Distinguere tra dati e informazioni

I dati sono informazioni non ancora sottoposte a elaborazione, cioè 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.

Differenza tra hacking, cracking e hacking etico.

L'**Hacking** (dall'inglese to hack, intaccare) **consiste nell'accedere a risorse di rete senza averne l'autorizzazione**. **Se tale accesso comporta un vantaggio personale** (ad es. rimozioni di protezioni a software o recupero di codici di attivazione), **un lucro si parla di cracking.**

Se, invece, l' hacker usa l'acceso alla rete altrui "a fin di bene" **per testarne il grado di sicurezza** al fine di evitare l'abuso da parte di malintenzionati, si parla di **hacker etico**.

Il crimine informatico è **un'attività illegale che avviene utilizzando dei mezzi informatici come la rete Internet e un computer**. Esempi di crimine informatico sono: la **frode informatica**[1], il **furto d'identità**[2] **e l'accesso non autorizzato a sistemi informatici**.

La frode informatica consiste: nella duplicazione di programmi o nello scaricare, tramite internet, di **musica, libri**, **film soggetti** alla tutela del **copyright** senza il permesso dell'autore. Infatti, quando si acquista un prodotto non si diventa proprietari senza alcun vincolo, ma si acquisisce soltanto la licenza d'uso, detta **EULA**.

il furto di Identità consiste nell'ottenere indebitamente le informazioni personali della vittima, come: il numero della carta d'identità, del bancomat, della carta di credito, dell'account di posta elettronica. ecc di un soggetto al fine di sostituirsi in tutto o in parte ad esso e compiere azioni illecite in suo nome

L'accesso non autorizzato a sistemi informatici è minacciato:

1) **da una forza maggiore involontaria** (fuoco, inondazione, guerra, terremoto, furti, atti vandalici, ecc). Essa è quella causata da un evento imprevisto della natura o dell'uomo che può minacciare la conservazione dei dati.
2) **da una forza volontaria come impiegati e fornitori di servizi** autorizzati all'accesso ai dati che possono rubarli per poi rivenderli.

Le misure per prevenire accessi non autorizzati ai dati sono: password e cifratura.

1) **La password** serve a **proteggere i dispositivi che permettono l'accesso ai dati riservati** (ad es. la password di un account di windows, protegge il computer)
2) **La cifratura** (**codifica dei dati** attraverso l'uso di un algoritmo crittografico) **nel caso i dati finissero nelle mani dei malintenzionati**, **serve a non permettere ai dati riservati di essere utilizzati**. Ciò è necessario se i dati fossero memorizzati su una memoria rimovibile (pen drive, disco esterno, ma anche hard disk smontato dal computer e collegato ad un altro).

[1] **Esempi di frodi informatiche** sono: la riproduzione, l'utilizzo su diversi computer, la duplicazione di programmi o lo scaricare, tramite internet, di musica, testi, film soggetti alla tutela del copyright senza il permesso dell'autore. Infatti, quando si acquista un prodotto non si diventa proprietari senza alcun vincolo, ma si acquisisce soltanto la licenza d'uso, detta **EULA**.

[2] **il furto di Identità** consiste nell'ottenere indebitamente le informazioni personali come: il numero della carta d'identità, del bancomat, della carta di credito, dell'account di posta elettronica. ecc di un soggetto al fine di sostituirsi in tutto o in parte ad esso e compiere azioni illecite in suo nome**.**

Esercizio: In Windows la protezione dei documenti avviene:
1) **con una password** durante la fase di salvataggio del file → casella strumenti → opzione generali → password di apertura
2) **con la cifratura** durante la preparazione del file (menu file → prepara → crittografa → password di accesso). Una cosa analoga avviene per file compressi.

Le caratteristiche fondamentali della sicurezza delle informazioni sono:
1) confidenzialità (cioè non devono essere diffuse a chi non è autorizzato)
2) integrità (cioè complete e senza modifiche rispetto all'originale)
3) disponibilità (cioè disponibili al momento del bisogno, cioè reperibili nei tempi necessari).

Leggi dello stato:
1) **Legge n. 675 del 31 dicembre 1996, tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali**

2) Decreto Legislativo n. 5 sulla protezione dei dati personali: è stato **emesso in Italia il 9 febbraio 2012** che ha aggiornato il Dlgs 196/2003, a seguito dell'approvazione da parte di tutti e 26 paesi della Commissione Europea. Esso dichiara inoltre che "c**hiunque per motivi professionali conserva o tratta dati sensibili altrui** (e quindi, tutte le organizzazioni, le aziende, gli enti pubblici, i professionisti, ecc) **è soggetto alle cautele e agli obblighi previsti dalla legge in quanto responsabile civilmente e penalmente**.

Ingegneria sociale: (dall'inglese social engineering) **è lo studio del comportamento individuale di una persona al fine di carpire informazioni utili**. Essa è usata al posto delle tecniche di hacking, quando queste sono molto impegnative per accedere a informazioni personali a causa di sistemi di protezione hardware e software sofisticati e difficilmente penetrabili.

i metodi applicati dall'ingegneria sociale, tramite internet, sono:
1) il pretexting: le chiamate telefoniche che cercano di ottenere informazioni personali mascherandole con sondaggi anonimi, tramite un pretesto.

2) **il phishing** (**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 usare un link esterno nel quale inserire le proprie credenziali per motivazioni di sicurezza, riscuotere premi in denaro, beni tecnologici, ripristinare password scadute, ecc. Cliccando su quel link, tuttavia, l'utente sarà condotto in un sito web solo all'apparenza originale, (perché simile all'originale) in cui dovrà fornire informazioni private. I criminali potranno poi utilizzare i dati lasciati in tale sito fittizio per rubare denaro alle loro vittime.

3) **Il pharming è una tecnica** per impadronirsi dei dati personali di un utente, principalmente i dati bancari, **simile al phishing**. **quando si digita l'indirizzo web della propria banca**, o si clicca sul relativo link, **si viene indirizzati in automatico al sito "clone**" anche in questo caso, nel momento in cui si inseriscono i dati bancari personali, i truffatori li copiano per utilizzarli in un secondo tempo per operare sul conto corrente.

i metodi applicati dall'ingegneria sociale, senza internet, sono:
1) **lo 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 telecamere[3]. Ciò può avvenire generalmente in luoghi affollati, come internet cafè e tramite i terminali esterni POS.

2) il **Bin raiding** ("rovistare nella spazzatura") cioè **furto di informazioni personali nei documenti cartacei allegati alle bollette** del: gas, luce o telefono **che si buttano nel cestino** e che possono essere raccolte semplicemente rovistano nei rifiuti.

3) Il **Furto o smarrimento dei portafogli che contengono bancomat, carte di redito e documenti di identità** come la patente di guida e le tessere di iscrizione a determinate associazioni.

4) **Skimming**[4]**,** consiste nella **clonazione di una carta di credito attraverso l'apparecchiatura elettronica modificata detta POS** utilizzata negli esercizi commerciali per pagare i beni acquistati **oppure nella sostituzione del lettore carte con uno skimmer, capace di leggere i dati della carta, per poi trasmetterli a organizzazioni criminali** oppure **nella sostituzione della tastiera originale del bancomat con una taroccata con keylogger.**

5) **Rubare l'identità di un deceduto come: la sua età, data di nascita ed indirizzo attraverso i manifesti funebri**[5].

6) **Questionari cartacei** spesso vengono inviati per posta, **se sono molto lunghi**, **richiedono la compilazione di molte informazioni private** date ad estranei.

7) **Tramite noi stessi quando inconsciamente raccontiamo in pubblico fatti che ci riguardano** (nell'anticamera del dottore, al supermercato durante la fila alla cassa, ecc.),

Una macro è un insieme di istruzioni scritte nel linguaggio Visual Basic for Application (VBA) che possono essere eseguite, all'interno di un software di ufficio (scrittura, foglio di calcolo, ecc...) automaticamente o alla pressione di una combinazione di tasti.

Le macro sono strumenti molto utili perchè automatizzano procedure lunghe, ma possono contenere **codice malevolo** che quindi può causare danni al computer. Ciò vale soprattutto quando l'origine della macro non e certa. In linea di massima **la cosa migliore e attivare le macro di cui si e certi, e disattivare quelle di incerta provenienza**. **Un file ad es. di excel contenente una macro ha un'icona con un punto esclamativo e un'estensione diversa (xlsm)**

Il malware (contrazione delle parole inglesi malicious e software) **indica un software malevolo, ma non un virus vero e proprio**, **creato con lo scopo di causare danni più o meno gravi a un sistema informatico su cui viene eseguito** e ai dati degli utenti.

---

[3] Nei bancomat fare attenzione che in alto in corrispondenza del tastierino numerico non ci sia un piccolo foro con all'interno installato una telecamera.

[4] Deriva da skimmer che è uno degli strumenti più diffusi per la clonazione delle carte di credito. Si tratta di dispositivi camuffati negli sportelli di pagamento usati per leggere e copiare i dati riportati sulla banda larga della propria carta di pagamento

[5] Ad esempio per iscriverli al sito del M5*, da usare per le votazioni delle primarie del partito.

il malware si può nascondere ne computer come:

1) **Trojan horse[6]: se è nascosto in programmi di utilizzo comuni dell'utente** che contengono istruzioni dannose che vengono eseguite all'insaputa dell'utilizzatore
2) **Backdoor:** ("porta sul retro"), **se usa una "porta di servizio" che gli consente un accesso non autorizzato al sistema su cui è in esecuzione.**
3) **Rootkit: se è progettato per fornire agli hacher accesso come amministratore (root) a ai programmi (kit) senza che l'utente ne sia consapevole.**

Il Virus[7] o malware infettivo è un codice eseguibile che si diffonde infettando altri file in modo da essere eseguiti ogni volta che i file infetti sono aperti.

La "vita" di un virus informatico si svolge in tre fasi: **trasmissione, riproduzione e alterazione.** Nella fase di trasmissione il virus "infetta" uno o più file del computer; nella fase di riproduzione il virus copia se stesso nel sistema, all'interno del singolo PC o nella rete. Nella fase di alterazione il virus svolge il suo compito, che spesso significa danneggiare dati e programmi.

Il Worm o verme[8] **è un codice eseguibile che si diffonde modificando il sistema operativo in modo da essere eseguito automaticamente ogni volta che viene acceso il sistema** e rimanendo attivo per tutta la durata di tempo, fin quando non si spegne il computer. **Esso si trasmette** utilizzano tecniche di ingegneria sociale, oppure **sfruttando** dei **difetti (Bug)** di alcuni programmi per diffondersi automaticamente. Il loro scopo e rallentare il sistema con operazioni inutili o dannose.

I tipi di malware usati per furto di dati sono;

1) L' **Adware è un programma che propone messaggi pubblicitari**, non richiesti dall'utente, **attraverso finestre popup nel browser** o durante il processo di installazione di un software. Può causare danni quali rallentamenti del pc e rischi per la privacy in quanto comunicano abitudini di navigazione ad un server remoto.[9]
2) **Lo Spyware[10] è un software che viene usato per raccogliere informazioni** (abitudini di navigazione e e-mail) **per essere vendute ad aziende per effettuare della pubblicità mirata ma indesiderata all'utente.**
3) **Il Keylogger**[11] è un programma **in grado di registrare tutto ciò che viene digitato sulla tastiera** consentendo il furto di password o di dati personali. Esempi di dispositivi di keylogger sono quelli usati dai ladri sotto le tastiere dei POS dei bancomat per intercettare il codice PIN. I keylogger possono essere anche di tipo hardware, se collegati al cavo tra tastiera e pc

[6] Per esempio, si potrebbe trovare un gioco gratuito disponibile in rete che, una volta scaricato ed eseguito, senza che l'utente stesso ne sia a conoscenza, avvia e installa il codice trojan nascosto nel programma

[7] Si usa il termine "virus" in quanto il suo comportamento può essere paragonato a quello biologico, per la similitudine del modo di propagarsi dell'infezione

[8] E' paragonato al verme animale che si insedia nel corpo principale del degli alberi facendoli seccare.

[9] Per limitare tali msg pubblicitari durante la navigazione, bisogna cancellare, a fine navigazione, la cronologia e i file temporanei ovvero la cosiddetta "cache" del browser.

[10] Spyware e Adware sono simili: lo spyware ha l'obiettivo di intercettare le mail che l'utente usa per venderle alle aziende (le mail sono intercettabili poichè sono trasmesse in chiaro), l'adware ha il principale obiettivo di proporre durante la navigazione dell'utente, messaggi pubblicitari attinenti alla sua navigazione, per distrarlo e ritardarlo dalla navigazione scelta.

[11] Un app keylogger per android gratuita si chiama custom keyboard. Essa registra sia gli sms scritti che i msg whapapp.

4) **Il Dialer è un programma che quando ci si connette con la normale linea telefonica, modifica il numero telefonico chiamato dalla connessione predefinita** per impostarla verso numeri telefonici molto costosi
5) **Il Botnet** è **una rete (net) controllata da remoto** da un botmaster (bot) e **composta da dispositivi infettati da malware specializzato** che è in grado di utilizzare **l**a rete stessa e i dispositivi ad essa collegati per svolgere attività non autorizzate.

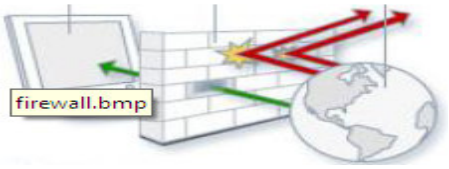
Il software antivirus e i suoi limiti. Esso è un software in grado di opporsi ai tentativi dei malware e virus di infettare il sistema. Esso **ha due funzioni principali**: quella di **controllare cartelle e file** in modo da individuare e rendere innocui eventuali file portatori di infezione virale e quella di **scansionare la memoria RAM** in modo da impedire l'esecuzione di codice virale. **I limiti dell'antivirus sono: deve essere aggiornato con frequenza**, in particolare l'archivio delle firme, in quanto nuovi malware vengono diffusi in continuazione e poi **a volte segnalano falsi positivi**, cioè indicano come virus programmi del tutto leciti. **La quarantena** è **una cartella creata dal software antivirus** e ,pertanto, facilmente controllabile, in cui chiede all'utente di inserire i file contenenti del codice virale o anche solo sospetti.

Ci sono tre tipi di scansione: con la **scansione Veloce** i virus sono cercati nei punti dove si nascondono più di frequente. Se si pensa che il computer sia infetto, nonostante la scansione veloce non abbia dato esito, si può eseguire la scansione Completa. **Nella scansione completa** sono controllati tutti i file del disco rigido e i programmi in esecuzione. Questo processo può durare alcune ore e le prestazioni del computer saranno rallentate. **La scansione Personalizzata** permette all'utente di scegliere le cartelle dell'hdd da esaminare.

Definizione di rete e di tipi di rete per estensione. Una rete informatica è un insieme di piu dispositivi, come computer o altro, in grado di comunicare tra di essi attraverso differenti mezzi. Una rete limitata a un locale o a un edificio prende il nome di **LAN** (Local Area Network). Se la rete e 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 una rete virtuale[12] privata (detta anche intranet o aziendale)** di dispositivi ubicati in luoghi fisici diversi che utilizza la rete pubblica Internet per funzionare. **L'admin di rete** ha il compito di rendere sicura una rete attraverso politiche di accesso alle risorse (file, cartelle, stampanti, accesso a internet) determinate da account personali di accesso con livelli diversi di permessi.

I principali vantaggi di una rete sono: condivisione risorse (file, periferiche), Indipendenza dei singoli elaboratori, Tolleranza ai guasti, Dischi e servizi di backup Condivisione delle informazioni, Possibilità di lavoro di gruppo

Il firewall e i suoi limiti. E' un dispositivo o un software **che 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



I limiti del firewall sono: per funzionare bene deve essere programmato in modo efficace, dato che si limita a seguire le **regole impostate** e il firewall non avrà effetto se l'attacco alla rete viene effettuato dall'interno, per esempio da un utente della rete[13].

[12] Il termine "Virtuale" è dovuto al fatto che i computer non sono effettivamente collegati solo tra loro, non hanno delle linee dedicate, ma utilizzano una struttura pubblica quale, appunto, la rete internet.
[13] Ad es, con un programma di cambio virtuale di indirizzo IP pubblico tipo ultrasurf

Esercizio: per accedere al firewall di windows, vai su pannello di controllo → windows firewall.

Connessione ad una rete. Una connessione ad una rete può avvenire utilizzando mezzi diversi: il doppino telefonico, la fibra ottica e le onde radio (in quest'ultimo caso si parla di rete wireless (senza cavo o wifi). La connessione ad una rete wireless avviene attraverso un programma del sistema operativo che avvisa l'esistenza di reti wifi disponibili. Le reti wifi protette hanno un lucchetto e ,pertanto, richiedono la password di accesso. Se la password inserita e corretta, al termine della procedura, viene segnalato che la connessione alla rete senza fili e stata stabilita.

I vantaggi di una rete cablata sono: la maggiore **sicurezza** e la **velocità** di trasmissione dei dati. **I vantaggi di una rete wifi** sono l'**economicità**[14], la **praticità** di utilizzo soprattutto con dispositivi mobili come notebook e tablet e la possibilità di essere **implementata facilmente.**

Sicurezza delle reti wifi: wep, wpa, wpa2.
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) nasce nel 1999 ma nel giro di pochi anni si è verificato che non è adeguatamente sicuro, in quanto essendo la chiave è troppo breve e abbastanza facile individuarla e poter quindi accedere e, quindi, intercettare il flusso dati o entrare in qualche cartella o disco condiviso della rete. **Una chiave WEP è una password alfanumerica**, impostata sul router, è può essere di diversa lunghezza, quali: 64bit, 128bit e 256bit.

Il WPA (Wifi Protected Access 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.

MAC address usato come altra sicurezza della WLAN
Il MAC detto anche Mac address[15], 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. **L'amministratore di rete può concedere l'accesso alla rete solo a dispositivi il cui MAC address è conosciuto e di cui ci si può fidare**. In questo modo, almeno in teoria, si crea un muro a difesa della propria rete. 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 piu metodi in combinazione si raggiunge un buon grado di sicurezza.**

Cambiare il SSID predefinito del router come altra sicurezza della WLAN
Il SSID è il nome predefinito del router. Ad es. Alice-12345611. Bene cambiarlo è utile.

[14] Non si deve posare un cavo di collegamento con tutti gli altri dispositivi
[15] Esercizio: per trovare l'indirizzo MAC del computer in uso, aprire il prompt dei comandi, digitare **ipconfig/all** e premere INVIO

Differenza MAC address e IP
La differenza tra l’indirizzo MAC e l’indirizzo IP, sta nel fatto che il MAC address è solitamente definito a livello hardware, assegnato dal produttore e non cambia mai nel tempo (a meno di interventi dell'amministratore di rete); l'indirizzo IP viene definito a livello software e può anche cambiare ad ogni nuova connessione alla rete.

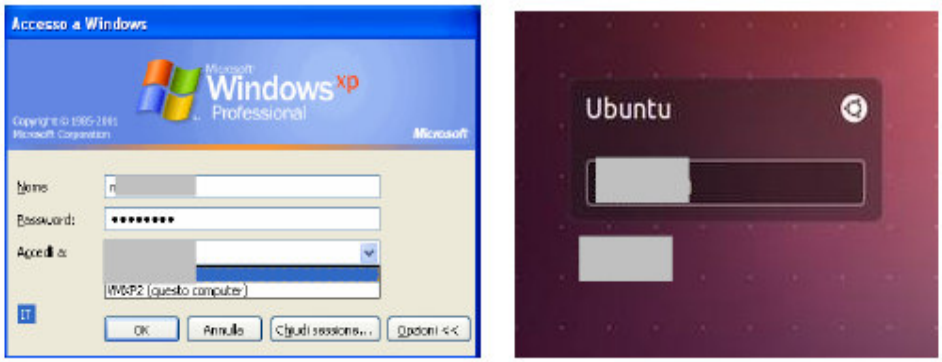
Spie digitali sono **dispositivi connessi ad una rete wireless non protetta che possono intercettare i dati presenti sui dispositivi connessi** o anche solo in transito.

Scheda di rete wireless e non è quella scheda che permette ad un dispositivi di connettersi ad una rete.

Per essere installata nel computer, dopo il suo inserimento richiede un driver diverso in base al sistema operativo usato, in genere a corredo della scheda o scaricabile dal sito del produttore.

Hotspot WiFi: sono dei punti di accesso ad internet, con tecnologia wireless, **aperti al pubblico.**

L’account di rete ovvero la **coppia username e password ha lo scopo di permettere solo ad utenti autorizzati l’accesso alla rete**. Esso avviene inserendo, in fase di avvio del computer, l’account in una mascherina.



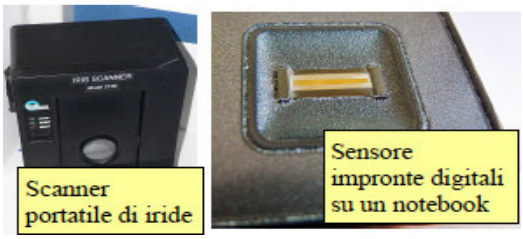
L’account di livello più elevato è **Administrator**: con questo account si può eseguire qualsiasi operazione sul computer o sulla rete: cambiare e modificare password, installare e disinstallare programmi, aprire e modificare qualsiasi file o cartella, cancellare o creare altri account. Quello a livello più basso è **Guest**: per questo account non è prevista la password e consente l'accesso solo temporaneo ad ospiti.

Architettura di rete paritetica (peer to peer) sono quelle in cui tutti **i computer svolgono funzioni simili**, poiché non ci sono server, ma ogni computer svolge sia le funzioni di client che di server. **L'autenticazione degli utenti avviene a livello locale sul singolo computer** (non richiede la connessione al server) e le risorse condivise sui vari computer sono accessibili in base alle impostazioni sui singoli computer.

Architettura di rete client server sono quelle in cui: 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.

La password garantisce la privacy dei propri dati e anche la sicurezza delle reti solo se risponda a **criteri di robustezza**[16] e venga gestita in modo corretto **mantenendola segreta** e **annotarla in un luogo sicuro** per evitare che venga dimenticata o persa.

Tecniche di sicurezza biometriche sono: il **riconoscimento vocale** (si rileva il timbro, la tonalità e la velocità con cui si parla), **la scansione delle impronte digitali** e la **scansione dell'iride dell'occhio** usate attualmente al posto delle password, per accedere al computer in modo sicuro.

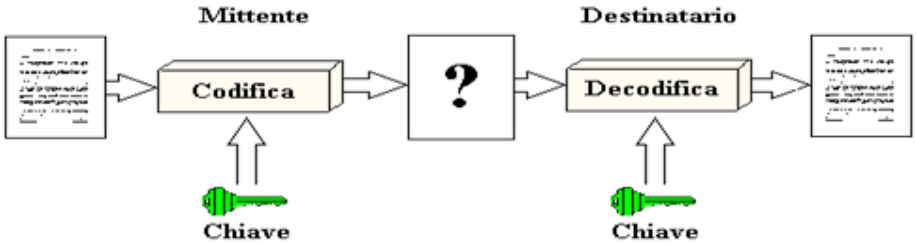


Certificati digitali

Il Certificato Digitale è un file, con una validità temporale limitata, **usato per garantire l'identità di un soggetto, sia esso un sito web o una persona**. Essi rappresentano quello che i documenti d'identità costituiscono nella vita reale; pertanto, servono per stabilire con esattezza, in una comunicazione, l'identità delle parti. **I certificati digitali sono rilasciati** dalle cosiddette **autorità di certificazione (Certification Authority**, solitamente abbreviato con C.A.). Essa rilascia i certificati a chi ne fa richiesta dopo averne attestato l'identità e svolge il ruolo di garante dell'identità di chi usa il certificato da lei rilasciato[17].

Crittografia a chiave[18] **simmetrica**

La crittografia **è simmetrica o a chiave privata, quando i due soggetti che vogliono comunicare in modo segreto stabiliscono un codice di comunicazione e la chiave che lo decifra**. Solo i possessori della chiave sono in grado di decifrare e comprendere i messaggi criptati. Il problema principale di questa tecnica è che la chiave deve essere comunicata al destinatario senza che nessun altro catturi questa informazione, ma quando i soggetti in gioco tra mittente e destinatario aumentano, il problema della distribuzione delle chiavi diventa critico allora in tal caso si passa alla crittografia asimmetrica o a chiave pubblica.



I certificati sono basati su un sistema di crittografia a chiave asimmetrica.

La crittografia a chiave asimmetrica consiste nell'utilizzo di una coppia di chiavi diverse, dette chiave pubblica e chiave privata, ognuna delle quali è in grado di effettuare una trasformazione del messaggio e di decodificare quello che l'altra ha codificato.

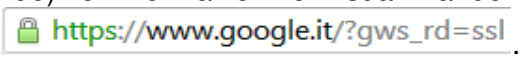
[16] Deve essere lunga almeno 8 caratteri, utilizzare lettere maiuscole e minuscole, numeri e anche caratteri speciali, come la @, il #, uno spazio vuoto o simili.
[17] Come ad esempio, le autorità di pubblica sicurezza (prefettura, comune, etc…) che emettono documenti di identificazione quali il passaporto o la carta d'identità.
[18] Una chiave è una stringa, un insieme di caratteri (lettere, numeri, simboli) di una certa lunghezza.

La chiave privata viene tenuta segreta, l'altra viene resa pubblica e ciascuno mette a disposizione degli altri la sua chiave pubblica, conservando invece gelosamente la propria chiave privata. **Un soggetto che voglia inviare un messaggio segreto lo codifica con la chiave pubblica del destinatario, il quale può leggerlo solo decodificandolo con la propria chiave privata.**

Un certificato digitale è composto da: la chiave pubblica del possessore; il nome del possessore[19], la data di scadenza della chiave pubblica; il nome della CA che ha emesso il certificato; la firma digitale della CA che ha emesso il certificato.

Un certificato digitale è personale se consente di verificare l'identità dell'utente e viene utilizzato quando si inviano informazioni personali tramite internet a un sito web. È possibile provare la propria identità con una chiave digitale privata di tipo hardware o software;

Un certificato digitale è di un sito web se consente di identificare l'autenticità di un sito web specifico e di verificare che l'identità del sito protetto originale non venga assunta da un altro sito web.

Esercizio: visita al sito web protetto: www.google.it.
Quando si visita google, un sito web protetto, il sito invia automaticamente il proprio certificato digitale all'utente, crittografando (cioè cifrando) le informazioni e visualizzando un'icona a forma di lucchetto nella barra degli indirizzi. 

. L'indirizzo della pagina inizia con la sigla https (Hyper Text Transfer Protocol Secure), invece che il "classico" http. Significa che **il sito trasmette i dati dopo averli cifrati con una chiave robusta in modo che: solo il sito web che li riceve e solo quello che li trasmette siano in grado di decodificarli**. **La "s" significa "sicuro".** Facendo clic sul lucchetto, appare il rapporto sulla sicurezza relativo al sito Web con le informazioni contenute nel certificato.

Esercizio2: visualizzare i certificati digitali presenti nel proprio computer
È possibile visualizzare i certificati presenti nel computer con il Gestore certificati. E' necessario:
1) essere connessi al computer come amministratore.
2) aprire gestore certificati, facendo clic sul pulsante Start, digitare certmgr.msc nella casella di ricerca di windows e premere invio.
3) Può essere richiesta una password amministratore o una conferma

Sicurezza dei Browser: eliminare Il complemento automatico. Esso è una opzione che **consente al browser di "ricordare" i dati inseriti** e riproporli all'utente. È sicuramente una bella comodità, che evita la riscrittura di informazioni lunghe e complesse come il codice fiscale o il numero di cellulare. **Se il proprio computer è utilizzato da più utenti è conveniente disabilitare[20]** queste opzioni di completamento e di salvataggio automatico del browser, per evitare la diffusione dei propri dati personali.

[19] Se il possessore è una persona fisica si tratterà di nome e cognome, data di nascita ecc. Se invece è un server web sarà presente l'indirizzo web e il nome della compagnia titolare del dominio
[20] In internet Explorer, menu strumenti → opzioni internet → scheda contenuto → riquadro complemento automatico.

OTP: One Time Password (password usata una volta) è una **password che è valida solo una volta, per una singola sessione di accesso** o una singola operazione. [21] L'OTP è generato da un dispositivo elettronoco (**Token**) o dal sito e inviato sullo smartphone e per mail.

Sicurezza del Browser: eliminare dati privati come cookie, cronologia e file temporanei.
Il **cookie** ("biscotti") **è una stringa di testo che viene inviata da un server web e memorizzata dal browser** con lo scopo di memorizzare alcune informazioni utili a velocizzare un accesso successivo. Ad esempio i dati relativi agli acquisti fatti in un sito, le impostazioni di visualizzazione di una pagina web, ecc. Quando si accede nuovamente alla stessa pagina, 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**. Inoltre i cookie possono costituire un rischio per la privacy in quanto tengono traccia dei siti visitati.

Esercizio1: I cookie memorizzati si possono eliminare in Internet Explorer dal menu strumenti → Opzioni internet → scheda Generale → pulsante elimina.

Esercizio2: È possibile bloccare o consentire la memorizzazione dei cookie nel menu strumenti → opzioni internet → scheda **privacy.** Conviene **spostare il livello in una zona intermedia** ovvero consentire i cookie di siti web che dispongono di informative sulla privacy e **bloccare quelli di siti web che memorizzano informazioni personali senza il consenso dell'utente**.

Esercizio3: Eliminare la cronologia (**ctrl+shift+canc**) di navigazione e i file temporanei.

Controllo Genitori o controllo parentale: consiste nell'impostare delle **restrizioni ai minori** come: 1) tempo di utilizzo del computer da parte di un utente, 2) i programmi e i giochi che possono utilizzare, 3) i siti internet che si possono visitare.

Esercizio: in windows impostare il controllo genitori su un utente minore ad es. luca. A tal fine: 1) si deve accedere all' utente admin del computer; 2) selezionare l'utente standard Luca e applicare il controllo genitori; 3) successivamente si possono specificare anche altre restrizione come: il tempo di connessione, l'intervallo orario di connessione, i giochi e programmi che si possono usare in base al contenuto, i siti internet.

Controllo parentale Qustodio: un software gratuito per uso personale per computer windows e mac osx e smatphone android e ios: scaricabile al link: https://www.qustodio.com/it/

Una comunità virtuale è un gruppo di persone riunite via Internet per valori o interessi comuni. Ad esempio, una passione, un divertimento o un mestiere o semplicemente per cercare nuove conoscenze.

Il **Social Network è una comunita virtuale il cui scopo è di mettere persone in contatto e far nascere relazioni. Essi offrono:** 1) la possibilità di creare una propria pagina web, con una struttura predefinita, dove inserire un profilo personale e dove si può raccontare qualcosa

[21] Nel caso delle OTP, dato che il valore è continuamente modificato, se un malintenzionato riesce ad conoscere una OTP già utilizzata per accedere a un servizio o eseguire una transazione, non può utilizzarla, in quanto non è più valida.

di proprio e 2) avere uno spazio gratuito per pubblicare link, immagini, musica video utilizzando tutte le modalità comunicative della rete (forum, chat, inserimento di testi ed immagini, condivisione di foto/video, e-mail, Instant Messaging, ecc.) in un unico ambiente.

Per la sicurezza, regole da seguire sui social network.
1) Non divulgare informazioni personali nelle reti sociali. I social network sites si basano sullo scambio di informazioni tra i partecipanti, così **incoraggiano gli utenti a mettere a disposizione una certa quantità di informazioni personali** (ad es. il proprio indirizzo, informazioni circa la propria vita e le proprie abitudini) non tenendo conto che queste possono cadere in mano a malintenzionati.
2) **Restringere il numero di amici a queli effettivamente conosciuti**, poiché si deve sempre tenere presente che internet è una risorsa pubblica e che chiunque, **anche un falso profilo detti fake**[22], può aver accesso ai dati pubblicati.
3) **non 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
4) **applicare impostazioni per la privacy del proprio account.**

Altri rischi nell'uso delle reti sociali: Cyberbullismo e addescamento (o grooming)
il **cyberbullismo** consiste **nell'utilizzo di internet per attaccare ripetutamente un individuo per danneggiare la sua reputazione in una comunità molto ampia**;

L'**adescamento consiste nel tentativo di acquisire la confidenza di una persona, generalmente un minore, allo scopo di indirizzarla verso comportamenti sessuali inappropriati**.

La posta elettronica. Essa 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 la posta elettronica sicura bisogna: **cifrarla** (ovvero usare la cosiddetta posta elettronica certificata)[23]

La firma digitale è un algoritmo, personale e legato alla cifratura dei dati. **Essa attesta l'identità' e l'autenticità di un documento elettronico**. Esse sono 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.

Per firmare digitalmente i documenti, una volta in possesso di una firma digitale, si può utilizzare il software predisposto dal fornitore oppure apporre la firma digitale nei differenti software di posta elettronica.

Esercizio: con Mozilla Thunderbird, si deve scegliere Modifica → Impostazioni account→ scheda Sicurezza e scegliere la firma digitale da utilizzare.

[22] Secondo la Cassazione chi crea una falsa identità sul web commette un reato, in quanto "si lede la fede pubblica degli utenti che credono di parlare con una persona diversa quella che si è nella quotidianità
[23] La posta certificata essendo sicura non è trasmessa in chiaro e quindi non è intercettabile dagli spyware e perciò non contiene spam.

Lo spam è l'invio di messaggi non richiesti (dagli spammer), generalmente di carattere pubblicitario, che hanno lo scopo di indurre i destinatari ad acquistare. In tutti i casi **è opportuno non rispondere a messaggi di questi tipo e ne aprire tali messaggi,** neppure per dire che non si e interessati, perche 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.

Allegati alla posta: Alcuni messaggi hanno **in allegato dei file infetti da malware**, che possono danneggiare il computer. Pertanto occorre fare molta attenzione prima di aprire un allegato, per esempio facendo una scansione con il software antivirus.

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 (Skype, Messenger, ecc.) di messaggistica istantanea danno anche la possibilità di chiamate audio e video.

Poca sicurezza della messaggistica istantanea: Come la posta elettronica, anche la messaggistica istantanea comporta il rischio di ricevere sul proprio computer dei malware che possono comprometterne la sicurezza rendendo possibile l'accesso al computer a persone non autorizzate.

Messa in sicurezza dei dispositivi informatici. 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, **usati spesso nelle aule delle scuole**.

Copie di backup. I dati si possono perdere per la rottura di un dispositivo di memorizzazione, o anche per lo smarrimento o il furto di un dispositivo portatile. E quindi importante avere **una copia di sicurezza (backup) dei dati che permetta di ricostruirli in caso di perdita**.

Copia di backup aggiornata. La copia 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, **e opportuno impostare un programma di copia in modo che questa avvenga automaticamente a scadenze regolari** quando il pc è acceso ma non è in uso.

Collocazione copia di backup. 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 (DropBox, Google Drive, ecc)

Ripristino dei dati: esso consiste nel trasferimento dei dati dalla copia di sicurezza (detta anche immagine dell’hard disk) alla posizione originale, in modo da verificare l'efficacia e la completezza dell'operazione.

Cancellazione e distruzione dei file. Anche se i file vengono cancellati dal Cestino, in realtà rimangono delle tracce sul disco e quindi possono essere recuperati.
Per cancellare documenti elettronici, è necessario sovrascriverli più volte o distruggere fisicamente le memoria di massa sui cui sono registrati. Invece, **per cancellare definitivamente i documenti cartacei**, **è opportuno utilizzare dei tritadocumenti,**