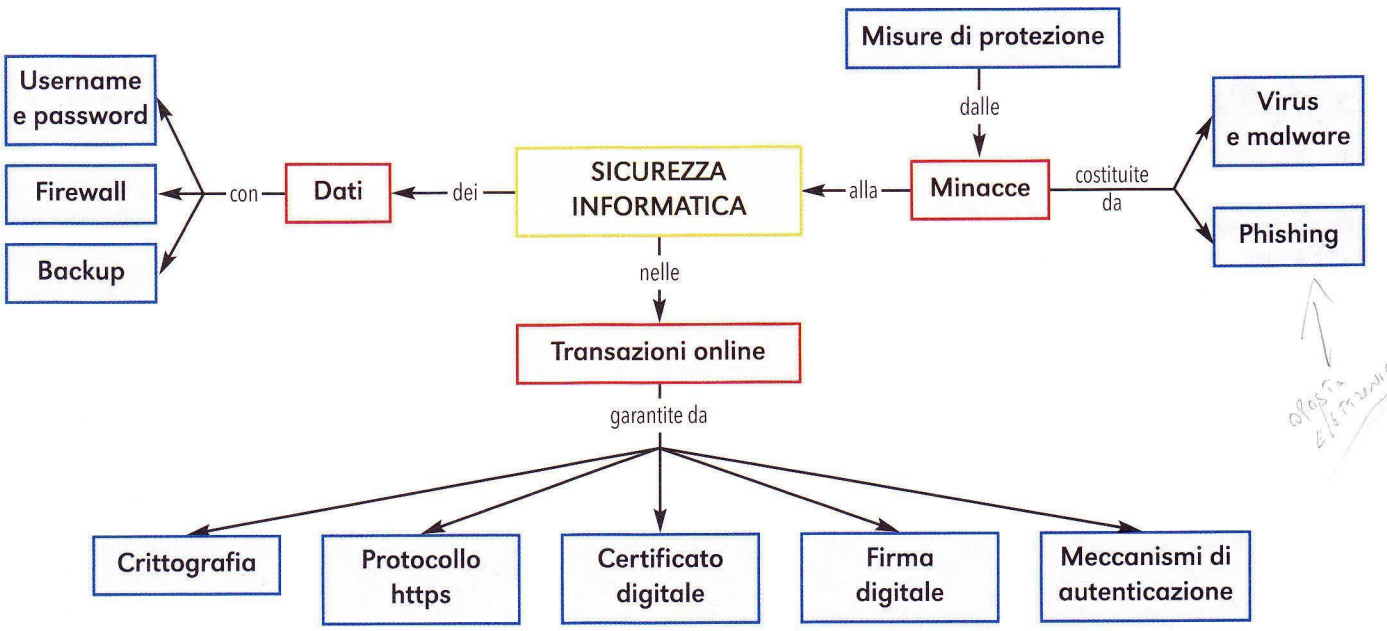
Uda 2 SICUREZZA INFORMATICA

OBIETTIVI UNITÀ

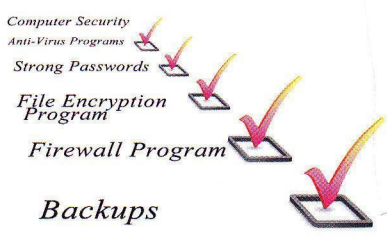
- Illustrare le regole da rispettare per preservare la sicurezza dei dati informatici.
- Individuare le principali minacce alla sicurezza e i comportamenti da adottare per tutelarsi.
- Conoscere gli strumenti che offrono garanzie riguardo la sicurezza nelle transazioni online.



Area digitale

- Rischi nell'uso di strumenti online

I dati che viaggiano sulla rete e quelli custoditi da privati o aziende richiedono una vera e propria **protezione** da accessi non autorizzati, frodi, furti, virus e altri malware.



Sicurezza dei dati

La **sicurezza dei dati** e il corretto impiego degli strumenti atti a preservarla è uno dei valori a cui prestare massima attenzione: per garantire questa tutela in maniera adeguata, è necessario **rispettare** una serie di **regole** elementari e **adottare corretti comportamenti** nell'uso dell'elaboratore.

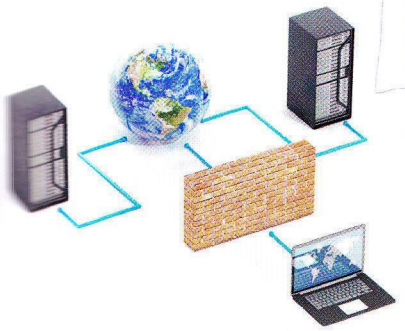
Username e password

Quando un elaboratore è utilizzato da più persone, solitamente si prevede, per ognuna di esse, uno specifico account, a cui si accede con username e password. **Ogni utente avrà** così **il proprio ambito di operatività**, in base anche ai permessi che gli sono stati assegnati in fase di creazione dell'account (*vedi* pag. 33, Area digitale, "Creare e gestire account"): in caso di **account standard**, egli potrà accedere esclusivamente ai propri dati, senza possibilità di accesso a quelli degli altri utenti. In genere, anche nelle aziende ogni dipendente esegue l'accesso al sistema mediante **login** al quale è associato lo **specifico livello di autorizzazioni** previsto per quel lavoratore.

Inoltre, username e password vengono normalmente richiesti anche per accedere ai diversi servizi Web, quali la posta elettronica, il servizio di e-banking ecc.

- Lo **username** (identificativo utente) è un nome mediante il quale il sistema attiva la procedura di riconoscimento e gli ambiti di operatività concessi al suo proprietario.
- La **password** (stringa di caratteri, anche alfanumerici) serve a verificare che l'identificativo sia di fatto adoperato dal suo assegnatario ed è efficace quando:
  - non è costituita da informazioni riconducibili al proprietario;
  - non è divulgata né annotata su fogli o post-it;
  - è abbastanza lunga e complessa, per esempio, alfanumerica;
  - è cambiata regolarmente;
  - è diversa per ogni servizio a cui si accede.

Il firewall



Il firewall (letteralmente "parafuoco") è un sistema di sicurezza, hardware e/o software, che **filtra le informazioni in entrata e in uscita da una rete o un computer**.

Applica regole che contribuiscono alla sicurezza e alla salvaguardia dei dati e dei sistemi da accessi non voluti o da esecuzioni di software provenienti dalla Rete, potenzialmente pericolosi.
Il firewall è un sistema utilizzato per proteggere un computer, un server o una rete bloccando e veicolando il traffico sia da altre reti locali, sia da Internet, in quanto può consentire il passaggio solamente di certi tipi di dati, da determinati terminali e specifici utenti.
Nell'ambito delle reti di computer, un firewall è un **dispositivo hardware** di difesa perimetrale che può anche svolgere funzioni di collegamento tra due o più tronconi di rete.
Esiste un secondo tipo di firewall (**software** o **logico**), installato direttamente sui sistemi da proteggere, che permette di impostare delle regole che concedono o negano l'accesso a Internet da parte dei programmi installati, per prevenire la possibilità che un virus possa connettere in automatico il computer all'esterno pregiudicandone la sicurezza.

Il backup

In caso di **inconvenienti** con un elaboratore, mentre in genere è possibile reinstallare i programmi, i dati archiviati potrebbero essere distrutti o diventare irrecuperabili. Le cause possono essere diverse:

- rottura dei dispositivi di memorizzazione;
- malfunzionamento del sistema operativo;
- contagio da virus;
- errori degli operatori;
- attacco da parte di hacker;
- black out elettrici;
- incendi o allagamenti.

La migliore precauzione rispetto a queste eventualità consiste nel fare regolarmente delle copie di **backup**.

Il backup consiste nel **copiare i dati** memorizzati in un elaboratore **su supporti di memorizzazione esterni**.

Tali supporti, come per esempio chiavetta o hard disk USB, nastri magnetici, server remoto ecc. andranno scelti in base alla quantità di dati da copiare.

SEGUIMI!

L'**attività opposta al backup**, con la quale si ricaricano su disco fisso tutti o parte degli archivi o dei software salvati, è detta **restore**.

Le copie vanno conservate in luogo sicuro, diverso da quello in cui si trovano gli originali, protetto da polvere, calore e campi magnetici. La **frequenza** con cui si realizzano i **backup** dipende dall'attività che si svolge: per esempio, mentre in una banca si procederà con il backup più volte al giorno, sarà sufficiente una frequenza giornaliera in un piccolo studio professionale e magari settimanale in un'abitazione privata.

Regole per proteggersi da virus e altri malware

Le principali misure che si possono adottare per **proteggere il proprio computer dai malware** sono:

- installare un programma antimalware/antivirus e aggiornarlo regolarmente;
- impostare l'antimalware in modo che blocchi l'apertura di file sospetti o proceda, dopo aver avvisato l'utente, alla loro eliminazione o messa in quarantena. Questa procedura consiste nell'isolare il file infetto in una specifica area del disco in modo da renderlo inoffensivo per il sistema;
- eseguire, con il software antimalware, la scansione (cioè il controllo) di tutti i file in ingresso, provenienti da Internet o da memorie esterne;
- essere prudenti nell'apertura degli allegati a messaggi di posta elettronica anche se inviati da mittenti conosciuti o creati con programmi noti;
- disattivare l'esecuzione automatica di macro.

AL VOLO!

Il firewall è un sistema di sicurezza:
○ hardware/software
○ software

Area digitale

- Quarantena ed eliminazione di file infetti

Minacce alla sicurezza

Eseguire il download di file dal Web, oppure scambiare file mediante chiavette USB, sono operazioni potenzialmente pericolose. Gli elementi scaricati o trasferiti da un PC a un altro, infatti, possono contenere **virus**, o altri **malware**, capaci di **provocare danni di vario genere**.

I virus e altri malware

Si definisce malware (termine che deriva dalla contrazione di *malicious* e *software*, "programma maligno") qualsiasi **software il cui scopo** è quello di **danneggiare**, in modo diretto o indiretto e più o meno grave, un **sistema informatico** mettendone a rischio il funzionamento e le prestazioni e/o violando la privacy del proprietario.

In base al modo in cui sono scritti o in cui si diffondono, i malware si distinguono in diverse categorie, ognuna con specifiche caratteristiche.

- **Virus**: sono parti di codice che si trasmettono riproducendosi all'interno di altri programmi (file eseguibili), o in una determinata sezione del disco fisso, in modo da essere eseguiti ogni volta che il file infetto viene aperto. Si trasmettono generalmente da un computer a un altro per azione dell'utente mediante il trasferimento dei file infetti.
- **Worms** ("vermi"): alterano il sistema operativo del computer in cui si installano, e riescono a eseguirsi automaticamente e ad autoreplicarsi utilizzando come canale di diffusione reti LAN o Internet, sfruttando la posta elettronica oppure bug di alcuni software. La tipica azione di un worm è quella di inviare a tutti i contatti registrati nella propria rubrica un messaggio con se stesso come allegato e, di conseguenza, chi lo riceve, conoscendo il mittente, apre l'allegato e viene infettato.
- **Trojan horses** ("cavalli di troia"): si nascondono all'interno di programmi apparentemente innocui che, non appena vengono lanciati, mandano in esecuzione il malware

SEGUIMI!

In informatica il termine ***bug*** ("baco") indica un **errore nella scrittura di un programma**.

AL VOLO!

Per proteggere l'elaboratore da malware è utile:
- ○ installare e aggiornare un antimalware
- ○ installare un antimalware

I virus si trasmettono senza l'azione dell'utente:
- ○ vero
- ○ falso

le cui istruzioni dannose possono rovinare i dati su disco. Non sono in grado di autoreplicarsi e, per contagiare, hanno bisogno dell'intervento dell'utente. Attraverso un trojan o un worm è possibile il contagio da **malware backdoor** ("porta sul retro"), che permettono a estranei di accedere senza autorizzazione al sistema, fino ad arrivare a prendere il controllo in remoto del computer contagiato.

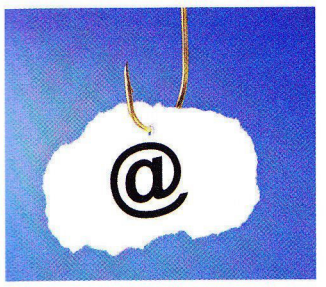
- **Spyware**: si appropriano delle informazioni del sistema su cui sono installati, inerenti, per esempio, l'attività online svolta dall'utente, o altre informazioni riservate, e le trasmettono a estranei. Questi malware ledono la privacy e solitamente gli effetti consistono nell'invio all'utente di pubblicità mirata non desiderata o, addirittura, in alcuni casi, nella sottrazione di denaro.

Come si trasmettono

La **trasmissione dei malware** avviene fondamentalmente attraverso:
- lo scambio di file o programmi infetti residenti su memorie di massa (chiavetta USB, CD ecc.);
- il download di file scaricati dalla Rete;
- l'apertura di allegati a e-mail, a messaggi istantanei o di file contenuti in cartelle condivise, anche online.

I rischi di essere vittime di malware e attacchi informatici, tuttavia, **dipendono** anche **dalla piattaforma e dai programmi che si utilizzano**, dal momento che, per molteplici ragioni (progettuali, tecniche, di diffusione ecc.), alcuni sistemi operativi e alcune applicazioni sono più soggetti ad attacchi informatici di altri.

Il phishing



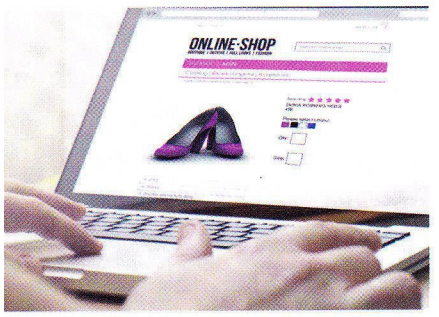
Il phishing è una **frode** ideata per indurre l'utente a **rivelare informazioni personali o finanziare**.

Il fenomeno del phishing si basa su **tecniche di *social engineering*** ("ingegneria sociale") che consistono nell'acquisire informazioni riservate direttamente dall'utente coinvolto, ottenendo la sua fiducia con l'inganno. Si realizza, per esempio, attraverso la ricezione di un messaggio di posta elettronica, in apparenza proveniente da un sito Web sicuro come la propria banca, con la richiesta di fornire informazioni riservate.

Il messaggio può essere un avviso in merito ad alcuni problemi riguardo al proprio conto corrente o account e invita ad attivare un link, presente nel testo del messaggio, per regolarizzare la propria posizione e risolvere il problema. Tale link però non conduce al sito ufficiale dell'Istituto di credito presso il quale si ha il conto corrente, ma a un suo clone molto simile, memorizzato in un server controllato dal *phisher*, in cui vengono registrate le informazioni personali dell'utente (numero di conto corrente, carta di credito ecc.) che il phisher poi utilizzerà per acquistare beni, sottrarre denaro ecc.

La tecnica del phishing spesso fa uso dello spamming, tecnica che consiste nell'invio massiccio di e-mail non richieste nelle caselle postali di più persone. Il phisher infatti non conosce la sua vittima e, di conseguenza, non sa di quale banca sia cliente. Tuttavia, inviando lo stesso messaggio a un numero molto elevato di indirizzi e-mail, spera di contattare casualmente almeno qualche utente che ha effettivamente un conto presso la banca presentata nel messaggio e, in caso l'utente risponda, la frode è compiuta.

Per evitare la truffa si raccomanda di **non collegarsi** mai **a siti di banche** o altre organizzazioni **mediante link** presenti **in e-mail** e di non fornire mai dati riservati.



Sicurezza nelle transazioni online

Aumentano ogni giorno gli utenti che acquistano prodotti o servizi online. Per non incorrere in frodi, occorre fare attenzione nel procedere a transazioni commerciali preferendo siti noti per la serietà e la reputazione ad altri poco conosciuti e fornendo esclusivamente le informazioni necessarie all'operazione da eseguire.
In generale, può essere rischioso fornire dati personali o finanziari su siti poco affidabili, perché tali informazioni potrebbero essere utilizzate per scopi diversi rispetto alle intenzioni dell'utente.
Di seguito vengono descritti alcuni indispensabili **strumenti** che garantiscono la **protezione** dei dati nello svolgimento delle **transazioni online**.

La crittografia

La crittografia è un procedimento matematico che impiega gli algoritmi per **rendere incomprensibile un messaggio a chi non ne ha la chiave**. Il suo scopo è proteggere le informazioni rendendole inaccessibili a tutti tranne che al destinatario.

SEGUIMI!

La **chiave pubblica** e la **chiave privata** sono utilizzate per **crittografare/decrittografare** le informazioni; mentre la prima, come dice il termine, può essere anche essere conosciuta, l'altra deve essere tenuta segreta dal possessore.

Per criptare i dati viene spesso utilizzata la **crittografia a doppia chiave, o asimmetrica**. Questo sistema prevede l'uso di due chiavi: la **chiave pubblica**, resa nota all'interno del certificato digitale, e la **chiave privata**, correlata in modo univoco alla pubblica, che rimane segreta e associata al titolare; a ogni coppia di chiavi corrisponde un solo utente.

Il protocollo https

Mentre si naviga in Internet e si visitano siti in cui si intende effettuare operazioni commerciali, alcuni elementi mostrati sulla barra dell'indirizzo possono fornirci indicazioni sulla sicurezza del sito.
Quando nel Web si eseguono per esempio operazioni bancarie online o pagamenti che comportano la comunicazione di informazioni strettamente riservate, quali il numero della carta di credito, il **protocollo https** (*Hyper Text Transfer Protocol Secure*, "protocollo criptato di trasferimento di ipertesti") **garantisce la trasmissione criptata**, o assoggettata ad autenticazione, di tali informazioni.
I server Web che richiedono per l'accesso il protocollo https, in luogo dell'http, attivano una **connessione SSL** (*Secure Socket Layer*, "sistema di accesso sicuro"), che aggiunge sicurezza alla transazione, garantendo la crittografia, o cifratura, dei dati trasmessi. In pratica, viene attivata una connessione protetta, un canale di comunicazione criptato tra il client, ovvero il PC dell'utente, e il server Web. Le informazioni inviate al server Web vengono crittografate nel computer client e decrittografate nel server Web: questo tipo di comunicazione garantisce che solamente il client e il server sono in grado di conoscere il contenuto della comunicazione.
Al momento dell'attivazione di una **connessione protetta**, nella barra dell'indirizzo di Google Chrome verrà visualizzata l'**icona di un lucchetto** (*Figura 1*). Operando sull'icona si viene informati che la connessione al server è crittografata e, facendo clic su **Dettagli** e poi su **View certificate**, si ottengono informazioni sul certificato che garantisce l'identità del computer remoto (server Web), sull'ente che lo ha rilasciato e sul periodo di validità.

SEGUIMI!

L'**https** viene considerato l'evoluzione del protocollo http, dal quale si differenzia per una **maggiore garanzia rispetto alla intercettazione dei dati**.
I server Web che richiedono tale protocollo per l'accesso trasmettono i dati utilizzando la porta 443 anziché quella di default (la 80), che risulta essere meno sicura.

Figura 1
Connessione protetta

AL VOLO!

Il phishing si basa sullo spamming:
○ falso
○ vero

Va sottolineato tuttavia che una **connessione protetta** non offre garanzie sull'onestà del sito, ma solo sulla certezza della sua identità, in base alle informazioni fornite dall'organizzazione certificante.

Il certificato digitale

Per ottenere la crittografia dei dati trasmessi, il sito coinvolto deve inviare all'utente un **certificato digitale** (*Figura 2*), documento elettronico che associa l'identità di una persona a una chiave pubblica di accesso: una sorta di carta d'identità elettronica di un utente di Internet.
Tale certificato, utilizzato per verificare l'identità di un utente o di un dispositivo, autenticare un servizio, crittografare la trasmissione di dati, contiene anche informazioni sull'identità del proprietario del sito o dell'organizzazione.

Figura 2
Certificato digitale

Un certificato digitale è un file elettronico che **identifica in modo univoco persone e siti Web su Internet** e che permette comunicazioni sicure e riservate, garantendo l'identità di un soggetto in Internet, sia esso un server o una persona.

I certificati digitali sono rilasciati da un'Autorità Certificativa (*Certification Authority*), ente che accerta la validità di tale certificato in modo da definire da un lato la vera identità dell'utente, dall'altro l'attendibilità del sito, verificando altresì che quest'ultimo renda disponibile un'informativa sulla privacy con informazioni dettagliate sull'utilizzo dei dati personali degli utenti.

La firma digitale

AL VOLO!

Accedendo a un sito il cui server Web richiede il protocollo https, è possibile ottenere informazioni sul suo certificato digitale:
○ falso
○ vero

La **firma digitale** equivale alla firma autografa apposta su carta, perciò possiede gli attributi di:

- **autenticità**, cioè dà garanzia sull'identità di colui che la sottoscrive;
- **integrità**, cioè attesta che il documento su cui è stata apposta non è stato modificato dopo la firma;
- **non ripudio**, cioè il sottoscrittore non può negare di aver sottoscritto il documento in cui è stata apposta, per cui tale documento acquista validità legale.

Essa **si basa sull'uso di una coppia di chiavi digitali asimmetriche**, assegnate in modo univoco a ogni utente. La chiave privata serve al titolare per generare la firma da apporre a un documento, quella pubblica viene usata dal destinatario per controllare l'autenticità della firma.

Meccanismi di autenticazione

In estrema sintesi, i **meccanismi di autenticazione** possono essere distinti in tre tipologie che si basano su:

- **conoscenza**, per esempio l'utente conosce la **password** per accedere a un servizio Web based;
- **possesso**, per esempio l'utente possiede la **chiavetta** fornita dal proprio Istituto di credito che genera password monouso per le transazioni monetarie online;
- **caratteristiche fisiche**, per esempio l'utente usa l'**impronta digitale** (riconoscimento biometrico) come "codice" per l'accesso alla sala server.

La scelta migliore, quando possibile, è data dall'utilizzo combinato delle tre tipologie, nella consapevolezza che ognuna di esse ha i suoi vantaggi e svantaggi.