ABNUT

Amici
Biblioteca
Nazionale
Universitaria
Torino

Corso gratuito

Il Computer: un po' di teoria e tanta pratica

A cura di
Giovanni Vagnone di Trofarello e Celle

RETRO CONSULTING GROUP

LEZIONE 2

I principali social a scopo di intrattenimento: fruire e creare contenuti in un contesto di algoritmi in cui siamo il prodotto

Che cosa sono i Social Media?

I social media sono piattaforme digitali che consentono agli utenti di creare contenuti, condividere informazioni e interagire tra loro tramite connessioni virtuali. (Qualche cenno sui meccanismi psicologici che sfruttano)

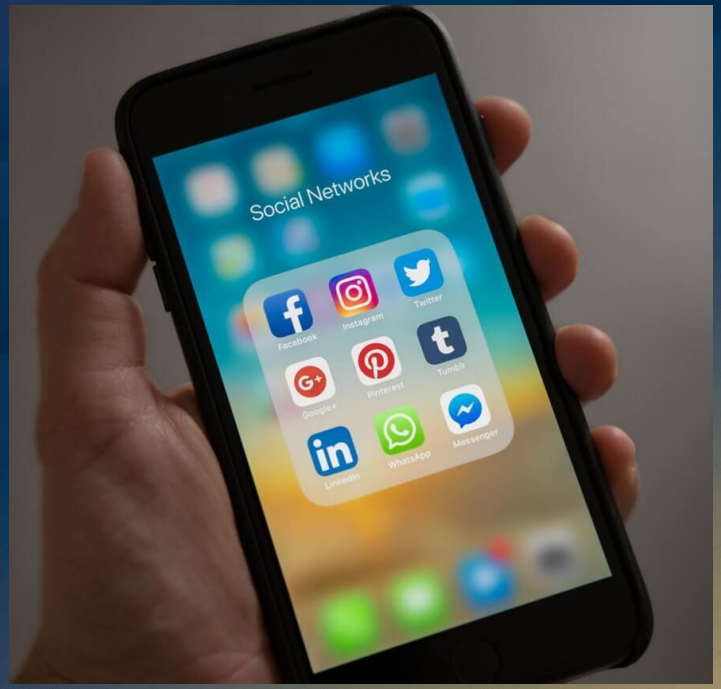
Facebook: Una piattaforma dove gli utenti possono condividere foto, aggiornamenti di stato e partecipare a gruppi di discussione.

Twitter: Nota per i suoi brevi messaggi chiamati "tweet", è ideale per le notizie in tempo reale e la comunicazione diretta con figure pubbliche e marchi.

Instagram: Focalizzata sulla condivisione di foto e video, è molto popolare tra gli artisti e le personalità per mostrare visivamente le loro attività.

LinkedIn: Utilizzata principalmente per le connessioni professionali e per la condivisione di esperienze lavorative e opportunità di carriera.

TikTok: Piattaforma di contenuti video fatti da “creator” che possono guadagnare dalle visualizzazioni: algoritmo molto adattivo sull’utilizzo, facile assuefazione.



Perché i Social Media sono importanti?

Comunicazione Globale: I social media eliminano le barriere geografiche permettendo a chiunque di connettersi con persone in tutto il mondo.

Fonte di Informazioni: Molti si rivolgono ai social media per ricevere aggiornamenti in tempo reale su eventi, notizie e tendenze.

Supporto e Comunità: Offrono la possibilità di trovare gruppi e comunità di interesse comune, fornendo supporto, intrattenimento e compagnia.

Impatto Sociale e Culturale: Hanno il potere di influenzare l'opinione pubblica e mobilizzare le masse, come dimostrato in eventi globali e movimenti sociali.

Creare e Gestire Password Forti

Importanza delle Password: Una password forte è la prima difesa contro l'accesso non autorizzato ai vostri account.

Creazione di una Password Forte:

1. **Lunghezza:** Assicurarsi che la password sia lunga almeno 12 caratteri.
2. **Complessità:** Utilizzare una combinazione di lettere maiuscole, minuscole, numeri e simboli.
3. **Unicità:** Non riutilizzare le stesse password per account diversi.
4. **Strumenti di Aiuto:** Considerare l'utilizzo di un gestore di password per generare e memorizzare password complesse in modo sicuro.

Impostazioni di Privacy e Segnali di Allarme

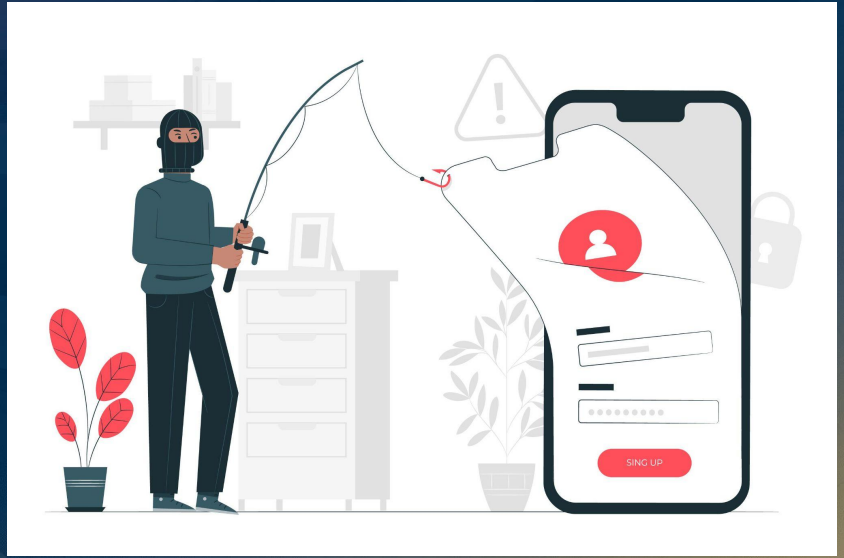
Impostazioni di Privacy:

Accesso: Verificare e personalizzare chi può vedere i vostri post e le vostre informazioni su ogni piattaforma.

Guida: Utilizzo delle guide passo-passo disponibili per ogni social media per configurare correttamente le impostazioni di privacy.

Segnali di Allarme di Sicurezza:

- **Phishing:** Email o messaggi che richiedono informazioni personali o finanziarie, spesso con un tono urgente.
- **Link Sospetti:** Non cliccare mai su link non richiesti o che sembrano sospetti, anche se provengono da amici.
- **Offerte Troppo Belle per Essere Vere:** Ignorare annunci o messaggi che promettono premi incredibili senza alcun impegno.
- **Profili clonati:** da segnalare



Tipi Comuni di Truffe sui Social Media

Truffe Romantiche:

Sceneggiatura: "Innamorato/a perdutamente di te dopo tre messaggi? Può sembrare un romanzo, ma è probabilmente un trucco per alleggerire il portafoglio!" (elementi psicologici che concorrono al raggiro)

Segnale d'Allarme: Dichiarazioni d'amore premature seguite da richieste di soldi per "emergenze improvvise".

Truffe legate a Falsi Investimenti:

Sceneggiatura: "Investi solo 100 euro e diventa milionario! Sembra un gioco da ragazzi, ma è più probabile che l'unico a guadagnare sia il truffatore!"

Segnale d'Allarme: Promesse di guadagni esorbitanti con minimi investimenti e zero rischi.

Truffe di Falsi Concorsi:

Sceneggiatura: "Congratulazioni, hai vinto un iPhone! Clicca qui per ritirarlo... e dire addio ai tuoi dati personali."

Segnale d'Allarme: Premi grandi annunciati via messaggi o email che richiedono di pagare una "tassa" o di fornire dati personali per ricevere il premio.

Cosa Fare se si Sospetta una Truffa

ABNUT
Amici Biblioteca Nazionale Universitaria Torino

Fermati Prima di Agire:

- **Regola d'Oro:** "Se sembra troppo bello per essere vero, probabilmente non lo è!"
- **Passo Prudente:** Prenditi il tempo di riflettere e discutine con un amico o un familiare.

Verifica l'Autenticità:

- **Indagine:** Ricerca su internet per recensioni o segnalazioni di truffe simili.
- **Sospetto?:** Controlla il profilo del mittente – spesso i truffatori hanno profili recenti o poco dettagliati.

Segnalazione:

Azione Responsabile: Segnala il profilo sospetto ai social media e, se appropriato, alle autorità locali o a organizzazioni come la polizia postale.

Cosa Sono i Dati Personali e Come vengono Raccolti

ABNUT
Amici
Biblioteca
Nazionale
Universitaria
Torino

Qualsiasi informazione che può identificarti direttamente o indirettamente, come nome, email, indirizzo, età, preferenze personali e cronologia di navigazione.

Esempi di Raccolta di Dati:

- **Social Media:** Registrazione delle attività, quali post che piacciono, commenti, luoghi visitati e ricerche.
- **Shopping Online:** Preferenze di acquisto e comportamenti di spesa.
- **App di Fitness:** Dati sulla salute e sull'attività fisica.

Se è Gratis, Il Prodotto Sei Tu!

ABNUT
Amici Biblioteca Nazionale Universitaria Torino

Uso dei Dati per Pubblicità Mirata:

- Le aziende analizzano i tuoi dati per capire le tue abitudini e preferenze, così da mostrarti pubblicità su misura—più efficaci e quindi più redditizie.
- Le aziende hanno speso globalmente oltre 455 miliardi di dollari in pubblicità digitale nel 2021, gran parte dei quali destinata a pubblicità basata sui dati degli utenti.
- **"Quando non paghi per il prodotto, il prodotto sei tu."** - Questo spiega come i servizi gratuiti online monetizzino i dati degli utenti.

Proteggere i Propri Dati Personali

ABNUT
Amici
Biblioteca
Nazionale
Universitaria
Torino

Consigli Pratici:

- **Leggi le Politiche di Privacy:** Sì, possono essere lunghe e complesse, ma è essenziale sapere cosa accetti.
- **Impostazioni di Privacy:** Regola le impostazioni di privacy sui social media per limitare chi può vedere i tuoi dati e come possono essere utilizzati.
- **Prudenza con le App:** Sii selettivo su quali app scaricare e quali autorizzazioni concedere. Chiediti: "Hanno davvero bisogno di accedere alla mia posizione o ai miei contatti?"
- **Mantenere Aggiornato il Software:** Aggiornamenti frequenti aiutano a proteggere i dati da vulnerabilità di sicurezza note.

Netiquette, come comportarsi (1)

1. Diffusione di Informazioni False o Fuorvianti

- **Rischi:** Contribuire alla diffusione di notizie false può creare confusione, panico o reazioni inappropriate.
- **Netiquette:** Verificare sempre l'autenticità delle informazioni prima di condividerle. Utilizzare fonti affidabili e controllare da più fonti.

2. Violazione della Privacy Altrui

- **Rischi:** Condividere informazioni personali di altri senza consenso può esporre queste persone a rischi di sicurezza o danneggiarne la reputazione.
- **Netiquette:** Chiedere sempre il permesso prima di postare foto o informazioni che coinvolgono altre persone.

3. Interazioni Inappropriate

- **Rischi:** Commenti offensivi o discorsi d'odio possono portare a conseguenze legali, oltre a danneggiare le relazioni interpersonali.
- **Netiquette:** Mantenere un tono rispettoso e costruttivo nei commenti e nelle discussioni. Evitare linguaggio offensivo o denigratorio.

Netiquette, come comportarsi (2)

ABNUT
Amici Biblioteca Nazionale Universitaria Torino

4. Sopravvalutazione della Propria Privacy

- **Rischi:** Assumere che la propria attività sui social sia privata può portare a condividere informazioni sensibili che possono essere usate a scopo fraudolento o malevolo..
- **Netiquette:** Essere consapevoli delle impostazioni di privacy e assicurarsi di comprendere chi può vedere i propri contenuti.

2. Dipendenza dai Social Media

- **Rischi:** L'uso eccessivo può portare a isolamento sociale, ansia e disturbi del sonno.
- **Netiquette:** Promuovere un uso equilibrato dei social media, riconoscendo l'importanza di mantenere relazioni nella vita reale e limitando il tempo trascorso online.

6. Mancato rispetto della diversità

- **Rischi:** Commenti o contenuti che non rispettano la diversità possono non solo ferire gli altri ma anche limitare la propria capacità di interagire in un ambiente globale.
- **Netiquette:** Celebrare la diversità e evitare generalizzazioni o stereotipi su basi etniche, religiose, di genere o altre.

Non siate “boomer”

- **Scrivere correttamente:** non rivelate di non vederci bene, o di non essere confidenti con l’uso di tastiere da smartphone, mettendo punti invece di spazi, o scrivendo in un italiano poco corretto, si nota subito.
- **Adattati agli Emoji:** Usa gli emoji con moderazione e cerca di capire il loro significato attuale. Evita di usare emoticon vecchio stile (es. :-)).
- **Tieniti Aggiornato con le Tendenze:** Segui influencer o pagine che trattano di tendenze attuali per restare aggiornato su ciò che è popolare.
- **Linguaggio e Abbreviazioni Moderne:** Impara e usa le abbreviazioni comuni come LOL (laugh out loud - ridere ad alta voce) e BRB (be right back - torno subito), ma evita di esagerare.
- **Presta Attenzione alla Qualità dei Contenuti:** Condividi foto e video di alta qualità. Le immagini sfocate o mal tagliate possono sembrare antiquate.
- **Evita Argomenti Triti e Ritriti:** Parla di argomenti attuali e vari. Non limitarti a temi come il meteo o ricette, a meno che non siano presentati in chiave moderna e originale.
- **Interazione Attiva e Positiva:** Commenta e interagisci con gli altri in modo costruttivo e attuale, mostrando apertura verso nuove idee e culture.

Non siate “boomer”