

Parte 1: Introduzione a Internet

1.1 Cos'è Internet?

Internet è una **rete globale di computer interconnessi** che comunicano e scambiano dati e informazioni utilizzando un linguaggio comune. È definita come una **rete di reti**, in quanto mette insieme diverse reti di computer locali.

Ecco alcuni aspetti chiave di Internet:

- **Infrastruttura:** Internet è costituita da computer, cavi, e dispositivi fisici collegati tra loro. Comprende anche server che forniscono servizi e risorse agli utenti.
- **Comunicazione:** Permette a milioni di utenti in tutto il mondo di collegarsi tra loro e scambiare documenti, immagini, messaggi e altri tipi di file.
- **Servizi:** Internet offre una varietà di servizi tra cui la posta elettronica (e-mail), il World Wide Web (WWW), l'e-commerce, l'e-learning, il download e l'upload di file, l'home banking, la messaggistica istantanea (IM), il telelavoro, il Voip (Voice Over Internet Protocol), videochiamate, feed RSS, blog, forum e streaming TV.
- **World Wide Web (WWW):** Il WWW è un sistema di informazioni organizzate in pagine ipertestuali, che contengono testo, immagini, video e link ad altre pagine. Il WWW è uno dei servizi più noti e utilizzati di Internet.
- **Nascita e sviluppo:** Internet ha avuto origine come rete militare chiamata ARPANET, creata dal Dipartimento della Difesa degli Stati Uniti durante la Guerra Fredda. Successivamente, è stata resa disponibile alle università per la diffusione di dati e informazioni scientifiche, diventando quella che conosciamo oggi.
- **Accesso:** L'accesso a Internet avviene tramite diversi tipi di connessione, come linea telefonica tradizionale, reti 3G/4G, connessioni via cavo, connessioni wireless (Wi-Fi), Wi-max e connessioni via satellite.

Altri aspetti importanti:

- **Indirizzi:** Ogni risorsa su Internet è identificata da un URL (Uniform Resource Locator), che specifica il tipo di protocollo, l'indirizzo del computer, il percorso e il nome della risorsa.
- **Browser:** Per navigare in Internet è necessario un browser, un programma che interpreta il codice HTML delle pagine web. Esempi di browser sono Internet Explorer, Firefox, Chrome e Safari.
- **Motori di ricerca:** I motori di ricerca sono siti web specifici che permettono di trovare informazioni sul web a partire da parole chiave. Esempi di motori di ricerca sono Google, Yahoo! e Bing.

- **Sicurezza:** Navigare in Internet comporta dei rischi, per cui è importante utilizzare password sicure, firewall e software antivirus per proteggere i propri dati e dispositivi. La crittografia è una tecnica per rendere incomprensibili i dati a chi non è autorizzato.

In sintesi, Internet è una vasta rete di computer interconnessi che offre una vasta gamma di servizi e opportunità, ma richiede anche consapevolezza e attenzione alla sicurezza.

Esercizio 1 - Terminologia di Base

Abbina ogni termine alla sua definizione:

1. URL
2. HTTP
3. Browser
4. DNS
5. IP Address

- (a) Sistema che traduce i nomi di dominio in indirizzi IP.
- (b) Protocollo utilizzato per la comunicazione tra browser e siti web.
- (c) Indirizzo univoco assegnato a un dispositivo su Internet.
- (d) Programma utilizzato per navigare sul web.
- (e) Indirizzo web di una risorsa su Internet.

(Trovi le soluzioni alla fine della dispensa)

Parte 2: Navigazione Web

2.1 Browser e Motori di Ricerca

Browser e motori di ricerca, le loro funzioni e differenze.

Browser:

- Un **browser** è un'applicazione software progettata per **interpretare il codice HTML** (HyperText Markup Language) delle pagine web e visualizzarle in un formato comprensibile.
- I browser permettono agli utenti di **navigare in Internet** e accedere ai contenuti del World Wide Web (WWW).
- Sono essenziali per la **visualizzazione** di testi, immagini, video e altri contenuti multimediali presenti nelle pagine web.
- Esempi comuni di browser includono **Microsoft Internet Explorer, Mozilla Firefox, Google Chrome e Apple Safari.**

- I browser possono essere **personalizzati** con barre degli strumenti e impostazioni per soddisfare le esigenze dell'utente.
- I browser memorizzano informazioni sulla navigazione, come **cronologia** e **cookie**, per migliorare l'esperienza utente. Queste informazioni possono essere eliminate per proteggere la privacy dell'utente.
- I browser offrono **funzionalità di sicurezza** come il blocco dei popup e la navigazione in incognito.
- I browser consentono anche di **salvare** i contenuti delle pagine web, come testo, immagini e video.

Motori di ricerca:

- Un **motore di ricerca** è un sito web specializzato che permette di **trovare informazioni** sul web a partire da parole chiave.
- I motori di ricerca sono **enormi archivi di dati** riguardanti miliardi di pagine web.
- Aggiornano costantemente le loro informazioni tramite programmi chiamati "spider".
- I motori di ricerca principali sono **Google, Yahoo! e Bing**.
- Gli utenti inseriscono **parole chiave** in una casella di ricerca per ottenere risultati pertinenti.
- I risultati di una ricerca vengono visualizzati come un **elenco di link** a pagine web che contengono le parole chiave.
- I motori di ricerca offrono **opzioni di ricerca avanzata** per restringere o ampliare i risultati in base a vari criteri.
- Possono essere utilizzati **operatori logici** come AND, OR e NOT per raffinare le ricerche.
- È possibile utilizzare i motori di ricerca per effettuare ricerche all'interno di **enciclopedie e dizionari online**.

Differenze chiave:

- Il **browser** è lo strumento che **visualizza le pagine web**, mentre il **motore di ricerca** è lo strumento che **aiuta a trovare le pagine web** in base a parole chiave.
- Il **browser** è un software installato sul computer, mentre il **motore di ricerca** è un sito web.
- Un browser può essere utilizzato per visitare qualsiasi sito web, mentre un motore di ricerca è specializzato nella ricerca di informazioni.

In sintesi, i **browser** sono necessari per accedere e visualizzare i contenuti del web, mentre i **motori di ricerca** sono fondamentali per trovare le informazioni rilevanti tra le miliardi di pagine disponibili online. Entrambi sono strumenti cruciali per la navigazione e l'utilizzo di Internet.

Esercizio 2 - Ricerca Online

1. Apri un motore di ricerca e cerca informazioni su "cos'è la crittografia online".
2. Trova un sito web ufficiale che spieghi il concetto di "VPN" e annotane l'URL.

(T trovi le soluzioni alla fine della dispensa)

Parte 3: Sicurezza Online

3.1 Minacce Informatiche

Phishing, malware e password deboli, come queste minacce possono compromettere la sicurezza dei dati personali e dei dispositivi.

Phishing:

- Il **phishing** è una **frode online** utilizzata per **sottrarre informazioni personali** come numeri di carte di credito, password e dati di account.
- I truffatori inviano **email o messaggi istantanei** che sembrano provenire da organizzazioni legittime, come banche o società di carte di credito, chiedendo di fornire informazioni personali.
- Spesso queste comunicazioni contengono un **link a un sito web falso**, che imita l'aspetto di un sito legittimo, inducendo la vittima a inserire i propri dati personali, che verranno poi utilizzati dai criminali.
- Il termine "phishing" deriva dall'assonanza con il termine inglese "fishing" (pescare), poiché i truffatori cercano di "pescare" le informazioni delle vittime con l'inganno.
- Le email di phishing possono ad esempio richiedere di "verificare un conto", "ripristinare password scadute", o riscuotere premi.
- È importante **non cliccare su link sospetti** e **verificare sempre l'attendibilità del mittente** prima di fornire informazioni personali.
- Il **filtro SmartScreen** di Internet Explorer aiuta a identificare i siti di phishing e a proteggere l'utente.

Malware:

- Il termine **malware** è l'abbreviazione di "malicious software", ovvero **software dannoso**.
- I malware sono programmi che vengono installati **senza il consenso dell'utente** con l'obiettivo di **danneggiare il software o l'hardware del computer, rubare dati o compiere azioni illegittime**.
- Un **virus** è un tipo di malware che si replica e si diffonde infettando altri file e programmi. Per attivarsi, un virus necessita di un'azione da parte dell'utente.
- Un **worm** è un tipo di malware che si diffonde automaticamente senza l'intervento dell'utente, attraverso le reti informatiche.
- Un **trojan** (o "cavallo di Troia") è un malware che si nasconde all'interno di programmi legittimi e, una volta eseguito, avvia azioni dannose all'insaputa dell'utente.
- Uno **spyware** è un malware che raccoglie informazioni sulle attività dell'utente e le trasmette a terzi, spesso per scopi pubblicitari o fraudolenti.
- Altri tipi di malware includono **adware, botnet, keylogger, dialer e ransomware**.

- I malware possono entrare nel computer attraverso **allegati di posta elettronica, download da siti web non sicuri, chiavette USB infette** e altri mezzi di comunicazione.
- Per difendersi dai malware è fondamentale utilizzare un **software antivirus e antimalware** aggiornato, eseguire scansioni periodiche e prestare attenzione ai file scaricati o agli allegati delle email.

Password deboli:

- Le **password deboli** sono combinazioni facili da indovinare o da forzare con attacchi automatici.
- Utilizzare password deboli è uno dei principali fattori di rischio per la sicurezza dei dati e degli account.
- Le password deboli spesso includono informazioni personali, parole comuni, sequenze di tasti o sono troppo corte.
- Una **password sicura** dovrebbe essere **lunga (almeno 8-10 caratteri, preferibilmente 14 o più), complessa (combinando lettere maiuscole e minuscole, numeri e simboli), non facilmente associabile all'utente e unica per ogni account.**
- È fondamentale **non riutilizzare la stessa password** per più account e **cambiarla regolarmente**, soprattutto in caso di dati sensibili.
- L'autenticazione tramite **nome utente e password** è fondamentale per accedere a reti aziendali, computer personali, posta elettronica, servizi di home banking e messaggistica istantanea.

In sintesi, **phishing, malware e password deboli** sono minacce significative alla sicurezza informatica. È importante essere consapevoli di questi rischi e adottare misure di protezione appropriate per evitare furti di dati, danni ai dispositivi e compromissione della privacy.

Esercizio 3 - Identificazione delle Minacce

Indica se le seguenti situazioni sono **sicure (S)** o **non sicure (NS)**:

1. Ricevi un'email che ti chiede di inserire i tuoi dati bancari. (** __)
2. Stai visitando un sito HTTPS per un acquisto online. (** __)
3. Hai la stessa password per tutti i tuoi account. (** __)
4. Utilizzi un antivirus aggiornato. (** __)

(Trovi le soluzioni alla fine della dispensa)

Parte 4: Comunicazione Online

4.1 Email e Social Media

Certamente, ecco una spiegazione dettagliata basata sulle fonti fornite, riguardo all'email e ai social media:

Email (posta elettronica):

- Un'e-mail, o posta elettronica, è un **servizio di comunicazione** che consente di inviare e ricevere messaggi digitali tramite Internet. È uno dei servizi più importanti offerti da Internet.
- L'e-mail è paragonabile alla posta tradizionale, dove un mittente invia un messaggio a un destinatario, ed entrambi hanno un indirizzo che li identifica.
- Un indirizzo e-mail è composto da **nomeutente@nomeprovider.suffisso**. Il nome utente identifica l'utente in modo univoco, il nome provider indica il fornitore del servizio di posta, e il suffisso specifica il dominio di appartenenza.
- **Vantaggi dell'e-mail:**
 - Possibilità di inviare un numero illimitato di messaggi al costo della connessione internet.
 - Invio contemporaneo a più destinatari.
 - Archiviazione dei messaggi sia per il mittente che per il destinatario.
 - Notifica immediata in caso di mancato recapito.
 - Possibilità di creare una rubrica di indirizzi.
 - Possibilità di allegare file di diversi formati, come documenti, immagini e programmi.
- **Modalità di visualizzazione e invio:**
 - **Posta offline:** si utilizza un programma specifico (es. Outlook) e si scarica la posta per visualizzare i messaggi anche senza connessione.
 - **Posta online:** si usano servizi offerti dai provider e si accede alla posta tramite browser, necessitando di una connessione per qualsiasi attività. Gmail è un esempio di servizio di posta elettronica fornito da Google.
- **Protocolli:** Le email utilizzano protocolli come **POP3** (Post Office Protocol version 3) e **IMAP** (Internet Message Access Protocol) per gestire l'invio e la ricezione dei messaggi. Questi protocolli sono utilizzati dai client di posta per scaricare i messaggi dai server.
- **Rischi:** le email possono essere veicolo di diffusione di malware, come virus e worm, e possono essere utilizzate per tentativi di phishing o truffe. È importante non aprire allegati da mittenti sconosciuti. Inoltre, i messaggi di posta elettronica sono normalmente inviati in chiaro e possono essere intercettati se non vengono adottate misure di sicurezza come la crittografia.

Social media:

- I **social media** sono strumenti online che permettono di creare, condividere e scambiare contenuti, favorendo il confronto e il dialogo tra gli utenti.
- Rientrano nei social media le reti sociali (social network), i blog, i forum, i gruppi di discussione e le comunità di condivisione di contenuti.

- Le **reti sociali** (social network) sono tra i più diffusi strumenti di social media e permettono lo scambio di informazioni e dati tra utenti tramite un sistema di amicizie reciproche. Esempi comuni sono Facebook, Twitter, LinkedIn e Google+.
- I social network permettono di creare pagine personali per condividere la propria vita con altre persone, connettersi e instaurare nuove relazioni.
- **Blog**: siti internet dove un utente condivide pubblicazioni personali, organizzate in ordine temporale.
- **Forum**: spazi di discussione dove gli utenti possono condividere opinioni su argomenti specifici.
- **Comunità virtuali**: ambienti online dove le persone possono interagire, scambiare informazioni, giocare e partecipare a dibattiti.
- **Importanza della privacy**:
 - È essenziale proteggere i propri dati personali sui social media, in quanto le informazioni condivise potrebbero cadere in mano a malintenzionati.
 - Bisogna prestare attenzione a ciò che si pubblica, perché le informazioni diventano disponibili a un vasto pubblico.
 - Le reti sociali offrono impostazioni per la privacy che permettono di controllare chi può vedere le informazioni e chi può contattare l'utente.
 - È importante impostare la privacy in modo che i dati siano visibili solo ai propri contatti e utilizzare la messaggistica privata.
 - Non è consigliabile divulgare pubblicamente dati personali come indirizzo, numero di telefono o email.
 - È importante bloccare utenti sconosciuti ed evitare di accettare richieste di amicizia da persone non conosciute.
- **Rischi**: l'uso dei social media può comportare rischi come adescamento, cyberbullismo e furto di identità. È importante essere consapevoli di tali rischi e utilizzare i social media in modo responsabile.
- **Microblogging**: servizio che permette di scrivere brevi messaggi testuali, come Twitter.

In sintesi, le email sono uno strumento di comunicazione digitale essenziale per lo scambio di messaggi, mentre i social media sono piattaforme per la connessione e l'interazione tra persone. Entrambi offrono numerosi vantaggi, ma richiedono consapevolezza dei rischi e attenzione alla sicurezza e alla privacy.

Esercizio 4 - Analisi di un'Email

Leggi l'email seguente e identifica 3 segnali di possibile truffa:

"Gentile utente, abbiamo notato attività sospette nel tuo conto. Clicca qui per confermare i tuoi dati."

(Trove le soluzioni alla fine della dispensa)

Parte 5: Gestione della Privacy

5.1 Protezione dei Dati Personali

Ecco una spiegazione dettagliata basata sulle fonti fornite, riguardo all'uso di password complesse e univoche, all'attivazione dell'autenticazione a due fattori (2FA) e al controllo delle impostazioni di privacy nei social network:

Password complesse e univoche:

- Le **password** sono stringhe di caratteri utilizzate per l'**autenticazione**, dimostrando l'identità dell'utente e garantendo l'accesso a una risorsa.
- Una **password complessa** è fondamentale per proteggere i propri dati e account.
- Una password efficace dovrebbe essere:
 - **Lunga**: idealmente 14 o più caratteri.
 - **Composta da lettere maiuscole e minuscole, numeri e simboli**.
 - **Non facilmente associabile alla vita dell'utente**. Non usare nomi, cognomi, soprannomi, date di nascita o indirizzi.
 - **Non contenere sequenze di tasti** o parole comuni.
 - **Unica per ogni account. Non riutilizzare la stessa password** per più account.
- **Evitare password deboli**, che sono facili da indovinare o forzare con attacchi automatici. Le password deboli includono informazioni personali, parole comuni, sequenze di tasti o sono troppo corte.
- **Cambiare regolarmente le password**, soprattutto per i dati sensibili.
- La sicurezza dei dati dipende dalla **forza della password**.
- È cruciale **conservare le password in modo sicuro** e non comunicarle a terzi non autorizzati.

Autenticazione a due fattori (2FA):

- L'**autenticazione a due fattori (2FA)**, o autenticazione a più fattori, è un metodo di sicurezza che aggiunge un ulteriore livello di protezione all'accesso a un account o risorsa online.
- Oltre alla password, che è il primo fattore di autenticazione (qualcosa che si conosce), la 2FA richiede un secondo fattore, come un **codice generato da un'app, un SMS, un token hardware o un'impronta digitale** (qualcosa che si ha o si è).
- Anche se un malintenzionato riesce ad entrare in possesso della password, non potrà accedere all'account senza il secondo fattore.
- La 2FA è una protezione molto utile contro il phishing e altre forme di attacco che possono compromettere la password.

Controllo delle impostazioni di privacy nei social network:

- I **social network** offrono impostazioni di privacy per controllare chi può vedere le informazioni e chi può contattare l'utente.
- È fondamentale **gestire attentamente queste impostazioni** per proteggere la propria privacy e prevenire abusi.
- **Impostazioni generali sulla privacy:**
 - **Chi può vedere i miei post:** si può scegliere di rendere i post pubblici, visibili solo agli amici, solo a se stessi, o solo agli amici degli amici.
 - **Chi può contattarmi:** si può limitare la possibilità di inviare messaggi o richieste di amicizia solo a persone selezionate o agli amici in comune.
 - **Blocco utenti:** si possono bloccare persone indesiderate per impedirgli di interagire.
- **Impostazioni specifiche per singoli contenuti:**
 - Si può impostare la privacy per le singole foto, video o post, decidendo chi può vederli.
- **Controllo delle applicazioni:** è bene verificare quali applicazioni possono accedere ai propri dati.
- È importante **non divulgare pubblicamente informazioni personali** come indirizzo, numero di telefono o email.
- Si consiglia di **usare la messaggistica privata** per comunicazioni personali.
- È necessario **bloccare utenti sconosciuti ed evitare di accettare richieste di amicizia da persone non conosciute.**
- Molti programmi di messaggistica istantanea consentono di creare profili. È meglio **ignorare questa opzione o non includere alcuna informazione di identificazione o fotografia** per proteggere la privacy.

In sintesi, l'utilizzo di password complesse e univoche, l'attivazione dell'autenticazione a due fattori (2FA) e un attento controllo delle impostazioni di privacy sui social network sono misure fondamentali per proteggere i propri dati personali e la propria privacy online.

Esercizio 5 - Creazione di una Password Sicura

Crea una password sicura che contenga almeno:

- 10 caratteri
- Una lettera maiuscola
- Un numero
- Un carattere speciale

Scrivila qui (senza condividerla con nessuno!):

Conclusione e Simulazione d'Esame

Esercizio 6 - Quiz Finale

1. Quale protocollo garantisce una connessione sicura?
 - a) HTTP
 - b) HTTPS
 - c) FTP
2. Qual è un segno comune di phishing?
 - a) Email con grammatica scorretta
 - b) Email di amici conosciuti
 - c) Offerte di sconti reali
3. Quale delle seguenti pratiche aumenta la sicurezza online?
 - a) Usare la stessa password per tutti gli account
 - b) Abilitare il 2FA
 - c) Condividere la password con gli amici

(Trove le soluzioni alla fine della dispensa)

Risposte agli esercizi

1. e - b - d - a - c
2. Ricerca online personale.
3. NS - S - NS - S
4. Email di phishing: link sospetti, tono allarmistico, richiesta di dati personali.
5. Password sicura creata dallo studente.
6. 1 - b, 2 - a, 3 - b.