Dato: qualsiasi oggetto memorizzabile in formati digitali diversi
Informazione: qualsiasi elaborazione di un dato
Crimine informatico: qualsiasi attività criminale perseguita utilizzando la tecnologia dell'informazione
Hacking: attività per acquisire profonda e completa conoscenza
Hacking etico: attività legali per testare robustezza ed efficienza di un sistema
Cracking: attività finalizzata a rompere e manomettere un sistema
Minacce da forza maggiore: incendi, alluvioni etc. Si prevengono con installazione in zone sicure, impianti antincendio, frequenti backup
Informazioni personali: permettono identificazione di una persona fisica (tutelate dalla privacy 196/2003 – European Data Protection Directive del 1995)
Autenticazione dei soggetti: dimostrazione della propria identità (possesso di oggetto es. chiave hardware; conoscenza di un codice es. PIN o pwd; caratteristica biometrica es. impronte digitali, retina)
Caratteristiche sicurezza delle informazioni:

- **Confidenzialità**: prevenzione dell'accesso da parte dei non autorizzati
- **Integrità**: tutela dall'alterazione dei dati da parte dei non autorizzati
- **Disponibilità**: prevenzione dalla non accessibilità ai legittimi utenti (anche banda di connessione, capacità di calcolo …)

Politiche per linee guida di utilizzo delle tecnologie ICT:

- **sicurezza aziendale**: come azienda intende proteggere informazioni
- **sicurezza per sistema informatico**: come deve essere protetto il sistema informatico
- **sicurezza tecnica**: cosa deve essere protetto

Ingegneria sociale: studio del comportamento dei singoli allo scopo di carpirne informazioni utili. Si esplica in 3 passaggi:

- **raccolta delle informazioni** (*footprinting*) con chiamate telefoniche, phishing (mail per dirottare su siti fasulli) e shoulder surfing (spiare alle spalle)
- **verifica delle informazioni**
- **utilizzo delle informazioni**

Furto di identità: acquisire identità di un altro e compiere azioni a suo nome.
Conseguenze:
furto di denaro
violazione della privacy (accesso a segreti aziendali)
azioni sconvenienti alla reputazione sociale e lavorativa (invio di insulti)
azioni con implicazioni legali
Modalità:
uso di oggetti scartati (vecchi PC o documenti gettati)
mistificazione di identità (fingersi altra persona)
skimming (uso di dispositivi skimmer, per leggere dati nelle bande magnetiche)
Cifratura o **crittografia**: procedimento per rendere incomprensibile a terzi il contenuto di un file o messaggio (anche se venisse violata la password). Quindi garantisce la *riservatezza*

Malware: software che cerca di arrecare danno a un PC o a una LAN; cercano di mettere i sistemi in condizioni tali che i servizi di sicurezza non siano disponibili o che tentano di rubare password / chiavi di rete. Si dividono in:

- infettivi (virus e worm)
- nascosti (trojan, rootkit e backdoor)
- per furto di dati (adware, spyware, botnet, keylogger e dialer)

I malware infettivi si propagano (attraverso la posta elettronica o lo scambio di file) infettando altri file o PC: *virus* (sono frammenti di codice non eseguibili) non possono farlo autonomamente, *worm* sono programmi autonomi e possono autoreplicarsi.
I malware nascosti si nascondono all'interno di altri programmi o si installano all'insaputa dell'utente: *trojans* contengono pericolose proprietà e permettono l'accesso al PC ad altri utenti collegati in rete (sono utilizzati dai cracker per diffondere virus o ottenere il controllo del PC); *rootkit* prendono il controllo del PC senza chiedere autorizzazioni; *backdoor* aprono falle in un sistema (consente di stabilire una connessione con altro PC all'insaputa dell'utente)
Malware per furto di dati: *adware* inseriscono pubblicità all'interno di programmi con licenza gratuita e minacciano la privacy aprendo pop up continui o inviando mail; *spyware* vengono installati insieme ad altre applicazioni (spesso con licenza gratuita) e raccolgono informazioni, provocano cambio della pagina iniziale e redirect ad altri siti; *botnet* è costituita da una rete infetta gestita dal programma bootmaster e provoca attacchi tipo DoS; *keylogger* driver di tastiera che rimangono permanentemente presenti ed intercettano tutti i tasti digitati; *dialer* programmi che attivano connessione a siti a tariffazione esosa.
Antivirus: programmi per rilevare, prevenire ed eventualmente rimuovere i vari malware. Agiscono cercando nella RAM gli schemi tipici di ogni virus (memorizzati nel database della definizione dei virus) o analizzando i pattern di comportamento dei vari programmi in esecuzione. *Limiti*: riconoscono solo i virus presenti nel database e quando hanno infettato un file e presenza di falsi positivi. Oltre alle scansioni programmate, si consiglia quella manuale quando si scaricano file o allegati. Se l'antivirus non riesce a ripulire il file, lo mette in *quarantena*, dove rimane per un periodo durante il quale si spera di trovare una soluzione.
Reti VPN (Virtual Private Network) collegano due LAN geograficamente distanti utilizzando una rete WAN come mezzo di collegamento. La connessione è resa sicura attraverso un protocollo di comunicazione che utilizza una connessione cifrata. La connessione fisica tra le due reti non esiste, è "virtuale".
Nelle LAN sono importanti la gestione utenti, la gestione condivisioni e l'assegnazione delle risorse condivise agli utenti. Tutte queste attività sono controllate dall'Amministratore di rete.
Firewall hardware o software, collocato tra LAN ed esterno, con lo scopo di filtrare e selezionare i pacchetti in input ed output.
Connessione ad una rete (cablata o wireless) comporta rischi di contrarre malware o di subire accessi non autorizzati. Le reti wireless consentono facili accessi di molti dispositivi, ma la connessione deve essere protetta con password. I protocolli sono:

- *WEP* (Wired Equivalent Protocol) protocollo di cifratura dei dati che utilizza algoritmo RC4, ma non è molto sicuro
- *WPA* (Wi-Fi Protected Access) sviluppato per superare i problemi di WEP ha aumentato la lunghezza degli chiavi di cifratura, rendendolo più sicuro.
- *MAC* (Media Access Control) protocollo di basso livello che utilizza il MAC address per identificare le schede connettibili

Connessioni pubbliche non protette rendono facile il furto di informazioni.
Account di rete username + password. L'efficacia della password dipende dalle politiche di sicurezza e di gestione degli utenti.
Pharming tecnica di cracking che mira ad ottenere le informazioni personali dell'utente attraverso l'inganno, utilizzando le connessioni dell'utente, facendogli credere di essere collegato al sito desiderato e non l'invio di messaggi di posta (*phishing*). La difesa dal pharming può essere il firewall, ma migliore è il *certificato digitale*, che garantisce l'identità del sito (contengono la *chiave* pubblica del soggetto, il nome dell'*autorità* di certificazione e la *data* di scadenza)
OTP (One Time Password, cioè password usa e getta) sono password generate da appositi dispositivi e che si usano una sola volta; servono per aumentare la sicurezza dei siti protetti da password
Strumento di riempimento automatico (memorizza i dati inseriti dall'utente durante la compilazione dei form e li suggerisce successivamente) andrebbe disabilitato
Cookie piccoli file di testo inviati dal server al browser perché li rimandi al server durante le successive navigazioni, al fine di tener traccia delle abitudini di navigazione e per mantenere informazioni sulle connessioni. Può essere necessario bloccare l'utilizzo dei cookie provenienti da uno o più siti.
Eliminazione della cronologia utile per preservare la sicurezza delle informazioni in caso di utilizzo del PC da parte di più utenti.
Controllo parentale (in famiglia) filtratura (in aziende)
Social network si possono condividere facilmente molte informazioni; attenzione a non divulgare informazioni personali, impostare un adeguato livello di privacy del proprio profilo. Rischi delle reti sociali: cyberbullismo, adescamento, invio di informazioni ambigue o pericolose, false identità, messaggi fraudolenti. Protezione: accurata selezioni delle informazioni pubblicate ad adeguato livello di privacy.
Servizi di comunicazione: posta elettronica e messaggistica istantanea.
Posta elettronica: essendo un servizio web, l'invio è in chiaro (*cifratura* possibile con molti Client di posta). *Firma digitale*, basata sullo stesso principio del certificato digitale, dà al documento la stessa validità della firma autografa; garantisce *autenticità* e *non ripudio*. Algoritmi di hash trasformano una stringa di lunghezza arbitraria in una di lunghezza fissa (*impronta* = hash o digest) che ha tre proprietà:

- dall'impronta non si può ricostruire il documento originario
- è statisticamente impossibile che due documenti generino la stessa impronta
- una piccola modifica del documento produce una grande modifica dell'impronta

Si può firmare digitalmente un messaggio di posta e un file di Office.
Spamming: l'attività di invio di *spam* (messaggi fraudolenti, messaggi che promettono facili guadagni, messaggi con insistenti offerte pubblicitarie)
Phishing: uso della posta per indirizzare l'utente su siti fasulli, molto somiglianti a quelli veri (le informazioni estorte vengono raccolte dal social engineering ed usate per violare l'account)
Malware: rischio di ricevere messaggi con malware allegati
Messaggistica istantanea (IM) conversazione in tempo reale fra due o più soggetti. E' sincrona (la posta è asincrona). Oltre al testo si possono scambiare file di vario tipo (multimediali, documenti etc.). E' necessario che il destinatario sia presente nella lista dei contatti. *Rischi*:

- propagazione di malware
- accesso da backdoor
- accesso ai file da utenti non autorizzati

Protezioni:

- cifratura
- non divulgare informazioni importanti
- limitare la condivisione dei file

Procedure per gestione sicura dei dati conservandone integrità e disponibilità
Preservare la sicurezza fisica (proteggere i dispositivi):

- registrare i contenuti dei vari dispositivi
- utilizzare cavi di sicurezza per il collegamento e l'alimentazione
- controllare l'accesso ai dispositivi con dispositivi biometrici

Salvaguardare i dati con copie di sicurezza, utili per recuperare i dati andati persi. Le copie di backup si fanno su supporti esterni, da conservare in luogo distinto dal computer (per includere un file o cartella in un backup, va attivato l'attributo "Archivio" / "File pronto per l'archiviazione")
Tipi di backup:

- normale: si fa il backup di tutti i file e poi si toglie l'attributo Archivio
- incrementale: si fa il backup solo dei file modificati dall'ultimo backup e poi si toglie l'attributo Archivio
- differenziale: si lascia l'attributo Archivio fino al successivo backup normale o incrementale
- giornaliero: copia i file con l'attributo Archivio attivato in quel giorno
- copia: come il backup normale ma non si toglie l'attributo Archivio

Supporti di backup:

- hard disk esterni (500 GB – 4 TB)
- pen drive USB (fino a 1 TB)
- archivi on line (gratuito 1 – 5 GB; a pagamento spazi superiori); vantaggio della disponibilità da qualsiasi connessione

Distruzione (smagnetizzazione, graffiatura con giravite etc.) sicura dei supporti con le copie per evitare furto di dati, perché formattazione e cancellazione non impediscono il data recovery. Esistono software di cancellazione sicura