

RETI E SICUREZZA INFORMATICA



UNITÀ 1 - RETI, INTERNET E SERVIZI

1. Le Reti Informatiche

Una rete informatica è un insieme di computer connessi tra loro che possono condividere risorse (dati, servizi, dispositivi) e scambiare informazioni utilizzando lo stesso protocollo di comunicazione.

💡 **CONCETTO CHIAVE:** Condivisione e Comunicazione

1.1 Topologia delle Reti

La topologia descrive come i computer (nodi) sono collegati fisicamente e logicamente in una rete. Può essere:

- **BUS:** tutti i nodi collegati a un cavo lineare (una "autostrada" di dati)
- **ALBERO (o ad albero):** struttura gerarchica con diramazioni dai bus secondari
- **ANELLO:** ogni nodo collegato al precedente e successivo, formando un anello chiuso
- **STELLA:** tutti i nodi connessi a un nodo centrale (hub), comunicazione mediata dal centro
- **MAGLIA:** ogni nodo può collegarsi a tutti gli altri - più affidabile ma complessa

1.2 Architetture di Rete

CLIENT/SERVER: i server offrono servizi e risorse, i client le richiedono e utilizzano

- **Server:** elaboratore potente che mette a disposizione risorse (hardware, software, servizi)
- **Client:** computer che richiede e utilizza i servizi del server
- **Software:** client software = programma sul client; server software = programma sul server

PEER TO PEER (P2P): i computer comunicano direttamente tra loro, ognuno è sia client che server

1.3 Estensione Geografica delle Reti

- **WPAN (Wireless Personal Area Network):** rete personale senza fili (es. Bluetooth, pochi metri)
- **LAN (Local Area Network):** rete locale di piccole dimensioni (casa, scuola, ufficio)
- **MAN (Metropolitan Area Network):** rete urbana che copre una città o area metropolitana
- **WAN (Wide Area Network):** rete geografica di grandi dimensioni (anche tra continenti diversi)
- **GAN (Global Area Network):** rete mondiale che permette elaboratori di connettersi in tutto il pianeta

1.4 Intranet e VPN

- **INTRANET:** rete interna di un'organizzazione, accessibile solo a utenti autorizzati
 - **VPN (Virtual Private Network):** rete privata virtuale che collega in modo sicuro utenti remoti attraverso Internet, usando crittografia
- 🔒 Le VPN garantiscono privacy e sicurezza anche su reti pubbliche

2. Internet

Internet è la più grande rete di computer al mondo, nata negli anni '60 come progetto militare (ARPANET) del Dipartimento della Difesa USA. È un sistema di reti interconnesse che permette lo scambio di informazioni globalmente.

🌐 Internet utilizza il protocollo TCP/IP

2.1 Come Connettersi a Internet

Per connettersi serve un contratto con un ISP (Internet Service Provider) come Tim, Vodafone, Wind. L'ISP è l'erogatore del servizio Internet che fornisce accesso alla Rete.

Tecnologie di Trasmissione:

- **ADSL (Asymmetric Digital Subscriber Line):** usa linee telefoniche esistenti (doppino, cavo telefonico)
- **Fibra ottica:** usa cavi di fibra di vetro che trasmettono informazioni ad altissima velocità

Piani Tariffari:

- **Flat:** tariffa fissa, canone mensile definito, non vincolata al tempo
- **A tempo:** in base alla quantità di dati scambiati o tempo di collegamento
- **A consumo:** tariffa variabile in base all'effettivo tempo di collegamento
- **A volume di traffico:** tariffa variabile in base alla quantità di dati scambiati
- **A fascia di consumo:** tariffa fissa con tetto massimo di dati scaricabili

2.2 Navigare in Internet e il Web

- **WORLD WIDE WEB (WWW o semplicemente Web):** insieme di pagine ipertestuali scritte in HTML (HyperText Markup Language), collegate tramite link
- **BROWSER:** programma applicativo per navigare in Internet e accedere al Web (es. Chrome, Firefox, Safari, Edge)

2.3 L'URL (Uniform Resource Locator)

L'URL è l'indirizzo univoco che identifica una risorsa su Internet.

Struttura di un URL:

<http://www.amazon.it/risorsa/esempio.html>

1. **http://** = protocollo (regole di comunicazione) usato per il trasferimento di pagine Web dal server al client - Il sito è connesso in rete (non si trova sul nostro pc)
 2. **www** = servizio (World Wide Web) - è il servizio a cui si vuole accedere tramite Internet
 3. **amazon** = nome del server/sito - dominio di secondo livello (il Server che ospita il sito)
 4. **.it** = dominio di primo livello (Italia) - indica appartenenza geografica o tematica o di una organizzazione.
 5. **/risorsa/esempio.html** = percorso del file sul server - risorse (sono ulteriori elementi dell'URL).
-

3. I Principali Servizi Internet

3.1 Il Web

Il **WWW** è il principale servizio Internet. Permette di consultare contenuti multimediali (testi, immagini, video) attraverso pagine ipertestuali collegate da link.

- **Web 1.0:** pagine statiche, l'utente consulta passivamente
- **Web 2.0:** utenti sono anche autori - creano contenuti, interagiscono, condividono (blog, social network, wiki)

3.2 E-mail (Posta Elettronica)

Protocolli: SMTP (invio), POP3 (ricezione), IMAP (gestione mail su server)

3.3 Social Network

Siti di reti sociali (Facebook, Instagram, Twitter, LinkedIn) che permettono di creare spazi virtuali per relazioni tra gruppi e individui, condividendo contenuti di vario tipo.

3.4 Blog

Pagine **Web** personali (da "web log" = diario del web) dove pubblicare informazioni, opinioni, pensieri. Possono essere personali o tematici. Gli utenti possono lasciare commenti.

3.5 Servizi VoIP

- **VoIP (Voice over Internet Protocol):** permette di fare telefonate e videotelefonate usando la connessione Internet invece della linea telefonica tradizionale
- **Esempi:** WhatsApp, Skype, Zoom, Teams

3.6 Forum

Spazi virtuali dove gli utenti possono lasciare messaggi su una tematica proposta. Permettono discussioni asincrone (non in tempo reale). Il moderatore gestisce il forum e fa rispettare le regole.

3.7 Webinar

Meeting online (da "web" + "seminar") che permette di svolgere conferenze con partecipanti dislocati in luoghi diversi. Include videoconferenza, condivisione documenti/applicazioni, chat.

3.8 Wiki

Insieme di pagine Web che promuovono la scrittura collaborativa. Tutti possono aggiungere, modificare, cancellare contenuti. Le attività sono registrate e tracciabili.

Esempio: Wikipedia - enciclopedia libera e collaborativa

3.9 Podcast

File audio o video (da "iPod" + "broadcast") che l'utente può scaricare e ascoltare/vedere quando vuole. Si possono aggregare a feed per ricevere automaticamente nuovi episodi.

4. E-Learning, Telelavoro e Smart Working

4.1 E-Learning

In ambito formativo, sfruttando le potenzialità di Internet, è possibile apprendere a distanza attraverso tecnologie multimediali, applicazioni Web e dispositivi connessi.

MOOC (Massive Open Online Courses)

Corsi online gratuiti o a pagamento disponibili su diverse piattaforme, fruibili attraverso dispositivi digitali. Permettono di partecipare contemporaneamente a un numero elevato di persone, anche da tutto il mondo.

Caratteristiche:

- Aperti a tutti
- Flessibili (si seguono quando si vuole)
- Possibilità di ottenere certificazioni
- Varietà di argomenti e livelli

Piattaforme: Coursera, EMMA, EduOpen, FutureLearn

4.2 Telelavoro e Smart Working

- **TELELAVORO:** modalità lavorativa in cui il lavoratore svolge a casa (o comunque in locali non aziendali) il proprio lavoro, collegandosi via Internet
- **SMART WORKING:** modalità lavorativa che si differenzia dal telelavoro perché la prestazione lavorativa non deve essere svolta sempre in un luogo fisso, ma può essere svolta anche in mobilità con connessione WiFi e dispositivi mobili

UNITÀ 2 - SICUREZZA INFORMATICA

La sicurezza informatica è fondamentale per proteggere dati, sistemi e utenti da accessi non autorizzati, frodi, furti, virus e attacchi informatici.

1. Sicurezza dei Dati

La sicurezza dei dati richiede attenzione massima per garantire la tutela. È necessario rispettare regole elementari e adottare corretti comportamenti.

1.1 Username e Password

Quando si condivide un elaboratore, ogni utente deve avere il proprio account (username e password) con specifico livello di autorizzazioni.

Regole per una Password Sicura:

- ✓ NON costituita da informazioni riconducibili al proprietario
- ✓ NON divulgata né annotata su post-it
- ✓ Abbastanza lunga e complessa (lettere maiuscole, minuscole, numeri, simboli)
- ✓ Cambiata periodicamente
- ✓ Diversa per ogni servizio

 Una buona password protegge i tuoi dati da accessi non autorizzati!

1.2 Il Firewall

- **FIREWALL** (letteralmente "parafuoco"): sistema di sicurezza (hardware e/o software) che filtra le informazioni in entrata e uscita da una rete o computer

Il firewall protegge il computer bloccando il traffico da reti esterne e permettendo il passaggio solo di determinati tipi di dati. Può evolvere in meccanismi di autenticazione più sofisticati.

Tipi di firewall:

- **Hardware di difesa perimetrale:** protegge reti collegando più tronconi

- **Logical software (o logico):** installato su sistemi di protezione, permette di impostare regole di accesso

1.3 Il Backup

- **BACKUP:** copiare i dati memorizzati su supporti di memorizzazione esterni (chiavette USB, hard disk, server remoti, cloud)

In caso di problemi (guasti, virus, errori, attacchi hacker, black-out), il backup permette di reinstallare programmi e recuperare dati archiviati.

Cause che richiedono backup:

- Rottura dispositivi di memorizzazione
- Malfunzionamento sistema operativo
- Contagio da virus
- Errori degli operatori
- Attacco da hacker
- Black-out elettrici
- Incendi o allagamenti

Frequenza del backup:

La frequenza dipende dall'attività svolta. In una banca è giornaliera, in un piccolo studio professionale può essere settimanale o mensile.

 Fare backup regolari = proteggere il proprio lavoro!

2. Minacce alla Sicurezza: Virus e Malware

2.1 Che cos'è il Malware?

- **MALWARE** (da "malicious" + "software"): programma maligno, qualsiasi software il cui scopo è quello di danneggiare, in modo diretto o indiretto, un sistema

informatico mettendone a rischio il funzionamento e le prestazioni, violando la privacy del proprietario

2.2 I Virus

- **VIRUS:** parti di codice che si trasmettono riproducendosi all'interno di altri programmi (file eseguibili, settori del disco fisso). Ogni volta che il file infetto viene aperto, si trasmettono da un computer a un altro tramite il trasferimento dei file.

Come si trasmettono i virus:

- Scambio di file o programmi infetti su memorie di massa (chiavette, CD)
- Download di file scaricati dalla Rete
- Apertura di allegati e-mail, messaggi o file in cartelle condivise online

2.3 I Worms ("vermi")

Alterano il sistema operativo del computer e si autoreplicano usando la posta elettronica. Sfruttano la posta elettronica (spam) o diffusione reti LAN/Internet. Inviano a tutti i contatti registrati messaggi con allegati infetti.

2.4 I Trojan Horse ("Cavalli di Troia")

Si nascondono all'interno di programmi apparentemente innocui. Non si replicano come i virus, ma aprono una "porta" sul sistema danneggiato per consentire al malware di impossessarsi dei dati e inviare informazioni riservate.

2.5 Regole per Proteggersi da Virus e Malware

- ✓ Installare un programma antimalware/antivirus e aggiornarlo regolarmente
- ✓ Impostare l'antimalware per bloccare file sospetti dopo averli avvisati
- ✓ Eseguire la scansione di tutti i file in ingresso
- ✓ Con il software antimalware, mettere in quarantena i file sospetti
- ✓ Essere prudenti nell'apertura degli allegati a messaggi di posta elettronica
- ✓ Disattivare l'esecuzione automatica di macro

⚠ **ATTENZIONE:**

I rischi dipendono dalla piattaforma e dai programmi utilizzati.

Alcuni sistemi operativi e applicazioni sono più soggetti ad attacchi!

3. Il Phishing

- **PHISHING:** frode ideata per indurre l'utente a rivelare informazioni personali o finanziarie

Si basa su tecniche di social engineering ("ingegneria sociale") che consistono nell'acquisire informazioni riservate direttamente dall'utente usando la sua fiducia o l'inganno.

3.1 La Tecnica del Phishing

Il phisher (truffatore) invia e-mail che sembrano provenire da siti Web sicuri (banca, posta, istituti di credito). Il messaggio sembra autentico ma contiene richieste ingannevoli.

Come funziona:

1. Si riceve un'e-mail che sembra provenire dalla propria banca
2. Viene richiesto di cliccare un link per "verificare" i dati
3. Il link porta a un sito clone (molto simile all'originale)
4. L'utente inserisce le proprie credenziali
5. I dati vengono rubati dal phisher

3.2 Come Evitare la Truffa del Phishing

- ✓ NON collegare mai a siti di banche o e-commerce tramite link presenti in e-mail
- ✓ NON fornire mai dati riservati (username, password, numeri carta) via e-mail
- ✓ Verificare sempre l'URL del sito (deve iniziare con https://)
- ✓ Controllare la presenza del lucchetto nella barra degli indirizzi
- ✓ In caso di dubbi, contattare direttamente la banca/servizio

 RICORDA:

Banche e istituti di credito **NON** chiedono **MAI** dati riservati via e-mail!
Se ricevi richieste simili, è **SEMPRE** phishing!

4. Sicurezza nelle Transazioni Online

Oggi sempre più utenti acquistano prodotti e servizi online. Per non incorrere in frodi è necessaria attenzione nel procedere alle transazioni commerciali.

4.1 La Crittografia

- **CRITTOGRAFIA:** procedimento matematico che usa algoritmi per rendere incomprensibile un messaggio a chi non ne ha la chiave

Lo scopo è proteggere le informazioni rendendole inaccessibili a tutti tranne che al destinatario.

Come funziona:

- **Crittografia a doppia chiave (asimmetrica):** usa due chiavi - la chiave pubblica (per cifrare) e la chiave privata (per decifrare)
- **Ogni copia di chiavi corrisponde a un solo utente**

4.2 Il Protocollo HTTPS

- **HTTPS (HyperText Transfer Protocol Secure):** garantisce la trasmissione sicura di dati

I server Web che richiedono l'accesso al protocollo HTTPS attivano un sistema di accesso che aggiunge sicurezza alla transazione. Quando si naviga verso siti con HTTPS, la comunicazione è crittografata.

Come riconoscere una connessione protetta:

- ✓ L'URL inizia con https:// (non solo http://)
- ✓ Compare un lucchetto nella barra degli indirizzi
- ✓ Cliccando sul lucchetto si vedono informazioni sul certificato

4.3 Il Certificato Digitale

- **CERTIFICATO DIGITALE:** file elettronico che identifica in modo univoco una persona, un sito Web, un server o un'organizzazione su Internet

Permette comunicazioni sicure e riservate, garantendo l'identità di un soggetto. Include una chiave pubblica di accesso (carta d'identità elettronica dell'utente di Internet).

Cosa contiene un certificato digitale:

- Identità dell'organizzazione che ha rilasciato il certificato
- Nome e cognome del proprietario (o nome del sito/server)
- Chiave pubblica del proprietario
- Data di validità del certificato

Certification Authority (CA): ente che accerta la validità del certificato in modo da definirne autenticità

4.4 La Firma Digitale

- **FIRMA DIGITALE:** equivalente alla firma autografa apposta su carta. Permette di dare validità legale a documenti elettronici

Caratteristiche della firma digitale:

- **Autenticità:** dà garanzia sull'identità di colui che l'ha sottoscritta
- **Integrità:** attesta che il documento non è stato modificato dopo la firma
- **Non ripudio:** il firmatario non può negare di aver sottoscritto il documento

Si basa sull'uso di una coppia di chiavi digitali asimmetriche: la chiave privata per firmare, la chiave pubblica per controllare l'autenticità

4.5 Meccanismi di Autenticazione

I meccanismi di autenticazione si basano su diverse tipologie:

- **CONOSCENZA:** l'utente conosce la password per accedere a un servizio Web

- **POSSESSO:** l'utente possiede il token fisico (chiavetta fornita dal proprio istituto di credito con password monouso per transazioni monetarie online)
- **TOKEN DIGITALE:** codice usa e getta inviato via **SMS** o app sul cellulare del cliente
- **CARATTERISTICHE FISICHE:** l'utente usa l'impronta digitale (riconoscimento biometrico) o "codice volto" per l'accesso alla sala server

La scelta migliore è usare una combinazione delle tre tipologie, aumentando così sicurezza e vantaggi/svantaggi di ognuna.

5. Privacy e Netiquette

5.1 La Privacy

Attraverso la Rete viaggiano enormi quantità di dati e informazioni personali, sempre più presenti in banche dati informatiche. Le normative europee e italiane stabiliscono regole precise per proteggere questi dati.

- **DIRITTO ALLA PRIVACY:** diritto di ciascuno a vedere tutelati i dati personali e la facoltà di accedere a tali informazioni

Regole sulla privacy:

- ✓ Buona norma adottare adeguate impostazioni per il proprio account
- ✓ Limitare la pubblicazione di informazioni personali
- ✓ Evitare di stringere relazioni o incontrare persone sconosciute

SOCIAL NETWORK:

- Facebook consente di fissare diversi livelli di protezione
- Si possono bloccare utenti sconosciuti, limitare la visibilità dei post
- Gestire gli accessi alla privacy

5.2 La Netiquette (Buone Regole del Comportamento)

- **NETIQUETTE** (da "net" + "etiquette"): insieme di regole di comportamento per relazionarsi correttamente nel Web

Regole principali:

- ✓ Rispettare la privacy altrui e in particolare la loro privacy
- ✓ NON assumere toni polemici
- ✓ NON utilizzare un linguaggio volgare
- ✓ Essere chiari e concisi nell'esprimere le proprie idee
- ✓ Essere disponibili alla collaborazione e condividere le conoscenze

✓ NON prevaricare sugli altri

Nelle chat e nei forum:

- Utilizzare emotion o icon (faccine) per esprimere il proprio stato d'animo
- Rafforzare il senso del messaggio se si invia al destinatario

💛 La netiquette rende il Web un luogo più civile e rispettoso!

Rispettare le regole significa rispettare gli altri utenti.

6. L'Ergonomia

- **ERGONOMIA:** disciplina che studia l'interazione tra individuo, strumenti e ambiente di lavoro per realizzare l'adattamento ottimale

Le norme di ergonomia aiutano a evitare problemi derivanti da un utilizzo prolungato del computer. Calibrano le caratteristiche psico-fisiche dell'individuo con l'ambiente lavorativo.

6.1 Postura Corretta

Regole per la postura:

- ✓ Occhi a distanza di 50/70 cm dallo schermo
- ✓ Il bordo superiore dello schermo all'altezza degli occhi
- ✓ Digitazione con gli avambracci sul piano di lavoro
- ✓ Schiena ben appoggiata allo schienale
- ✓ Piedi ben appoggiati al pavimento (o su apposito supporto)
- ✓ Altezza della sedia regolata correttamente

6.2 Configurazione della Postazione

PIANO DI LAVORO:

- Stabile, regolabile in altezza
- Ampiezza sufficiente per favorire una posizione comoda

SEDIA:

- Stabile, dotata di 5 ruote
- Funzione di rotazione
- Piano e schienale regolabili in modo indipendente
- Permette un buon appoggio ai piedi

MONITOR:

- Frequenza di refresh superiore a 72 Hz

- Buona regolazione della luminosità e contrasto
- Orientato e inclinato per evitare fastidiosi riflessi

6.3 Lavoro Continuativo

In caso di lavoro continuativo su videoterminali, la legge prevede una pausa di quindici minuti ogni due ore di lavoro per evitare:

- Affaticamento visivo
- Possono condurre a stati ansiosi
- Attività circolazione del sangue
- Disturbi muscolo-scheletrici

Altri problemi da evitare:

- Salute delle articolazioni
- Alterazione ritmi delle connessioni WiFi e radiazioni
- Uso eccessivo dello smartphone



RIEPILOGO GENERALE

Concetti Fondamentali da Ricordare

RETI INFORMATICHE

- ✓ Permettono condivisione di risorse e comunicazione
- ✓ Diverse topologie: bus, albero, anello, stella, maglia
- ✓ Architetture: client/server e peer-to-peer
- ✓ Estensione: WPAN, LAN, MAN, WAN, GAN

INTERNET E WEB

- ✓ Internet = rete globale di computer
- ✓ Usa protocollo TCP/IP
- ✓ Web = servizio principale di Internet (pagine ipertestuali)
- ✓ Browser = programma per navigare
- ✓ URL = indirizzo univoco delle risorse

SERVIZI INTERNET

- ✓ E-mail, Web, social network
- ✓ Blog, forum, wiki
- ✓ VoIP, webinar, podcast
- ✓ E-learning, MOOC
- ✓ Telelavoro e smart working

SICUREZZA INFORMATICA

- ✓ Password sicure e diverse per ogni servizio
- ✓ Firewall per proteggere la rete

- ✓ Backup regolari dei dati importanti
- ✓ Antimalware/antivirus aggiornato

MINACCE

- ✓ Virus, worm, trojan horse
- ✓ Phishing (frode per rubare dati)
- ✓ Malware (software dannosi)

TRANSAZIONI ONLINE

- ✓ Crittografia per proteggere i dati
- ✓ Protocollo HTTPS per connessioni sicure
- ✓ Certificati digitali per autenticazione
- ✓ Firma digitale per validità legale

PRIVACY E COMPORTAMENTO

- ✓ Proteggere i propri dati personali
- ✓ Rispettare la netiquette
- ✓ Configurare correttamente le impostazioni privacy

ERGONOMIA

- ✓ Postura corretta davanti al computer
- ✓ Pause regolari (15 minuti ogni 2 ore)
- ✓ Postazione di lavoro ben configurata

Suggerimento per lo Studio

 Per ottenere il massimo da questa dispensa:

1. Leggi ogni sezione con attenzione
2. Sottolinea i concetti chiave
3. Crea schemi personali
4. Ripeti ad alta voce i contenuti
5. Fai esempi pratici
6. Verifica la comprensione con domande

Questa dispensa è pensata per essere accessibile a tutti!

Usa gli spazi bianchi per annotazioni personali.

Dispensa creata con cura per scopi educativi. Ultimo aggiornamento: gennaio 2026

SparkStudio-Educational.it

@sparkstudio_educational