5. IT SECURITY

 info@ninolopez.com

 gooddesignsociety.blogspot.com

 @ninolopez

 ninolopez1

CONCETTI DI SICUREZZA
MALWARE
SICUREZZA IN RETE
USO SICURO DEL WEB
COMUNCIAZIONI
GESTIONE SICURA DEI DATI

CONCETTI DI SICUREZZA

Minacce informatiche
Valore delle Informazioni
Sicurezza personale
Protezione file

Minacce ai dati

Distinguere tra dati e informazioni

I **dati** sono valori (numeri, immagini, testo) che rappresentano fatti, non ancora organizzati.

Le **informazioni** sono dati organizzati in modo da essere significativi per l'utente.

Minacce ai dati

Comprendere il termine crimine informatico

Crimine attuato per con l’abuso di strumenti informatici:

- frode informatica
- furto d'identità
- accesso non autorizzato a sistemi informatici

Minacce ai dati

Differenza tra hacking, cracking e hacking etico.

Hacking (to hack – intaccare) insieme di tecniche volte a conoscere, accedere e modificare un sistema Hw o Sw.

Hacker è detto chi pratica l'hacking.

Quando l'hacker ruba dati o danneggia il sistema violato, si parla di **cracking** e di **cracker**.

Hacking etico utilizzo delle tecniche di hacking per monitorare la sicurezza dei sistemi e delle reti.

L'hacker etico, o white hat in opposizione al termine black hat (cracker), identifica chi pratica l'hacking etico.

Minacce ai dati

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

I dati, oltre che dalle persone, possono essere minacciati anche da

- **eventi naturali** (incendi, inondazioni, terremoti)
- **eventi artificiali** (guerra, vandalismo).

È quindi necessario tenerne conto per prevenirne la perdita.

Minacce ai dati

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

La perdita di dati può dipendere anche da altri fattori:

dipendenti che possono perderli o rubarli per rivenderli

fornitori di servizi (chi manutiene le attrezzature hardware o l'infrastruttura di rete) possono danneggiare involontariamente i dati oppure prenderne illegalmente possesso

persone esterne, clienti e fornitori o ospiti, possono accedere alla rete aziendale tramite pc o dispositivi portatili, ad esempio tramite il wifi, e mettere a rischio i dati.

Valore delle informazioni

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

È evidente che è opportuno proteggere le informazioni personali:

- le credenziali di accesso all'e-mail o a una rete sociale possono essere usati illegalmente facendo ricadere la colpa su di noi.
- i numeri della carta di credito o di accesso all'home banking, possono essere utilizzati per sottrarre danaro

Valore delle informazioni

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

Per le aziende che trattano dati di clienti è ancora più importante proteggere queste informazioni, in quanto responsabili in caso di utilizzo illegale.

Valore delle informazioni

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

I dati riservati possono essere protetti con determinate tecniche per mezzo delle quali non potrebbero essere utilizzati.

- **password** robuste perproteggere i dispositivi
- **cifratura**, con un algoritmo crittografico, dei dati stessi.
  La password da sola non garantisce i dati quando i dati sono memorizzati su una memoria rimovibile.
  Esistono algoritmi e software sicuri e semplici da utilizzare.

Valore delle informazioni

Drag'n'Crypt ULTRA (Sw cifrare file)
http://www.bitcore.de/dcu/download.html

Trascinare il file (anche intere cartelle o più file) da crittografare all'interno dell'icona di Drag'n'Crypt ULTRA.
Il programma sostituisce i file crittografati con dei file con estensione .dcu.
Per togliere la protezione trascinare i file .dcu nell'icona del programma e inserire la password nella finestra che si apre in pop-up

Valore delle informazioni

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

Per essere sicure, le informazioni devono

- avere un alto grado di **confidenzialità**: non devono essere diffuse a chi non è autorizzato
- essere **integre**: complete e senza modifiche rispetto all'originale
- essere **disponibili** al momento del bisogno: non avrebbe alcuna utilità curare la sicurezza dei dati se poi, quando servono, non si riesce a recuperarle nei tempi necessari.

Valore delle informazioni

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

In Italia è stato emesso un Decreto Legislativo n. 5 del 09/02/2012 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 e di una direttiva che disciplina i trattamenti per finalità di giustizia e di polizia.

Valore delle informazioni

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

È quindi importante attenersi alle regole che disciplinano l'utilizzo delle ICT per preservare i dati, personali e aziendali, dal furto, dallo smarrimento e da un utilizzo non consentito.

Sicurezza personale

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

L'**ingegneria sociale** (social engineering) è lo studio del comportamento di una persona al fine di carpire informazioni. Viene utilizzata, al posto delle tecniche di hacking, per accedere a informazioni riservate aggirando i sistemi di protezione hardware e software.

Sicurezza personale

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

I mezzi utilizzati dall'ingegneria sociale sono:

- **chiamate telefoniche** cercano di ottenere informazioni mascherandole con sondaggi, a volte promettendo premi
- **phishing** tecnica basata sull'invio di messaggi e-mail da parte di un servizio bancario che minacciando la chiusura del conto chiede di inserire le proprie credenziali per poterle verificare.
- **shoulder surfing** carpire le credenziali dell'utente spiandolo, standogli nei pressi, o per mezzo di lenti o telecamere.

Sicurezza personale

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

Sicurezza personale

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

- **frugare negli scarti delle persone** (foglio con una Pw)
- **fingere di essere qualcun altro** (**phishing**) che ha diritto ad avere le credenziali
- **skimming** acquisire immagini di oggetti su cui sono impressi dati sensibili (pin, bancomat). Quando si preleva da un bancomat è importante non farsi vedere da nessuno e stare attenti che non ci siano webcam che riprendono la tastiera.

Sicurezza dei file

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

Una macro è un insieme di istruzioni scritte in un linguaggio di programmazione che possono essere eseguite, all'interno di un software (ie videoscrittura).

Utili per automatizzare procedure lunghe e noiose, possono contenere codice malevolo che può causare danni al pc.

È possibile disattivare una macro.

Sarebbe bene attivare le macro quando si è certi dell'origine.

Sicurezza dei file

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

È possibile impostare una **password** per i file (windows 7):

- aprire il file
- selezionare Windows→Prepara→Crittografa documento
- inserire e confermare la password da applicare

Per un archivio compresso:

- durante la compressione: scheda Avanzati, Cliccare su Parola chiave, inserire la Pw (possibile con alcuni formati tra cui zip)

Sicurezza dei file

Comprendere i vantaggi e i limiti della cifratura

Un file protetto protegge i dati da accessi indesiderati.

Bisogna considera che

- c'è il rischio che si dimentichi la password e non si possa più aprire il file
- è importane scegliere una password robusta

MALWARE

Definizione e funzione
Tipologie di minacce
Protezione dai malware

Definizione e funzione

Comprendere il termine Malware

Indica un software creato per causare danni a un sistema informatico su cui viene eseguito e ai dati dell'utente.
Il termine deriva dalle parole inglesi malicious e software (programma malevolo).

Definizione e funzione

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

Si distinguono molte categorie di malware:

- **Trojan horse**: software apparentemente utile, che contiene istruzioni dannose che vengono eseguite all'insaputa dell'utilizzatore
- **Backdoor**: programmi che consentono un accesso non autorizzato al sistema su cui sono in esecuzione
- **Rootkit**: non dannosi in sé, hanno la funzione di nascondere la presenza di particolari file o impostazioni del sistema e vengono utilizzati per mascherare spyware e trojan.

Tipi

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

Virus parti di codice che si diffondono copiandosi all'interno di altri programmi, o in una sezione del disco fisso, in modo da essere eseguiti ogni volta che il file infetto viene aperto.

Si trasmettono da un computer all’altro tramite lo spostamento di file infetti

Tipi

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

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 Bug di alcuni programmi. Il loro scopo è rallentare il sistema con operazioni inutili o dannose.

Tipi

Riconoscere i tipi di malware usati per furto di dati, profitto/ estorsione e comprendere come operano, ad esempio adware, spyware, botnet, keylogger e dialer. (1/2)

Adware software che presentano all'utente messaggi pubblicitari durante l'uso. Possono causare rallentamenti del pc e rischi per la privacy in quanto comunicano le abitudini di navigazione ad un server remoto.

Spyware software che raccoglie informazioni (abitudini di navigazione, Pw) per comunicarle a un destinatario interessato

Tipi

Riconoscere i tipi di malware usati per furto di dati… (2/2)

Keylogger programmi in grado di registrare ciò che viene digitato sulla tastiera consentendo il furto di password

Botnet è l'infezione di una rete informatica che viene controllata da remoto dal botmaster, che è in grado di utilizzare la rete e i dispositivi ad essa collegati per svolgere attività non autorizzate

Dialer programmi che modificano (quando ci si connette con la normale linea telefonica) il numero telefonico chiamato con uno a tariffazione speciale

Protezione

Comprendere come funziona il software anti-virus e quali limitazioni. (1/2)

Per proteggersi dai tentativi dei malware di infettare il sistema seve installare un software **Antivirus**.

Un antivirus ha due funzioni:

- controllare cartelle e file in modo da individuare e rendere innocui eventuali file infetti.
- scansionare la RAM in modo da impedire l'esecuzione di codice virale, che riconosce con un confronto con un archivio di “firme” dei malware conosciuti, o con metodi euristici basati sulla somiglianza di codice virale con quello analizzato.

Protezione

Comprendere come funziona il software anti-virus e quali limitazioni (2/2)

Un antivirus non riesce ad essere sicuro al 100%.

Per essere efficace, deve essere frequentemente aggiornato con frequenza, in quanto nuovi malware nascono.

A volte indicano come virus programmi leciti.

Protezione

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

Esistono diversi antivirus, a pagamento o gratis, che consentono di effettuare la scansione dell'intero HD o di parti di esso

È possibile pianificare scansioni a intervalli di tempo regolari.

Protezione

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

Quando un antivirus individua dei file infetti o sospetti, chiede all'utente se intende metterli in quarantena, una apposita cartella creata dall’antivirus, e resi non eseguibili attraverso la modifica dei permessi (Linux o Mac) o dell'estensione del file (Windows).

Protezione

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

È fondamentale scaricare frequentemente gli aggiornamenti sia del software antivirus, sia soprattutto delle definizioni dei virus.

Tutti gli antivirus si aggiornano automaticamente, ma è bene verificare che lo facciano.

Il mancato aggiornamento automatico potrebbe essere causato proprio da un virus che cerca di evitare di essere individuato.

SICUREZZA IN RETE

Networks

Connessioni di rete

Sicurezza delle connessioni wireless

Controllo degli accessi

Reti

Comprendere il termine rete e riconoscere i più comuni tipi di rete, quali LAN, WAN, VPN. (1/4)

Una rete di calcolatori è un insieme di computer indipendenti collegati tra loro in modo da potersi scambiare informazioni attraverso un mezzo trasmissivo (architettura distribuita).

Le reti permettono di:

- condividere risorse, file e stampanti
- comunicare, tra persone
- utilizzare servizi, consultare informazioni, fare e-commerce

Reti

Comprendere il termine rete ... (2/4)

Le reti si possono classificare secondo:

- **Tecnologia di trasmissione**

Broadcast hanno unico canale di comunicazione condiviso

Point to point usano collegamenti dedicati tra coppie di stazioni

Indipendentemente dalla tecnologia, un msg può essere inviato a:

- una stazione ben precisa: point to point
- a tutte le stazioni: broadcast
- un gruppo di stazioni: multicast

Reti

Comprendere il termine rete ... (3/4)

- **Dimensioni**

Lan (Locali)

Reti private al max di qualche km, con una velocità compresa tra 10 Mbps e 1000 Mbps. In genere usano il broadcasting.

Man (Metropolitane)

Possono coprire suolo pubblico o privato. Coprono gruppi di edifici o una città. In genere usano il broadcasting.

Wan (Geografiche)

Coprono una grande area (nazione, continente, pianeta).
In genere usano il point to point.

Reti

Comprendere il termine rete ... (3/4)

VPN (Virtual Private Network) sistema per avere una rete privata che utilizza una rete pubblica per funzionare.
Normalmente una VPN viene implementata per collegare in modo sicuro computer lontani per mezzo di internet.
Un software si occupa di creare un tunnel sicuro attraverso la criptazione dei dati e l'autenticazione della comunicazione.

Reti

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, stampanti, internet).

Per definire tali politiche è necessario che gli utenti della rete abbiano un account col proprio nome utente e password.

Reti

Comprendere la funzione e i limiti di un firewall.

Un firewall è un dispositivo o un software che controlla il traffico di rete, allo scopo di evitare accessi non autorizzati, in base a delle regole definite dall'amministratore

L’efficacia del firewall è legata alle regole, una cattiva programmazione può impedire un uso legittimo della rete.

Essendo generalmente posto tra la LAN e internet, un firewall non avrà effetto se l'attacco rete viene effettuato dall'interno, da un utente della rete o dal un malware che precedentemente ha infettato un dispositivo della rete.

Connessioni di rete

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

Una rete connette dispositivi utilizzando mezzi diversi:

- cavi, in rame o in fibra ottica
- onde radio, in questo caso si parla di rete wireless 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

Connessioni di rete

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

Attraverso la rete, locale o internet, è possibile

- che il computer venga infettato da virus o altro malware scaricato attraverso la posta elettronica o pagine web.
- vi siano accessi non autorizzati ai dispositivi connessi, a causa di falle di sicurezza
- sia messa a rischio la privacy degli utenti, se i dati personali non sono adeguatamente protetti

Sicurezza su reti wireless

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

Una rete cablata richiedendo un collegamento fisico rende quasi impossibile collegare un dispositivo senza autorizzazione da parte dell'amministratore, una rete senza fili invece può essere facilmente agganciata da un dispositivo mobile in un raggio coperto dal segnale wireless.

Una rete senza fili non protetta da password è accessibile quindi da chiunque, con il rischio di accessi non autorizzati che possono danneggiare rete, dispositivi e dati.

Sicurezza su reti wireless

Riconoscere diversi tipi di sicurezza per reti wireless, quali WEP, WPA, MAC.

Negli corso degli anni sono stati elaborati diversi algoritmi di crittazione dei dati sulle reti wifi.

WEP (Wired Equivalent Privacy) 1999. Rivelatasi non sicuro, per la brevità della chiave

WPA (Wifi Protected Access), **WPA2** 2003/2004 maggiore sicurezza ma non totale.

Sicurezza su reti wireless

Riconoscere diversi tipi di sicurezza per reti wireless. (2/2)

MAC, indirizzo fisico che identifica univocamente una scheda di rete, cablata o wireless.

Consente di stilare delle ACL (Access List) di dispositivi autorizzati all'accesso alla rete. Un dispositivo con un Mac address non conosciuto, non potrà accedere alla rete anche con l'immissione della giusta password da parte del proprietario.

Esistono tuttavia dei software in grado di modificare il Mac address di un dispositivo.

Nessun metodo garantisce la sicurezza totale, solo combinando metodi diversi si raggiunge un buon grado di sicurezza.

Sicurezza su reti wireless

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

Una rete senza fili non protetta corre il rischio che qualcuno possa accedervi, con la possibilità di intercettare i dati presenti sui dispositivi connessi.

Sicurezza su reti wireless

Connettersi ad una rete wireless protetta/non protetta.

Perché un dispositivo possa connettersi a una rete senza fili, deve avere una scheda di rete wifi.

Per connettersi i sistemi operativi dispongono di un programma che avvisa l'utente della disponibilità di reti senza fili.

In Windows si accede all'elenco di connessioni di rete dall'icona in basso sulla barra delle applicazioni.

Oppure Pannello di controllo→Centro di connessioni di rete→Gestisci reti wireless

Sicurezza su reti wireless

Controllo di accesso

Comprendere lo scopo di un account di rete e come accedere alla rete usando un nome utente e una password. (1/2)

Impostare per ciascun utente un account personale (nome utente e password) permette di limitare ai solo utenti autorizzati l'accesso alla rete.

L'accesso alla rete dipende dall'architettura di rete. Esistono essenzialmente due tipologie di reti:

- le reti paritetiche
- le reti client/server

Controllo di accesso

Comprendere lo scopo di un account di rete e come accedere alla rete usando un nome utente e una password. (2/2)

Reti paritetiche tutti i computer svolgono funzioni simili, l'autenticazione utenti avviene sul singolo computer, le risorse condivise sui vari computer sono accessibili in base alle impostazioni sui singoli computer.

Reti client/server il server si occupa dell'autenticazione degli utenti sui client e gestisce i permessi di accesso alle risorse. L'accesso alla rete avviene inserendo nome utente e password in fase di avvio del computer.

Controllo di accesso

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. (1/2)

Perché la password garantisca effettivamente la privacy deve

- essere gestita correttamente
- rispondere a criteri di robustezza

Controllo di accesso

Riconoscere buone politiche per la password. (2/2)

Corretta gestione

- mantenerla segreta
- annotarla per evitare che venga dimenticata
- modificarla con regolarità
- non utilizzare la stessa password per tutti gli account

Robustezza

- essere lunga almeno 8 caratteri
- contenere M/m, numeri, caratteri speciali (@, _, #)
- evitare le accentate che differiscono in base al SO e alla lingua

Controllo di accesso

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

In alternativa alle password, per accedere al pc in modo sicuro, esistono sistemi basati su tecniche biometriche, ovvero sull'univocità delle caratteristiche fisiche degli utenti:

- scansione delle impronte digitali
- scansione dell'iride dell'occhio (meno usata, anche per i costi)

USO SICURO DEL WEB

Navigazione Web
Social Networking

Navigazione in rete

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

Le reti, e soprattutto internet che è pubblica, non sono sicure.

È quindi necessario usarle con accortezza, prendendo degli accorgimenti quando si usano.

In particolare quando si effettuano acquisti o transazioni finanziarie.

Navigazione in rete

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

HTTP (Hyper Text Transfer Protocol) non è sicuro in quanto trasmette i dati senza cifratura.

HTTPS (Secure) trasmette i dati dopo averli cifrati

in modo che possano essere decodificati solo dal sito che li riceve e li trasmette.

Navigazione in rete

Essere consapevoli del pharming.

Il pharming è una tecnica (simile al phishing), che dirige l'utente verso un altro sito web, identico a quello cercato, ma falso, facendo corrispondere l'indirizzo a un IP diverso.

L'utente non ha modo di accorgersi della differenza se non controllare il certificato digitale di una pagina che utilizza il protocollo https.

Su questo sito clonato l'eventuale immissione di dati personali possono essere intercettati.

Navigazione in rete

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.

Navigazione in rete

Comprendere il termine “one-time password”.

È un metodo che viene utilizzato per proteggere gli utenti che hanno spesso la tendenza a utilizzare password poco robuste o a non preoccuparsi della loro sicurezza.

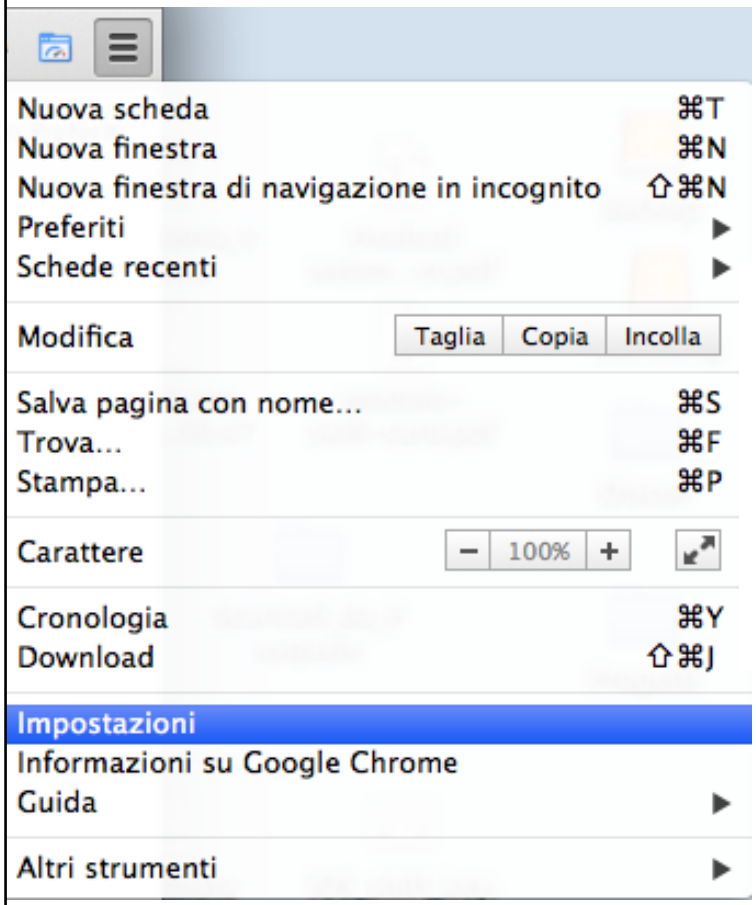
È una password da utilizzare una volta, generata al momento da un sito o da un dispositivo e inviata all'utente per mezzo di un SMS.

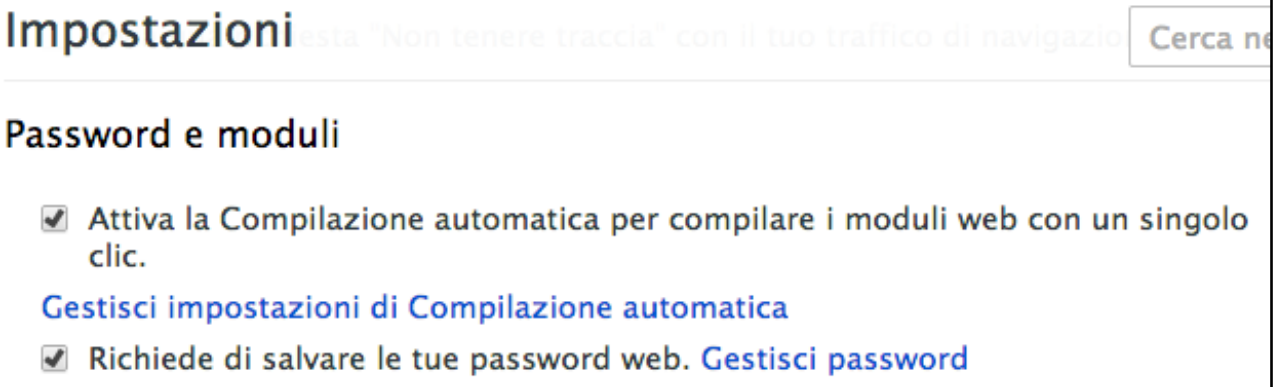
Navigazione in rete

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

Il completamento e il salvataggio automatico del browser è una funzionalità comoda, che conviene disabilitare quando il computer è utilizzato da più persone.

Navigazione in rete





Navigazione in rete

Comprendere il termine “cookie”.

Un cookie (biscottino) è un file di informazioni inviato da un sito web e memorizzato sul computer dell'utente durante la navigazione, allo scopo di identificare chi ha visitato il sito in precedenza, per offrire delle impostazioni personalizzate al successivo accesso

Si tratta quindi di uno strumento utile, tuttavia può essere usato in modo illecito per tracciare i comportamenti degli utenti.

Navigazione in rete

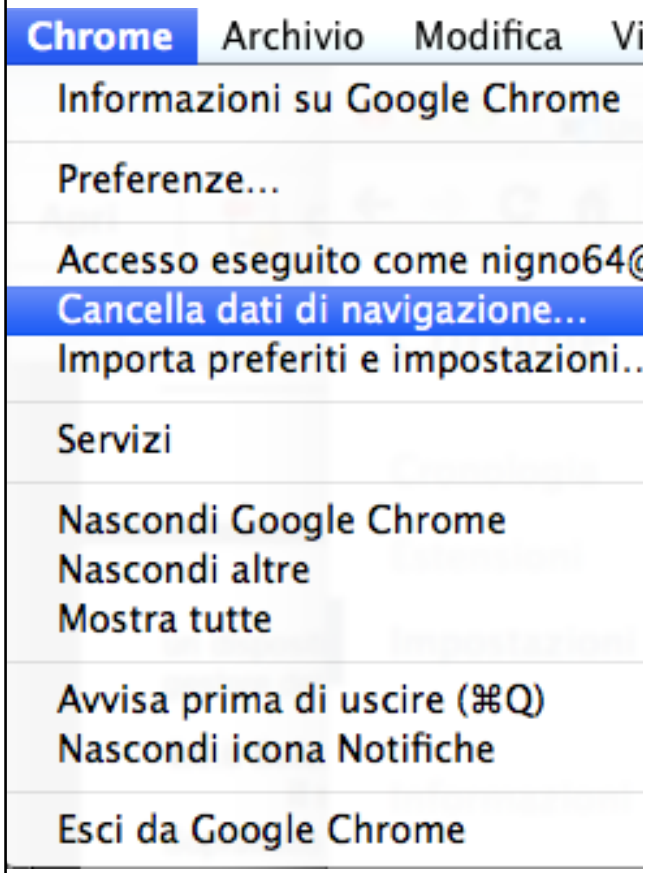
Selezionare impostazioni adeguate per consentire, bloccare i cookie.

Tutti i browser offrono strumenti per far sparire i cookie, o impostare alcune eccezioni.

Disattivarli completamente può rendere difficoltosa la navigazione, una soluzione ottimale potrebbe essere gestire le eccezioni.

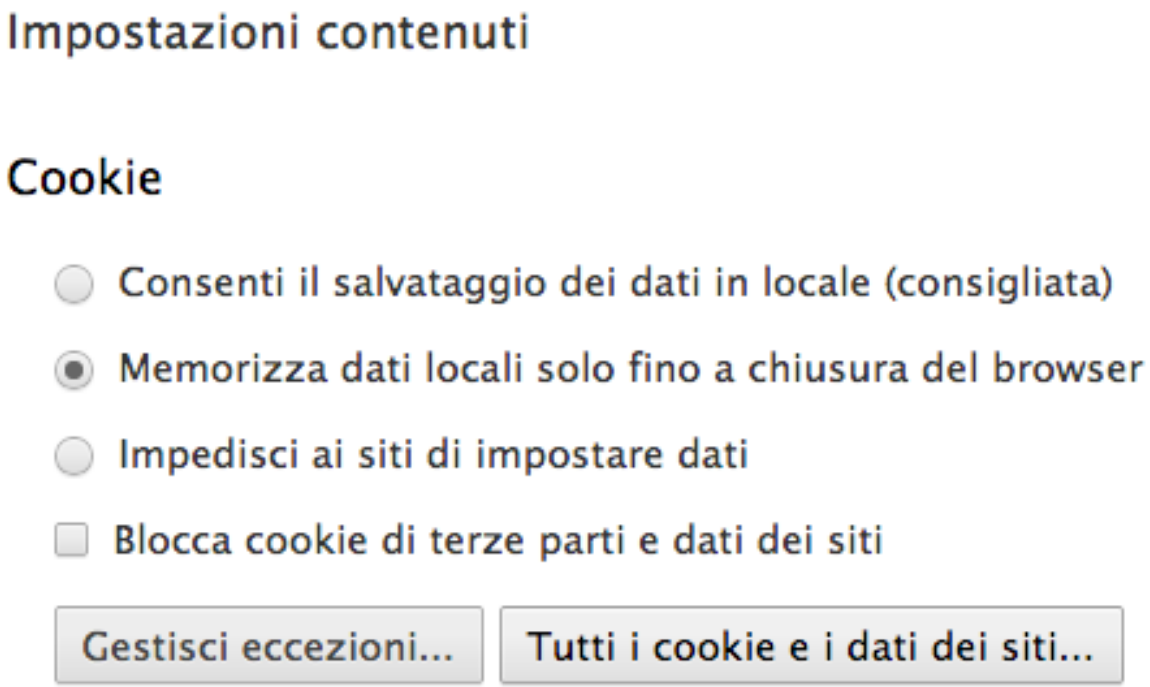
Navigazione in rete

Eliminare tutti i cookie



Gestire le eccezioni

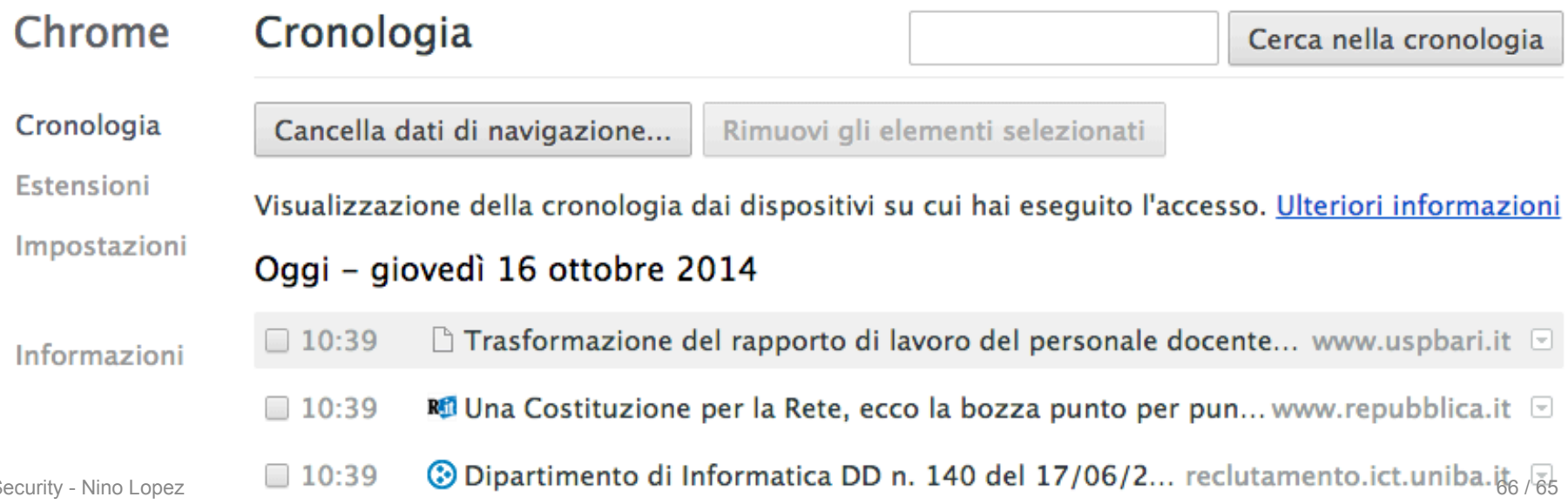
Impostazioni>Impostazioni avanzate>Privacy



Navigazione in rete

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

Tutti i browser offrono la possibilità di eliminare i dati di navigazione. Accedendo in genere da impostazioni.



Navigazione in rete

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 software che limitano l'accesso internet agli utenti, impedendo

- l'accesso a determinati siti web;
- lo scaricamento di determinati tipi di file (eseguibili, video)
- l'utilizzo di porte usate da determinati programmi (file sharing)

I software di di controllo parentale svolgono funzioni di filtraggio dei contenuti e di programmazione dell'accesso a internet.

Reti sociali

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

Le diffusione delle reti sociali tra tutte le fasce delle popolazione ha posto il problema della privacy in maniera scottante.

È importante comprendere che tutto ciò che viene diffuso su internet diventa di pubblico dominio e se ne perde il controllo.

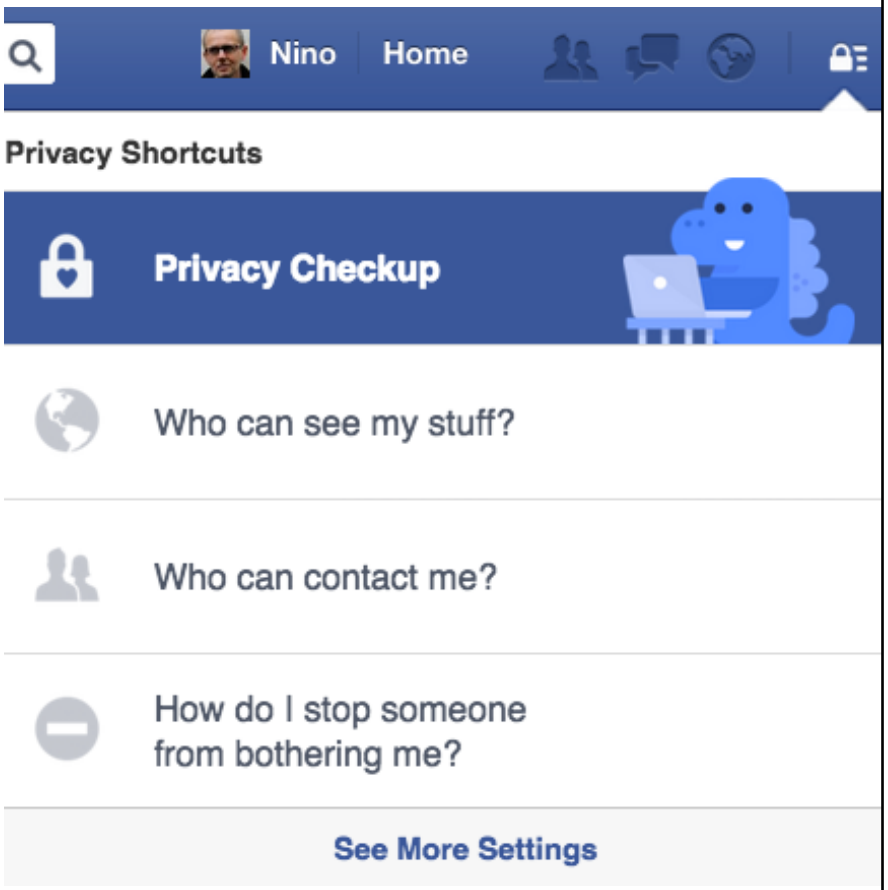
Bisogna quindi usare questi strumenti con attenzione:

- Evitando di comunicare dati riservati e personali
- Valutando attentamente se pubblicare immagini private e divulgare idee di carattere religioso e politico

Reti sociali

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

Tutte le reti sociali offrono la possibilità di impostare la privacy del proprio profilo, anche in modo articolato.



Reti sociali

Comprendere i rischi potenziali durante l'uso di siti di reti sociali, quali cyberbullismo, adescamento, informazioni fuorvianti/pericolose, false identità, link o messaggi fraudolenti. (1/2)

Utilizzando le reti sociali si può essere vittima di:

- **Cyberbullismo** uso di internet per attaccare un individuo
- **Adescamento** tentativo di acquisire la confidenza di una persona, spesso un minore, per indirizzarla verso comportamenti inappropriati

Reti sociali

Comprendere i rischi potenziali durante l'uso di siti di reti sociali... (2/2)

Inoltre bisogna essere consapevoli che

- **le informazioni vanno verificate**, in quanto possono essere fuorvianti o pericolose
- **esistono false identità (Fake)**, falsi profili spesso usati per adescamento e cyberbullismo
- **link o messaggi fraudolenti (phishing)**, hanno lo scopo di carpire informazioni basandosi sull'ingegneria sociale.

COMUNICAZIONI	Posta elettronica Messaggistica istantanea

Posta elettronica

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

I messaggi di posta elettronica vengono inviati in chiaro, e quindi non sono sicuri.

C'è quindi bisogno di cifrare il messaggio, in modo che possa essere letto solo dal destinatario, che è in possesso di una chiave di decodifica.

Posta elettronica

Comprendere il termine firma digitale.

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 il mittente di un messaggio di posta elettronica.

Rende la posta elettronica sicura.

Posta elettronica

Creare e aggiungere una firma digitale.

Le firme digitali vengono rilasciate da aziende o enti che garantiscono l'identità del proprietario della firma, e utilizzano dispositivi, che garantiscano la generazione sicura della firma, come smart card e relativo lettore, chiavette USB, token.

si può utilizzare il

Per firmare digitalmente i documenti, si può usare il software del fornitore, o altri software che lo pemettono.

Posta elettronica

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

La posta elettronica è utilizzata talora in modo non corretto.

Si tratta del cosiddetto spam, invio di messaggi non richiesti essenzialmente di due tipi:

- pubblicitari, per vendere o promuovere un prodotto/servizio
- fraudolenti (phishing), per indurre i destinatari a fornire inconsapevolmente dati riservati.

  Questi messaggi, facilmente riconoscibili, vanno eliminati, senza nemmeno aprirli.

Posta elettronica

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.

Il phishing consiste nell'invio di messaggi fraudolenti nei quali, spacciandosi per altri (banche, carte di credito) si chiede di confermare le proprie credenziali per scongiurare problemi.
Nel messaggio di phishing viene generalmente riportato il link a un sito fasullo, identico all'originale, ma con l'URL diverso, a meno che sia stata usata anche la tecnica del pharming.
In ogni modo, nessuna banca o azienda chiederebbe di confermare via email le proprie credenziali.

Posta elettronica

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

I file in allegato a un messaggio potrebbero essere infetti e danneggiare il computer.

Bisogna fare attenzione prima di aprire un allegato, soprattuto se il messaggio proviene da un mittente sconosciuto.

Si può fare una scansione con il software antivirus.

Posta elettronica

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

I file in allegato a un messaggio potrebbero essere infetti e danneggiare il computer.

Bisogna fare attenzione prima di aprire un allegato, soprattuto se il messaggio proviene da un mittente sconosciuto.

Si può fare una scansione con il software antivirus.

Messaggistica istantanea

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

La messaggistica istantanea è una modalità comunicativa mediata dal computer di tipo sincrono che sfrutta internet.
Esistono molti software sul mercato, generalmente gratuiti, che consentono anche funzionalità di chiamate audio/video e di invio file.
È utilizzata sia in contesti formali e aziendali, sia per lo scambio di messaggi tra amici.

Messaggistica istantanea

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

La messaggistica istantanea comporta il rischio:

- come tutti i software di poter far accedere al computer persone non autorizzate
- Come la posta elettronica di ricevere dei malware

Messaggistica istantanea

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

Perché la comunicazione sia sicura, è opportuno:

- utilizzare metodi di cifratura
- non divulgare informazioni e file personali indiscriminatamente
- stare attenti ad aprire file ricevuti da altri

GESTIONE SICURA DEI DATI

Protezione e backup

Messa in sicurezza e salvataggio dei dati

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 mettere al sicuro i dispositivi da furti o smarrimento è utile:

- tenere traccia della collocazione e dei dettagli, in modo da poter verificare eventuali mancanze
- utilizzare i cavi di sicurezza, i più diffusi seguono lo standard Kensington Security Lock.
- controllare gli accessi ai locali nei quali sono collocati, in modo da poter più facilmente risalire all'autore di eventuali furti.

Messa in sicurezza e salvataggio dei dati

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 mettere al sicuro i dispositivi da furti o smarrimento è utile:

- tenere traccia della collocazione e dei dettagli, in modo da poter verificare eventuali mancanze
- controllare gli accessi ai locali nei quali sono collocati, in modo da poter più facilmente risalire all'autore di eventuali furti
- utilizzare i cavi di sicurezza, i più diffusi seguono lo standard Kensington Security Lock.

Messa in sicurezza e salvataggio dei dati

Cavo di sicurezza, standard Kensington Security Lock

Messa in sicurezza e salvataggio dei dati

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

I dati possono essere persi anche per per la rottura dei dispositivi.

È quindi fondamentale avere una copia dei dati (backup):

- tutti i file realizzati
- font
- impostazioni software: profili colore, preferiti browser, ecc.

Messa in sicurezza e salvataggio dei dati

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

Perché sia efficace, l'operazione di backup si deve:

- stabilire la frequenza a seconda del numero di documenti elaborati quotidianamente
- impostare la copia automatica a scadenze regolari con un programma di backup preferibilmente quando il computer non viene utilizzato, per evitare che rallenti il lavoro.
- collocare la copia preferibilmente in altro luogo. Una buona soluzione è effettuarla online, su server remoti.

Messa in sicurezza e salvataggio dei dati

Effettuare la copia di sicurezza di dati.

Windows 7 permette di fare il backup su un hard disk esterno, senza installare programmi aggiuntivi, con i seguenti passi:

- Start→Pannello di Controllo→Backup e ripristino→Crea un'immagine del sistema
- Selezionare l'hard disk esterno su cui creare l'immagine del sistema e cliccare prima su Avanti e poi su Avvia backup.
- Al termine della procedura, Windows chiede di creare un disco di ripristino. Inserire quindi un CD/DVD vuotoe selezionare l'unità del masterizzatore dal menu Unità, clicca sul pulsante Crea disco.

Messa in sicurezza e salvataggio dei dati

Ripristinare e validare i dati sottoposti a copia di sicurezza.

Per ripristinare un'immagine del sistema su Windows 7:

Pannello di Controllo→Backup e ripristino→Ripristina le impostazioni di sistema o l'intero computer e Metodi di ripristino avanzati.

Nella finestra che si apre, cliccare su Utilizza un'immagine di sistema creata in precedenza e seguire la procedura guidata.

Distruzione sicura

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

I dati possono essere eliminati in modo permanente dai diversi dispositivi: quando no servono più, o quando ci si deve disfare di un dispositivo.

Distruzione sicura

Distinguere tra cancellare i dati e distruggerli in modo permanente.

La cancellazione di un file non garantisce la sua effettiva rimozione. Per cancellare un file bisogna:

- prima spostarlo nel cestino, da dove è facilmente recuperabile
- poi svuotare il cestino. Anche dopo questa operazione rimangono delle tracce sul disco, sia pure non visibili con gli strumenti quali il terminale.

  Appositi Sw possono ricostruirli integralmente o quasi, a seconda del tempo trascorso e dell'uso fatto del computer.

  Smart Data Recovery (Windows)

Distruzione sicura

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 la cancellazione definitiva dei dati vi sono i seguenti metodi:

- per il cartaceo, il tritadocumenti che riduce a coriandoli i fogli
- le memorie di massa posso essere rese inutilizzabili o smagnetizzate per mezzo dei degausser, apparecchi in grado di applicare intensi campi magnetici
- se la memoria di massa deve essere riutilizzata, appositi Sw sovrascrivono i file più volte rendendoli non recuperabili.

Riferimenti

Wikipedia

Prof. Fabio Frittoli