NAVIGARE E CERCARE INFORMAZIONI SUL WEB

Prof Polizzi Francesco

Navigare in Rete - Concetti di Base

- Cos'è Internet e come funziona
- Indirizzi IP e nomi di dominio
- Il World Wide Web (WWW)
- Protocolli di comunicazione (HTTP, HTTPS)
- Breve storia di internet

Cos'è Internet e come funziona

Internet è una rete globale di computer interconnessi che comunicano tra loro, consentendo lo scambio di informazioni e la comunicazione a livello mondiale.

Internet è definita "rete di reti" perché collega reti di computer di varie dimensioni, dalle reti domestiche alle grandi reti aziendali e governative.I dati vengono trasmessi attraverso cavi in fibra ottica, cavi di rame, onde radio e satelliti. La comunicazione avviene tramite "pacchetti" di dati, che vengono instradati attraverso la rete. Internet si basa su protocolli di comunicazione standardizzati, come il TCP/IP (Transmission Control Protocol/Internet Protocol), che definiscono come i dati vengono formattati, trasmessi e ricevuti.Questi protocolli garantiscono l'interoperabilità tra i dispositivi, consentendo a computer di diversi tipi e sistemi operativi di comunicare tra loro.Ogni dispositivo connesso a Internet ha un indirizzo IP univoco, che lo identifica sulla rete.Gli indirizzi IP consentono ai dispositivi di comunicare tra loro, inviando e ricevendo pacchetti di dati. I nomi di dominio, come google.com, sono versioni più facili da ricordare degli indirizzi IP. Il sistema DNS (Domain Name System) traduce i nomi di dominio in indirizzi IP, consentendo ai browser web di trovare i siti web. **World Wide Web (WWW):**I WWW è un servizio di Internet che permette di accedere a documenti ipertestuali (pagine web). Le pagine web sono ospitate su server web e vengono trasmesse ai browser tramite il protocollo HTTP/HTTPS.

In sintesi, Internet è un'infrastruttura complessa e decentralizzata che consente la comunicazione e lo scambio di informazioni tra miliardi di dispositivi in tutto il mondo.

Indirizzi IP e nomi di dominio

Per comprendere appieno il funzionamento di Internet, è fondamentale conoscere il ruolo degli indirizzi IP e dei nomi di dominio. Questi due elementi sono essenziali per consentire ai dispositivi di comunicare e agli utenti di accedere ai siti web. Un indirizzo IP (Internet Protocol) è un'etichetta numerica univoca assegnata a ogni dispositivo connesso a una rete informatica che utilizza il protocollo Internet per la comunicazione. Funziona come un "indirizzo di casa" per un computer, consentendogli di inviare e ricevere dati su Internet. **Tipi di indirizzi IP: IPv4:** Il formato originale, composto da quattro gruppi di numeri (ad esempio, 192.168.1.1). A causa della crescita esponenziale di Internet, gli indirizzi IPv4 si stanno esaurendo. **IPv6:** Un formato più recente che utilizza un sistema alfanumerico (ad esempio, 2001:0db8:85a3:0000:0000:8a2e:0370:7334), fornendo un numero molto maggiore di indirizzi disponibili. Gli indirizzi IP consentono ai dispositivi di identificarsi e comunicare tra loro su Internet. Quando un computer invia dati a un altro, l'indirizzo IP del destinatario viene utilizzato per instradare i dati alla destinazione corretta. **Nomi di dominio:** Un nome di dominio è una traduzione testuale di un indirizzo IP, progettata per essere più facile da ricordare per gli esseri umani. Ad esempio, "google.com" è un nome di dominio.

Sistema DNS (Domain Name System): Il DNS è un sistema che traduce i nomi di dominio in indirizzi IP. Quando un utente digita un nome di dominio in un browser web, il DNS cerca l'indirizzo IP corrispondente e indirizza il browser al server web corretto.**Struttura di un nome di dominio:** I nomi di dominio sono strutturati in gerarchie, con domini di primo livello (TLD) come ".com", ".org" e ".net",esistono anche domini di primo livello nazionali (es. .it). I sottodomini (ad esempio, "www.google.com") forniscono ulteriori livelli di organizzazione. **Funzione:** I nomi di dominio rendono Internet più facile da usare, consentendo agli utenti di accedere ai siti web utilizzando nomi facili da ricordare anziché indirizzi IP numerici.

In sintesi, gli indirizzi IP sono gli "indirizzi" numerici dei dispositivi su Internet, mentre i nomi di dominio sono le versioni testuali di tali indirizzi, rese possibili dal sistema DNS.

Il World Wide Web (WWW)

Il World Wide Web (WWW), spesso abbreviato in "Web", è un sistema di informazioni che consente l'accesso a documenti e altre risorse tramite Internet. Ecco una spiegazione più dettagliata: È un sistema di informazioni ipertestuali: ciò significa che i documenti (pagine web) sono collegati tra loro tramite collegamenti ipertestuali (link). Permette di accedere a una vasta gamma di contenuti: testo, immagini, video, audio e altri tipi di file. Utilizza Internet come infrastruttura: il Web si basa su Internet per trasmettere dati tra computer.

Come funziona il WWW?

Gli utenti accedono al Web tramite software chiamati browser web (come Chrome, Firefox, Safari). I browser interpretano il codice delle pagine web e le visualizzano sullo schermo.Le pagine web sono memorizzate su computer chiamati server web.Quando un utente richiede una pagina web, il browser invia una richiesta al server web, che risponde inviando la pagina. Il protocollo HTTP (Hypertext Transfer Protocol) è utilizzato per trasferire dati tra browser e server. HTTPS è una versione sicura di HTTP che utilizza la crittografia per proteggere i dati. Le pagine web sono scritte in HTML, un linguaggio di markup che definisce la struttura e il contenuto delle pagine. **URL(Uniform Resource Locator):** gli URL sono gli indirizzi delle pagine web.

Il WWW è un servizio di Internet, ma non è Internet stesso. Internet è l'infrastruttura, mentre il Web è uno dei servizi che utilizza tale infrastruttura. Tim Berners-Lee è considerato l'inventore del World Wide Web, sviluppato al CERN nel 1989. Il Web ha rivoluzionato l'accesso alle informazioni e la comunicazione, diventando una parte essenziale della vita quotidiana. In sintesi, il World Wide Web è un sistema che rende facile l'accesso e la condivisione di informazioni su Internet, grazie all'uso di ipertesti, browser web e protocolli standardizzati.

Protocolli di comunicazione (HTTP, HTTPS)

I protocolli di comunicazione HTTP e HTTPS sono fondamentali per il funzionamento del World Wide Web. Ecco una breve descrizione:

HTTP (Hypertext Transfer Protocol):

- È il protocollo di applicazione che definisce come i messaggi vengono formattati e trasmessi sul World Wide Web.
- È il fondamento della comunicazione dati per il World Wide Web.
- HTTP funziona come un protocollo di richiesta-risposta tra un client e un server.
- Il client, di solito un browser web, invia una richiesta HTTP al server, e il server risponde con i dati richiesti, come una pagina web.
- Una delle principali debolezze di HTTP è che i dati trasmessi non sono crittografati, il che significa che possono essere intercettati e letti da terzi.

HTTPS (Hypertext Transfer Protocol Secure):

- È la versione sicura di HTTP.
- Utilizza la crittografia SSL/TLS (Secure Sockets Layer/Transport Layer Security) per proteggere la comunicazione tra il client e il server.
- La crittografia garantisce che i dati trasmessi siano protetti da intercettazioni e manomissioni.
- HTTPS è essenziale per la trasmissione di informazioni sensibili, come password, dati di carte di credito e altre informazioni personali.
- Quando un sito web utilizza HTTPS, l'URL inizia con "https://" e di solito viene visualizzata un'icona a forma di lucchetto nella barra degli indirizzi del browser. Questo indica che la connessione è sicura.
- HTTPS è considerato uno standard di sicurezza sul web.

Differenze principali:

- **Sicurezza:** HTTPS è crittografato, HTTP no.
- **Porta:** HTTP utilizza la porta 80, mentre HTTPS utilizza la porta 443.
- **Lucchetto:** HTTPS visualizza un'icona a forma di lucchetto nel browser, indicando una connessione sicura.

Breve storia di internet

La storia di Internet è un percorso affascinante che ha trasformato radicalmente il modo in cui comunichiamo, lavoriamo e viviamo.
ARPANET: Le radici di Internet risalgono agli anni '60, durante la Guerra Fredda. L'ARPA (Advanced Research Projects Agency) del Dipartimento della Difesa degli Stati Uniti sviluppò ARPANET, una rete di computer progettata per resistere a eventuali attacchi nucleari. L'obiettivo era creare una rete decentralizzata in grado di mantenere la comunicazione anche in caso di danni parziali.Nel 1969, fu stabilita la prima connessione tra computer presso l'Università della California a Los Angeles e lo Stanford Research Institute.

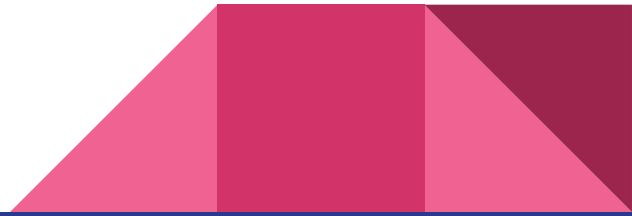
Gli anni '70 e '80: lo sviluppo dei protocolli: TCP/IP: Negli anni '70, Vinton Cerf e Robert Kahn svilupparono il protocollo TCP/IP (Transmission Control Protocol/Internet Protocol), che divenne la base per la comunicazione su Internet.Questo protocollo standardizzato permise a reti diverse di comunicare tra loro, gettando le basi per l'interconnessione globale. La nascita della posta elettronica: Negli anni '70, fu sviluppata la posta elettronica, che rivoluzionò la comunicazione interpersonale.

Breve storia di internet

Gli anni '90: l'avvento del World Wide Web: Il World Wide Web (WWW):Nel 1989, Tim Berners-Lee, un informatico del CERN (Organizzazione europea per la ricerca nucleare), inventò il World Wide Web.Il WWW introdusse il concetto di ipertesto, che permetteva di collegare documenti e risorse tramite link. Nel 1991, Berners-Lee pubblicò il primo sito web, aprendo la strada alla diffusione globale del Web.La diffusione dei browser:La nascita di browser web come Mosaic e Netscape Navigator rese l'accesso al Web più facile e intuitivo, contribuendo alla sua rapida crescita.
Gli anni 2000 e oltre: l'era della connettività globale: La diffusione della banda larga:L'introduzione della banda larga permise connessioni Internet più veloci e affidabili, favorendo lo sviluppo di servizi online come lo streaming video e i social media.La rivoluzione mobile:La diffusione degli smartphone ha portato Internet nelle mani di miliardi di persone in tutto il mondo, trasformando il modo in cui accediamo alle informazioni e comunichiamo. Il Web 2.0 e i social media:L'avvento del Web 2.0 ha dato vita a piattaforme interattive come i blog, i social network e i wiki, che hanno trasformato gli utenti da semplici consumatori di contenuti a creatori e partecipanti attivi.
Internet continua a evolversi rapidamente, con nuove tecnologie come l'intelligenza artificiale, l'Internet delle cose (IoT) e la realtà virtuale che stanno plasmando il futuro della rete.

La Sicurezza durante la Navigazione in Rete

- Rischi online: malware, phishing, furto d'identità
- Come riconoscere siti web sicuri (HTTPS, lucchetto)
- Password sicure e gestione delle password
- Importanza degli aggiornamenti software
- Consigli per navigare in sicurezza (non condividere informazioni personali, attenzione ai link)



Rischi online: malware, phishing, furto d'identità

I rischi online sono in costante aumento e possono avere conseguenze devastanti per la tua vita digitale e reale. Ecco una panoramica dettagliata dei tre rischi principali: malware, phishing e furto d'identità:

1. Malware (Software Maligno):

- **Definizione:**
  - Il malware è un termine generico che indica software progettato per danneggiare o compromettere sistemi informatici.
  - Esistono diverse tipologie di malware, tra cui virus, worm, trojan, ransomware e spyware.
- **Rischi:**
  - Danneggiamento o cancellazione di file.
  - Furto di dati personali e finanziari.
  - Controllo remoto del tuo dispositivo.
  - Ricatto tramite ransomware (richiesta di denaro per sbloccare i file).
- **Prevenzione:**
  - Installa un software antivirus e antimalware affidabile e mantienilo aggiornato.
  - Evita di scaricare file o aprire allegati da fonti sconosciute.
  - Mantieni aggiornato il tuo sistema operativo e le tue applicazioni.
  - Esegui scansioni regolari del tuo sistema.

Rischi online: malware, phishing, furto d'identità

2. Phishing:

- **Definizione:**
  - Il phishing è una tecnica fraudolenta utilizzata per ingannare le persone e indurle a rivelare informazioni personali, come password, numeri di carta di credito o dati bancari.
  - I truffatori si spacciano per entità legittime (banche, aziende, social media) tramite email, messaggi o siti web falsi.
- **Rischi:**
  - Furto di dati personali e finanziari.
  - Perdita di denaro.
  - Furto d'identità.
- **Prevenzione:**
  - Sii cauto con email e messaggi sospetti.
  - Non cliccare su link o allegati da mittenti sconosciuti.
  - Verifica sempre l'URL dei siti web (cerca "HTTPS" e il lucchetto).
  - Non fornire mai informazioni sensibili tramite email o messaggi.

Rischi online: malware, phishing, furto d'identità

3.Furto d'Identità:

- **Definizione:**
  - Il furto d'identità si verifica quando qualcuno ruba le tue informazioni personali e le utilizza per scopi fraudolenti.
  - I truffatori possono utilizzare i tuoi dati per aprire conti bancari, ottenere prestiti, effettuare acquisti o commettere altri crimini a tuo nome.
- **Rischi:**
  - Danni finanziari.
  - Danni alla reputazione.
  - Problemi legali.
- **Prevenzione:**
  - Proteggi le tue informazioni personali (documenti, password, dati bancari).
  - Sii cauto con i social media e le informazioni che condividi online.
  - Monitora regolarmente i tuoi conti bancari e le tue carte di credito.
  - Utilizza password forti e uniche per ogni account.
  - Abilita l'autenticazione a due fattori(2FA) quando possibile.

Consigli generali:

- Sii sempre vigile e cauto online.
- Non condividere mai informazioni personali con persone o siti web sconosciuti.
- Utilizza software di sicurezza affidabile.
- Mantieni aggiornati i tuoi dispositivi e le tue applicazioni.
- In caso di dubbi, contatta le autorità competenti.

Come riconoscere siti web sicuri (HTTPS, lucchetto)

Riconoscere un sito web sicuro è fondamentale per proteggere i tuoi dati personali e finanziari durante la navigazione online. Ecco i principali indicatori di sicurezza:

1. HTTPS (Hypertext Transfer Protocol Secure):

- **Cos'è:**
  - HTTPS è un protocollo di comunicazione sicuro che crittografa i dati scambiati tra il tuo browser e il server del sito web.
  - Questo impedisce a terzi di intercettare e leggere le tue informazioni sensibili.
- **Come riconoscerlo:**
  - L'URL del sito web inizia con "https://".
  - La maggior parte dei browser moderni visualizza un'icona a forma di lucchetto accanto all'URL.

2. Lucchetto:

- **Cos'è:**
  - L'icona del lucchetto indica che il sito web utilizza un certificato SSL/TLS (Secure Sockets Layer/Transport Layer Security).
  - Questo certificato conferma l'identità del sito web e garantisce che la connessione sia crittografata.
- **Come interpretarlo:**
  - Cliccando sul lucchetto, puoi visualizzare informazioni sul certificato, come l'autorità di certificazione e la validità.
  - Un lucchetto chiuso e verde (o grigio, a seconda del browser) indica una connessione sicura.
  - Un lucchetto con un punto esclamativo o un avviso indica potenziali problemi di sicurezza.

Come riconoscere siti web sicuri (HTTPS, lucchetto)

3. Altri indicatori di sicurezza:

- **Informazioni di contatto:**
  - Un sito web affidabile dovrebbe fornire informazioni di contatto chiare, come un indirizzo fisico, un numero di telefono e un indirizzo email.
- **Politica sulla privacy:**
  - Verifica che il sito web abbia una politica sulla privacy che spieghi come vengono raccolti e utilizzati i tuoi dati.
- **Recensioni e valutazioni:**
  - Cerca recensioni e valutazioni del sito web online per verificare la sua reputazione.
- **Aspetto professionale:**
  - Un sito web sicuro e affidabile di solito ha un aspetto professionale, con un design curato e contenuti privi di errori grammaticali.
- **Certificati di sicurezza:**
  - alcuni siti web, soprattutto quelli di e-commerce, mostrano dei sigilli di fiducia, che certificano che il sito ha superato dei controlli di sicurezza.

Importante:

- La presenza di HTTPS e del lucchetto non garantisce al 100% la sicurezza del sito web.
- I truffatori possono creare siti web falsi con certificati SSL.
- Sii sempre cauto e verifica l'identità del sito web, soprattutto quando inserisci informazioni sensibili.

Password sicure e gestione delle password

1. Caratteristiche di una Password Sicura:

- **Lunghezza:**
  - Una password dovrebbe essere lunga almeno 12-16 caratteri. Più lunga è, più difficile sarà da decifrare.
- **Metodi:**
  - Utilizza una combinazione di:
    - Lettere maiuscole e minuscole (A-Z, a-z)
    - Numeri (0-9)
    - Simboli speciali (!@#$%^&* etc.)
    - Non riutilizzare mai la stessa password per account diversi.
    - Evita parole di uso comune, nomi propri, date di nascita o altre informazioni personali facilmente reperibili.
    - Abilita 2FA dove possibile per aggiungere un ulteriore livello di sicurezza.
    - 2FA richiede un secondo fattore di autenticazione (es. codice inviato tramite SMS, app di autenticazione) oltre alla password.
    -

Importanza degli aggiornamenti software

Gli aggiornamenti software sono fondamentali per la sicurezza e il corretto funzionamento dei tuoi dispositivi e applicazioni. Ecco perché sono così importanti:

1. Correzione di Vulnerabilità di Sicurezza:

- I produttori di software rilasciano regolarmente aggiornamenti per correggere vulnerabilità di sicurezza (bug) che potrebbero essere sfruttate da hacker e malware.
- Mantenere aggiornato il software riduce il rischio di attacchi informatici, furto di dati e infezioni da malware.
- Molti attacchi informatici di successo sfruttano vulnerabilità note che sono state già corrette dagli aggiornamenti.

2. Miglioramento delle Prestazioni:

- Gli aggiornamenti software spesso includono ottimizzazioni che migliorano le prestazioni e la stabilità delle applicazioni e dei sistemi operativi.
- Questo può tradursi in un funzionamento più veloce, efficiente e fluido dei tuoi dispositivi.
- Gli aggiornamenti possono anche risolvere bug e problemi che causano blocchi, crash o rallentamenti.
- Gli aggiornamenti software possono introdurre nuove funzionalità, miglioramenti e interfacce utente aggiornate.
- Gli aggiornamenti software spesso includono definizioni di virus aggiornate e miglioramenti nei sistemi di protezione contro malware e virus.

Consigli per navigare in sicurezza (non condividere informazioni personali, attenzione ai link)

Navigare in sicurezza online è essenziale per proteggere la tua privacy e i tuoi dati personali. Ecco alcuni consigli fondamentali:

1. Protezione delle Informazioni Personali:

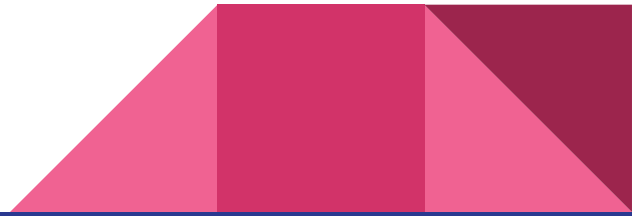
- **Minimizza la Condivisione:**
  - Evita di condividere informazioni personali sensibili (nome completo, indirizzo, numero di telefono, dati finanziari) su siti web, social media o tramite email, a meno che non sia strettamente necessario e il sito sia affidabile.
  - Sii cauto nel condividere informazioni personali sui social media. Imposta le impostazioni sulla privacy per limitare chi può vedere i tuoi post.
- **Verifica l'Autenticità:**
  - Non fornire mai informazioni personali a siti web o persone che non conosci o di cui non ti fidi.
  - Verifica sempre l'autenticità di email, messaggi o chiamate che richiedono informazioni personali.

2. Attenzione ai Link e agli Allegati:

- **Link Sospetti:**
  - Non cliccare su link sospetti o da fonti sconosciute, soprattutto in email, messaggi o annunci pubblicitari.
  - Prima di cliccare su un link, passa il mouse sopra di esso per visualizzare l'URL di destinazione. Verifica che sia un sito web legittimo.
  - Non aprire allegati di email da mittenti sconosciuti o sospetti.
  - Fai attenzione ai file con estensioni eseguibili (.exe, .bat, .vbs), che possono contenere malware.
  - Verifica sempre l'URL e cerca il simbolo del lucchetto (HTTPS) nella barra degli indirizzi.

Usare il Browser - Primi Passi

- Cosa sono i browser e quali sono i più comuni (Chrome, Firefox, Safari, Edge)
- Interfaccia del browser: barra degli indirizzi, barra dei menu, barra dei segnalibri
- Come aprire un sito web
- Come navigare tra le pagine



Cosa sono i browser e quali sono i più comuni

(Chrome, Firefox, Safari, Edge)

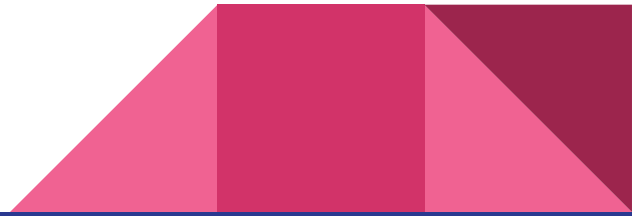
Un browser, o browser web, è un'applicazione software che consente agli utenti di visualizzare pagine web e interagire con i contenuti presenti su Internet. In pratica, è lo strumento che utilizziamo per navigare sul web, accedere a siti web, guardare video, leggere notizie e molto altro.

I browser interpretano il codice HTML, CSS e JavaScript delle pagine web e lo trasformano in un'interfaccia grafica comprensibile all'utente. Oltre alla visualizzazione di pagine web, i browser offrono diverse funzionalità, tra cui:

- **Navigazione tramite link:** Cliccando sui link, è possibile passare da una pagina web all'altra.
- **Gestione dei segnalibri:** Permette di salvare i siti web preferiti per accedervi rapidamente.
- **Cronologia di navigazione:** Registra i siti web visitati in precedenza.
- **Gestione dei cookie:** Memorizza piccoli file di testo che i siti web utilizzano per tracciare le preferenze dell'utente.
- **Estensioni:** Offrono funzionalità aggiuntive al browser, come blocchi pubblicitari, gestori di password e strumenti di traduzione.

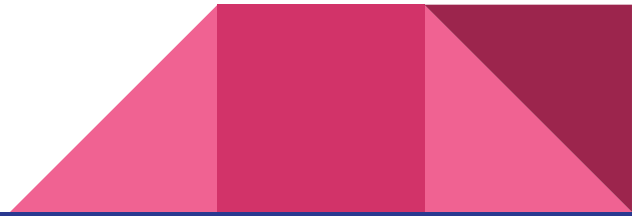
Finestre e Schede del Browser

- Come aprire nuove finestre e schede
- Come organizzare le schede (raggruppamento, blocco)
- Modalità di navigazione in incognito



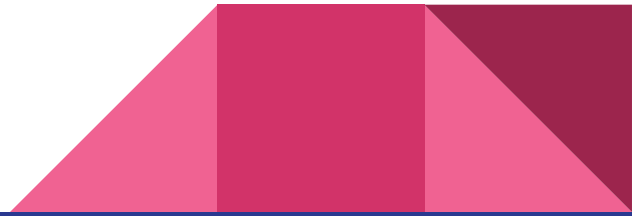
Configurare il Browser

- Impostazioni di base: pagina iniziale, motore di ricerca predefinito
- Gestione dei cookie e della privacy
- Estensioni e componenti aggiuntivi utili
- Aggiornamenti del browser



Gli Strumenti del Browser - La Cronologia

- Come visualizzare e cancellare la cronologia
- Importanza della cronologia per ritrovare siti visitati
- Impostazioni della cronologia

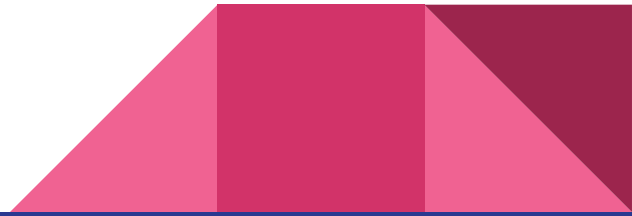


Gestire i Preferiti (Segnalibri)

- Come aggiungere e organizzare i preferiti
- Come creare cartelle per i preferiti
- Sincronizzazione dei preferiti tra dispositivi

Strumenti di Interazione con il Web

- Moduli web e come compilarli
- Download e upload di file
- Uso dei social media tramite browser
- traduzione delle pagine web



Eseguire Ricerche sul Web - I Motori di Ricerca

- Come funzionano i motori di ricerca
- Tecniche di ricerca avanzata (parole chiave, operatori booleani)
- I motori di ricerca più popolari (Google, Bing, DuckDuckGo)

Valutare le Informazioni sul Web

- Come riconoscere fonti affidabili
- Verifica delle informazioni (fact-checking)
- Rischi delle fake news e della disinformazione
- come capire se un sito è sicuro

Usare la Posta Elettronica - Nozioni di Base

- Cos'è la posta elettronica e come funziona
- Indirizzi email e struttura dei messaggi
- Client di posta elettronica (Gmail, Outlook, Yahoo Mail) e webmail
- differenza tra POP3 e IMAP

Cos'è la posta elettronica e come funziona

La posta elettronica, comunemente chiamata email, è un servizio di comunicazione digitale che permette agli utenti di scambiarsi messaggi attraverso Internet. Funziona in modo simile alla posta tradizionale, ma con la differenza che i messaggi vengono inviati e ricevuti in formato digitale.

Come funziona:

1. **Indirizzo email:** Ogni utente ha un indirizzo email univoco, composto da un nome utente, il simbolo "@" e il nome del dominio del fornitore di posta elettronica (ad esempio, [indirizzo email rimosso]).
2. **Server di posta:** I messaggi email vengono inviati e ricevuti attraverso server di posta, che sono computer specializzati nella gestione del traffico email.
3. **Invio di un'email:** Quando un utente invia un'email, il messaggio viene inviato al server di posta del mittente, che lo inoltra al server di posta del destinatario.
4. **Ricezione di un'email:** Il server di posta del destinatario memorizza il messaggio finché il destinatario non lo scarica utilizzando un client di posta elettronica (come Outlook, Gmail o l'app Mail del telefono).
5. **Protocolli email:** I server di posta utilizzano protocolli specifici per comunicare tra loro e con i client di posta. I protocolli più comuni sono:
    - **SMTP (Simple Mail Transfer Protocol):** utilizzato per l'invio di email.
    - **POP3 (Post Office Protocol 3):** utilizzato per scaricare le email dal server al client.
    - **IMAP (Internet Message Access Protocol):** utilizzato per accedere alle email sul server senza scaricarle.

Differenza tra POP3 e IMAP

POP3 (Post Office Protocol 3) e IMAP (Internet Message Access Protocol) sono entrambi protocolli utilizzati per la ricezione di email, ma funzionano in modo diverso:

POP3:

- **Scaricamento delle email:** POP3 scarica le email dal server al dispositivo dell'utente (computer, smartphone, ecc.) e, per impostazione predefinita, le cancella dal server.
- **Accesso offline:** Una volta scaricate, le email sono disponibili offline sul dispositivo.
- **Utilizzo singolo dispositivo:** POP3 è progettato per l'utilizzo su un singolo dispositivo.
- **Spazio server:** Libera spazio sul server una volta scaricate le email.
- **Cartelle:** Le cartelle di posta sono gestite localmente sul dispositivo.

IMAP:

- **Sincronizzazione delle email:** IMAP sincronizza le email tra il server e i dispositivi dell'utente, mantenendo una copia delle email sul server.
- **Accesso da più dispositivi:** IMAP consente di accedere alle email da più dispositivi, con le modifiche sincronizzate tra tutti i dispositivi.
- **Accesso online:** Le email sono accessibili online, anche se è possibile scaricarle per la visualizzazione offline.
- **Spazio server:** Le email rimangono sul server, occupando spazio di archiviazione.
- **Cartelle:** Le cartelle di posta sono gestite sul server, con le modifiche sincronizzate tra i dispositivi.
- Se si utilizza un solo dispositivo per accedere alla posta e si desidera avere le email disponibili offline, POP3 può essere una buona opzione.
- Se si accede alla posta da più dispositivi e si desidera mantenere le email sincronizzate, IMAP è la scelta migliore.

Oggi, IMAP è generalmente preferito per la sua flessibilità e la capacità di sincronizzare le email tra più dispositivi.

Inviare le Email

- Come scrivere e inviare un'email
- Allegare file
- Utilizzare la copia carbone (CC) e la copia carbone nascosta (CCN)
- etichetta della posta elettronica

Strumenti della Posta Elettronica

- Gestione della posta in arrivo (filtri, etichette)
- Creazione di contatti e rubriche
- Calendario e promemoria
- Antispam