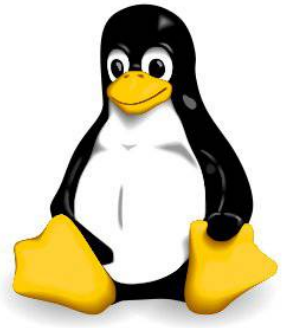
ECDL

con software libero



Modulo 12

IT Security

ECDL

AICA
Associazione Italiana per l'Informatica ed il Calcolo Automatico

Indice generale

IT SECURITY

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, ecc...) che rappresentano fatti o eventi non ancora organizzati. Le **informazioni** sono dati organizzati in modo da essere comprensibili e significativi per l'utente.

1.1.2 Comprendere il termine crimine informatico.

Un crimine informatico è un crimine attuato per mezzo dell'abuso degli strumenti informatici, come computer e internet. Esempi di crimine informatico sono la frode informatica, il furto d'identità o l'accesso non autorizzato a sistemi informatici.

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

Il termine hacking deriva dal verbo inglese to hack (intaccare) 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. Colui che pratica l'hacking viene identificato come hacker.

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, si parla di cracking. Colui che pratica il cracking viene identificato come cracker.

Per hacking etico si intende l'utilizzo delle tecniche di hacking per monitorare la sicurezza dei sistemi e delle reti informatiche 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.

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

I 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; così, 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.

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 o informazioni di carattere finanziario, è per certi aspetti ancora più essenziale proteggere queste informazioni, in quanto se venissero utilizzate illegalmente la società che li deteneva 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 proteggerli con determinate tecniche per mezzo delle quali, anche se finissero nelle mani di malintenzionati (per esempio se immagazzinati su dispositivi mobili che possono più facilmente essere rubati), non potrebbero essere utilizzati.

La prima cosa da fare è proteggere con password robuste 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).

La crittografia ha una lunga storia alle spalle, ed è stata utilizzata anche in tempi antichi per evitare che i messaggi venissero compresi da nemici. In campo informatico esistono oggi algoritmi e software sicuri e semplici da utilizzare.

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, 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 aggiornato il 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 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).

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 social engineering) è lo studio del comportamento individuale di una persona al fine di carpire informazioni utili.

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. Uno di questi sono le chiamate telefoniche che, a volte promettendo premi, cercano di ottenere informazioni personali mascherandole con sondaggi anonimi.

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 shoulder surfing (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 a un servizio (accesso a un PC, a una rete locale, a internet, alla posta elettronica, a una rete sociale, a un servizio di internet banking) allo scopo di usarlo a proprio vantaggio, per compiere crimini informatici come frodi o furti.

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 (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 semsibili, 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 della tastiera.

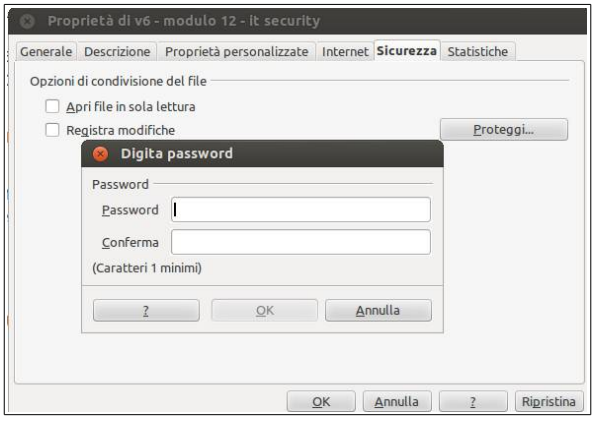
1.4 SICUREZZA DEI FILE

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 e 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...) automaticamente o alla pressione di una combinazione di tasti.

Le macro sono strumenti molto utili perché automatizzano procedure lunghe e noiose, ma possono contenere codice malevolo che quindi può 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.



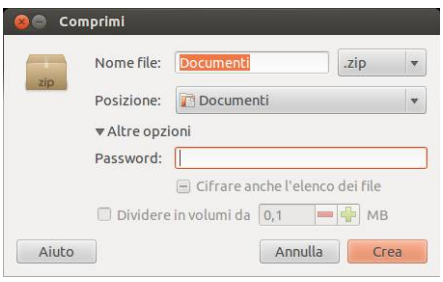
Al contrario, disattivare una macro non ne consente l'esecuzione e quindi impedisce di avvalersi delle sue funzionalità, ma mette al sicuro il computer da possibile codice malevolo.

In linea di massima la cosa migliore è attivare le macro di cui si è certi, e disattivare quelle di incerta provenienza.

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

È possibile impostare una password per proteggere un file da accesi indesiderati. Per farlo utilizzando le applicazioni di Libreoffice occorre:

- aprire il file da proteggere
- scegliere Proprietà... dal menu File
- nella scheda Sicurezza cliccare sul pulsante Proteggi...
- inserire e confermare la password da applicare

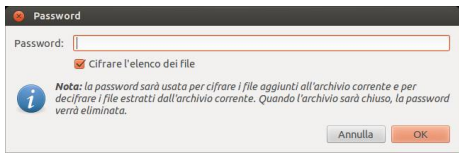


Per proteggere con password un archivio compresso, si può procedere in

due modi a seconda che l'archivio sia già stato creato oppure ancora da creare:

- durante la creazione di un archivio compresso si deve scegliere Altre opzioni e indicare la password (da notare che ciò è possibile solo con alcuni formati di compressione, tra cui zip)
- per proteggere un archivio già creato in precedenza si deve aprire il file col programma Gestore archivi, scegliere Modifica password dal menu Modifica

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.

Inoltre, perché la protezione funzioni, è necessario scegliere una password robusta, che corrisponda a determinati criteri che la rendono inattaccabile, e che sia ben protetta, cioè non diffusa o facilmente ricostruibile con una delle tecniche sopra accennate.

2 Malware

2.1 DEFINIZIONE E FUNZIONE

2.1.1 Comprendere il termine malware.

Il termine malware indica un software creato con lo scopo di causare danni più o meno gravi a un sistema informatico su cui viene eseguito e ai dati degli utenti.

Il termine deriva dalla contrazione delle parole inglesi *malicious* e *software* e ha dunque il significato letterale di "programma malevolo".

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 horse**: software che oltre ad avere delle funzionalità "lecite", utili per indurre l'utente ad utilizzarli, contengono istruzioni dannose che vengono eseguite all'insaputa dell'utilizzatore
- **Backdoor**: letteralmente "porta sul retro". Sono dei programmi che consentono un accesso non autorizzato al sistema su cui sono in esecuzione
- **Rootkit**: 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.

- i **Virus** sono parti di codice che si diffondono copiandosi all'interno di altri programmi, o in una particolare sezione del disco fisso, in modo da essere eseguiti ogni volta che il file infetto viene aperto. Si trasmettono da un computer a un altro tramite lo spostamento di file infetti ad opera degli utenti
- i **Worm** non hanno bisogno di infettare altri file per diffondersi, perché modificano il sistema operativo in modo da essere eseguiti automaticamente e tentare di replicarsi sfruttando per lo più Internet. Per indurre gli utenti ad eseguirli utilizzano tecniche di ingegneria sociale, oppure sfruttano dei difetti (Bug) di alcuni programmi per diffondersi automaticamente. Il loro scopo è rallentare il sistema con operazioni inutili o dannose.

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.

- Gli **Adware** sono software che presentano all'utente messaggi pubblicitari durante l'uso. Possono causare danni quali rallentamenti del pc e rischi per la privacy in quanto comunicano le abitudini di navigazione ad un server remoto.
- Uno **Spyware** è un software che viene usato per raccogliere informazioni (abitudini di navigazione, ma anche password) per trasmetterle ad un destinatario interessato

- I **Keylogger** sono dei programmi in grado di registrare tutto ciò che viene digitato sulla tastiera consentendo il furto di password
- I **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
- una **botnet** è l'infezione di una rete informatica che viene controllata da remoto dal botmaster, che è in grado di utilizzare la rete stessa e i dispositivi ad essa collegati per svolgere attività non autorizzate.

2.3 PROTEZIONE

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

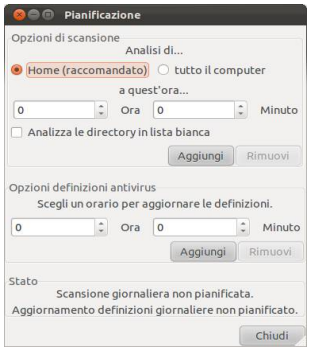
Soprattutto sui dispositivi con sistema operativo Windows, è necessario avere installato un software antivirus, che sia in grado di opporsi ai tentativi dei malware di infettare il sistema. In realtà nessun sistema operativo è immune dai malware, ma Windows è più vulnerabile sia per motivi strutturali, 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 portyatori 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 anche 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 indicano come virus programmi del tutto leciti.

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



Nell'ambito Linux esistono pochi software antivirus dei quali il solo ClamAv, un antivirus utilizzato generalmente sui server da linea di comando, è open source. Esiste un'interfaccia grafica denominata Clamtk, che si può installare utilizzando Ubuntu Software Center o da terminale col comando sudo apt-get install clamtk.

L'interfaccia è minimale, e permette di effettuare la scansione dell'intera cartella home, di un file o di una cartella.

È anche possibile pianificare scansioni scegliendo Pianificatore... dal menu Avanzate o anche con la combinazione di tasti Ctrl + T.

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 una apposita cartella creata dal software antivirus e pertanto facilmente controllabile, e resi non eseguibili attraverso la modifica dei permessi (in ambiente Linux o Mac) o dell'estensione del file (in ambiente Windows).

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.

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 comprende più dispositivi, come computer o altro, in grado di comunicare tra di essi attraverso differenti mezzi.

Una rete può essere limitata nello spazio, per esempio a un locale o a un edificio e prende il nome di **LAN** (Local Area Network).

Se la rete è estesa a un'area cittadina prende il nome di **MAN** (Metropolitan Area Network). Se la rete è molto estesa come ad esempio Internet, prende il nome di **WAN** (Wide Area Network).

Una **VPN** (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.

Una rete viene gestita da un amministratore che si occupa di renderla sicura ed efficiente attraverso l'implementazione di politiche di accesso alle risorse (file, cartelle, stampanti, accesso a internet, ecc...).

Per definire tali politiche è necessario che gli utenti dei dispositivi che fanno parte della rete dispongano di un account attraverso il quale vengano autenticati col proprio nome utente e password.

3.1.3 Comprendere la funzione e i limiti di un firewall.

Un firewall è un dispositivo o un software che monitora e controlla in base a delle regole, definite dall'amministratore, il traffico di rete, generalmente tra la rete locale (LAN) e internet, allo scopo di evitare intrusioni e accessi non autorizzati.

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 del firewall non sarà efficace.

Inoltre, dato che il firewall è generalmente posto tra la rete locale e internet, non avrà effetto se l'attacco alla rete viene effettuato dall'interno, per esempio da un utente della rete o dal un malware che precedentemente ha infettato 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 (senza cavo) o wifi.

I vantaggi di una rete cablata sono la maggiore sicurezza, dovuta al fatto che è necessario connettere fisicamente i dispositivo 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.

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 laddove, 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 da internet 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.

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.

Il **WEP** (Wired Equivalent Privacy, cioè sicurezza della privacy equivalente a quella delle reti cablate) nasce nel 1999 ma nel giro di pochi anni si è verificato che non è adeguatamente sicuro, in quanto essendo la chiave troppo breve, è abbastanza facile individuarla e poter quindi accedere.

Il **WPA** (Wifi Protected Access, accesso protetto alle reti senza fili) e il successivo WPA2 sono stati elaborati nel 2003/2004 e mettono a disposizione una maggiore sicurezza rispetto al precedente WEP, che tuttavia non è totale.

Il **MAC**, detto anche 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".

Se una rete senza fili non è protetta con uno o più dei metodi sopra presentati, 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.

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. In tal caso tutti i sistemi operativi dispongono di un programma di connessione che, generalmente, avvisa l'utente della disponibilità di reti senza fili.

In Ubuntu nel pannello superiore, tra l'icona del Bluetooth e quella del volume, appare l'icona della connessione di rete. In figura è presente quella di una connessione wireless, mentre quando si è connessi a una rete cablata,

l'icona è differente, formata da due frecce con direzione opposta.

Per connettersi ad una rete wireless basta cliccare sul nome presente nell'elenco. Se la rete è non è protetta (lo si capisce perché in basso a destra non è presente il lucchetto), si viene connessi automaticamente. Se la rete è protetta (lo si capisce perché è presente un lucchetto), viene chiesta la password di accesso.

Se la password inserita è corretta, al termine della procedura, viene segnalato che la connessione alla rete senza fili è stata stabilita.

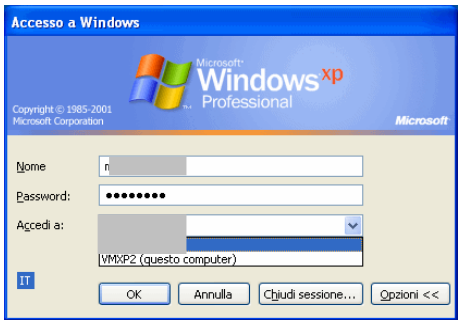
3.4 CONTROLLO DI ACCESSO

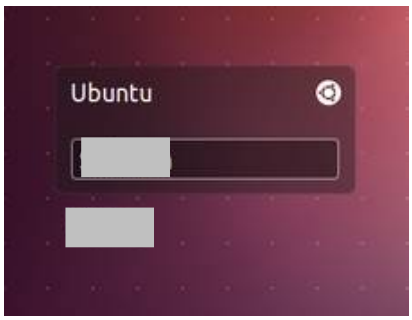
3.4.1 Comprendere lo scopo di un account di rete e come accedere alla rete usando un nome utente e una password.

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.

L'accesso alla rete dipende dalla sua architettura. Esistono infatti differenti tipi di rete che possono essere raggruppate in due gruppi: le reti paritetiche e le reti client/server.

Nelle reti paritetiche tutti i computer svolgono funzioni simili, l'autenticazione degli utenti avviene a livello locale sul singolo computer e le risorse condivise sui vari computer sono accessibili in base alle impostazioni sui singoli computer.





Nelle reti client/server il server (server di dominio) si occupa dell'autenticazione degli utenti anche su tutti i client e centralizza i permessi di accesso alle risorse di tutta la rete.

L'accesso alla rete avviene inserendo, in fase di avvio del computer, il proprio nome utente e la propria password nel modulo di login.

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.

La corretta gestione delle password consiste nel mantenerla segreta, quindi non dirla a nessuno per nessun motivo (è importante però annotarla in un luogo sicuro per evitare che venga dimenticata o persa).

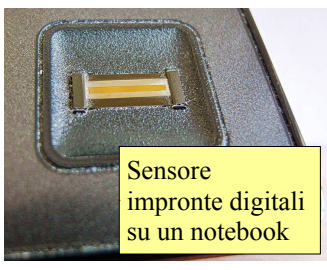
Inoltre è importante modificare con regolarità la password, per evitare che qualcuno possa venirne a conoscenza utilizzando una delle tecniche viste in precedenza (shoulder surfing, malware, ingegneria sociale). È anche importante non utilizzare la stessa password per tutti gli account, perché nel caso venisse individuata, potrebbe essere utilizzata per tutti i servizi.

Infine è importante che la password risponda a criteri di robustezza: generalmente si intende che una password robusta debba essere lunga almeno 8 caratteri, utilizzare lettere maiuscole e minuscole, numeri e anche caratteri speciali, come la @, il #, uno spazio vuoto o simili. Meglio evitare le lettere accentate in quanto differenti in base alla lingua della tastiera e al sistema operativo utilizzato.

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 su

Scanner portatile di iride



Sensore impronte digitali su un notebook

tecniche biometriche, cioè su tecniche basate sull'univocità di caratteristiche fisiche degli utenti.

La tecnica biometrica più utilizzata è senz'altro la scansione delle impronte digitali: diversi notebook e altri dispositivi mobili ne sono provvisti.

Un'altra tecnica biometrica, usata meno frequentemente nell'infor-matica tradizionale per motivi di costi e ingombri, è la scansione dell'iride dell'occhio.

4 Uso sicuro del web

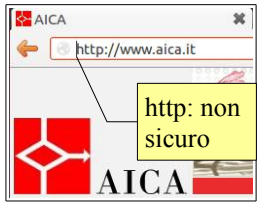
4.1 NAVIGAZIONE IN RETE

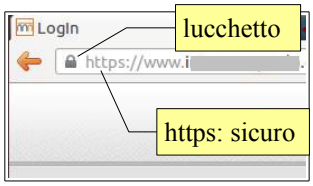
4.1.1 Essere consapevoli che alcune attività in rete (acquisti, transazioni finanziarie) dovrebbero essere eseguite solo su pagine web sicure.

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.

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

In particolare, quando si utilizza il web per trasferimenti di denaro, occorre fare particolare attenzione. I browser utilizzano normalmente il protocollo http che non è sicuro in quanto trasmette i dati senza alcuna cifratura. E quindi soggetto ad essere intercettato e utilizzato da malintenzionati.





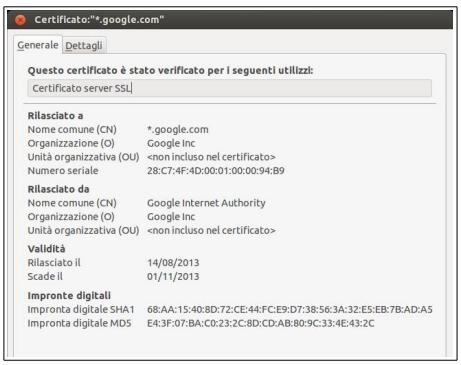
Esiste però anche un protocollo sicuro, https (Hyper Text Transfer Protocol Secure) che trasmette i dati dopo averli cifrati con una chiave robusta in modo che il solo sito web che li riceve e li trasmette sia in grado di decodificarli.

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 il protocollo https.

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.

Premesso che i siti web vengono identificati dal loro indirizzo IP, quando si digita un indirizzo alfanumerico questo viene tradotto nel corrispondente IP da un server DNS (Domain Name System): per esempio l'indirizzo IP di google.it è 173.194.35.63.



La tecnica del pharming modifica il riferimento e fa sì che l'indirizzo alfanumerico corrisponda a un IP diverso. L'utente non ha strumenti per rendersi conto della differenza se non controllare il certificato digitale di una pagina che utilizza il protocollo https.

4.1.4 Comprendere il termine “certificato digitale”. Convalidare un certificato digitale.

Un certificato digitale è un documento digitale che attesta la veridicità di chi pubblica la pagina web sicura o di chi invia un messaggio di posta elettronica.

In questa immagine si vede quello di Google.

4.1.5 Comprendere il termine “one-time password”.

Il significato è la traduzione in italiano, cioè una password valida una sola volta. È un metodo che viene utilizzato per proteggere gli utenti che hanno spesso la tendenza ad utilizzare password poco robuste o a non preoccuparsi della loro sicurezza.

Consiste nel richiedere una password aggiuntiva generata al momento da

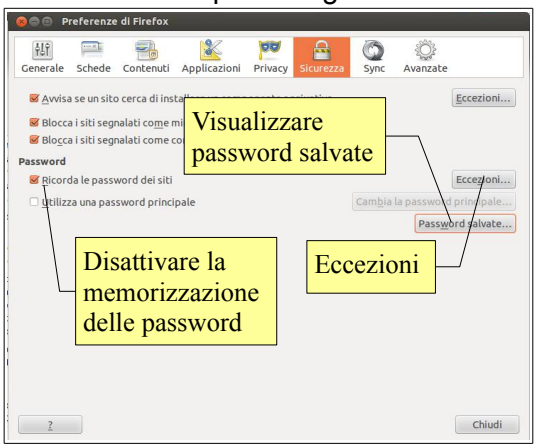
un dispositivo in possesso dell'utente, per esempio una applicazione per smartphone, o inviata all'utente dal gestore del sito per mezzo di un SMS.

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.

Per disattivare il completamento automatico con Firefox bisogna accedere alle Preferenze dal menu Modifica. Dopo aver aperto la scheda Privacy bisogna attivare Utilizza impostazioni personalizzate in Impostazioni cronologia.

In tal modo si può scegliere se utilizzare sempre la navigazione anonima, che non conserva traccia dei siti visitati, o in alternativa quali aspetti della navigazione (cronologia dei siti visitati, cronologia delle ricerche, dati dei moduli) conservare e quali no. È anche possibile indicare dei siti per i quali avere un comportamento diverso dalla regola generale.



Per disattivare il salvataggio delle password si deve accedere ancora alle preferenze di Firefox e alla scheda Sicurezza. Qui è possibile nella sezione Password disattivare la memorizzazione delle password. È anche possibile visualizzare i siti web per cui sono già state salvate le password, eventualmente eliminarle una per una o anche visualizzarle, nel caso siano state scordate.

Anche in questo caso si possono impostare delle eccezioni per determinati siti web.

4.1.7 Comprendere il termine “cookie”.

Un cookie (letteralmente biscottino) è una stringa di testo contenente informazioni personali che viene inviata da un server web e memorizzata dal browser, per esempio i dati relativi agli acquisti fatti in un negozio online, il cosiddetto carrello della spesa.

Quando si accede nuovamente allo stesso sito web, il cookie viene inviato dal browser al server per automatizzare la ricostruzione dei propri dati.

Si tratta quindi normalmente di uno strumento utile quando viene utilizzato in modo lecito. In alcuni casi i cookie sono stati usati in modo illecito per tracciare i comportamenti degli utenti, come uno spyware. Pertanto occorre fare attenzione a questi tipi di cookie e Firefox dà la possibilità di ispezionarli, cliccando sul pulsante Mostra i cookie...

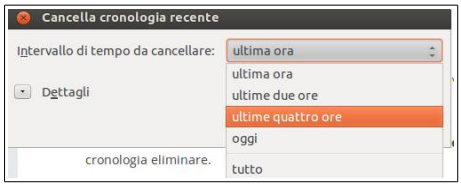
4.1.8 Selezionare impostazioni adeguate per consentire, bloccare i cookie.

Per disattivare i cookie occorre accedere alle Preferenze di Firefox, scheda Privacy, e disattivare la voce Accetta cookie dai siti.

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

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

Per eliminare i dati recenti, in Firefox occorre scegliere Cancella la cronologia recente... dal menu Cronologia. Si accede alla finestra di dialogo qui a fianco, in cui si possono cancellare i dati memorizzati, anche selettivamente cliccando su Dettagli, delle ultime ore oppure anche tutta quanta.



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.

Esistono dei software che filtrano l'accesso a internet da parte degli utenti. Questi software vengono utilizzati spesso a livello aziendale per evitare che i dipendenti perdano tempo e utilizzino la banda condivisa per motivi non utili al lavoro, a volte anche illeciti (come lo scaricamento illegale di contenuti protetti da diritti d'autore) e funzionano impedendo lo scaricamento di determinati tipi di file (audio, video, eseguibili), l'accesso a determinati siti web (reti sociali) o l'utilizzo di porte usate da determinati programmi (file sharing).

I software di controllo dei genitori, più comunemente detti di controllo parentale, vengono utilizzati e svolgono funzioni di filtraggio dei contenuti e di programmazione dei tempi consentiti per accedere a internet, per esempio quando i genitori sono presenti in casa, bloccandolo in orari differenti.

4.2 RETI SOCIALI

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

Le reti sociali (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 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. È importante sapere che esiste questa possibilità ed evitare di lasciare pubblico il proprio profilo. La cosa migliore è rendere accessibile il proprio profilo solo a persone che si conoscono anche nella vita reale.

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, infatti, può essere vittima di diversi tipi di attacco:

- il **cyberbullismo** consiste nell'utilizzo di internet per attaccare ripetutamente un individuo
- l'**adescamento** consiste nel tentativo di acquisire la confidenza di una persona, generalmente un minore, allo scopo di indirizzarla verso comportamenti inappropriati
- **informazioni fuorvianti o pericolose** possono essere pubblicate, spesso allo scopo di cyberbullismo
- le **false identità**, dette anche Fake, consistono nel creare falsi profili su una rete sociale e vengono spesso usate per tentativi di adescamento e ancora per il cyberbullismo
- i **link o messaggi fraudolenti**, detti anche phishing, hanno lo scopo di carpire informazioni basandosi sull'ingegneria sociale.

5 Comunicazioni

5.1 POSTA ELETTRONICA

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

La posta elettronica è normalmente un mezzo di comunicazione non sicuro in quanto i messaggi vengono inviati in chiaro. Per fare un paragone con la posta tradizionale, l'invio di un messaggio di posta elettronica può essere paragonato, più che a una lettera in busta chiusa, ad una cartolina postale.

Per rendere l'invio di un messaggio sicuro, occorre pertanto cifrare il messaggio stesso, in modo che solo il legittimo destinatario, in possesso di una chiave di decodifica, sia in grado di leggerlo. Cifrare un messaggio di

posta elettronica equivale a inserirlo in una busta e chiuderla prima di inviarlo.

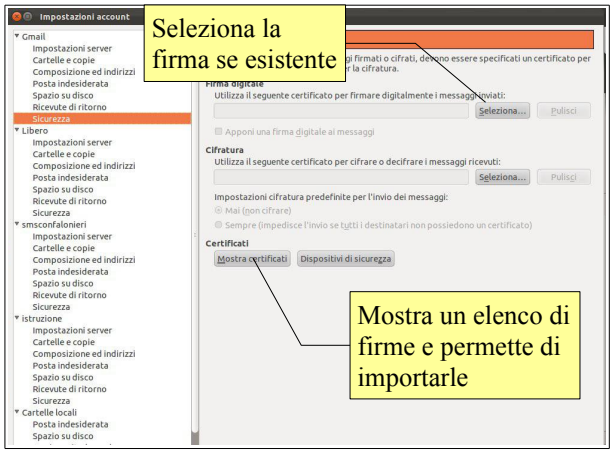
5.1.2 Comprendere il termine firma digitale.

La posta elettronica è un mezzo di comunicazione non sicuro anche per il fatto che non è difficile inviare messaggi facendo finta di essere una persona diversa da quella che si è. Per fare un paragone con la posta tradizionale, l'invio di un messaggio dotato di firma digitale, equivale a una raccomandata.

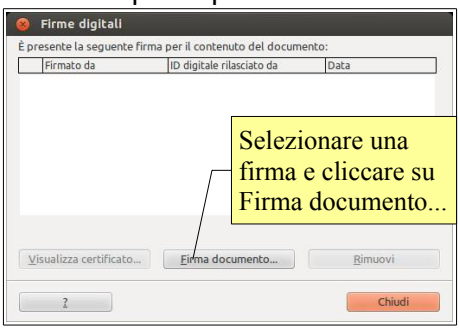
La firma digitale è un algoritmo, personale e legato alla cifratura dei dati, che permette di certificare che il mittente di un messaggio di posta elettronica è veramente chi dice di essere. Ciò pertanto, unitamente alla cifratura del messaggio, rende la posta elettronica davvero sicura.

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.



Una volta in possesso di una firma digitale si può utilizzare il software predisposto dal fornitore per firmare digitalmente i documenti, oppure apporre la firma digitale dai differenti software.



Per esempio per apporre la firma digitale a un messaggio di posta elettronica con Mozilla Thunderbird, si deve scegliere Modifica → Impostazioni account... e, nella scheda Sicurezza scegliere la firma digitale da utilizzare.

In LibreOffice è possibile firmare digitalmente un documento scegliendo Firme digitali... dal menu File. Nella finestra di dialogo si può scegliere la firma digitale se esistente, oppure importarne uno cliccando su Firma documento.

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

La posta elettronica è uno strumento molto comodo e utile, a volte viene usato in modo non corretto da parte di alcune persone per motivi diversi, ma quasi sempre per trarne vantaggio economico o per carpire informazioni riservate.

Un esempio di utilizzo scorretto della posta elettronica è la cosiddetta spam, cioè l'invio di messaggi non richiesti, generalmente di carattere pubblicitario, che hanno lo scopo di indurre i destinatari ad acquistare qualcosa.

Un altro esempio è il phishing, cioè l'invio di messaggi fraudolenti che inducono i destinatari a fornire inconsapevolmente a chi li ha inviati dati riservati, allo scopo di frode.

In tutti i casi è opportuno non rispondere a messaggi di questi tipo, neppure per dire che non si è interessati, perché in tal modo si confermerebbe che l'indirizzo email in questione è attivo e viene utilizzato, invogliando gli spammer (chi invia messaggi spam) ad inviare sempre più messaggi all'indirizzo in questione.

La cosa migliore da fare è quella din non aprire neppure messaggi di questo tipo, che in realtà sono abbastanza facilmente riconoscibili.

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.

Come già accennato in precedenza, il phishing consiste nell'invio di messaggi fraudolenti nel quali, fingendo che sia stato inviato da una banca, si chiede di confermare le proprie credenziali pena la decadenza del conto bancario in questione.

Nel messaggio di phishing viene generalmente riportato il link a un sito web fasullo, ma identico nell'aspetto al sito legittimo. Per distinguerlo da quello vero occorre controllare il dominio presente nella barra dell'indirizzo, che è diverso da quello originale, salvo quando viene usata anche la tecnica del pharming.

In ogni caso è sufficiente ricordare che nessuna persona seria, banca o azienda chiederebbe di confermare via email le proprie credenziali, per il semplice fatto che la posta elettronica è un mezzo di comunicazione non sicuro.

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.

Alcuni messaggi hanno in allegato dei file infetti, che possono danneggiare il computer. Pertanto occorre fare molta attenzione prima di aprire un allegato, per esempio facendo una scansione con il software antivurs.

5.2 MESSAGGISTICA ISTANTANEA

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

La messaggistica istantanea è un mezzo di comunicazione via internet molto utilizzato e consiste nello scambio di messaggi di testo tra due o più persone. Viene utilizzata, soprattutto dai giovani ma anche tra colleghi, per conversazioni testuali e per lo scambio di file. Alcuni software di messaggistica istantanea danno anche la possibilità di chiamate audio e video.

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

Come la posta elettronica, anche la messaggistica istantanea comporta il rischio di ricevere sul proprio computer dei malware che possono comprometterne la sicurezza. Inoltre come tutti i software, anche quelli di messaggistica istantanea possono avere delle vulnerabilità e rendere possibile l'accesso al computer a persone non autorizzate.

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 file a persone non affidabili.

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.

Per far sì che i dati non vengano persi o rubati, prima di tutto è necessario che i dispositivi informatici siano messi in sicurezza, cioè che non vengano sottratti o smarriti.

Un metodo, adatto in particolare per notebook e computer desktop predisposti, sono i cavi di sicurezza, tra cui i più diffusi seguono lo standard Kensington Security Lock.

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

Infine è utile controllare gli accessi ai locali nei quali i dispositivi sono collocati, in modo da poter più facilmente risalire all'autore di eventuali furti.

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.

Queste precauzioni tuttavia non sono sufficienti ad evitare completamente la perdita di dati. Ciò per vari motivi: per esempio si possono perdere i dati per la rottura di un dispositivo di memorizzazione, o anche per lo smarrimento o il furto di un dispositivo portatile.

È quindi importante avere una copia di sicurezza (backup) dei dati che permetta di ricostruirli in caso di perdita.

Tra i dati da salvare nella copia di sicurezza vanno compresi i file realizzati in proprio (documenti, immagini, ecc...), le informazioni di carattere finanziario, i segnalibri e la cronologia salvati nel browser.

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

Si è detto che è importante avere una copia di sicurezza dei propri dati. Vediamo ora come va organizzata la procedura di copia affinché sia davvero efficace in caso di perdita dei dati.

Una copia di sicurezza dei dati serve se è aggiornata. Pertanto, in base al numero di documenti che vengono memorizzati ogni giorno nella memoria del dispositivo, occorre stabilire se fare una copia quotidiana, settimanale, o mensile dei dati.

Per evitare di dimenticarsi di effettuare la copia di sicurezza, è opportuno impostare un programma di copia in modo che questa avvenga automaticamente a scadenze regolari in un momento in cui il computer rimane acceso ma non viene utilizzato, ad evitare che la copia dei dati rallenti il lavoro.

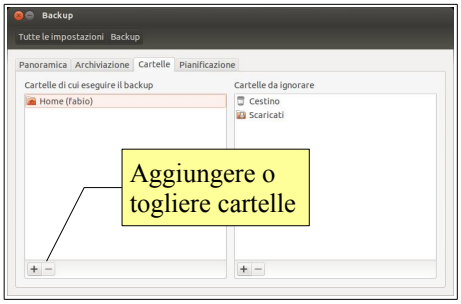
Infine occorre prestare attenzione alla collocazione della copia di sicurezza: se la copia viene posta accanto al dispositivo, anch'essa corre il rischio di essere persa (furto, danneggiamento a causa di eventi, ecc...). la copia di sicurezza va quindi posta in un luogo, il più sicuro possibile, diverso dall'originale. Negli ultimi tempi per questo motivo sempre più spesso la copia dei sicurezza dei dati viene effettuata online, su server remoti.

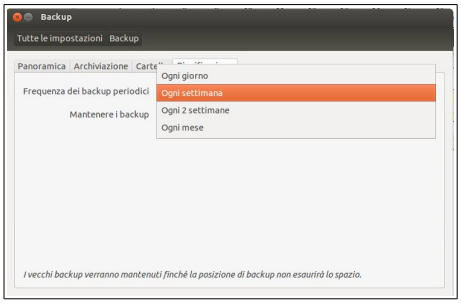
6.1.4 Effettuare la copia di sicurezza di dati.

In Ubuntu esiste un programma che si occupa di effettuare le copie di sicurezza. Per avviarlo occorre digitare backup nella Dash.

Nella scheda Panoramica vengono visualizzate molte informazioni importanti, e impostare la pianificazione dei backup.

Nella scheda Archiviazione si imposta la collocazione della copia di sicurezza. Come impostazione predefinita viene indicato Ubuntu One, cioè lo spazio online gratuito a disposizione degli utenti di Ubuntu. Si possono anche scegliere altre posizioni, come si vede nell'immagine qui a fianco.





Nella scheda Cartelle si impostano le cartelle da copiare. Come impostazione predefinita viene indicata la propria cartella home, esclusi il Cestino e la cartella Scaricati. In ogni caso è possibile aggiungere o togliere cartelle in base alle proprie esigenze.

L'ultima scheda riguarda la pianificazione dei backup automatici, se impostati. Si può stabilire se effettuare una copia di sicurezza giornaliera, settimanale, quindicinale o mensile. In questa scheda si può anche decidere quanto tempo mantenere le copie di backup (per sempre, un anno a scalare, fino a un minimo di un mese).

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

Una volta fatta la copia di sicurezza dei dati, è opportuno provare a ripristinarli, cioè trasferirli dalla copia di sicurezza alla posizione originale, in modo da verificare l'efficacia e la completezza dell'operazione.

Per ripristinare una copia dei dati, nella scheda Panoramica premere il pulsante Ripristina...

Viene chiesto da quale posizione ripristinare: nella finestra cui si accede scegliere la posizione e proseguire cliccando su Avanti. Proseguire fino al termine del ripristino, poi verificare che tutti i file siano stati ripristinati correttamente.

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 non servono più, si possono eliminare i dati dalle morie di massa dei dispositivi o dai supporti di backup. Ciò vale anche quando ci si deve disfare di un dispositivo o di un supporto di memoria.

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:

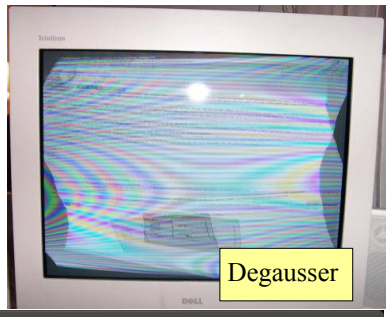
- i moderni sistemi operativi dispongono di una cartella speciale, chiamata Cestino, dove vengono spostati i file cancellati. È pertanto sempre possibile ripristinare dati cancellati in questo modo
- anche si i file vengono cancellati dal Cestino, in realtà rimangono delle tracce sul disco. Pertanto, anche se non saranno visibili con gli strumenti tradizionali (nautilus, terminale) 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.

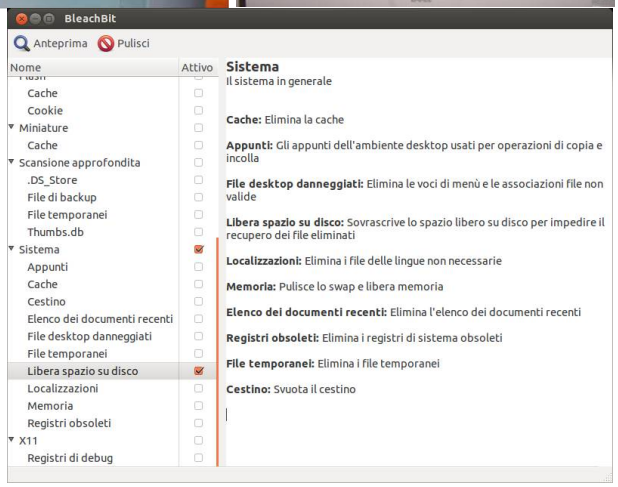
6.2.3 Identificare i metodi più comuni per distruggere i dati in modo permanente, quali uso di trita documenti, distruzione di memorie di massa/dispositivi, smagnetizzazione, uso di utilità per la cancellazione definitiva dei dati.

Per cancellare definitivamente i dati 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 o smagnetizzate per mezzo di apparecchi (degausser) in grado di applicare intensi campi magnetici
- se la memoria di massa deve essere riutilizzata è opportuno eliminare i file in modo definitivo e sicuro per mezzo di appositi software che sovrascrivono i file più volte in modo da renderli non recuperabili. In Ubuntu esistono diversi software che funzionano nel terminale, come shred e wipe. Un software con interfaccia grafica è bleachbit, in cui si possono scegliere quali cartelle cancellare. Se si sceglie di cancellare in modo sicuro il Cestino, in file in esso contenuti saranno eliminati in modo sicuro. Se il Cestino è stato già svuotato, si può scegliere di cancellare in modo sicuro lo Spazio libero su disco.

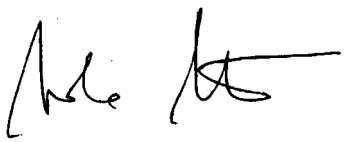

Trita documenti


Degausser



marzo 2014

L'autore, prof. Fabio Frittoli



NB=tutte le immagini utilizzate nella presente dispensa sono state realizzate in proprio o tratte da http://wikimediafoundation.org