NUOVA ECDL

IT Security
V 1.0

Giorgio Mortali – Vania Nanni

SOMMARIO

Finalità del Manuale
Il presente modulo definisce i concetti e le competenze fondamentali per comprendere l'uso sicuro dell'ICT nelle attività quotidiane e per utilizzare tecniche e applicazioni rilevanti che consentono di gestire una connessione di rete sicura, usare Internet in modo sicuro e senza rischi e gestire in modo adeguato dati e informazioni.

Perché sostenere questo modulo?
- Questo modulo certifica la capacità di individuare e comprendere i concetti principali alla base di un uso sicuro della Tecnologia dell'Informazione e Comunicazione (ICT).
- Contiene le competenze per proteggere i propri dati e quelli dell'organizzazione per la quale lavorano.

Al superamento della prova d'esame, il candidato sarà in grado di:
- comprendere i concetti fondamentali relativi all'importanza di rendere sicure informazioni e dati, di assicurare protezione fisica e privacy, e di difendersi dal furto di identità;
- proteggere un computer, un dispositivo o una rete da malware e da accessi non autorizzati;
- comprendere i tipi di reti, i tipi di connessioni e le problematiche specifiche alle reti, firewall inclusi;
- navigare nel World Wide Web e comunicare in modo sicuro su Internet;
- comprendere i problemi di sicurezza associati alle comunicazioni, inclusa la posta elettronica e la messaggistica istantanea;
- effettuare copie di sicurezza e ripristinare i dati in modo corretto e sicuro, ed eliminare dati e dispositivi in modo sicuro.

Modalità di erogazione esame
Automatica mediante piattaforma ATLAS o AICE

Software Suite utilizzata per sostenere l'esame:
- Generica

Domande
IT-Security rel. 2.01 - nuova release
- 36 domande delle quali 35 di carattere tecnico ed 1 pratica
- Disponibile in italiano ed in inglese
- Tempo di esecuzione: 45 minuti
- Superamento esame con il 75% delle risposte esatte

IT-Security rel. 1.0 - disponibile fino al 31 luglio 2016
- 32 domande delle quali 30 di carattere teorico e 2 pratiche
- Disponibile in italiano
- Tempo di esecuzione: 45 minuti
- Superamento esame con il 75% delle risposte esatte

Questo Manuale
Questo manuale non vuole essere solo di aiuto al conseguimento della **Certificazione NUOVA ECDL IT Security – Sicurezza Informatica** ma cerca di offrire delle informazione in più che riteniamo utile per l'utente di tutti i giorni

Questo libro nasce per fornire un supporto a chiunque voglia conoscere, studiare e approcciarsi ad un uso sicuro dell'ICT nelle attività quotidiane e per utilizzare le tecniche e le applicazioni rilevanti che consentono di gestire una connessione di rete sicura, oltre ad usare Internet in modo sicuro e senza rischi e gestire in modo adeguato dati e informazioni.

In particolare è stato pensato come un manuale pratico da consultare e da poter studiare per ottenere la **Certificazione NUOVA ECDL IT Security– Sicurezza Informatica**.
Il presente testo infatti tratta in dettaglio gli argomenti necessari per affrontare il test di verifica per il conseguimento della **Certificazione NUOVA ECDL IT Security– Sicurezza Informatica**, programma sviluppato in Italia da **AICA**, **A**ssociazione per l'**I**nformatica ed il **C**alcolo **A**utomatico, e riconosciuto ed accettato dalla Fondazione **ECDL**, **E**uropean **C**omputer **D**riving **L**icence, di Dublino.

Il manuale è strutturato "passo passo" seguendo le voci del **Syllabus V. 1**, **Allegato A**, in modo da poter spiegare e chiarire concetti teorici e tutto ciò che riguarda

Convenzioni utilizzate in questo libro:

Grassetto	nomi dei capitoli e sottocapitoli, acronimi e riferimenti a funzionalità del programma ed altro, che riteniamo importanti per il lettore.
Grassetto Corsivo	I riferimenti ai menù di Sistema ….
Evidenziato	Concetti fondamentali, utili da "tenere a mente" per il superamento della Certificazione ECDL Computer Essentials.

Scopo di questo manuale
È rendere comprensibile il tema trattato per chi non ha basi solide sull'argomento e si avvicina per la prima volta all'ITC, attraverso l'impiego di un linguaggio semplice, anche se informatico, che lo aiuterà nella riuscita completa dello studio ed esercizio nell'apposito piano di lavoro.
Utile anche a chi ha intenzione, avendo già conoscenze relative alla problematiche, di migliorare ed acquisire ulteriori nozioni allo scopo di applicarsi con maggiori elementi sul sistema.

In conclusione, si augura un buon lavoro a chi intraprenderà la lettura di questo manuale ed allo studio in questo percorso formativo nell'uso sicuro nell'ambito dell'ITC.

Gli autori

1 Concetti di sicurezza

1.1 Minacce ai Dati

1.1.1 Distinguere tra dati e informazioni.

I ***dati*** sono numeri o altro, immagini, testo, etc..., che rappresentano fatti o eventi non ancora organizzati.
Le ***informazioni*** sono dati organizzati in modo da essere comprensibili e significativi per l'utente. In informatica, di solito, i dati sono elementi di ingresso nel processo del calcolo o della ricerca, invece le informazioni sono il risultato del calcolo o della ricerca, cioè il risultato di una elaborazione di dati.

1.1.2 Comprendere il termine crimine informatico.

Un ***crimine informatico*** è un crimine attuato per mezzo dell'abuso degli strumenti informatici, hardware o software; ad esempio la frode informatica, il furto d'identità o l'accesso non autorizzato a sistemi informatici, il phishing o il pharming con cui si tenta di carpire i dati sensibili di un individuo o di utilizzare in modo fraudolento il nome, il logo o il sito di un ente o una società.

1.1.3 Comprendere la differenza tra hacking, cracking e hacking etico.

Hacking

Il termine deriva dal verbo inglese *to hack*, cioè intaccare o colpire e, ha diverse valenze: restringendo il campo al settore dell'informatica, si intende per hacking l'insieme dei metodi, delle tecniche e delle operazioni volte a conoscere, accedere e modificare un sistema hardware o software, a neutralizzare le difese informatiche di banche dati, reti, sistemi operativi, etc.... Colui che pratica l'hacking viene identificato come ***hacker***.

Cracking

Quando lo scopo principale dell'hacker è quello di utilizzare il sistema informatico a cui ha avuto accesso a proprio vantaggio per rubarne i dati o danneggiarlo, ad esempio aggirare le difese software di sistemi operativi proprietari e programmi commerciali per rivendere copie pirata, praticare phishing, introdursi abusivamente in una rete sociale per modificare profili o postare falsi commenti, ecc…, si parla di ***cracking***. Colui che pratica il cracking viene identificato come ***cracker***.

Hacking etico

si intende l'utilizzo delle tecniche di hacking per monitorare la sicurezza dei sistemi e delle reti informatiche e renderne pubblici i difetti al fine di evitare l'abuso da parte di malintenzionati. Colui che pratica l'hacking etico viene identificato come ***hacker etico***, o anche ***white hat***, cappello bianco, in opposizione al termine ***black hat***, che identifica un ***cracker***.

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

I dati possono essere minacciati non solo da persone, ma anche da ***eventi naturali*** come incendi, inondazioni, terremoti o, artificiali come la guerra o il vandalismo. È pertanto necessario tenerne conto per prevenirne la perdita: in ogni azienda il responsabile della sicurezza deve compilare un documento in cui vengano riportate le norme di comportamento del personale che avrà accesso al centro di calcolo e tutti gli accorgimenti che dovranno garantire il funzionamento ininterrotto dei computer e altre apparecchiature informatiche. Prima di tutto si cerca di prevenire eventi negativi prevedibili con:

- corsi di formazione del personale addetto;
- controllo accessi al centro di calcolo;
- installazione di firewall che impediscano l'accesso alla rete da parte di malintenzionati e di malware;
- installazione di gruppi di continuità elettrica che entrino in funzione automaticamente in caso di mancanza di alimentazione elettrica normale;
- programmi di manutenzione tecnica adeguati.

Esistono poi minacce non prevedibili come incendi, inondazioni, terremoto, ecc… per le quali il responsabile per la sicurezza ha il compito di stendere un piano denominato ***Disaster Recovery Plan*** in base al quale l'azienda deve disporre di un secondo sistema informatico o di una copia dei dati aziendali, copia di ***backup***, sempre aggiornata, entrambi installati in un luogo distante da dove è installato il centro di calcolo aziendale.

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

In vari casi l'origine della perdita di dati può dipendere anche da altri fattori, più o meno volontari, come gli stessi dipendenti di un'azienda che, essendo autorizzati all'accesso ai dati, possono involontariamente perderli o anche rubarli per poi rivenderli.
Anche i fornitori di servizi, pensiamo a chi manutiene le attrezzature hardware o l'infrastruttura di rete, potenzialmente sono in grado di danneggiare involontariamente i dati oppure di prenderne illegalmente possesso.
Infine può capitare che persone esterne, clienti e fornitori o semplici ospiti, possano accedere alla rete aziendale o scolastica tramite computer o altri dispositivi portatili, ad esempio tramite il WiFi e, mettere a rischio i dati.

1.2 Valore delle informazioni

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

Dovrebbero essere abbastanza evidenti i motivi per cui è opportuno proteggere le proprie informazioni personali: se qualcuno entra in possesso di dati riservati, come le credenziali di accesso alla posta elettronica o a una rete sociale, ne può fare un uso illegale facendo ricadere la colpa su di noi; se un malintenzionato entra in possesso del numero di carta di credito o dei dati di accesso a un servizio di Internet banking, li può utilizzare a proprio vantaggio.
Il furto di identità è considerato uno dei maggiori rischi della sicurezza informatica e quindi gli utenti devono porre molta attenzione a mantenere riservato il proprio account e a cambiare periodicamente la propria password.

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

Per un'azienda che tratta dati di clienti, progetti o trattative in corso, informazioni di carattere finanziario è ancora più essenziale proteggere queste informazioni, dato che se venissero utilizzate illegalmente la società che le detiene ne sarebbe responsabile.

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

Per proteggere i dati riservati, propri o altrui, è essenziale usare determinate tecniche per mezzo delle quali, anche se finissero nelle mani di malintenzionati, ad esempio immagazzinati su dispositivi mobili che possono più facilmente essere rubati, non potrebbero essere utilizzati.
La prima cosa da fare è proteggere con un **autenticazione**, cioè uso di **account + password** i dispositivi che permettono l'accesso ai dati.
La seconda è quella di **cifrare**, attraverso un opportuno algoritmo crittografico, i dati stessi. Ciò è necessario perché la password da sola garantisce i dati quando l'accesso avviene dal dispositivo su cui sono memorizzati, mentre non avrebbe effetto se i dati fossero memorizzati su una memoria rimovibile: Pen Drive, Disco Esterno, ma anche Hard Disk smontato dal computer e collegato ad un altro.

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

Per essere sicure, le informazioni devono avere un alto grado di **confidenzialità** o **riservatezza**, cioè non devono essere diffuse a chi non è autorizzato. Devono essere **integre**, cioè complete e senza modifiche rispetto all'originale. Infine devono essere **disponibili** al momento del bisogno: non avrebbe alcuna utilità curare la sicurezza dei dati e delle informazioni se poi, quando servono, per qualche motivo non si riesce a recuperarle nei tempi necessari.

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

In Italia è stato emesso ***Decreto Legislativo n. 5 del 9 febbraio 2012*** che ha preso il posto del precedente Dlgs 196/2003, a seguito dell'approvazione da parte della Commissione Europea nel gennaio 2012 di un regolamento sulla protezione dei dati personali, in sostituzione della **direttiva 95**/46/CE, **European Data Protection Directive**, in tutti e 27 gli stati membri dell'Unione Europea e di una direttiva che disciplina i trattamenti per finalità di giustizia e di polizia, attualmente esclusi dal campo di applicazione della direttiva 95/46/CE.
Punti essenziali della legge sono:

- nessuno può raccogliere e conservare dati personali altrui, senza il consenso scritto dell'interessato;
- chi conserva i dati deve nominare un responsabile del trattamento dati che garantisca l'applicazione della legge;
- i soggetti interessati possono informarsi presso il responsabile circa il trattamento dei loro dati e chiederne la cancellazione anche dopo aver dato il consenso;
- i dati personali devono essere cancellati non appena cessa il motivo del loro utilizzo.

1.2.6 Comprendere l'importanza di creare e attenersi a linee guida e politiche per l'uso dell'ICT.

A seguito di queste premesse, si comprende quanto sia importante attenersi alle regole che disciplinano l'utilizzo delle tecnologie informatiche e delle telecomunicazioni, ICT, per preservare i dati, personali e aziendali, dal furto, dallo smarrimento e da un utilizzo non consentito.

1.3 Sicurezza Personale

1.3.1 Comprendere il termine "ingegneria sociale" e le sue implicazioni, quali raccolta di informazioni, frodi e accesso a sistemi informatici.

L'**ingegneria sociale,** dall'inglese **S**ocial **E**ngineering, è lo studio del comportamento individuale di una persona al fine di carpire informazioni utili, ad esempio attraverso colloqui amichevoli supportati da riferimenti reali, con individui deboli come bambini o anziani..

Viene a volte utilizzata, al posto delle tecniche di ***Hacking***, per accedere a informazioni riservate aggirando sistemi di protezione hardware e software dei dati sempre più sofisticati e difficilmente penetrabili.

1.3.2 Identificare i metodi applicati dall'ingegneria sociale, quali chiamate telefoniche, phishing, shoulder surfing al fine di carpire informazioni personali.

L'**ingegneria sociale** utilizza diversi mezzi per carpire informazioni personali e riservate.

Il **Phishing** è una tecnica basata sull'invio di ingannevoli messaggi di posta elettronica: il phisher si finge un servizio bancario e, minacciando la chiusura del conto o della carta di credito, chiede di inserire le proprie credenziali per poterle verificare. Ovviamente si tratta di un trucco per entrarne in possesso.

Il **Trashing** è una raccolta illecita di informazioni ottenuta recuperando ricevute postali o bancarie o altro nei cestini della spazzatura o nei cassonetti.

Le **Chiamate Telefoniche** con cui si cercano di ottenere informazioni personali mascherandole con sondaggi anonimi a volte anche promettendo premi.

Il **Pretexting** con cui si usano riferimenti esistenti per convincere la vittima ad abbassare le difese e fornire informazioni personali.

Il **Shoulder Surfing**, dall'inglese "fare surf sulla spalla", consiste nel carpire le credenziali immesse dall'utente di un servizio spiandolo direttamente, standogli nei pressi, oppure anche da lontano, per mezzo di lenti o telecamere. Ciò può avvenire generalmente in luoghi affollati, come internet cafè o simili.

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

Il furto di identità nel campo informatico consiste nell'appropriazione indebita delle credenziali di accesso ad un servizio, accesso ad un PC, ad una rete locale, ad internet, alla posta elettronica, ad una rete sociale, ad un servizio di Internet banking, allo scopo di usarlo a proprio vantaggio, per compiere crimini informatici come frodi o furti fingendo di essere una persona differente, ben definita.

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

Per il furto di identità vengono usati vari metodi, tra cui per esempio frugare negli scarti delle persone tra cui potrebbe nascondersi qualche riferimento ai propri dati sensibili ***trashing***, ad esempio un foglietto su cui è annotata la password di accesso a un servizio. In alcuni casi ci si finge qualcun altro dotato di diritto ad avere le credenziali, per esempio nel caso del ***phishing***.

Infine in altri casi viene usata la tecnica dello ***Skimming***, che consiste nell'acquisire immagini o filmati di oggetti su cui sono impressi dei dati sensibili, per esempio la carta di credito o il PIN del bancomat. Quando si preleva da un bancomat è importante non solo non farsi vedere da qualcuno, ma anche stare attenti che non ci siano webcam posizionate sopra la tastiera.

1.4 Sicurezza dei File

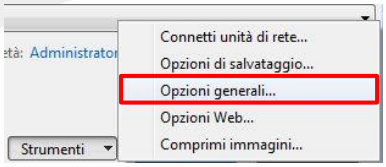
1.4.1 Comprendere l'effetto di attivare/disattivare le impostazioni di sicurezza delle macro.

Una ***macro*** è un insieme di istruzioni, a volte molto complesse, che utilizzano un linguaggio di programmazione, come *Visual Basic* o *Libreoffice Basic*, che possono essere eseguite, all'interno di un software di produttività, videoscrittura, foglio di calcolo, ecc ..., in automatico od alla pressione di una combinazione di tasti.
Le macro sono strumenti molto utili perché automatizzano procedure lunghe e noiose, ma possono contenere codice malevolo e quindi causare danni al computer. Ciò vale soprattutto quando l'origine della macro non è certa.
Pertanto attivare una macro ne consente l'esecuzione con i vantaggi sopra descritti, ma può mettere a rischio il computer.
Al contrario, disattivare una macro non ne consente l'esecuzione e quindi impedisce di avvalersi delle sue funzionalità, ma mette al sicuro il computer da possibile codice malevolo.
In linea di massima la cosa migliore è attivare le macro di cui si è certi e solo dopo averle esaminate con un programma antivirus aggiornato, non aprire mai file allegati di posta che provengano da fonti non certificate e, disattivare le macro di incerta provenienza.

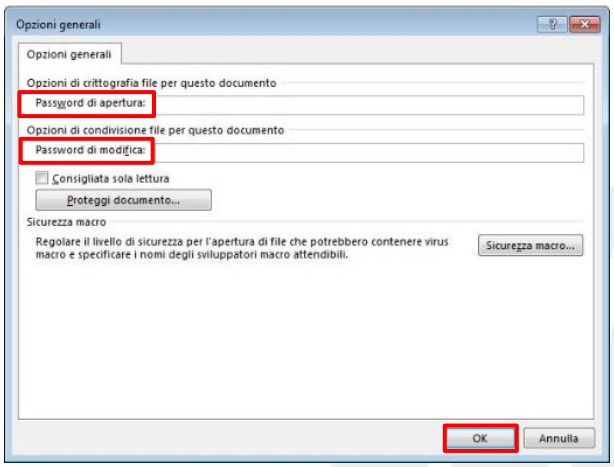
1.4.2 Impostare una password per file quali documenti, file compressi, fogli di calcolo.

È possibile impostare una password anche per proteggere documenti, fogli elettronici e file compressi.

Per proteggere con una password di "sola lettura" un **file di Microsoft Word 2010:**



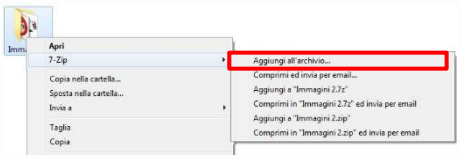
- aprire il documento, fare clic su ***File > Salva con nome***;
- dalla finestra che si apre selezionare il pulsante ***Strumenti*** che si trova in basso a destra;
- dal menù a tendina che appare scegliere ***Opzioni generali***.



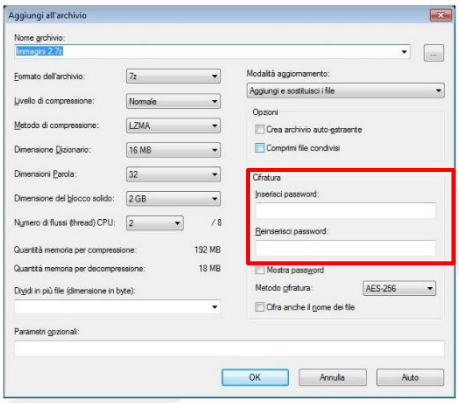
Si aprirà una nuova finestra in cui scegliere il tipo di protezione:
- password *di apertura*
- password *di modifica*.

Si digita la password e si fa clic su ***OK***, il programma chiederà di reinsirire la password per conferma, dopo di che si preme ***Salva***. Ora alla riapertura del file il programma chiederà di digitare la password.

Per inserire una password in un file compresso, va impostata in fase di compressione; vediamo come effettuare l'operazione utilizzando un programma tipo ***ZIP*** installato nel Sistema Operativo.



Fare clic con il tasto destro del mouse sulla cartella da comprimere, poi su ***7-Zip*** > ***Aggiungi all'archivio***.



Si apre una finestra in cui digitare la password, due volte, nel riquadro ***Cifratura***, infine confermare l'operazione cliccando ***OK***.

1.4.3 Comprendere i vantaggi e i limiti della cifratura.

Un file protetto non può essere letto né modificato se non da chi conosce la password e ciò garantisce che i dati in esso contenuti non cadano nelle mani sbagliate. Ci può essere il rischio che si dimentichi la password e quindi non si sia più in grado di aprire il file, pur essendone i legittimi proprietari.
La password va quindi conservata in modo da poterla ritrovare in caso di necessità.

I metodi della crittografia sono due:

- ***Crittografia a chiavi simmetriche*** in cui esiste una unica chiave per crittografare e decrittografare. E' un metodo debole perché dovendo far conoscere alla persona che riceverà il messaggio qual è la chiave, altri possono intercettare il messaggio.
- ***Crittografia a chiavi asimmetriche*** in cui esiste una coppia di chiavi, una pubblica ed una privata. Tutti possono conoscere la chiave pubblica, solo il proprietario conosce quella privata. I messaggi crittografati con chiave pubblica possono essere decrittografati solo con la corrispondente chiave privata e i messaggi crittografati con chiave privata, solo con la corrispondente chiave pubblica.

Se la chiave di decodifica viene smarrita, i file diventano inutilizzabili.

2 Malware

2.1 Definizione e funzione

2.1.1 Comprendere il termine malware.

Spesso si parla di virus informatici anche se sarebbe più corretto parlare di "***malware***", dall'inglese **M**alicious **S**oftware o *software malvagio*, cioè qualsiasi software creato al solo scopo di causare danni più o meno gravi al computer su cui viene eseguito, a volte per trarne vantaggi economici e, per diffondersi da un computer all'altro.

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

Si distinguono molte categorie di malware, tra cui:

Trojan, è un tipo di malware che deve il suo nome al fatto che le sue funzionalità sono nascoste all'interno di un programma apparentemente utile; è dunque l'utente stesso che installando ed eseguendo un certo programma, inconsapevolmente, installa ed esegue anche il codice trojan nascosto al suo interno. Questo malware raccoglie informazioni riservate sulla persona che utilizza il computer, ad esempio nome utente, password, codici di carte di credito, ecc.. per poi inviarle a dei cracker mentre il computer è collegato ad Internet. Alcuni trojan permettono di controllare il computer su cui è installato il virus, visionarne il contenuto, copiarlo o modificarlo, anche utilizzare eventuali microfoni o webcam, questo sempre quando il computer è collegato in rete.

Backdoor, letteralmente "porta sul retro". Sono dei programmi che consentono un accesso non autorizzato al sistema su cui sono in esecuzione usando una porta sul retro già aperta da altri programmi, ad esempio Emule o Skype, e per questo sono difficili da individuare per i programmi antivirus. Creano un collegamento nascosto tra computer attaccato e computer attaccante che può dare un gran numero di comandi senza che il proprietario se ne renda conto.

Rootkit che non sono dannosi in sé, ma hanno la funzione di nascondere la presenza di particolari file o impostazioni del sistema e vengono utilizzati per mascherare spyware e trojan.

2.2 Tipi

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

Esistono altre due famiglie di malware:

Virus, è un software che è in grado di infettare dei file eseguibili in modo da riprodursi facendo copie di se stesso, e di diffondersi tramite Internet oppure supporti removibili.
A differenza dei worm, per manifestarsi e contagiare , hanno bisogno di un programma qualsiasi che li ospiti.

Worm, è una particolare categoria di malware in grado di autoreplicarsi. È simile ad un virus, ma a differenza di questo non necessita di legarsi ad altri eseguibili per diffondersi. Si propaga principalmente attraverso la posta elettronica: quando un computer è contagiato da un worm, infatti, invia automaticamente dei messaggi di posta elettronica, ai quali è allegata una copia dello stesso worm, a tutti gli indirizzi presenti nella rubrica, sfruttando i momenti nei quali l'utente si collega ad Internet, senza che questo se ne accorga; la persona che lo riceve, aprendolo contagia il proprio computer. Con questa continua moltiplicazione il worm occupa sempre più spazio nella memoria del computer, rallentandone le prestazioni.

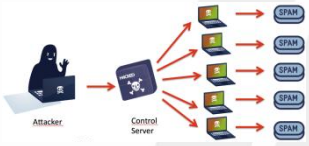
2.2.2 Riconoscere i tipi di malware usati per furto di dati, profitto/estorsione e comprendere come operano, ad esempio adware, spyware, botnet, keylogger e dialer.

Adware sono software che presentano all'utente messaggi pubblicitari o banner durante l'uso del computer. Possono causare danni quali rallentamenti del pc e rischi per la privacy in quanto comunicano le abitudini di navigazione ad un server remoto. In fase di installazione di programmi, l'azione di un adware può essere molto fastidiosa in quanto l'utente può essere indotto a scaricare software differenti da quello voluto.

Spyware, è un software che raccoglie informazioni riguardanti l'attività online di un utente senza il suo consenso, trasmettendole tramite Internet ad un'organizzazione che le utilizzerà per trarne profitto, solitamente attraverso l'invio di pubblicità mirata.

Keylogger sono malware che una volta installati nel computer attraverso dei trojan, rimangono sempre attivi e sono in grado di registrare tutto ciò che viene digitato sulla tastiera consentendo il furto di password e numeri di carte di credito.

Dialer sono programmi che modificano, quando ci si connette con la normale linea telefonica, il numero telefonico chiamato dalla connessione predefinita con uno a tariffazione speciale allo scopo di trarne illecito profitto all'insaputa dell'utente. Il raggiro è possibile solo per collegamenti ad Internet fatti via modem analogico.



Botnet è una rete informatica di computer infestati da software malevolo, tipo trojan, collegata ad Internet, che viene controllata da remoto dal botmaster, in grado di utilizzare la rete stessa e i dispositivi ad essa collegati per svolgere attività non autorizzate, come ad esempio lo l'invio dispamgamento peer-to-peer.

2.3 Protezione

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

Soprattutto sui dispositivi con sistema operativo ***Windows***, è necessario avere installato un ***software antivirus***, che sia in grado di opporsi ai tentativi dei malware di infettare il sistema. In realtà nessun sistema operativo è immune dai malware, ma Windows è più vulnerabile sia per motivi strutturali, sia per il fatto che, essendo più diffuso degli altri, viene più preso di mira da questi software.

Un antivirus ha due funzioni principali:

- la prima è quella di controllare cartelle e file in modo da individuare e rendere innocui eventuali file portatori di infezione virale;
- la seconda è quella di scansionare la memoria RAM in modo da impedire l'esecuzione di codice virale, che è in grado di riconoscere o a seguito di un confronto con un archivio contenente le "firme" dei malware conosciuti o con metodi di indagine euristica, cioè basata sulla somiglianza di frammenti di codice virale con quello analizzato.

Un antivirus non può essere efficace al 100% e proteggere completamente un dispositivo informatico. Inoltre, per poter essere efficace, l'antivirus deve essere aggiornato con frequenza, in particolare l'archivio delle firme, in quanto nuovi malware vengono diffusi in continuazione.

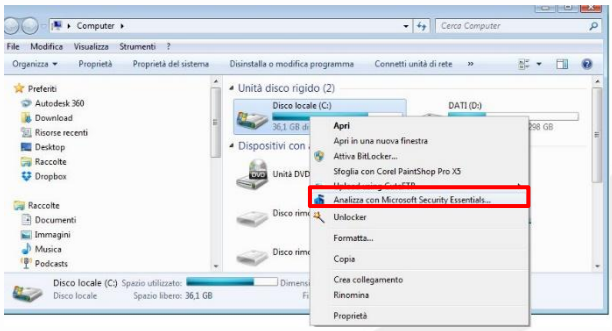
Infine, un altro limite che i software antivirus hanno, è che a volte segnalano falsi positivi, cioè indica no come virus programmi del tutto leciti.

I moderni Sistemi Operativi tendono ad incorporare determinate sicurezze e di base offrono un software firewall, ad esempio i sistemi operativi Windows prevedono un software anti-spyware e quelli più recenti hanno incorporato il programma antivirus ***Microsoft Security Essential***, che può essere scaricato gratis dal sito Microsoft.

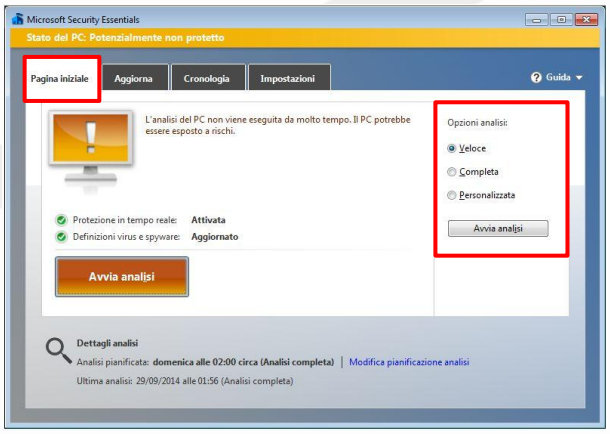
Alcuni tra i più famosi antovirus presenti sul mercato

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

I programmi antivirus possono essre usati in modo automatico o non automatico, possono essere impostati in modo che propongano in modo automatico la scansione ogni volta che un evento lo richiede, ad esempio l'inserimento di una chiavetta USB, un DVD, ecc… o per scandire intere unità disco ad orari programmati, di solito fuori dall'orario di lavoro.



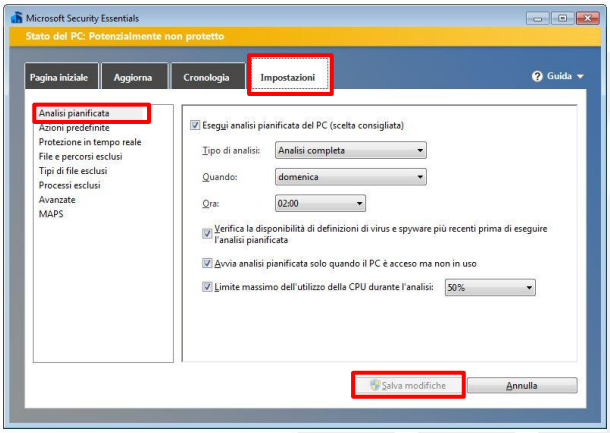
Per avviare una scansione con ***Microsoft Security Essential*** si fa clic su ***Start > Computer***, poi si seleziona l'unità da scansionare e ci si fa clic sopra con il tasto destro del mouse, apparirà un menu a tendina in cui si sceglierà ***Analizza con Microsoft Security Essential…***



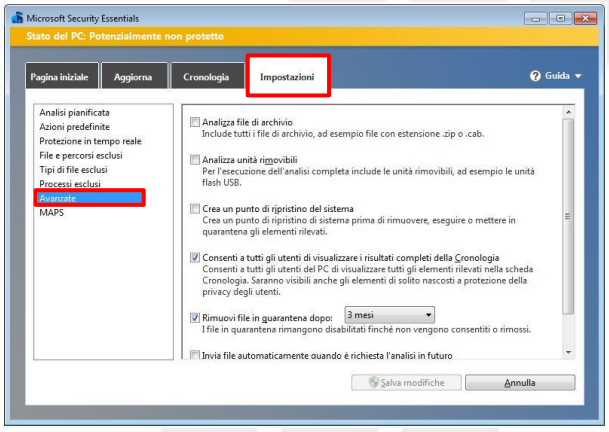
Appare la finestra di ***Microsoft Security Essential***.
L'interfaccia grafica presenta quattro schede:
– *Pagina iniziale;*
– *Aggiorna;*
– *Cronologia*;
– *Impostazioni.*

Nella scheda ***Pagina iniziale*** si sceglie quale tipo di analisi si vuole:
– ***Veloce***;
– ***Completa***
– ***Personalizzata,*** dove è possibile scegliere la Cartella o la periferica da analizzare.

si avvia facendo clic su ***Avvia analisi***.



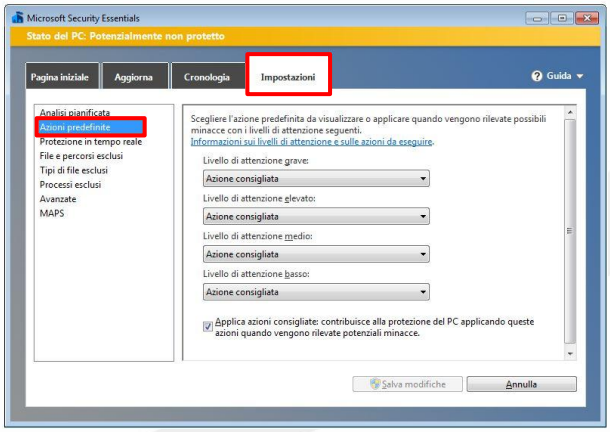
Nella scheda ***Impostazioni***, facendo clic su ***Analisi pianificata***, si sceglie il tipo di analisi e in quale giorno e a quale ora verrà automaticamente avviata. Per salvare si fa clic su ***Salva modifiche***.



Sempre nella scheda ***Impostazioni*** facendo clic su ***Avanzate***, possiamo selezionare diverse opzioni: *Analizza file di archivio, Analizza unità rimovibili, ecc…* e anche scegliere quando rimuovere i file messi in quarantena. Per salvare si fa clic su ***Salva modifiche***.

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

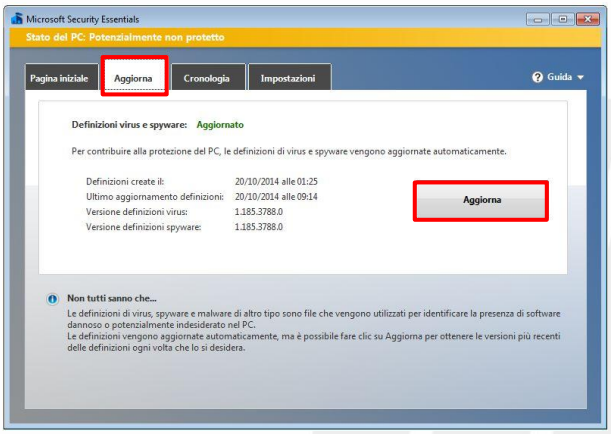
Quando un software antivirus individua dei file contenenti del codice virale o anche solo sospetti, chiede all'utente se intende metterli in quarantena, cioè a dire in isolamento in una apposita cartella creata dal software antivirus e pertanto facilmente controllabile, con l'intenzione di poterli riesaminare meglio in un momento successivo, prima di chiedere se renderli ancora utilizzabili o eliminarli in modo definitivo.



Con ***Microsoft Security Essential***, per programmare i livelli di attenzione e mettere in qurantena i file sospetti si va nella scheda ***Impostazioni*** > ***Azioni predefinite*** e si sceglie l'azione predefinita da applicare ad ogni possibile minaccia.
Per salvare si fa clic su ***Salva modifiche***.

2.3.4 Comprendere l'importanza di scaricare e installare aggiornamenti di software, file di definizione di anti-virus.

Come già accennato in precedenza, è essenziale scaricare con assiduità gli aggiornamenti sia del software antivirus, che soprattutto delle definizioni dei virus, in modo che il programma sia in grado di riconoscere e debellare il maggior numero possibile di infezioni virali.
Attualmente tutti i software antivirus si aggiornano automaticamente, ma è bene controllare che lo facciano con frequenza. Il mancato aggiornamento automatico potrebbe essere indice di un malfunzionamento, magari dovuto proprio ad un virus che cerca di impedire al programma di individuarlo.



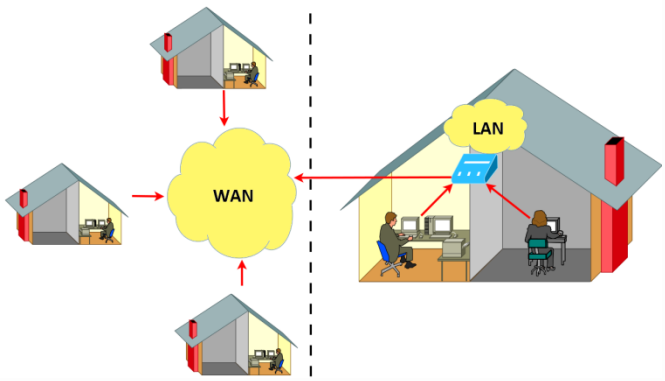
Con ***Microsoft Security Essential***, o ***Windows Defender*** per aggiornare i *file definizione*, cioè le impronte o firme dei malware riconosciuti, si va nella ***Scheda Aggiorna*** e si preme il pulsante ***Aggiorna***.

3 Sicurezza in rete

3.1 Reti

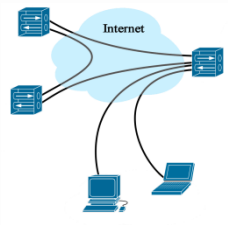
3.1.1 Comprendere il termine rete e riconoscere i più comuni tipi di rete, quali LAN (rete locale), WAN (rete geografica), VPN (rete privata virtuale).

Una rete informatica permette di collegare tra di loro vari computer e altri dispositivi, come stampanti, supporti di archiviazione di rete, etc … per condividerne le risorse, intese come dati, file, e servizi, ad esempio l'accesso a internet o la stampa, con enormi vantaggi funzionali ed economici. Ciò presuppone che le risorse siano condivise, cioè che sia data facoltà agli utenti della rete di potervi accedere.



WAN o **Wide Area Network**, quando la rete è così estesa che per i trasporti dei dati tra i vari segmenti di rete occorre utilizzare, per esempio, la rete telefonica.
Diventa cioè una rete geografica, il cui maggior esempio è Internet.

LAN o **Local Area Network**, una rete privata di computer e dispositivi limitata ad un'area circoscritta in cui, di solito, esiste un computer principale più potente definito *Server*, che mette le sue risorse a disposizione degli altri dispositivi collegati, chiamati client. La più diffusa di questo tipo di reti si chiama Ethernet.



VPN o **Virtual Private Network**: è un sistema per avere una rete virtuale privata che però utilizza una rete pubblica per funzionare. Normalmente una VPN viene implementata per poter collegare in modo sicuro più computer lontani tra di loro per mezzo di Internet. Un apposito software si occupa di creare un tunnel sicuro attraverso al criptazione dei dati e l'autenticazione della comunicazione.

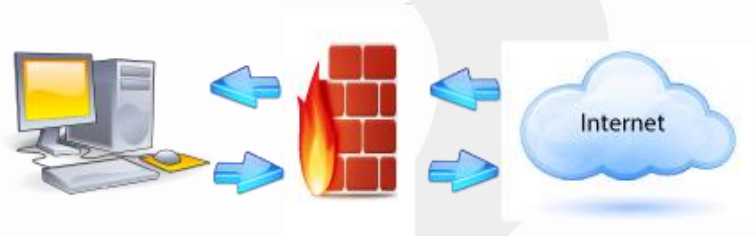
3.1.2 Comprendere il ruolo dell'amministratore di rete nella gestione delle operazioni di autenticazione, autorizzazione e assegnazione degli account all'interno di una rete.

Con la diffusione di Internet, ha assunto particolare rilievo la figura professionale dell'***Amministratore di rete*** che ha tra i suoi compite principali: *garantire l'autenticazione degli ingressi alla rete; provvedere all'assegnazione degi account; provvedere e controllare l'autorizzazione degli account*.
Con ***autenticazione*** si intendono tutte le norme che servono a controllare la corretta identità di un utente, cioè l'account, o di un computer o un software che chiedono di accedere ai servizi di rete. Si possono utilizzare riconoscimenti degli account associati alle rispettive password, frasi di riconoscimento, tesserini identificativi letti da apposite apparecchiature, **PIN** cioè numero di identificazione personale oppure riconoscimenti biometrici come voce, retina, impronte digitali, ecc..
Per ***assegnare*** un account, l'Amministratore di rete deve produrre uno schema in cui riportare:

- le norme per l'assegnazione dell'account, ad esempio identificazione dell'utente, ruolo in azienda, procedure affidate, ecc…;
- le norme per la costruzione, come lunghezza, tipo di caratteri e, per la gestione della password associata all'account;
- la metodologia per il recupero della password in caso venga dimenticata.

Per ***autorizzazione*** si intende la procedura con cui l'Amministratore di rete rende i vari account riconoscibili salla rete stessa. L'Amministratore può anche atturae la procedura inversa, cioè revocare l'accesso alla rete ad un account.

3.1.3 Comprendere la funzione e i limiti di un firewall.



Un **firewall**, termine inglese *muro tagliafuoco*, è un componente di difesa di un computer o di una rete.
Può essere un apparato di rete hardware o un software, di solito già compreso all'interno dei sistemi operativi, che monitorizza il traffico di rete e lo filtra in base ad opportune regole che garantiscono la sicurezza di tutti i dati in entrata e in uscita da e verso la rete o il computer, bloccando ciò che si ritiene pericoloso o indesiderato.
Un **firewall**, quindi, riduce il rischio di accessi indesiderati dall'esterno, di solito da Internet, al proprio computer o alla propria rete locale. Per funzionare bene il **firewall** deve essere programmato in modo efficace, dato che si limita a seguire le regole impostate. Se le regole non sono ben organizzate il funzionamento non sarà efficace.
Inoltre, dato che il **firewall** è generalmente posto tra la rete locale e Internet, non avrà effetto se l'attacco viene effettuato dall'interno, per esempio da un utente della rete o da un malware che ha infettato in precedenza un dispositivo della rete.
Infine un **firewall**, soprattutto se mal programmato, può impedire agli utenti un uso legittimo della rete.

3.2 Connessioni di Rete

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

Come accennato in precedenza, una rete può connettere dispositivi informatici utilizzando mezzi diversi. I più usati sono il cavo, generalmente in rame ma può essere anche in fibra ottica e, le onde radio: in quest'ultimo caso si parla di rete wireless, cioè senza cavo o WiFi.

I vantaggi di una **rete cablata** sono la maggiore sicurezza, dovuta al fatto che è necessario connettere fisicamente i dispositivi alla rete e quindi in modo visibile e, la velocità di trasmissione dei dati, anche se la continua evoluzione tecnologica fa sì che anche le reti senza fili oggi siano in grado di raggiungere elevate velocità di trasmissione dei dati. Nelle reti moderne il protocollo usatoè TCP/IP e il cavo dati che collega i computer termina con due connettori denominati RJ45.

I vantaggi di una **rete senza fili** sono l'economicità, dovuta al fatto di non avere la necessità di posare i cavi, la praticità di utilizzo soprattutto con dispositivi mobili come notebook e Tablet e, la possibilità di essere implementata anche dove, per motivi tecnici, non è materialmente possibile far arrivare il cavo.

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

Un computer trae grandi vantaggi dalla connessione a una rete, e tuttavia dalla rete possono arrivare anche minacce.
Attraverso la rete, locale o Internet, è possibile che il computer venga infettato da virus o altro ***malware*** che spesso viene scaricato attraverso la posta elettronica o pagine web.
Attraverso la rete sono possibili ***accessi non autorizzati*** ai dispositivi connessi, dovuti a falle di sicurezza o infezioni virali.
La rete può mettere a rischio anche la ***privacy*** degli utenti connessi, in quanto i dati personali, se non adeguatamente protetti, possono essere accessibili da persone interessate in vari modi, come accennato in precedenza.
Contro questi rischi possono essere messi inatto strumenti preventivi come:

- installazione di un **firewall** che limiti gli accesi non autorizzati;
- obbligo di digitare **account** e **password** per collegarsi;
- presenza di **software antivirus** costantemente aggiornato.

3.3 Sicurezza su reti wireless

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

Mentre una rete cablata richiede un collegamento fisico agli apparati di rete e quindi è quasi impossibile collegare un dispositivo senza autorizzazione da parte dell'amministratore di rete, una rete senza fili può essere facilmente agganciata da un dispositivo mobile, anche posto all'esterno dell'edificio, fin dove arriva il segnale ***wireless***.
Chiunque pertanto potrebbe connettersi all'insaputa dell'amministratore di rete se la rete senza fili non fosse protetta da password, che permette l'accesso ai soli utenti che la conoscono. Tutti gli altri invece vengono esclusi, diminuendo i rischi di accessi non autorizzati che possono danneggiare la rete, i dispositivi ad essa connessi e i dati in essi contenuti.

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

Per migliorare la sicurezza delle reti wireless nel corso degli anni sono stati elaborati degli **algoritmi di crittazione** dei dati trasmessi nelle reti senza fili. Una rete può dirsi sicura se rispetta tre principi: *Riservatezza*, *Integrità* e *Accesso autorizzato*. L'insieme di questi tre punti è previsto negli obiettivi di tre protocolli di sicurezza per reti wireless:

WEP	**Wired Equivalent Privacy**, si pone l'obiettivo di fornire, via onde radio, la stessa sicurezza e riservatezza che offrono le reti LAN cablate. Può avere una frase di sicurezza a 40 o 128 bit, maggiore è il numero dei bit maggiore è la sicurezza, più 24 bit di controllo.
WPA	**Wifi Protected Access**, accesso protetto alle reti senza fili, ed il successivo WPA2 sono stati elaborati nel 2003/2004 e mettono a disposizione una maggiore sicurezza e un sistema più efficiente per garantire l'interità del messaggio. Ha una frase di sicurezza più lunga, 128 bit + 48 bit di controllo.
MAC	**Media Access Control** o **MAC Address** consiste nell'indirizzo fisico della scheda di rete, cablata o wireless, ed è univoco per cui individua in modo inequivocabile un dispositivo tra tutti gli altri. Ciò consente di stilare all'interno degli apparati di rete delle ACL, Access List, liste di indirizzi MAC, di dispositivi autorizzati all'accesso alla rete. Un dispositivo con un Mac address differente, anche se il proprietario conosce la password di accesso alla rete senza fili, non verrà connesso alla rete. Questo metodo in realtà non è del tutto sicuro, in quanto esistono dei software in grado di modificare il Mac address della scheda di rete di un dispositivo.

Come si può capire da quanto detto in precedenza, nessun metodo rende sicura al 100% una rete senza fili, tuttavia utilizzando più metodi in combinazione si raggiunge un buon grado di sicurezza.

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

Di solito chi si collega ad una ***rete Wi-Fi non protetta*** non riesce ad entrare nei computer che fanno parte della rete wireless LAN, perché non conosce i vari account e le rispettive password. Esistono però vari trucchi per introfularsi nei computer collegati aggirando account e password, soprattutto se una rete senza fili non è protetta con uno o più dei metodi sopra presentati, ed è molto facile che qualche malintenzionato possa accedervi e quindi abbia la possibilità di intercettare i dati presenti sui dispositivi connessi o anche solo in transito. Chi opera in questo modo per entrare in una rete di computer, è definito ***spia digitale***.

3.3.4 Connettersi ad una rete wireless protetta/non protetta.

Per connettere un dispositivo a una rete senza fili, prima di tutto occorre accertarsi che sia dotato di scheda di rete wifi. Di solito tutti i sistemi operativi dispongono di un programma di connessione che, generalmente, avvisa l'utente della disponibilità di reti senza fili.

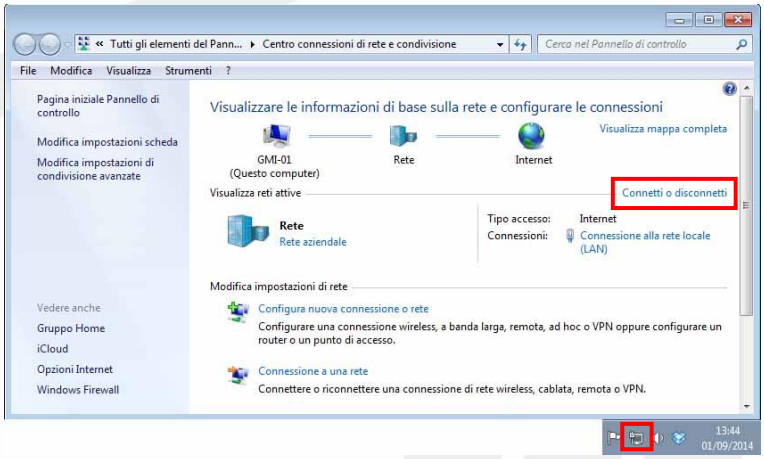
Per visualizzare un elenco delle reti wireless eventualmente disponibili nella zona in cui ci si trova, basta fare clic sull'icona del wireless che compare nella barra delle applicazioni di Windows, di solito a fianco dell'orologio oppure in alto se si usa un tablet o uno smartphone.

Per alcune reti protette o sicure è necessario avere una chiave di sicurezza rete o una password per collegarsi. Esistono anche reti aperte che consentono la connessione libera, ma in questo caso chiunque può essere in grado di rilevare ogni operazione che eseguiamo. Per sapere se una rete è protetta basta portare il puntatore su una delle reti disponibili e comparirà un riquadro con le principali caratteristiche della rete.

Icone rete Wireless

Icone rete Wireless protetta

Potenza segnale



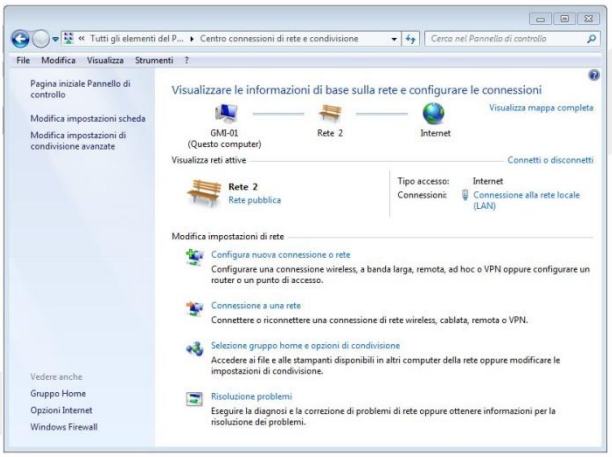
Per collegarsi ad una rete wireless disponibile da un elenco, basta fare clic su di essa e poi su ***Connetti***. Se si tratta di una rete protetta ci verrà chiesto di digitare la chiave di protezione o la password necessarie.

3.4 Controllo di Accesso

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

Per motivi di sicurezza, come indicato nei paragrafi precedenti, è opportuno che ciascun utente di una rete sia in possesso di ***credenziali personali***, nome utente e password, in modo che solo utenti autorizzati possano accedere alla rete.

La procedura che si usa per collegarsi ad un computer, una rete o un'applicazione è detta login. Se questi sono protetti, il ***login*** consiste nella digitazione di un nome riconoscibile, cioè un account e, della relativa password. L'esibizione di un account valido è condizione imprescindibile. Per le password, invece, sono previste anche procedure che consentano il recupero della password dimenticata o scaduta e la possibilità di produrne una nuova.



Per accedere ad una rete si va su ***Start*** > ***Pannello di controllo*** > ***Centro connessioni di rete e condivisione***

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

Si è detto in precedenza che la password garantisce la ***privacy*** dei propri dati e anche la sicurezza delle reti. Ciò è vero ma solo a condizione che la password venga gestita in modo corretto e risponda a ***criteri di robustezza***.

Esistono applicazioni in grado di decodificare le password all'insaputa dei legittimi proprietari, quindi una password, per essere sicura, deve rispondere a un certo numero di requisiti:

- DEVE essere abbastanza lunga, minimo 8 caratteri;
- NON deve essere una parola facilmente individuabile o corrispondente a dati personali, come il nome o la data di nascita propri o di persone care, numeri di telefono, ecc..;
- NON DEVE corrispondere a sequenze prevedibili, quali "12345", "password", ecc..;
- DEVE contenere caratteri maiuscoli e minuscoli, caratteri speciali e numeri. Meglio evitare le lettere accentate in quanto differenti in base alla lingua della tastiera e al sistema operativo utilizzato.

Inoltre è buona norma non comunicare la password a nessuno o scriverla in luoghi accessibili ad altri, non usare la stessa password per tutti i servizi che ne richiedono una e cambiarla con una certa frequenza.

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

In alcuni casi, al posto delle password, per accedere al computer in modo sicuro vengono utilizzati dei sistemi che si basano sulla ***biometria*** e sulle ***tecniche biometriche***, cioè su tecniche basate sull'univocità di caratteristiche fisiche degli utenti come ad esempio:

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

Questi parametri devono essere forniti al programma che provvede al riconoscimento, prima della richiesta di accesso alla rete. La tecnica biometrica più utilizzata è senz'altro la scansione delle impronte digitali; diversi notebook ed altri dispositivi mobili ne sono già provvisti.

4 Uso sicuro del web

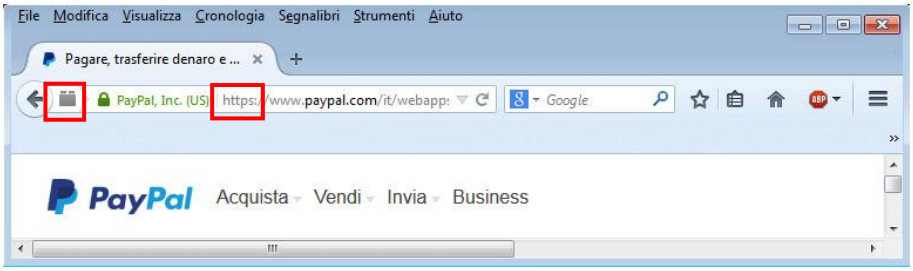
4.1 Navigazione in rete

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

Da quanto detto in precedenza è evidente che i computer e le reti, in particolare Internet che è pubblica, non sono sicuri e quindi è necessario prendere dei provvedimenti quando si usano questi strumenti.
Si dovrebbe far riferimento solo a siti Internet ritenuti sicuri, come i siti degli Istituti bancari conosciuti, i siti commerciali di utilizzo diffuso ed associati a marchi riconoscibili. Siti che esibiscono il ***certificato digitale*** controllabile direttamante in linea, oltre al ***simbolo del lucchetto chiuso***, accanto all'indirizzo della pagina, con ***protocollo https***.

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

È pertanto essenziale per la sicurezza dei dati trasmessi che quando si utilizza il web per un pagamento, per esempio acquisti online, o transazioni finanziarie per esempio operazioni sul proprio conto corrente bancario, ci si accerti che il browser utilizzi un protocollo sicuro, cioè ***https***: **H**yper **T**ext **T**ransfer **P**rotocol **S**ecure, che trasmette i dati dopo averli cifrati con una chiave robusta in modo che il solo sito web che li riceve e li trasmette sia in grado di decodificarli.
Quando un sito web utilizza il protocollo ***https***, lo stesso browser, cioè l'applicazione che utilizziamo per navigare in Internet, ce lo indica, facendo comparire nella barra degli indirizzi l'immagine di un ***lucchetto chiuso***. Inoltre il nome del sito sicuro non comincia con http ma con ***https***: la s finale è l'iniziale di *secure*, cioè sicuro.



4.1.3 Essere consapevoli del Pharming.

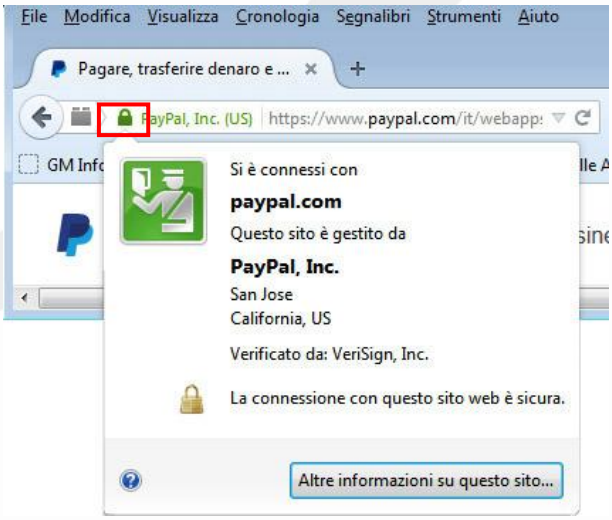
Il ***Pharming*** è una tecnica per certi aspetti simile al phishing, di cui si è già parlato, ma più sofisticata in quanto fa sì che, digitando l'indirizzo di un sito web lecito, si venga diretti verso un altro sito web, identico a quello lecito ma falso. Se questo sito clonato richiede l'immissione di dati personali, questi verranno comunicati inconsapevolmente dall'utente e potranno poi essere utilizzati a suo danno.
L'utente non ha strumenti per rendersi conto della differenza se non controllare il certificato digitale di una pagina che utilizza il protocollo https. Nei siti clonati, infatti la barra degli indirizzi *non ha il simbolo del lucchetto ed il protocollo è http*.

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

Un ***certificato digitale*** è, come dice il termine, un documento emesso da un'autorità di certificazione che controlla e garantisce l'identità del mittente di un messaggio di posta elettronica o dell'intestatario di un sito web.

Si utilizza quindi nel momento in cui è necessario essere sicuri, per esempio nel caso di una transazione economica con carta di credito o un'operazione sul proprio conto corrente bancario, soprattutto data la diffusione di un tipo di truffa telematica che consiste nell'imitazione in tutto e per tutto siti famosi per confondere le persone e portarle a digitare dati personali e finanziari.

È possibile visualizzare il certificato digitale, le generalità del sito e l'ente certificatore, si fa clic *sull'icona del lucchetto chiuso* che compare nella barra di stato del browser.



4.1.5 Comprendere il termine "one-time password".

Uno dei maggiori rischi per la sicurezza delle reti aziendali, deriva dagli accessi effettuati dai dipendenti che lavorano fuori sede, di solito venditori o tecnici d'assistenza, i quali attraverso i normali dispositivi palmari si collegano alla rete aziendale. Ogni volta che digitano il loro account e password, mettono un estraneo in condizione di entrare in modo abusivo nella rete aziendale.

Per evitare questo rischio è stato inventato il metodo della ***one time password***, cioè *password valida una sola volta*, tipico delle reti **VPN**.

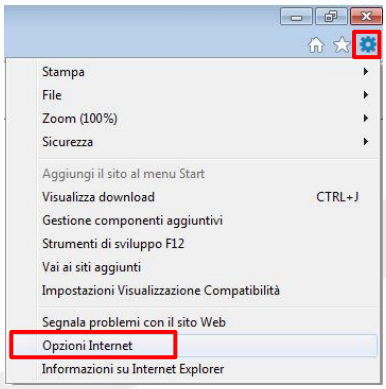
Consiste nel richiedere una password aggiuntiva generata al momento da un dispositivo in possesso dell'utente, per esempio una applicazione per smartphone, o inviata all'utente dal gestore del sito per mezzo di un SMS dopo aver verificato le credenziali dell'utente che chiede l'accesso.

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

Soprattutto quando il computer è utilizzato da o accessibile a più persone, conviene disabilitare le opzioni di completamento e di salvataggio automatico del browser, per evitare la diffusione dei propri dati personali.

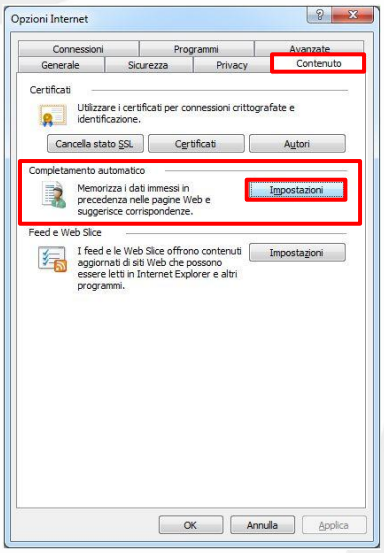
Il ***completamento automatico***, usato spesso per la compilazione veloce dei moduli online, potrebbe infatti facilitare il compito della solita spia informatica.

L'attivazione e la disattivazione del ***completamento automatico*** sono operazioni che vanno eseguite sul browser Internet utilizzato. La disattivazione non comporta automaticamente la cancellazione dei dati conservati in precedenza, i quali vanno perciò cancellati a parte.

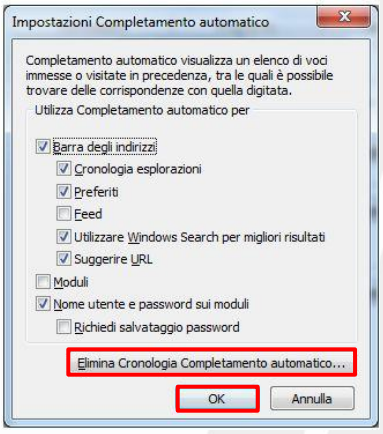


Per attivare o disattivare il completamento automatico si apre il browser, ad esempio Internet Explorer:

- si fa clic su ***Strumenti***, rappresentato dall'ingranaggio che si trova in alto a destra;
- dal menu a tendina che appare si sceglie ***Opzioni Internet***.



Nella finestra che appare si fa clic sulla scheda ***Contenuto*** e poi sul pulsante ***Impostazioni***.



Appare una nuova finestra in cui attivare con un ***segno di spunta***, o disattivare togliendolo, ciò per cui vogliamo utilizzare il completamento automatico. Per confermare si fa clic su ***OK***.

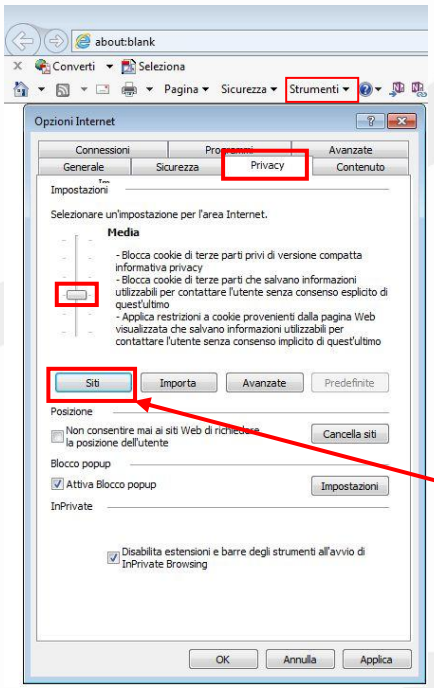
Se vogliamo eliminare anche la cronologia fare clic sul pulsante ***Elimina Cronologia Completamento automatico*** e poi su ***OK***

4.1.7 Comprendere il termine "cookie".

I **Cookies**, letteralmente "biscottini", sono piccoli file di testo che i siti Web sui quali navighiamo, utilizzano per immagazzinare alcune informazioni nel computer dell'utente e per controllare quante volte si accede ad un determinato sito o rendere più semplice la navigazione dell'utente nel sito stesso. Alcuni cookies contengono informazioni sulle password usate in un dato sito, in modo da non doverle reinserire ogni volta che ci si collega o, tengono memoria delle preferenze dell'utente sulla configurazione dei servizi offerti dal sito.

Le informazioni contenute all'interno del **Cookie** sono spesso codificate e non comprensibili, e non contengono informazioni che violano la Privacy, ma bisogna sempre valutare come possibile pericolo l'uso che possono farne i proprietari dei siti web.

4.1.8 Selezionare impostazioni adeguate per consentire, bloccare i cookie.



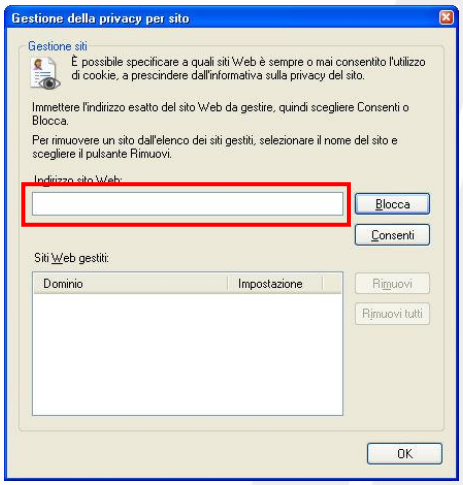
Per bloccarli si fa clic su ***Strumenti*** > ***Opzioni Internet*** > ***Privacy*** > ***Predefinite*** e poi, muovendo il cursore di scorrimento si sceglie tra diverse opzioni:

- ***Accetta tutti i cookie;***
- ***Bassa;***
- ***Media;***
- ***Medio alta;***
- ***Alta;***
- ***Blocca tutti i cookie***.

Anche in questo caso è possibile scegliere se bloccarli o attivarli in tutti i siti o solo in alcuni.

Disattivare completamente i cookie rende difficoltosa la navigazione o addirittura impossibile in alcuni siti, per cui è consigliabile, nel caso, impostare alcune eccezioni per i siti web attendibili e sicuri.

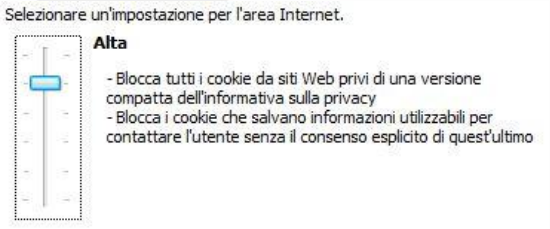
Cliccare su **Siti** per impostare le eccezioni per i siti web.

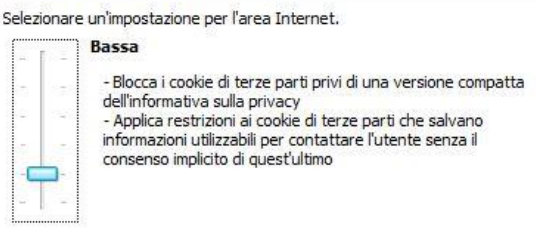


Inserire nel riquadro il nome del sito completo sito per l'eccezione:

- ***Blocca;***
- ***Consenti***

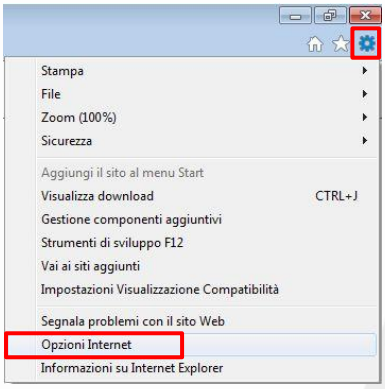
Di seguito esempio di altre impostazioni dei cookie:





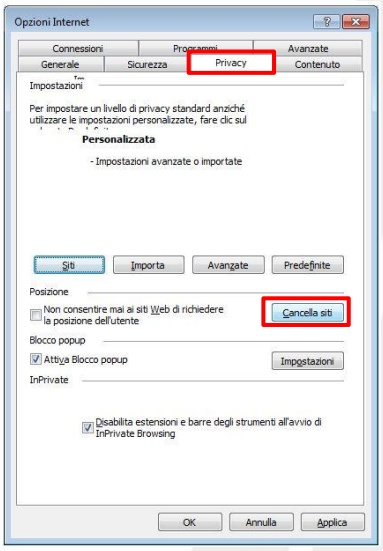
4.1.9 Eliminare dati privati da un browser, quali cronologia di navigazione, file temporanei di internet, password, cookie, dati per il completamento automatico.

Quando si lavora su di un computer occasionale, occorre ricordarsi di non lasciare tracce di alcun tipo, di cancellare tutti i dati di navigazione, cronologia e file temporanei.



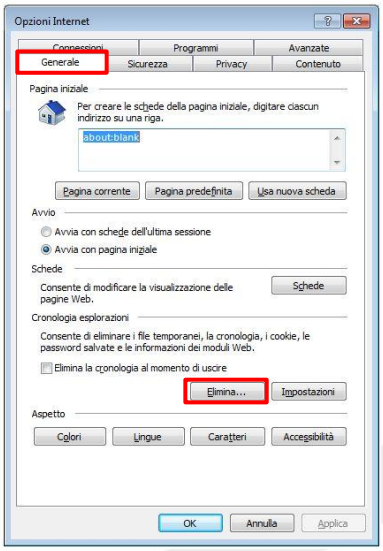
Per cancellare tutti i dati di navigazione si apre il browser, ad esempio Internet Explorer:

– si seleziona il pulsante ***Strumenti***, a forma di ingranaggio, che si trova in alto a destra.



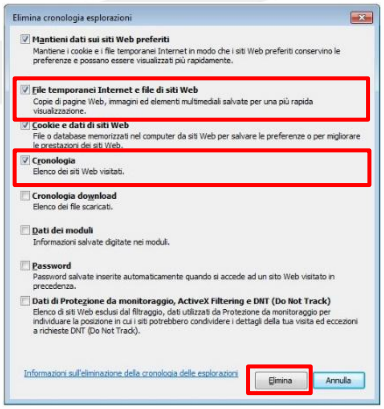
Si seleziona la scheda ***Privacy*** e si fa clic sul pulsante ***Cancella Siti***.

Per eliminare la cronologia ed i file temporanei:



Si apre il browser, ad esempio Internet Explorer:

- si seleziona il pulsante ***Strumenti***, a forma di ingranaggio, che si trova in alto a destra;
- poi si fa clic su ***Opzioni Internet*** e nella finestra che si apre si seleziona la scheda ***Generale*** e si fa clic sul pulsante ***Elimina***.

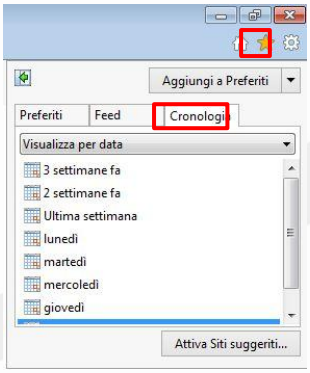


Nella finestra ***Elimina cronologia esplorazioni*** che si apre,:

- si selezionano le opzioni ***File temporanei Internet*** e ***Cronologia;***
- poi si fa clic sul pulsante ***Elimina***.

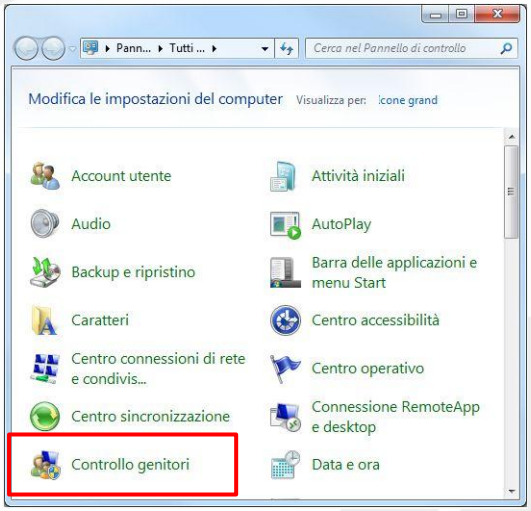
4.1.10 Comprendere lo scopo, la funzione e i tipi di software per il controllo del contenuto, quali software per il filtraggio di Internet, software di controllo genitori.

Internet offre di tutto, nel bene e nel male, tuttavia non sempre è opportuno un accesso completo ai suoi contenuti, che possono essere inadatti per esempio ad un minore, come pornografia, violenza, gioco d'azzardo.
In altre situazioni, soprattutto di carattere aziendale, può essere opportuno evitare che gli utenti producano eccessivo traffico da e per Internet, intasando la connessione e rendendo lento e difficile il lavoro.
Esistono pertanto dei software che, in assenza dei genitori, nelle scuole o nelle aziende, da un lato svolgono un'opera di filtraggio dei contenuti delle pagine web, rendendone impossibile l'accesso, dall'altro possono impedire il download di determinati tipi di file. Se si utilizzano connessioni ad Internet il cui costo è legato alla quantità di dati scaricati, è consigliabile impostare un limite allo scaricamento dei dati, in modo da essere avvisati ed impedire ulteriori connessioni.

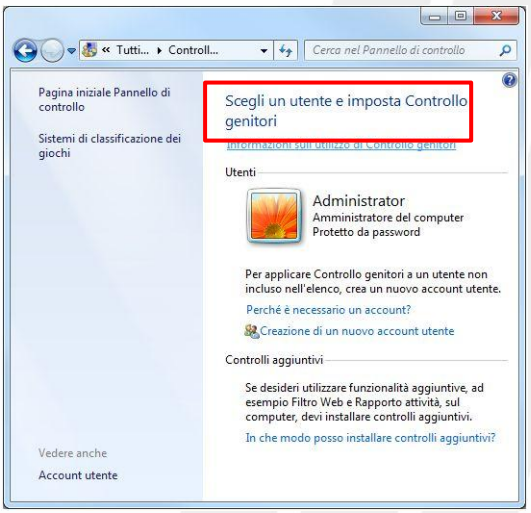


Ad esempio, tutti i browser dispongono di una funzione di ***Cronologia*** che consente di verificare quali siti sono stati visitati e in quale occasione.
In Internet Explorer si fa clic su ***Preferiti***, rappresentato dal simbolo della stella;

– nel menu a tendina che appare si sceglie la scheda ***Cronologia***.



I sistemi operativi possiedono specifiche sezioni che permettono di limitare l'accesso a siti a rischio, le ore di utilizzo del computer e l'utilizzo di alcune applicazioni, ad esempio in *Windows 7* si va su ***Start > Pannello di controllo > Controllo genitori***.



Si apre una finestra in cui impostare diversamente ogni utente.

4.2 Reti Sociali

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

Le reti sociali o ***social network***, sono strumenti di comunicazione e gestione delle conoscenze molto diffusi al giorno d'oggi sia tra i giovani che tra gli adulti.

A volte questi strumenti, per certi aspetti così utili, vengono utilizzati in modo poco attento, dimenticando che tutto ciò che viene messo su Internet diventa di pubblico dominio in modo rapido, anche se posto in rete per pochi attimi e, di fatto, se ne perde il controllo.

Per questo motivo è importante non utilizzare questi strumenti per comunicare dati riservati, come credenziali di accesso a servizi e sistemi informatici, PIN e qualsiasi altro dato personale e aziendale, soprattutto se di carattere economico e finanziario. Anche la pubblicazione di immagini private dovrebbe essere considerato con attenzione prima della pubblicazione, così come la divulgazione di idee e tendenze di carattere religioso, politico, sessuale.

Infatti tali informazioni potrebbero essere utilizzate per attuare furti o per profilare l'utente, con grave lesione di carattere finanziario o della privacy.

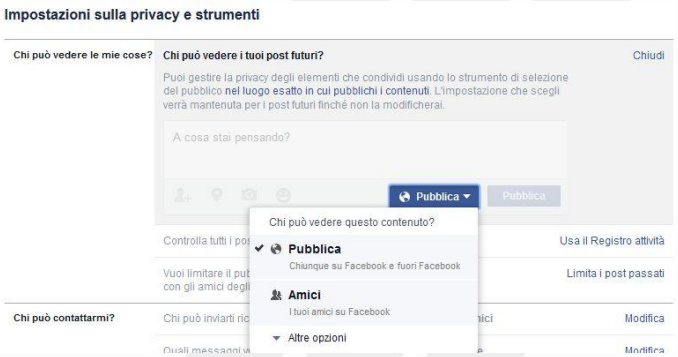
4.2.2 Essere consapevoli della necessità di applicare impostazioni adeguate per la privacy del proprio account su una rete sociale.

Utilizzando le reti sociali è possibile impostare la ***privacy*** del proprio profilo. I Social Networki mettono a disposizione dei loro utenti una serie di restrizioni nella diffusione delle notizie e delle immagini.

Ad esempio su Facebook, una delle reti sociali più diffuse, si fa clic sulla ***freccia nera*** rivolta in giù che si trova sulla Facebook toolbar e poi, dal menu a tendina che compare, si seleziona ***Impostazioni***.

Nella finestra che compare si seleziona ***Privacy*** ed appare la pagina ***Impostazione della privacy e strumenti*** che, prevede tre argomenti:

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



Per l'argomento "*Chi può vedere le mie cose*?" è possibile scegliere tra diverse opzioni:

- ***Pubblica;***
- ***Amici tranne conoscenti;***
- ***Solo io;***
- ***Personalizzata;***
- ***Amici più stretti;***
- ***Familiari;***
- ***Altre liste***.

Solo l'opzione ***Pubblica*** prevede la visualizzazione da chiunque nella rete, senza alcuna restrizione.

Si consiglia di non scegliere questa opzione, ma di selezionarne una un po' più "privata".

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

Chi utilizza le reti sociali può essere vittima di diversi tipi di attacco:

il ***Cyberbullismo*** consiste nell'utilizzo di Internet per attaccare ripetutamente un individuo attraverso e-mail, SMS, post su reti sociali, etc…, anche con informazioni fuorvianti o pericolose, contando sul fatto di non poter essere facilmente individuati;

*l'**Adescamento*** o ***Grooming*** consiste nel tentativo di acquisire la confidenza di una persona, generalmente un minore, allo scopo di indirizzarla verso comportamenti inappropriati;

le ***False Identità***, dette anche ***Fake***, consistono nel creare falsi profili su una rete sociale e vengono spesso usate per tentativi di adescamento e per il cyberbullismo;

i ***Link*** o ***Messaggi Fraudolenti***, sono truffe messe in atto attraverso la rete, come il *phishing* ed il *pharming*, che hanno lo scopo di carpire informazioni e trarre in inganno.

5 Comunicazioni

5.1 Posta elettronica

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

I messaggi di posta elettronicaa, se usati per scopi professionali, possono contenere informazioni molto riservate che una spia informatica potrebbe intercettare. Per evitare questo, di solito, i messaggi commerciali viaggiano in rete ***criptati***, cioè scritti con una ***chiave pubblica*** e leggibili solo con la corrispondente ***chiave privata***, in possesso del destinatario.

> La **crittografia** nasce dall'unione di due parole greche: *kryptós* che significa "nascosto", e *graphía* che significa "scrittura"; è la branca della crittologia che tratta delle "scritture nascoste", ovvero dei metodi per rendere un messaggio "offuscato" in modo da non essere comprensibile/intelligibile a persone non autorizzate a leggerlo.

5.1.2 Comprendere il termine firma digitale.

La ***firma digitale*** è un algoritmo, personale e legato alla sicurezza detta a ***chiavi asimmetriche***, che permette di certificare che il mittente di un messaggio di posta elettronica è veramente chi dice di essere. Ciò pertanto, unitamente alla cifratura del messaggio, rende la posta elettronica davvero sicura.

Nella ***crittografia a chiavi asimmetriche*** esiste una coppia di chiavi, una pubblica ed una privata. Tutti possono conoscere la chiave pubblica, solo il proprietario conosce quella privata. I messaggi crittografati con chiave pubblica possono essere decrittografati solo con la corrispondente chiave privata e i messaggi crittografati con chiave privata, solo con la corrispondente chiave pubblica.

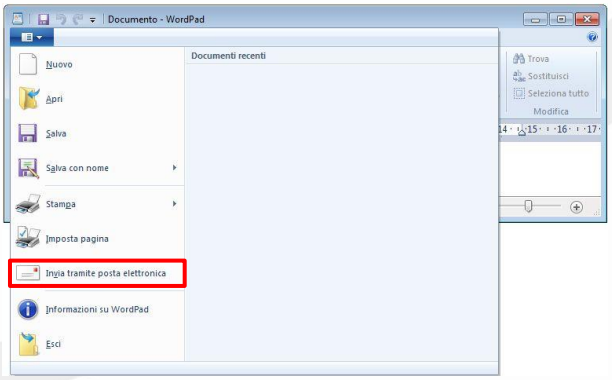
Quindi la ***firma digitale*** è costituita dal fatto che chi riceve il messaggio lo può rileggere solo con la corrispondente chiave pubblica di chi lo ha inviato, il quale non potrà mai negare di aver inviato l'offerta criptata con la sua chiave privata perché un messaggio che può essere reso leggibile con la chiave pubblica di una determinata persona, azienda o ente, attesta in modo assoluto l'identità di chi ha inviato il messaggio stesso.

5.1.3 Creare e aggiungere una firma digitale.

Per apporre una ***firma digitale***, prima di tutto occorre possederne una: le firme digitali vengono rilasciate da aziende o enti che garantiscono la vera identità del proprietario della firma, e utilizzano dispositivi, che garantiscano la generazione sicura della firma, come smart card e relativo lettore oppure chiavette USB o token.

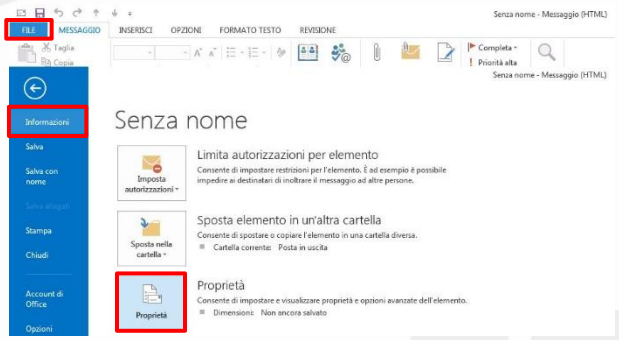
La creazione di una firma digitale consiste nella procedura che genera una coppia di chiavi, una pubblica a disposizione di tutti e una corrispondente privata che deve essere conservata dal titolare. E' un'operazione che occorre fare una sola volta. La firma ha una scadenza temporale stabilita e va abbinata al programma di posta in uso, utilizzando un'apposita estensione che varia a seconda del programma di posta e della procedura utilizzata per la generazione delle chiavi.

Bisogna conservare anche la frase usata nella procedura di generazione perché potrebbe servire per annullare in qualsiasi momento la firma digitale generata.



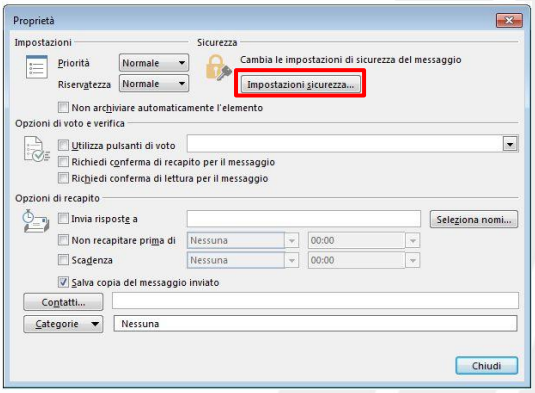
Con Wordpad, per esempio:

- si apre il documento da firmare;
- si fa clic su  e dal menu a tendina che appare si sceglie ***Invia tramite posta elettronica***.

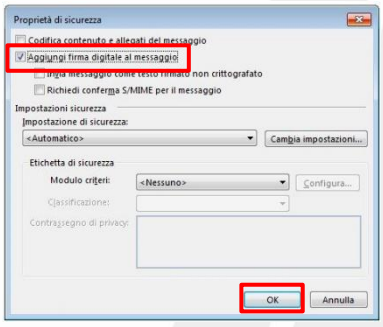


Nella finestra che si apre:

- si fa clic su ***File;***
- poi dal menu che appare su ***Informazioni;***
- poi su ***Proprietà***.



Si apre una nuova finestra in cui dobbiamo fare clic sul pulsante ***Impostazioni sicurezza***.



Nella finestra che appare si seleziona con il segno di spunta ***Aggiungi firma digitale al messaggio*** e poi si fa clic su ***OK***.

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

La posta elettronica è diventata nel corso degli anni anche uno strumento per inviare pubblicità indesiderata, chiamata in gergo "**spam**", o altri messaggi non richiesti tipo catene di Sant'Antonio. Si calcola che più della metà dei messaggi di posta elettronica in circolazione siano di questo tipo, cosa che ha costretto i provider di posta ad attivare filtri antispam sui propri server.
Chi utilizza un programma di posta può anche configurarlo per decidere all'arrivo quali messaggi gradisce che gli vengano proposti. Si tratta di filtri in base ai quali, tutti i messaggi che hanno un certo mittente, o alcune parole o un certo argomento come oggetto, vanno a finire nel cestino.

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

Con il termine ***phishing***, dall'inglese fishing, pescare, si intende il tentativo da parte di malintenzionati, di carpire dati riservati di un utente mediante l'invio di messaggi di Posta Elettronica fasulli ma apparentemente autentici, ad esempio sembrano provenire dalla banca, dall'ufficio postale, ecc…che detiene e vuole controllare le credenziali dell'utente.
In tal modo, l'utente ignaro viene indotto a fornire le proprie credenziali, tipo nome utente e password o altri dati riservati, come il numero della carta di credito, senza rendersi conto che le fornisce ad un perfetto sconosciuto, probabilmente malintenzionato.
Un tentativo di ***phishing*** è facilmente riconoscibile in varie modalità:

- prima di tutto NESSUNA istituzione chiederà mail a conferma delle credenziali tramite e-mail;
- spesso il linguaggio utilizzato non è la lingua dell'utente, oppure è una cattiva traduzione;
- un messaggio di phishing di solito contiene un link a un sito web dove inserire le credenziali, apparentemente identico a quello ufficiale dell'istituzione, ma ospitato su un server con un nome di dominio differente; è quindi sufficiente controllare nella barra dell'indirizzo se il dominio è davvero quello dell'istituzione o differente, cioè se è certificato, e se la comunicazione avviene in modo sicuro, con protocollo ***https***.

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

I messaggi di posta possono anche contenere ***malware***, generalmente sotto forma di allegati. Prima di aprire un allegato è bene essere certi che il mittente sia fidato, che lo abbia inviato volontariamente, perché se il computer del mittente è stato infettato da un virus i messaggi vengono spediti a tutti gli indirizzi della sua rubrica senza che il proprietario del computer se ne renda conto.
È quindi utile, attraverso una ***scansione antivirus***, controllare che gli allegati ricevuti non siano infetti.

5.2 Messaggistica Istantanea

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

Il sistema di **Messaggistica Istantanea**, in inglese ***Instant Messaging***, consente di scambiare in tempo reale, fra utenti connessi in rete, frasi e brevi testi e pure parlare in videoconferenza grazie all'uso di una webcam.
Si utilizza, di solito, un'applicazione specifica come *Whastsapp*, *Yahoo Messenger*, *Facebook Messenger*, ecc… o un analogo servizio integrato in una applicazione, come ad esempio la messaggistica istantanea di *Skype*, e sullo schermo del nostro computer, tablet o smartphone appare un riquadro con la lista dei contatti, dalla quale vediamo quante e quali persone sono collegate al momento.

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

Quando si utilizza la messaggistica istantanea, si sta al computer per molto tempo e il collegamento prolungato ad Internet può consentire a chi vuole introdursi in modo furtivo da una "porta posteriore" di farlo con più certezza di riuscita. Spesso girano in rete programmi appositi alla ricerca di "porte aperte".
Questi malware sono chiamati ***backdoor*** che in inglese significa appunto porta posteriore.

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

Come per la posta elettronica e le reti sociali, per ridurre il rischio di infezioni e di perdita di dati personali, è opportuno ricorrere a metodi di ***cifratura delle comunicazioni***, ma anche stare attenti a non divulgare informazioni personali e commerciali, ridurre allo stretto necessario la condivisione di file e provvedere a cancellarli, una volta terminato il lavoro in comune.
Inoltre, come per gli allegati della posta elettronica, occorre stare attenti quando si apre un file ricevuto da altre persone tramite un programma di messaggistica istantanea.

6 Gestione sicura dei dati

6.1 Messa in Sicurezza e salvataggio di dati

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

La sicurezza fisica dei dispositivi, ad esempio computer, periferiche, apparecchiature di rete, memorie di massa, tablet, etc… è molto importante non tanto per il loro valore economico, quanto per il valore del software installato e per i dati aziendali che si trovano al loro interno.

Non esistono metodi sicuri per evitare che un'apparecchiatura venga smarrita, sottratta o danneggiata, ma esistono precauzioni per limitare i danni:

- le apparecchiature elettroniche aziendali vanno installate in un unico locale soggetto a sorveglianza e con accesso limitato agli operatori. In caso di grandi aziende di solito esiste un sito distante da quello utilizzato in cui sono duplicate almeno le apparecchiature essenziali, come le unità centrali, le unità di memorizzazione di massa, ecc…;
- le apparecchiature presenti negli uffici, tipo PC, stampanti, ecc.. vanno inventariate e controllate periodicamente;
- le apparecchiature installate in luoghi aperti al pubblico vanno bloccate al banco, tavolo o altro dove sono in mostra, utilizzando l'opportuno ***Cavo di Sicurezza,*** che in caso di PC portatili, termina con un lucchetto che si blocca nel guscio del PC stesso, nel **Kensington Security Slot** che è un piccolo foro presente in quasi tutti i computer portatili o monitor LCD, ideato per assicurali al tavolo ed evitarne il furto.
  Questo foro e l'apposito cavo compatibili con il foro Kensington sono principalmente distinguibili in due categorie, quelli con la chiave o quelli che utilizzano un codice numerico, come per le valigie.
  Uno dei maggiori deterrenti del **Cavo Kensington** è il fatto che la forzatura di questo lucchetto provoca una distruzione delle plastiche intorno al portatile, con una conseguente impossibilità a rivendere lo stesso, quindi scoraggiando lo scippo.




È inoltre importante tenere traccia della collocazione dei dispositivi, così come dei loro dettagli, in modo da poter verificare in modo preciso eventuali mancanze.

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

Il sistema operativo di un computer o i programmi possono facilmente essere reinstallati se il computer, per qualche motivo, si guasta e non funziona più, in quanto è sempre possibile riutilizzare i supporti su cui erano stati memorizzati o, al limite, riacquistarli.

I propri dati, quelli creati dall'utente del computer e memorizzati su un supporto magnetico, in caso di guasto non recuperabile del computer e, in particolare, del disco rigido, oppure di cancellazione involontaria degli stessi, non possono essere recuperati, salvo in rari casi e a costi molto elevati.

Pertanto è utile, e **per le aziende è obbligatorio**, predisporre delle copie di sicurezza dei dati, chiamate ***backup***, che devono essere custodite lontano da polvere, calore e fonti magnetiche e soprattutto in un luogo diverso da quello in cui si trova il computer per garantire l'integrità dei dati anche in caso di eventi catastrofici che possono coinvolgere l'intero edificio, tipo furti, incendio, terremoto, ecc...

La copia di sicurezza può essere fatta su supporti magnetici come ad esempio:

- chiavetta USB;
- disco rigido esterno;
- nastro;
- NAS;

oppure di tipo ottico come ad esempio:

- CD o DVD

oppure, ed oggi è sempre più diffuso, direttamente su un server remoto via internet denominato ***cloud***, come ad esempio Dropbox, Google Drive e Onedrive, etc.

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

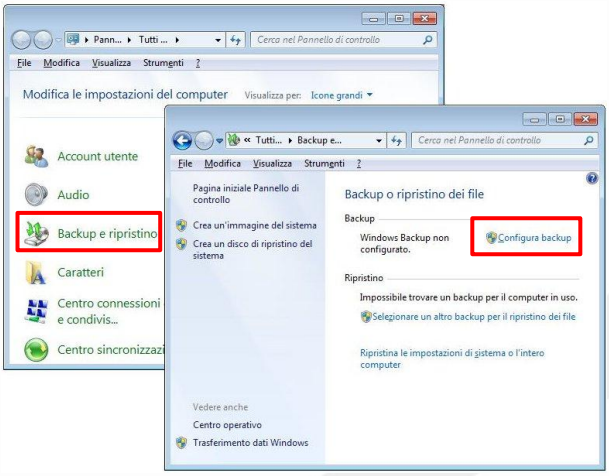
Di solito nelle aziende le copie di sicurezza sono organizzate in una procedura detta ***backup programmato***, cioè le copie dei dati vengono fatte a scadenze regolari in un momento in cui il computer rimane acceso ma non viene utilizzato, per evitare che la copia dei dati rallenti il lavoro.

Infine occorre prestare attenzione alla collocazione della copia di sicurezza: se la copia viene posta accanto al dispositivo, anch'essa corre il rischio di essere persa, per furto, danneggiamento, a causa di eventi naturali, ecc... La copia di sicurezza va quindi posta in un luogo, il più sicuro possibile, diverso dall'originale. Negli ultimi tempi per questo motivo sempre più spesso la copia dei sicurezza dei dati viene effettuata online, su appositi ***Service Provider*** che offrono il servizio di conservazione dei dati in rete, ***storage network*** in inglese.

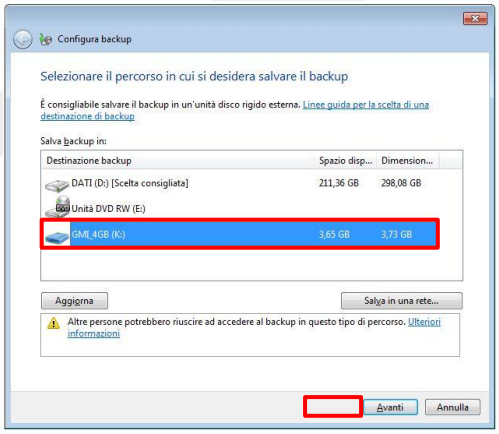
Tutte le grandi organizzazioni che sono soggette all'obbligo di legge della conservazione dei dati per lunghi periodi, tra i cinque e i dieci anni, di solito, se non ricorrono all'archiviazione presso ***Service Provider***, adottano per la procedura di backup i supporti a nastro magnetico. Questi hanno caratteristiche di compattezza, velocità di scrittura, capacità fino a 4GB, possibilità di riuso e basso costo e sono una tecnologia stabile nel tempo, essendo rimasti uguali a tanti anni fa e, possono per questo garantire il riuso di dati registrati anni indietro.

I piccoli utenti, di solito, si affidano invece al programma di backup che è ormai presente in tutti i sistemi operativi per PC ed utilizzano come supporto dati un DVD o un disco esterno USB.

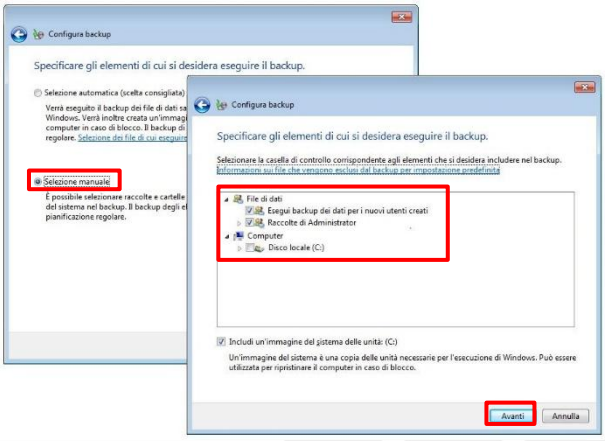
6.1.4 Effettuare la copia di sicurezza di dati.



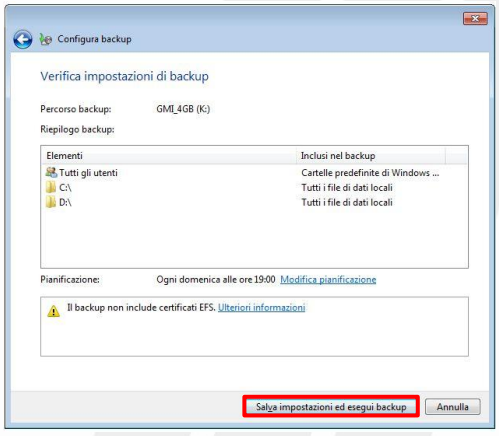
Per eseguire un backup di un'unità di disco in *Windows 7* si va su ***Start > Pannello di controllo > Backup e ripristino***. Si apre una finestra in cui fare clic su ***Configura backup*.**



Nella nuova finestra che appare si sceglie l'unità di destinazione si seleziona il disco o la chiavetta USB su cui copiare i dati e si fa clic sul pulsante ***Avanti***.



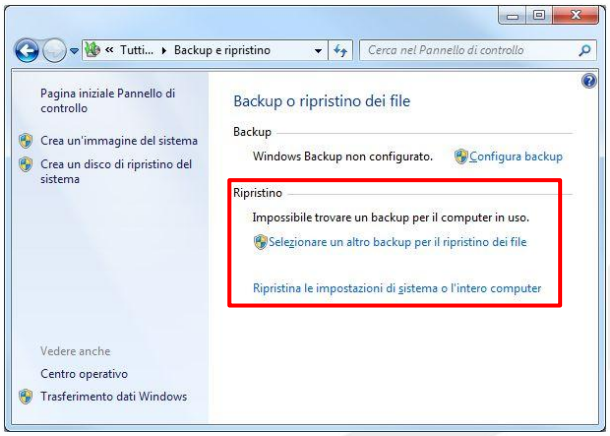
Si apre un'altra finestra in cui specificare gli elementi di cui si desidera eseguire il backup. Fare clic su ***Selezione manuale*** e poi su ***Avanti***, nella finestra che si apre selezionare con il ***segno di spunta*** gli elementi di cui fare la copia, poi fare clic su ***Avanti***.



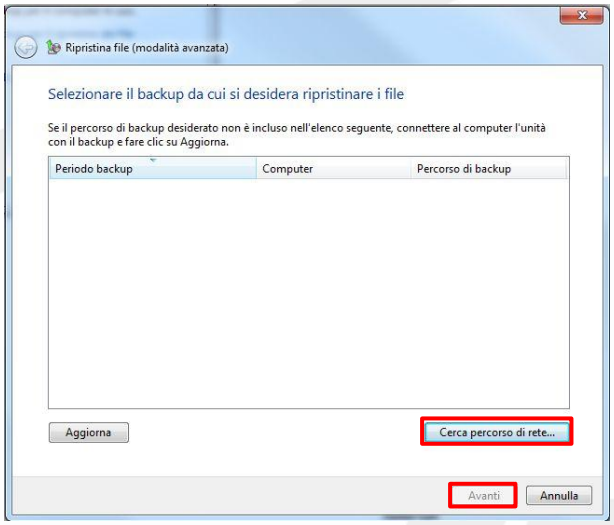
Si verificano le impostazioni date e si fa clic su ***Salva impostazioni ed esegui backup***.

6.1.5 Ripristinare e validare i dati sottoposti a copia di sicurezza.

L'operazione di ripristino può essere fatta per ritrovare file o cartelle che protrebbero essere andati persi.



Per eseguire un backup di un'unità di disco in *Windows 7* si va su ***Start > Pannello di controllo > Backup e ripristino***. Si apre una finestra in cui fare clic su ***Selezionare backup per il ripristino dei file***.



Si apre una finestra in cui selezionare il backup da cui si desidera ripristinare i file facendo clic sul pulsante ***Cerca percorso di rete.*** Dopo di che si fa clic su ***Avanti***, nella finestra che appare si seleziona la destinazione del ripristino e ancora clic su ***Avanti***.

6.2 Distruzione Sicura

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

Quando un dispositivo che contiene una memoria di massa si guasta e non è più utilizzabile, prima di smaltirlo come rifiuto occorre formattare le memorie di massa eliminando qualsiasi dato aziendale o personale che potrebbe essere recuperato da una spia digitale e qualsiasi programma commerciale che potrebbe essere riusato violando le regole il contratto di vendita.

6.2.2 Distinguere tra cancellare i dati e distruggerli in modo permanente.

È importante essere coscienti del fatto che la semplice cancellazione di un file non garantisce la sua effettiva rimozione. Ciò per due motivi:

- i moderni sistemi operativi dispongono di una cartella speciale, chiamata ***Cestino***, dove vengono spostati i file cancellati. È pertanto sempre possibile ripristinare dati cancellati in questo modo;
- anche se i file vengono cancellati dal ***Cestino***, in realtà ne rimangono delle tracce sul disco. Pertanto, anche se non saranno visibili con gli strumenti tradizionali, con programmi specifici possono essere ricostruiti integralmente o quasi, a seconda del tempo che passa dalla loro cancellazione e dall'uso che viene fatto del computer.
- Un sistema per cancellare in modo definitivo i dati è la *formattazione completa del disco* che distrugge i dati rendendoli irrecuperabili. Un sistema migliore è la *riscrittura del disco* eseguita più volte, attraverso particolari programmi di cancellazione.

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

Per cancellare in modo definitivo i dati, compito importante perché ha riflessi economici ed anche legali, è necessario pertanto utilizzare altri metodi:

- per i documenti cartacei è opportuno utilizzare dei ***tritadocumenti***, che tagliano a striscioline o riducono a coriandoli i fogli;
- le memorie di massa da eliminare vanno rese inutilizzabili in modo meccanico o smagnetizzate per mezzo di apparecchi come ad esempio il ***degausser***, un macchinario in grado di applicare intensi campi magnetici;
- i CD e i DVD vengono resi inservibili deformandoli in modo meccanico.

Appendice A - Syllabus

Scopo

Questo documento presenta il Syllabus di ***ECDL IT Security – Sicurezza Informatica***.
Il Syllabus descrive, attraverso i risultati del processo di apprendimento, la conoscenza e le capacità di un candidato.
Il Syllabus fornisce inoltre le basi per il test teorico e pratico relativo a questo modulo.

Nota del traduttore

La versione ufficiale in lingua inglese del Syllabus ***ECDL IT Security – Sicurezza Informatica*** è quella pubblicata sul sito web della Fondazione ECDL che si trova all'indirizzo **www.ecdl.org**.
Tanto la natura "definitoria" del testo, quanto la sua forma schematica costituiscono ostacoli di fronte ai quali è necessario trovare qualche compromesso; pur cercando di rendere al meglio in lingua italiana i concetti espressi nell'originale inglese, in alcuni casi sono evidenti i limiti derivanti dall'uso di un solo vocabolo per tradurre una parola inglese. Tale limite è particolarmente riduttivo per i verbi che dovrebbero identificare con maggiore esattezza i requisiti di conoscenza o competenza: moltissime voci contengono verbi come understand, know, know about, che sono stati solitamente tradotti con "comprendere", "conoscere", "sapere", ma che potrebbero valere anche per "capire", "intendere", "definire", "riconoscere", "essere a conoscenza"...
Per alcuni vocaboli tecnici è inoltre invalso nella lingua l'uso del termine inglese (es. *hardware*, *software*), e in molti casi – pur cercando di non assecondare oltre misura questa tendenza – si è ritenuto più efficace attenersi al vocabolo originale o riportarlo tra parentesi per maggior chiarezza. Si invitano i lettori che abbiano particolari esigenze di analisi approfondita dei contenuti a fare riferimento anche alla versione inglese di cui si è detto sopra.

Limitazione di responsabilità

Benché la Fondazione ECDL abbia messo ogni cura nella preparazione di questa pubblicazione, la Fondazione ECDL non fornisce alcuna garanzia come editore riguardo la completezza delle informazioni contenute, né potrà essere considerata responsabile per eventuali errori, omissioni, inaccuratezze, perdite o danni eventualmente arrecati a causa di tali informazioni, ovvero istruzioni ovvero consigli contenuti nella pubblicazione. Le informazioni contenute in questa pubblicazione non possono essere riprodotte né nella loro interezza né parzialmente senza il permesso e il riconoscimento ufficiale da parte della Fondazione ECDL. La Fondazione ECDL può effettuare modifiche a propria discrezione e in qualsiasi momento senza darne notifica.

[1] Tutti i riferimenti alla Fondazione ECDL riguardano la European Computer Driving Licence Foundation Ltd.

Sezione	Tema	Rif.	Argomento
1. Concetti di sicurezza	*1.1 Minacce ai dati*	1.1.1	Distinguere tra dati e informazioni
		1.1.2	Comprendere il termine crimine informatico
		1.1.3	Comprendere la differenza tra hacking, cracking e hacking etico
		1.1.4	Riconoscere le minacce ai dati provocate da forza maggiore, quali fuoco, inondazione, guerra, terremoto
		1.1.5	Riconoscere le minacce ai dati provocate da impiegati, fornitori di servizi e persone esterne
	1.2 Valore delle informazioni	1.2.1	Comprendere i motivi per proteggere le informazioni personali, quali evitare il furto di identità o le frodi
		1.2.2	Comprendere i motivi per proteggere informazioni commercialmente sensibili, quali prevenzione di furti, di uso improprio dei dati dei clienti o di informazioni finanziarie
		1.2.3	Identificare le misure per prevenire accessi non autorizzati ai dati, quali cifratura, password
		1.2.4	Comprendere le caratteristiche fondamentali della sicurezza delle informazioni, quali confidenzialità, integrità, disponibilità
		1.2.5	Identificare i requisiti principali per la protezione, conservazione e controllo di dati/privacy che si applicano in Italia
		1.2.6	Comprendere l'importanza di creare e attenersi a linee guida e politiche per l'uso dell'ICT
	1.3 Sicurezza personale	1.3.1	Comprendere il termine "ingegneria sociale" e le sue implicazioni, quali raccolta di informazioni, frodi e accesso a sistemi informatici
		1.3.2	Identificare i metodi applicati dall'ingegneria sociale, quali chiamate telefoniche, phishing, shoulder surfing al fine di carpire informazioni personali
		1.3.3	Comprendere il termine furto di identità e le sue implicazioni personali, finanziarie, lavorative, legali.
		1.3.4	Identificare i metodi applicati per il furto di identità, quali acquisire informazioni a partire da oggetti e informazioni scartati, fingendosi qualcun altro o mediante skimming
	1.4 Sicurezza file	1.4.1	Comprendere l'effetto di attivare/disattivare le impostazioni di sicurezza delle macro
		1.4.2	Impostare una password per file quali documenti, file compressi, fogli di calcolo
		1.4.3	Comprendere i vantaggi e i limiti della cifratura
2. Malware	*2.1 Definizione e funzione*	2.1.1	Comprendere il termine malware
		2.1.2	Riconoscere diversi modi con cui il malware si può nascondere, quali trojan, rootkit e backdoor
	2.2 Tipi	2.2.1	Riconoscere i tipi di malware infettivo e comprendere come funzionano, ad esempio virus e worm
		2.2.2	Riconoscere i tipi di malware usati per furto di dati, profitto/estorsione e comprendere come operano, ad esempio adware, spyware, botnet, keylogger e dialer
	2.3 Protezione	2.3.1	Comprendere come funziona il software anti-virus e quali limitazioni presenta

3 Sicurezza in rete	*3.1 Reti*	3.1.1	Comprendere il termine rete e riconoscere i più comuni tipi di rete, quali LAN (rete locale), WAN (rete geografica), VPN (rete privata virtuale)
		3.1.2	Comprendere il ruolo dell'amministratore di rete nella gestione delle operazioni di autenticazione, autorizzazione e assegnazione degli account all'interno di una rete
		3.1.3	Comprendere la funzione e i limiti di un firewall
	3.2 Connessioni di rete	3.2.1	Riconoscere le possibilità di connessione ad una rete mediante cavo o wireless
		3.2.2	Comprendere che la connessione ad una rete ha implicazioni di sicurezza, quali malware, accessi non autorizzati ai dati, mantenimento della privacy
	3.3 Sicurezza su reti wireless	3.3.1	Riconoscere l'importanza di richiedere una wireless password per proteggere gli accessi a reti wireless
		3.3.2	Riconoscere diversi tipi di sicurezza per reti wireless, quali WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access), MAC (Media Access Control)
		3.3.3	Essere consapevoli che usando una rete wireless non protetta si rischia che i propri dati vengano intercettati da "spie digitali"
		3.3.4	Connettersi ad una rete wireless protetta/non protetta Comprendere il ruolo dell'amministratore di rete nella gestione delle operazioni di autenticazione, autorizzazione e assegnazione degli account all'interno di una rete
	3.4 Controllo di accesso	3.4.1	Comprendere lo scopo di un account di rete e come accedere alla rete usando un nome utente e una password
		3.4.2	Riconoscere buone politiche per la password, quali evitare di condividere le password, modificarle con regolarità, sceglierle di lunghezza adeguata e contenenti un numero accettabile di lettere, numeri e caratteri speciali
		3.4.3	Identificare le comuni tecniche di sicurezza biometriche usate per il controllo degli accessi, quali impronte digitali, scansione dell'occhio
4 Uso sicuro del web	*4.1 Navigazione in rete*	4.1.1	Essere consapevoli che alcune attività in rete (acquisti, transazioni finanziarie) dovrebbero essere eseguite solo su pagine web sicure
		4.1.2	Identificare un sito web sicuro, ad esempio associato ad https, simbolo del lucchetto
		4.1.3	Essere consapevoli del pharming
		4.1.4	Comprendere il termine "certificato digitale". Convalidare un certificato digitale
		4.1.5	Comprendere il termine "one-time password
		4.1.6	Selezionare impostazioni adeguate per attivare, disattivare il completamento automatico, il salvataggio automatico quando si compila un modulo
		4.1.7	Comprendere il termine "cookie"
		4.1.8	Selezionare impostazioni adeguate per consentire, bloccare i cookie
		4.1.9	Eliminare dati privati da un browser, quali cronologia di navigazione, file temporanei di internet, password, cookie, dati per il completamento automatico
		4.1.10	Comprendere lo scopo, la funzione e i tipi di software per il controllo del contenuto, quali software per il filtraggio di internet, software di controllo genitori

	4.2 Reti sociali	4.2.1	Comprendere l'importanza di non divulgare informazioni riservate su siti di reti sociali.
		4.2.2	Essere consapevoli della necessità di applicare impostazioni adeguate per la privacy del proprio account su una rete sociale.
		4.2.3	Comprendere i rischi potenziali durante l'uso di siti di reti sociali, quali cyberbullismo, adescamento, informazioni fuorvianti/pericolose, false identità, link o messaggi fraudolenti.
5 Comunicazioni	*5.1 Posta elettronica*	5.1.1	Comprendere lo scopo di cifrare, decifrare un messaggio di posta elettronica
		5.1.2	Comprendere il termine firma digitale
		5.1.3	Creare e aggiungere una firma digitale
		5.1.4	Essere consapevoli della possibilità di ricevere messaggi fraudolenti e non richiesti
		5.1.5	Comprendere il termine phishing. Identificare le più comuni caratteristiche del phishing, quali uso del nome di aziende e persone autentiche, collegamenti a falsi siti web
		5.1.6	Essere consapevoli del rischio di infettare il computer con malware attraverso l'apertura di un allegato contenente una macro o un file eseguibile
	5.2 Messaggistica istantanea	5.2.1	Comprendere il termine messaggistica istantanea (IM) e i suoi usi
		5.2.2	Comprendere le vulnerabilità di sicurezza della messaggistica istantanea, quali malware, accesso da backdoor, accesso a file
		5.2.3	Riconoscere metodi per assicurare la confidenzialità durante l'uso della messaggistica istantanea, quali cifratura, non divulgazione di informazioni importanti, limitazione di condivisione di file
6 Gestione sicura	*6.1 Messa in sicurezza e*	6.1.1	Riconoscere modi per assicurare la sicurezza fisica dei dati salvataggio di dati di dispositivi, quali registrare la collocazione e i dettagli degli apparati, usare cavi di sicurezza, controllare gli accessi
		6.1.2	Riconoscere l'importanza di avere una procedura di copie di sicurezza per ovviare alla perdita di dati, di informazioni finanziarie, di segnalibri/cronologia web
		6.1.3	Identificare le caratteristiche di una procedura di copie di sicurezza, quali regolarità/frequenza, pianificazione, collocazione della memoria di massa
		6.1.4	Effettuare la copia di sicurezza di dati
		6.1.5	Ripristinare e validare i dati sottoposti a copia di sicurezza
	6.2 Distruzione sicura	6.2.1	Comprendere il motivo per eliminare in modo permanente i dati dalle memorie di massa o dai dispositivi
		6.2.2	Distinguere tra cancellare i dati e distruggerli in modo permanente
		6.2.3	Identificare i metodi più comuni per distruggere i dati in modo permanente, quali uso di trita documenti, distruzione di memorie di massa/dispositivi, smagnetizzazione, uso di utilità per la cancellazione definitiva dei dati

"La maggior parte degli insegnanti perdono tempo a fare domande che mirano a scoprire ciò che l'alunno non sa, mentre la vera arte del fare domande mira a scoprire ciò che l'alunno sa o è capace di sapere.
Il valore di un'educazione superiore non sta nell'insegnare molti fatti, ma nell'allenare la mente a pensare ciò che non si può trovare sui manuali"

Albert Einstein