IT Security

Presentazione

L'IT Security è uno dei moduli necessari per il conseguimento dell'ECDL Full Standard.

Il modulo tratta i problemi della sicurezza dei sistemi informatici sia a livello personale che a livello aziendale.

In particolare vengono analizzati i seguenti temi:

Valore dei dati e delle informazioni e loro sicurezza.
Tipi di malware e relativi pericoli.
Sicurezza delle reti di trasmissione dei dati.
Controllo degli accessi alle banche dati, ai servizi e alle reti di comunicazione.
Uso sicuro dei servizi World Wide Web.
Sicurezza nelle comunicazioni.
Gestione sicura dei dati.

La numerazione usata nel testo e gli argomenti trattati sono quelli del Syllabus Versione 2.0, rilasciato dall'AICA nel settembre 2015.

Per facilitare la ricerca all'interno del testo sono stati inseriti alcuni collegamenti ipertestuali e delle intestazioni.

Il testo è suddiviso in sette lezioni, il cui indice si trova nella pagina successiva a questa. Ogni voce dell'indice è un collegamento ipertestuale alla pagina iniziale di ogni lezione.

Ogni lezione inizia con i titoli dei temi e degli argomenti trattati. L'indicazione numerica posta tra parentesi è il riferimento usato nel Syllabus, ed è un collegamento ipertestuale alla pagina relativa.

Oltre questo file, che contiene tutto il materiale relativo a questo modulo, ce n'è un altro che contiene la copertina e le informazioni di copyright.

Indice delle lezioni

Lezione 1
1 Concetti di sicurezza

*In questa lezione si imparerà a capire quali sono le **Minacce ai dati (1.1)**, cioè a distinguere tra dati e informazioni (1.1.1), a comprendere i termini "crimine informatico" e "hacking" (1.1.2), a riconoscere le minacce dolose e accidentali ai dati provocate da singoli individui, fornitori di servizi, organizzazioni esterne (1.1.3), a riconoscere le minacce ai dati provocate da circostanze straordinarie, quali fuoco, inondazioni, guerre, terremoti (1.1.4), a riconoscere le minacce ai dati provocate dall'uso del cloud computing, quali: controllo sui dati, potenziale perdita di riservatezza (privacy) (1.1.5), a capire il **Valore delle informazioni (1.2)**, cioè a comprendere le caratteristiche fondamentali della sicurezza delle informazioni, quali: confidenzialità, integrità, disponibilità (1.2.1), a comprendere i motivi per proteggere le informazioni personali, quali evitare il furto di identità o le frodi, mantenere la riservatezza (1.2.2), a comprendere i motivi per proteggere informazioni di lavoro su computer e dispositivi mobili, quali: evitare furti, utilizzi fraudolenti, perdite accidentali di dati, sabotaggi (1.2.3), a identificare i principi comuni per la protezione, conservazione e controllo dei dati e della riservatezza, quali: trasparenza, scopi legittimi, proporzionalità delle misure in rapporto ai danni (1.2.4), a comprendere i termini "soggetti dei dati" e "controllori dei dati", e come si applicano nei due casi i principi di protezione, conservazione e controllo dei dati e della riservatezza (1.2.5), a comprendere l'importanza di attenersi alle linee guida e alle politiche per l'uso dell'ICT e come fare per ottenerle (1.2.6), a comprendere la **Sicurezza personale (1.3)**, cioè a comprendere il termine "ingegneria sociale" e le sue implicazioni, quali accesso non autorizzato a sistemi informatici, raccolta non autorizzata di informazioni, frodi (1.3.1), a identificare i metodi applicati dall'ingegneria sociale, quali chiamate telefoniche, phishing, shoulder surfing (spiare alle spalle), al fine di carpire informazioni personali (1.3.2), a comprendere il termine "furto di identità" e le sue implicazioni personali, finanziarie, lavorative, legali (1.3.3), a identificare i metodi applicati per il furto di identità, quali acquisire informazioni a partire da oggetti e informazioni scartati (information diving), uso di dispositivi fraudolenti di lettura (skimming), inventare uno scenario pretestuoso (pretexting) (1.3.4), a comprendere la **Sicurezza dei file (1.4)**, cioè a comprendere gli effetti di attivare/disattivare le impostazioni di sicurezza relative alle macro (1.4.1), a comprendere i vantaggi e i limiti della cifratura, comprendere l'importanza di non divulgare o di non perdere la password, la chiave o il certificato di cifratura (1.4.2), a cifrare un file, una cartella, una unità disco (1.4.3), a impostare una password per file quali: documenti, fogli di calcolo, file compressi (1.4.4).*

1.1 Minacce ai dati

1.1.1 Distinguere tra dati e informazioni.

I termini dato e informazione sono spesso utilizzati come sinonimi, ma i due termini hanno significati diversi.
Per dato si intende una rappresentazione originaria e non interpretata di un evento, di un fatto o di un oggetto. Dato può essere quindi la rappresentazione del nome di una azienda, del prezzo di un prodotto, del cognome di un dipendente, della data di nascita di una persona.
L'informazione è l'insieme di uno o più dati, opportunamente correlati ed interpretati in un certo contesto. Uno o più dati vengono, quindi, trasformati in una o più informazioni mediante un processo elaborativo. L'elaborazione può essere fatta manualmente o con l'uso di computer. L'informazione può anche derivare da un singolo dato, ad esempio il dato 23/12/2015 diventa una informazione se sai che rappresenta la data di una fattura o il giorno di nascita di una persona.
Per analogia con il processo produttivo, si può dire che i dati costituiscono la materia prima con la quale vengono costruite le informazioni.

E’ inoltre importante osservare che un’informazione è tale soltanto in funzione del suo destinatario e del momento e del luogo del suo utilizzo. Ad esempio il totale di una fattura è un’informazione per l’Ufficio Fatturazione, ma è un dato per l’Ufficio Marketing interessato ad elaborazioni di tipo statistico.
In questo contesto il dato possiede come caratteristica fondamentale quella dell’oggettività, mentre l’informazione è soggettiva, in quanto destinata ad un certo utente, in un determinato momento, per un certo scopo.
Dati e informazioni sono rappresentati da numeri, testi, immagini, suoni.

1.1.2 Comprendere i termini “crimine informatico” e “hacking”.

Il crimine informatico è una azione illecita fatta con l’uso di strumenti informatici, hardware e software.
Molti sono i tipi di crimini informatici:
frodi informatiche, realizzate modificando a proprio vantaggio i processi di elaborazione;
intercettazione di dati:
sabotaggio, danneggiamento, cancellazione, alterazione di dati e di programmi;
accessi illegali e non autorizzati a sistemi informatici;
utilizzo non autorizzato di sistemi informatici e di reti di trasmissione dati;
utilizzo, riproduzione e commercio non autorizzati di programmi protetti;
furto d’identità:
furto di informazioni;
documenti informatici falsi;
spionaggio industriale;
commercio di codici d’accesso avuti in modo illegale;
diffusione di malware.
Alcuni di questi argomenti verranno approfonditi in seguito.
Spesso, chi compie crimini informatici viene chiamato hacker, o pirata informatico. Il termine hacker è sbagliato.
In modo corretto, hacker è un esperto informatico che usa tecniche di hacking per accedere, conoscere e modificare sistemi informatici hardware e software in modo legittimo.
Spesso le operazioni hanno lo scopo di verificare i sistemi informatici e le reti telematiche, per impedirne l’accesso fraudolento. Questi tipi di operazioni rientrano nella categoria dell’hacking etico. L’hacker etico è anche chiamato white hat hacker (hacker con il cappello bianco).
Colui che accede ai sistemi informatici in modo illegittimo, per trarne vantaggio, viene chiamato cracker, o anche black hat hacker (hacker con il cappello nero).
La repressione dei crimini informatici in Italia è compito della Polizia Postale.

1.1.3 Riconoscere le minacce dolose e accidentali ai dati provocate da singoli individui, fornitori di servizi, organizzazioni esterne.

Internet è sempre più usata non solo per cercare informazioni ma anche per la grande quantità di servizi disponibili.
Molti di questi servizi prevedono la comunicazione di dati riservati. Ne sono un esempio le operazioni fatte con la propria banca (e-banking), o l’acquisto di beni e servizi (e-commerce), nelle quali si effettuano pagamenti in modo elettronico (ad esempio con la carta di credito).
Tutte queste operazioni prevedono di inviare al sito, che gestisce il servizio, dati importanti per autorizzare i pagamenti (come ad esempio i dati della propria carta di credito o i dati riservati per fare un addebito sul proprio conto corrente).
Per questi tipi di operazioni sono usate misure di sicurezza sempre più sofisticate, in modo da garantire che i dati rimangano riservati e non possano venire usati in modo fraudolento.

Ma contemporaneamente all'evoluzione dei sistemi di sicurezza anche le tecniche usate per venire a conoscenza dei dati riservati diventano sempre più sofisticate ed efficaci.
Il livello di sicurezza usato dipende dai danni che può causare un accesso non autorizzato ai dati sensibili.
L'uso del codice utente e della password come credenziali di accesso offrono un livello di protezione basso; puoi usarli per proteggere dati sensibili non importanti. Le credenziali di accesso devono essere in ogni caso protette. Devi evitare di essere visto quando inserisci tali dati dalla tastiera e proteggerli da eventuali furti. Inoltre non lasciare il tuo computer incustodito; proteggi il computer e fai in modo che si disattivi automaticamente in caso di tua assenza.
Puoi avere un maggiore livello di protezione sostituendo alla digitazione del tuo codice utente l'uso di una carta a microchip come tessera di riconoscimento personale (come viene fatto ad esempio per il Bancomat).
Le minacce dolose possono provenire anche da siti, fornitori di servizi. Accedi e usa solo dati e servizi di organizzazioni note, e evita di scaricare programmi e archivi di cui non conosci la provenienza.
Non tutti i pericoli arrivano da Internet.
Nelle aziende gli attacchi possono provenire dall'ambiente interno, sia dai dipendenti sia da persone esterne che frequentano l'azienda o che hanno accesso a dati riservati del sistema informativo aziendale. Infatti, spesso la manutenzione dei sistemi informatici e dei programmi applicativi è affidata ad aziende esterne che operano con propri dipendenti.
Anche le reti senza fili non protette sono un facile punto di accesso per personal computer portatili, tablet e smartphone.
I dipendenti possono essere una minaccia ai dati aziendali, sia involontariamente sia in modo fraudolento.
Queste operazioni possono portare gravi danni all'azienda, di tipo finanziario, commerciale e industriale.
Inoltre, l'azienda è responsabile della protezione dei dati di clienti, fornitori, in base alla legge sulla privacy.
La violazione del sistema informativo aziendale è anche un grande rischio per la reputazione dell'azienda.

1.1.4 Riconoscere le minacce ai dati provocate da circostanze straordinarie, quali fuoco, inondazioni, guerre, terremoti.

Per evitare la perdita di dati fai periodicamente il backup, ossia la copia degli archivi, in modo da poter ripristinare i dati nel caso di loro danneggiamento.
Come protezione a fronte di eventi straordinari come incendi, inondazioni, atti terroristici, terremoti o guerre, le copie di backup devono essere conservate in luoghi lontani dagli archivi originali, in modo che non vengano coinvolte nell'evento.
Le copie possono essere fatte con la trasmissione via rete a sistemi informatici che forniscono questi tipi di servizi.
Il livello massimo di sicurezza, nelle aziende di grandi dimensioni, viene raggiunto con la realizzazione di sistemi di disaster recovery, in grado di garantire la ripartenza del sistema informativo in tempi brevi, anche nel caso di distruzione del sistema informatico a causa di grandi eventi catastrofici.
Con il disaster recovery i dati e i sistemi fondamentali dell'azienda vengono riprodotti in un sito secondario, lontano dal sito principale. In caso di blocco del sito principale, il servizio viene gestito dal sito secondario.
L'uso di questa soluzione ha costi molto elevati, poiché deve essere riprodotta tutta la struttura di elaborazione ritenuta indispensabile: hardware, software, reti telematiche, banche dati aggiornate.

1.1.5 Riconoscere le minacce ai dati provocate dall'uso del cloud computing, quali: controllo sui dati, potenziale perdita di riservatezza (privacy).

Il cloud computing (in italiano nuvola informatica) è un modello di utilizzo di risorse informatiche, rese disponibili via Internet in base alle esigenze del momento.
Le risorse di elaborazione, archiviazione e trasmissione dati sono assegnate all'utente dinamicamente e in modo automatico in base alle sue richieste. Quando una risorsa viene rilasciata da un utente diventa disponibile per un altro utente.
Il cloud computing espone gli utenti ad alcuni rischi legali.
Nel caso di registrazione di dati personali sensibili, nascono potenziali problemi di violazione della privacy. I dati sono memorizzati nei sistemi informatici dell'azienda che fornisce il servizio, azienda che può trovarsi in una nazione diversa da quella dell'utente. Il fornitore del servizio può comportarsi in modo scorretto e usare i dati personali per propri fini, diversi da quelli dichiarati dall'azienda che usa il servizio e che ha raccolto i dati. I pericoli aumentano nel caso di collegamenti con reti senza fili. Nel caso di violazione delle leggi sulla privacy, se fornitore e utente del servizio si trovano in nazioni diverse, ciò diventa una complicazione per raggiungere un accordo in campo legale. Le due nazioni possono avere leggi diverse.
Per i dati aziendali c'è il pericolo di spionaggio industriale.
Ulteriori problemi si hanno quando dati pubblici sono registrati in archivi privati. Possono venir meno le garanzie sulla disponibilità di questi dati anche per il futuro.
Il passaggio da un fornitore del servizio ad un altro può comportare problemi e costi elevati, in quanto non esistono standard comuni tra i possibili fornitori.

1.2. Valore delle informazioni

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

Per quanto riguarda la sicurezza, le informazioni devono avere tre caratteristiche fondamentali: la confidenzialità (riservatezza), l'integrità e la disponibilità.
La confidenzialità deve garantire che l'informazione sia disponibile solo agli utenti autorizzati.
L'integrità deve garantire che le informazioni non possano essere modificate o aggiornate se non da operazioni autorizzate.
La disponibilità deve garantire che le informazioni siano a disposizione delle persone autorizzate quando servono.

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

La protezione dei dati personali è necessaria per evitare che questi vengano utilizzati da altri in modo illegale, e ne venga compromessa la riservatezza.
L'accesso a servizi riservati con l'uso non autorizzato delle credenziali (codice utente e password) di un altro utente costituisce un furto di identità.
Le conseguenze per l'utente vittima del furto possono essere di varia natura: economiche se il furto di identità è usato per effettuare operazioni di pagamento o trasferimento di soldi, ma anche di immagine e reputazione se vengono usati servizi come la posta elettronica o le reti sociali. Ma le conseguenze possono essere anche più gravi nel caso di truffe o di atti di natura criminale che vengono addebitati al legittimo proprietario dei dati, che ha subito il furto.
Tramite le reti, ed in particolare con Internet, possono essere tentate frodi. Come difesa, in questo caso, verifica sempre che le richieste (di informazioni, di effettuare operazioni, eccetera) arrivino da interlocutori a te noti (se tramite posta elettronica) o da siti web garantiti.

1.2.3 Comprendere i motivi per proteggere informazioni di lavoro su computer e dispositivi mobili, quali: evitare furti, utilizzi fraudolenti, perdite accidentali di dati, sabotaggi.

Il furto d'identità è un problema per il singolo utente ma soprattutto per le aziende. A livello privato essere consapevoli del problema e porre attenzione alle soluzioni di protezione necessarie può essere sufficiente per evitare conseguenze.
Nelle aziende il problema è aggravato dal numero di utenti coinvolti, dalla quantità e qualità di dati riservati, dall'elevato numero di programmi usati e dall'elevato livello di integrazione. Il furto di identità di un solo utente può recare danni gravissimi all'intero sistema informativo aziendale.
Per le aziende è necessario impostare e usare dei piani per la sicurezza. Nei piani particolare attenzione deve essere data ai dispositivi mobili, che possono essere facilmente rubati o smarriti.
Per limitare usi fraudolenti o sabotaggi, o anche perdite accidentali di dati, ogni dipendente deve essere abilitato solo alla parte del sistema informativo che è necessaria in funzione delle attività svolte.

1.2.4 Identificare i principi comuni per la protezione, conservazione e controllo dei dati e della riservatezza, quali: trasparenza, scopi legittimi, proporzionalità delle misure in rapporto ai danni.

I sistemi informativi aziendali gestiscono anche dati esterni di clienti e fornitori.
Credo che ormai il concetto di privacy sia noto a tutti; tutte le volte che ti vengono chiesti dati personali ti viene richiesta una autorizzazione al loro utilizzo, di cui sono specificati obiettivi e modalità. In definitiva per privacy possiamo intendere il diritto di una persona di controllare che le informazioni che la riguardano vengano gestite e viste solo per gli scopi che sono stati dichiarati al momento della richiesta di autorizzazione, ma anche il diritto di verificare che ciò avvenga.
Tutto questo sta diventando sempre più importante anche a fronte degli sviluppi delle tecnologie informatiche e telematiche, di cui sono un esempio la tracciabilità dei telefoni cellulari o la facilità con cui vengono reperiti gli indirizzi di posta elettronica e le conseguenti attività di spam.
Le leggi, che sono state promulgate a livello internazionale, hanno l'obiettivo di evitare che l'integrazione di banche dati digitali, di natura diversa, consentano di creare informazioni che violano la riservatezza delle persone fisiche e giuridiche, in particolare per quanto riguarda dati sensibili (come ad esempio quelli che riguardano la salute).
Tali leggi regolano i diritti dei proprietari dei dati personali, le modalità con cui vengono raccolti i dati e come ne viene garantita la riservatezza, i doveri e le responsabilità dei gestori delle banche dati.
In Italia è attualmente in vigore il Decreto Legislativo n. 196/2003, Codice in materia di protezione dei dati personali.
Con il termine dato personale si indica qualsiasi informazione riguardante persona fisica o giuridica, azienda, ente o associazione. Alla base di tutte queste leggi ci sono tre principi fondamentali: la trasparenza, la legittimità degli scopi e la proporzionalità delle misure in rapporto ai possibili danni.
Per quanto riguarda la trasparenza, la raccolta di dati deve essere nota e espressamente dichiarata, ne devono essere indicati gli obiettivi, devono essere dichiarate le procedure per eventuali verifiche e contestazioni.
Per la legittimità, i dati non devono violare i diritti del soggetto dei dati.
Infine, in merito alla proporzionalità, i dati raccolti devono essere solo quelli necessari per rispondere agli obiettivi per cui sono raccolti.

1.2.5 Comprendere i termini “soggetti dei dati” e “controllori dei dati”, e come si applicano nei due casi i principi di protezione, conservazione e controllo dei dati e della riservatezza.

La legge prevede obblighi precisi per chi tratta dati personali. Innanzitutto deve darne comunicazione al Garante della privacy. Nella legge, è indicato come soggetto dei dati la persona o l’organizzazione a cui i dati si riferiscono. Per quanto riguarda la responsabilità sono previste due figure professionali: il titolare, cioè colui che stabilisce gli obiettivi e le modalità della gestione dei dati, e il responsabile che, su incarico del titolare, ne realizza le direttive.
Gli adempimenti sono indicati nella legge: definizione dei dati raccolti, individuazione del titolare e del responsabile, notifica al Garante, richiesta di autorizzazione scritta o orale al soggetto dei dati.
I dati personali oggetto di trattamento devono essere raccolti e trattati secondo gli scopi dichiarati nella richiesta di consenso, corretti e se necessario aggiornati, conservati solo per il periodo necessario, protetti da accessi non autorizzati.

1.2.6 Comprendere l’importanza di attenersi alle linee guida e alle politiche per l’uso dell’ICT e come fare per ottenerle.

E’ già stato detto che, a fronte della complessità dei sistemi informativi aziendali, devono essere predisposti dei piani per la sicurezza, ossia delle linee guida che hanno come obiettivo di spiegare perché è necessario proteggere tutti gli strumenti informatici e cosa si deve fare per mettere in pratica le politiche di protezione.
Proteggere un sistema informatico significa difendere le sue risorse dall'uso non autorizzato e salvaguardare le banche dati da letture o manipolazioni non autorizzate, accidentali (non dolose) o volontarie (dolose).
Un sistema è sicuro quando garantisce la disponibilità del servizio, la riservatezza dei dati e l’integrità delle informazioni.
Per raggiungere questi obiettivi servono delle politiche per la sicurezza (cosa deve essere fatto, ossia le modalità di gestione di tutti gli strumenti informatici) e dei meccanismi per la sicurezza (come deve essere fatto).
Le indicazioni riguardano la prevenzione (come realizzare le difese), il controllo (verifica continua del sistema di sicurezza e eventuali interventi correttivi) e il ripristino (come rendere operativi dati e servizi, dopo un aver subito un attacco).
Le linee guida devono essere conosciute e adottate da tutto il personale, devono essere facilmente consultabili con l’intranet aziendale. E’ sufficiente la presenza di un punto vulnerabile per mettere in crisi l’intero sistema informativo aziendale.

1.3 Sicurezza personale

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

L'ingegneria sociale (in inglese social engineering) si occupa delle tecniche che permettono di venire a conoscenza di dati sensibili (ad esempio le credenziali di accesso a servizi riservati) e di effettuare frodi, studiando il comportamento delle persone.
Queste tecniche si basano sullo studio sociologico dei rapporti interpersonali e sfruttano spesso l’ingenuità e la buona fede delle persone.
Normalmente chi svolge l’attività di ingegneria sociale prepara l’attacco (l’azione criminosa), raccogliendo informazioni sulla vittima, informazioni del tipo indirizzo di posta elettronica, numeri di telefono, dati personali, abitudini, eccetera.

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

L'ingegneria sociale usa vari metodi.
Con le chiamate telefoniche, spesso si finge di fare un sondaggio e ti vengono chiesti dati di tipo personale. Spesso sei allettato con la promessa di premi.
Una tecnica molto usata è quella del phishing, una truffa via Internet volta ad accedere ad informazioni personali sensibili. Tale truffa può essere realizzata anche con contatti telefonici o con SMS.
Il truffatore invia a caso messaggi, imitando la grafica di siti noti, quali la tua banca, le poste, altri siti che prevedono accesso protetto. Questi messaggi normalmente dichiarano che sono scadute le tue credenziali, identificativo utente e password, e ti chiedono di collegarti ad un indirizzo inserito nel messaggio; fai attenzione si tratta di tecniche per catturare i tuoi dati di accesso.
Il termine è una variazione di fishing (pescare), e la tecnica può essere assimilata a quella della pesca con le reti, nella quale stendo la rete e poi verifico cosa ho pescato; nel phishing il pirata informatico invia una grande quantità di messaggi e poi verifica quanti utenti sono stati tratti in inganno.
I messaggi inviati segnalano quasi sempre problemi che riguardano situazioni anomale del tuo conto corrente o utenze scadute, e contengono un link al quale collegarti per risolvere il problema. Il link porta ad un sito gestito dal truffatore, e in fase di collegamento vengono ad esempio chiesti i tuoi dati di identificazione (utenza e password) per l'accesso, o anche di confermare tali dati. Per rendere maggiormente credibile il messaggio, spesso il nome del sito a cui collegarsi è molto simile a quello dell'azienda, da cui differisce per l'omissione o l'inserimento di un carattere o la trasposizione di due caratteri. Se attivi il collegamento e inserisci le informazioni richieste, il truffatore entra in possesso delle tue credenziali per effettuare operazioni fraudolente come acquisti o trasferimenti di denaro. Se ricevi tale tipo di attacco, invia una copia del messaggio alle autorità competenti e alla banca o all'organizzazione interessata, in modo che possano identificare e bloccare il sito da cui proviene l'attacco truffaldino. Per sicurezza puoi verificare se la segnalazione dei problemi è corretta, controllando il tuo conto o effettuando l'accesso alla tua utenza.
In altri casi la comunicazione riguarda opportunità di lavoro o proposte di investimenti finanziari a condizioni molto vantaggiose. Ti possono essere anche richieste le coordinate bancarie del tuo conto per ricevere denaro da trasferire in un conto estero, trattenendone una percentuale significativa a titolo di commissione; in questo caso si tratta di riciclaggio di denaro sporco, che costituisce un reato penale. Quando si verificano queste situazioni, contatta subito la tua banca in modo che venga cancellata l'operazione di accredito.
Una tecnica semplice e che non ha come presupposto l'uso di strumenti sofisticati è il shoulder surfing (fare surf sulla spalla), cioè spiare sopra la tua spalla mentre inserisci nome utente e password in un computer, in un dispositivo mobile (tablet, smartphone), in una postazione Bancomat, in un sistema di pagamento. Per rendere più difficile questa tecnica, quando digiti la password i caratteri digitati sulla tastiera sono sostituiti sullo schermo da una serie di asterischi.
Per carpire informazioni si può anche fare amicizia con la vittima o spacciarsi per un tecnico in grado di intervenire per correggere errori inesistenti del computer o dispositivo mobile dove sono registrate le informazioni riservate.

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

E' già stato detto che il furto d'identità consiste nell'usare senza autorizzazione le credenziali di accesso di un altro utente. L'utente che effettua il furto si spaccia per l'utente che ha subito il furto.
Come è già stato detto, i pericoli del furto d'identità sono molti.

Le credenziali rubate possono essere usate per accedere a sistemi di pagamento; in questo caso la vittima del furto può subire danni di tipo economico (perdite di denaro) nel trasferimento di moneta elettronica, e nel pagamento di acquisti.
Se l'identità rubata viene utilizzata per la posta elettronica e nelle reti sociali, ne possono derivare perdite di immagine e di credibilità, in quanto con la falsa identità vengono trasmessi pensieri, informazioni, dichiarazioni e fatti che non corrispondono alla realtà e al modo di pensare della persona che ha subito il furto.
Messaggi di posta elettronica inviati da falsi utenti possono creare problemi anche nelle attività lavorative.
Queste operazioni possono essere fatte con il preciso scopo di screditare la persona fisica vittima del furto.
In particolare, nelle reti sociali le tutele sulla riproduzione dei dati personali sono scarse, in modo molto facile altri utenti possono riprodurre i dati personali pubblicati nel tuo profilo, incluse le fotografie personali che ti identificano. In molti casi il furto di identità diventa un'azione di cyberbullismo, cioè di bullismo fatto tramite la rete.
Il furto d'identità usato per attuare truffe e altre azioni criminali può creare notevoli problemi di natura legale.

1.3.4 Identificare i metodi applicati per il furto di identità, quali acquisire informazioni a partire da oggetti e informazioni scartati (information diving); uso di dispositivi fraudolenti di lettura (skimming); inventare uno scenario pretestuoso (pretexting).

Per rubare l'identità possono essere usati vari metodi.
Abbiamo già analizzato il phishing, il trashing.
Un altro sistema molto semplice consiste nel rovistare nella spazzatura (dumster diving, o information diving o trashing), alla ricerca di foglietti di appunti, scontrini, ricevute, fatture, estratti conto, lettere, ma anche giornali e riviste che possono aiutare nel ricostruire le abitudini della vittima. Ad esempio il truffatore può conoscere i dati della tua carta di credito recuperando gli scontrini di acquisto.
Un'altra tecnica è lo skimming: che consiste nel copiare, fotografare o filmare documenti nei quali sono presenti i dati (ad esempio la carta di credito, la tessera Bancomat, ma anche il PIN del Bancomat). Sono usate videocamere nascoste, poste in modo da riprendere la tastiera della postazione self-service. Ad esempio, nel prelievo di denaro da un terminale Bancomat, un dispositivo installato dal ladro legge i dati dalla carta a microchip e una telecamera o un dispositivo collegato alla tastiera leggono il PIN digitato.
Con la tecnica del pretexting si usa uno scenario inventato (il pretesto) per indurre la vittima a dare le informazioni volute. Nel pretexting, fatto spesso telefonicamente, il truffatore finge di essere un rappresentante della banca, un poliziotto o un agente assicurativo per guadagnare la tua fiducia e indurti a fornire le informazioni volute.

1.4 Sicurezza dei file

1.4.1 Comprendere gli effetti di attivare/disattivare le impostazioni di sicurezza relative alle macro.

Una macro è un insieme di istruzioni, che possono essere eseguite all'interno di un programma, come ad esempio in uno dei programmi di Office (elaborazione testi, foglio di calcolo, eccetera).
Le macro sono utili perché ti aiutano nell'uso del programma, evitandoti di inserire più volte tutte le operazioni che sono contenute nelle macro.

Le macro possono essere eseguite in modo automatico o premendo una combinazione di tasti della tastiera.
Ma le macro possono essere pericolose perché possono essere un codice malevolo, che può danneggiare il computer in modo automatico o all'esecuzione di particolari operazioni.
Se attivi il giusto livello di sicurezza, i programmi che hanno macro al loro interno sono in grado di segnalarne la presenza all'avviamento del programma. Se sei certo dell'origine delle macro puoi autorizzarne l'esecuzione, in caso contrario puoi disattivare le macro.
In questo caso rinunci alle funzionalità delle macro, ma metti in sicurezza il computer.

1.4.2 Comprendere i vantaggi e i limiti della cifratura. Comprendere l'importanza di non divulgare o di non perdere la password, la chiave o il certificato di cifratura.

In campo militare si è sempre sentita l'esigenza di proteggere i messaggi trasmessi, in modo da renderli illeggibili per il nemico. Nella storia si conoscono sistemi di mascheramento dei messaggi usati dagli Ebrei, dagli Spartani e da Giulio Cesare che dalla Gallia rimaneva in contatto con i suoi alleati per preparare il suo ritorno a Roma.
La crittografia è la cifratura del messaggio, ossia la sua trasformazione in modo che diventi incomprensibile per chi non conosce le regole per tornare al messaggio originale. Il termine deriva dalle parole greche che corrispondono a: " nascosto" e "scrittura".
Con lo sviluppo di Internet e delle comunicazioni ad essa associate, e i problemi di sicurezza, di cui abbiamo appena parlato, la crittografia è diventata un argomento di grande interesse.
Un sistema molto semplice, ad esempio, consiste nella sostituzione di ogni lettera dell'alfabeto con un'altra corrispondente. Utilizzando un'apposita tabella di codifica per crittografare il messaggio e la stessa tabella per decrittarlo, si ottiene lo scopo. Questo sistema è facilmente individuabile in quanto ogni lingua presenta delle regolarità e delle frequenze di utilizzo delle lettere dell'alfabeto; ad esempio in italiano la lettera che compare con maggiore frequenza è la E, per cui se il messaggio è abbastanza lungo basta cercare la lettera che compare più volte e sostituirla con la E. Analogamente si può fare per diverse altre lettere, per cui questo sistema di crittografia è assai poco sicuro.
In genere si può dire che ogni sistema crittografico ha due elementi base: un algoritmo di codifica, che è l'insieme delle regole per passare dal messaggio in chiaro a quello criptato, e una chiave, che viene usata dall'algoritmo per criptare e poi per decriptare il messaggio stesso.
Per interpretare il messaggio occorre conoscere sia l'algoritmo che la chiave.
La sicurezza di un sistema di crittografia dipende dalla facilità con cui un malintenzionato può riuscire a decifrarlo. Se si fa uso di un algoritmo troppo semplice e di una chiave di lunghezza limitata, si sarà costretti a ripetere dei caratteri o delle sequenze di caratteri nel messaggio criptato: questo potrebbe fornire uno schema a chi cerca di interpretare il messaggio.
Altro fattore di sicurezza è il numero di chiavi che l'algoritmo ammette: se la chiave ha dimensioni ridotte si potrebbe pensare che con i moderni computer una persona che non conosca la chiave potrebbe in un tempo accettabile provarle tutte fino a trovare quella voluta (utilizzando l'approccio cosiddetto della "forza bruta" (brute force attack), basato non sull'intelligenza, ma solamente sulla velocità con cui si possono fare i tentativi). Con questo metodo occorre usare sistemi informatici potenti, in quanto le risorse informatiche necessarie aumentano in modo esponenziale con la lunghezza della password.
I primi sistemi di crittografia, adottati in campo informatico e telematico, erano basati su un sistema simmetrico, a chiave segreta. Questi sistemi prevedono l'utilizzo della stessa chiave per criptare e decriptare i messaggi. La chiave deve pertanto rimanere segreta, conosciuta solo ai due interlocutori che si scambiano il messaggio criptato. Questa soluzione presenta due svantaggi. Da un lato il proliferare di chiavi dovuto al fatto che deve essere generata una chiave per ogni coppia di interlocutori, dall'altro la vulnerabilità del sistema dovuta alla fase di comunicazione della chiave, durante la quale la chiave potrebbe essere intercettata.

La soluzione consiste nell'adozione di un sistema asimmetrico, a chiavi pubbliche, che prevede siano utilizzate due chiavi diverse per crittare e decriptare. La prima, chiave pubblica, è di pubblico dominio, in quanto inserita in cataloghi consultabili in Internet, la seconda, chiave privata, è conosciuta solo dal suo proprietario. Un messaggio criptato con una delle due chiavi, può essere decriptato solo con la seconda chiave.
La crittografia asimmetrica può quindi essere utilizzata sia come protezione della segretezza che per individuare con sicurezza l'autore del messaggio.
Come abbiamo detto, ogni utente possiede due chiavi: una pubblica e una privata.
Per proteggere la trasmissione di un messaggio, il mittente cripta il messaggio con la chiave pubblica del destinatario. Solo il destinatario, che possiede la corrispondente chiave privata, può decodificare il messaggio. La cifratura rende molto difficile decifrare il messaggio anche nel caso di intercettazione.
Nel caso di cifratura di un proprio file, il proprietario possiede entrambe le chiavi per cifrare e decifrare il messaggio. Anche in questo caso è possibile aprire e leggere il file solo se si è in possesso della chiave necessaria. I file rimangono protetti anche nel caso di furto del computer o del dispositivo mobile.
Un problema della crittografia asimmetrica è che entrambi i processi sono caratterizzati da elaborazioni complesse e quindi comportano tempi lunghi quando si devono trattare grandi quantità di dati. Quando il problema è quello della segretezza si ricorre all'uso del sistema simmetrico, molto più veloce, avendo però cura che la trasmissione della chiave venga criptata con il sistema asimmetrico, che ne garantisce la segretezza.
Quando la cifratura viene fatta su iniziativa dell'utente, che ne definisce la chiave, se si dimentica la chiave il file non può più essere usato, è quindi necessario proteggere la chiave ma anche non perderla.
La coppia di chiavi viene rilasciata da una Autorità di Certificazione, che invia al richiedente un Certificato elettronico. Sia la chiave segreta che il certificato devono essere protetti, valgono in questo caso tutte le regole che si applicano per la protezione delle password.

1.4.3 Cifrare un file, una cartella, una unità disco.

Windows dà la possibilità di crittografare un file, una cartella o un intero disco.
Per effettuare l'operazione, apri il menu "Start" con il tasto WINDOWS o con i tasti CRTL + ESC.
Con il tasto TAB spostati nel riquadro di destra e con FRECCIA GIU' seleziona "Computer" e premi il tasto INVIO.
Si apre la finestra "Esplora risorse" ed è selezionata la voce "Computer".
Se vuoi usare un'altra voce del menu di sinistra ("Preferiti", "Raccolte", eccetera) premi il tasto TAB o MAIUSC + TAB sino a spostare la selezione nel riquadro di sinistra, e con le frecce sulla voce che desideri.
Premi il tasto TAB e la selezione è spostata nel riquadro di destra.
Procedi nello sfogliare le risorse del computer.
Usa le frecce per selezionare la cartella o il file che vuoi cifrare.
Apri il menu contestuale con i tasti MAIUSC + F10 o APPLICAZIONI.
Nel menu contestuale spostati con FRECCIA GIU' sino a "Proprietà".
Premi il tasto INVIO.
Nella finestra "Proprietà" è aperta la scheda "Generale".
Con FRECCIA GIU' seleziona "Avanzate" e premi INVIO.
Nella finestra "Attributi avanzati" usa il tasto TAB per selezionare la casella di controllo "Crittografa contenuto per la protezione dei dati" e premi il tasto SPAZIO.
Nella finestra "Proprietà" premi TAB sino a selezionare il pulsante OK e premi INVIO.
Nella finestra "Conferma cambiamenti attributi" seleziona con TAB il pulsante OK e premi INVIO.

Le versioni di Windows più recenti hanno la funzione BitLocker Drive Encryption, che permette di crittografare l'intero disco. Per usare la funzione nel "Pannello di controllo", seleziona la categoria "Sistema e sicurezza" e "Crittografia unità BitLocker". Il sistema apre una finestra di dialogo che ti permette di scegliere le unità su cui puoi attivare la funzione. Seleziona "Attiva BitLocker" e il sistema avvia la procedura guidata che ti chiede la password di cifratura e come salvare la chiave, per recuperare il contenuto dell'unità se ti dimenticassi la password.

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

Puoi proteggere un file da accessi non autorizzati con l'uso una password, che il sistema richiede nella fase di apertura. Solo chi conosce la password può leggere e modificare il file.
Ad esempio, usando un'applicazione Office come Word, Excel o PowerPoint 2010:
Apri il documento che vuoi proteggere.
Premi i tasti ALT + F della tastiera.
Nel menu "File", con le frecce seleziona "Informazioni" e premi INVIO.
Con TAB seleziona il pulsante "Proteggi documento" e premi INVIO.
Nel menu a discesa, con FRECCIA GIU' seleziona "Crittografa con Password" e premi INVIO.
Si apre la finestra "Crittografa con password" ed è selezionata la casella "Password".
Digita la password e premi INVIO.
Conferma la password e premi INVIO.
Il documento è protetto.
Per creare un file compresso protetto da password puoi usare il programma WinRAR:
Seleziona il file o la cartella da comprimere.
Premi i tasti MAIUSC + F10 o APPLICAZIONI per aprire il menu contestuale.
Nel menu seleziona "Aggiungi a un archivio".
Si apre una finestra che permette di scegliere il formato di compressione, la cartella di salvataggio, eccetera.
Con TAB seleziona la scheda "Avanzate" e con le frecce seleziona "Parola chiave".
Digita la password e confermala nella finestra successiva.
Seleziona il pulsante OK e dai INVIO.
Nella finestra principale seleziona OK e dai INVIO.
Ora hai un file protetto da password, che deve essere usata per visualizzare il contenuto.

Lezione 2
2 Malware

*In questa lezione si imparerà a capire quali sono i **Tipi e metodi del malware (2.1)**, cioè a comprendere il termine "malware", riconoscere diversi modi con cui il malware si può nascondere nei computer, quali: trojan, rootkit e backdoor (2.1.1), a riconoscere i tipi di malware infettivo e comprendere come funzionano, ad esempio virus e worm (2.1.2), a riconoscere i tipi di malware usati per furto di dati, profitto/estorsione e comprendere come operano, ad esempio: adware (proposta di pubblicità attraverso banner e popup), ransomware (blocco doloso di un programma con lo scopo di chiedere un riscatto per sbloccarlo), spyware (software che invia ad un server remoto i dati di navigazione), botnet (software capace di prendere il controllo di una rete di computer), keylogger (software capace di inviare ad un server remoto i caratteri digitati su una tastiera) e dialer (software capace di cambiare la connessione del modem da un provider ad un altro) (2.1.3), a capire i sistemi di **Protezione (2.2)**, cioè a comprendere come funziona il software antivirus e quali limitazioni presenta (2.2.1), a comprendere che il software antivirus dovrebbe essere installato su tutti i sistemi informatici (2.2.2), a comprendere l'importanza di aggiornare regolarmente vari tipi di software, quali: antivirus, browser web, plug-in, applicazioni, sistema operativo (2.2.3), a eseguire scansioni di specifiche unità, cartelle, file usando un software antivirus, pianificare scansioni usando un software antivirus (2.2.4), a comprendere i rischi associati all'uso di software obsoleto e non supportato, quali: maggiori minacce da parte del malware, incompatibilità (2.2.5), a effettuare la **Risoluzione e rimozione (2.3)**, cioè a comprendere il termine "quarantena" e l'effetto di messa in quarantena file infetti/sospetti (2.3.1), a mettere in quarantena, eliminare file infetti/sospetti (2.3.2), a comprendere che un attacco da malware può essere diagnosticato e risolto usando risorse online quali: siti web di sistemi operativi, antivirus, fornitori di browser web, siti web di autorità preposte (2.3.3).*

2.1 Tipi e metodi

2.1.1 Comprendere il termine "malware". Riconoscere diversi modi con cui il malware si può nascondere nei computer, quali: trojan, rootkit e backdoor.

Ormai anche i non addetti ai lavori hanno sentito parlare dei cosiddetti virus informatici, anche perché con una certa frequenza si trovano articoli allarmistici, anche sui quotidiani.
In realtà il termine è improprio, sarebbe più corretto parlare di malware, in quanto i virus sono solo uno dei possibili tipi di questo software. Nell'uso comune il termine virus viene utilizzato come sinonimo di malware e questo è in parte dovuto al fatto che i programmi antivirus proteggono anche da altre categorie di software maligno, oltre che dai virus propriamente detti.
Il termine malware indica un qualsiasi software creato con l'obiettivo di causare danni ad un computer o anche ad un dispositivo elettronico o di accedere a informazioni riservate, da utilizzare in modo fraudolento. Il termine deriva dalle parole inglesi "malicious" e "software" e ha dunque il significato di programma maligno.
Alcuni di questi programmi sono abbastanza innocui: si limitano a far comparire scritte o immagini sullo schermo, ma altri possono giungere a danneggiare in modo irreparabile i dati e i programmi contenuti nelle memorie di massa del computer.
Si distinguono parecchie categorie di malware, anche se spesso questi programmi sono composti di più parti con caratteristiche diverse, per cui rientrano in più di una tipologia.
I trojan horse (cavalli di troia) devono il loro nome al fatto che il software maligno è inserito in un programma che svolge funzioni utili, interessanti per l'utente, che viene allettato in questo modo ad

installare ed eseguire il programma, e quindi le istruzioni dannose. I trojan horse non si replicano automaticamente, come i virus e i worm, ma conquistano nuovi utenti con le funzioni disponibili nel programma che li ospita.
I rootkit sono programmi che sono in grado di prendere il controllo del tuo sistema informatico senza la tua autorizzazione. Questi programmi non producono direttamente danni, ma servono per nascondere spyware e trojan horse. Sono molto pericolosi perché difficili da individuare ed eliminare.
I programmi backdoor (porta posteriore) permettono un accesso remoto e non autorizzato al tuo sistema informatico e consentono di prendere il controllo del sistema. In questo modo è possibile effettuare operazioni non lecite e accedere ai dati riservati.

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

Alcuni tipi di malware, come i virus e i worm sono in grado di replicarsi, all'insaputa dell'utente, contagiando i sistemi con cui entrano in contatto, e portando a termine l'azione per cui sono stati programmati.
I virus sono serie di istruzioni, normalmente di piccole dimensioni, che si diffondono copiandosi all'interno di altri programmi, o in una particolare sezione del disco fisso, in modo da attivarsi ogni volta che il file infetto viene aperto. Si trasmettono da un computer a un altro con lo spostamento di file infetti. Quando un virus contagia un programma ospite, inserisce all'inizio del programma un'istruzione che rinvia all'esecuzione delle operazioni del virus, alla fine delle quali è posta una istruzione che rinvia all'inizio del programma ospite. L'utente vede l'esecuzione del programma richiesto e non si accorge delle operazioni eseguite dal virus.
Una sottocategoria è costituita dai macro virus, che possono inserirsi, ad esempio, nei programmi della suite di Office, nella forma di macro, cioè sequenze di istruzioni che possono essere previste ovviamente per altri scopi, nei programmi Word, Excel, Access e Power Point. In questi casi la difesa è semplice, in quanto all'apertura del programma sei avvisato della presenza di macro e ti si chiede l'autorizzazione per eseguirle. Se non sei certo che il programma debba contenere macro per determinate elaborazioni è sufficiente non autorizzare la loro esecuzione.
L'attivazione del virus, come abbiamo detto, avviene quando viene eseguito il programma ospite, ma le conseguenze possono essere immediate, all'esecuzione di un particolare comando, o a data stabilita. I danni provocati possono essere danneggiamento o cancellazione di programmi o di archivi, esecuzione di operazioni non previste, segnalazione di guasti inesistenti, rallentamento delle prestazioni del computer.
I worm (vermi) infettano direttamente il sistema operativo, modificandolo, e si attivano automaticamente quando è avviato il computer; per diffondersi sfruttano la rete Internet, e in particolare la posta elettronica. Un'azione tipica dei worm è quella di falsificare l'indirizzo del mittente, creando un effetto di proliferazione di messaggi falsi. Il programma antivirus è in grado di riconoscerli e di respingere il messaggio infetto, la notifica al mittente viene inviata a un indirizzo diverso da quello corretto, che è stato modificato dal worm. Il loro principale obiettivo è quello di rallentare il sistema con l'esecuzione di operazioni inutili.

2.1.3 Riconoscere i tipi di malware usati per furto di dati, profitto/estorsione e comprendere come operano, ad esempio: adware (proposta di pubblicità attraverso banner e popup), ransomware (blocco doloso di un programma con lo scopo di chiedere un riscatto per sbloccarlo), spyware (software che invia ad un server remoto i dati di navigazione), botnet (software capace di prendere il controllo di una rete di computer) , keylogger (software capace di inviare ad un server remoto i caratteri digitati su una tastiera) e dialer (software capace di cambiare la connessione del modem da un provider ad un altro).

Alcuni tipi di malware sono usati per il furto di dati e per operazioni di estorsione.
L'adware (advertising-supported software, software sovvenzionato da pubblicità) è un software che presenta inserzioni pubblicitarie rivolte all'utente, con spesso l'obiettivo di vendere prodotti e servizi. Questi annunci possono essere inseriti nell'interfaccia utente del programma o durante l'installazione. Alcuni di questi programmi inviano a un server, a tua insaputa, informazioni quali indirizzi dei siti e delle pagine Internet visitate, prodotti acquistati, tutti dati utili per fare operazioni pubblicitarie mirate.
I programmi adware possono mettere a rischio la stabilità e la sicurezza del sistema. In ogni caso la continua apertura di popup pubblicitari risulta fastidiosa e causa un rallentamento nell'utilizzo del servizio. Per questo motivo alcuni antivirus considerano gli adware come software rischiosi.
Un ransomware è un tipo di software maligno che causa un blocco doloso del programma che infetta o ne limita l'accesso, allo scopo di chiedere un riscatto per rimuovere l'impedimento. In alcuni casi il file viene criptato e viene chiesto il riscatto per avere la chiave che permette di decriptare il file.
Gli spyware (software spia) sono software che raccolgono informazioni riservate registrate nel sistema e le inviano all'autore dello spionaggio. Le informazioni raccolte possono essere più o meno pericolose: pagine di siti Internet visitate, chiavi usate per crittografare file, credenziali per l'accesso a siti riservati (codice utente e password), dati sensibili. Gli spyware si attivano quando sono installati i programmi nei quali sono nascosti, e non sono in grado di replicarsi automaticamente.
Un botnet, il cui nome è dato dalla contrazione delle parole robot e network, è un insieme di computer collegati in rete e controllati a distanza, in grado di svolgere un attacco simultaneo. L'obiettivo è quello di effettuare massicci invii di messaggi di posta elettronica (spam), o grandi quantità di messaggi inviati a un unico server, che viene così bloccato.
I keylogger sono programmi che possono registrare e trasmettere i caratteri e i comandi inseriti nel computer tramite la tastiera. In questo modo vengono aggirati i sistemi di crittografia delle trasmissioni, perché i dati vengono catturati prima del processo di cifratura. Tra i dati spiati ci possono essere le credenziali (codice utente e password) per accedere a servizi riservati, quali, ad esempio, quelli bancari.
Un dialer è un programma in grado di modificare il numero di telefono chiamato, quando il collegamento a Internet viene fatto con linea analogica commutata, componendo il numero di telefono dell'Internet Provider. All'insaputa dell'utente viene stabilito un collegamento ad un numero a pagamento, i cui ricavi vengono accreditati a chi ha realizzato questo tipo di truffa. Il dialer non funziona nel caso di collegamenti fissi, come ad esempio le linee ADSL.

2.2 Protezione

2.2.1 Comprendere come funziona il software antivirus e quali limitazioni presenta.

Una buona difesa contro il malware è data dai programmi antivirus.
La difesa deve essere usata in tutti i casi in cui vengono importati file dall'ambiente esterno, quindi non solo dalla rete ma anche quando vengono letti CD, DVD, pendrive, dischi rimovibili.
L'antivirus è un programma in grado di riconoscere il software maligno e di eliminarlo o isolarlo, quando non è possibile l'eliminazione.
Tieni sempre attivo il programma antivirus, in modo che effettui un controllo continuo sulle attività svolte, e aggiornalo in continuazione, perché sia in grado di riconoscere anche il malware di nuova produzione. E' infatti importante isolare il malware prima che possa produrre danni.
L'antivirus può intervenire solo sui programmi maligni che è in grado di riconoscere e che sono registrati nel suo database.
Quando questo non avviene, soprattutto a fronte di nuovi malware, scopri che il tuo computer è stato infettato proprio perché ne riscontri gli effetti. Fai, quindi, periodicamente una scansione del sistema; in questo modo l'antivirus rileva la presenza di software infetti e cerca di cancellare il codice virale che vi è stato aggiunto (disinfezione); se l'operazione non riesce, il programma ti consiglia di rimuovere integralmente i file infetti (o di metterli in quarantena) per evitare il propagarsi dell'infezione.
Anche se i programmi antivirus non garantiscono di individuare tutti i file infetti, non è possibile usare due programmi antivirus contemporaneamente. I due programmi sono incompatibili, un antivirus vede l'altro come malware e segnala la presenza di un'infezione che in realtà non esiste.
Nessun antivirus è in grado di garantire il 100% di protezione. Quindi è necessario disporre di un piano di backup, da utilizzare frequentemente, per essere sicuri di non perdere archivi e programmi nel caso di infezione.
L'antivirus per funzionare usa le risorse del sistema, questo può causare un rallentamento delle prestazioni del computer.
Inoltre il cracker può criptare e comprimere il codice maligno per renderlo più difficilmente rintracciabile da parte degli antivirus. Se l'operazione di mascheramento ha successo il malware viene riconosciuto solo quando se ne vedono gli effetti.
Un altro limite degli antivirus è che talvolta vengono segnalati come malware programmi che non sono infettati.

2.2.2 Comprendere che il software antivirus dovrebbe essere installato su tutti i sistemi informatici.

Windows è il sistema operativo più diffuso per i personal computer. Per questo motivo, e anche per alcune sue caratteristiche funzionali, molti programmi maligni sono realizzati per attaccare i sistemi Windows.
Ma anche i sistemi Linux e Mac OS sono soggetti ad attacchi di malware, anche se in misura più limitata.
Un discorso analogo può essere fatto per i dispositivi mobili. Anche in questo caso, la loro enorme diffusione ha stimolato i pirati informatici a sviluppare malware specializzato per questi sistemi.

Ne consegue l'esigenza di proteggere con programmi antivirus tutti i sistemi informatici, in modo da neutralizzare il maggior numero possibile di infezioni da malware.

2.2.3 Comprendere l'importanza di aggiornare regolarmente vari tipi di software, quali: antivirus, browser web, plug-in, applicazioni, sistema operativo.

E' già stato detto che devi aggiornare in continuazione il software antivirus, per poter affrontare i nuovi malware. Normalmente i software antivirus hanno l'aggiornamento automatico.
Ma è anche opportuno aggiornare altri tipi di software, che grazie ai continui aggiornamenti possono presentare migliori difese agli attacchi virali.
Di volta in volta i browser, con successivi aggiornamenti, pongono rimedio alle falle che sono state individuate e introducono variazioni per una maggiore efficacia nella difesa da virus, trojan horse, spam, phishing.
Oltre al browser tieni aggiornati i plug-in, cioè i programmi che interagiscono con altri programmi per aggiungere ulteriori funzioni o per ampliare le funzioni esistenti.
L'utente non vede la presenza di questi programmi, che sono numerosi e importanti per avere certi tipi di servizi.
Per fare alcuni esempi di plug-in usati dai browser:
Java è usato nella realizzazione di molte pagine web;
Adobe Flash Player permette di vedere video e animazioni;
Real Player serve per vedere i video in streaming;
Adobe Acrobat per aprire i file in formato pdf.
Anche i programmi applicativi possono essere soggetti ad attacchi da parte dei programmi malevoli, e possono presentare maggiori difese nelle versioni aggiornate.
Sicuramente importante è l'aggiornamento del sistema operativo, in quanto componente fondamentale nel funzionamento di tutto il computer.
Molti programmi, tra cui il sistema operativo, hanno la funzione di aggiornamento automatico, che segnala la disponibilità di nuovi aggiornamenti, che puoi scaricare nel computer in modo automatico.

2.2.4 Eseguire scansioni di specifiche unità, cartelle, file usando un software antivirus. Pianificare scansioni usando un software antivirus.

Per effettuare la scansione del sistema:
apri il menu START con il tasto WINDOWS della tastiera, o con i tasti CTRL + ESC;
con il tasto TAB seleziona "Tutti i programmi";
con FRECCIA DESTRA apri il sottomenu "Programmi";
FRECCIA GIU' seleziona il programma antivirus che hai installato.
Può darsi che la funzione per avviare il programma sia in un ulteriore sottomenu, in tal caso spostati con FRECCIA DESTRA.
Quando hai selezionato l'antivirus premi INVIO. Si apre una finestra che normalmente riporta due date fondamentali, quella dell'ultima scansione e quella dell'ultimo aggiornamento. Normalmente puoi selezionare due opzioni; con l'opzione interattiva ad ogni codice infetto trovato il programma ti chiede come procedere, con l'opzione automatica i risultati sono riportati in un rapporto finale,

che indica quanti interventi sono stati effettuati direttamente dal programma e ti chiede di decidere come procedere su ogni singolo problema non risolto.
Nella finestra puoi scegliere su quali componenti effettuare la scansione (intere unità di memoria, cartelle, singoli file).
Segui le indicazioni della finestra per avviare la scansione. Il programma segnala il procedere dell'operazione. Per i file in quarantena, ossia isolati, puoi decidere se riattivarli o eliminarli in modo definitivo.
Puoi anche pianificare la scansione, fissando l'intervento in date e orari prestabiliti.

2.2.5 Comprendere i rischi associati all'uso di software obsoleto e non supportato, quali: maggiori minacce da parte del malware, incompatibilità.

Abbiamo detto che per difendere il software dal malware è opportuno tenere sempre aggiornati i programmi usati.
Gli aggiornamenti sono disponibili solo per le versioni più recenti. Le vecchie versioni non sono più supportate dai produttori, e quindi non vengono effettuati gli aggiornamenti necessari per una protezione efficace.
Inoltre, le vecchie versioni di un programma possono essere non compatibili con altri programmi con i quali devono interagire.
Per questo evita l'uso di programmi obsoleti e per i quali non sono garantiti l'aggiornamento e la manutenzione.

2.3 Risoluzione e rimozione

2.3.1 Comprendere il termine "quarantena" e l'effetto di messa in quarantena di file infetti/sospetti.

Il software maligno può infettare tutti i tipi di file: programmi del sistema operativo, programmi applicativi, documenti creati dall'utente.
In alcuni casi il programma antivirus riesce a eliminare il codice virale. In altri casi questa operazione non è possibile.
Nel caso di cancellazione del file, puoi ripristinare facilmente i programmi, partendo dalle loro versioni originali. Nel caso di file da te realizzati, la cancellazione del file comporta anche la perdita dei dati, che puoi recuperare solo se hai a disposizione i backup aggiornati.
In questo caso, per evitare di eliminare file preziosi, il programma antivirus isola i file infetti, e ti chiede se i file devono essere eliminati o messi in quarantena, cioè registrati in una apposita cartella gestita dal programma antivirus. I file di tale cartella non possono essere aperti, e quindi viene bloccata l'esecuzione del codice maligno, ma potrebbero essere recuperati successivamente se il nuovo aggiornamento dell'antivirus riesce a fare la disinfezione.

2.3.2 Mettere in quarantena, eliminare file infetti/sospetti.

In quarantena possono essere messi file sospetti, ma anche i file che sono stati cancellati, in modo che tu possa recuperarli in caso di necessità.
In quarantena normalmente un file viene conservato per un periodo di tempo limitato e successivamente cancellato automaticamente.

La gestione dei file in quarantena viene fatta con il programma antivirus. In questo programma puoi accedere alla funzione quarantena, e operare sui file, effettuandone la cancellazione o il ripristino.

2.3.3 Comprendere che un attacco da malware può essere diagnosticato e risolto usando risorse online quali: siti web di sistemi operativi, antivirus, fornitori di browser web, siti web di autorità preposte.

Tra i tanti servizi che i siti web possono fornire c'è anche quello di scansione online per controllare la presenza di malware.
In genere le caratteristiche di questi servizi sono: semplicità d'uso, limitato uso delle risorse del sistema controllato, aggiornamento continuo garantito, prevedono la scansione intera del sistema o solo di cartelle specifiche indicate dall'utente. Inoltre in caso di necessità puoi controllare il file sospetto con più antivirus online.
Il servizio può essere fornito da siti specializzati o anche da alcuni siti web ufficiali di sistemi operativi, di browser o di autorità di controllo. Ad esempio il servizio antivirus è fornito dalla TIM. per gli utenti ADSL che ne fanno richiesta.

Lezione 3
3 Sicurezza in rete

*In questa lezione si imparerà a conoscere i tipi di **Reti e connessioni (3.1)**, cioè a comprendere il termine "rete" e riconoscere i più comuni tipi di rete, quali LAN (rete locale), WLAN (rete locale wireless), WAN (rete geografica), VPN (rete privata virtuale) (3.1.1), a comprendere che la connessione ad una rete ha implicazioni di sicurezza, quali malware, accessi non autorizzati ai dati, difesa della riservatezza (3.1.2), a comprendere il ruolo dell'amministratore di rete nella gestione delle operazioni di autenticazione, autorizzazione e assegnazione degli account all'interno di una rete; verifica e installazione di patch e aggiornamenti di sicurezza importanti; controllo del traffico di rete e trattamento del malware rilevato su una rete (3.1.3), a comprendere la funzione e i limiti di un firewall in ambiente domestico e di lavoro (3.1.4), ad attivare, disattivare un firewall personale, consentire o bloccare l'accesso attraverso un firewall personale a un'applicazione, servizio/funzione (3.1.5), a capire la **Sicurezza su reti wireless (3.2)**, cioè a riconoscere diversi tipi di sicurezza per reti wireless e i loro limiti, quali: WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access) / WPA2 (Wi-Fi Protected Access 2), filtraggio MAC (Media Access Control), SSID nascosto (Service Set Identifier) (3.2.1), a essere consapevoli che usando una rete wireless non protetta si va incontro ad attacchi da parte di intercettatori (e avesdropping), dirottatori di rete (network hijacking), violatori di comunicazioni private (man in the middle) (3.2.2), a comprendere il termine "hotspot personale" (3.2.3), ad attivare, disattivare un hotspot personale sicuro, connettere in modo sicuro e disconnettere dispositivi informatici (3.2.4).*

3.1 Reti e connessioni

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

Con il termine rete telematica si intende una serie di computer, apparecchiature specializzate e di collegamenti che consente il trasferimento di dati e informazioni tra utenti collegati alla rete.
Gli obiettivi della rete sono la possibilità di scambiare dati in maniera rapida ed efficiente, e di condividere archivi e risorse hardware e software, quali dischi di elevata capacità, stampanti veloci, collegamenti ad altre reti, funzioni aziendali, eccetera.
La rete di fatto aumenta in modo significativo le capacità lavorative dei singoli utenti, ma soprattutto rende possibile il lavoro di gruppo, ossia l'attività di più persone sullo stesso progetto, i cui dati, grazie alla rete, sono resi disponibili a tutte le persone coinvolte e autorizzate.
Il tutto deve garantire adeguati livelli di sicurezza, per assicurare la riservatezza e la protezione dei dati trasmessi sulla rete.
Ci sono vari tipi di reti.
La LAN (Local Area Network, in italiano rete locale), è una rete che si estende in un'area limitata come una azienda, un ufficio, un campus universitario, una abitazione. In funzione della estensione limitata, nella LAN sono usati collegamenti ad alta velocità. Con la fibra ottica attualmente si possono raggiungere velocità di Gb/sec.
Le reti locali possono essere realizzate senza cavi di collegamento, con la tecnologia wireless. Queste reti hanno il nome di WLAN (Wireless LAN) e possono fornire collegamenti di tipo pubblico anche a utenti occasionali, come studenti di una università, clienti di un centro

commerciale, utenti di una biblioteca, eccetera. Inoltre possono essere usate nelle abitazioni per evitare la stesura di cavi. Le velocità di trasmissione sono inferiori a quelle delle LAN.
I vantaggi delle LAN sono:
maggiori velocità,
stabilità garantita dal cavo,
maggiore sicurezza.
Gli svantaggi delle LAN sono:
possibilità di collegamento solo vicino alle prese di rete,
costi maggiori di realizzazione dell'impianto.
I vantaggi delle WLAN sono:
costi contenuti nella creazione della rete,
possibilità di spostarsi all'interno della rete con PC portatili, tablet e smartphone.
Gli svantaggi delle WLAN sono:
minori velocità,
rischio di interferenze,
sicurezza limitata e legata prevalentemente all'uso di password.
Quando la rete si estende a livello territoriale viene chiamata WAN (Wide Area Network, in italiano rete geografica). In questo caso le velocità di trasmissione sono minori.
La diffusione delle reti aziendali, con collegamenti di reti remote, ha fatto nascere l'esigenza di realizzare reti private, usando sistemi di trasmissione pubblici, condivisi con altri utenti, come ad esempio la rete Internet. Queste reti vengono chiamate VPN (Virtual Private Network, rete privata virtuale). Le reti VPN consentono di ridurre i costi rispetto alle reti dedicate, garantendo contemporaneamente un elevato livello di sicurezza.

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

Accanto ai grandi vantaggi che derivano dal connettere il computer a una rete, devi tener presente i rischi che derivano dal collegamento.
Innanzitutto il contagio da malware, che può arrivare dalla rete quando prelevi dati da siti web o tramite la posta elettronica (del malware abbiamo già parlato nella lezione 2).
Inoltre il problema di accessi non autorizzati a dati riservati, quali codice utente e password, che possono essere usati per accedere ai servizi personali di siti Internet (esempio i servizi bancari), o per un furto d'identità da usare per attività illecite (temi già trattati nella lezione 1).
La rete, se non è sufficientemente protetta, può permettere accessi non autorizzati ai dispositivi collegati.
Ma anche dati come le pagine web da te visitate possono essere interessanti per chi vuole costruire un tuo profilo.
Molti rischi non sono strettamente legati all'uso della rete: ad esempio, malware può essere introdotto nel tuo computer da unità di memoria mobili (dischi esterni, chiavette USB, eccetera), le credenziali di accesso possono essere conosciute con le tecniche di phishing, shoulder surfing (spiare alle spalle), eccetera.
Molti sono anche i rischi che la rete presenta, proprio per le sue caratteristiche. Molti dei servizi della rete garantiscono l'anonimato o permettono di usare facilmente false identità.

In una rete sociale è possibile registrarsi con dati diversi da quelli reali e risulta quasi impossibile distinguere le identità reali da quelle false.
Ciò facilita molte attività illecite, quali:
Collegamenti a pagine con messaggi e informazioni fraudolente, che talvolta hanno l'obiettivo di ricavare dati riservati.
Pubblicazioni di informazioni false e pericolose, che rinviano spesso a siti usati per allettarti con false promesse o scaricamento di file gratuiti e che nascondono attività di adescamento o frode.
Adescamento, soprattutto di minori, tramite reti sociali nelle quali risulta facile creare rapporti confidenziali, che possono portare ai reati di pedofilia.
Cyberbullismo (bullismo online), consistente nell'attacco fatto da uno o più minorenni a una persona (nella maggior parte dei casi un minorenne), facendo circolare in rete foto o filmati spiacevoli, minacce e informazioni offensive spesso false.
Quando in rete vieni in contatto con utenti non conosciuti, è importante verificarne l'identità e analizzare i motivi che hanno generato il contatto.
Inoltre è opportuno che tu sia prudente nel pubblicare nelle reti sociali i tuoi dati personali e che selezioni solo informazioni che rispondono agli obiettivi prefissati. Anche se le informazioni possono essere cancellate, nel periodo della loro pubblicazione possono essere state viste, copiate e usate da altri utenti.
L'uso dei servizi delle reti sociali online è gratuito; alcune delle informazioni registrate dagli utenti sono usate per operazioni di marketing e anche commenti sull'uso di prodotti e servizi possono costituire un efficace sistema di passaparola, che favorisce le attività commerciali.
Una particolare attenzione devi dare ai dati personali sensibili, quali orientamento sessuale, idee politiche e religiose, condizioni economiche, ma anche a dati aziendali riservati, legati alla tua attività lavorativa.
In generale, tutte le volte che devi inserire nella tua pagina personale un'informazione, chiediti sempre quale è l'obiettivo della sua pubblicazione, e che rischi sono legati ad un suo uso non autorizzato.

3.1.3 Comprendere il ruolo dell'amministratore di rete nella gestione delle operazioni di autenticazione, autorizzazione e assegnazione degli account all'interno di una rete; verifica e installazione di patch e aggiornamenti di sicurezza importanti; controllo del traffico di rete e trattamento del malware rilevato su una rete.

L'amministrazione della rete è una funzione svolta da una o più persone, interne o esterne all'azienda, e ha il compito di gestire gli aspetti tecnici e organizzativi della rete.
Tra gli altri compiti l'amministratore di rete ha quello di garantire e assicurare la sicurezza e l'efficienza della rete, cioè:
garantire il corretto funzionamento della rete e delle apparecchiature collegate;
installare e aggiornare il software usato per la protezione della rete (ad esempio il firewall);
tenere aggiornato il software usato in rete, con l'installazione di patch (correzioni) e di nuove funzioni;
ottimizzare la gestione delle risorse;
controllare il traffico della rete e effettuare eventuali interventi correttivi;
intervenire per eliminare eventuali malware rilevati nella rete;
definire e attuare le politiche per la sicurezza;

gestire, aggiornare e cancellare le abilitazioni degli utenti all'accesso della rete (autorizzazione all'uso di programmi applicativi, risorse informatiche e a banche dati in funzione delle mansioni);
assegnare codici utenti e password per i nuovi utenti;
supportare gli utenti nel caso di smarrimento delle credenziali di accesso (codici utenti e password dimenticate).

3.1.4 Comprendere la funzione e i limiti di un firewall in ambiente domestico e di lavoro.

Il firewall (in italiano muro o porta tagliafuoco), è un programma, talvolta installato su un hardware dedicato, che regola il traffico tra i sistemi privati e Internet, impedendo gli accessi non autorizzati.
Il sistema funziona in ingresso, bloccando le richieste di utenti esterni a programmi e informazioni non autorizzate, e in uscita, impedendo il collegamento a determinati siti e servizi Internet.
In definitiva il firewall difende il proprio sistema da accessi indesiderati provenienti dalla rete e impedisce l'accesso a siti che non si vuole siano accessibili.
Nelle aziende il firewall può essere inserito tra la rete Internet ed il sistema informatico interno all'azienda, ma, per aumentare il livello di sicurezza, viene normalmente posto tra il sito Web aperto a tutti gli utenti ed i sistemi informatici che gestiscono le applicazioni aziendali accessibili agli utenti autorizzati.
Il firewall, oltre a bloccare gli accessi non autorizzati, segnala all'utente e all'amministratore della rete i tentativi di accesso bloccati.
La protezione del firewall varia in funzione dei parametri usati nella sua personalizzazione. La politica di sicurezza può essere più o meno restrittiva; ad esempio nell'accesso a siti esterni può essere dato l'elenco dei siti web ai quali si può accedere (politica restrittiva, l'accesso è consentito solo al limitato numero di siti indicati) o l'elenco e la tipologia dei siti web ai quali è vietato l'accesso (politica permissiva, l'accesso è possibile a tutti i siti tranne quelli indicati).
Queste regole devono garantire un elevato livello di sicurezza e contemporaneamente non costituire un limite per le attività aziendali.
Quando il firewall divide la rete aziendale dalla rete esterna viene chiamato firewall perimetrale.
E' possibile installare il firewall anche su singoli personal computer (firewall personali). Questo viene fatto per proteggere il computer in ambiente domestico, ma anche in azienda per dare maggiore flessibilità di accesso a un singolo computer. In questo caso, infatti, è l'utente che può negare o autorizzare l'accesso ad un sito web o a un servizio.
Il firewall personale è gestito dal sistema operativo del computer che protegge; c'è quindi il rischio che possa essere neutralizzato da malware che prende il controllo del computer. Nel caso di personal computer domestici, inoltre, non sempre l'utente ha l'esperienza per gestire il firewall e definirne la giusta configurazione.

3.1.5 Attivare, disattivare un firewall personale. Consentire o bloccare l'accesso attraverso un firewall personale a un'applicazione, servizio/funzione.

Come abbiamo detto, il firewall può anche essere un programma installato su un singolo PC, del quale si vogliono controllare gli accessi. In questo caso si parla di personal firewall (firewall personale). Il firewall personale controlla esclusivamente il PC sul quale è installato. Per questo

motivo può dialogare con l'utente, chiedendo l'autorizzazione a procedere nel caso di operazioni sospette e segnalando eventuali tentativi di intrusione.
Le comunicazioni in ingresso e in uscita dal PC stesso sono vietate o ammesse secondo regole di sicurezza, impostate dall'utente quando configura il programma.
Sul mercato sono disponibili vari firewall personali, in alcuni casi anche gratuiti.
Nelle versioni successive a Vista, Windows mette a disposizione un firewall personale (Windows firewall).
Per attivare il programma:
Premi i tasti CTRL + ESC o WINDOWS per aprire il menu START.
Premi TAB per spostarti nel riquadro di destra.
Premi FRECCIA GIU' sino alla voce "Pannello di controllo".
Se non sei posizionato sulla casella di ricerca, premi TAB o MAIUSC + TAB sino a selezionare la casella.
Digita "Firewall" e premi INVIO.
Nella finestra con FRECCIA GIU' seleziona la voce "Controlla stato del firewall".
Premi INVIO.
Con TAB seleziona "Attiva/Disattiva Windows Firewall".
Premi INVIO.
Con TAB spostati su ognuna delle reti disponibili
Con FRECCIA GIU' o FRECCIA SU seleziona il pulsante di controllo dell'operazione che ti interessa (attiva o disattiva).
Con TAB seleziona il pulsante OK.
Premi il tasto INVIO.

3.2 Sicurezza su reti wireless

3.2.1 Riconoscere diversi tipi di sicurezza per reti wireless e i loro limiti, quali: WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access) / WPA2 (Wi-Fi Protected Access 2), filtraggio MAC (Media Access Control), SSID nascosto (Service Set Identifier).

Le reti wireless sono poco sicure, il pericolo di accessi non autorizzati è alto. E' indispensabile che siano protette con delle password. Inoltre le trasmissioni protette sono criptate secondo algoritmi, che negli anni hanno avuto una continua evoluzione.
Il WEP (Wired Equivalent Privacy, sicurezza della privacy equivalente a quella delle reti cablate), è stato il primo algoritmo, sviluppato nel 1999. Ora non è quasi più utilizzato in quanto poco sicuro.
Per migliorare i livelli di sicurezza, nel 2003/2004 sono stati sviluppati il WPA (Wifi Protected Access, accesso protetto alle reti senza fili) e il successivo WPA2.
Un ulteriore miglioramento si ha con il MAC (Media Access Control), che consiste nel gestire l'indirizzo fisico della scheda di rete, cablata o wireless. Tale indirizzo individua in modo univoco il dispositivo. In questo modo è possibile gestire le liste degli indirizzi dei dispositivi autorizzati ad accedere alla rete. Anche questo sistema non garantisce il 100% di sicurezza perché esistono programmi in grado di modificare gli indirizzi fisici dei dispositivi collegati.
Si può raggiungere un buon livello di sicurezza usando più tipi di sicurezza contemporaneamente.
In uno stesso posto possono essere attive più reti wireless. Ogni rete si identifica ai propri utenti con un SSID (Service Set Identifier). Spesso i punti di accesso inviano in continuazione il loro

identificativo, in modo che i dispositivi in grado di collegarsi possano avere la lista delle reti disponibili, dando all'utente la possibilità di scegliere a quale rete collegarsi. Per proteggere una rete si può nascondere il nome della rete (SSID), in modo che non compaia nell'elenco delle reti disponibili e gli utenti indesiderati non possano collegarsi.

3.2.2 Essere consapevoli che usando una rete wireless non protetta si va incontro ad attacchi da parte di intercettatori (e avesdropping), dirottatori di rete (network hijacking), violatori di comunicazioni private (man in the middle).

Come conseguenza dell'evoluzione dei sistemi di sicurezza, quasi tutte le reti wireless sono protette. Questo garantisce sia il proprietario e gestore della rete, sia gli utenti che si collegano.
Le reti non protette espongono gli utenti a vari pericoli. Eventuali attacchi da parte di hacker possono riguardare:
intercettazioni (e avesdropping), i messaggi vengono letti da persone non autorizzate;
dirottamenti (network hijacking), i messaggi vengono instradati ad altri destinatari,
violazioni di comunicazioni private (man in the middle), i messaggi vengono intercettati e modificati.
Inoltre, se il tuo computer non è configurato in modo corretto, alcuni dati registrati possono essere condivisi con tutti gli utenti della rete, e se non è sufficientemente protetto alcuni dati potrebbero essere sottratti o danneggiati.
Alcune reti wireless potrebbero essere non protette in modo intenzionale, proprio per poter effettuare operazioni illegali nei confronti di chi si collega.
Le reti non protette, quindi, riducono i livelli di sicurezza, aumentando i rischi.

3.2.3 Comprendere il termine hotspot personale.

Le reti Wi-Fi sono spesso utilizzate per creare accessi a Internet aperti al pubblico, in luoghi molto frequentati, come:
università, biblioteche, scuole;
centri commerciali e supermercati;
alberghi, residence, villaggi turistici e campeggi;
bar, ristoranti e autogrill;
fiere e manifestazioni;
aeroporti, porti e stazioni ferroviarie;
comuni, enti pubblici e ospedali;
eccetera.
Questi luoghi, che forniscono il servizio di accesso a Internet aperto al pubblico, sono detti hotspot.
Il collegamento dei dispositivi mobili, dotati di scheda wireless, avviene tramite un access point, che è collegato a una rete cablata oppure a un altro access point via radio.
Il numero di frequenze disponibili è limitato e ciò può creare problemi se in un'area sono necessari molti access point, in quanto risulta difficile trovare canali liberi da interferenze.
L'hotspot può essere realizzato anche a livello personale per usare lo smartphone per connettere a Internet uno o più dispositivi mobili che non possono collegarsi direttamente, in zone nelle quali non è disponibile un servizio Wi-Fi. Il tutto viene realizzato con una connessione Wi-Fi sicura e condivisibile con un dispositivo scelto previa autorizzazione e impostazione di una password. In

definitiva puoi sfruttare la funzione hotspot personale per generare una rete wireless e sfruttare la rete dati dei cellulari per connettere computer portatili, tablet o altri dispositivi che in quel momento non hanno accesso alla rete.

3.2.4 Attivare, disattivare un hotspot personale sicuro, connettere in modo sicuro e disconnettere dispositivi informatici.

Per attivare l'hotspot personale usa la funzione di impostazione del cellulare e attiva la funzione hotspot personale. Con l'attivazione di questa funzione viene realizzata la rete wireless per collegare i dispositivi informatici.
Se vuoi, puoi impostare una password personalizzata per proteggere il sistema.
Una volta disponibile l'hotspot dello smartphone puoi collegarti a quest'ultimo da qualsiasi computer, tablet o altro dispositivo usando la procedura standard per connetterti a una rete wireless. Ad esempio, nel caso di un personal computer Windows usa l'icona della rete presente nell'area di notifica.
Per disconnettere un dispositivo è sufficiente chiudere il collegamento. Normalmente se non è attivo nessun dispositivo la funzione hotspot si disattiva automaticamente. Se questa funzione non è disponibile disattiva direttamente la funzione hotspot.

Lezione 4
4 Controllo di accesso

*In questa lezione si imparerà a conoscere i **Metodi (4.1)**, cioè ad identificare i metodi per impedire accessi non autorizzati ai dati, quali: nome utente, password, PIN, cifratura, autenticazione a più fattori (4.1.1), a comprendere il termine "one–time password" e il suo utilizzo tipico (4.1.2), a comprendere lo scopo di un account di rete (4.1.3), a comprendere che per accedere alla rete sono necessari un nome utente e una password, e che è importante disconnettere l'account, al termine del collegamento (4.1.4), a identificare le comuni tecniche di sicurezza biometrica usate per il controllo degli accessi, quali impronte digitali, scansione dell'occhio, riconoscimento facciale, geometria della mano (4.1.5), a conoscere la **Gestione delle password (4.2)**, cioè a riconoscere buone linee di condotta per la password, quali scegliere le password di lunghezza adeguata e contenenti un numero sufficiente di lettere, numeri e caratteri speciali; evitare di condividerle, modificarle con regolarità, scegliere password diverse per servizi diversi (4.2.1), a comprendere la funzione e le limitazioni dei software di gestione delle password (4.2.2).*

4.1 Metodi

4.1.1 Identificare i metodi per impedire accessi non autorizzati ai dati, quali: nome utente, password, PIN, cifratura, autenticazione a più fattori.

Nelle lezioni precedenti abbiamo più volte parlato di password, PIN e cifratura come metodi per impedire accessi non autorizzati a dati e applicazioni.
La password (in italiano parola chiave) è una serie di caratteri alfanumerici e speciali, usata per accedere in modo esclusivo e riservato a risorse informatiche (hardware, software, dati) e per effettuare operazioni di cifratura dei dati.
La password è spesso associata a un nome utente (identificativo utente, in inglese user name o user id).
Il nome utente serve per identificare chi chiede l'accesso alla risorsa, la password serve per certificare la sua identità. Nome utente e password sono le credenziali per l'accesso.
Un esempio di password è il PIN (Personal Identification Number), usato per i servizi Bancomat e per le carte di credito.
L'uso delle sole credenziali di accesso ha un livello di sicurezza non elevato quando si devono proteggere dati sensibili.
Un livello di sicurezza maggiore si ha con la cifratura dei dati, argomento già trattato nella lezione 1, al punto 1.4.2.
Anche per questa operazione serve una password, che è usata dall'algoritmo di cifratura per codificare e decodificare i dati, in modo da impedirne l'accesso a chi non è autorizzato (e non conosce la password).
Spesso per aumentare la sicurezza sono usati contemporaneamente più sistemi di protezione. Ad esempio, nei servizi Bancomat, il riconoscimento dell'utente è fatto leggendo i dati da una carta a microchip (smart card), mentre la password (PIN) è digitata sulla tastiera dall'utente.

4.1.2 Comprendere il termine "one–time password" e il suo utilizzo tipico.

Uno dei problemi nell'uso delle password è che gli utenti spesso usano password facilmente individuabili e non si curano a sufficienza della loro riservatezza.

Normalmente, per ridurre i rischi che ne derivano i sistemi di sicurezza richiedono che la password sia cambiata frequentemente, spesso ogni mese. Il cambio frequente della password ne riduce la validità nel tempo, e diminuisce i rischi che possa essere utilizzata per scopi illeciti.
Nelle applicazioni critiche, come ad esempio le operazioni finanziarie fatte via Internet, possono essere usate one-time password, cioè password che possono essere usate una sola volta e che sono generate dai sistemi informatici. Se anche la password viene intercettata, non può essere utilizzata in quanto è già stata usata.
La password viene generata in modo casuale e normalmente ha validità temporale limitata, anche se non viene usata.
All'utente la password può essere comunicata da piccoli apparecchi tascabili delle dimensioni di una chiave USB e dotati di un piccolo display o con messaggi SMS sul telefono cellulare.

4.1.3 Comprendere lo scopo di un account di rete.

Un account indica un insieme di caratteristiche e autorizzazioni associate ad utente di risorse informatiche.
Con il sistema dell'account, a un utente riconosciuto dal suo user id vengono messe a disposizione risorse e autorizzazioni all'uso di file e servizi, definite attraverso il suo profilo. In ambito aziendale il profilo viene stabilito in funzione dell'attività svolta dall'utente in azienda.
Questo vale per tutte le risorse informatiche, ma a maggior ragione per le reti, e in particolare per le reti esterne, dove ancora maggiori sono i problemi di sicurezza. Nelle reti a un account sono associati i servizi che può usare e i siti a cui può accedere.

4.1.4 Comprendere che per accedere alla rete sono necessari un nome utente e una password, e che è importante disconnettere l'account, al termine del collegamento.

L'accesso a un account avviene tramite la procedura di riconoscimento dell'utente (user name) e di autenticazione (password).
L'utilizzo delle credenziali ha l'obiettivo di identificare l'utente, permettendo l'accesso alla rete solo a chi ne ha diritto, e di autorizzarlo all'utilizzo delle risorse previste dal suo profilo.
Al termine del collegamento è necessario disconnettere l'account, per evitare che altri possano usare le credenziali già inserite per effettuare operazioni alle quali non sono abilitati.

4.1.5 Identificare le comuni tecniche di sicurezza biometrica usate per il controllo degli accessi, quali impronte digitali, scansione dell'occhio, riconoscimento facciale, geometria della mano.

Sempre più spesso, per identificare l'utente vengono usati sistemi di riconoscimento biometrico, ossia sistemi informatici in grado di riconoscere una persona in base a una o più caratteristiche biologiche e comportamentali.
Il riconoscimento avviene mediante il confronto dei dati acquisiti al momento dell'accesso con i dati registrati negli archivi.
Le caratteristiche che possono essere usate devono essere universali (presenti in tutte le persone), uniche (non devono essere uguali in due o più individui), permanenti (non devono cambiare nel tempo) e misurabili (devono poter avere una misura quantitativa).
Le caratteristiche fisiologiche che possono essere usate sono:

le impronte digitali,
il colore e la dimensione dell'iride,
la retina dell'occhio,
la sagoma della mano,
la geometria della mano,
la vascolarizzazione,
la forma dell'orecchio,
la fisionomia del volto,
l'altezza,
il peso.
Le caratteristiche comportamentali che possono essere usate sono azioni che normalmente l'individuo compie, quali:
la firma,
l'impronta vocale,
la scrittura grafica,
lo stile di battitura sulla tastiera,
i movimenti del corpo.
Le caratteristiche fisiologiche sono abbastanza stabili nel tempo, soggette solo a piccole variazioni. Le caratteristiche comportamentali possono variare più frequentemente a fronte di vari fattori, spesso di natura emotiva, perciò devono essere spesso aggiornati i dati di riferimento.
I sistemi biologici puntano al riconoscimento dell'utente in base alle sue caratteristiche e non mediante documenti che possiede (carte a microchip) e codici che conosce.
Il riconoscimento biometrico può affiancare sistemi più tradizionali come smart card e password.

4.2 Gestione delle password

4.2.1 Riconoscere buone linee di condotta per la password, quali scegliere le password di lunghezza adeguata e contenenti un numero sufficiente di lettere, numeri e caratteri speciali; evitare di condividerle, modificarle con regolarità, scegliere password diverse per servizi diversi.

L'efficacia della password è strettamente legata alla sua segretezza, e quindi agli opportuni accorgimenti da prendere perché non venga scoperta. Innanzitutto la password deve essere personale e non condivisa con altri utenti. Deve essere memorizzata dal proprietario e non devono esistere copie scritte. Perché questo sia possibile occorre che sia di media lunghezza (solitamente almeno 8 caratteri), non troppo lunga in modo che il proprietario la possa ricordare senza dover fare copie scritte e nello stesso tempo non troppo corta perché non sia facile da individuare per tentativi. Non deve essere prevedibile, pertanto non deve fare riferimento a dati personali che possono essere conosciuti facilmente (esempio nome dell'utente, data di nascita, targa della vettura, eccetera). Non deve essere una parola di senso compiuto come ad esempio luna, pizza, eccetera. E' opportuno che sia formata da combinazioni di cifre, lettere dell'alfabeto maiuscole e minuscole, e caratteri speciali. Non deve avere vocali accentate che possono essere interpretate in modo diverso in funzione della tastiera e del sistema operativo usato.
Inoltre è bene che venga cambiata con frequenza e che la nuova chiave non abbia un legame logico con la precedente (esempio Ctrpo001, Ctrpo002, Ctrpo003, ecc.).

E’ opportuno usare password diverse per accedere a servizi diversi. Evita di scrivere le password sul tuo computer, perché potrebbero essere scoperte con programmi di facile utilizzo.
Inoltre la password deve essere protetta da possibili intercettazioni, mettendo in atto tutte le possibili difese ai vari tipi di attacchi che sono stati descritti nella lezione 1.
Alcuni programmi e siti Internet consentono all’utente di attivare l’inserimento automatico della password, quando si inserisce il nome utente. Usa questa possibilità se sei sicuro che il tuo computer non possa essere usato da altri.

4.2.2 Comprendere la funzione e le limitazioni dei software di gestione delle password.

Se usi password diverse per ognuno dei servizi usati, potresti dover gestire un elevato numero di password.
Per semplificare questa gestione sono disponibili vari software gratuiti e a pagamento, in grado di registrare le credenziali di accesso in un archivio protetto da una password generale (detta master password). Basta che ti ricordi la master password per poter disporre di tutte le tue password.
Le credenziali di accesso sono registrate nell’archivio in modo criptato (una cassaforte virtuale), con un elevato livello di sicurezza garantito da una chiave di decifratura generata dinamicamente, e sono disponibili solo al legittimo proprietario.
Normalmente l’archivio criptato è registrato in un computer remoto con la tecnica del cloud computing (nuvola informatica). Questo ti permette di disporre delle credenziali contemporaneamente su PC desktop, PC portatile, smartphone. Il sistema garantisce inoltre il backup.
Dopo aver salvato le credenziali di accesso a un servizio, ad esempio a un sito web, ogni volta che ti colleghi al sito puoi usare la funzione di compilazione automatica dei dati di accesso.
Quando devi aggiungere la password per un nuovo servizio o sostituirne una vecchia, puoi chiedere che questa venga generata in automatico dal programma; infatti non hai più il problema di ricordarti la password e puoi usare password più complesse.
Il rischio di questa soluzione è che se dimentichi la master password non hai più le password dei singoli servizi. Inoltre se un malintenzionato dovesse riuscire ad avere la master password, disporrebbe di tutte le tue password.

Lezione 5
5 Uso sicuro del web

*In questa lezione si imparerà a conoscere le **Impostazioni del browser (5.1)**, cioè a selezionare impostazioni adeguate per attivare, disattivare il completamento automatico, il salvataggio automatico quando si compila un modulo (5.1.1), a eliminare dati privati da un browser, quali cronologia di navigazione, cronologia di scaricamento, file temporanei di internet, password, cookie, dati per il completamento automatico (5.1.2), a conoscere la **Navigazione sicura in rete (5.2)**, cioè a essere consapevoli che alcune attività in rete (acquisti, transazioni finanziarie) devono essere eseguite solo su pagine web sicure e con l'uso di una connessione di rete sicura (5.2.1), a identificare le modalità con cui confermare la autenticità di un sito web, quali: qualità del contenuto, attualità, validità URL, informazioni sulla società o sul proprietario, informazioni di contatto, certificato di sicurezza, validazione del proprietario del dominio (5.2.2), a comprendere il termine "pharming" (5.2.3), a comprendere la funzione e i tipi di software per il controllo del contenuto, quali software per il filtraggio di internet, software di controllo genitori (5.2.4).*

5.1 Impostazioni del browser

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

I browser ti permettono di gestire la sicurezza e la privacy secondo le tue esigenze, impostando opportunamente i parametri relativi. Queste possibilità sono particolarmente utili quando il computer è usato da più utenti.
La funzione di completamento automatico ti consente una navigazione più veloce e un rapido accesso ai servizi online, che richiedono l'uso di nome utente e password, di completare automaticamente i dati inseriti nei moduli, ma costituisce anche un rischio per la tua privacy.
Questa funzione può essere attivata o disattivata secondo le tue esigenze.
Con Internet Explorer puoi gestire la funzione da una finestra del browser:
Apri il programma Internet Explorer.
Apri il menu "Strumenti" con i tasti ALT + E. Oppure, premi il tasto ALT e poi spostati con FRECCIA DESTRA fino a raggiungere la scelta "Strumenti"; premi poi INVIO per aprire il menu.
Usa FRECIA GIU' per spostarti nel menu sino alla voce "Opzioni Internet".
Premi il tasto INVIO.
Nella finestra "Opzioni Internet" è aperta la scheda "Generale".
Premi i tasti CTRL + TAB sino alla scheda "Contenuto".
Premi il tasto TAB sino a selezionare il pulsante "Opzioni" del riquadro "Completamento automatico".
Premi il tasto INVIO.
Si apre la finestra "Impostazioni Completamento automatico".
Scorri con il tasto TAB le caselle di controllo della finestra:
"Barra degli indirizzi",
"Cronologia esplorazioni",
"Preferiti",
"Feed",
"Utilizzare Windows Search per migliori risultati",
"Suggerire URL",
"Moduli",
"Nome utente e password sui moduli",
"Richiedi salvataggio password".

Per ogni voce selezionata (casella con segno di spunta), premi la BARRA SPAZIATRICE se vuoi togliere la selezione.
Per ogni voce non selezionata (casella senza segno di spunta), premi la BARRA SPAZIATRICE se vuoi mettere la selezione. Per le voci selezionate viene attivato il completamento automatico.
Quando hai impostato tutte le caselle secondo le tue esigenze, seleziona con TAB il pulsante OK e premi INVIO.
Nella finestra "Opzioni di Internet" seleziona con il tasto TAB il pulsante OK e premi INVIO.

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

Se hai attivato alcune delle funzioni automatiche elencate al punto precedente, in qualsiasi momento puoi eliminare tutti i dati salvati.
Apri Internet Explorer e premi i tasti CTRL + MAIUSC + CANC. Oppure con ALT accedi alla barra dei menu, con FRECCIA DESTRA raggiungi la scelta "Strumenti", aprila con INVIO e scegli "Elimina cronologia esplorazioni" che apri con INVIO.
Si apre la finestra "Elimina cronologia esplorazioni".
Nella finestra è presente una lista di dati che puoi eliminare , associati a una casella di controllo e a una breve descrizione del significato del dato:
I dati che puoi eliminare sono:
"Mantieni dati sui siti preferiti",
"File temporanei Internet e file di siti Web",
"Cookie e dati di siti Web",
"Cronologia",
"Cronologia download",
"Dati dei moduli",
"Password",
"Dati di protezione da monitoraggio".
Scorri con il tasto TAB le caselle di controllo della finestra, metti il segno di spunta alla casella di controllo dei dati che vuoi eliminare:
Per ogni voce selezionata (casella con segno di spunta), premi la BARRA SPAZIATRICE se vuoi togliere la selezione.
Per ogni voce non selezionata (casella senza segno di spunta), premi la BARRA SPAZIATRICE se vuoi mettere la selezione.
Quando hai impostato tutte le caselle secondo le tue esigenze, seleziona con TAB il pulsante ELIMINA e premi INVIO.

5.2 Navigazione sicura in rete

5.2.1 Essere consapevoli che alcune attività in rete (acquisti, transazioni finanziarie) devono essere eseguite solo su pagine web sicure e con l'uso di una connessione di rete sicura.

Come abbiamo detto, le reti di trasmissione dei dati presentano rischi per quanto riguarda la sicurezza e la privacy. Questo è vero in particolare per Internet, che è una rete pubblica.
Inoltre, se la rete è usata per operazioni che prevedono movimenti di denaro, come acquisti, pagamenti, trasferimento di fondi ne possono derivare danni economici anche rilevanti.
Per questo motivo per le operazioni finanziarie è necessario usare reti protette e accedere solo a siti sicuri.

Alcuni siti in rete sono protetti, cioè le comunicazioni con il sito sono criptate. Se visiti un sito protetto, al momento della connessione viene inviato al browser il certificato del sito. Se il certificato è scaduto vieni avvisato con un messaggio. Inoltre, nella barra degli indirizzi compare l'immagine di un lucchetto (la cui etichetta indica l'ente certificatore), e il protocollo di trasmissione si modifica da HTTP a HTTPS (HyperText Transfer Protocol over Secure Socket Layer).
Nel protocollo HTTPS, tra il protocollo http, normalmente usato, e quello TCP viene inserita una fase di crittografia dei dati, in modo che quanto trasmesso sia comprensibile solo per il server e il computer utente collegato.

5.2.2 Identificare le modalità con cui confermare la autenticità di un sito web, quali: qualità del contenuto, attualità, validità URL, informazioni sulla società o sul proprietario, informazioni di contatto, certificato di sicurezza, validazione del proprietario del dominio.

Abbiamo già parlato di come Internet sia ormai diventata la fonte primaria di informazioni in molti campi. Ma quando utilizzi tali informazioni è necessario che tu abbia presente che chiunque può inserire notizie su Internet, perseguendo propri obiettivi, e che manca un qualsiasi controllo, contrariamente a quello che avviene con i giornali e le trasmissioni televisive e radiofoniche, nelle quali esiste una persona responsabile di quanto viene comunicato.
La conseguenza è che non tutte le informazioni sono affidabili, per cui è necessario valutarle con senso critico.
L'attendibilità delle informazioni è strettamente legata alla tipologia di sito. Un sito dedicato alle informazioni come quello di un giornale riporta notizie sicuramente più controllate, e quindi più precise, rispetto ad un sito che raccoglie opinioni dai singoli utenti.
Nei siti per l'informazione, quali giornali online ed enciclopedie, l'attendibilità è pari a quelle dei loro equivalenti cartacei; per i giornali le informazioni sono influenzate da orientamenti politici, ma anche dai loro obiettivi e a quale tipo di utente si rivolgono, nelle enciclopedie digitali è importante la competenza degli autori.
I siti per l'intrattenimento mettono a disposizione giochi, film, registrazioni audio: anche se direttamente non fanno informazione, i contenuti possono indirizzare volontariamente l'opinione pubblica.
I siti dedicati ai dibattiti, quali social network, forum, blog, pubblicano opinioni personali degli utenti che lasciano i loro commenti, in forma anche anonima; la loro attendibilità è legata all'autore del messaggio. Spesso questi siti sono la causa del diffondersi di notizie false, inserite per burla, ma anche talvolta con intenti illegittimi.
I siti commerciali hanno l'obiettivo di vendere prodotti e servizi; in questi siti possiamo trovare due tipi di informazione; per quelle di tipo commerciale tieni presente quale ne è lo scopo e quindi valutale con senso critico, possono avere contenuti prettamente pubblicitari, mentre per le informazioni tecniche l'attendibilità è elevata in quanto l'obiettivo è di fornire assistenza nell'utilizzo dei prodotti e dei servizi.
In tutti i casi, l'importante è la valutazione personale delle informazioni acquisite, ma questo non riguarda solo Internet, ma i sistemi di comunicazione in generale. Quello che aggrava la situazione di Internet è che l'informazione può essere comunicata, con la copertura dell'anonimato, e quindi senza nessuna responsabilità.
In mancanza di altri riferimenti, per valutare la credibilità di un sito web puoi prendere in considerazione una serie di fattori. Innanzitutto a chi è intestato il sito e di conseguenza come si finanzia; ad esempio il sito di un quotidiano a livello nazionale non può permettersi di pubblicare informazioni false, rischiando cause per diffamazione o di vedere compromessa la propria immagine. In ogni caso, per verificare una notizia puoi anche assicurati che sia pubblicata su più giornali.

Molte informazioni sono firmate, nel senso che ne è noto l'autore, che, se conosciuto e stimato, deve evitare di compromettere la propria immagine. Per l'autore dell'informazione valgono le considerazioni già dette: un autore conosciuto e stimato deve porre la massima attenzione a non mettere in gioco la sua credibilità, compromettendo la sua immagine immediata e futura.
Una notizia può risultare attendibile se integrata con riferimenti, quali la provenienza, le fonti esterne, dettagli.
Infine, per le notizie di attualità è fondamentale l'aggiornamento continuo e tempestivo, che può essere verificato se data e ora accompagnano la notizia; questo, ad esempio, è fondamentale per le quotazioni dei titoli in borsa.
I siti, ed in particolare quelli che devono offrire un elevato livello di garanzia, sono in possesso di un certificato digitale.
Un certificato digitale è un documento digitale che attesta l'identità di chi pubblica la pagina web sicura o di chi invia un messaggio di posta elettronica.
I siti certificati hanno nella barra dell'indirizzo l'icona di un lucchetto.
In qualsiasi momento puoi avere informazioni sul certificato selezionando con TAB il pulsante del lucchetto e premendo INVIO. Si apre la finestra che indica chi ha effettuato la verifica, chi è il proprietario del sito, e la conferma che la connessione al server è crittografata. Per avere ulteriori informazioni con TAB vai al pulsante "Visualizza certificati" e premi INVIO. Si apre una finestra con più schede, con ulteriori dettagli. Nel certificato, tra gli altri dati, è presente la data di scadenza. Per chiudere la finestra premi ALT + F4.
Analizziamo ora con maggior dettaglio le più importanti caratteristiche del certificato. Innanzitutto, il documento riporta il numero del certificato, l'organizzazione che lo ha rilasciato, il soggetto a cui si riferisce, la chiave pubblica, e il tipo di algoritmo utilizzato nella crittografia, la data di rilascio e la data di scadenza.
Avrai notato che parliamo di soggetti a cui è stato rilasciato il certificato e non di siti web. Questo perché il certificato può essere rilasciato anche a persone, aziende, organizzazioni.
Non solo, alla stessa persona possono essere rilasciati più certificati nel caso ricopra più ruoli (ad esempio presidente di una organizzazione e amministratore delegato di un'altra.
Essi vengono emessi da un'Autorità di Certificazione, Certificate Authority (CA) e sono firmati con la chiave privata dell'Autorità.
L'autorità di Certificazione ha il compito di identificare il soggetto certificato, rilasciare il certificato, assegnargli la coppia di chiavi crittografiche, gestire le banche dati delle chiavi pubbliche, determinare e controllare la scadenza dei certificati, revocare, al verificarsi di certi eventi, il certificato e le chiavi rilasciate. In sintesi il certificato garantisce la corrispondenza tra le chiavi pubbliche e i soggetti a cui sono state rilasciate.

5.2.3 Comprendere il termine "pharming".

In precedenza abbiamo già parlato del phishing, una pratica fraudolenta che ha l'obiettivo di ottenere le credenziali di accesso personali a siti web.
Lo stesso obiettivo ha il pharming, che usa tecniche più sofisticate.
Nel pharming l'utente digita l'URL, cioè l'indirizzo, di un sito lecito, in forma di stringa di caratteri alfanumerici. Questo indirizzo mnemonico viene trasformato nell'indirizzo IP (numerico) non del sito voluto, ma di un altro sito, creato per spiare le credenziali di accesso, da usare successivamente per scopi illeciti.
Per ingannare l'utente, il sito verso cui viene indirizzato si presenta esteticamente come il sito lecito.
L'attacco può essere fatto al server dell'Internet Service Provider, che effettua la conversione dell'URL in indirizzo IP o direttamente al personal computer della vittima.
Nel caso di attacco al PC dell'utente la difesa può essere data dall'uso di un firewall.

Nel caso di attacco al server, l'unica difesa realmente efficace è costituita dai siti con certificato digitale. Deve essere però cura dell'utente verificare i dati del certificato e non accontentarsi della presenza dell'icona con il lucchetto, nella barra dell'indirizzo.

5.2.4 Comprendere la funzione e i tipi di software per il controllo del contenuto, quali software per il filtraggio di internet, software di controllo genitori.

Molti contenuti pubblicati su Internet non sono controllati prima della loro pubblicazione. La rete può essere usata per distribuire contenuti illeciti anche dal punto di vista penale, quali pedofilia, informazioni sulla costruzione di armi e esplosivi, eccetera.
Altri contenuti possono essere non adatti ad utenti giovani:
la pornografia,
le immagini e i filmati violenti,
il bullismo,
le scommesse.
La rete è usata anche per l'adescamento e lo sfruttamento sessuale di minorenni.
Il firewall è una possibile soluzione alla navigazione senza controlli. Infatti il firewall permette di bloccare l'accesso a siti non idonei o può limitare l'accesso solo ai siti segnalati al programma.
Del firewall e delle sue modalità di utilizzo abbiamo già parlato nella lezione 3.
Un'altra soluzione è il filtro famiglia o controllo genitori (in inglese parental control). Il filtro famiglia è un programma o un servizio di Internet, che permette di indicare le pagine Internet alle quali è vietato l'accesso, o anche a quali pagine è consentito l'accesso.
Puoi anche creare una navigazione differenziata, distinta tra utente minorenne e utente adulto. La navigazione differenziata riconosce le parole usate nella ricerca e blocca le pagine che contengono certi termini (ad esempio parole come nudo, sesso, pornografia, eccetera). La navigazione differenziata può limitare anche i tempi di collegamento.
Windows 7 ha una funzione di controllo.
Per usare la funzione:
Apri il menu "Start" premendo il tasto WINDOWS della tastiera o i tasti CTRL + ESC.
Premi il tasto TAB per spostarti sul menu di destra.
Premi FRECCIA GIU' sino alla voce "Pannello di controllo".
Premi il tasto INVIO della tastiera.
Windows apre la finestra "Modifica le impostazioni del computer".
Nel pannello impostato a visualizzare le icone, usa le frecce direzionali per trovare la voce "Controllo genitori" (le funzioni sono in ordine alfabetico).
Premi il tasto INVIO.
Windows apre la finestra nella quale ci sono gli utenti registrati sul computer.
Con TAB spostati sino all'account che vuoi controllare.
Premi il tasto INVIO.
Se la funzione "Controllo genitori" non è attiva, con FRECCIA SU seleziona il pulsante di opzione "Attivato, applica le impostazioni correnti".
Il controllo è attivato.
Con TAB seleziona il pulsante OK.
Premi il tasto INVIO.
Con i tasti ALT + F4 chiudi la finestra.
In aggiunta o sostituzione alle funzioni del Controllo genitori di Windows, puoi usare programmi che permettono di controllare tutte le operazioni fatte sul computer.
Puoi sapere cosa è stato fatto durante la tua assenza, o limitare a certi giorni e a certe ore l'accesso a Internet. Alcuni di questi programmi sono gratuiti.

Lezione 6
6 Comunicazioni

*In questa lezione si imparerà a conoscere la **Posta elettronica (6.1)**, cioè a comprendere lo scopo di cifrare, decifrare un messaggio di posta elettronica (6.1.1), a comprendere il termine "firma digitale" (6.1.2), a identificare i possibili messaggi fraudolenti o indesiderati (6.1.3), a identificare le più comuni caratteristiche del phishing, quali: uso del nome di aziende e di persone autentiche, collegamenti a falsi siti web, uso di loghi e marchi falsi, incoraggiamento a divulgare informazioni personali (6.1.4), a essere consapevoli che è possibile denunciare tentativi di phishing alle organizzazioni competenti o alle autorità preposte (6.1.5), a essere consapevoli del rischio di infettare un computer o un dispositivo con malware attraverso l'apertura di un allegato contenente una macro o un file eseguibile (6.1.6), a conoscere le **Reti sociali (6.2)**, cioè a comprendere l'importanza di non divulgare su siti di reti sociali informazioni riservate o informazioni personali che permettono l'identificazione (6.2.1), a essere consapevoli della necessità di applicare e di rivedere con regolarità le impostazioni del proprio account su una rete sociale , quali riservatezza dell'account e propria posizione (6.2.2), ad applicare le impostazioni degli account di reti sociali: riservatezza dell'account e propria posizione (6.2.3), a comprendere i pericoli potenziali connessi all'uso di siti di reti sociasli, quali cyberbullismo, adescamento (grooming), divulgazione dolosa di informazioni personali, false identità, link o messaggi fraudolenti o malevoli (6.2.4), a essere consapevoli che è possibile denunciare usi o comportamenti inappropriati della rete sociale al fornitore del servizio o alle autorità preposte (6.2.5), a conoscere i servizi **VoIP e messaggistica istantanea (6.3)**, cioè a comprendere le vulnerabilità di sicurezza della messaggistica istantanea e del VoIP (Voice over IP) , quali malware, accesso da backdoor, accesso a file, intercettazione (eavesdropping) (6.3.1), a riconoscere i metodi per assicurare la confidenzialità durante l'uso della messaggistica istantanea e del VoIP (Voice over IP), quali cifratura, non divulgazione di informazioni importanti, limitazione alla condivisione di file (6.3.2), a conoscere i problemi dei **Dispositivi mobili (6.4)**, cioè a comprendere le possibili implicazioni dell'uso di applicazioni provenienti da "appstore" non ufficiali, quali malware per dispositivi mobili, utilizzo non necessario delle risorse, accesso a dati personali, bassa qualità, costi nascosti (6.4.1), a comprendere il termine "autorizzazioni dell'applicazione" (6.4.2), a essere consapevoli che le applicazioni mobili possono estrarre informazioni private dal dispositivo mobile, quali dettagli dei contatti, cronologia delle posizioni, immagini (6.4.3), a essere consapevoli delle misure precauzionali e di emergenza da adottare in caso di perdita di un dispositivo mobile, quali disattivazione remota, cancellazione remota dei contenuti, localizzazione del dispositivo (6.4.4).*

6.1 Posta elettronica

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

Come è già stato detto nella lezione 1, la cifratura dei messaggi ha origini storiche molto lontane nel tempo. La cifratura può essere fatta per proteggere qualsiasi dato, ma ha una particolare importanza nella posta elettronica per proteggere i messaggi trasmessi con reti telematiche.

La posta elettronica non è normalmente un sistema di comunicazione sicuro se i messaggi sono trasmessi in chiaro.

Per aumentare il livello di sicurezza il messaggio deve essere cifrato, in modo che solo il destinatario, in possesso della chiave per decodificarlo, può leggerlo.

Sempre nella lezione 1 sono già stati trattati i sistemi di cifratura disponibili.

Nel caso sia usato il sistema di cifratura a doppia chiave, quando il messaggio inviato viene criptato con la chiave pubblica del destinatario, solo quest'ultimo conosce la corrispondente chiave privata

ed è in grado di decriptare e quindi leggere il messaggio; che risulta segreto per tutti salvo che per il destinatario.

6.1.2 Comprendere il termine "firma digitale".

Un altro problema della posta elettronica è che il messaggio può essere inviato da una persona che usa una falsa identità.
Per risolvere il problema, si può usare il sistema di crittografia a doppia chiave. Il mittente del messaggio può criptare il messaggio con la sua chiave privata. Il messaggio così codificato può essere trasformato in chiaro solo con la chiave pubblica del mittente. Si ha così la certezza su chi ha scritto il messaggio, il messaggio ha la firma digitale.
Il messaggio può anche essere criptato con la chiave privata del mittente e con la chiave pubblica del destinatario; in questo caso si raggiungono entrambi gli obiettivi: segretezza e autenticazione del messaggio.
Per poter usare la firma digitale occorre possedere la coppia di chiavi (privata e pubblica) che sono utilizzate per la codifica e la decodifica. Le chiavi sono rilasciate da "Autorità di Certificazione", insieme a un "Certificato" che garantisce l'identità della persona, azienda, ente, o sito Internet a cui le chiavi sono rilasciate.
Il file firmato elettronicamente ha il formato .p7m.
Per funzionare il sistema necessita di cataloghi on line delle chiavi pubbliche, ma è anche indispensabile che sia garantita l'identità del possessore delle chiavi, ossia ne siano verificate le generalità. Questo tema verrà sviluppato nel capitolo dedicato al certificato digitale.
L'unica controindicazione della crittografia asimmetrica è che entrambi i processi (codifica e decodifica) sono caratterizzati da elaborazioni complesse e quindi comportano tempi lunghi quando si devono trattare grandi quantità di dati.
Per la firma digitale il problema viene risolto criptando la traccia del documento, ossia un suo riassunto digitale, mentre l'intero documento viene trasmesso in chiaro. Quando il problema è quello della segretezza si ricorre all'uso del sistema simmetrico, molto più veloce, avendo però cura che la trasmissione della chiave venga criptata con il sistema asimmetrico, che ne garantisce la segretezza.

6.1.3 Identificare i possibili messaggi fraudolenti o indesiderati.

La posta elettronica è uno dei servizi Internet più usati. I suoi vantaggi rispetto ad altri sistemi di comunicazione sono molti.
Proprio per la sua ampia diffusione la posta elettronica è spesso usata in modo scorretto.
La maggior parte dei messaggi indesiderati sono dovuti allo spam, cioè l'invio di messaggi non richiesti, in generale di tipo pubblicitario, e che hanno spesso l'obiettivo di vendere prodotti o servizi.
Altri esempi sono il phishing, di cui abbiamo già parlato nella Lezione 1, e il pharming, trattato nella lezione 5. In questo caso l'attacco è maggiormente pericoloso perché l'obiettivo è quello di conoscere le credenziali di accesso a siti e risorse informatiche riservate.
Quando ricevi messaggi di questo tipo, non rispondere, per evitare che il cracker abbia la conferma che l'indirizzo email è attivo e quindi può usarlo per successive operazioni illecite.

Tieni comunque presente che spesso i programmi di gestione elettronica hanno funzioni di filtro per riconoscere e isolare gli spam, che vengono registrati in una apposita cartella, in modo da poter recuperare i messaggi che sono stati individuati come spam per errore.

6.1.4 Identificare le più comuni caratteristiche del phishing, quali: uso del nome di aziende e di persone autentiche, collegamenti a falsi siti web, uso di loghi e marchi falsi, incoraggiamento a divulgare informazioni personali.

Come già detto nella Lezione 1, il phishing è l'invio di messaggi falsi, nei quali si finge che il messaggio sia stato inviato da un sito web che usa le credenziali per l'accesso riservato e ti chiede di confermare le tue credenziali con il collegamento a un indirizzo indicato nel messaggio, pena l'interruzione del servizio reale.
Per ingannare la vittima nel messaggio di phishing viene usato il nome di aziende o persone vere, sono usati loghi e marchi uguali a quelli originali.
Nel messaggio di phishing viene riportato il link a un sito web falso, ma che imita nell'aspetto il sito legittimo.
Per distinguerlo da quello vero puoi verificare con attenzione l'indirizzo scritto nella casella dell'indirizzo, che è diverso da quello originale, salvo quando viene usata anche la tecnica del pharming, di cui abbiamo parlato nella lezione 5, al punto 5.2.3.
Puoi inoltre verificare se le credenziali sono scadute con un accesso diretto al sito vero.
In ogni caso, nessuna organizzazione o persona seria userebbe la posta elettronica per chiedere le tue credenziali o per segnalarti un indirizzo web diverso da quello usato normalmente.

6.1.5 Essere consapevoli che è possibile denunciare tentativi di phishing alle organizzazioni competenti o alle autorità preposte.

Se ricevi un messaggio di phishing, avvisa il proprietario del vero sito che viene simulato nel messaggio, in modo che possa fare eventuali verifiche e avvisare i propri utenti della minaccia.
Se il phishing va a buon fine, cambia immediatamente la password di accesso nel vero sito, o chiedi venga bloccato il tuo accesso al sito se il cambio di password non è più possibile, perché la password è già stata cambiata da chi si è impossessato delle tue credenziali di accesso.
Se ti sono stati sottratti i dati di una carta di credito o Bancomat, chiedi ne venga bloccato l'utilizzo, denuncia il furto alle Forze di Polizia e porta copia della denuncia all'organizzazione che gestisce il servizio, in modo da non essere più responsabile di pagamenti effettuati successivamente.

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

Uno dei sistemi più diffusi per inviare malware via email è quello di allegare file infetti al messaggio di posta elettronica. Il computer viene contaminato all'apertura del file che contiene il malware.
Se il contagio è un macrovirus e sono state attivate le protezioni opportune, al momento dell'apertura il sistema ti avverte della presenza di una macro. Se non sei certo che il file debba contenere una macro chiedi al sistema di bloccarne l'esecuzione.
Comunque verifica sempre gli allegati con un antivirus.

Diffida degli allegati che hanno estensione .exe o .com, in quanto sono programmi autoeseguibili (la loro esecuzione è automatica). Inoltre, guarda attentamente gli allegati, quando non capisci perché ti arrivano, anche se i messaggi sono spediti da interlocutori abituali. Gli allegati possono essere file infetti non noti a chi ha mandato il messaggio.

6.2 Reti sociali

6.2.1 Comprendere l'importanza di non divulgare su siti di reti sociali informazioni riservate o informazioni personali che permettono l'identificazione.

La parola rete sociale (in inglese social network) indica un gruppo di persone che hanno dei rapporti sociali perché sono parenti o amici, o si conoscono tra di loro, o hanno attività lavorative comuni o hanno gli stessi interessi o hobby. Sempre più persone usano Internet e partecipano alle comunità online (comunità virtuali) e il numero di utenti è in continuo aumento. Alcune comunità hanno centinaia di milioni di utenti.
Le reti sociali diventano sempre più grandi perché ogni persona coinvolge altre persone tra i suoi familiari e amici.
Singole persone o organizzazioni possono partecipare a una o più reti.
Alcune di queste comunità si occupano di argomenti particolari, come ad esempio argomenti scientifici, medicina alternativa, musica, giochi, teatro e tanti altri.
Altre comunità hanno temi generali, come ad esempio la politica, l'impegno sociale o la difesa della natura.
Per partecipare ad una comunità online basta l'iscrizione, che è gratuita.
La grande partecipazione alle comunità online è l'indicazione di un grande successo, ma presenta anche notevoli rischi.
Quando sei iscritto a una comunità e pubblichi informazioni personali, devi essere consapevole che quanto scrivi nella rete diventa di dominio pubblico.
Evita quindi di pubblicare dati riservati: informazioni personali o aziendali, di natura economica e finanziaria, immagini private, idee di tendenze religiose, politiche e sessuali. Tieni presente che se anche cancelli le informazioni che non vuoi rimangano di dominio pubblico, moltissimi utenti della rete hanno avuto la possibilità di vederle prima della loro eliminazione.

6.2.2 Essere consapevoli della necessità di applicare e di rivedere con regolarità le impostazioni del proprio account su una rete sociale, quali riservatezza dell'account e propria posizione.

Come abbiamo detto, le informazioni inserite nelle comunità virtuali, compresi i dati personali, possono essere di dominio pubblico. In alcuni casi questo è l'obiettivo di chi partecipa alla comunità con lo scopo di farsi conoscere.
Ma è opportuno sapere i pericoli di questa operazione. I dati, in particolare quelli sensibili, possono essere utilizzati in modo improprio, ed anche fraudolento.
Le informazioni richieste nelle registrazioni sono quelle essenziali, dati aggiuntivi sono una tua scelta, pertanto valuta attentamente quali comunicare. Evita di usare il canale pubblico, ma fai ricorso a messaggi privati, quando la comunicazione riguarda solo interlocutori che conosci personalmente.

Puoi comunque tutelare la tua privacy con l'uso delle funzioni fornite dal programma, gestendo in modo opportuno la visibilità delle foto e dei messaggi pubblicati.
Il tuo profilo deve essere definito in fase di registrazione iniziale, ma anche aggiornato periodicamente, per tenere conto di eventuali nuove esigenze e di nuovi obiettivi che vuoi dare alla tua partecipazione alla rete sociale.

6.2.3 Applicare le impostazioni degli account di reti sociali: riservatezza dell'account e propria posizione.

A fronte di questi problemi, i programmi che gestiscono le reti sociali mettono a disposizione funzioni per la protezione della privacy del tuo profilo. Per ogni informazione memorizzata puoi scegliere se limitarne la visibilità solo a te, solo ai tuoi amici o a tutti. Puoi inoltre nascondere la lista dei tuoi amici, rendendola visibile solo a te o ai tuoi amici. Puoi tutelare la tua privacy vietando che altre persone possano trovarti nelle ricerche online, o possano effettuare rinvii al tuo diario.
Puoi attivare o disattivare la geolocalizzazione, cioè l'identificazione della tua posizione geografica, nel momento in cui inserisci nuove informazioni.
Puoi verificare eventuali accessi con una segnalazione via posta elettronica o vedendo gli accessi più recenti alla tua pagina personale. In questo modo puoi segnalare all'amministratore del sistema eventuali interlocutori non noti. Puoi fare in modo che la tua pagina personale non sia modificabile nella struttura, richiedendo che l'installazione di nuove applicazioni sia controllata da una password.

6.2.4 Comprendere i pericoli potenziali connessi all'uso di siti di reti sociali, quali cyberbullismo, adescamento (grooming), divulgazione dolosa di informazioni personali, false identità, link o messaggi fraudolenti o malevoli.

Inoltre, poni particolare attenzione nello stabilire contatti personali tramite la comunità. Questo vale in particolare per i minori.
La rete sociale può essere usata per: cyberbullismo, (attacchi ripetuti a un individuo, di cui abbiamo già parlato nella lezione 1), di adescamento (grooming, tentativi di entrare in confidenza con una persona per spingerla a comportamenti non appropriati o pericolosi), pedofilia.
I tuoi dati possono essere usati per creare false identità o falsi profili in rete, per mascherare operazioni illecite o per creare collegamenti non autorizzati o per pubblicare messaggi malevoli e fraudolenti, senza essere riconosciuti.

6.2.5 Essere consapevoli che è possibile denunciare usi o comportamenti inappropriati della rete sociale al fornitore del servizio o alle autorità preposte.

Nel caso di comportamenti non corretti nei confronti della tua pagina personale nella rete sociale, puoi farne denuncia al fornitore del servizio, che ha la possibilità di sospendere o cancellare l'utenza che ha compiuto l'azione illecita.
Puoi, ad esempio, segnalare accessi alla tua pagina riservata da parte di utenti non autorizzati.
Tieni presente che anche una azienda, che invia legittimamente messaggi promozionali sfruttando gli indirizzi indicati nella tua pagina, deve aver ottenuto preventivamente il tuo consenso.
Anche le reti sociali sono soggette ad attività di spamming (social spamming).

Alcune violazioni possono avere la gravità di reati. In questo caso inoltra la denuncia al Garante della Privacy, se si tratta di reati amministrativi, o all'Autorità Giudiziaria per i reati di natura penale.

6.3 VoIP e messaggistica istantanea

6.3.1 Comprendere le vulnerabilità di sicurezza della messaggistica istantanea e del VoIP (Voice over IP) , quali malware, accesso da backdoor, accesso a file, intercettazione (eavesdropping).

La messaggistica istantanea IM (Instant Messaging) è un sistema di comunicazione in tempo reale in rete, che permette ai suoi utilizzatori lo scambio di brevi messaggi scritti. Nei primi sistemi di messaggistica istantanea e in alcuni di quelli recenti, il servizio è esclusivamente sincrono, in quanto l'invio di un messaggio è possibile solo quando anche il destinatario è collegato al sistema e solitamente le comunicazioni non sono automaticamente memorizzate dalle applicazioni. Per facilitare questo scambio, al momento della connessione l'utente ha la possibilità di sapere chi è collegato in rete e quindi disponibile.

Alcuni sistemi di messaggistica istantanea offrono la possibilità di memorizzare i messaggi, provenienti da interlocutori conosciuti, in una rubrica, solitamente chiamata "lista dei contatti" o "degli amici". In questo caso vengono superati gli svantaggi della trasmissione sincrona. I messaggi vengono archiviati per un periodo limitato di tempo, e vengono resi disponibili non appena il destinatario si collega al servizio.

I sistemi di messaggistica istantanea offrono spesso anche la possibilità di scambiare file, di conversare tramite voce con tecnologie VoIP, o di effettuare videoconferenze.

I rischi del servizio di Instant Messaging sono molto simili a quelli della posta elettronica: contagio da malware, uso di backdoor, che possono prendere il controllo del sistema per accedere alle risorse installate e agli archivi memorizzati, furto d'identità, intercettazione dei dati trasmessi (eavesdropping).

Il servizio VoIP (Voice over Internet Protocol, Voce tramite Protocollo Internet), rende possibile effettuare una conversazione telefonica sfruttando una connessione Internet. Il principale vantaggio è costituito dall'abbattimento dei costi, che inoltre sono indipendenti dalla distanza tra gli interlocutori.

La tecnologia usata sfrutta la possibilità di instradare più telefonate sulla stessa connessione di rete, mediante l'allocazione dinamica delle risorse, caratteristica della commutazione di pacchetto usata da Internet. Ciò comporta un significativo risparmio nell'utilizzo delle risorse di rete.

Inoltre sono possibili servizi aggiuntivi, quali la videotelefonata, videochiamata e la videoconferenza. Inoltre, permette di memorizzare i messaggi vocali sul proprio computer.

Le aziende telefoniche hanno reso disponibili interfacce per permettere la comunicazione via VoIP con utenti della rete telefonica fissa.

Le conversazioni VoIP possono anche usare come mezzo di trasmissione una qualsiasi rete privata basata sul protocollo IP, per esempio una rete locale aziendale. In questo modo una rete aziendale può essere sfruttata anche per le comunicazioni vocali, permettendo di realizzare economie per l'installazione e il supporto delle infrastrutture di rete.

L'uso del servizio VoIP sta diventando sempre più importante, e di conseguenza la sua sicurezza è diventata fondamentale.

L’autenticazione nelle chiamate avviene tramite credenziali, che possono essere intercettate per rubare l’identità di uno o più utenti. Le false identità possono essere usate per accedere alle segreterie telefoniche, per dirottare i trasferimenti di chiamata o per accedere a dati personali o aziendali riservati. Il servizio può essere usato per operazioni di phishing (vishing, VoIP phishing) e di spamming ed è vulnerabile al malware come qualsiasi altra applicazione. Inoltre è soggetto ad attacchi che ne degradano le prestazioni, inondando l’applicazione con grandi quantità di falsi messaggi di chiamata, che possono arrivare a paralizzare il sistema, rendendolo vulnerabile ad attacchi di controllo a distanza. Le telefonate in corso possono essere manomesse, inserendo rumori nel flusso di comunicazione, e dirottate tramite un reindirizzamento.

6.3.2 Riconoscere i metodi per assicurare la confidenzialità durante l’uso della messaggistica istantanea e del VoIP (Voice over IP), quali cifratura, non divulgazione di informazioni importanti, limitazione alla condivisione di file.

Per proteggere la privacy delle conversazioni, i messaggi possono essere criptati, come nella posta elettronica. In ogni caso, evita di trasmettere informazioni riservate e proteggi gli archivi, limitando la condivisione dei file.

6.4 Dispositivi mobili

6.4.1 Comprendere le possibili implicazioni dell’uso di applicazioni provenienti da “appstore” non ufficiali, quali malware per dispositivi mobili, utilizzo non necessario delle risorse, accesso a dati personali, bassa qualità, costi nascosti.

La grande diffusione di dispositivi mobili, e in particolare degli smartphone, ha stimolato lo sviluppo di sistemi di attacco alla loro sicurezza. I dispositivi mobili usano moltissime app, scaricate direttamente dalla rete, per cui le app sono diventate uno degli strumenti più usati per diffondere il malware.
Le app contraffatte sono particolarmente pericolose, perché in apparenza funzionano come le loro corrispondenti autentiche, ma nel programma sono nascoste le istruzioni malevole, che assumono il controllo del dispositivo. Le conseguenze possono essere l’uso non necessario di risorse del dispositivo, accesso ai dati personali, scarsa qualità del servizio, costi nascosti (non dichiarati).
Le versioni virali delle app sono realizzate riproducendo le funzioni delle app originali, anche se spesso non hanno la stessa qualità; inoltre introducono le istruzioni del malware. Spesso, è difficile eliminare dal sistema le app pericolose, anche con operazioni drastiche come il reset del telefono.
Siti ufficiali, che distribuiscono le app, sono controllati, per cui le app sono garantite. Il problema si ha quando le app sono scaricate da appstore non ufficiali.
Inoltre l’utente può essere allettato da app distribuite gratuitamente e che promettono funzioni interessanti; anche in questo caso è necessario verificare le fonti, per non incorrere nel pericolo di venire contagiati da software malevolo.
In definitiva, nei confronti delle app per i dispositivi mobili occorre usare la stessa prudenza necessaria quando si effettuano download di programmi da siti Internet.

6.4.2 Comprendere il termine "autorizzazioni dell'applicazione".

Purtroppo non è semplice individuare quali siano le app sicure e quali invece utilizzeranno i vostri dati per scopi illeciti.
Nei sistemi operativi dei dispositivi mobili sono disponibili funzioni che forniscono un aiuto contro i pericoli delle app contenenti software malevolo. Queste funzioni ti permettono di gestire le autorizzazioni delle applicazioni, cioè a quali operazioni le singole app sono abilitate.
Nelle versioni più recenti del sistema operativo i permessi per ogni singola operazione vengono richiesti al momento dell'esecuzione dell'app.
Per le app ufficiali, come quelle presenti in Play Store, il negozio virtuale di Google, puoi controllare i permessi richiesti per ogni applicazione consultando direttamente il servizio.
Ad esempio l'accesso illimitato a Internet deve essere consentito solo alle applicazioni sicure, poiché queste avranno il permesso di scambiare e condividere dati sulla rete in completa autonomia. Le app dannose possono creare molti problemi se in possesso di queste autorizzazioni.
Nelle chiamate telefoniche dirette, app come Skype o Facebook Messenger possono comporre automaticamente i numeri di telefono, ma app fraudolente possono usare questa autorizzazione per comporre numeri a pagamento, senza che tu te ne accorga. In modo analogo app maligne possono inviare SMS a servizi a pagamento.
Alcune app devono avere l'autorizzazione a leggere, cancellare e modificare i dati degli archivi USB e delle schede SD (Secure Digital, schede di memoria di tipo flash). Evita di autorizzare a queste operazioni app che per le loro funzioni non necessitano di fare queste operazioni.
In generale prima di autorizzare un app a effettuare determinate operazioni, chiediti se queste operazioni sono giustificate dal servizio richiesto dall'app.

6.4.3 Essere consapevoli che le applicazioni mobili possono estrarre informazioni private dal dispositivo mobile, quali dettagli dei contatti, cronologia delle posizioni, immagini.

Molte app usano l'autorizzazione ad accedere alla rubrica dei contatti, con la possibilità di leggerne e modificarne il contenuto. Ad esempio, le applicazioni che gestiscono i calendari usano i contatti per inserirli nell'evento e per inviare gli inviti a partecipare. L'accesso ai contatti può però essere usato da app maligne per operazioni illecite, e.mail, SMS, invio di dati riservati, eccetera.
Alcune app usano il sistema di geolocalizzazione (GPS, Global Positioning System), per determinare la posizione del dispositivo. Questa informazione è necessaria per i navigatori, ma può anche essere utile per i social network. L'autorizzazione può essere usata per ricostruire i percorsi da te fatti o per inviarti pubblicità mirate relative a prodotti e servizi della zona in cui ti trovi.

6.4.4 Essere consapevoli delle misure precauzionali e di emergenza da adottare in caso di perdita di un dispositivo mobile, quali disattivazione remota, cancellazione remota dei contenuti, localizzazione del dispositivo.

Può capitare che il dispositivo mobile venga perso o rubato. Per evitare problemi fai in modo che sia attiva e configurata in modo opportuno la funzione antifurto.
Con questa funzione, in caso di necessità puoi effettuare alcune operazioni per rintracciare il tuo dispositivo mobile o per bloccarne un uso non autorizzato.

Puoi fare squillare lo smartphone a tutto volume per alcuni minuti. Il telefono squilla anche se è in modalità silenziosa o vibrazione e si interrompe solo se qualcuno risponde alla chiamata.
Puoi bloccare il dispositivo con una password.
Nel caso peggiore, per proteggere i tuoi dati, puoi effettuare la cancellazione remota. Tutti i dati vengono eliminati dal dispositivo (e dalla scheda di memoria SD, se presente), inclusi email, calendario, contatti, foto, musica e file personali dell'utente.
Puoi inoltre usare la funzione che ti permette di individuare su una mappa la posizione del dispositivo e di sapere quando è stato usato l'ultima volta.

Lezione 7
7 Gestione sicura dei dati

*In questa lezione si imparerà a conoscere la **Messa in sicurezza e salvataggio di dati (7.1)**, cioè a riconoscere i modi per assicurare la sicurezza fisica di computer e dispositivi mobili, quali non lasciarli incustoditi, registrare la collocazione e i dettagli degli apparati, usare cavi antifurto, controllare gli accessi alle sale dei computer (7.1.1), a riconoscere l'importanza di avere una procedura di copie di sicurezza da computer e da dispositivi mobili (7.1.2), a identificare le caratteristiche di una procedura di copie di sicurezza, quali regolarità/frequenza, pianificazione, collocazione del supporto dei dati salvati, compressione dei dati (7.1.3), a effettuare la copia di sicurezza di dati su un supporto quale: unità disco/dispositivo locale, unità esterna, servizio su cloud (7.1.4), a ripristinare i dati da una copia di sicurezza su unità disco /dispositivo locale, unità esterna, servizio su cloud (7.1.5), a conoscere la **Cancellazione e distruzione sicura (7.2)**, cioè a distinguere tra cancellare i dati ed eliminarli in modo permanente (7.2.1), a comprendere i motivi per eliminare in modo permanente i dati dalle memorie di massa o dai dispositivi mobili (7.2.2), a essere consapevoli che l'eliminazione del contenuto dai servizi potrebbe non essere permanente, come nel caso dei siti di reti sociali, blog, forum su internet, servizi su cloud (7.2.3), a identificare i metodi più comuni per distruggere i dati in modo permanente, quali uso di tritadocumenti, distruzione di memorie di massa/dispositivi, smagnetizzazione, uso di software per la cancellazione definitiva dei dati (7.2.4).*

7.1 Messa in sicurezza e salvataggio di dati

7.1.1 Riconoscere i modi per assicurare la sicurezza fisica di computer e dispositivi mobili, quali non lasciarli incustoditi, registrare la collocazione e i dettagli degli apparati, usare cavi antifurto, controllare gli accessi alle sale dei computer.

Il problema del furto di personal computer e di dispositivi mobili non riguarda solo la perdita economica dovuta alla sottrazione dell'apparecchiatura, ma rappresenta anche una grave sottrazione delle informazioni registrate.
Nelle aziende il pericolo è maggiore, a fronte di una grande concentrazione di strumenti informatici e di una maggiore presenza di persone esterne all'azienda.
Per ridurre i rischi occorre adottare una serie di misure.
Avere un controllo degli accessi e in particolare degli ingressi di perone esterne all'azienda.
Innanzitutto occorre non lasciare incustoditi i computer e soprattutto i dispositivi mobili, che per le loro ridotte dimensioni sono più facili da rubare.
E' necessario avere un inventario degli strumenti informatici, di tutte le apparecchiature collegate e della loro collocazione, per poter riscontrarne tempestivamente eventuali perdite.
Per i computer e soprattutto per i dispositivi mobili usare cavi antifurto.
Infine controllare gli accessi ai locali, per impedire l'ingresso alle persone non autorizzate e per verificare in caso di necessità chi era presente. Il controllo degli accessi deve essere ancora più restrittivo per i locali che contengono apparecchiature importanti e dati sensibili.

7.1.2 Riconoscere l'importanza di avere una procedura di copie di sicurezza da computer e da dispositivi mobili.

Normalmente gli archivi di lavoro e i loro aggiornamenti vengono registrati nel disco fisso. Molti di questi dati sono importanti e la loro perdita può causare problemi rilevanti.

Le cause della perdita dei dati possono essere varie.
I dischi possono avere dei guasti, che rendono illeggibili i dati registrati.
I computer, e in particolare i dispositivi mobili possono essere rubati.
Gli archivi possono essere danneggiati da malware.
Gli archivi possono essere cancellati per un errore dell'utente o per azioni dolose.
Le attrezzature informatiche possono essere distrutte da eventi eccezionali, come incendi o inondazioni.
Per risolvere il problema è necessario creare copie degli archivi (copie di backup). Se i dati originali vengono persi, si possono recuperare dalle copie di backup.

7.1.3 Identificare le caratteristiche di una procedura di copie di sicurezza, quali regolarità/frequenza, pianificazione, collocazione del supporto dei dati salvati, compressione dei dati.

Le operazioni di backup non devono essere un fatto occasionale, ma occorre stabilire una procedura che valuti quali siano le operazioni da effettuare sulla base delle specifiche esigenze.
Gli archivi devono essere regolarmente salvati su un supporto mobile (chiavetta USB, disco esterno, CD o DVD). La frequenza con cui effettuare il salvataggio dipende dalla frequenza con cui i dati sono aggiornati. Puoi anche ricorrere al backup automatico a scadenze prefissate, quando il computer può essere acceso, ma non è usato per le normali attività, per evitare che venga rallentato il lavoro. Nelle aziende questa attività viene svolta normalmente di notte e il salvataggio avviene su un server della rete.
Il supporto di backup deve essere conservato in luogo sicuro, il più possibile lontano dai dati originali.
Se è possibile effettua il backup su un computer remoto collegato in rete.

7.1.4 Effettuare la copia di sicurezza di dati su un supporto quale: unità disco/dispositivo locale, unità esterna, servizio su cloud.

Windows ha una funzione di backup e ripristino.
Per usare la funzione:
Apri il menu "Start" con i tasti WINDOWS o CTRL + ESC.
Premi TAB per spostarti nel riquadro di destra.
Con FRECCIA GIU' seleziona "Pannello di controllo" e premi INVIO.
Nel pannello impostato alla visualizzazione per icone, con le frecce seleziona "Backup e ripristino" e premi INVIO.
Nella finestra "Backup o ripristino dei file", con TAB seleziona "Configura backup" e premi INVIO.
Viene avviata una procedura guidata, che ti permette, in finestre successive, di scegliere l'unità locale o di rete su cui fare il backup, le cartelle e i file da copiare, quando fare il backup. Alla fine seleziona con TAB il pulsante OK e premi INVIO.
Il backup può essere fatto anche usando i servizi del cloud computing.
Quando hai configurato il backup questo opera in modo autonomo.

Nella finestra “Backup o ripristino dei file” trovi le informazioni relative alle scelte da te fatte, che puoi modificare con il pulsante “Cambia impostazioni”. Puoi avviare in ogni momento il backup con il pulsante “Esegui backup”.

7.1.5 Ripristinare i dati da una copia di sicurezza su unità disco /dispositivo locale, unità esterna, servizio su cloud.

Per effettuare il ripristino usa la stessa funzione.
Apri il menu “Start” con i tasti WINDOWS o CTRL + ESC.
Premi TAB per spostarti nel riquadro di destra.
Con FRECCIA GIU’ seleziona “Pannello di controllo” e premi INVIO.
Nel pannello impostato alla visualizzazione per icone, con le frecce seleziona “Backup e ripristino” e premi INVIO.
Nella finestra “Backup o ripristino dei file” usa il pulsante “Ripristina file personali”.
Anche in questo caso hai una procedura guidata, che ti permette di scegliere le cartelle e i file che vuoi ripristinare, dove li vuoi ripristinare (posizione originale o nuova posizione).

7.2 Cancellazione e distruzione sicura

7.2.1 Distinguere tra cancellare i dati ed eliminarli in modo permanente.

La cancellazione di una cartella o di un file dal disco fisso o da altri supporti di registrazione non comporta, in generale, la loro distruzione. I sistemi operativi e alcuni programmi effettuano il trasferimento dell’oggetto nel cestino. Dal cestino l’oggetto può essere recuperato sino a quando non viene cancellato anche dal cestino o il cestino viene svuotato.
Quando avviene la cancellazione definitiva, sul disco viene liberato lo spazio precedentemente occupato, e tale spazio diventa disponibile per nuove registrazioni, che si sovrappongono alle precedenti. Prima della sovrascrittura, i dati registrati non sono più disponibili per l’utente, ma possono essere recuperati con programmi specializzati.
Quindi, neppure la cancellazione dei dati dal cestino garantisce la loro definitiva eliminazione.

7.2.2 Comprendere i motivi per eliminare in modo permanente i dati dalle memorie di massa o dai dispositivi mobili.

La cancellazione dei dati sensibili è fondamentale, quando il computer o il dispositivo vengono rottamati, venduti o prestati ad altri utenti. Questo vale anche per memorie di massa mobili, quali chiavette USB o dischi esterni. Per la maggior parte degli utenti la cancellazione è sufficiente, ma, come abbiamo già detto, se lo strumento informatico è dato a un tecnico, la cancellazione dei dati non garantisce che questi non siano visti con programmi specializzati.
Il tema della loro eliminazione definitiva viene trattato al punto 7.2.4.

7.2.3 Essere consapevoli che l'eliminazione del contenuto dai servizi potrebbe non essere permanente, come nel caso dei siti di reti sociali, blog, forum su internet, servizi su cloud.

I rischi che la cancellazione di dati non porti alla loro effettiva eliminazione è maggiore quando si usano servizi in rete quali le reti sociali, i blog, i forum, i servizi su cloud.
In questi casi l'utente generalmente non conosce le procedure di cancellazione che vengono adottate e che sono sotto il controllo del fornitore del servizio.

7.2.4 Identificare i metodi più comuni per distruggere i dati in modo permanente, quali uso di tritadocumenti, distruzione di memorie di massa/dispositivi, smagnetizzazione, uso di software per la cancellazione definitiva dei dati

Nelle lezioni precedenti abbiamo detto che molte sono le fonti che persone malintenzionate possono usare per accedere ai nostri dati personali. Per eliminare in modo definitivo i dati devi utilizzare modalità diverse in funzione del supporto su cui i dati sono registrati.
Puoi rendere inutilizzabili le memorie magnetiche usando appositi apparecchi in grado di smagnetizzare le registrazioni, con campi magnetici di elevata intensità. Se però vuoi usare nuovamente la memoria magnetica puoi eliminare definitivamente le registrazioni con programmi che sovrascrivono più volte i file, in modo da renderli illeggibili.
Se la memoria ausiliaria non deve essere più utilizzata puoi ricorrere alla sua distruzione fisica.
Nel caso di documenti cartacei puoi usare un tritadocumenti, che taglia i fogli di carta in striscioline difficili da ricomporre.