**, che indica il modo in cui i *nodi* della Rete sono collegati tra di loro (possiamo distinguere tra Rete a *stella*, a *bus*, ad *anello* o *token ring* e *mesh*).
- **Protocolli**, che indicano il modo in cui i dati e le informazioni vengono scambiati tra i vari nodi (come sappiamo, abbiamo il *client-server* e il *peer-to-peer*).

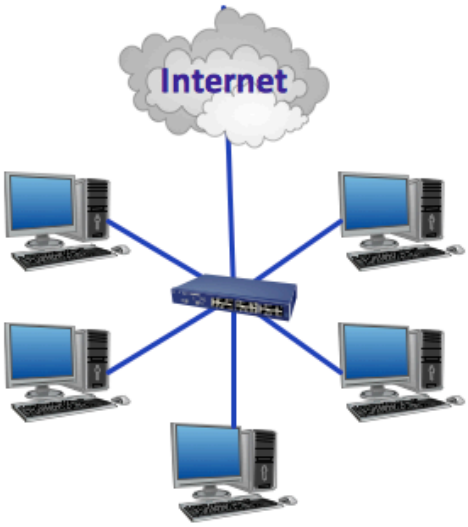
Delle differenze tra il *peer-to-peer* e un'architettura *client-server* abbiamo già detto; vediamo i diversi sistemi di collegamento dei nodi di una LAN.

LAN a stella

È il più elementare esempio di rete LAN. In questa tipologia, c'è un dispositivo *centrale* della Rete (**centrostella**), cui sono collegati tutti gli altri *nodi*. Questa tipologia garantisce che i dati tra i vari *nodi* viaggino abbastanza spediti e rende meno probabile che le comunicazioni siano intercettate.

Dall'altro lato, però, il *centrostella* sarà spesso oberato dal carico di dati da smistare tra i vari client e, in caso di sua rottura, l'intera Rete locale smetterà di funzionare.

Figura 24 | LAN a stella

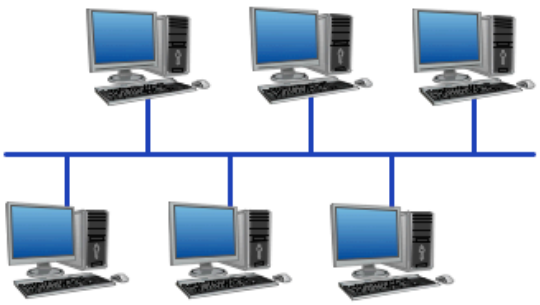


LAN a bus

Tutti i *nodi* collegati sono agganciati direttamente al medesimo *cavo fisico*: è facile e poco costosa da realizzare ma è anche poco affidabile.

I dati che viaggiano sull'unico canale di comunicazione sono infatti facilmente intercettabili da qualsiasi altro *nodo* della Rete stessa e, inoltre, è molto complicato trovare il punto preciso di un eventuale guasto

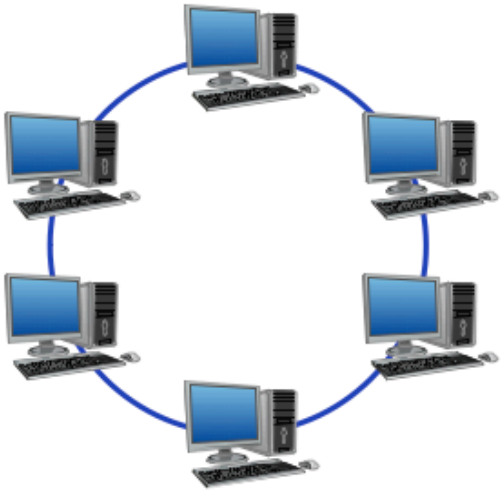
Figura 25 | LAN a bus



LAN ad anello

È un esempio di Rete *peer-to-peer*: tutti i *nodi* possono ricoprire sia il ruolo di *server* che di *client*. Ogni nodo è collegato ad un altro, in fila; l'ultimo si dovrà collegare al primo, chiudendo il cerchio. Il passaggio di dati da un *nodo* all'altro è regolato da un particolare messaggio, detto **token**: un nodo in possesso del *token* è autorizzato a trasmettere dati a uno dei due *nodi* collegati (quello che lo precede o quello che lo segue).

Figura 26 | LAN ad anello



Una volta terminata la trasmissione dei dati, il *nodo* passerà il testimone (il *token*) a un nodo limitrofo: se questo ha dei dati da trasmettere si attiverà, diversamente, passerà subito il token al nodo successivo. Anche questa tipologia presenta problemi di affidabilità: i dati sono facilmente intercettabili e nel caso di rottura di uno dei nodi la comunicazione si ferma.

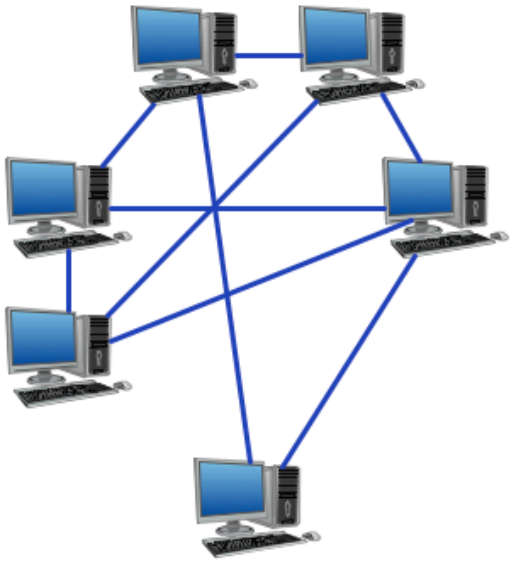
LAN mesh

Anche la LAN *a maglia* è un esempio tipico di connessione *p2p*: non esiste un ordine gerarchico tra i *nodi*, che:

- Possono comportarsi, a seconda dei casi, come *server* o *client*
- Sono collegati ad un numero variabile di altri *nodi*, senza seguire uno schema preciso.

In questo caso, la rottura di un *nodo* non comporta l'interruzione della comunicazione: esisterà sempre un percorso alternativo che permetterà di aggirare l'ostacolo del *nodo* non funzionante e portare a termine la comunicazione.

Figura 27 | LAN mesh



Tutti i sistemi elencati sono **vulnerabili** di attacchi di tantissime tipologie diverse. Normalmente queste reti sono gestite da un *amministratore di sistema* (IT manager) che deve riconoscere la natura di questi attacchi e mettere in pratica le giuste contromisure.

Gli attacchi possono provenire da:

- **Interno**: utenti che fanno parte della Rete ma che non dovrebbero accedere alla totalità dei dati scambiati, potrebbero trafugare o anche solo visualizzare informazioni private, senza autorizzazione;
- **Esterno**: soprattutto se, come nell'esempio indicato in figura 24, la Rete è connessa ad Internet, può essere infettata da qualunque tipo di *malware*, che potrebbero inficiare le prestazioni del sistema;
- **Stakeholder**: aziende, persone, fornitori, clienti con cui l'azienda si confronta quotidianamente, potrebbero accedere e acquisire dati, senza autorizzazione.

Se ci troviamo a gestire una LAN, quindi, per garantirne la sicurezza è necessario pianificare ed attuare una serie di interventi integrati:

- Difesa dei singoli dispositivi connessi alla LAN,
- Protezione della Rete nel suo complesso,
- Protezione dei dati memorizzati nei database.

5.2 Il firewall

Riprendiamo, adesso, il discorso intrapreso sul *firewall*, per vedere come gestire praticamente le diverse opzioni disponibili.

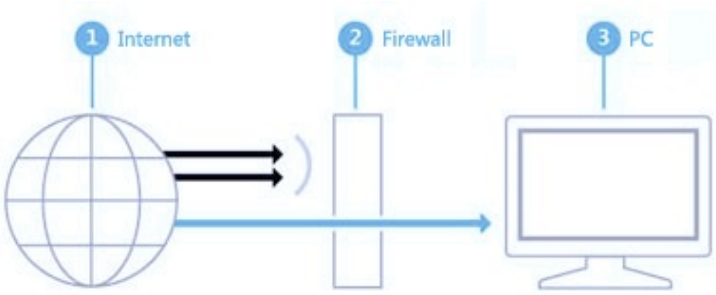
Già sappiamo che, se ben configurato e usato correttamente, il *firewall* è un valido strumento aggiuntivo che impedisce a un virus di infettare il PC prima che venga individuato dall'*antivirus*. Permette, inoltre, di nascondere parzialmente o totalmente il PC sulla Rete, evitando attacchi informatici.

Per comprendere bene come funziona (il *firewall* può essere sia un *software* che un *hardware*), facciamo un esempio molto semplice: è come se questi dispositivi rappresentassero i punti di una *dogana*: controllano, quindi,

- il traffico di Rete che proviene dall'esterno,
- il traffico dei dati generati dal PC e inviati all'esterno,

permettendo soltanto quello effettivamente autorizzato.

Figura 28 | Funzionameto del *firewall*



Per comprendere tecnicamente il funzionamento del *firewall*, dobbiamo fare una breve premessa circa i protocolli che consentono ai computer in Rete di riconoscersi e comunicare.

Facciamo riferimento al protocollo più utilizzato in Internet, il **TCP/IP** (*Transport Control Protocol/Internet Protocol*).

In un network basato sul TCP/IP, ciascun computer:

- é identificato in modo univoco da un *indirizzo IP* (costituito da quattro *ottetti*, del tipo *aaa.bbb.ccc.ddd*),
- Comunica con altri sistemi scambiando messaggi sotto forma di *pacchetti* (detti *datagrammi*).

Affinchè ci sia una comunicazione, quindi, è necessario che, in ogni computer connesso, ci siano due elementi:

- L'*indirizzo IP* che, come un numero di telefono, rende riconoscibile e contattabile il computer da un altro in Rete,
- Una *porta di comunicazione* che serve a individuare l'applicazione usata per la comunicazione stessa e consiste in un *numero* (il numero di porta del servizio *http* è 80, ad esempio).

Una volta instaurata la connessione, il *firewall* inizia a svolgere la sua funzione di *filtro*, analizzando tutti i *pacchetti* che lo attraversano: saranno automaticamente bloccati tutti quei pacchetti che corrispondono al *set di regole* definito dall'utente.

In linea generale, queste regole comportano l'accettazione o il blocco dei pacchetti in transito, sulla base dei loro elementi distintivi, vale a dire *indirizzo IP* e *porta della sorgente* nonché *indirizzo IP* e *porta della destinazione*.

Dal punto di vista del funzionamento interno, i *firewall* possono essere ulteriormente distinti in due gruppi:

- *A filtraggio di pacchetti*, più comuni e meno costosi, esaminano le informazioni contenute nella *intestazione* del pacchetto relativa al protocollo IP e le confrontano con il loro *set di regole* interno, permettendone o bloccandone il transito. Il vantaggio di questi dispositivi, oltre al costo contenuto, è rappresentato dalla velocità; per converso, i punti deboli sono:
    - Una certa vulnerabilità nei confronti di determinati tipi di attacco (come quelli basati sull'IP **spoofing**),
    - Essendoci una *connessione diretta* tra *sorgente* e *destinazione*, una volta che il *firewall* lascia transitare un *pacchetto*, non c'è più alcuna difesa contro ogni successivo attacco portato dallo stesso *pacchetto*.
- *A livello di circuito*. Molto più costosi, forniscono un livello di protezione più elevato poiché esaminano non soltanto l'*intestazione* ma anche il

contenuto dei *pacchetti* in transito, in modo da verificare sempre che il sistema di destinazione abbia effettivamente richiesto la comunicazione stessa.

5.2.1 Attivare il firewall

Vediamo come funziona il sistema su Windows 8.

Microsoft fornisce un apposito *software* (Windows Firewall) attivato per impostazione predefinita, secondo le seguenti opzioni:

- Firewall attivato per tutte le connessioni di rete.
- Blocco di tutte le connessioni in entrata, tranne quelle consentite in modo esplicito.
- Firewall attivato per tutti i tipi di rete (privata, pubblica o di dominio).

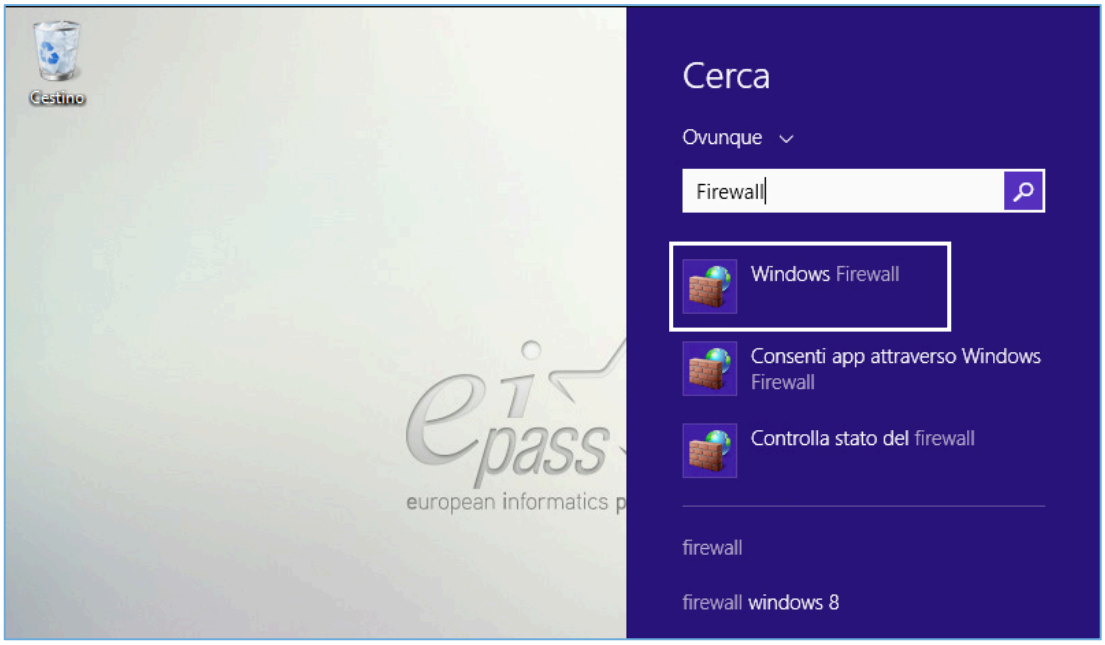
È consigliabile disattivare Windows Firewall solo se e quando decidi di acquisire e installare un altro *firewall*. Vediamo come procedere.

1. Apri Windows Firewall. Per farlo, porta il cursore nella parte in *basso a destra* dello schermo. Non cliccare. Si aprirà il menù che vedi nell'immagine che segue. Clicca su **Ricerca**.

Figura 29 | Attivazione menù Windows

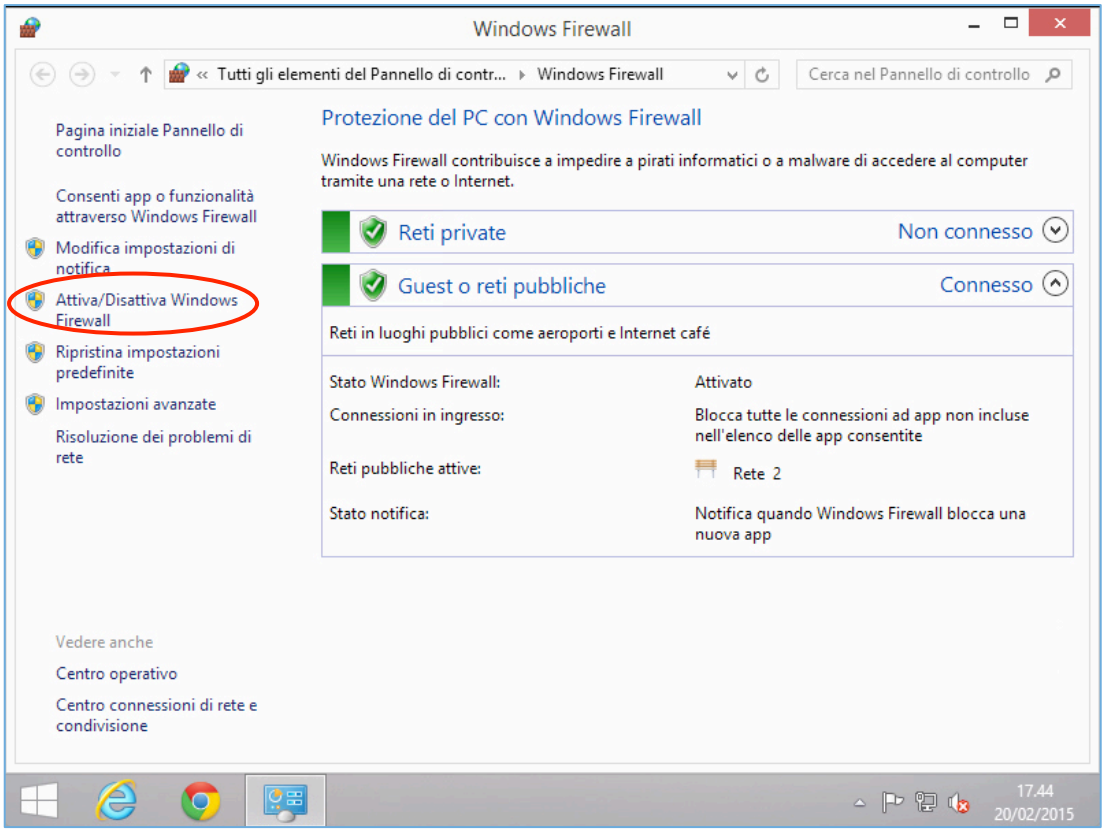
1. Digita **firewall** nel campo di ricerca.
2. Clicca su **Windows Firewall**.

Figura 30 | Attivazione menù Windows



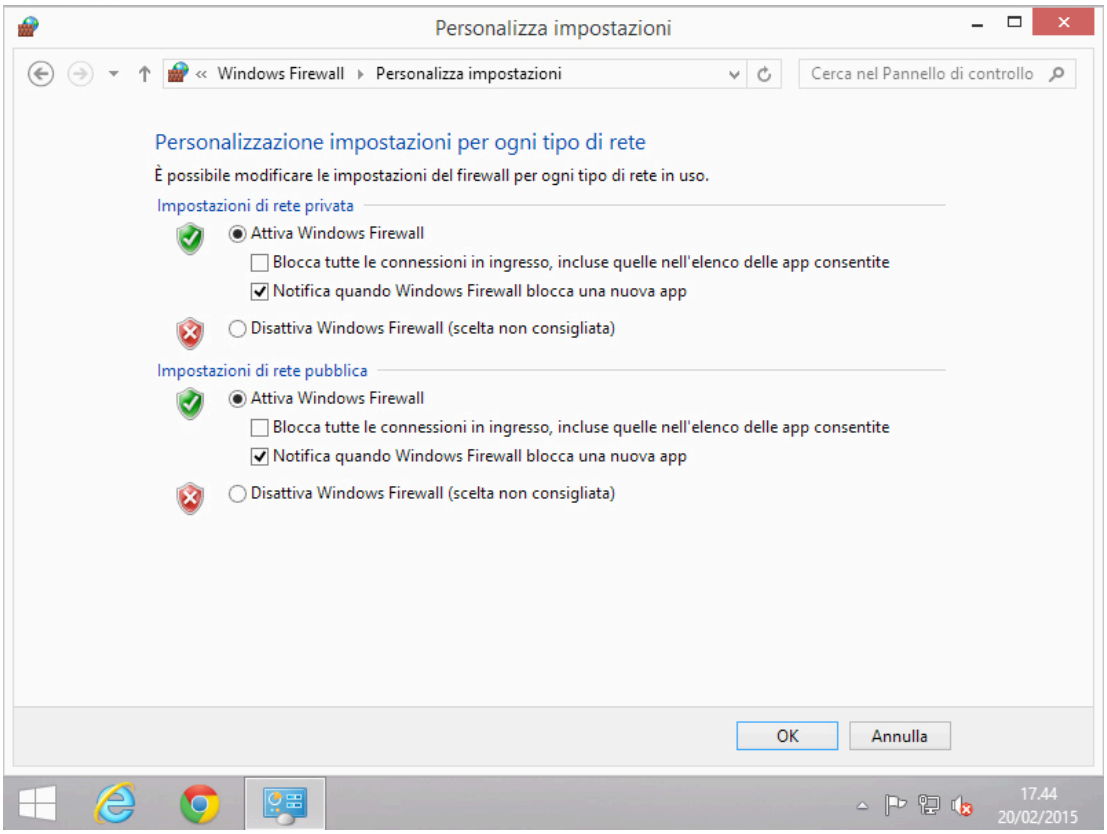
3. Nella finestra che si apre, clicca su **Attiva/Disattiva Windows Firewall**.

Figura 31 | Attivazione menù Windows



4. Nella finestra che si apre, esegui una delle operazioni seguenti:
    - Clicca su **Attiva Windows Firewall** per ogni tipo di rete per cui desideri attivare la protezione e quindi clicca su **OK**.
    - Clicca su **Disattiva Windows Firewall** (scelta non consigliata) per ogni tipo di rete che non desideri più proteggere. Clicca su **OK**.

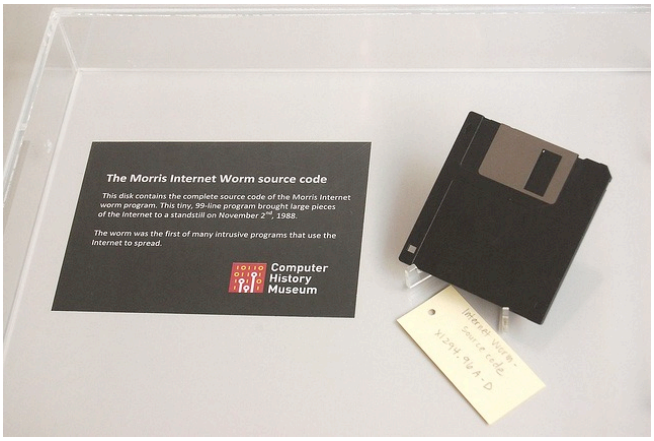
Figura 32 | Attivazione menù Windows



5.3 Le minacce su Internet

Per concludere questa panoramica sul tema della sicurezza, riprendiamo l'argomento delle *minacce informatiche* per conoscere altre regole alla base di un uso sicuro e sempre ragionato del computer e di Internet. Il primo *malware*, conosciuto come *Brain*, fece la sua apparizione nel 1986.

Figura 33 | Un floppy con un virus



Allora i computer erano davvero molto pochi rispetto ad oggi: la propagazione era poi limitata dal fatto che, per infettare un PC, era necessario che vi fosse materialmente inserito un *floppy* infetto.

Sta di fatto che *Brain* costituì una vera ispirazione per gli appassionati di *software* che, da allora, iniziarono a gareggiare per dimostrarsi più bravi degli altri nell'accedere a sistemi governativi o sviluppare programmi capaci di diffondersi rapidamente in tutto il mondo (è il caso del virus *Morris*, finito in un museo, come puoi vedere nella figura precedente).

I primi virus, in ogni caso, non erano molto dannosi (le finalità erano, appunto, goliardiche) ed erano facilmente rimovibili. Si continuò così fino al 2000.

Con il nascere del nuovo millennio, le cose sono cambiate di molto: l'aumento esponenziale di connettività e numero di utenti, ha indotto molti ad utilizzare i malware per fini criminali.

Oggi i numeri sono impressionanti:

- Nei database degli *antivirus* ci sono più di 40.000.000 codici di virus conosciuti.
- Ogni giorno sono messi in Rete fino a 70.000 nuovi virus che occorre analizzare e neutralizzare.

Ciò detto, è ancora più evidente quanto non sia sufficiente affidarsi ad *antivirus*, *firewall*, ecc. per evitare brutte sorprese; piuttosto, è necessario che, quando navighi, usi sempre *cautela* e *buon senso*.

5.3.1 Il furto d'identità

Una delle principali finalità di chi tenta di scardinare le tue difese e accedere ai tuoi dati è quello di… rubarti l'identità!

Avremo modo di approfondire il tema nel modulo dedicato alla navigazione online: qui diciamo che questa fattispecie è emblematica del fatto che tenere un certo comportamento online è il modo migliore per evitare problemi anche gravi (un maleintenzionato che acquisice l'*account* del tuo conto corrente, ad esempio, può fare acquisti indiscriminati usando il tuo *home banking*; se acquisisce i dati del tuo *account* Facebook o di posta elettronica, potrà inviare messaggi a tutti i tuoi contatti, chiedendo qualsiasi cosa e così via).

Riprendiamo quanto visto fin qui per fissare le regole più importanti per evitare brutte sorprese. Le riprenderemo altrove, per approfondire specifici aspetti.

Proteggi le tue transazioni online utilizzando *firewall*, *antivirus* e *antispyware*, e nascondendo la tua connessione wireless domestica. Mantieni aggiornati tutti i *software* (browser compreso) attraverso gli aggiornamenti automatici.

Fai attenzione a offerte troppo vantaggiose, agli avvisi della banca che comunica l'immediata chiusura del tuo conto se non esegui azioni immediate, agli avvisi di vincita di lotteria o ai rifiuti di un incontro di persona per concludere una transazione. Lo scopo di questi messaggi è quello di spingerti a visitare un sito Web fasullo, in cui i gestori possono carpire i tuoi dati.

Crea password complesse, ne abbiamo già parlato. Tieni segreti *password* e *PIN* (numeri di identificazione personale) e non inviarli mai per email o con messaggi istantanei. Devi utilizzare password diverse per ognuno dei tuoi *account*; se utilizzi sempre la stessa, chiunque se ne impadronisca, metterà a rischio tutte le tue informazioni sensibili.

Digita tu stesso gli indirizzi dei siti Web a cui vuoi accedere: se lo fai cliccando su collegamenti contenuti in messaggi in email, SMS, messaggi istantanei o pubblicità pop-up, potresti essere portato su siti legittimi solo in apparenza ma, in realtà, per niente affidabili.

Controlla gli indicatori di protezione delle informazioni dei siti che stai visitando. Se sei in un sito e-commerce e intendi fare un acquisto online, prima di immettere i tuoi dati, verifica che nella barra degli indirizzi, prima del nome del sito, ci sia la dicitura **https** (la **s** sta per *secure*) ed il logo del lucchetto chiuso. Sono indicatori che ti fanno capire che il sito è sicuro.

Usa solo il tuo PC per fare ogni transazione finanziaria. Non pagare, non fare acquisti o altre attività finanziarie su un computer pubblico o condiviso, oppure su dispositivi come *PC portatili* e *smartphone*, che siano connessi a Reti pubbliche wireless. La protezione, in questi casi, non è affidabile.

Usa sempre il buon senso e se hai dubbi di qualsiasi tipo, prima di fare alcunchè, chiedi informazioni ai tuoi genitori, al tuo docente o a un amico che ne sappia più di te.

5.3.2 Spyware

Si definiscono *spyware*, i *software* tramite cui è possibile rubare l'identità degli utenti di Internet. Ne abbiamo accennato brevemente prima. Approfondiamo un attimo il tema, sapendo che, comuqnue, ne riparleremo ancora altrove.

Sono utilizzati per spiare e raccogliere informazioni circa dati e abitudini degli utenti che, inconsapevolmente, hanno scaricato questo tipo di *malware* sul proprio dispositivo. Una volta raccolti, i dati ritenuti interessanti (*password*, *numero della carta di credito, documenti* e così via), vengono inviate via Internet agli utenti designati dai programmatori, che li utilizzeranno per i fini più disparati.

Gli spyware si diffondono in due maniere:

- Possono essere installati automaticamente sul tuo PC, attraverso siti Internet infetti;
- Puoi installarli manualmente (ma in maniera involontaria), scegliendo di utilizzare programmi gratuiti (*software freeware*) che riescono ad infettare PC che non abbiano difese sufficientemente alte.

Come riconoscere la presenza di uno spyware sul tuo PC

Quando un PC è infetto, normalmente si attivano delle azioni che, altrimenti, non si attiverebbero mai. Te ne indichiamo alcune:

- Mentre lavori, **compaiono in continuazione pop-up pubblicitari**.
- **Si sono modificate impostazioni che sei certo di non aver cambiato personalmente e non riesci a risettarle**. L'esempio più classico è la modifica della pagina iniziale del tuo browser. Anche ripristinando la tua preferita, a ogni riavvio torna quella indesiderata.
- **Il tuo browser contiene componenti aggiuntive che non ricordi di aver scaricato**. Succede spesso, ad esempio, che compaiano *barre degli strumenti* che non ti servono o non desideri che, come sopra, anche se elimini, ricompaiono a ogni riavvio del computer.
- **Il computer è lento**. I malware non sono efficienti; non c'è alcuna necessità che lo siano: le risorse che utilizzano per monitorare le tue attività e inviare pubblicità possono, quindi, rallentare il PC e/o provocare errori del sistema operativo.

Prevenire e rimuovere uno spyware

Come per altri virus, anche per gli *spyware* ci sono programmi specifici che consentono di disinfettare il nostro PC: consentono, cioè, di *individuare*, *rimuovere* e/o *mettere in quarantena* la minaccia. Eccone alcuni:

Ad-Aware SE Personal Edition	*Emsisoft Anti-Malware*	*Malwarebytes' Anti-Malware*
HijackThis	*Norman Malware Cleaner*	*Spybot - Search and Destroy*
SpywareBlaster	*Spyware Terminator*	*SUPERAntispyware*

5.3.3 Codice attivo e cookies

Nel modulo in cui tratteremo di navigazione online, avremo modo di parlare diffusamente dei **cookies**.

Introduciamo qui il tema, per la rilevanza che hanno nell'ambito della sicurezza, accennando anche ai *codici attivi*.

Il codice attivo

L'avvento del Web Design, ha reso molto più gradevoli (*frendly*, si dice) i siti, dando la possibilità ai tecnici di inserire specifici codici (**script**) che ne aumentano le funzionalità o consentono di inserire animazioni (un esempio classico, sono i *menù a tendina*).

In italiano, questi *script* si definiscono **codici attivi**.

Il lato negativo della cosa è che i *codici attivi* sono spesso usati dai malintenzionati per eseguire codici *malevoli* sul computer dell'utente.

I codici attivi più diffusi sono **JavaScript** (e altri similari, come *VBScript*, *ECMAScript* e *Jscript*), i **Controlli ActiveX** e **Applet Java**.

Questi codici, quindi, non sono pericolosi in sé ma sono spesso utilizzati per attacchi malevoli.

Il Javascript ed altre forme di codice attivo non sono pericolosi di per sè, ma sono strumenti comunemente impiegati per gli attacchi malevoli. È questo il motivo per cui praticamente tutti i browser consentono di **disabilitarli**, anche se ciò può limitare la funzionalità di alcuni dei siti visitati.

In ogni caso, mentre navighi, se apri il collegamento di un sito Web che non conosci o che ti sembra sospetto, è buona norma disabilitare l'esecuzione di *codici attivo*.

Stesso discorso possiamo fare per le email, dato che normalmente per visualizzare comunicazioni scritte in HTML si usano gli stessi programmi che usano i browser.

I cookies

Mentre navighi in Internet, il tuo computer e/o i siti che visiti, conservano alcune tue informazioni, con la finalità di rendere più veloce e funzionale un tuo eventuale successivo accesso allo stesso sito.

Questo sistema pone delle questioni di sicurezza dei dati memorizzati, soprattutto se valuti il fatto che ce ne sono di due tipologie differenti:

- I **cookies di sessione** memorizzano le informazioni soltanto fino a quando utilizzi il browser; quindi, quando lo chiudi, le informazioni sono automaticamente cancellate.
- I **cookies persistenti** sono immagazzinati sul tuo PC in modo da potere mantenere le vostre preferenze personali. È grazie a questi *cookies* che il tuo indirizzo email appare automaticamente quando apri il tuo *account* di posta elettronica. Ecco perché, se un malintenzionato accede al vostro computer, può ottenere informazioni personali su di te.

Ecco perché, anche se le funzionalità sono molto comode, è meglio eliminare o limitare i cookies, soprattutto se stai navigando su un computer utilizzato anche da altre persone.

Come detto, avremo modo di approfondire il tema.

Sitografia

http://www.treccani.it

http://motherboard.vice.com/it/read/la-storia-dei-primi-sei-anni-di-Anonymous

http://windows.microsoft.com/it-it/windows7/create-a-restore-point

http://windows.microsoft.com/it-it/windows/back-up-files#1TC=windows-7

http://www.windowsphone.com/it-it/how-to/wp8/settings-and-personalization/back-up-my-stuff

http://www.di.unisa.it/~ads/corso-security/www/CORSO-0304/SPAM/testo.htm

www eipass com

info@eipass.com

NUMERO VERDE
800.088.331