



CREW

Creativity, Resilience,
Empowerment for Work



IO1 CORSO DI FORMAZIONE
NELL'ALFABETO DIGITALE



- 04 Obiettivi e finalità di IO1
- 05 Modulo 1 - Teoria e metodologia dell'alfabetizzazione digitale
- Acquisizione delle informazioni
 - Valutazione delle informazioni
 - Creazione di informazioni digitali come processo di apprendimento
- 13 Modulo 2 - Sviluppo delle competenze maggiori
- L'alfabetizzazione digitale come approccio culturale
 - Ridurre l'ansia sviluppando le competenze digitali e l'insegnamento
 - Concetto di consumatore intelligente
 - Pensiero critico e tecniche di valutazione
 - Percezione culturale e comprensione sociale
 - Creazione, gestione e implicazioni dell'identità virtuale
- 40 Modulo 3 - Gli strumenti più importanti nell'alfabetizzazione mediatica in generale
- Software di base e strumenti di comunicazione
 - Motori di ricerca
 - E-mail
 - Social network
 - Software aziendale
 - Sviluppo siti web, blogging e marketing
 - Narrazione personale
 - Firma elettronica e servizi elettronici
 - Software di sicurezza
 - Sicurezza e hardware del dispositivo fisico
 - Internet delle cose (IoT)

76	Modulo 4 - Esempi, casi di studio e precauzioni contro cui sviluppare la resilienza
	<ul style="list-style-type: none">• Violazioni della privacy e furto di dati• Hacking ed estorsioni informatiche• Furti di identità• Cyber bullismo• Tecniche di phishing• Reati finanziari e frodi sugli investimenti• Notizie false e propaganda• Pubblicità fraudolenta (prodotti contraffatti, integratori)• PC/giochi online, casinò, dipendenza
109	Modulo 5 - Ruolo del governo e istituzioni a cui candidarsi
	<ul style="list-style-type: none">• Regolamento e-privacy nell'UE• GDPR e CCPA• Autorità statali per la protezione dei dati
118	Modulo 6 - Strumenti di autovalutazione
	<ul style="list-style-type: none">• Evita la "crisi" di metà carriera: rimani aggiornato sulla tecnologia• Giochi e app interattivi
122	Bibliografia



Obiettivi e finalità di IO1

Internet è diventato una merce nel XXI secolo, quasi come l'olio, il grano o lo zucchero. È l'ingrediente principale per l'esistenza dei servizi in molti settori, come la finanza, la salute, il marketing, l'intrattenimento, l'istruzione. Internet è una sorta di materia prima o una struttura stessa, che viene utilizzata come materiale da costruzione per una varietà di altri servizi ed ecosistemi, che si evolvono attorno ad essa.

Man mano che gli strumenti digitali e online si evolvono rapidamente, si fondono e producono una gamma ancora più ampia di servizi e prodotti innovativi, mentre i dispositivi utilizzati nelle attività quotidiane personali e pubbliche diventano più veloci, ampiamente adottati e connessi, le competenze di alfabetizzazione digitale diventano essenziali nella costruzione della carriera e concorrenza vincente nel mercato del lavoro. Il costante sviluppo delle competenze, l'impegno significativo e propositivo nel mondo digitale, la capacità di consumare, valutare e creare le informazioni su Internet, rimanendo allo stesso tempo al sicuro e resilienti contro informazioni false e di bassa qualità - tutto ciò non è da meno importanza.

Man mano che gli strumenti digitali e online si evolvono rapidamente, si fondono e producono una gamma ancora più ampia di servizi e prodotti innovativi, mentre i dispositivi utilizzati nelle attività quotidiane personali e pubbliche diventano più veloci, ampiamente adottati e connessi, le competenze di alfabetizzazione digitale diventano essenziali nella costruzione della carriera e concorrenza vincente nel mercato del lavoro. Il costante sviluppo delle competenze, l'impegno significativo e propositivo nel mondo digitale, la capacità di consumare, valutare e creare le informazioni su Internet, rimanendo allo stesso tempo al sicuro e resilienti contro informazioni false e di bassa qualità - tutto ciò non è da meno importanza.

Pertanto, l'obiettivo di questo corso è quello di aiutare ad estendere le competenze di base già possedute dagli individui migliorando le loro competenze complessive di alfabetizzazione digitale e responsabilizzandoli per un ulteriore sviluppo, aiutando le persone con competenze tecniche inferiori a combattere la loro ansia nel miglioramento delle competenze digitali. Questo corso è rivolto a studenti adulti meno competenti, aiutandoli a essere più coinvolti nella società e nel mercato del lavoro, nonché a educatori, organizzazioni e istituzioni che organizzano corsi di apprendimento, coinvolti nell'insegnamento e nella formazione dell'alfabetizzazione digitale e delle materie correlate, che possono beneficiare utilizzando i nostri corsi per i loro scopi didattici.

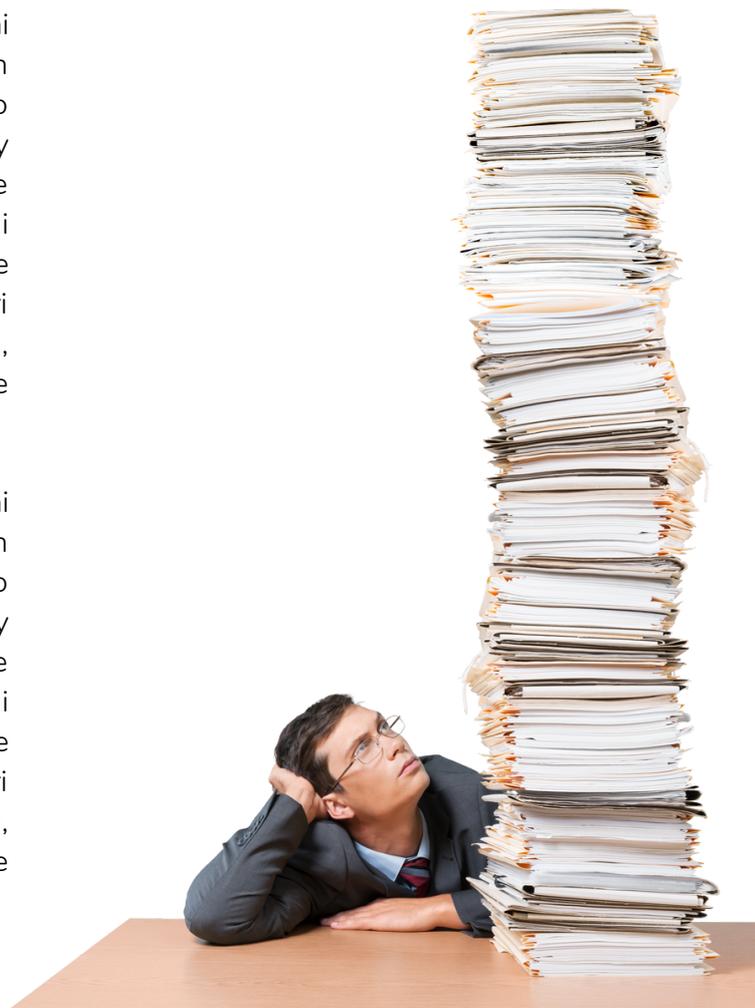


TEORIA E METODOLOGIA DELL'ALFABETIZZAZIONE DIGITALE

1.1 ACQUISIZIONE DI INFORMAZIONI

Anche se il termine di acquisizione delle informazioni non è qualcosa di nuovo, crea nuove percezioni in un mondo così ampiamente connesso all'inizio del terzo decennio del XXI secolo. L'American Library Association (ALA, 1989) definisce l'alfabetizzazione informativa come la capacità di accertare quali informazioni sono necessarie, comprendere come vengono preparate le informazioni, trovare le migliori fonti di informazione per una data esigenza, identificare tali fonti, valutare analiticamente le fonti e condividere queste informazioni.

Anche se il termine di acquisizione delle informazioni non è qualcosa di nuovo, crea nuove percezioni in un mondo così ampiamente connesso all'inizio del terzo decennio del XXI secolo. L'American Library Association (ALA, 1989) definisce l'alfabetizzazione informativa come la capacità di accertare quali informazioni sono necessarie, comprendere come vengono preparate le informazioni, trovare le migliori fonti di informazione per una data esigenza, identificare tali fonti, valutare analiticamente le fonti e condividere queste informazioni.



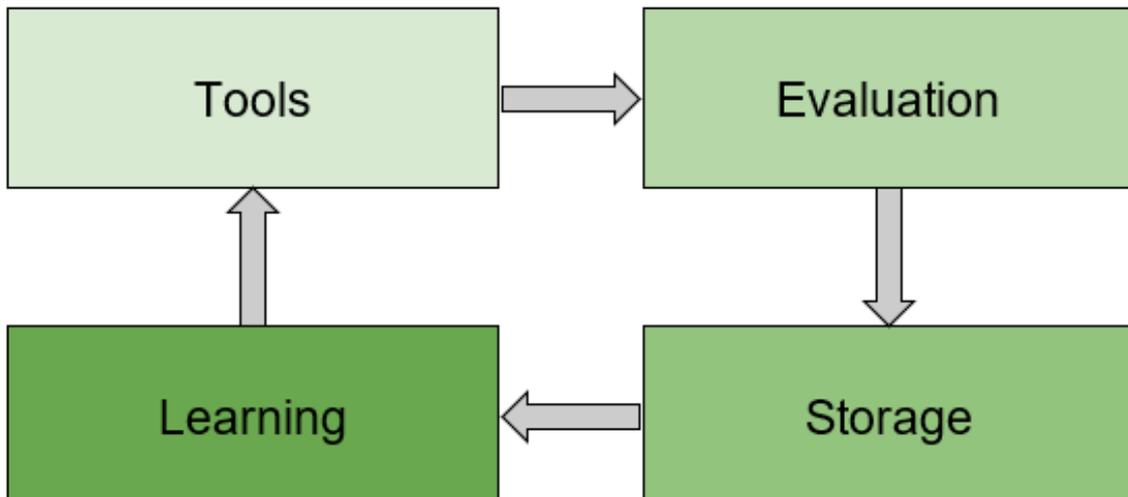
Ci atteniamo alle basi e sottolineiamo i seguenti pilastri principali di cosa sia l'acquisizione di informazioni nell'ambito dell'alfabetizzazione digitale:

1. E' saper utilizzare correttamente gli strumenti online per acquisire informazioni;
2. Valutare criticamente le informazioni e filtrare attraverso fonti di informazione irrilevanti di bassa qualità;
3. Essere in grado di archiviare e gestire in modo sicuro le informazioni acquisite;
4. Acquisire la nuova conoscenza stessa ed essere in grado di sviluppare continuamente nuove competenze e continuare ad apprendere senza sosta per acquisire informazioni di maggiore e migliore qualità.





Figura 1.1. Un'illustrazione del ciclo continuo di acquisizione delle informazioni e miglioramento della qualità



Gli strumenti di base per acquisire le informazioni digitalizzate sono generalmente abbastanza conosciuti e popolari:

- Google e altri motori di ricerca
- Wikipedia
- Google e altri motori di ricerca
- Social media - Facebook, Twitter, LinkedIn
- Google e altri motori di ricerca

L'archiviazione delle informazioni è un argomento piuttosto tecnico, quindi tratteremo argomenti quali sicurezza, affidabilità e best practice o argomenti correlati per l'archiviazione delle informazioni in ulteriori capitoli.

La parte di valutazione è fondamentale per sviluppare le competenze digitali necessarie; pertanto, approfondiremo questo argomento nel prossimo capitolo.

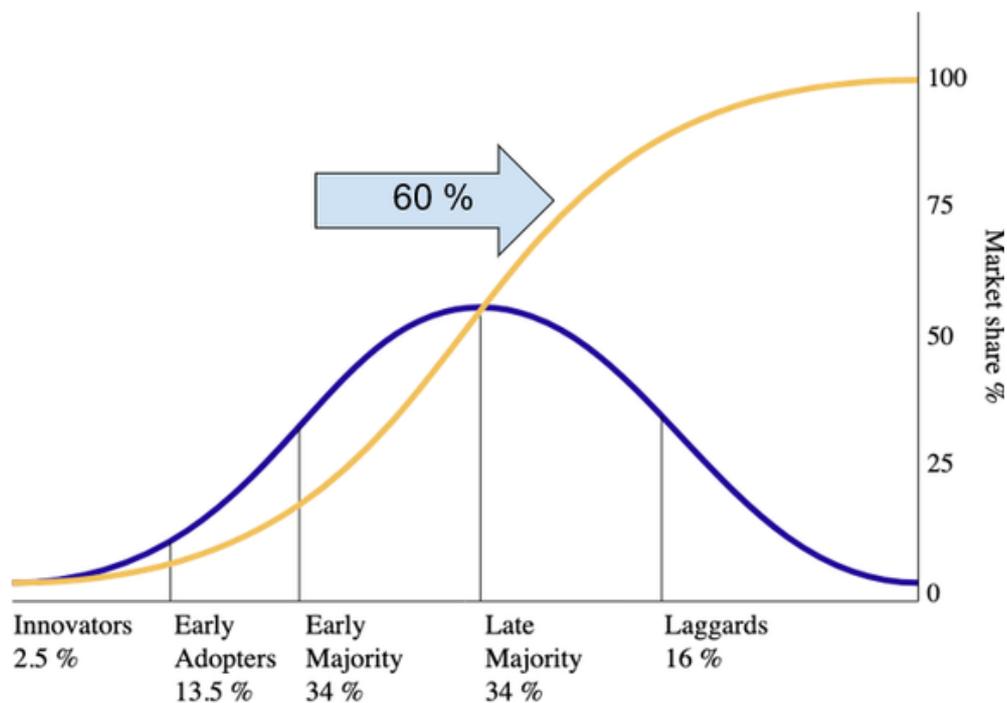
Qual è l'attuale adozione di quanto Internet è al momento?

Secondo il modello di diffusione delle innovazioni di Everett Rogers, che può essere usato per descrivere bene l'evoluzione e l'adozione di qualsiasi tecnologia, siamo ancora lontani dall'adozione di Internet in tutto il mondo.

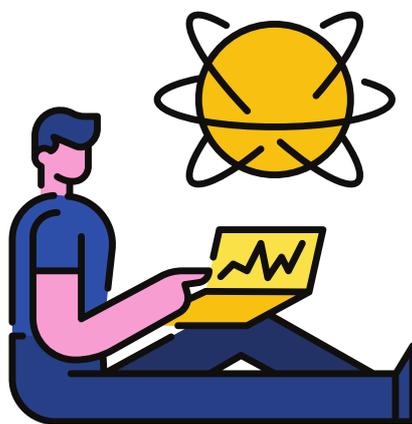




Figura 1.2. Adozione di Internet basata su una penetrazione di Internet pari al 60% nel 2021
[fonte: Statista.com]



Nonostante l'adozione disomogenea di Internet in tutto il mondo, possiamo ancora considerare gli strumenti digitali e la connessione a Internet come il principale fattore positivo per diffondere le idee, educare le persone, combattere la povertà e la disoccupazione.





1.2 VALUTAZIONE INFORMAZIONI

Perché dobbiamo valutare le informazioni?

Una volta trovate le informazioni che corrispondono all'argomento e ai requisiti della tua ricerca, dovresti analizzare o valutare queste fonti di informazioni. La valutazione delle informazioni ti incoraggia a pensare in modo critico all'affidabilità, alla validità, all'accuratezza, all'autorità, alla tempestività, al punto di vista o ai pregiudizi delle fonti di informazione.

Solo perché un libro, un articolo o un sito web corrisponde ai tuoi criteri di ricerca e quindi sembra, a prima vista, essere rilevante per la tua ricerca, non significa che sia necessariamente una fonte di informazioni affidabile. È importante ricordare che le fonti di informazione che compongono le raccolte cartacee ed elettroniche della Biblioteca sono già state valutate per l'inclusione tra le risorse della Biblioteca. Tuttavia, questo non significa necessariamente che queste fonti siano rilevanti per la tua ricerca.

Ciò non si applica necessariamente alle fonti di informazione sul Web per il pubblico in generale. Molti di noi con account Internet/Web sono potenziali editori di siti web; la maggior parte di questi contenuti è pubblicata senza revisione editoriale. Pensaci. Sono disponibili molte risorse per aiutare nella valutazione delle pagine web.



Il modo più semplice per valutare le informazioni è porre domande appropriate. Quali criteri dovresti usare per giudicare le fonti di informazione?

1. Inizialmente, guarda l'autore, il titolo, l'editore e la data di pubblicazione. Queste informazioni possono essere trovate nella citazione bibliografica e possono essere determinate anche prima di avere l'elemento fisico in mano.
2. Quindi, guarda il contenuto, ad es. pubblico previsto, obiettività della scrittura, copertura, stile di scrittura e, se disponibili, recensioni valutative.





Ad esempio, dovrebbero essere poste le seguenti domande per valutare passo dopo passo la qualità delle informazioni:

Chi è l'autore (può essere un individuo o un'organizzazione) e/o editore?

1. Chi è l'autore (può essere un individuo o un'organizzazione) e/o editore?
2. Quanto sono obiettivi, affidabili e autorevoli?
3. Hanno scritto altri articoli o libri?
4. L'autore o gli autori sono elencati con le informazioni di contatto (indirizzo civico, e-mail)?
5. L'editore ha pubblicato altre opere?
6. Sono specializzati nella pubblicazione di determinati argomenti o campi?
7. L'editore è accademico (stampa universitaria, associazioni accademiche)? Commerciale? Agenzia governativa? Self ("vanità") stampa?



Cosa si può dire del contenuto, del contesto, dello stile, della struttura, della completezza e dell'accuratezza delle informazioni fornite dalla fonte?

1. Vengono offerte conclusioni? In caso affermativo, sulla base di quali evidenze e supportate da quale documentazione primaria e secondaria?
2. Cosa implica il contenuto?
3. Sono rappresentate prospettive diverse?
4. Il contenuto è pertinente alle tue esigenze di informazione?



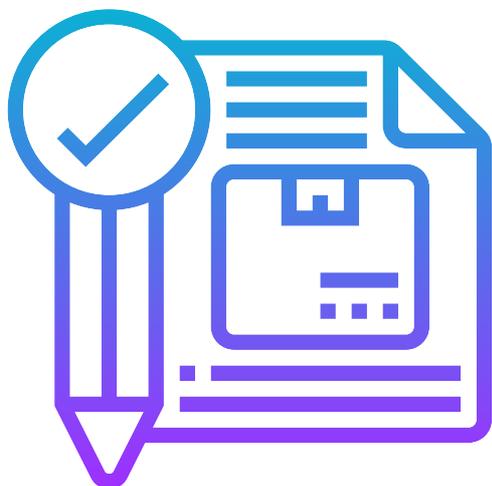


Quando sono state pubblicate le informazioni?

1. La data di pubblicazione si trova generalmente sul frontespizio o sul retro del frontespizio (data del copyright).
2. Le informazioni fornite dalla fonte sono nella loro forma originale o sono state riviste per riflettere i cambiamenti nelle conoscenze?
3. Queste informazioni sono tempestive e vengono aggiornate regolarmente?

Dove altro si possono trovare le informazioni fornite dalla fonte?

1. Queste informazioni sono autentiche?
2. Queste informazioni sono uniche o sono state copiate?
3. Perché sono state pubblicate le informazioni fornite dalla fonte?



Qual è il contesto intorno a queste informazioni?

1. Quali sono le prospettive, le opinioni, i presupposti e i pregiudizi di chi è responsabile di queste informazioni?
2. Chi è il pubblico previsto?
3. Viene venduto qualcosa?

Una corretta introduzione alla valutazione delle informazioni è fondamentale per ottenere risultati desiderabili per il miglioramento delle competenze di alfabetizzazione digitale, in particolare fornendo agli studenti le indicazioni e le linee guida per il loro auto-miglioramento e autoapprendimento attraverso la pratica.





1.3. LA CREAZIONE DI INFORMAZIONI DIGITALI COME PROCESSO DI APPRENDIMENTO

Le informazioni in qualsiasi formato vengono prodotte per trasmettere un messaggio e vengono condivise tramite un metodo di consegna e distribuzione selezionato. I processi iterativi di ricerca, creazione, revisione e condivisione delle informazioni variano, quindi l'intero processo stesso è una parte importante del processo di apprendimento costante mentre l'informazione viene creata, consumata e distribuita.



Le informazioni in qualsiasi formato vengono prodotte per trasmettere un messaggio e vengono condivise tramite un metodo di consegna e distribuzione selezionato. I processi iterativi di ricerca, creazione, revisione e condivisione delle informazioni variano, quindi l'intero processo stesso è una parte importante del processo di apprendimento costante mentre l'informazione viene creata, consumata e distribuita.

Prendendo la creazione di siti Web come esempio di approccio pratico. Per essere in grado di costruire un sito web, un individuo deve avere conoscenze di base e capacità di utilizzo del computer, che lo aiuterebbe a trovare le istruzioni e i requisiti necessari per la costruzione del sito web. Tali abilità di base possono essere acquisite prima durante l'istruzione formale, tuttavia una conoscenza più approfondita verrà acquisita dopo il completamento delle attività pratiche.

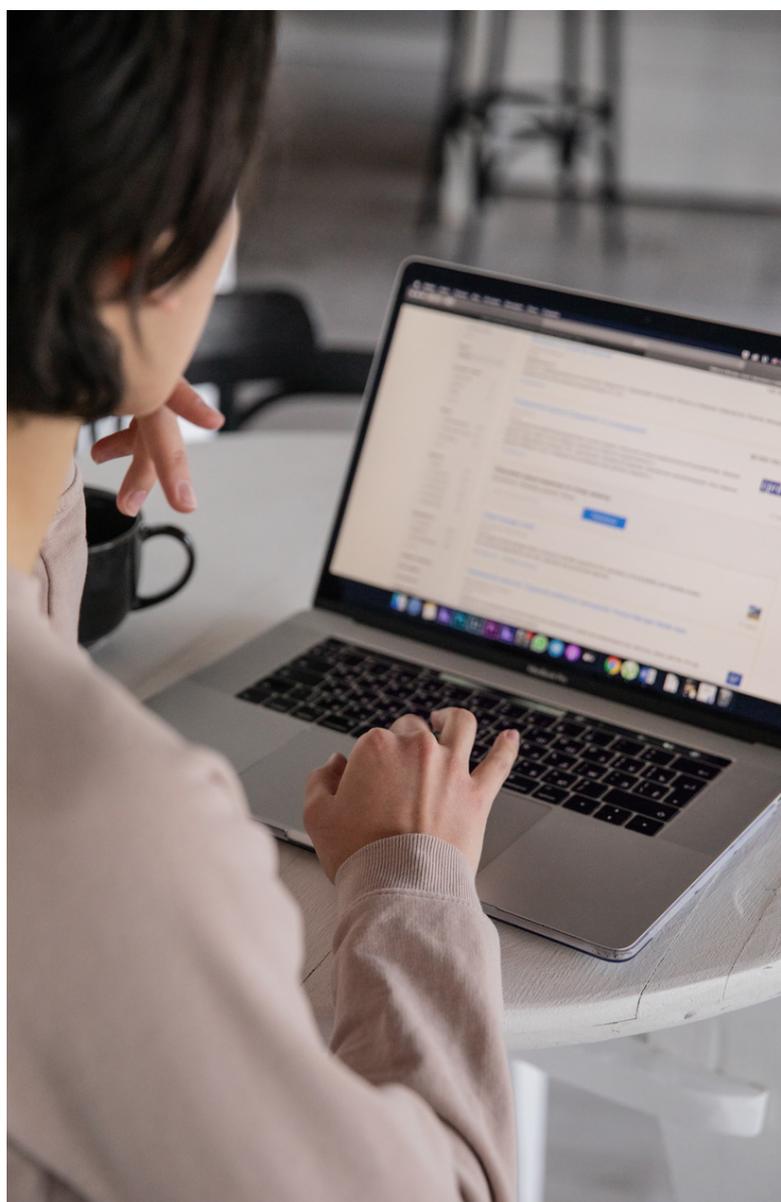




La creazione di siti Web è un compito complesso, che richiede di migliorare le competenze nella ricerca e valutazione delle informazioni, nell'archiviazione, anche nella creazione e distribuzione, quindi sottolineiamo che questo tipo di esercizio è un modo perfettamente adatto per il miglioramento delle competenze digitali. Se necessario, gli esercizi di creazione di siti Web possono comportare marketing e comunicazione, scrittura di articoli di qualità integrati con aggiunte interattive e multimediali, ricerche sul comportamento e sull'esperienza degli utenti di Internet, sicurezza e privacy e come il design, la struttura o le funzionalità di un sito Web possono aiutare a raggiungere il migliori risultati.

Gli studenti possono scegliere di lavorare alla creazione di un blog personale o alla creazione di un semplice sito Web di e-commerce, che li costringe ad acquisire le competenze necessarie in aree quali finanze, creazione di identità digitali, precauzioni contro i crimini informatici, utilizzo della firma elettronica e e-government Servizi. Dovrebbero anche iniziare a considerarsi parte di un processo senza fine sia nella creazione di informazioni che nel consumo di informazioni allo stesso tempo, che amplia la loro percezione nell'alfabetizzazione digitale nel suo insieme.

La nostra raccomandazione metodologica per l'educazione all'alfabetizzazione digitale è quella di utilizzare un approccio pratico alla creazione di siti Web e adattare esercizi particolari in base alle reali competenze, motivazioni e aspettative degli studenti.



2 MODULO



SVILUPPO DELLE PRINCIPALI COMPETENZE

2.1. ALFABETIZZAZIONE DIGITALE COME APPROCCIO CULTURALE

Stiamo assistendo a un periodo di sviluppo tecnologico senza precedenti e ampiamente dirompente. Nel breve tempo dalla creazione di Internet, molto è cambiato, tra cui il design delle interfacce informatiche, la velocità di elaborazione e la portabilità dei dispositivi, l'accessibilità delle informazioni e delle conoscenze, le nostre modalità di comunicazione, il mantenimento delle nostre relazioni, il commercio, la protezione della privacy personale, processi creativi, pubblicazione di contenuti e nascita di nuove tribù digitali e clan virtuali (Wheeler, 2009).



Diversi articoli pubblicati di recente hanno esplorato la nozione di "alfabetizzazione digitale" e, come previsto, ci sono numerosi punti di vista. Anderson (2010), ad esempio, descrive l'alfabetizzazione digitale come la capacità di sfruttare il potenziale delle tecnologie informatiche. Le alfabetizzazioni, in tutte le loro forme, sono allo stesso tempo culturali, sociali e personali (Kress, 2009) e ci consentono di interagire pienamente in culture specifiche. Alcuni avvertono che senza un adeguato livello di alfabetizzazione, i media digitali hanno la capacità di svantaggiare alcuni (van Dijk, 2005), mentre altri mettono in guardia sulla natura del web per minare la conoscenza e la competenza (Carr, 2008; Keen, 2007). Tuttavia, la stragrande maggioranza dei commentatori elogia il potenziale del social web per liberare l'istruzione e democratizzare l'apprendimento, con l'avvertenza che vengono praticate le alfabetizzazioni digitali. La task force sull'alfabetizzazione digitale dell'American Library Association offre questa definizione: "L'alfabetizzazione digitale è la capacità di utilizzare le tecnologie dell'informazione e della comunicazione per trovare, valutare, creare e comunicare informazioni, che richiedono abilità sia cognitive che tecniche".



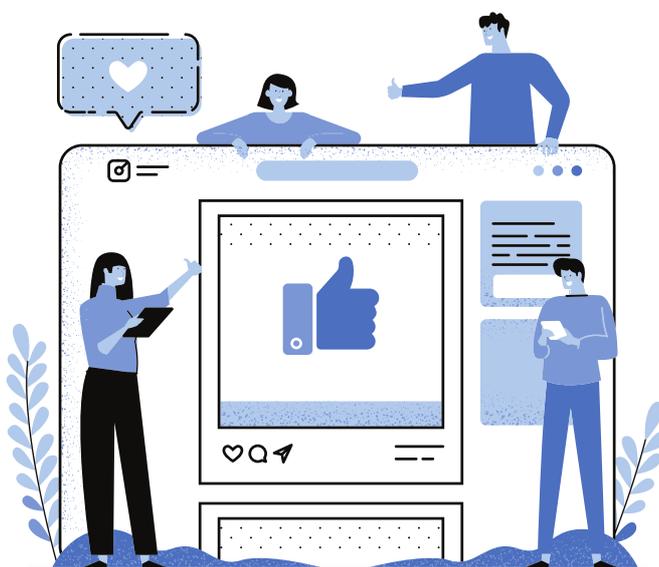


Il termine "alfabetizzazione digitale" è diventato così popolare e diffuso negli ultimi 10 anni che è quasi scontato. Con vari gradi di complessità, l'espressione alfabetizzazione digitale viene ora utilizzata per descrivere i nostri impegni con le tecnologie digitali in quanto mediano molte (se non la maggior parte) delle nostre interazioni sociali.

Con questa definizione di alfabetizzazione digitale dell'American Library Association come luce guida, è importante capire che anche i nativi digitali che sanno come inviare un testo e un post sui social media non sono considerati "alfabetizzati digitalmente" in alcun modo. È importante notare che la semplice lettura online o l'abbonamento a un servizio di eBook non rende uno studente dotato di alfabetizzazione digitale.

Con questa definizione di alfabetizzazione digitale dell'American Library Association come luce guida, è importante capire che anche i nativi digitali che sanno come inviare un testo e un post sui social media non sono considerati "alfabetizzati digitalmente" in alcun modo. È importante notare che la semplice lettura online o l'abbonamento a un servizio di eBook non rende uno studente dotato di alfabetizzazione digitale.

Con questa definizione di alfabetizzazione digitale dell'American Library Association come luce guida, è importante capire che anche i nativi digitali che sanno come inviare un testo e un post sui social media non sono considerati "alfabetizzati digitalmente" in alcun modo. È importante notare che la semplice lettura online o l'abbonamento a un servizio di eBook non rende uno studente dotato di alfabetizzazione digitale.



Sviluppare il tuo pensiero critico è essenziale quando ti trovi di fronte a così tante informazioni in formati diversi: la ricerca, il vaglio, la valutazione, l'applicazione e la produzione di informazioni richiedono tutti un pensiero critico.

Anche la comunicazione è un aspetto chiave dell'alfabetizzazione digitale. Quando si comunica in ambienti virtuali, la capacità di esprimere chiaramente le proprie idee, porre domande pertinenti, mantenere il rispetto e creare fiducia è importante quanto quando si comunica di persona.

Hai anche bisogno di abilità pratiche nell'uso della tecnologia per accedere, gestire, manipolare e creare informazioni in modo etico e sostenibile. È un processo di apprendimento continuo a causa di nuove app e aggiornamenti costanti e devi tenere in ordine la tua vita digitale!





L'alfabetizzazione digitale è molto importante ora e sarà davvero importante nel tuo futuro professionale. Sul posto di lavoro ti viene richiesto di interagire con le persone in ambienti digitali, utilizzare le informazioni in modo appropriato e creare nuove idee e prodotti in modo collaborativo. Soprattutto, devi mantenere la tua identità digitale e il tuo benessere mentre il panorama digitale continua a cambiare a un ritmo veloce.

Come accennato, le competenze digitali si sviluppano attraverso un continuum e vengono costantemente aggiornate in linea con i cambiamenti tecnologici. I quadri delle competenze digitali svolgono un ruolo fondamentale nell'acquisizione della gamma di competenze e di questi cambiamenti, consentendo in tal modo ai responsabili delle politiche e ai fornitori di competenze digitali di garantire che i loro programmi e programmi di formazione rimangano pertinenti e attuali. Molte organizzazioni e agenzie internazionali hanno sviluppato quadri di competenze digitali. Evidenziamo il lavoro della Commissione europea, il Digital Competence Framework for Citizens (o DigComp) che fornisce un linguaggio comune su come identificare e descrivere le aree chiave della competenza digitale e offre quindi un riferimento comune a livello europeo.

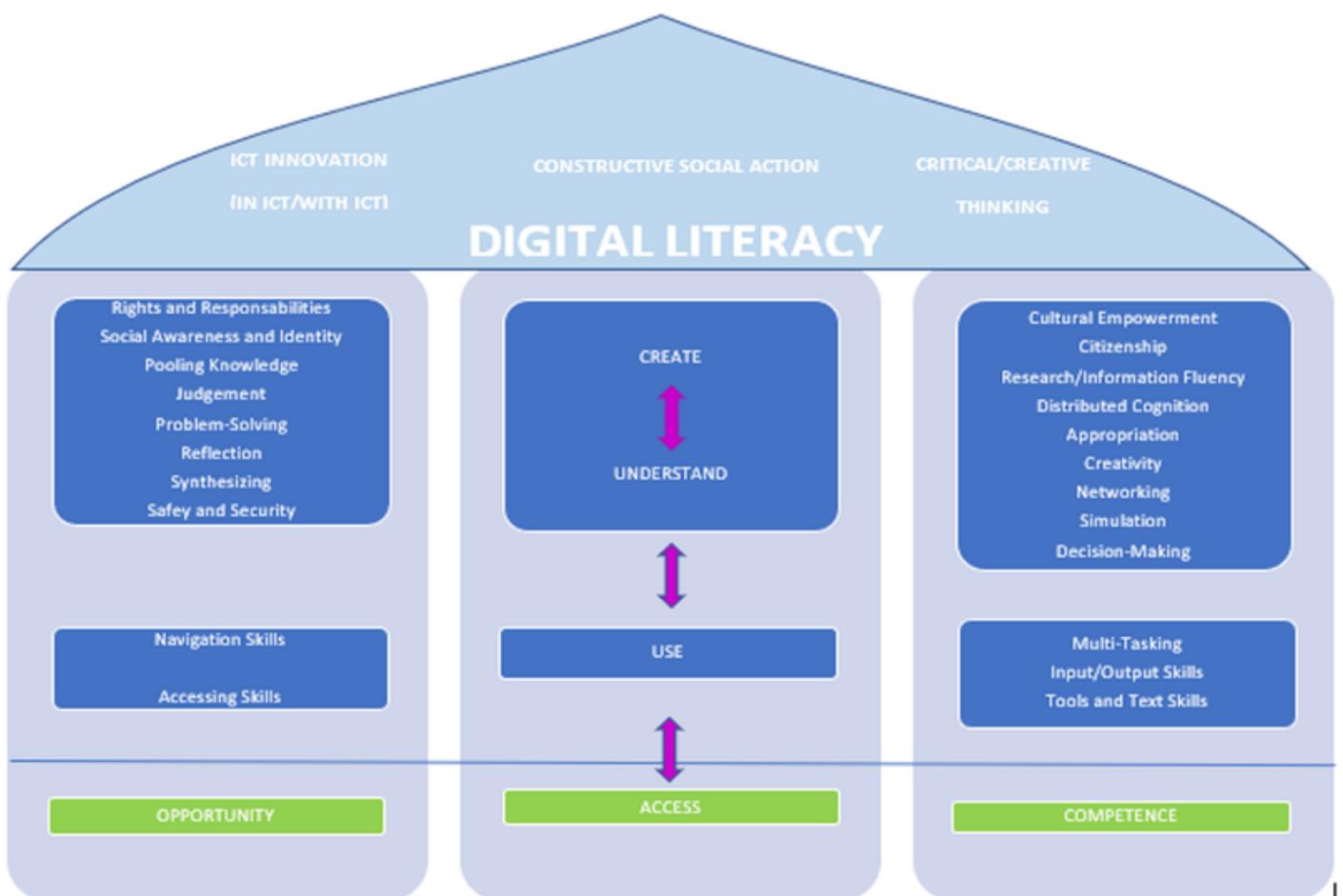
A livello globale, la International Society for Technology in Education (ISTE) inquadra i suoi parametri di riferimento per l'alfabetizzazione digitale intorno a sei standard: creatività e innovazione; comunicazione e collaborazione; scioltezza nella ricerca e nell'informazione; pensiero critico, problem solving e processo decisionale; cittadinanza digitale; e operazioni e concetti tecnologici.

Questo modello mostra i molti elementi interconnessi che rientrano nell'ambito dell'alfabetizzazione digitale. C'è una progressione logica dalle competenze più fondamentali verso i livelli più alti e più trasformativi, ma farlo non è necessariamente un processo sequenziale: molto dipende dalle esigenze dei singoli utenti, dalle vostre esigenze.





Questa cifra si basa sui modelli del Report of the Digital Britain Media Literacy Working Group. (marzo 2009), DigEuLit – a European Framework for Digital Literacy (2005) e Jenkins et al., (2006) Confronting the Challenges of Participatory Culture: Media Education for the 21st Century.



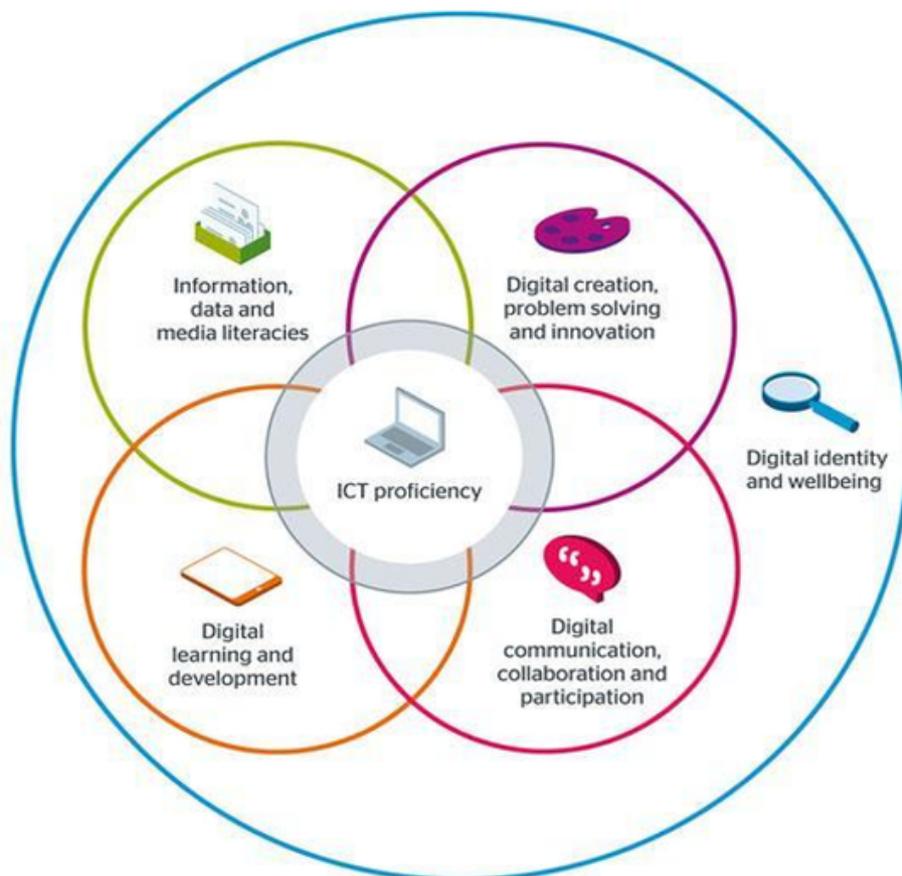
Quali sono gli elementi che ti rendono digitalmente alfabetizzato?

L'alfabetizzazione digitale va oltre le competenze informatiche funzionali per descrivere un insieme più ricco di comportamenti, pratiche e identità digitali.





Figura 2.1. Il modello Jisc



Il modello Jisc di seguito illustra l'idea che la competenza in ICT (Information and Communication Technology) è un elemento fondamentale della nostra alfabetizzazione digitale, mentre altre competenze si sovrappongono e si basano su questa capacità, e su tutto ciò c'è la nostra identità digitale e il nostro benessere

Recuperato da <https://www.jisc.ac.uk/rd/projects/building-digital-capability>





2.2. RIDURRE L'ANSIA SVILUPPANDO LE COMPETENZE DIGITALI E L'INSEGNAMENTO

Per alcuni adulti, compresi i giovani adulti, il loro uso incompleto di Internet è legato a scarse competenze alfabetiche e matematiche e alla mancanza di fiducia e motivazione per apprendere nuove competenze e applicarle nella loro vita. Le competenze digitali sono fondamentali per l'inclusione nella società. Acquisire queste abilità, insieme alla fiducia e alla motivazione per usarle nella vita reale, può aiutare le persone ad avere una vita migliore. Le persone possono sentirsi imbarazzate per non sapere come usare Internet e l'ansia da computer è una conseguenza. L'ansia da computer è un fenomeno ampiamente diffuso dall'introduzione dei computer nella nostra vita, dimostrando che gli utenti che conoscono poco i computer hanno maggiori probabilità di provare ansia per loro, ma l'ansia digitale può essere ridotta aumentando la loro capacità di risolvere problemi tecnologici e digitali. L'ansia stessa è definita come un disturbo di salute mentale che comprende paure e preoccupazioni "eccessive". Questa disabilità spesso "silenziosa" può manifestarsi in molti modi e la vita quotidiana non fa eccezione.

Segni comuni che potresti provare stress digitale quando non sei esperto mentre inizi a utilizzare gli strumenti digitali includono quanto segue:

1. Ansia o attacchi di panico
2. Isolamento o ritiro dalle attività sociali
3. Maggiore segretezza
4. Rabbia
5. Depressione
6. Voti insufficienti
7. Ribellione
8. Mal di stomaco, mal di testa o altri dolori generali del corpo non spiegati da una condizione medica



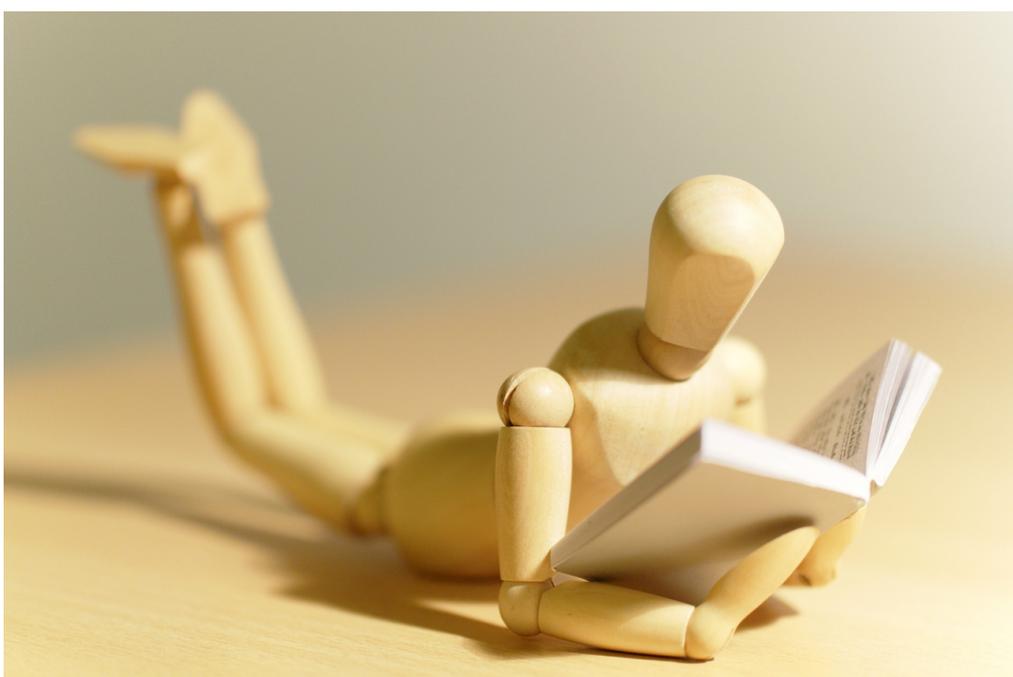


L'accesso alla tecnologia e alle competenze digitali è fondamentale per accedere ad aree chiave della scuola e della vita sociale, ma la tecnologia contribuisce all'apparente crescita dei problemi di ansia osservati nel mondo moderno? Cosa c'è nel digitale e nelle nuove tecnologie che rende molti di noi ansiosi e stressati? L'ansia informatica è caratterizzata da sentimenti di preoccupazione e apprensione insieme a tensione fisica relativa all'uso attuale o futuro del computer, ad esempio la paura di commettere errori o di perdere dati. Può anche portare a tecnostress. Nella sua forma più estrema, l'ansia informatica può diventare "tecnofobia", che comporta la resistenza all'uso della tecnologia e può provocare una mancanza di informazioni sulla tecnologia e sull'alfabetizzazione digitale.

Come puoi far fronte a questa ansia informatica e digitale?

Essere preparato

Questo è il motto dei Boy Scout per un motivo: è un consiglio intelligente. Quando si ha a che fare con i computer e le competenze digitali necessarie, molti di noi sono un po' intimiditi, vogliono solo imparare le basi e affrontare le cose tecniche il meno possibile. Anche se questo è comprensibile, puoi risparmiarti lo stress della mappa imparando le basi di come funzionano i tuoi sistemi leggendo i manuali e forse un libro o due sui computer, e pratica, pratica e pratica.





Eseguire il backup spesso

Se non lo hai già fatto funzionare nella tua routine, è fondamentale che inizi a eseguire regolarmente il backup dei tuoi file (si consiglia una volta alla settimana), in modo che se incontri difficoltà principali, non perdi molto del tuo tempo prezioso e lavoro.



FOMO

Ma cosa succede se non hai paura di usare il computer ma hai bisogno di controllare costantemente la posta elettronica ed essere attivo nei social media e hai la sensazione di dover essere costantemente connesso e interagire e se non lo sei, sei perso?

Figure 5. Fear Of Missing Out' explanation

F	Fear
O	Of
M	Missing
O	Out

Abbiamo tutti un rapporto di amore-odio con l'e-mail e i social media e a volte ci lamentiamo di ricevere troppe e-mail ma, al contrario, le controlliamo troppo spesso per paura di perderci (FOMO). La posta elettronica è spesso esacerbata da più account di posta elettronica per coprire diverse aree della tua vita, ad esempio affari, personali e interessi come club sportivi / gruppi religiosi, ecc. Inoltre, hai la necessità di controllare i social media ancora e ancora e ancora così da non sentirti fuori dal giro: così, sai che stai andando bene, quindi non ti senti escluso.

Come gestire la tua paura di perderti? FOMO è una tortura psicologica auto-inventata ed è un'invenzione della peggiore immaginazione della nostra mente.





Ecco i suggerimenti per mantenere la tua salute mentale durante la tua sensazione FOMO

1. Notifiche

Sii gentile con te stesso e disattiva tutti gli annunci e-mail sul desktop e sul telefono cellulare. Ciò include la disattivazione del fastidioso numero di conteggio delle e-mail che appare spesso sull'immagine del tuo client di posta elettronica. Vedere 100 e-mail non lette non farà altro che aumentare i tuoi livelli di stress e ti invoglierà a dare un'occhiata alle tue e-mail.

Non è necessario vedere tutte le e-mail, anche dalle parti interessate chiave; l'e-mail non è un messaggio diretto e ti allontana dal fare un lavoro approfondito.

Già che ci sei, disattiva tutte le notifiche non essenziali, inclusi Facebook, Twitter e WhatsApp: disattivare le notifiche può essere incredibilmente liberatorio. Inoltre, sposta le tue applicazioni di posta elettronica nella seconda pagina del tuo smartphone.

2. Distanza salutare

Non dire "sì" agli eventi per paura di perderli e mantieni una sana distanza dalle versioni schermate delle vite degli altri. Per una settimana, registra la quantità di tempo che dedichi a controllare e-mail, messaggi di testo o social media su base giornaliera. Cos'altro potresti fare con quel tempo? La paura di perdere l'occasione è reale e la FOMO può essere pericolosa, ma se sai cosa cercare la FOMO è reversibile. Pensa a JOMO. Gioia di perdersi.



3. Stabilisci le priorità

Ricorda che la quantità di informazioni che sei in grado di gestire è limitata e concentrati sulle persone e sui dati che ti interessano davvero o che potrebbero esserti utili.

4. Agire

Se sei permanentemente connesso per paura di ciò che potresti perdere, ciò che ti manca davvero è la vita. Invece di guardare cosa stanno facendo gli altri e trascorrere il tuo tempo libero fotografando, registrando e pubblicando le tue attività, goditi le esperienze positive e condividile con le persone a cui tieni.





2.3. CONCETTO DI CONSUMATORE INTELLIGENTE

Il rapido sviluppo di tecnologie user-friendly e l'accesso immediato alle informazioni ha reso i clienti di oggi intelligenti e consapevoli. Con possibilità sempre maggiori disponibili con un semplice tocco del touchscreen, il comportamento e le preferenze dei consumatori sono sempre in evoluzione.

Quando senti la parola consumare, dove va la tua mente? Probabilmente inizia a pensare al cibo e a ciò che mangi. Per essere onesti, non è troppo lontano. Il consumo è più di quello che metti in bocca. È quello che fai con i tuoi soldi e il tuo tempo. I tuoi soldi comprano cibo, riparo, vestiti, giochi, auto, conoscenze, pensioni, ecc. Il tuo tempo viene speso per imparare una nuova abilità o consumare l'ultimo evento della giornata. Ottenere questo equilibrio tra creare e consumare può essere complicato. Se ottieni il giusto equilibrio, otterrai una migliore capacità finanziaria.



Le nuove tecnologie stanno cambiando il modo in cui i consumatori agiscono. Grazie alla tecnologia, i consumatori stanno diventando sempre più informati, responsabilizzati ed esigenti. Armati di conoscenze raccolte da una moltitudine di fonti, stanno usando i loro soldi per beni e servizi che apprezzano. Vogliono interagire in un modo sia pertinente che tempestivo: rilevante per qualunque cosa stiano acquistando, indipendentemente da dove, quando e come lo stanno acquistando e tempestivi nel soddisfare le loro esigenze. In breve, i consumatori di oggi stanno diventando più intelligenti. Ma come puoi essere un consumatore più intelligente?

I consumatori di tutte le età e in tutte le parti del mondo si accalcano sui social media. Comprendere i social media non è più facoltativo; è un imperativo per essere un consumatore intelligente. La saturazione dei media deve diventare più attiva come consumatori, in parte per gestire il torrente di dati che si riversa su di noi ogni giorno, ma anche per esprimere giudizi informati sul significato di ciò che vediamo.





Quali sono i modi migliori per combattere le “fake news” e sviluppare competenze informatiche-digitali? La proliferazione di notizie false negli ultimi anni è stata accompagnata da una proliferazione di raccomandazioni su come affrontarle. Le abilità coinvolte nella lotta alla disinformazione sono infatti le abilità che devi sviluppare. La tua sfida è pensare a come fattori esterni alla fonte stessa, come l'identità dell'autore, il pubblico e lo scopo, possono produrre sottili distorsioni. Combattere le "notizie false" richiede quindi di esercitare il cervello in modo più faticoso, leggere non solo con comprensione, ma anche discernimento, in breve, applicare il pensiero critico a ciò che stai leggendo e acquistando.

Ecco alcuni consigli su come essere un consumatore più intelligente nell'era digitale:

1. Inizia con la consapevolezza che tutto può esistere - ed esiste - online.

Ciò significa che il reale esiste insieme al falso, il buono insieme al cattivo, il legale all'illegale e tutto il resto. Internet può essere una stanza piena di sogni ed è anche un luogo dove puoi vedere la parte più delicata della bestia sociale. Può essere pieno di possibilità, comodità e divertimento; può anche essere un luogo sleale in attesa di ingannare, incitare, essere immorale e degradare. Acquirente attenzione, volte un milione. Più identifichi la dualità di Internet, più ovviamente la vedrai per quello che è, e anche per tutto ciò che non è.

2. Sii il tuo ricercatore.

Chiunque online può tecnicamente essere un "leader di pensiero", ma dipende da noi decidere di dare a questi individui concreti abbastanza potere per ottenere veramente quel piedistallo come "guidato". Siamo tutti seguaci di influencer sociali, personalità o marchi vogliamo imitare, o quelli che permettiamo di influenzare i nostri pensieri o scelte di acquisto. Solo perché pubblicano informazioni online non significa che siano una fonte di informazioni valide - questa non è un'equazione 1: 1. Quello che consumi online dovrebbe sempre interrogato, ricercato e verificato.





3. Considera come vengono utilizzati i tuoi dati.

Più dati fornisci online, più annunci mirati riceverai. Ma tieni presente che, oltre a ciò che offri, altre informazioni private vengono estratte da fonti diverse. Ad esempio, pensa a fondo prima di consentire ai quiz online di accedere alle informazioni del tuo profilo, che includono data di nascita, numero di telefono, posizione, elenco di amici, luogo di lavoro, ecc.

4. Proteggi te stesso e le tue informazioni.

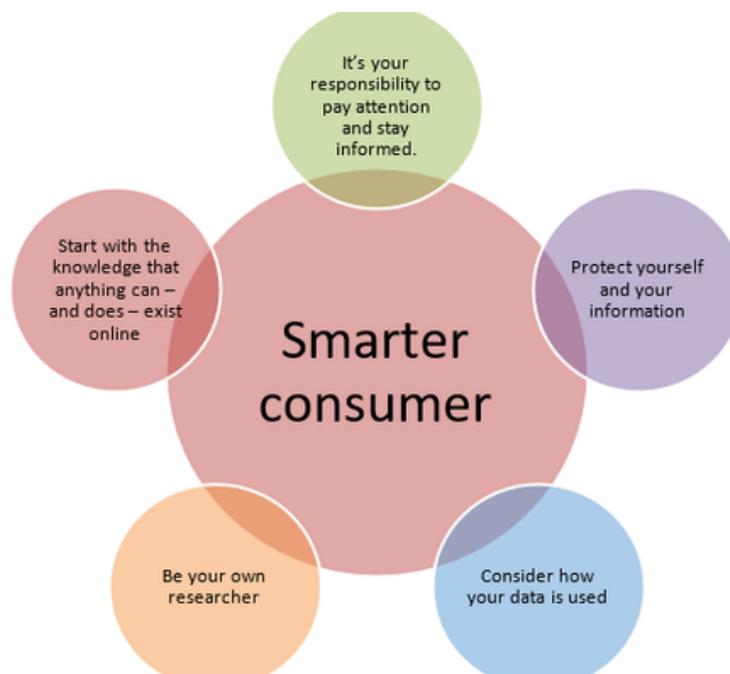
La condivisione o la condivisione eccessiva delle informazioni può provocare la ricezione di fastidiose pubblicità per cose che sembrano importanti o, peggio, possono essere utilizzate per manipolarti nella creazione di opinioni specifiche, spendere soldi o aggiungere il tuo nome come approvazione di cose che potresti non comprendere appieno o supporto.

5. È tua responsabilità prestare attenzione e rimanere informato.

È facile voler ignorare ciò che sta accadendo o dire a te stesso che puoi fidarti degli altri per rimanere aggiornati sulle modifiche all'utilizzo di Internet, alle leggi sulla privacy e agli accordi con gli utenti della piattaforma. Tuttavia, se continui a utilizzare le parti preziose di Internet, devi accettare che esiste un livello di responsabilità che possiedi come compromesso per tali vantaggi.

La nostra società moderna è diventata molto più consapevole dei prodotti e dei servizi disponibili per l'acquisto, con pubblicità e marketing altamente intelligenti che ci convincono che abbiamo bisogno di quell'anello di diamanti, dell'ultimo telefono o dei giocattoli per gli spettacoli che i nostri figli guardano in TV. Riconoscendo questo, c'è un argomento per praticare buone abitudini.

Figura 2.3. Consumatore più intelligente (Fonte: Elaborazione propria).



2.4. PENSIERO CRITICO E TECNICHE DI VALUTAZIONE

L'uso di Internet è probabilmente un'attività quotidiana per molti di voi, ma a volte è così naturale che non ci fermiamo a pensare a ciò che sta alla base delle informazioni che utilizziamo. Viviamo in un'era in cui le informazioni sono ampiamente disponibili. Ogni volta che le persone si trovano di fronte a una domanda, la loro risposta predefinita è "Google it" piuttosto che un brainstorming per una risposta. Ciò è in netto contrasto con quanto accadeva in passato, quando i libri erano la principale fonte di informazioni. Al giorno d'oggi, il tuo pensiero critico è un fattore chiave quando si analizzano le informazioni digitali che ci circondano.

Ci sono molte definizioni di pensiero critico, nella sua forma più elementare, si tratta di essere in grado di pensare da soli. Per essere in grado di pensare in modo critico, devi essere in grado di:

1. Esaminare e valutare informazioni e argomenti
2. Vedi modelli e connessioni,
3. Identificare e costruire informazioni significative

Qualcuno con capacità di pensiero critico può:

1. Comprendere i collegamenti tra le idee.
2. Determinare l'importanza e la pertinenza di argomenti e idee.
3. Riconoscere, costruire e valutare argomenti.
4. Identificare incongruenze ed errori nel ragionamento.
5. Affrontare i problemi in modo coerente e sistematico.
6. Riflettere sulla giustificazione dei propri presupposti, credenze e valori.

Figura 2.3. Capacità di pensiero critico





Probabilmente hai già pratica del pensiero critico in altre aree della vita, come decidere quale telefono, computer o auto acquistare, dove vivere o anche cosa indossare in un'occasione particolare. In ogni situazione, probabilmente non fai solo ciò che qualcun altro ti dice di fare, ma prendi una decisione in base a una serie di fattori. Applicare l'abilità critica nelle tue abilità digitali significa usare la tua capacità per trovare, valutare, gestire, curare, organizzare e condividere le informazioni digitali. Inoltre, questa è la capacità di interpretare le informazioni digitali per scopi accademici e professionali e di rivedere, analizzare e rappresentare le informazioni digitali in diversi contesti. Un approccio critico alla valutazione delle informazioni in termini di provenienza, rilevanza, valore e credibilità. Una comprensione delle regole del diritto d'autore e delle alternative aperte, ad es. Creative Commons; la capacità di fare riferimento alle opere digitali in modo appropriato in contesti diversi.

Uno degli elementi più importanti dell'essere online è la capacità di essere criticamente consapevoli della provenienza dei contenuti e di chi li ha creati. Dovresti essere in grado di porre domande che ti consentiranno di comprendere meglio il contesto.

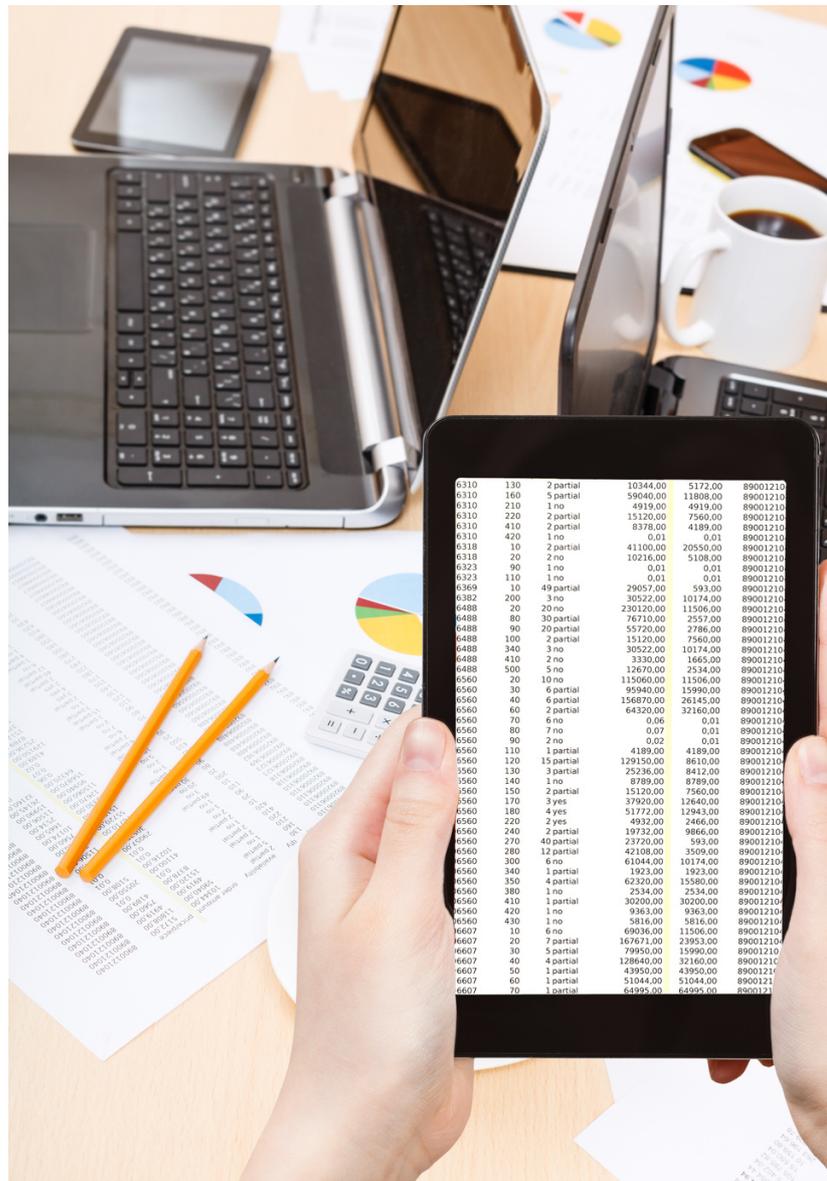
In relazione alla tua abilità critica, è importante la capacità di raccogliere, gestire, accedere e utilizzare i dati digitali in fogli di calcolo, database e altri formati e di interpretare i dati eseguendo query, analisi dei dati e report: la tua alfabetizzazione dei dati e le pratiche di personalizzare la sicurezza dei dati.





Una comprensione di come i dati vengono utilizzati nella vita professionale e pubblica; di linee guida legali, etiche e di sicurezza nella raccolta e nell'uso dei dati della natura degli algoritmi e di come i dati personali possono essere raccolti e utilizzati. Non devi essere un esperto o un professionista dei dati, ma devi essere consapevole della loro esistenza e dei pericoli che il loro uso improprio può causare.

Un altro fattore importante è la tua capacità di ricevere e rispondere in modo critico ai messaggi in una vasta gamma di media digitali - testo, grafica, video, animazione, audio - e di curare, modificare e riutilizzare i media, dando il dovuto riconoscimento ai creatori. Un approccio critico alla valutazione dei messaggi dei media in termini di provenienza e scopo. Una comprensione dei media digitali come strumento sociale, politico ed educativo e della produzione di media digitali come pratica tecnica.



Quando si tratta di valutare i contenuti digitali, si vuole cercare i migliori contenuti digitali disponibili. Ad esempio, vuoi evitare contenuti che sono semplicemente una versione elettronica del libro di testo senza alcun valore aggiunto. L'alfabetizzazione digitale riguarda la ricerca, la valutazione, l'utilizzo e la creazione di contenuti digitali in modi significativi e responsabili. Richiede capacità di pensiero e abilità tecniche.

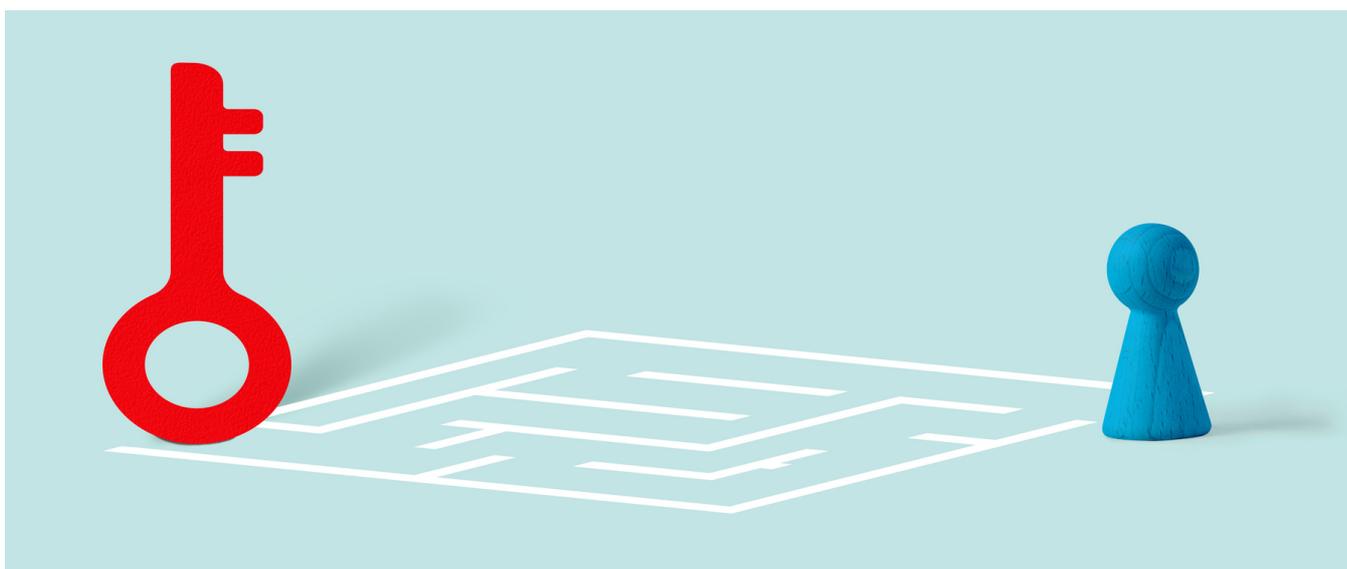




Tenendo conto che trovare contenuti digitali sull'utilizzo di varie strategie di ricerca per aiutare a reperire informazioni di qualità, utilizzare più motori di ricerca per sfidare le bolle di filtro personali utilizzando risorse scritte, visive e audio per navigare tra le informazioni in una varietà di modalità raccogliendo una serie di informazioni che possono poi essere valutato per soddisfare le vostre esigenze.

Un altro punto importante è che prima di iniziare a cercare contenuti digitali rilevanti, devi considerare qual è la domanda di richiesta a cui stai cercando di rispondere o l'argomento che stai esplorando le informazioni che hai già quali informazioni ti servono il tipo di informazioni di cui hai bisogno, ad esempio , una panoramica, un'analisi/ricerca dettagliata o statistiche di quante informazioni hai bisogno - quali lacune ci sono nella tua conoscenza.

Nell'attuale era digitale, chiunque può distribuire qualsiasi informazione sui propri siti Web, piattaforme di social media e altri forum online. Sfortunatamente, coloro che cercano informazioni parallele non verificano realmente l'autenticità delle informazioni. Di conseguenza, la propaganda e le informazioni false spesso vengono interpretate come verità, causando problemi decisionali. Non esiste uno standard per la verifica delle informazioni.



Come rendere efficace la ricerca di contenuti digitali? Trovi risultati migliori utilizzando parole chiave e strategie di ricerca precise. Pensa alle parole chiave della tua domanda o argomento di richiesta, inclusi sinonimi, dizionari e un thesaurus sono utili per compilare un elenco di parole chiave. Guarda la domanda o l'argomento su cui desideri informazioni e scegli la fonte più pertinente per la tua ricerca, ad esempio motori di ricerca e/o database online e prova a utilizzare parole chiave e tecniche di ricerca diverse per ampliare o restringere la ricerca.





Le tecniche di ricerca comuni per Internet includono

Escludi parole dalla tua ricerca

Metti - davanti a una parola che vuoi omettere. Ad esempio, la velocità del giaguaro - auto.

Cerca una corrispondenza esatta

inserisci una parola o una frase tra virgolette. Ad esempio, "edificio più alto".

Cerca all'interno di un intervallo di numeri

inserisci .. tra due numeri. Ad esempio: fotocamera € 50.. € 100.

Combina ricerche

inserisci "OR" tra ogni query di ricerca. Ad esempio, maratona O gara.

Cerca un sito specifico:

inserisci "site:" davanti a un sito o dominio. Ad esempio, sito: youtube.com o sito:.gov.

Ricerca di siti correlati

inserisci "related:" davanti a un indirizzo web che già conosci. Ad esempio, correlato: time.com.

La maggior parte delle informazioni trovate su Internet ha una ragione nascosta dietro di essa. Le aziende e gli scrittori che mettono le informazioni su Internet stavano probabilmente cercando di vendere qualcosa ai lettori. Altri sono propagandisti che cercano di influenzare il modo di pensare di un lettore. Il pensiero critico ci aiuta a pensare ai problemi e ad applicare le giuste informazioni quando sviluppiamo soluzioni. È importante che l'era digitale impari a distinguere le informazioni fattuali da quelle false. Inoltre, è bene che le informazioni provengano da varie fonti online e offline in modo che siano accurate e contengano abbastanza dati.

Fare domande è sempre una buona idea. Ti renderà uno studente e un pensatore migliore. Fare domande critiche significa approfondire le tue domande e non solo chiedere chi, cosa, quando, dove, perché e come, ma invece porre domande più descrittive come "Chi trae vantaggio da questo?" "Cosa ostacola l'azione?" "Perché è stato così per così tanto tempo?" o "Come possiamo cambiare questo per il nostro bene?"

Come dice Jesse R. Sparks:

“Dobbiamo sviluppare le competenze di alfabetizzazione informatica necessarie per valutare la veridicità, la pertinenza, la credibilità e la qualità delle argomentazioni delle informazioni per apprendere, risolvere problemi e prendere decisioni in modo efficace nel mondo di oggi”.





2.5. PERCEZIONE CULTURALE E COMPRESIONE SOCIALE

Le tecnologie digitali hanno trasformato profondamente la scena culturale. Quella tecnologia si è infiltrata nelle nostre vite, ora puoi fare acquisti, effettuare operazioni bancarie, comunicare, socializzare, navigare e collaborare con le persone sul tuo smartphone o dispositivo. In questo senso, dobbiamo sapere che la cultura digitale non è solo connessa alla digitalizzazione dei termini analogici, ma si riferisce anche a uno spazio altamente dinamico in cui convivono modalità multimediali, cross media, transmedia, realtà aumentata e realtà virtuale. Tuttavia, la scena digitale non è priva di rischi.

Le nuove tecnologie hanno modificato lo spazio, il tempo, le relazioni e i tipi di comunicazione che ancora continuano a convivere con gli altri campi del sapere insiti in una cultura. È chiaro che le nuove tecnologie implicano grandi vantaggi in termini di accesso alla cultura ed è anche evidente che nell'era digitale ci sono molte più offerte culturali di quelle a cui gli utenti erano abituati in passato.



La cultura digitale si riferisce alla conoscenza, alle credenze e alle pratiche delle persone che interagiscono su reti digitali che possono ricreare culture del mondo tangibile o creare nuovi ceppi di pensiero e pratica culturale nativi delle reti digitali. La cultura digitale è Internet, transumanesimo, intelligenza artificiale, etica informatica, sicurezza, privacy e policy. È hacking, ingegneria sociale e psicologia moderna (Digital Culturist, 2015).





I telefoni cellulari sono ampiamente utilizzati da giovani e adulti. Siti web come YouTube e Wikipedia sono il primo punto di riferimento per molte persone che cercano informazioni su un'area di interesse selezionata. TV, film e musica sono archiviati e accessibili su computer, lettori MP3 e online. Lo shopping e il banking online sono diventati più dominanti e i servizi governativi sono diventati sempre più basati su Internet. La posta elettronica consente la comunicazione istantanea tra persone in tutto il mondo. Sia i giochi online che quelli offline hanno un ruolo di primo piano nella vita di molte persone e le tecnologie Web 2.0 come i siti di social network consentono alle persone di collaborare condividendo e modificando i contenuti online.

La società odierna, spesso chiamata "l'era dell'informazione", è caratterizzata dal rapido sviluppo delle risorse di comunicazione e informazione.

La comprensione culturale e sociale ti fornisce un linguaggio e un contesto per la tua alfabetizzazione digitale. Certamente, lo sviluppo della comprensione culturale e sociale è fondamentale per consentire alle persone di contribuire non solo socialmente e culturalmente, ma anche politicamente, economicamente e intellettualmente. Devi riconoscere che ci sono alcune influenze sociali, culturali e storiche che modellano la tua comprensione e il tuo apprendimento.

Quanto potrebbe cambiare la cultura quando determinate pratiche si spostano online? Quante volte le credenze e le aspettative culturali attuali possono essere trasportate in un'altra realtà? Spesso pensiamo all'informazione e alla comunicazione in modo tecnico e strumentale, come dati e trasmissione di dati. Tuttavia, l'informazione e la comunicazione sono anche fenomeni sociali.



La propagazione della tecnologia non riguarda solo lo status di classe sociale, ma la formazione, la divisione e gli aspetti della classe sociale che contribuiscono a ciascun gruppo. Tuttavia, molte persone capiscono meno dove rientrano all'interno della classe sociale poiché le culture digitali confondono i tipi di capitale. Questa mancanza di una chiara identificazione o comprensione non diminuisce il significato della gerarchia di classe poiché lo spazio digitale classifica i contenuti attraverso aspetti come le questioni di classe e dei lavoratori non chiaramente affrontate attraverso tale supervisione o mancanza di coesione sociale di classe digitale.



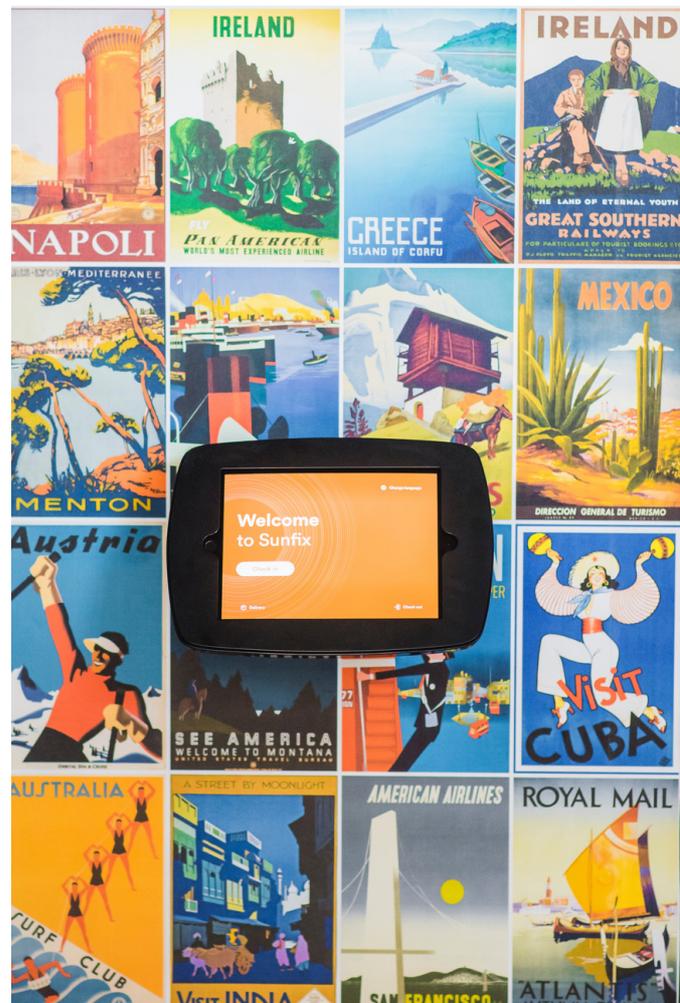


La cultura e la tecnologia digitali hanno formato nuovi modi di vedere teoricamente la classe sociale, incluso il lavoro immateriale, il lavoro digitale, il lavoro informativo e culturale, "il concetto di lavoro libero nelle condizioni della New Economy, così come le ormai famose nozioni di fabbrica sociale" (Qiu, 2018).

La costruzione di una cultura online globale attraverso i nuovi media dovrebbe concentrarsi su come i cambiamenti radicali vengono adottati dalle regole e dai principi democratici. Le tecnologie digitali, principalmente gli spazi online, offrono opportunità per molte nuove forme di interazione. Queste interazioni sono sempre più mediate da diverse modalità di rappresentazione come immagini e suoni. Essere in grado di decodificare questi testi multimodali richiede una comprensione delle pratiche sociali e culturali che circondano la tua creazione.

Differenziamo le epoche culturali in base alla tecnologia di comunicazione utilizzata. Nella cultura orale, il trasferimento di conoscenza poteva avvenire solo nella comunicazione diretta. Nella cultura scritta potrebbero essere preservati certi tipi di conoscenza o la memoria di una particolare persona e messaggi scritti potrebbero essere inviati attraverso lo spazio ed essere registrati (e conservati) per il futuro. La cultura della stampa e della radiodiffusione ha consentito la distribuzione di massa di messaggi provenienti da fonti centralizzate. Oggi possiamo fare riferimento a concetti come cultura digitale, internet e la sua natura partecipativa, convergenza, intelligenza ambientale, ecc.

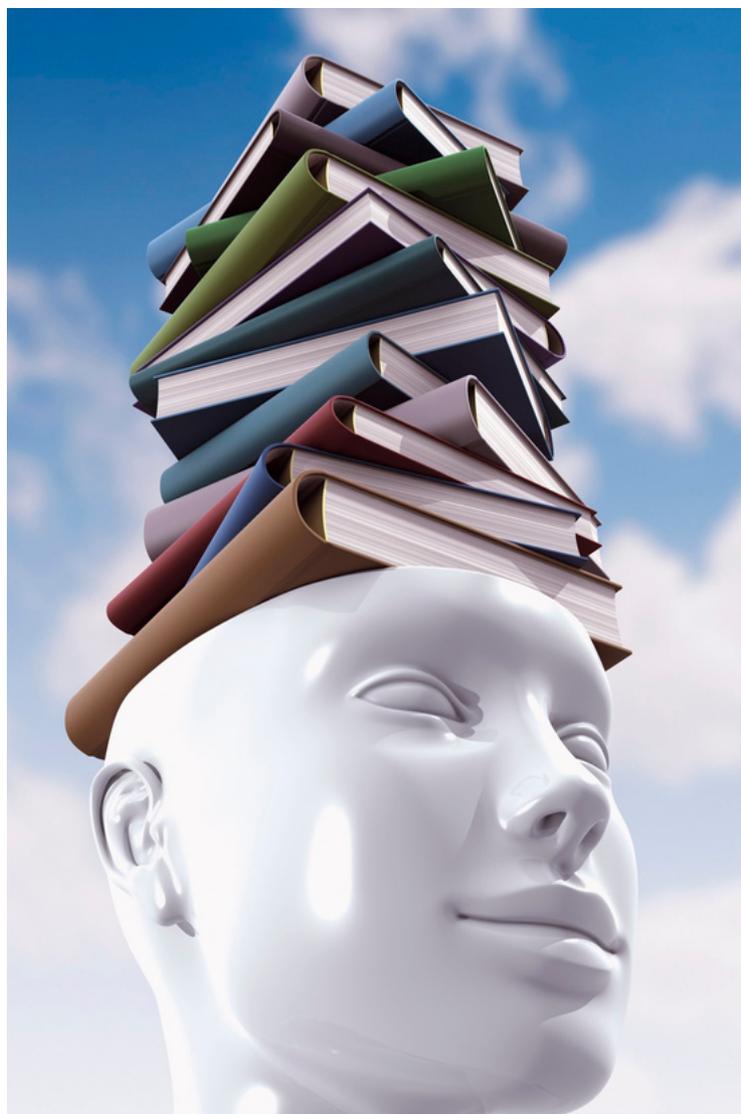
L'effetto delle tecnologie di comunicazione sulla cultura è importante perché il modo in cui le usiamo può modificare l'essenza stessa dei nostri modelli culturali e di comunicazione, ma sebbene gli strumenti digitali intensifichino le tue possibilità, paradossalmente, la crescita esponenziale dell'offerta di contenuti da tutto il mondo a volte ha l'effetto opposto: si traduce in un eccesso che può distogliere l'attenzione.





Sulla base di queste idee presentate, pensa a:

1. In che misura le competenze dei cittadini digitali continuano a migliorare i loro stili di comunicazione e le loro capacità attraverso i nuovi media?
2. Che tipo di esperienze autentiche online sono associate allo sviluppo di stili e abilità di comunicazione attraverso i nuovi media?
3. Quali sono i modelli di partecipazione dei cittadini digitali agli stili e alle abilità di comunicazione attraverso i nuovi media?
4. Quali sono gli impatti degli stili e delle abilità di comunicazione tramite il nuovo?



Gli individui possono diventare partecipanti attivi nelle loro costruzioni di conoscenza piuttosto che ricettacoli passivi. In questo ambiente costruttivista, i cittadini digitali possono lavorare su complessi progetti globali attraverso i nuovi media.





2.6. CREAZIONE, GESTIONE E IMPLICAZIONI DELL'IDENTITÀ VIRTUALE

La nostra identità è, letteralmente, chi siamo e presentarsi online utilizzando un blog personale, una pagina web o un sito di social network richiede una selezione mirata di testo, immagini, grafica e audio per generare un'impressione. Questo non è fatto per caso. Il mondo online richiede alle persone di scrivere se stesse e quindi i loro profili offrono l'opportunità di creare l'impressione prevista attraverso il linguaggio, le immagini e i media.



Al Meeting Annuale del World Economic Forum di Davos 2018 sono stati individuati un primo set di cinque elementi che una buona identità deve soddisfare:

1. Adatto allo scopo. Una buona identità digitale offre alle persone un modo affidabile per creare fiducia in chi afferma di essere, per esercitare i propri diritti e libertà e/o dimostrare la propria leggibilità per accedere ai servizi.
2. Inclusivo. L'identità inclusiva consente a chiunque ne abbia bisogno di stabilire e utilizzare un'identità digitale, libera dal rischio di discriminazione basata sui propri dati identificativi e senza affrontare processi di autenticazione che li escludano.
3. Utile. Le identità digitali utili offrono accesso a un'ampia gamma di servizi e interazioni utili e sono facili da stabilire e utilizzare.
4. Offre la scelta. Gli individui possono scegliere quando possono vedere come i sistemi utilizzano i propri dati e sono in grado di scegliere quali dati condividere per quale interazione, con chi e per quanto tempo.
5. Sicuro. La sicurezza include la protezione di individui, organizzazioni, dispositivi e infrastrutture dal furto di identità, dalla condivisione non autorizzata dei dati e dalle violazioni dei diritti umani.





Figura 2.4. Cinque elementi di buona identità

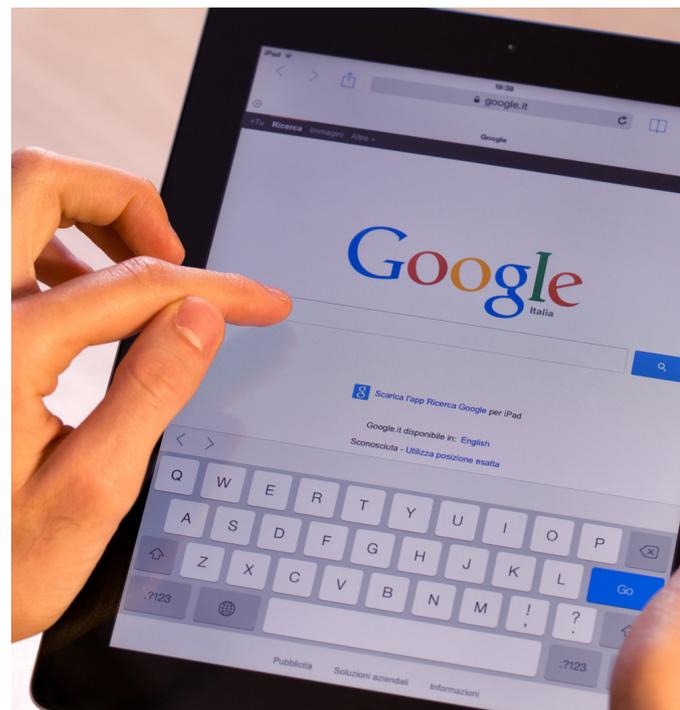


Risorsa: Insight Report - Identità in un mondo digitale Un nuovo capitolo nel contratto sociale. Forum economico mondiale (settembre 2018)

http://www3.weforum.org/docs/WEF_INSIGHT_REPORT_Digital%20Identity.pdf

Se cercassi su Google il tuo nome, cosa troveresti? Tenendo presente che la tua identità online non è la stessa della tua identità nel mondo reale perché le caratteristiche che rappresenti online differiscono dalle caratteristiche che rappresenti nel mondo fisico; potresti aver sentito parlare dell'idea di un'impronta digitale.

Questo si riferisce alle tracce delle tue informazioni personali e professionali che vengono lasciate nelle reti online, sia intenzionalmente che non intenzionalmente. A volte, potresti sentire consigli su come non pubblicare nulla che non vuoi che nessuno veda. Ha senso, ma pensa anche a cosa vorresti che vedessero le generazioni future.





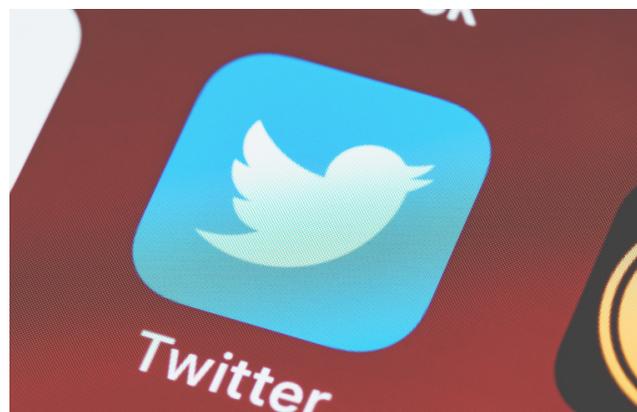
Questo si riferisce alle tracce delle tue informazioni personali e professionali che vengono lasciate nelle reti online, sia intenzionalmente che non intenzionalmente. A volte, potresti sentire consigli su come non pubblicare nulla che non vuoi che nessuno veda. Ha senso, ma pensa anche a cosa vorresti che vedessero le generazioni future.

Cosa devi sapere durante la procedura di creazione e protezione della tua identità online?

Ci sono diversi modi per utilizzare i social media online quando cerchi lavoro, tra cui:

- 1.. Siti di social network come Facebook, Twitter e LinkedIn
2. Partecipazione a forum online e liste di discussione
3. Creare un blog personale

Quando si partecipa ai social media è sempre prudente presentarsi in modo professionale ed è anche importante proteggere le proprie informazioni personali.



Alcuni suggerimenti di base da ricordare quando sei online:

1. Internet è uno spazio pubblico. Quando pubblichi online, rinunci al tuo diritto alla privacy
2. I contenuti online possono essere permanenti: possono essere ricercati; può raggiungere molte persone e può rivelare la tua posizione
3. Quando fornisci informazioni, assicurati di sapere come vengono utilizzate
4. Fornire informazioni sensibili o riservate solo attraverso siti Web sicuri
5. Usa saggiamente i social network; regola le tue impostazioni sulla privacy in base al tuo livello di comfort
6. Nonostante tutte le precauzioni, non aver paura di partecipare e connetterti!





Qual è la tua identità professionale?

I datori di lavoro di oggi vogliono sapere chi hanno assunto e molti reclutatori controllano i social media dei potenziali dipendenti. I siti di social network sono ottimi modi per trasmettere i tuoi interessi, le tue capacità e il tuo bisogno di lavoro. Secondo un sondaggio del 2017, il 70% dei datori di lavoro utilizza i social media per selezionare i candidati prima di assumere. Inoltre, il 69% dei datori di lavoro utilizza motori di ricerca online come Google, Yahoo e Bing per ricercare candidati. Costruisci e gestisci i tuoi profili pubblici online in modo che i potenziali datori di lavoro trovino informazioni positive e professionali su di te, è un punto importante quando cerchi un lavoro.



Facebook, LinkedIn, Twitter, Pinterest (e ogni altra community online) possono essere ottimi strumenti per fare networking, trovare risorse e promuovere interessi personali o professionali, ma solo se usati in modo intelligente e intenzionale. Le prime impressioni prendono forma prima ancora di incontrare fisicamente qualcuno. Proprio come il detto "La tua reputazione ti precede", la tua reputazione online oggi spesso precede incontri e interviste di persona.

La cosa da tenere a mente è che la gestione della reputazione online è una di quelle cose che funziona meglio se la implementi prima di averne effettivamente bisogno.





I 5 migliori consigli e trucchi

1. Google te stesso.

Può sembrare vano ma, in questo caso, sei scusato: devi sapere cosa vedono le persone quando ti cercano.

2. Se non lo stai utilizzando, eliminalo.

Trova tutti i tuoi vecchi profili e tutti gli account inutilizzati che non usi più ed eliminali.

3. Ricorda, c'è più di una pagina su Google.

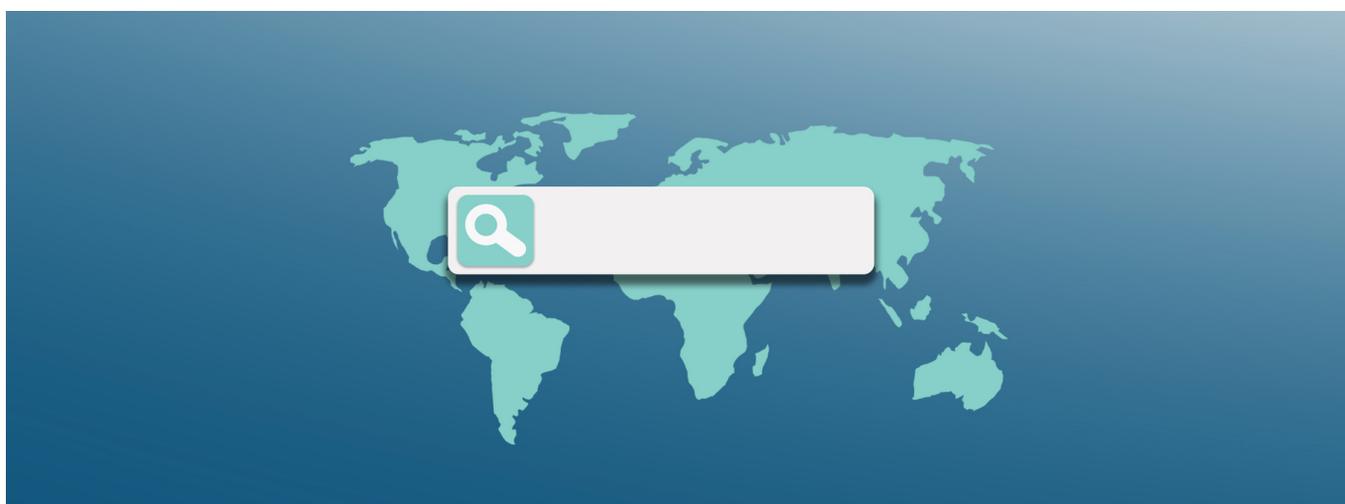
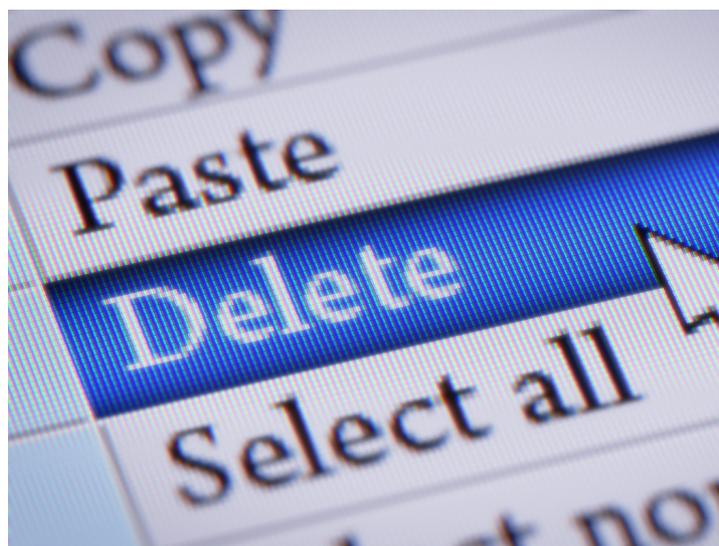
Assicurati di controllare più che puoi su Google nel caso ti mancasse qualcosa

4. La primavera pulisce la tua storia.

Ci vorrà del tempo, ma controlla il tuo Twitter/Instagram/Facebook e controlla ogni post ed elimina quelli che ti mettono in cattiva luce.

5. Sbarazzati delle prove.

Elimina tutte le foto che ti fanno fare brutta figura e chiedi agli amici di fare lo stesso





Now what?

Pensa a cosa stai postando. Hai passato tutto quel tempo a ripulire la tua impronta digitale. Non annullare tutto questo buon lavoro scivolando nelle vecchie abitudini e fai attenzione ai contenuti che condividi.

Vai in blocco

Assicurati di rafforzare le tue impostazioni di sicurezza su piattaforme come Facebook in modo che solo gli amici possano vederti.

Fai attenzione a premere il pulsante **Aggiungi**

Tutti amiamo un nuovo amico di Facebook o un follower di Twitter, ma fai attenzione. A volte non è saggio aggiungere colleghi o docenti sui social media. È sempre una buona idea mantenere la tua vita privata, la privacy.



Crea contenuti interessanti

Fai cose che ti danno un bell'aspetto e rendile parte della tua impronta digitale. Se il tuo capo va su Facebook, fagli trovare un album di foto di te che fai volontariato nella comunità. Se non lo usi già, LinkedIn è un ottimo modo per mostrare tutte le cose fantastiche che fai e può agire come un CV online.



3 MODULO



STRUMENTI PIÙ IMPORTANTI NELL'ALFABETIZZAZIONE MEDIATICA IN GENERALE

3.1. SOFTWARE DI BASE E STRUMENTI DI COMUNICAZIONE

Il software di base e i programmi per computer che consentono l'esecuzione della maggior parte delle attività comuni per gli utenti di computer possono essere suddivisi in due gruppi: software gratuito e uno a pagamento. Vorremmo sottolineare il software libero, tuttavia i prodotti a pagamento e con licenza hanno i loro vantaggi, ad esempio il supporto e una gamma più ampia di strumenti e possibilità aggiuntivi. La maggior parte del software con licenza a pagamento fornisce anche versioni limitate, ma gratuite, insolitamente per uso personale



Per semplificare, abbiamo preparato un elenco delle attività più comuni che possono essere risolte utilizzando software gratuito o a pagamento. Questo elenco copre anche la maggior parte degli strumenti solitamente richiesti dai datori di lavoro.

Condividiamo anche i collegamenti a strumenti alternativi online, poiché molti dei compiti possono essere risolti utilizzando soluzioni basate su cloud, soprattutto perché l'evoluzione digitale si sta rapidamente spostando verso il cloud computing. I dispositivi personali stanno diventando più simili a terminali per accedere a macchine remote e potenti e visualizzare i risultati. Si noti che la maggior parte degli strumenti e dei programmi ha le proprie versioni alternative nei dispositivi smartphone e sono disponibili per il download negli app store.



Figura 3.1. Un elenco di software gratuito e pad di base

A task or purpose	Free (install)	Paid / alternative (install)	Access and use Online
Accessing the internet	Chrome, Firefox, Opera	Google News (app)	N/A
Searching for information	Google, Yahoo, Bing, Yandex	Duckduckgo	Quora, Wikipedia
Accessing and creating email accounts	Thunderbird	Microsoft Outlook	Gmail
Collaboration and communication	Skype, Telegram, Viber	Slack, Zoom	Trello, Asana
Editing documents, saving and viewing PDF	OpenOffice (Writer)	Microsoft Word	Google Docs
Making calculations, drawing tables and diagrams	OpenOffice (Calc)	Microsoft Excel	Google Sheets, Infogram.com
Protecting computer from viruses	GIMP	Photoshop	Snappa.com, Canva.com
Photo editing	VLC	Vimeo.com	Youtube.com
Media Player	Avast, Avira	ESET Antivirus	Eset online scanner
Securing and managing the passwords	LastPass (for individuals)	1password, Bitwarden	N/A
Secure browsing tools (VPN)	Opera built-in VPN	Nord VPN, Express VPN	N/A

Approfondiremo alcuni strumenti e software di base in ulteriori capitoli.





3.2. MOTORI DI RICERCA

Un motore di ricerca è un sito web attraverso il quale gli utenti possono cercare contenuti su Internet. I motori di ricerca consentono agli utenti di cercare contenuti in Internet utilizzando parole chiave. Ogni motore di ricerca funziona in modo simile.

Se vai alla home page di un motore di ricerca, troverai una singola casella. Digita semplicemente quello che vuoi cercare in quella casella. I motori di ricerca sono un ottimo modo per trovare cose sul web. Se cerchi con attenzione puoi trovare informazioni affidabili e affidabili. Con una tale diversità di contenuti e con l'enorme volume di informazioni su Internet, il recupero delle informazioni rilevanti potrebbe essere particolarmente impegnativo



Parole chiave nei tuoi criteri di ricerca

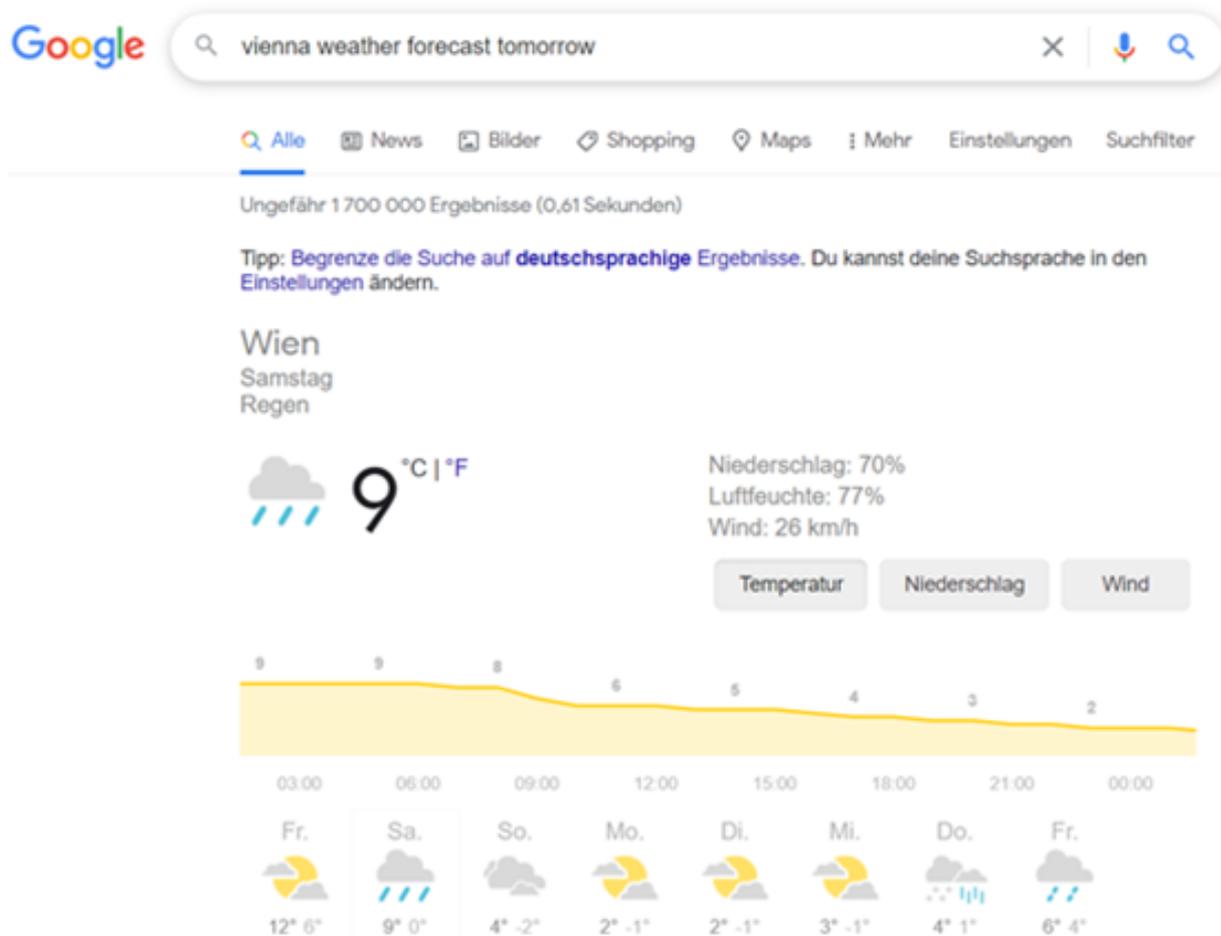
Devi pensare attentamente alle parole chiave che inserisci nella tua ricerca. Devono essere pertinenti. Ad esempio, per scoprire quali sono le previsioni del tempo per domani, puoi digitare le parole chiave come: "Previsioni del tempo di Vienna domani" e verranno visualizzati i risultati di ricerca più pertinenti.

Devi anche pensare al numero di parole chiave che usi. Se utilizzi poche parole chiave potresti ottenere troppi risultati e non tutti saranno pertinenti. Tuttavia, se utilizzi troppe parole chiave, potresti non ottenere alcun risultato. Per rendere la tua ricerca più specifica, puoi utilizzare le "virgolette" attorno a una serie di parole per trovare una frase esatta.





Figura 3.1. Esempio di ricerca: "Previsioni del tempo di Vienna domani" (Fonte: Google)



Se aggiungi un simbolo meno (-) prima di una parola, le pagine che contengono quella parola verranno escluse. Ad esempio, "Imperatori romani - Cesare" cercherà pagine con "Romani" e "imperatori", ma non "Cesare".

Cosa è un URL?

Ogni sito web ha il proprio indirizzo online, chiamato URL che sta per Uniform Resource Locator. Quando stai visualizzando una pagina sul World Wide Web, è l'indirizzo lungo che appare nella barra degli indirizzi nella parte superiore del browser.

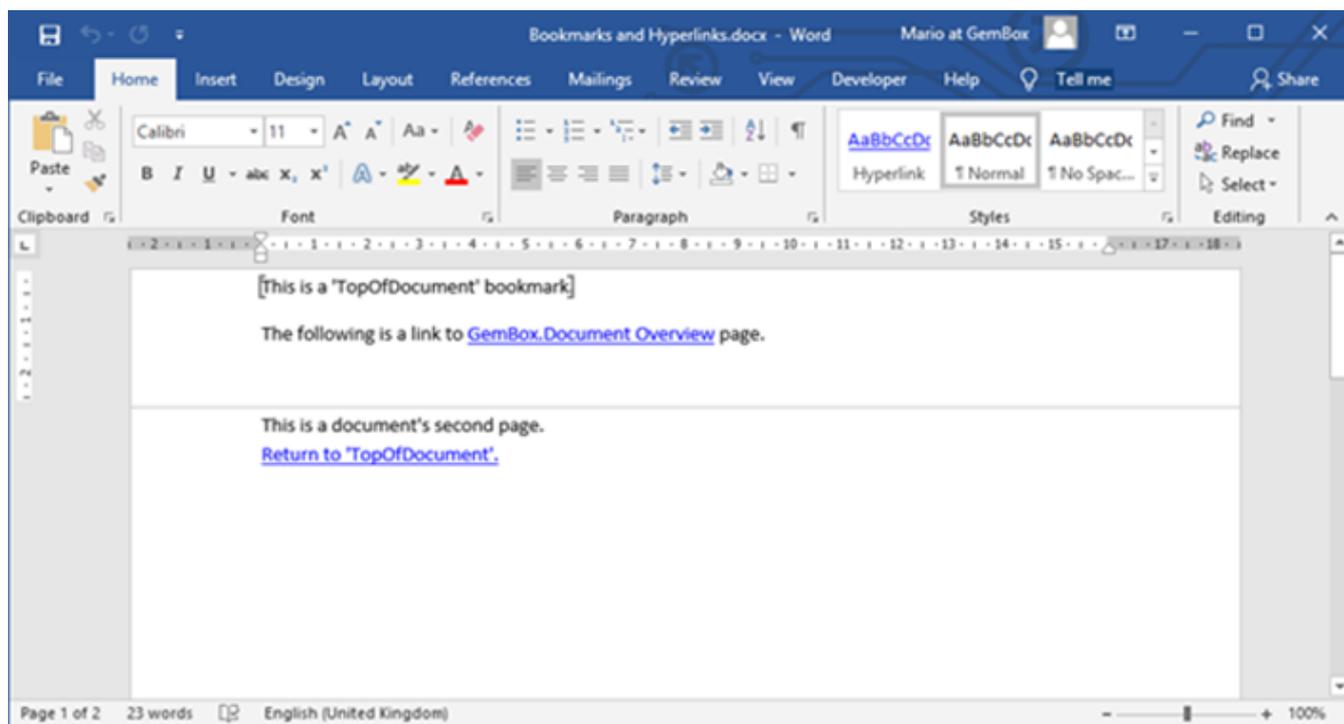




Esistono altri metodi diversi per individuare le informazioni su Internet.

1. Puoi accedere direttamente a una pagina Web semplicemente conoscendone la posizione (ad esempio, desideri visitare il sito Web dell'azienda in cui stai facendo domanda per il lavoro e conosci l'indirizzo esatto del loro sito Web).
2. Il collegamento ipertestuale proveniente da una pagina Web fornisce associazioni integrate alle altre pagine che il suo autore ritiene forniscano informazioni pertinenti

Figura 3.2. Segnalibri e collegamenti ipertestuali. (Fonte: Elaborazione propria)



“I servizi "Narrowcast" possono "spingere" verso di te le pagine che soddisfano il tuo profilo utente.

È noto che Google è il motore di ricerca online più famoso al mondo, ma sono disponibili anche molte altre opzioni. Inoltre, alcuni di questi motori di ricerca alternativi sono immensamente popolari di per sé: semplicemente non sembrano estremamente popolari rispetto a Google. Tuttavia, se non sei disposto a scambiare la privacy per comodità o hai esigenze di ricerca specifiche, esistono diverse alternative a Google che offrono un'esperienza di ricerca più adatta. Conoscere il motore di ricerca giusto per fare la tua query significa che non spendi il tuo tempo prezioso sfogliando cose che non ti servono. Ci si potrebbe facilmente perdere nel vasto mondo di Internet senza strumenti adeguati.

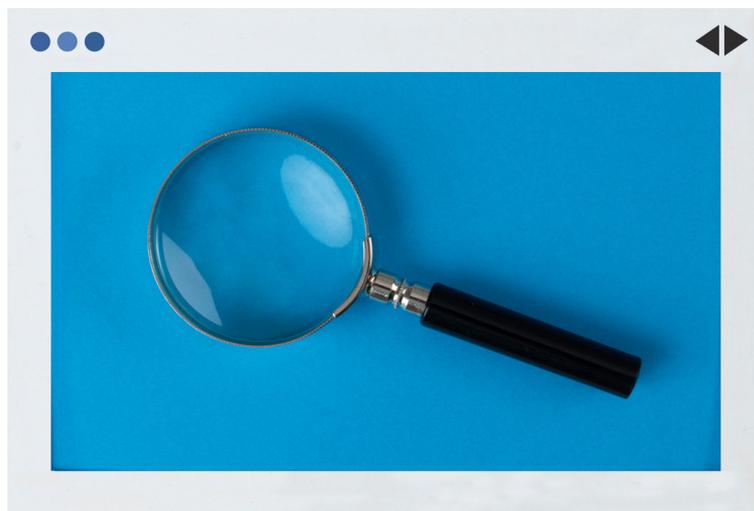
Di seguito ti presentiamo 15 motori di ricerca da provare come alternative a Google per risultati di ricerca migliori.





Most popular search engines

1. https://duckduckgo.com/	6. https://www.aol.com/	11. https://swisscows.com/
2. https://www.bing.com/	7. http://seznam.com/	12. https://startpage.com/
3. https://www.yahoo.com/	8. https://usearch.com/	13. https://www.ecosia.org/
4. https://yandex.com/	9. https://www.yippy.com/	14. https://www.naver.com/
5. https://www.ask.com/	10. https://www.searchencrypt.com/	15. https://www.baidu.com/





3.3. EMAIL

La posta elettronica (e-mail o posta elettronica) è un metodo di scambio di messaggi ("posta") tra persone che utilizzano dispositivi elettronici. È come la posta tradizionale, ma presenta anche alcune differenze fondamentali.

Ad esempio: la posta tradizionale viene indirizzata con il nome, la via, l'indirizzo, la città, lo stato o la provincia e il codice postale del destinatario. Le e-mail vengono consegnate elettronicamente attraverso Internet. Un'e-mail include un nome utente, il simbolo @ (at) e il dominio del provider di posta elettronica. I nomi utente spesso includono numeri e versioni abbreviate di un nome per creare un indirizzo email univoco e di solito avranno questo aspetto: emarosa82@gmail.com



Quando invii un'email a qualcuno, arriva quasi istantaneamente e aspetta nella "posta in arrivo" finché il destinatario non la legge. Con l'e-mail è possibile aggiungere immagini. Tuttavia, prima di approfondire i dettagli, è importante spiegare come creare un account di posta elettronica.

Per iniziare a inviare e-mail, avrai bisogno di un indirizzo e-mail che sarà univoco per te. Per ottenerlo, dovrai creare un account con un provider di posta elettronica – puoi scegliere tra i vari provider – Yahoo, Gmail, Hotmail, Outlook, GMX... Dipende dalle tue preferenze e necessità riguardo alla posta elettronica. Ad esempio, se hai bisogno di spazio e semplicità, Gmail è molto adatto. Se hai solo bisogno di un semplice programma di posta elettronica per inviare e ricevere posta, con poche funzionalità, Yahoo può essere una buona scelta. Puoi ottenere informazioni su ciascun fornitore di servizi digitando il suo nome nella casella di ricerca del motore di ricerca ed eseguire il confronto.





Poiché Gmail era il provider più popolare nel 2020, ora spiegherò come creare un account Gmail (tieni presente che questa metodologia di creazione di un'email può essere applicata a quasi tutti i fornitori di servizi).

Passaggio 1. Digita nel tuo motore di ricerca www.gmail.com che ti porterà a questa pagina. Fare clic su "crea account", nell'angolo in basso a sinistra e apparirà la seguente pagina:

Figura 3.3. Modulo di accesso di Google

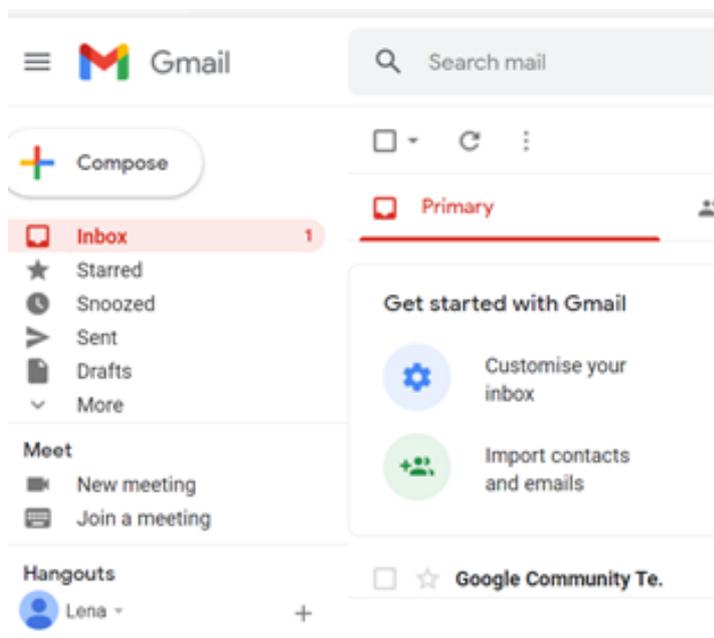
Figure 3.4. Form for account in Google creation

Digita il tuo nome, cognome, nome utente e password. Fai attenzione quando scegli la password giusta, assicurati che non sia facile da indovinare (evita la data del tuo compleanno ad esempio perché la tua famiglia, amici e conoscenti potrebbero facilmente indovinarla e accedere alla tua posta privata). Puoi creare una combinazione di lettere, numeri e segni per creare una password sicura e affidabile per il tuo account. Dopo aver creato un account, potrai accedere all'interfaccia di Gmail.





Figure 3.5. Gmail pagina principale



Come puoi vedere, è molto facile da usare e intuitivo. Se vuoi creare un'e-mail, fai clic sul pulsante "componi" e nell'angolo in basso a destra verrà visualizzata una finestra più piccola in cui dovrai digitare il nome (indirizzo e-mail) del destinatario e l'oggetto della tua e-mail.

Il posto per il testo è sotto la riga "oggetto". Nella parte inferiore della finestra, vedrai un pulsante "invia" e il simbolo "graffetta" se desideri aggiungere alcuni file alla tua e-mail o "inserisci emoji" se desideri aggiungere facce sorridenti alla tua email. Quando hai composto la tua email, clicca sul pulsante "invia" e la tua email verrà consegnata all'indirizzo email desiderato e memorizzata nei messaggi "inviati".

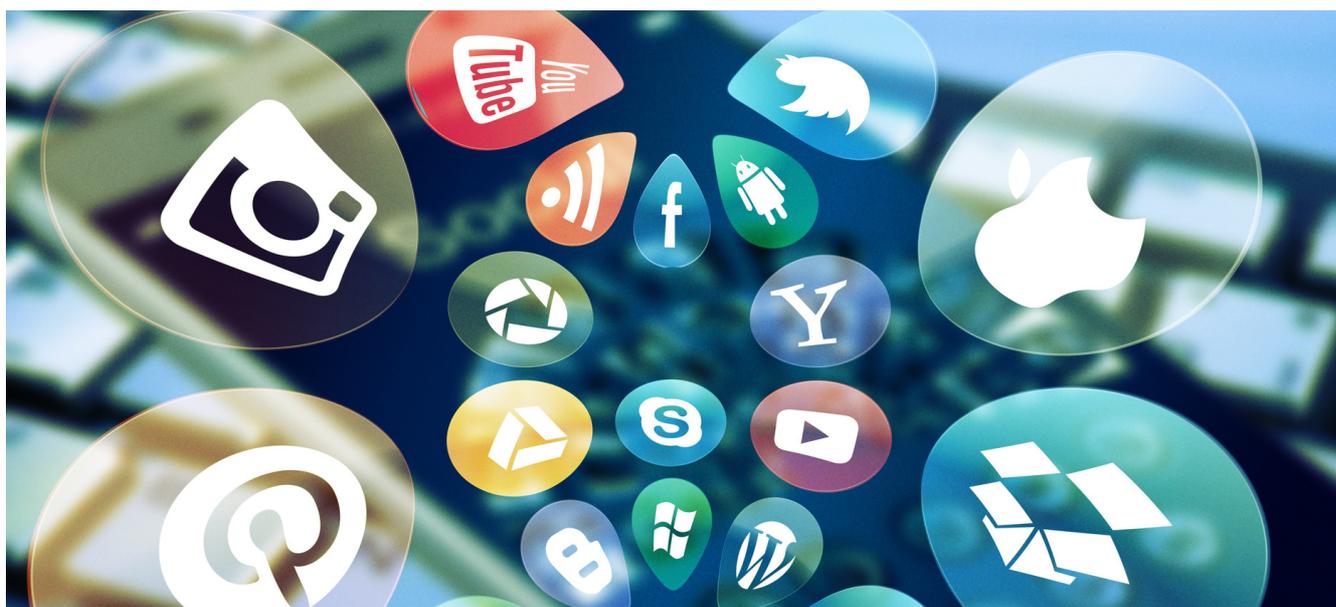
Se ricevi un'email da qualcuno, apparirà nella tua "posta in arrivo" come un messaggio in grassetto e non letto. I messaggi più importanti potrebbero essere contrassegnati con "asterisco" e sarà più facile trovarli cercando nella sezione "speciali".





3.4. SOCIAL NETWORKS

Un social network è definito come una catena di individui e le loro connessioni personali. In alternativa indicato come comunità virtuale o sito di profilo, un social network è un sito Web che riunisce le persone per parlare, condividere idee e interessi o fare nuove amicizie. Questo tipo di collaborazione e condivisione è noto come social media.



Espandere le proprie connessioni con altre persone è una tecnica che può essere utilizzata sia per motivi personali che di lavoro. Le applicazioni di social networking utilizzano le associazioni tra individui per facilitare ulteriormente la creazione di nuove connessioni con altre persone. Questo potrebbe essere utilizzato per incontrare nuovi amici e connettersi con quelli vecchi, come accade su Facebook, o per espandere le proprie connessioni professionali attraverso una rete aziendale come accade su LinkedIn.

Il processo per creare un nuovo account è diverso per ogni social network. In generale, visita il sito Web del social network al quale vuoi iscriverti e cerca il comando "Iscriviti" o "Crea nuovo account". Segui i passaggi per la creazione dell'account per creare il tuo nuovo account. Probabilmente dovrai fornire almeno il tuo nome, l'età e l'indirizzo e-mail. Potrebbero essere necessarie ulteriori informazioni, a seconda dei requisiti del social network. Fai attenzione alle impostazioni sulla privacy.

Anche per essere visto da aziende e reclutatori, devi assicurarti di avere un profilo pubblico. Se utilizzi Facebook anche come social network per il tempo libero, puoi modificare le tue impostazioni sulla privacy per limitare alcuni contenuti solo agli amici e allo stesso tempo mantenere una buona immagine pubblica, a seconda del tipo di lavoro a cui aspiri.





I 10 migliori siti di social media di cui devi preoccuparti nel 2021

Nome	link	Informazioni
Facebook	www.facebook.com	Il social network più popolare per creare uno spazio personale e connettersi con gli amici, condividere immagini, condividere film, ecc.
Youtube	www.youtube.com/	Una rete eccellente per pubblicare video blog o blog e altri video divertenti ed emozionanti
Twitter	www.twitter.com	Un mezzo molto popolare per comunicare (età 30-65), ultime notizie, digerire contenuti di dimensioni ridotte (sono consentiti 150 caratteri). Usando l'hashtag puoi filtrare le informazioni
Instagram	www.instagram.com	Social network diffuso utilizzato dagli appassionati di fotografia (20-35 anni)
Tik tok	www.tiktok.com	Contenuti video divertenti, interessanti e comici in forma breve, solitamente impostati sulle melodie di canzoni popolari





Nome	Link	Informazioni
Snapchat	https://www.snapchat.com	App molto utilizzata da utenti di età inferiore a 25 anni con narrazione basata su video
LinkedIn	www.linkedin.com/	social network professionale, con offerte di lavoro, gruppi di discussione e forum per lo scambio di opinioni.
Pinterest	www.pinterest.com	Strumento di social bookmarking molto popolare per salvare idee e trovare ispirazione creativa dalla cucina ai progetti per la casa fai-da-te, idee per le vacanze, interior design. Usato principalmente dalle donne.
Reddit	www.reddit.com	Community di utenti registrati (redditor) che inviano contenuti che vengono votati dalla community
Google+	https://plus.google.com/collections/featured	Entra a far parte di "cerchi", gruppi che parlano di determinati argomenti e scegli quello che ti interessa.





3.5. BUSINESS SOFTWARE

I software aziendali sono in molti casi strumenti necessari per effettuare una vasta gamma di operazioni aziendali. Pertanto, praticamente tutte le posizioni della maggior parte delle aziende richiedono conoscenze e competenze di base negli strumenti aziendali più comunemente utilizzati.

I software aziendali sono in molti casi strumenti necessari per effettuare una vasta gamma di operazioni aziendali. Pertanto, praticamente tutte le posizioni della maggior parte delle aziende richiedono conoscenze e competenze di base negli strumenti aziendali più comunemente utilizzati.



Vale la pena ricordare che molti software e strumenti utilizzati dalle aziende sono installati su un computer come programma autonomo o è possibile accedervi tramite strumenti online, che sta diventando un settore in continua crescita: il SaaS. SaaS sta per "Service as a Software", che di solito prevede l'accesso a pagamento.

Il tipo di software e l'insieme di strumenti utilizzati dalle aziende dipendono principalmente dal settore in cui operano, dal tipo di clienti a cui prestano servizio, nonché dalle dimensioni dell'azienda. Le piccole aziende di solito utilizzano un'ampia gamma di software che invece sono essenziali per le grandi aziende. Tuttavia, il successo di qualsiasi azienda dipende molto dalle capacità e dall'esperienza che i dipendenti possiedono, soprattutto nell'utilizzo di strumenti digitali.





Elenco degli strumenti digitali di uso comune:

Riunioni a distanza	„Zoom“, „Skype“, „Google Hangouts“
Marketing e pubblicità	Facebook Ads, Google Local Business and Maps, Google Ads, LinkedIn Ads
Email, risposte automatiche e follow-up	„Mailchimp“, „MailerLite“, „Woodpecker“
Marketing automation e CRM	„Hubspot“, „Salesforce“
Project management, planning ed efficienza	„Trello“, „TeamGantt“
Collaborazione e comunicazione	„Slack“, „Microsoft Teams“, „Asana“
Monitoraggio e ottimizzazione delle prestazioni del sito web	„Google Analytics“, „Hotjar“, „Google Optimize“
Email account	Google Workspace“
Archiviazione Cloud	„Google“ diskas, „Dropbox“
Flusso di dati, automazione della reportistica e integrazione degli strumenti	„Zappier“, „Supermetrics“, „Google Data Studio“
Accordo elettronico e firma dei documenti	„DocuSign“, „Docobit“
Condivisione e trasferimento di file	„WeTransfer“
Assistente della scrittura	„Grammarly“.

Questo elenco non comprende tutti i grandi strumenti che le aziende utilizzano nelle loro attività quotidiane, ci sono molti più strumenti per scopi più di nicchia e per i diversi tipi di attività.

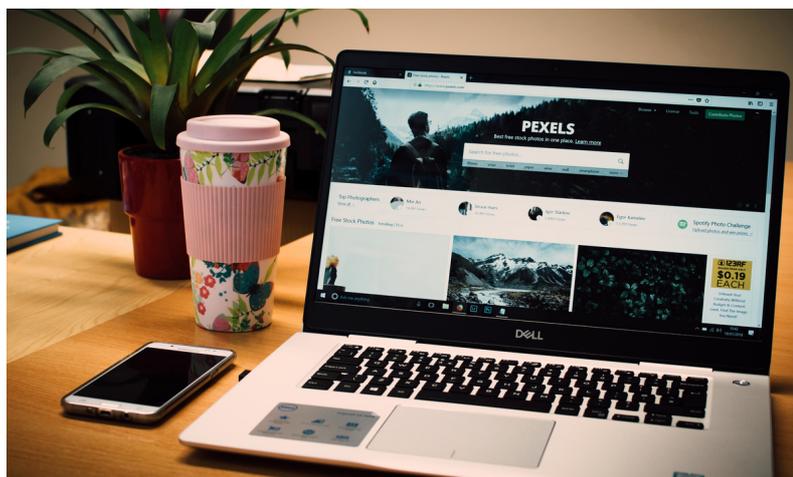




3.6. SVILUPPO SITI WEB, BLOG E MARKETING

I siti web sono senza dubbio l'elemento più importante di Internet, poiché consentono di visualizzare contenuti come testi, immagini e video su Internet.

La pagina centrale di un sito Web è chiamata home page o pagina iniziale/pagina indice. L'utente quindi approfondisce le sottopagine del sito.



A seconda delle dimensioni del sito Web, i visitatori del sito hanno l'opportunità di accedere alle sottopagine del sito Web.

I collegamenti ipertestuali, o semplicemente "collegamenti", vengono utilizzati per collegare singoli documenti HTML di un sito Web

- I collegamenti a sottopagine importanti (ad es. reparti, categorie di prodotti o pagine informative rappresentative) sono generalmente combinati nella navigazione e possono essere trovati nell'intestazione del sito web. Vengono visualizzati in ogni sottopagina del sito Web e non solo nella home page.
- La navigazione aiuta l'utente ad orientarsi e vedere una panoramica della struttura del sito web.
- I collegamenti a più sottopagine possono essere inseriti anche negli elementi di testo e immagine nel contenuto del sito web.
- Il piè di pagina in fondo a una pagina contiene spesso collegamenti a ulteriori informazioni come il proprietario del sito e il quadro giuridico.





Come creare un sito web gratuito con WORDPRESS

WordPress.com è la prima soluzione da considerare per creare un sito web gratuito utilizzando il famoso CMS. Questa piattaforma permette di creare il proprio sito web con un dominio di terzo livello (www.nomesitoweb.wordpress.com) mettendo a disposizione uno spazio di archiviazione di 3 GB.

Vai alla home page <https://wordpress.com/>, clicca su Crea il tuo account. Successivamente, indicare nell'apposito campo di testo l'indirizzo gratuito.

Figure 14. Creating a wordpress account

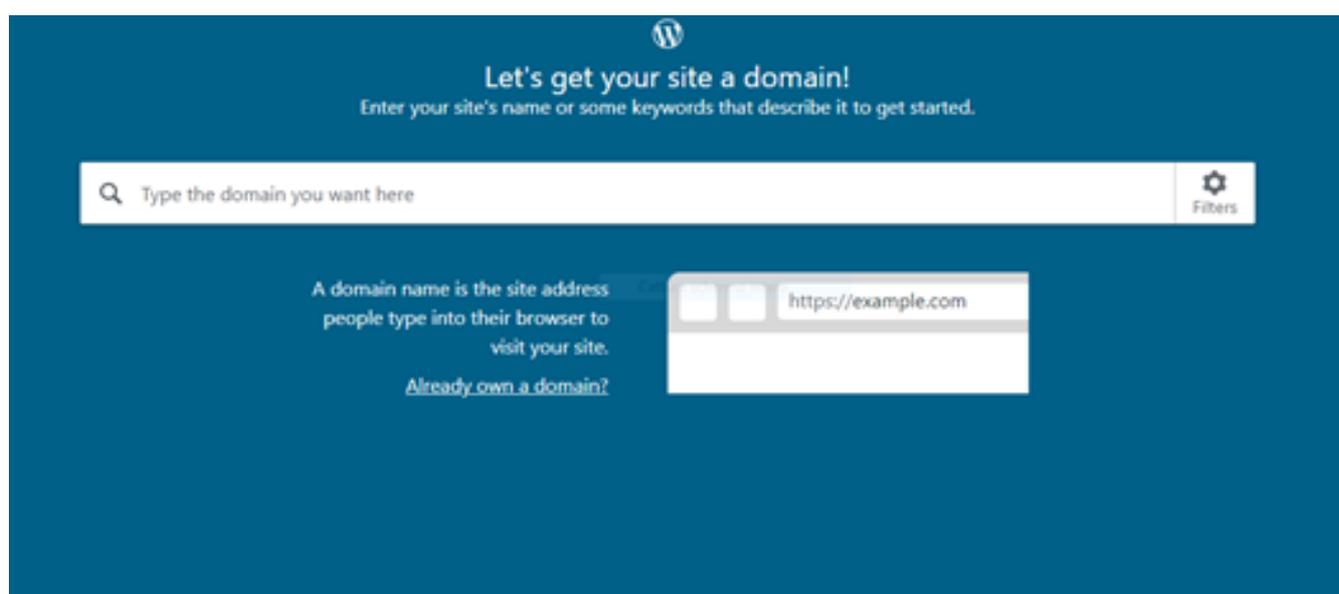
The screenshot shows the 'Let's get started' page for creating a WordPress.com account. It features a dark blue header with the text 'Let's get started' and 'First, create your WordPress.com account.' Below this are three input fields: 'Your email address', 'Choose a username', and 'Choose a password'. The password field includes a strength indicator icon. A pink button labeled 'Create your account' is positioned below the fields. A note states: 'By creating an account, you agree to our [Terms of Service](#).' Below the button, there is a section titled 'Or create an account using:' with two options: 'Continue with Google' (with the Google logo) and 'Continue with Apple' (with the Apple logo). At the bottom, a dark blue box contains the text: 'If you continue with Google or Apple and don't already have a WordPress.com account, you are creating an account and you agree to our [Terms of Service](#).' Below this box is a link: '[Log in to create a site for your existing account](#)'.





Quindi, inserisci il nome che desideri mostrare nel dominio del tuo sito web nel campo "Inserisci un nome o una parola chiave" e fai clic sul pulsante Seleziona per l'opzione Gratuita. Nella nuova pagina aperta, pigia sul pulsante Inizia con gratis, inserisci i dati richiesti nei campi Il tuo indirizzo e-mail, Scegli un nome utente e Scegli una password, clicca due volte consecutive sul pulsante Continua e il gioco è fatto.

Figure 15. Entering a domain name



Ora premi il pulsante Visualizza sito per guardare il tuo sito web creato con WordPress.com. Per aggiungere nuove pagine e articoli, clicca sul pulsante Aggiungi relativo alle opzioni Pagine Sito e Articoli Blog, mentre selezionando la voce Personalizza nella barra laterale di sinistra puoi modificare l'aspetto e scegliere un altro tema gratuito disponibile. Seleziona uno dei tanti template disponibili: per farlo, clicca sull'anteprima di quello che ti interessa e clicca sul pulsante Applica, per applicarlo direttamente al sito che hai creato; oppure fai clic sul pulsante Personalizza se desideri modificarlo un po'.





Per aggiungere nuove pagine o nuovi post al sito, invece, clicca sulla dicitura Pagine o Post (a sinistra) e clicca sul pulsante (+) Nuova pagina o (+) Nuovo post collocato in alto a sinistra. Nella schermata che si apre, puoi creare una nuova pagina o un nuovo post digitandone titolo e corpo negli appositi campi di testo. Utilizzando i pulsanti della barra degli strumenti collocata in alto, puoi anche formattare il testo, inserire link, immagini, ecc. Cliccando sui pulsanti Anteprima e Pubblica, invece, puoi visualizzare in anteprima il contenuto e pubblicarlo.



Sebbene l'esecuzione di un sito Web tramite la soluzione di hosting Wordpress.com sia facile e conveniente, soprattutto per i principianti, a volte è più adatto scegliere un approccio completamente personalizzabile per la creazione di un sito Web e ospitarlo da soli. Dovresti acquistare un piano di hosting da uno dei tanti fornitori di servizi di hosting e installare Wordpress CMS utilizzando una gamma di strumenti forniti dall'host.

Poiché Wordpress è una piattaforma, originariamente creata per i blogger, è cresciuta in popolarità fino a diventare la scelta numero uno per tutti i tipi di sviluppatori di siti Web individuali e anche per le aziende. Supporta un'ampia gamma di strumenti e plug-in, che consentono di adattare Wordpress a e-commerce, forum, aste o persino piattaforme di social media. I professionisti di Wordpress lo vedono piuttosto come un nucleo molto ben ottimizzato per qualsiasi tipo di sviluppo di progetti online, con i componenti Wordpress originali eliminati.



Esistono molte piattaforme CMS alternative per Wordpress e tra quelle più popolari ci sono Joomla, Drupal come piattaforme CMS, mentre Wix.com, Shopify.com sono piattaforme web e pacchetti di servizi, dedicati a particolari esigenze, come e-commerce e altri.

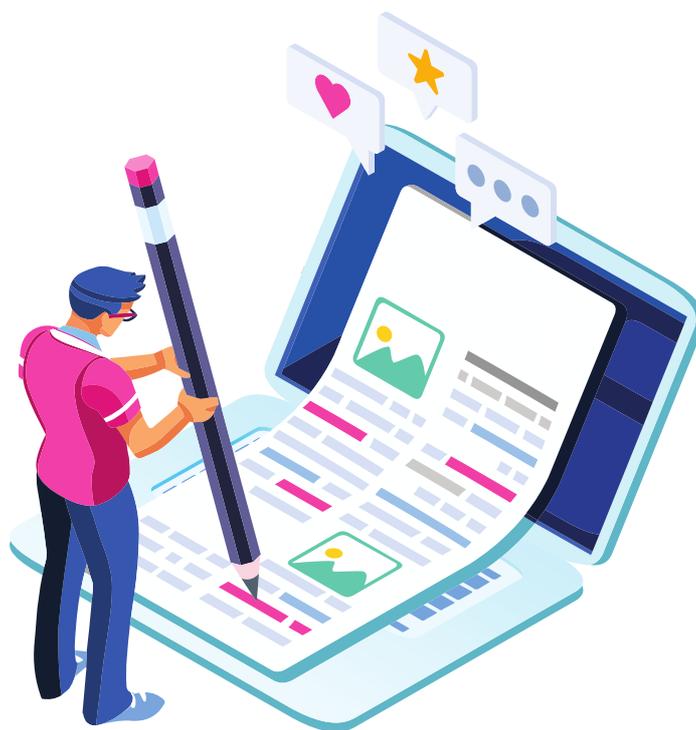




Figura 3.9. Alcune delle piattaforme e dei servizi CMS più popolari



Per concludere, vale la pena sottolineare che un sito Web di vero successo è solitamente quello che fornisce un valore reale ai visitatori del sito Web: gli utenti di Internet. Un modo per fornire valore può essere la creazione di contenuti di qualità essendo in grado di scrivere articoli e storie interessanti e coinvolgenti, quindi le abilità di narrazione sono utili durante la creazione di qualsiasi tipo di contenuto su Internet. Abbiamo preparato alcuni suggerimenti per uno storyteller di successo nel capitolo seguente introducendo cos'è lo storytelling personale e queste abilità possono essere utili.





3.7. PERSONAL STORYTELLING

Lo storytelling è la capacità di affascinare qualcuno o un gruppo di persone con una narrativa coinvolgente che li influenza e li fa sentire come se fossero parte della storia. Le persone ricordano le storie molto meglio di fatti e cifre. È una delle abilità più importanti che puoi imparare a padroneggiare.



Punti chiave:

1. Lo storytelling influenza il cambiamento nella pratica individuale così come a livello organizzativo
2. L'ascolto di storie facilita una migliore assistenza centrata sulla persona e può portare a servizi migliori
3. Ascoltare storie personali genera maggiore comprensione, empatia e riflessione
4. Rapporti, fiducia e cura possono essere coltivati nelle relazioni tra professionisti e utenti del servizio attraverso lo storytelling
5. Lo storytelling personale avvantaggia il narratore in quanto può potenziare, incoraggiare la crescita personale e costruire resilienza





Perché lo storytelling è prezioso per il narratore?

Riformula l'identità personale e incoraggia lo sviluppo personale

L'evidenza suggerisce che il processo di narrazione personale consente al concetto di sé e alla storia della vita di connettersi in un modo che facilita una riformulazione dell'identità e incoraggia la crescita personale. Nell'impartire una storia, un individuo esprime gli eventi significativi con le proprie parole e nel proprio tempo, ed è autorizzato a riflettere. Il processo fa emergere una nuova consapevolezza e nuovi significati del sé.

È una relazione che co-produce significato

La relazione narrativa implica un ascolto e un coinvolgimento diverso da quello di un attore-pubblico o di un intervistatore-partecipante. È una relazione che colma il divario tra la persona e coloro che forniscono supporto, ad esempio professionista-utente del servizio.

Promuove la resilienza

La resilienza implica la volontà di trasformare le emozioni negative coinvolte negli eventi di vita dirompenti in qualcosa di rafforzante e potenziante. La resilienza si sviluppa attraverso un processo di riflessione sui significati, che consente intuizioni emotive. Il supporto di reti paritarie e di altre reti è la chiave per formare legami e sentirsi in contatto con altre persone. La combinazione di questi fattori si traduce in una forza nelle persone, che si basa sulla premessa che le esperienze di vita (comprese le esperienze negative) offrono opportunità di crescita personale.

È terapeutico

Il valore terapeutico del raccontare una storia è spesso riportato nel lavoro di narrazione (Hardy, 2007; Scottish Recovery Network, 2012). Mentre la preoccupazione per il benessere degli individui nella narrazione è spesso espressa e alcuni narratori hanno riportato un certo turbamento nel riferire la loro storia, è riconosciuto che, per la maggior parte, gli aspetti positivi del raccontare la loro storia superano di gran lunga qualsiasi disagio emotivo incontrato. È più spesso che l'atto di raccontare una storia e riflettere su di essa ha un effetto catartico ed è un catalizzatore per la guarigione.



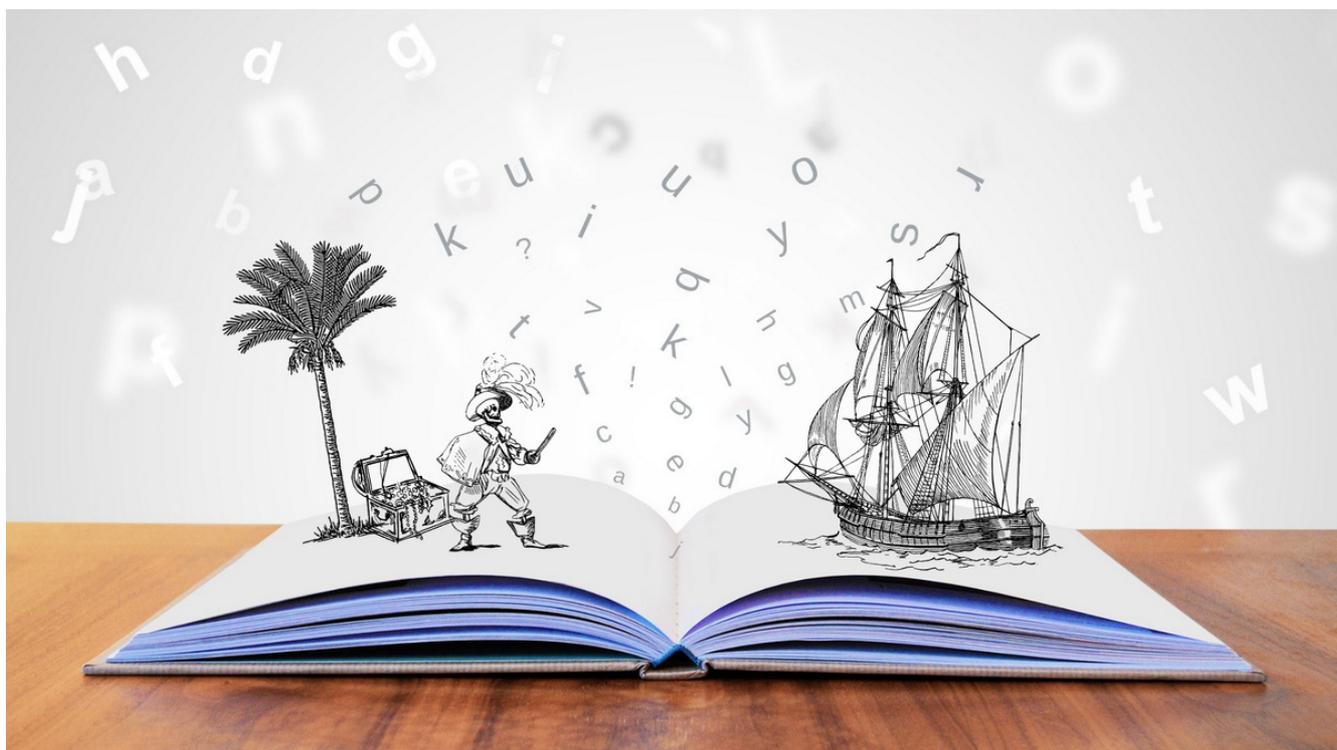


Tecniche di narrazione

I migliori storyteller sono in grado di compiere scelte narrative utili a far avanzare le proprie storie, a coinvolgere il target di riferimento attraverso la diffusione di informazioni importanti, a mantenere l'attenzione, sanno fare riferimento alle proprie esperienze di vita per dare emozione al testo.

Dovresti anche essere in grado di entrare intimamente in contatto con te stesso, al punto che parole ed emozioni diventino un tutt'uno, capace di suscitare consapevolezza e riflessioni tra gli interlocutori.

Questi ultimi rappresentano il target, ovvero un gruppo di potenziali clienti a cui un'azienda vuole vendere i propri prodotti, servizi o il contenuto stesso, e dovrà "innamorarsi" dell'idea e della storia raccontata. Lo storytelling può essere adattato a qualsiasi ambito che debba essere supportato dal punto di vista comunicativo: un'azienda, un prodotto intellettuale o fisico, un servizio, un marchio, una persona o un evento.





3.8. FIRMA ELETTRONICA E SERVIZI ELETTRONICI

Firme elettroniche

Le firme elettroniche offrono un modo per firmare documenti nel mondo online, proprio come si firma un documento con una penna nel mondo reale (offline). In passato, solo le firme autografe erano legalmente valide. La direttiva su un quadro comunitario per le firme elettroniche (direttiva firme elettroniche), adottata nel 1999, ha esteso tale riconoscimento alle firme elettroniche. Un sistema affidabile di firme elettroniche che funzioni in tutti i paesi dell'UE è fondamentale per un commercio elettronico sicuro e un'erogazione elettronica efficiente dei servizi pubblici alle imprese e ai cittadini. La direttiva sulla firma elettronica ha stabilito il quadro giuridico a livello europeo per le firme elettroniche e i servizi di certificazione. L'obiettivo è rendere le firme elettroniche più facili da usare e aiutarle a essere riconosciute legalmente all'interno dell'UE.



La definizione di firme elettroniche varia a seconda della giurisdizione applicabile. Un denominatore comune nella maggior parte dei paesi è il livello di una firma elettronica avanzata (una firma elettronica che soddisfa i requisiti stabiliti dal regolamento UE) che richiede che:

1. Autenticità: il messaggio ha origine dal mittente specificato e il mittente può essere identificato in modo univoco.
2. Integrità: la manipolazione della firma del documento firmato può essere rilevata immediatamente.





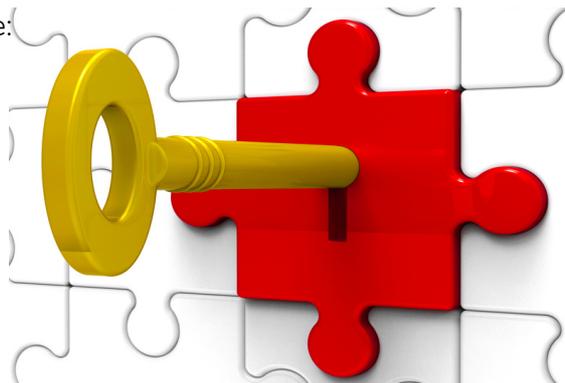
Con l'invenzione della firma del telefono cellulare, sono stati progettati strumenti per firmare elettronicamente documenti, fatture e contratti legalmente vincolanti. È possibile aggiungere una firma elettronica al documento PDF in modo rapido e sicuro, che è l'equivalente legale di una firma autografa. L'autenticità della firma e la genuinità dei dati trasmessi può essere verificata in qualsiasi momento dal mittente o dal destinatario.

Firme digitali

Le firme digitali presentano implementazioni crittografiche delle firme elettroniche utilizzate come prova di autenticità, integrità dei dati e non ripudio delle comunicazioni condotte su Internet. Se implementata in conformità agli standard di firma digitale, la firma digitale dovrebbe fornire privacy end-to-end con il processo di firma facile da usare e sicuro. Le firme digitali vengono generate e verificate attraverso framework standardizzati come il Digital Signature Algorithm (DSA).

Ci sono in genere tre algoritmi coinvolti nel processo di firma digitale:

1. Generazione di chiavi: questo algoritmo fornisce una chiave privata insieme alla corrispondente chiave pubblica.
2. Firma: questo algoritmo produce una firma alla ricezione di una chiave privata e del messaggio che viene firmato.
3. Verifica: questo algoritmo verifica l'autenticità del messaggio verificandolo insieme alla firma e alla chiave pubblica.



Il processo di firma digitale richiede che la firma generata sia dal messaggio fisso che dalla chiave privata possa poi essere autenticata dalla sua chiave pubblica accompagnata. Utilizzando questi algoritmi crittografici, la firma dell'utente non può essere replicata senza avere accesso alla sua chiave privata. In genere non è richiesto un canale protetto. Applicando metodi di crittografia asimmetrica, il processo di firma digitale impedisce diversi attacchi comuni in cui l'attaccante tenta di accedere tramite i seguenti metodi di attacco.





Firma biometrica

La firma elettronica può anche riferirsi a forme elettroniche di elaborazione o verifica dell'identità attraverso l'uso di "firme" biometriche o qualità di identificazione biologica di un individuo. Tali firme utilizzano l'approccio di allegare una misurazione biometrica a un documento come prova. Le firme biometriche includono impronte digitali, geometria della mano (lunghezza delle dita e dimensione del palmo), modelli dell'iride, caratteristiche della voce o persino modelli della retina. Tutti questi vengono raccolti utilizzando sensori elettronici di qualche tipo. Poiché ognuna di queste caratteristiche fisiche ha pretese di unicità tra gli umani, ognuna è in una certa misura utile come firma.

Figure 17. richiesta di firma elettronica. (Fonte: <https://bit.ly/2ZdPQmX>)





Cinque servizi di firma elettronica più popolari:

1. „eSignly“

è una soluzione di firma elettronica leader per milioni di utenti in tutto il mondo per la facilità che offre nella firma e nella gestione dei documenti. L'app offre diverse funzionalità come la firma di persona, la firma programmata, la firma automatica, la gestione del team, la sicurezza di alto livello, l'integrazione con le applicazioni di lavoro più diffuse, l'audit trail ecc.

2. „PandaDoc“

è disponibile per piattaforme mobili Android e iOS. Il software online è un pluripremiato software di firma elettronica dotato di un'interfaccia utente di facile utilizzo.

3. „Adobe Sign“

è disponibile su entrambe le piattaforme mobili iOS e Android. Adobe è un nome comune nel mondo della grafica e come tale, si dice che sia uno dei pionieri nei servizi di eSign. Il software è ricco di funzionalità e offre all'utente la possibilità di gestire flussi di lavoro continui da qualsiasi luogo o dispositivo. L'app ha sia le firme digitali che quelle elettroniche.

4. „SignEasy“

è un altro software di firma elettronica compatibile con le piattaforme Android e iOS. SignEasy non è un'applicazione di firma pesante perché offre un'interfaccia utente minima con l'intenzione di renderla facile da usare. La firma con SignEasy consente la firma automatica, la firma remota e la firma di persona.

5. „RightSignature“

è un'applicazione mobile, utilizza le piattaforme Android e iOS. Questa app di firma elettronica utilizza la velocità per impressionare i suoi utenti, poiché i documenti arrivano più velocemente durante l'invio e la ricezione delle firme. Con esso, puoi caricare, formattare e inviare documenti nel più breve tempo possibile.





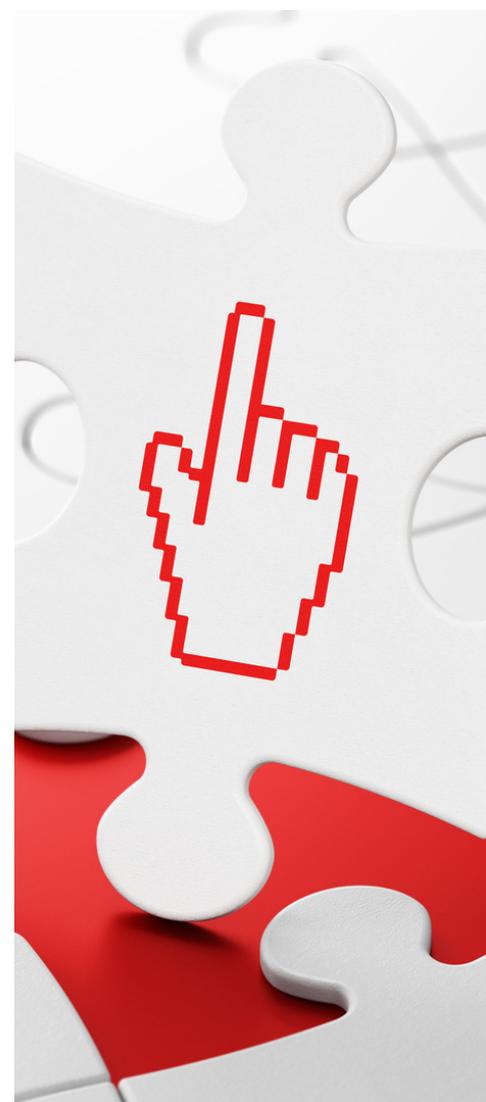
Aggiunta o rimozione di una firma elettronica da Microsoft Word o Adobe

Utilizzando una riga di firma elettronica in un documento di Word, è possibile richiedere informazioni sul firmatario e fornire istruzioni. Quando una copia elettronica va al firmatario, questa persona vede la riga della firma e una notifica che richiede la sua firma. Il firmatario può:

1. Digita una firma
2. Seleziona un'immagine di una firma inchiostrata
3. Scrivi una firma utilizzando la funzione di input penna su un computer touchscreen o un altro dispositivo

Come creare una riga della firma in Word o Excel (Office 365 o 2019):

1. Nel documento, posiziona il cursore nel punto in cui desideri una riga della firma.
2. Nella scheda Inserisci nel gruppo Testo, fare clic sull'elenco Riga della firma. Quindi, fare clic su Riga della firma di Microsoft Office.
3. Nella finestra di dialogo Impostazione firma, digitare le informazioni che verranno visualizzate sotto la riga della firma:
 - Firmatario suggerito: il nome completo del firmatario
 - Titolo del firmatario suggerito: il titolo del firmatario, se presente
 - Indirizzo e-mail del firmatario suggerito: l'indirizzo e-mail del firmatario, se necessario
 - Istruzioni per il firmatario: istruzioni per il firmatario, ad esempio "Prima di firmare il documento, verifica che il contenuto sia corretto"
4. Select one or both of the following checkboxes:
 - Consenti al firmatario di aggiungere commenti nella finestra di dialogo Firma: il firmatario può digitare lo scopo della firma.
 - Mostra la data della firma nella riga della firma: la data in cui il documento è stato firmato apparirà con la firma.



Inoltre, puoi rimuovere una firma facendo clic sulla freccia accanto alla firma nel riquadro Firma e quindi facendo clic su Rimuovi firma.

In alternativa, potresti richiedere una firma elettronica in un documento PDF. Vedere la sezione successiva per come utilizzare le firme elettroniche nei file PDF



Firmare elettronicamente un file PDF

Il Portable Document Format (PDF) di Adobe è un formato comune per i documenti a layout fisso. Come Word, Adobe PDF ha aggiunto una gamma di funzionalità da quando è stato introdotto sul mercato nel 1993. Ora è possibile firmare elettronicamente un file PDF per l'autenticazione.

Se sei un utente Windows, probabilmente hai familiarità con i lettori PDF. Sono programmi per computer che consentono di aprire file PDF, ovvero file con estensione .pdf. L'opzione più popolare in questi giorni è Adobe Acrobat Reader.

Per aggiungere una firma elettronica a un PDF, segui questi passaggi:

1. Open the PDF file in Adobe Acrobat Reader.
2. Fare clic su Compila e firma nel riquadro Strumenti a destra.
3. Fare clic su Firma, quindi selezionare Aggiungi firma.
4. Si aprirà un popup. Seleziona un'opzione: Scrivi, Disegna o Immagine.
5. Fare clic sul pulsante Applica.
6. Trascina, ridimensiona e posiziona la firma all'interno del tuo file PDF.





E-services

E-service (o eservice) è un termine molto generico, di solito riferito a 'La fornitura di servizi via Internet (il prefisso 'e' sta per 'elettronico', come avviene in molti altri usi). I servizi elettronici includono tutti i servizi e le attività creati per mezzo di computer e offerti ed eseguiti in modo interattivo tramite mezzi elettronici, come Internet.

I servizi elettronici possono essere informazioni e servizi educativi come e-education, e-learning, e-teaching, e-publishing, e-book, e-zine e e-catalog, appalti, commercio e servizi di ordinazione come e-business, e-commerce, e-procurement, e-cash, e-shop, e-intermediary, e-auction, servizi culturali e amministrativi come e-culture, e-government o e-vote, miglioramento del marketing, del prodotto o del cliente servizi di relazione, servizi di consulenza elettronica come e-consultancy o e-advising, servizi relativi alla sicurezza (e-security), servizi di produzione, scientifici o logistici.

I servizi elettronici verranno utilizzati in molte altre applicazioni in futuro.



Come si utilizzano i servizi elettronici?

Per utilizzare i servizi, devi prima registrarti come nuovo utente in cima a qualsiasi pagina.

1. Selezionerai il link "Registrati" e completerai i campi richiesti.
2. Al momento della registrazione riceverai una conferma di iscrizione, che consentirà l'applicazione per qualsiasi servizio governativo online.





3.9. SOFTWARE DI SICUREZZA

Qualsiasi dispositivo connesso può essere un gateway per una minaccia alla sicurezza. Il modo migliore per proteggere un dispositivo, in particolare uno connesso a Internet, è utilizzare un software di sicurezza adeguato e aggiornato, generalmente noto come antivirus.

Un ulteriore livello di sicurezza dei dati personali e sia per le informazioni trasferite su Internet che per il dispositivo stesso può essere fornito da un set speciale di strumenti chiamati VPN, che stanno per Virtual Private Network.

Durante la navigazione o, in particolare, effettuare transazioni finanziarie mentre si è connessi a una rete Wi-Fi non sicura, le persone possono esporre se stesse e i propri dati sensibili a una minaccia alla sicurezza.

Gli strumenti e i servizi antivirus di solito forniscono una serie di strumenti che monitorano il traffico Internet, scansionano i file e cercano di rivelare potenziali minacce alla sicurezza anche di virus sconosciuti. Tali strumenti aiuterebbero a evitare malvertising, bloccare siti Web potenzialmente dannosi e utilizzare altre soluzioni per proteggere il dispositivo e le informazioni dell'utente.

Gli strumenti VPN aiutano a connettersi a Internet tramite un server remoto protetto, che nasconde l'indirizzo IP originale degli utenti consentendo agli utenti di crittografare il proprio traffico e mascherare la propria identità online. In questo modo l'anonimato e la sicurezza aumentano durante la navigazione utilizzando hot-spot Wi-Fi pubblici o altre connessioni di rete non sicure.

Alcuni software antivirus possono fornire anche un servizio VPN.

Alcuni software antivirus possono fornire anche un servizio VPN:

- Avira
- Avast
- McAfee
- ESET
- Bitdefender
- AVG
- Kaspersky
- Microsoft security essentials
- Norton

Strumenti VPN più comunemente usati:

- Nord VPN
- Express VPN
- Surfshark
- Tunnelbear





3.10. SICUREZZA E HARDWARE DEI DISPOSITIVI FISICI



Sappiamo tutti quanto sia fastidioso perdere un telefono, rubarlo o semplicemente lasciarlo cadere a terra e rompere lo schermo a un livello tale da rendere il dispositivo inutilizzabile. Il problema di solito non è considerato importante finché non si verifica. Per evitare ogni tipo di danno a un dispositivo. Parlando di sicurezza fisica, assumiamo che qualsiasi dispositivo potrebbe subire danni fisici dovuti a caduta, guasto hardware, danni causati dall'acqua o potrebbe essere perso o rubato.

Abbiamo compilato un elenco di modi e soluzioni per evitare le perdite utilizzando semplici tecniche di sicurezza di un dispositivo fisico:

Password o crittografia

Evita di perdere informazioni a causa di tentativi di furto. Usa una password sicura, un'impronta digitale o altri dati biometrici per proteggere l'accesso al tuo dispositivo, sia mobile che desktop. Evita di utilizzare la stessa password ovunque e blocca con password o crittografia i file importanti. Abilita il software di tracciamento integrato o installato fornito da alcuni fornitori per poter tracciare il tuo dispositivo utilizzando i servizi di localizzazione, anche se è bloccato in caso di smarrimento o furto.

Salvataggio

Esegui sempre il backup dei file importanti, archiviali su CD o memory stick o anche su cloud storage di terze parti.

Buon senso

Non tentare i ladri con dispositivi mobili incustoditi, in particolare nei luoghi pubblici. Non lasciare la borsa del laptop in macchina, incustodita in un bar, in aeroporto o in altri luoghi pubblici.

Aggiornamenti

Mantieni aggiornati il tuo software e i tuoi dispositivi, installa gli aggiornamenti del sistema operativo quando richiesto.

Agire rapidamente

A seconda della situazione, se il dispositivo viene smarrito, niente panico, inizia cambiando la password ai sistemi più importanti, informa il tuo supervisore o IT se il dispositivo aziendale è stato perso e, se necessario, informa la polizia.

Elimina informazioni personali

Se vendi un vecchio dispositivo, un telefono, un tablet o un computer, assicurati che tutte le tue informazioni personali siano eliminate definitivamente dal disco rigido o dalla memoria del dispositivo. È possibile utilizzare software speciali come Eraser, File shredder o WipeFile o altri strumenti simili.





3.11. INTERNET OF THINGS (IOT)

L'idea di dispositivi interconnessi in cui i dispositivi sono abbastanza intelligenti da condividere informazioni con noi, con applicazioni basate su cloud e tra loro (da dispositivo a dispositivo).

I dispositivi intelligenti o "Dispositivi connessi", come vengono comunemente chiamati, sono progettati per acquisire e utilizzare ogni bit di dati condiviso o utilizzato nella vita di tutti i giorni



L'Internet of Things (IoT) è un sistema di dispositivi informatici interconnessi, macchine meccaniche e digitali, oggetti, animali o persone che sono dotati di identificatori univoci e la capacità di trasferire dati su una rete senza richiedere l'interattività umana interazione con il computer.

Questa nuova ondata di connettività sta andando oltre laptop e smartphone, sta andando verso auto connesse, case intelligenti, dispositivi indossabili connessi, città intelligenti e assistenza sanitaria connessa. Insomma, una vita connessa.

E questi dispositivi utilizzeranno questi dati per interagire con te su base giornaliera e completare le attività. Colmeranno il divario tra il mondo fisico e quello digitale per migliorare la qualità e la produttività della vita, della società e delle industrie.

E questi dispositivi utilizzeranno questi dati per interagire con te su base giornaliera e completare le attività. Colmeranno il divario tra il mondo fisico e quello digitale per migliorare la qualità e la produttività della vita, della società e delle industrie.





10 applicazioni del mondo reale di Internet of Things (IoT) - Spiegate nei video

Applicazione	Spiegazione	Video link
1. Casa intelligente	Smart Home è diventata la scala rivoluzionaria del successo negli spazi residenziali e si prevede che le case intelligenti diventeranno comuni come gli smartphone.	https://youtu.be/NjYTzvAVozo
2. Indossabili	I prodotti Smart Home sono promessi per risparmiare tempo, energia e denaro	https://youtu.be/h8-TAqzYrno
3. Auto connesse	I dispositivi indossabili sono installati con sensori e software che raccolgono dati e informazioni sugli utenti. Questi dati vengono successivamente pre-elaborati per estrarre informazioni essenziali sull'utente.	https://youtu.be/0HxZuQ0woLY





Applicazione	Spiegazione	Video link
4. Internet industriale	Industrial Internet è il nuovo ronzo nel settore industriale, chiamato anche Industrial Internet of Things (IIoT). Sta fornendo all'ingegneria industriale sensori, software e analisi dei big data per creare macchine brillanti.	https://youtu.be/8NGzrtK7eV0
5. Città intelligenti	Secondo Jeff Immelt, CEO di GE Electric, IIoT è una risorsa "bella, desiderabile e investibile". La filosofia alla base dell'IIoT è che le macchine intelligenti sono più precise e coerenti degli esseri umani nella comunicazione attraverso i dati. E questi dati possono aiutare le aziende a individuare prima le inefficienze e i problemi.	https://youtu.be/Br5aJa6MkBc





Applicazione	Spiegazione	Video link
6. IoT in agriculture	<p>IIoT ha un grande potenziale per il controllo della qualità e la sostenibilità. Le applicazioni per il monitoraggio delle merci, lo scambio di informazioni in tempo reale sull'inventario tra fornitori e rivenditori e la consegna automatizzata aumenteranno l'efficienza della catena di approvvigionamento. Secondo GE, il miglioramento della produttività del settore genererà dai 10 ai 15 trilioni di dollari di PIL in tutto il mondo nei prossimi 15 anni.</p>	<p>https://youtu.be/q0FnMD2_0Fw</p>
7. Vendita al dettaglio intelligente	<p>Il potenziale dell'IoT nel settore della vendita al dettaglio è enorme. L'IoT offre ai rivenditori l'opportunità di connettersi con i clienti per migliorare l'esperienza in negozio.</p>	<p>https://youtu.be/gUcuqhduWao</p>
8. Impegno energetico	<p>Gli smartphone saranno il modo per i rivenditori di rimanere in contatto con i propri consumatori anche fuori dal negozio. L'interazione tramite smartphone e l'utilizzo della tecnologia Beacon possono aiutare i rivenditori a servire meglio i propri consumatori. Possono anche tenere traccia dei percorsi dei consumatori attraverso un negozio e migliorare il layout del negozio e posizionare prodotti premium in aree ad alto traffico.</p>	<p>https://youtu.be/JwRTpWZReJk</p>



Applicazione	Spiegazione	Video link
9. IOT in sanità	Guarda questo video per scoprire come la vendita al dettaglio connessa ti semplificherà la vita.	https://youtu.be/8AkXW9EPFJg
10. IoT nel pollame e nell'agricoltura	<p>Il monitoraggio del bestiame riguarda la zootecnia e il risparmio sui costi. Utilizzando le applicazioni IoT per raccogliere dati sulla salute e il benessere del bestiame, gli allevatori che conoscono in anticipo l'animale malato possono ritirarsi e aiutare a prevenire un gran numero di bovini malati.</p> <p>Con l'aiuto dei dati raccolti e gli allevatori possono aumentare la produzione di pollame. Guarda questo video interessante.</p>	https://youtu.be/eZ2sVriiluU



4 MODULE



ESEMPI, CASI DI STUDIO E PRECAUZIONI CONTRO CUI SVILUPPARE LA RESILIENZA

4.1. ESEMPI, CASI DI STUDIO E PRECAUZIONI CONTRO CUI SVILUPPARE LA RESILIENZA



Che cos'è la violazione della privacy dei dati?

1. Una violazione dei dati è un incidente in cui le informazioni vengono rubate o sottratte da un sistema senza la conoscenza o l'autorizzazione del proprietario del sistema. Una piccola azienda o una grande organizzazione può subire una violazione dei dati.
2. Si verifica una violazione della privacy quando qualcuno accede alle informazioni senza permesso. Inizia con una violazione della sicurezza - penetrando in una rete di computer protetta - e termina con l'esposizione o il furto di dati. Tali dati possono includere informazioni di identificazione personale come nome, indirizzo, numero di previdenza sociale e dettagli della carta di credito.

Quali sono i tuoi rischi per la privacy?

1. La privacy si riferisce a tutti i diritti che hai per controllare le tue informazioni personali e come tali informazioni vengono utilizzate. Le tue informazioni sono in molti posti. Ciò include agenzie governative, organizzazioni sanitarie, istituzioni finanziarie, piattaforme di social network, produttori di app per computer e molti altri luoghi.
2. Le tue informazioni hanno valore. Ecco perché i criminali informatici spesso prendono di mira le organizzazioni in cui possono raccogliere dati personali. Possono usarlo per commettere crimini come il furto di identità o venderlo sul dark web.
3. Un'altra somiglianza tra violazioni della privacy e violazioni dei dati? Non c'è molto che puoi fare per prevenirli. La sicurezza delle tue informazioni è nelle mani di qualcun altro. Anche così, ci sono cose che puoi fare per proteggerti.





Come prevenire una violazione dei dati?

1. Crea password complesse. Usane di diversi per ogni account e cambia le password se un'azienda con cui hai interagito di recente viene violata.
2. Utilizzare l'autenticazione a più fattori quando disponibile. Ciò consente l'accesso solo dopo che sono state presentate due o più prove, di solito una password e un codice che viene inviato all'utente tramite telefono, SMS o e-mail durante il login.
3. Acquista con carta di credito. Potresti avere una minore responsabilità per addebiti fraudolenti sulla carta di credito.
4. Fai attenzione alle frodi. Se ricevi una notifica sulla violazione dei dati, chiama l'azienda per confermare che è legittima, utilizzando un numero che sai essere valido anziché un numero che potrebbe essere elencato nell'avviso.
5. Guardia contro il furto di identità. A livello globale, il 65% delle violazioni dei dati provoca il furto di identità, il che lo rende il risultato più comune. Se diventi vittima di un furto di identità, contatta ciascuna società di carte di credito per impostare avvisi di frode e bloccare i tuoi account. Quindi mettiti in contatto con l'ufficio locale della sicurezza sociale per i passaggi successivi.
6. Imposta gli avvisi dell'account. Potresti essere in grado di ricevere notifiche di acquisti sospetti o quelli che superano un determinato importo in dollari. Questo potrebbe darti un avvertimento che sei stato violato.

Video: i pericoli di una violazione dei dati <https://www.youtube.com/watch?v=0kK902-ZvNM>





4.2. HACKING ED ESTORSIONE INFORMATICA



L'hacking è un tentativo di sfruttare un sistema informatico o una rete privata all'interno di un computer. In poche parole, è l'accesso non autorizzato o il controllo sui sistemi di sicurezza della rete di computer per scopi illeciti.

L'estorsione informatica è un crimine su Internet in cui qualcuno tiene in ostaggio file elettronici o dati aziendali fino a quando non paghi un riscatto.

Video: Cyber Extortion <https://www.youtube.com/watch?v=UNCBuFJRyK>





L'impatto finanziario negativo degli attacchi informatici può essere mitigato dall'assicurazione contro i rischi informatici. È particolarmente rilevante per le aziende che dispongono di un grande IT e/o gestiscono database personali di grandi dimensioni. Molte compagnie assicurative forniscono questi servizi in Lituania. L'idea principale di tale assicurazione è che man mano che le aziende diventano sempre più dipendenti dai sistemi informatici e dalla sicurezza dei dati, cresce il rischio di essere vittime di reati digitali.

Le compagnie di assicurazione di solito si offrono di coprire non solo le perdite relative ai danni al patrimonio dell'azienda a causa di attacchi informatici, ma anche le perdite causate dalla fuga di dati personali di terzi archiviati dall'azienda.

Il miglior esempio di ciò è il caso della società lituana di car sharing City Bee quando sono stati sequestrati 110.000 dati di utenti, per saperne di più su <https://www.euronews.com/2021/02/17/thousands-of-citybee-users-have-their-personal-data-leaked-online>.

Maggiori informazioni sull'assicurazione contro i rischi informatici: <https://youtu.be/F7mYEm-kx-Q> (disponibile solo in lituano)





4.3. FURTI D'IDENTITÀ



Il furto di identità è il reato di ottenere informazioni personali o finanziarie di un'altra persona per utilizzare la propria identità per commettere frodi, come effettuare transazioni o acquisti non autorizzati. Il furto di identità viene commesso in molti modi diversi e in genere le vittime subiscono danni al credito, alle finanze e alla reputazione.

Il furto di identità si verifica quando qualcuno ruba le tue informazioni personali e le credenziali per commettere una frode. Esistono varie forme di furto di identità, ma la più comune è quella finanziaria. La protezione dal furto di identità è un settore in crescita che tiene traccia dei rapporti di credito delle persone, dell'attività finanziaria e dell'utilizzo del numero di previdenza sociale.

Video: What is Identity Theft? <https://www.youtube.com/watch?v=kDFeSUUwRnA>





Tipologie di furti di identità

Furto di identità finanziaria	qualcuno utilizza l'identità o le informazioni di un'altra persona per ottenere credito, beni, servizi o benefici.
Furto di identità della previdenza sociale	se i ladri di identità ottengono il tuo numero di previdenza sociale, possono utilizzarlo per richiedere carte di credito e prestiti.
Furto di identità medica	qualcuno si spaccia per un'altra persona per ottenere cure mediche gratuite.
Furto di identità sintetico	un criminale combina informazioni reali (di solito rubate) e false per creare una nuova identità, che viene utilizzata per aprire conti fraudolenti ed effettuare acquisti fraudolenti.
Furto d'identità di un minore	qualcuno usa l'identità di un minore per varie forme di guadagno personale.
Furto di identità fiscale	qualcuno utilizza le tue informazioni personali, incluso il tuo numero di previdenza sociale, per presentare una falsa dichiarazione dei redditi statale o federale a tuo nome e ottenere un rimborso.
Furto di identità criminale	un criminale finge di essere un'altra persona durante un arresto per cercare di evitare una citazione, impedire la scoperta di un mandato emesso a suo vero nome o evitare un arresto o una condanna.

Video: Watch Out These 8 Types of Identity Theft -
<https://www.youtube.com/watch?v=EZa2um76rFY>





Protezione contro il furto di identità

Un modo è controllare continuamente l'esattezza dei documenti personali e affrontare tempestivamente eventuali discrepanze. Esistono diversi servizi di protezione dal furto di identità che aiutano le persone a evitare e mitigare gli effetti del furto di identità. In genere, tali servizi forniscono informazioni che aiutano le persone a salvaguardare le proprie informazioni personali; monitorare i registri pubblici e privati, come i rapporti di credito, per avvisare i propri clienti di determinate transazioni e cambiamenti di stato; e fornire assistenza alle vittime per aiutarle a risolvere i problemi associati al furto di identità. Alcune agenzie governative e organizzazioni senza scopo di lucro forniscono assistenza simile, in genere con siti Web che contengono informazioni e strumenti per aiutare le persone a evitare, rimediare e segnalare incidenti di furto di identità. Molti dei migliori servizi di monitoraggio del credito forniscono anche strumenti e servizi di protezione dell'identità.

Per prevenire il furto di dati personali, è necessario:

- Proteggi tutti i documenti con informazioni personali, come patente di guida, passaporto, estratti conto bancari, bollette, ecc.;
- Distruggi i documenti vecchi o non necessari che mostrano il nome, l'indirizzo o altre informazioni personali di una persona;
- Monitora il rapporto sulla tua storia creditizia e controlla regolarmente la tua carta di credito e gli estratti conto bancari per le transazioni completate;
- Quando si cambia il luogo di residenza, informare la propria banca, carta di credito, telefonia mobile, provider di servizi TV/Internet e altri fornitori di servizi del cambio di indirizzo in modo che messaggi e lettere con informazioni personali non raggiungano altre persone;
- Ricorda che meno informazioni una persona fornisce su se stesso, minore è il rischio che le informazioni cadano nelle mani sbagliate;
- Quando acquisti beni online, scegli un sito Web sicuro che mostri le informazioni di contatto dell'azienda, una chiara politica sulla privacy, garanzia di beni e servizi e resi;
- Quando scegli un sito web di trading di posta elettronica, assicurati che applichi la crittografia dei dati inviati (certificato SSL corretto e valido) e verifica che l'indirizzo del sito web inizi con HTTPS.





4.4. CYBERBULLISMO



Il cyberbullismo può essere definito come un atto aggressivo, intenzionale e ripetuto, compiuto da un gruppo o individualmente, eseguito tramite mezzi elettronici come telefoni cellulari o Internet, contro una vittima che non può difendersi facilmente (Slonje, Smith e Frisé, 2013).

Il bullismo, in generale, è separato da altri comportamenti aggressivi in base a due aspetti. Il primo è la ripetizione, come menzionato nella definizione sopra, e il secondo è lo squilibrio di potere. Di solito, l'intenzione dell'autore non è quella di ripetere l'atto abusivo, ma a causa dell'uso eccessivo della tecnologia, questo potrebbe sfuggirgli di controllo. Ad esempio, un'immagine con contenuto offensivo può essere pubblicata su Internet una volta, ma di conseguenza può essere condivisa più volte da altre persone, non dall'autore iniziale. In questo modo la ripetizione è inevitabile e l'imbarazzo è sperimentato molte volte dalla vittima.

Per quanto riguarda lo squilibrio di potere in termini di cyberbullismo, non è necessariamente riferito alla "debolezza" fisica o psicologica, ma anche alla mancanza di conoscenza nelle ICT e/o all'anonimato offerto dal cyberspazio (Slonje, Smith e Frisé, 2013). Gli studi condotti finora, indicano che esiste una correlazione tra studenti con conoscenze ICT avanzate e attività svolte, delinquenti, online. Per quanto riguarda l'anonimato, di solito la vittima non è a conoscenza dell'identità dell'autore e, quindi, è difficile affrontarlo in modo efficiente (Slonje, Smith e Frisé, 2013).





Motivi

I motivi del cyberbullismo possono essere suddivisi in due categorie: interni ed esterni. I motivi interni includono rabbia, gelosia, volontà di vendetta o persino noia (Slonje, Smith e Frisé, 2013). Questi possono anche indicare problemi familiari problematici. Inoltre, il comportamento di cyberbullismo può soddisfare il bisogno di imposizione di potere (Nika, Gioldasi e Vitta, 2017).

Per quanto riguarda i motivi esterni, questi possono essere la possibile assenza di gravi conseguenze contro l'autore o il fatto che l'autore può essere riluttante o timoroso a procedere in un incontro faccia a faccia con la possibile vittima (Slonje, Smith e Frisé, 2013).

Conseguenze

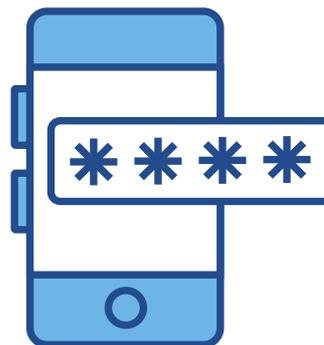
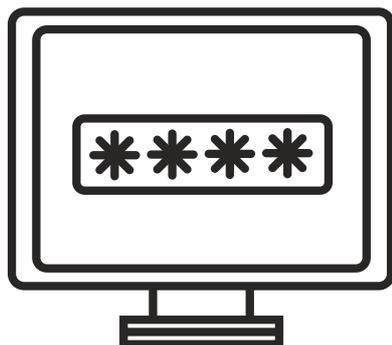
1. La vittima e l'autore a volte provano emozioni negative come rabbia, tristezza, ansia, imbarazzo, paura, autoaccusa e mancanza di autostima.
2. Per quanto riguarda il contesto scolastico, sono state notate concentrazione negativamente influenzate, scarso rendimento scolastico ma anche assenza dalla scuola (Šléglová e Cerna, 2011).
3. Le vittime possono sentirsi così indifese, sole, imbarazzate e disperate che possono decidere di suicidarsi.
4. Sia le vittime che gli autori possono essere socialmente emarginati e quindi le emozioni sopra menzionate sono intensificate.
5. Le vittime potrebbero non cercare di difendersi perché pensano che questo comportamento abusivo sia "normale" o previsto o che lo meritino, quando si sentono inferiori (Šléglová e Cerna, 2011).





Modi per contrastare

1. È molto importante sia gli adolescenti che gli adulti essere informati e consapevoli della sicurezza in Internet e delle differenze funzionali tra i diversi mezzi tecnologici (Olweus, 2012).
2. Altre soluzioni pratiche stanno bloccando le persone sconosciute sui social media e cambiando spesso password e nomi utente.
3. Chiedere aiuto a una persona familiare o a un esperto (Slonje, Smith e Frisé, 2013). Aperti su una brutta esperienza che stai attraversando o che hai vissuto in passato e condividi i tuoi sentimenti. Questo ti aiuterà a sentirti più sollevato e a trovare più facilmente una soluzione.
4. I genitori devono essere di mentalità aperta ed essenzialmente vicini ai loro figli, in modo che questi si sentano liberi di discutere questioni come il cyberbullismo e la cybervittimizzazione.
5. È di vitale importanza quando si naviga in Internet essere consapevoli dei diritti delle persone e di come rispettarli.
6. Organizzare corsi di formazione o seminari sul cyberbullismo e sui modi per contrastarlo.



Casi di studio

Brandy Vela (1998-2016), 18 anni, era una studentessa delle superiori che si è suicidata nel novembre 2016 dopo anni di bullismo di persona e online da parte dei suoi coetanei sul suo peso. Secondo sua sorella, i bulli hanno creato siti di incontri, dove hanno mentito sulla sua età, hanno messo la sua foto e hanno usato il suo numero di telefono per dire alle persone che si è data per il sesso gratuitamente per chiamarla. Brandy si è sparata al petto con una pistola ed è morta in ospedale il giorno dopo. Dopo la sua morte, un paio di adolescenti sono stati arrestati per bullismo (contribuenti di Wikipedia, 2020).

Megan Meier (1992-2006), 13 anni, era un'adolescente americana del Missouri, che si è suicidata impiccandosi poche settimane prima del suo quattordicesimo compleanno. Un anno dopo, i suoi genitori, dopo aver svolto un'indagine sulla vicenda del suo suicidio, hanno scoperto che era stato attribuito al cyberbullismo attraverso il sito di social network Myspace. Gli individui intendevano utilizzare i messaggi di Meier per saperne di più su di lei e in seguito umiliarla (contribuenti di Wikipedia, 2020)



4.5. TECNICHE DI PHISHING



Il furto di dati è chiamato phishing, termine inglese che deriva dalla password fishing. Si tratta di una forma di frode nei confronti di enti o privati nell'utilizzo di messaggi di posta elettronica non richiesti o di pagine web falsificate, con l'obiettivo di ottenere password per l'accesso ai sistemi informativi e ad altre informazioni riservate. dati.

Nella maggior parte dei casi, attacchi di questo tipo sono diretti contro clienti bancari al fine di scoprire le loro password per la connessione ai sistemi bancari elettronici o i dati delle carte di credito. Successivamente, le informazioni così ottenute possono essere utilizzate nella commissione di atti criminali: collegamenti illeciti a sistemi informatici, furto di denaro da conti o pagamento di merci con carte straniere nello spazio elettronico.

Il furto di dati viene effettuato in due modi principali:

1. Contattare direttamente le persone e indurle a rivelare volontariamente tali informazioni;
2. Utilizzando tecnologie dedicate che copiano dati da vari siti web o dispositivi che servono per navigare in internet e/o utilizzare servizi remoti.





Il tipo più comune di phishing è il cosiddetto phishing ingannevole. In questo caso un truffatore impersona un'istituzione o una società legittima (ad es. agenzia governativa, agenzia delle forze dell'ordine, fornitore di servizi finanziari, grande azienda di marca ben nota, ecc.) e si rivolge direttamente alle persone con una richiesta di inserimento dei dati personali. La stessa e-mail o altro tipo di messaggio viene inviato a migliaia di persone sperando che alcuni di loro rispondano.

Tali messaggi di solito richiedono una reazione molto rapida, osservando che potrebbero esserci conseguenze negative indesiderabili se un individuo non risponde in tempo (ad esempio l'istituzione intraprenderà azioni legali, i fondi dalla banca dell'individuo potrebbero essere rubati, il premio sarà assegnato a un'altra persona e così via).

Molto spesso tali messaggi potrebbero contenere collegamenti dannosi e/o altri riferimenti a siti speciali che chiedono alle persone di inserire lì le informazioni richieste. Non appena un individuo fornisce queste informazioni su tali siti, queste diventano disponibili per il truffatore.

I truffatori più avanzati potrebbero sfruttare il meccanismo di controllo della sessione e dirottare la sessione di un sito legittimo. Quando un individuo accede a un'applicazione web, il server imposta un cookie di sessione temporaneo nel suo browser. I truffatori potrebbero rubare tali cookie di sessione o fornire a un individuo un collegamento contenente un ID di sessione preparato prima che acceda a tale sessione di autenticazione. Queste azioni consentono ai truffatori di dirottare in seguito la sessione utilizzando lo stesso ID di sessione per la propria sessione del browser.



I metodi di phishing possono essere utilizzati anche creando falsi e-shop o altri siti. Per rendere tali siti più evidenti, i truffatori allettano le persone con prezzi bassi, consegna rapida di merci o altri vantaggi. Diversi motori di ricerca vengono utilizzati per raggiungere un pubblico mirato e indirizzarlo a tali siti. I dati vengono rubati mentre un individuo mirato cerca di registrare o acquistare la merce in tali siti.



I truffatori potrebbero trarre vantaggio dai siti legittimi esistenti alterando un indirizzo IP in modo che reindirizzi a un sito falso anziché al sito a cui una persona intendeva andare.

Anche l'invio di collegamenti o altri riferimenti a file infetti da determinati virus è una tecnica molto diffusa. Tali file infettano computer o altri dispositivi e potrebbero essere programmati per chiedere di ridigitare password o altre credenziali durante la connessione a servizi bancari online o altri servizi remoti solo allo scopo di trasferire tali informazioni a truffatori.





In primo luogo, è importante comprendere ed essere consapevoli che phishing e furti di dati possono avvenire ovunque, in qualsiasi forma e in qualsiasi momento, quindi è necessario essere costantemente attenti e vigili.

In secondo luogo, prendi precauzioni per mantenere al sicuro i dispositivi che usi:

- 1 Utilizza strumenti e software che aiutano a proteggere il tuo computer o altro dispositivo (programmi antivirus, ecc.). Scarica tali strumenti o software solo da fonti ufficiali e attendibili. Aggiorna questi strumenti e software in tempo.
- 2 Evitare di visitare siti oscuri e inaffidabili, registrarsi o scaricare file da tali siti. Tali siti possono contenere collegamenti o file che possono infettare il tuo computer o altro dispositivo con virus che raccolgono i tuoi dati personali.
- 3 Dopo aver utilizzato il tuo account personale, esci da esso e chiudi la finestra del browser.
- 4 Scegli password sicure e forti composte da numeri, lettere e altri simboli. Non utilizzare password facili da indovinare (ad es. 12345, solo il tuo nome o cognome o data di nascita). Nel caso tu abbia più account diversi, usa sempre password diverse.
- 5 Quando crei account o e-mail, scegli fornitori di servizi che utilizzano sistemi di autenticazione a due fattori (ad esempio una password e un numero di telefono).
- 6 Fai attenzione ai comuni falsi online che imitano:
 - a) siti web di posta elettronica che forniscono servizi di posta (gmail.com, yahoo.com, hotmail.com, ecc.);
 - b) siti web social (facebook.com, vk.com);
 - c) posta elettronica, molto diffusa all'estero. sistema di pagamento Paypal (paypal.com);
 - d) altri siti web popolari.
- 7 Non fare clic su collegamenti sospetti o poco chiari ricevuti nelle e-mail o trovati su pagine Web con contenuti sospetti.
- 8 Prima di inserire i tuoi dati personali sui siti web online, assicurati sempre che il sito web non sia falso. È necessario prestare attenzione al nome a dominio e agli indirizzi dei link presenti nella pagina. I sistemi di e-banking utilizzano sempre un protocollo di connessione SSL sicuro, l'indirizzo deve avere HTTPS all'inizio e il certificato del sito può essere verificato. L'indirizzo dei siti Web falsi inizia quasi sempre con HTTP (senza s).





In terzo luogo, tieni presente che le istituzioni legittime e le società di servizi (ad esempio banche o altri fornitori di servizi finanziari) non richiedono ai propri clienti di divulgare le password di accesso o altre credenziali. Tali informazioni sono personali e solo tu sei autorizzato a conoscerle. Se tali informazioni vengono a conoscenza di terzi, è necessario informare immediatamente questi fornitori di servizi di queste circostanze e modificare le password o altre credenziali..

In quarto luogo, se ricevi una richiesta di informazioni sensibili, presta attenzione a queste circostanze:

1

L'indirizzo del mittente. Verificare se i dettagli dell'ente/azienda nelle e-mail o in altri messaggi corrispondono ai dati pubblicati sui loro siti web ufficiali o su altre fonti pubbliche. Le istituzioni/aziende di solito usano le loro caselle di posta dedicate invece delle caselle di posta generali disponibili pubblicamente (ad es. @ gmail.com, @ yahoo.com, ecc.).

2

Qualità e contenuto del testo. E-mail o messaggi ingannevoli spesso contengono errori materiali o stilistici. Il testo potrebbe essere tradotto letteralmente senza seguire le regole di quella lingua (usando programmi di traduzione disponibili pubblicamente). Il testo può anche utilizzare la lingua familiare, nomi o forme giuridiche imprecise di istituzioni o società (ad es. un'autorità pubblica può essere indicata come una società). I motivi o altre circostanze per contattarti possono essere descritti in modo tale da poter essere adattati a qualsiasi situazione (ad es. presumibilmente il dipartimento di polizia ti informa che i tuoi dati di accesso ai servizi bancari sono stati rubati e devi modificare immediatamente tali dati di accesso, ma non nomina nemmeno la banca).

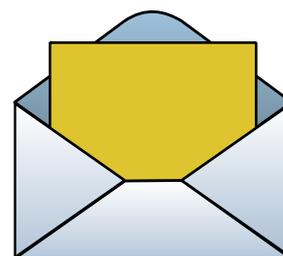
3

Collegamenti forniti. I link fraudolenti spesso contengono una serie di numeri o indirizzi web sconosciuti. Se non sei sicuro che un collegamento sia legittimo, non fare clic su di esso.

4

Probabilità di ottenere la richiesta o l'offerta. Dovresti valutare se avresti potuto aspettarti una lettera del genere e se è in linea con i fatti reali o con la pratica normale (ad esempio ricevi un'e-mail che ti informa che hai vinto alla lotteria anche se non hai partecipato ad alcuna lotteria; ricevi un messaggio presumibilmente dalla tua banca, anche se non invia mai messaggi in questo modo).

In caso di dubbi su un'e-mail o un messaggio ricevuto, contattare l'istituzione/società (che presumibilmente ti ha raggiunto) tramite i suoi dettagli di contatto pubblicamente disponibili sul sito Web ufficiale o su un'altra fonte affidabile.





4.6. REATI FINANZIARI E FRODI SUGLI INVESTIMENTI

I crimini finanziari sono crimini in cui le organizzazioni criminali beneficiano finanziariamente. Nei reati finanziari, di solito, una parte fornisce un vantaggio finanziario e l'altra parte subisce una perdita finanziaria. Questi sono spesso commessi a vantaggio personale del criminale e comportano la conversione illegale della proprietà dei beni coinvolti.

Quando parliamo di "frode dei consumatori" quando qualcuno subisce una perdita finanziaria che implica l'uso di pratiche commerciali ingannevoli, sleali o false. Negli ultimi due anni, ad esempio, il 60% dei consumatori europei che hanno acquistato online in un lasso di tempo di 12 mesi ha subito frodi. Nonostante le forti misure di sicurezza informatica adottate dalle istituzioni finanziarie (banche, società di pagamento, ecc.), i truffatori continuano a farsi strada sfruttando l'anello più debole della catena: gli esseri umani e la loro predilezione a fidarsi dei loro pari.

I tipi più comuni di frode:

- Phishing** | Email e telefonate, in cui i truffatori fingono di essere un'istituzione legittima per ottenere dati personali dalle loro vittime.
- Pharming** | è un reindirizzamento automatico dell'utente a pagine false gestite da truffatori con l'obiettivo di sottrarre informazioni personali riservate come password o numeri di conto bancario. A differenza di altri tipi di frode, il pharming non richiede azioni speciali da parte dell'utente (vittima). Nell'attacco, i truffatori cambiano semplicemente il DNS o altre query automaticamente, inserendo i propri siti Web invece di quelli desiderati dall'utente (vittima).
- Manipolazione di dispositivi** | Hacking di sistemi POS (point-of-sale), ATM. Smartphone o PC per accedere a dati e/o denaro.
- Frodi di identità** | Utilizzo dei dati personali dei consumatori per cancellare carte di credito, modificare password, aprire conti ecc.
- Ingegneria sociale** | Manipolazione delle vittime per ottenere informazioni riservate.
- Muli del denaro** | Ingannare persone innocenti nel riciclaggio di denaro rubato o illegale attraverso il loro conto bancario.





Come evitare di diventare una vittima di frode finanziaria:

- 1 Controlla regolarmente il tuo conto bancario e segnala qualsiasi attività sospetta alla tua banca.
- 2 Tieni presente che la tua banca non ti chiederà mai informazioni sensibili (ad esempio le credenziali del conto online) per telefono o e-mail.
- 3 Se pensi di aver fornito i dettagli del tuo account a un truffatore, contatta immediatamente la tua banca.
- 4 Effettua pagamenti online solo su siti sicuri: controlla la barra degli URL per il lucchetto e https e utilizza solo connessioni sicure (rete mobile invece di Wi-Fi pubblico).
- 5 Se un'offerta sembra troppo bella per essere vera, è quasi sempre una truffa.
- 6 Mantieni le tue informazioni personali al sicuro e protette.
- 7 Fai molta attenzione alla quantità di informazioni personali che condividi sui siti di social network. I truffatori possono utilizzare le tue informazioni e le tue immagini per creare un'identità falsa o per prenderti di mira con una truffa.
- 8 Segnala sempre qualsiasi tentativo di frode sospetto alla polizia, anche se non sei caduto vittima della truffa.





La frode sugli investimenti comporta la vendita illegale o presunta vendita di strumenti finanziari. I tipici schemi di frode sugli investimenti sono caratterizzati da offerte di investimenti a basso o nessun rischio, rendimenti garantiti, rendimenti eccessivamente consistenti, strategie complesse o titoli non registrati.



Tipi di frodi sugli investimenti:

Lo schema piramidale

È quando i truffatori affermano di poter trasformare un piccolo investimento in grandi profitti in un breve periodo di tempo. Ma in realtà, i partecipanti fanno soldi inserendo nuovi partecipanti nel programma. I truffatori dietro questi schemi in genere fanno di tutto per far sembrare i loro programmi legittimi schemi di marketing multilivello.

Lo schema Ponzi

Si verifica quando un truffatore o "hub" raccoglie denaro da nuovi investitori e lo utilizza per pagare presunti ritorni agli investitori nella fase precedente, piuttosto che investire o gestire il denaro come promesso. Gli schemi Ponzi richiedono un flusso costante di denaro in entrata per rimanere a galla. Ma a differenza degli schemi piramidali, gli investitori in uno schema Ponzi in genere non devono reclutare nuovi investitori per guadagnare una quota di "profitti".

Pump-and-Dump

È uno schema in cui un truffatore acquista deliberatamente azioni di un titolo a un prezzo molto basso di una piccola società poco quotata e quindi diffonde informazioni false per suscitare interesse nelle azioni e aumentare il prezzo delle azioni. Credendo che stiano ottenendo un buon affare su un titolo promettente; gli investitori creano domanda di acquisto a prezzi sempre più elevati. Il truffatore quindi scarica le sue azioni al prezzo elevato e svanisce, lasciando molte persone catturate con azioni senza valore.

Advance Free Fraud

È un tipo di frode che gioca sulla speranza di un investitore di essere in grado di invertire un precedente errore di investimento che implica l'acquisto di un'azione a basso prezzo. La truffa generalmente inizia con un'offerta per pagarti un prezzo allettantemente alto per azioni senza valore. Per accettare l'affare, è necessario inviare una commissione in anticipo per pagare il servizio. Ma se lo fai, non vedrai mai più quei soldi - o nessuno dei soldi dell'affare.





Come evitare di diventare una vittima di frode sugli investimenti:

1

Verificare la licenza della persona che vende l'investimento

2

Verificare che l'investimento sia registrato

3

Attenzione alle promesse di alti tassi di rendimento e/o rapidi profitti quick

4

Diffidare delle vendite ad alta pressione

5

Attenzione alle offerte indesiderate

6

Richiedi un prospetto o una circolare di offerta

7

Parla con una persona di terze parti

8

Fai attenzione alle truffe online





4.7. FAKE NEWS E PROPAGANDA

La propaganda è definita come la diffusione deliberata e coerente di teorie e idee in filosofia, scienza, religione, ecc., al fine di educare le persone ad utilizzarle, influenzando le opinioni, gli stati d'animo delle persone, manipolando, promuovendo determinate azioni che potrebbero contribuire agli obiettivi definiti dal propagandista.

L'efficacia della propaganda consiste nel fornire parzialmente la verità ma non fornendo tutte le informazioni e nascondendo alcuni fatti, distorcendo l'intero contesto. Pertanto, riconoscere la propaganda a volte può essere difficile in quanto l'esattezza dei fatti presentati può essere verificata, il messaggio inviato dalla propaganda sembra essere vero quindi questo può essere fuorviante.

La propaganda è spesso definita in un contesto negativo come un mezzo inaccettabile e basato sulla disinformazione per plasmare l'opinione pubblica. I sinonimi usati per descrivere la propaganda includono, ma non si limitano a, bugia, inganno, distorsione, manipolazione, lavaggio del cervello, controllo del pensiero e guerra psicologica.

Tuttavia, la propaganda viene utilizzata anche per scopi di marketing, sociali ed educativi, i. e. la propaganda può funzionare in un contesto positivo e la cosa più importante è a cosa serve. Ad esempio, le rappresentazioni del danno del fumo sui contenitori di sigarette è anch'essa propaganda in quanto ha un tentativo di influenzare le persone con le emozioni e cambiare il loro comportamento, i. e. per costringerli a smettere di fumare.



Tuttavia, la propaganda viene spesso utilizzata per scopi negativi per incitare all'odio e all'ostilità. Costantemente influenzata da cambiamenti sociali, tecnologici, culturali ed economici, deve quindi adattarsi e agire in modo coerente con la personalità dell'uomo moderno. La propaganda è spesso associata ai manifesti della seconda guerra mondiale, ma ora ha assunto una varietà di forme più sottili, può essere ovvio come una svastica o sottile come un commento su un portale di notizie.





Secondo l'obiettività, la propaganda può essere suddivisa in bianco, grigio e nero.

La propaganda bianca



è la rappresentazione più trasparente e aperta dei fatti. Viene utilizzato per vari programmi e iniziative sociali. La propaganda bianca cerca di presentare i risultati di esperti indipendenti che riflettono punti di vista chiave.

Tuttavia, con la concorrenza alle stelle tra le diverse organizzazioni pubbliche e commerciali, sta diventando sempre più difficile determinare l'equità dell'approccio e le opinioni degli esperti sulle stesse questioni stanno diventando molto diverse. Pertanto, chiamiamo propaganda bianca un'intenzione di fornire spiegazioni ragionate senza alcuno sforzo per distorcere i fatti.

Molto spesso, la propaganda bianca parla dei risultati raggiunti dal paese, dall'azienda o dall'organizzazione ed è positiva.

Propaganda grigia

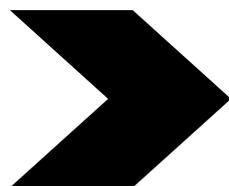


I suoi rappresentanti associano deliberatamente i fatti accertati a quelli non confermati, presentando solo un'interpretazione a loro favore, e distorcono deliberatamente il contesto dell'evento. La propaganda grigia viene utilizzata in modo intensivo nei conflitti informativi, politici o economici guidati.

La propaganda grigia forma un approccio unilaterale all'argomento, evitando le critiche. Tale propaganda, ad esempio, afferma che il proprio esercito ha sempre ragione. I rappresentanti di questa propaganda evitano il dialogo aperto che può sfociare in una divulgazione, ma non si attengono a una bugia unilaterale, lasciando al loro atteggiamento l'opportunità di cambiare.

La propaganda grigia è diffusa sui canali televisivi russi ORT e RTV durante la presidenza di Vladimir Putin, quando qualsiasi informazione su Putin e sulla Russia viene presentata positivamente, anche se il forum internazionale critica fortemente la Russia per alcune decisioni.

La propaganda nera



si basa sulla deliberata falsificazione di eventi e fatti, i. e. bugie. Era particolarmente diffuso nella Germania nazista, dove venivano usati metodi di messa in scena degli eventi. I nazisti, ad esempio, travestiti con le uniformi dei soldati sovietici, devastarono i villaggi polacchi, intimidendo la gente del posto con l'imminente governo comunista e le sue conseguenze.

Anche la propaganda nera si basa sulla tecnologia nera. Ad esempio, durante un'elezione, le informazioni vengono diffuse per conto di un avversario o gli eventi vengono organizzati in modo che in seguito complichino notevolmente le possibilità dell'avversario di essere eletto. La propaganda nera e la tecnologia nera sono perseguitate in molte democrazie.



Pertanto, la comunicazione propagandistica di solito non è del tutto obiettiva e presenta i fatti in modo selettivo per influenzare gli atteggiamenti. Il linguaggio sovraffollato viene spesso utilizzato per suscitare una risposta emotiva alle informazioni presentate piuttosto che alla mente.

Nell'era digitale in cui viviamo ora, questo tentativo consapevole di diffondere informazioni distorte si sta verificando anche su piattaforme digitali. Il suo scopo è di trarre in inganno e ingannare. Quindi possiamo parlare audacemente di "propaganda digitale" (Bjola, 2018, p. 307).

Da quando il processo di propaganda si è spostato nello spazio online, sono emerse nuove forme di propaganda note come troll e bot. Il loro scopo è influenzare i risultati elettorali, demoralizzare, screditare o isolare gli oppositori politici, partecipare ai sondaggi dell'opinione pubblica e diffondere notizie false.

I troll sono decine di migliaia di persone assunte dai propagandisti per lavorare tutto il giorno (o la notte) sui portali di notizie destinate al pubblico, sui social network per commentare le ultime notizie e post per aumentare gli utenti di Internet, diffondere la disinformazione, disprezzare i valori prevalenti (Grigaliūnas, 2016).



Come riconoscere un troll?

- Errori di ortografia;
- Spesso un account femminile;
- Piccolo numero di follower;
- Condivide i messaggi @ il nome di una persona specifica, come @putin_leader;
- Afferma di fare riferimento a fonti alternative ma non le indica;
- Commenta o condivide post, post solo su un argomento specifico





Un bot è un programma per computer che esegue automaticamente determinate azioni che una persona che lavora su un computer può eseguire. Nella propaganda, i bot vengono utilizzati per scrivere commenti di propaganda sui portali di notizie e post sui social network. Questi programmi generano commenti diversi: viene creato un modello e da quel modello viene rigenerato un nuovo commento. I server proxy forniscono indirizzi IP diversi, quindi sembra che molte persone diverse scrivano commenti. Ad esempio, circa il 15% degli utenti di Twitter sui social network sono bot.



Come riconoscere un bot?

- Prestare attenzione alla foto del profilo. Di solito si tratta di disegni, immagini della natura, foto di politici o celebrità o nessuna foto del profilo. Puoi trovare l'origine di una foto del profilo utilizzando la ricerca di Google Immagini.
- Nome utente lungo. Il nome utente di molti bot è insolito, con numeri o nessun significato.
- Contenuti generici o post o messaggi duplicati. I bot sono progettati per dominare un argomento particolare o taggare # sui social network. Per raggiungere questo obiettivo, un messaggio o un post viene condiviso molte volte.
- L'account utente è vuoto. Gli account utente creati dall'uomo contengono molte informazioni personali, create da bot: nessuna o solo informazioni di base.
- I bot seguono molte più persone sui social network di quanti ne abbiano loro stessi.
- I bot condividono molti post e messaggi. Se un utente condivide costantemente molti record, anche di notte, ci sono buone probabilità che si tratti di un bot.
- I bot condividono post o messaggi di contenuto politico radicale. Questi sono solitamente cliché ideologici, testi patriottici, militaristici contro valori e atteggiamenti prevalenti.
- Molte registrazioni stereotipate, come sentimenti, video con animali e così via, nel feed delle notizie degli utenti. Tali contenuti vengono utilizzati dai bot durante le pause tra le elezioni o altri eventi rilevanti

Puoi verificare se non stai seguendo i bot sul social network Twitter qui: <https://botcheck.me>

A proposito, non ci sono solo troll ma anche elfi. Si tratta di solito di persone attive che mostrano la disinformazione e le manipolazioni, combattendo i divulgatori di notizie false e propaganda nello spazio online.





Mezzi che possono essere usati nella propaganda

La generalizzazione

è un tentativo di influenzare le emozioni usando le astrazioni; è una delle forme più semplici di propaganda. Questo metodo è spesso utilizzato durante le campagne elettorali dei politici. Questo metodo è particolarmente efficace in tempi difficili, come una crisi economica. Vengono spesso utilizzate affermazioni sommative emotive, come Meritiamo di vivere meglio, Per il futuro, Ogni uomo è della massima importanza, ecc.

I simboli

aiutano a migliorare la propria immagine. Ad esempio, una persona in una fotografia è circondata da determinati oggetti simbolici che formano un'immagine che quella persona sta promuovendo i valori simboleggiati.

L'etichettatura

è quando un'idea, un'azione, un termine negativi sono associati a una persona, un'organizzazione specifica e così via. Il sarcasmo o il ridicolo sono spesso usati. Questo è un modo efficace di propaganda, perché le etichette come - bugiardi, terroristi, corrotti - sono difficili da eliminare.

Il sentimento del branco

crea un'immagine di accettazione diffusa da parte del gruppo, che isola e fa sentire fuori luogo chi non l'accetta.

L'eccitazione emotiva

cerca di evocare emozioni così forti come paura, rabbia, tristezza e risentimento. Il tentativo più comune è mostrare che l'uno o l'altro fenomeno avrà conseguenze negative, utilizzando una varietà di paure umane.

Insabbiamento dei fatti

è quando vengono raccontati solo i fatti positivi e i fatti negativi vengono messi a tacere. Sebbene gli argomenti utilizzati nell'utilizzo di questa tecnica siano generalmente validi, spesso vengono presentate statistiche che possono distorcere la situazione perché le informazioni vengono estrapolate dal contesto o vengono omessi fatti importanti. Nelle campagne politiche, un candidato viene presentato solo sul lato positivo, omettendo il negativo.



C.R.A.P. test

Un rapido controllo dell'esattezza delle informazioni di un sito può essere effettuato utilizzando C.R.A.P. test (valuta, affidabilità, autorità e scopo/punto di vista). Questo test consente di scoprire quando e in quali circostanze è stato scritto il testo pubblicato, quanto sia affidabile il suo autore e, infine, lo scopo e l'atteggiamento di queste informazioni (CyberWise, 2019).

<p style="text-align: center;">Affidabilità</p> <ul style="list-style-type: none"> • Che tipo di informazioni sono incluse nella notizia? • Il contenuto della risorsa è principalmente un'opinione? È equilibrato? • Il creatore fornisce riferimenti o fonti per dati o citazioni? 	<p style="text-align: center;">Attualità</p> <ul style="list-style-type: none"> • Quanto sono recenti le informazioni? • Quanto recentemente è stato aggiornato il sito web? • È abbastanza attuale per il tuo argomento?
<p style="text-align: center;">Autore</p> <ul style="list-style-type: none"> • Chi è il creatore o l'autore? • Quali sono le credenziali? Si trovano informazioni sul background dell'autore? • Chi pubblica o chi è lo sponsor? • Sono fonti rispettabili? • Qual è l'interesse dell'editore (se presente) in queste informazioni? • Ci sono pubblicità sul sito web? In caso affermativo, vengono cancellati contrassegnati? 	<p style="text-align: center;">Scopo/Punto di vista</p> <ul style="list-style-type: none"> • Si tratta di un fatto o di un'opinione? L'autore elenca le fonti? • È di parte? Sembra che l'autore stia cercando di spingere un'agenda o un lato particolare? • Il creatore/autore sta cercando di venderti qualcosa? Se sì, è chiaramente indicato?





Modi per contrastare

Con così tante informazioni disponibili su tutte le piattaforme digitali, è facile essere ingannati. Gli studi dimostrano che circa il 75% delle persone che vedono notizie false non è in grado di riconoscere che sono effettivamente false.

Pertanto, un modo rapido per verificare se un'informazione è reale o meno è utilizzare il C.R.A.P. Test. Scopri se l'articolo è attuale, affidabile, se l'autore è credibile e infine lo scopo e il punto di vista dell'articolo (CyberWise, 2019).

Sicuramente è sempre necessario il buon senso. Alcuni modi per individuare le notizie false sono brevemente mostrati di seguito (Come individuare le notizie false, n.d.).

- Considera la fonte: cerca di saperne di più sulla fonte e valuta se è credibile.
 - Leggi oltre: i titoli possono essere scandalosi, al fine di ottenere più clic. Cerca ulteriori informazioni sulla storia narrata e cerca di scoprire la verità.
 - Controlla l'autore: l'autore ha pubblicato altri post, oltre a quello attuale? Ha ricevuto commenti o giudizi sulla sua credibilità?
 - Fonti di supporto: di solito un sito Web elenca altri collegamenti relativi all'argomento dell'articolo fornito. Controlla se questi link sono realmente correlati all'articolo iniziale o se sono solo fuorvianti.
-
- Controlla la data: le informazioni sono aggiornate o sono state ripubblicate?
 - È uno scherzo? Nel caso in cui l'informazione sia davvero bizzarra, potrebbe essere satira. Devi controllare di nuovo l'autore e la fonte, per essere sicuro.
-
- Controlla i tuoi pregiudizi: pensa se le notizie che stai leggendo, come influenzano i tuoi pregiudizi. Probabilmente potresti rifiutarli, perché non sei d'accordo. Ma questo non rende la notizia falsa.
 - Chiedi agli esperti: ci sono alcuni siti di verifica dei fatti che puoi visitare per essere sicuro delle informazioni fornite.





Casi studio

Un esempio di campagna di propaganda è quella tra Russia e Stati Uniti d'America, riguardante le elezioni presidenziali del 2016. Il motivo principale alla base della formazione dei risultati elettorali è stata la comparsa di una serie di fake news per indirizzare i cittadini americani a votare per Trump.

Cambridge Analytica, una società specializzata nell'analisi dei dati e nella costruzione di profili psicologici per scopi politici utilizzando i dati raccolti dagli utenti americani di Facebook, ha compilato i profili elettorali di migliaia di persone nel periodo precedente alle elezioni presidenziali per sostenere la campagna elettorale di Donald Trump.

Gli utenti di Facebook che sono stati analizzati sono stati divisi in due categorie. Il primo includeva gli elettori che intendevano votare per l'avversario di Trump, mentre il secondo includeva coloro che intendevano astenersi. Questa è stata seguita da una campagna mirata di notizie false su Hillary Clinton.



Le "notizie" presentate agli elettori di prima classe avevano lo scopo di persuaderli a non votare, mentre quelle viste sul cellulare di seconda classe avevano lo scopo di esortarli a votare per Trump. Secondo un sondaggio della Stanford University, il 41% delle fake news nell'ultimo mese prima delle elezioni è diventato virale. Facebook ha ufficialmente ammesso che 126 milioni di americani, circa il 40% della popolazione totale degli Stati Uniti, hanno visto notizie e post sui social network, che sono stati "piantati" dall'ormai famigerata Internet Research Agency, con sede a St. Louis. Pietroburgo (Tsompanidis, 2018).

Un esempio della facilità con cui oggi si diffondono le fake news è la scoperta di nuove ricette fatte in casa, che dovrebbero uccidere il Covid-19, il nuovo coronavirus. Abbiamo sentito cose come "bere alcol uccide il virus", "bere biossido di cloro rafforza il sistema immunitario". Queste opinioni sono, almeno, pericolose. Ma una ricetta che è stata rapidamente diffusa sui social media è stata quella che sostiene che l'aglio bollito uccide il Covid-19 "Buone notizie, il coronavirus di Wuhan può essere curato con una ciotola di acqua all'aglio appena bollita. Il vecchio medico cinese ha dimostrato la sua efficacia. Molti pazienti hanno anche dimostrato che questo è efficace. Otto (8) spicchi d'aglio tritati aggiungere sette (7) tazze d'acqua e portare a ebollizione. Mangia e bevi l'acqua bollita dell'aglio, miglioramento notturno e guarigione. Felice di condividere questo " (Spencer, 2020). Questa voce è stata così diffusa che l'Organizzazione Mondiale della Sanità (OMS) l'ha smentita riportando che "L'aglio è un alimento sano che può avere alcune proprietà antimicrobiche. Tuttavia, non ci sono prove dall'attuale epidemia che mangiare aglio abbia protetto le persone dal nuovo coronavirus "(Spencer, 2020).



I modi migliori per respingere la propaganda è:

- Utilizzare media responsabili e indipendenti;
- Decostruire i miti e evitare la comunicazione strategica;
- Costruire una società libera ed educata;
- Sviluppare continuamente la capacità di valutare criticamente le informazioni;
- Formazione e rafforzamento della narrativa e della memoria storica nazionale.

Esempio: La storia lituana di Bayraktar

"Centinaia di lituani hanno raccolto circa 4,7 milioni dollari in tre giorni e mezzo per comprare il Bayraktar senza pilota in Ucraina. È stato abbattuto in 3,5 minuti dopo la sua prima ascesa".

È stato presentato da un "canale Twitter anonimo che pubblica notizie di fantasia". I commentatori non sembravano aver prestato attenzione a questo dettaglio e hanno preso sul serio il messaggio.

Nel maggio 2022, centinaia di lituani si sono uniti per acquistare un drone militare avanzato per supportare l'Ucraina nella sua guerra contro la Russia in segno di solidarietà con un altro paese dell'ex Unione Sovietica.

L'obiettivo di 5 milioni di euro è stato raccolto in soli tre giorni e mezzo, in gran parte in piccoli importi compresi tra 5 e 100 euro, per finanziare l'acquisto di un drone militare Bayraktar TB2, secondo Laisves TV, l'emittente Internet lituana che ha lanciato la notizia.

Il drone si è dimostrato efficace negli ultimi anni contro le forze russe e i loro alleati nei conflitti in Siria e Libia, e il suo acquisto è orchestrato dal Ministero della Difesa lituano.

Per accedere alla storia completa <https://lithuania.postsen.com/news/7172/Russian-propaganda-lie-Bayraktar-for-whom-Lithuanians-raised-money-has-already-been-shot-down.html>

Per maggiori informazioni sulla propaganda nell'era digitale e sulle fake news puoi visitare:

https://www.youtube.com/watch?v=5__dZBZuzZc&ab_channel=OsloFreedomForum

https://www.youtube.com/watch?v=V4o0B6IDo50&ab_channel=CyberWise

<https://www.cyberwise.org/fake-news>

<https://www.cybercivics.com/>

Lithuania Posts English > الأرشيف > Breaking News

✔ Russian propaganda lie: Bayraktar, for whom Lithuanians raised money, has already been shot down

BREAKING NEWS Glenn • Breaking News • 3 months ago • 190





COMPITO PRATICO. Scuoti il cane

Incoraggia il gruppo di partecipanti a guardare Wag the Dog, una commedia nera di satira politica americana del 1997 prodotta e diretta da Barry Levinson e interpretata da Dustin Hoffman e Robert De Niro.

Scopo dell'attività:

praticare e analizzare le capacità di osservazione personale/pensiero critico.

Abilità che l'attività sviluppa:

osservazione critica.

Per quante persone è adatta l'attività:

lavoro individuale con successiva discussione di gruppo.

Tempo richiesto per l'attività

97 minuti per la visione di film e fino a 15 minuti per una discussione moderata

Istruttori necessari?

Uno per moderare la discussione.

Altri requisiti per l'attività (spazio, attrezzatura...):

a casa/auditorium/sessione online.

Descrizione dell'attività:

mentre guardi il film, chiedi ai partecipanti di osservare come stanno andando le cose. Invita i membri del gruppo a riflettere su diversi aspetti della frase politica "il cane scodinzola".

In primo luogo, può essere utilizzato per indicare che l'attenzione viene volutamente deviata da qualcosa di maggiore importanza a qualcosa di minore importanza.

In secondo luogo, se dici che il cane scodinzola, significa che una parte piccola o non importante di qualcosa sta diventando troppo importante e sta controllando l'intero processo dei fatti.





4.8. PUBBLICITÀ FRAUDOLENTA (PRODOTTI FALSI, INTEGRATORI)



Ogni volta che si tratta di denaro, c'è sempre l'opportunità di una frode. Da un punto di vista tecnico, la frode pubblicitaria online è stata un'attività relativamente facile (e sì, redditizia) per i truffatori e un disastro finanziario per gli inserzionisti, gli editori e le stesse piattaforme pubblicitarie online.

Il business degli annunci online è stato costruito su una serie di tecnologie Internet Open Standard che non hanno mai inteso essere a prova di frode / truffa / furto. Di conseguenza, i truffatori pubblicitari hanno avuto un enorme vantaggio. Secondo Juniper, nel 2019 l'industria della pubblicità online ha dovuto affrontare una straordinaria perdita di \$ 42 miliardi a causa di frodi pubblicitarie e sfortunatamente non c'è motivo di credere che la cifra sarà inferiore quest'anno.

Per chiarire, la frode pubblicitaria digitale è un'attività intenzionale che impedisce agli annunci pubblicitari di essere consegnati al pubblico o alla posizione giusta. I rischi dannosi che i professionisti del marketing devono affrontare oggi stanno diventando sempre più sofisticati, e quindi maggiori, di quanto previsto in precedenza.

L'ambiente della pubblicità digitale ora coinvolge migliaia di intermediari, presentando una pletera di angoli oscuri in cui i truffatori possono nascondere attività criminali. I truffatori sanno quando vengono osservati e sono diventati ancora più pericolosi, il che rende ancora più difficile prevenire le frodi pubblicitarie.





Di conseguenza, il 96 per cento dei consumatori afferma di avere poca fiducia nella pubblicità digitale, rendendo più difficile per i professionisti del marketing dimostrare che i propri annunci sono legittimi. Quindi, quali misure dovrebbero intraprendere le organizzazioni per evitare di perdere gran parte del loro budget a causa di frodi e, con esse, di fiducia dei consumatori?

Anche se una piccola percentuale di consumatori fa ancora clic sugli annunci fraudolenti e acquista prodotti o servizi falsi, è ancora un'enorme intenzione commerciale e monetaria sviluppare le tecniche e gli sforzi di marketing.

Il consumatore intelligente deve assumersi parzialmente la responsabilità di mitigare le frodi nella pubblicità segnalando falsi e scoraggiando le persone meno abili intorno a loro a interagire con tali annunci.

Come riconoscere le pubblicità false?

È relativamente facile una volta compreso e conosciuto lo schema:

- 1 La qualità degli annunci online di solito si distingue per essere scarsa e ripetitiva nei contenuti;
- 2 Affermazioni e promesse enormi e irrealistiche di fornire risultati piuttosto impossibili per arricchirsi rapidamente o per far ricrescere i capelli persi;
- 3 Le pagine di destinazione saranno ospitate sotto nomi di dominio strani, marchi sconosciuti, verranno utilizzate foto di celebrità o professionisti inesistenti;
- 4 Il carattere utilizzato nelle pagine di destinazione si distingue per essere colorato, molto incentivante ad agire e vengono offerti grandi sconti;
- 5 La pagina di destinazione e la pagina di descrizione del prodotto potrebbero contenere una grande quantità di recensioni false e per lo più molto positive





4.9. PC/GIOCHI ONLINE, CASINÒ, DIPENDENZA

Il gioco è una pulsione umana innata, che appare nella prima infanzia (Kuss & Griffiths, 2012, p. 5). Dopo il millennio il gioco su Internet è aumentato notevolmente a causa dell'enorme sviluppo tecnologico. I giochi per PC e, in generale, i giochi online offrono ai giocatori l'opportunità di sperimentare diversi ambienti di gioco contemporaneamente, di progettare e sviluppare personaggi virtuali con cui potrebbero identificarsi e anche di giocare con altri giocatori di tutto il mondo in qualsiasi momento (Kuss & Griffiths, 2012, pag. 5).

Inoltre, il gioco online consente ai giocatori di comunicare con gli altri tramite chat e, quindi, stabilire nuove relazioni (Kuss, 2013, p. 125). Un altro motivo per cui il gioco su Internet sembra così attraente per alcune persone è che dà la possibilità di sfuggire ai problemi della vita reale e in questo modo il gioco online si trasforma in una strategia di coping. (Bacio, 2013, pag. 125).

Una delle categorie più famose di giochi online sono i Massively Multiplayer Online Role-Playing Games (MMORPG), come "World of Warcraft". Questo tipo di giochi consente ai giocatori di fissare obiettivi e raggiungerli, come l'avanzamento di livello, guadagnando così uno status virtuale e un potere più elevati nell'ambiente di gioco. I giocatori possono anche motivare a causa dell'ammirazione che potrebbero ricevere dalla comunità di gioco (Kuss, 2013, p. 125).



D'altro canto, gli aspetti della socializzazione e della fuga possono essere predittivi di una dipendenza dal gioco online (Kuss, 2013, p. 125). Altre conseguenze negative sono l'ignoranza delle relazioni della vita reale, il rifiuto del sonno, del lavoro e dello studio, l'ossessione per il gioco, la mancanza di attenzione con conseguente aggressività e aumento dello stress, difficoltà con la memoria verbale e alti livelli di solitudine (Kuss, 2013, pag. 125).

In alcuni paesi, come i paesi del sud-est asiatico, le conseguenze negative del gioco online sono state così gravi che i governi hanno preso provvedimenti e misure per ridurre questi impatti negativi. Ad esempio, in Giappone, il governo ha riconosciuto la gravità delle conseguenze che portano allo sviluppo di "campi di digiuno", in cui le persone dipendenti dal gioco online sono aiutate dalla totale esclusione dalla tecnologia (Kuss, 2013, p. 125).





Casino addiction

Il gioco d'azzardo nei casinò è un'attività molto popolare in tutto il mondo. Negli ultimi quindici anni l'ambiente del gioco d'azzardo è cambiato in modo significativo attraverso l'aumento della disponibilità del gioco d'azzardo online (Gainsbury, 2015, p. 190). Al giorno d'oggi un dispositivo abilitato a Internet e un clic di un pulsante è tutto ciò che serve per avere accesso a un ambiente di gioco. Oltre a ciò, l'accesso è abilitato anche grazie alla facilità con cui è possibile spendere denaro tramite carte di credito, bonifici bancari elettronici e portafogli elettronici.

Casinò online e gioco d'azzardo hanno sollevato polemiche sulla possibile dipendenza conseguente (Gainsbury, 2015, p. 190). La quinta edizione del Manuale Diagnostico e Statistico dei Disturbi Mentali (DSM-5) ha aggiunto una nuova categoria di Dipendenza comportamentale non da sostanze nel contesto della categoria Dipendenza da sostanze. Per diagnosticare una dipendenza dal gioco, l'individuo deve menzionare quattro o più dei seguenti (DSM-5):

- 1 Ha bisogno di scommettere con quantità di denaro crescenti per raggiungere l'eccitazione desiderata.
- 2 È irrequieto o irritabile quando cerca di ridurre o interrompere il gioco d'azzardo.
- 3 Ha compiuto ripetuti sforzi infruttuosi per controllare, ridurre o interrompere il gioco d'azzardo.
- 4 È spesso preoccupato per il gioco d'azzardo (ad esempio, ha pensieri persistenti di rivivere esperienze di gioco passate, handicap o pianificazione della prossima impresa, pensando a modi per ottenere denaro con cui giocare).
- 5 Spesso gioca d'azzardo quando si sente angosciato (ad esempio, impotente, colpevole, ansioso, depresso).
- 6 Bugie per nascondere l'entità del coinvolgimento con il gioco d'azzardo.
- 7 Ha compromesso o perso una relazione significativa, un lavoro o un'opportunità educativa e/o di carriera a causa del gioco d'azzardo.
- 8 Si affida ad altri per denaro per alleviare situazioni finanziarie disperate causate dal gioco d'azzardo





Fattori di rischio per il gioco d'azzardo su Internet (Gainsbury, 2015, p. 190)

- Giovani adulti e adolescenti più grandi
- Maschio
- Abuso di alcol o droghe
- cognizioni irrazionali
- Forza di volontà per fare soldi velocemente e facilmente

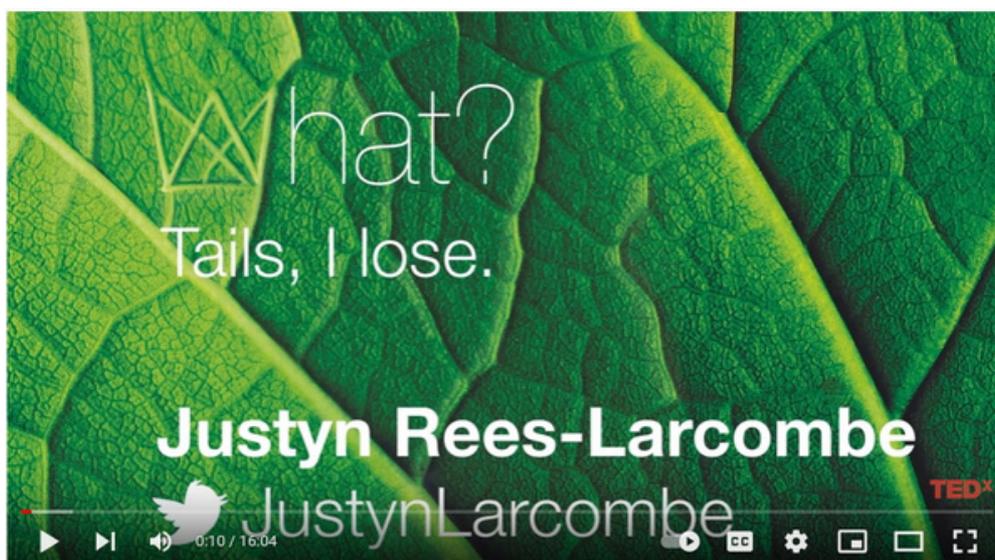


Tuttavia, gli studi condotti finora non definiscono uno specifico modello personale e comportamentale per distinguere tra giocatori d'azzardo problematici su Internet e non.



Nel seguente link puoi trovare la storia di un uomo, di nome Justyn Rees Larcombe, che ha scommesso 750.000 sterline e ha perso anche la sua famiglia.

https://www.youtube.com/watch?v=7AN3VLLikdl&ab_channel=TEDxTalks





RUOLO DEL GOVERNO E ISTITUZIONI DOVE CANDIDARSI

5.1. REGOLAMENTO SULLA PRIVACY ELETTRONICA NELL'UE



Il Regolamento ePrivacy (ePR) è una proposta per la regolamentazione di varie tematiche legate alla privacy, principalmente in relazione alle comunicazioni elettroniche all'interno dell'Unione Europea. Il suo nome completo è "Regolamento del Parlamento europeo e del Consiglio relativo al rispetto della vita privata e alla protezione dei dati personali nelle comunicazioni elettroniche e che abroga la direttiva 2002/58/CE (Regolamento sulla privacy e sulle comunicazioni elettroniche)." Abroga la direttiva 2002 sulla privacy e sulle comunicazioni elettroniche (direttiva ePrivacy) e sarebbe *lex specialis* del regolamento generale sulla protezione dei dati. Sarebbe dettagliare e integrare quest'ultimo per quanto riguarda le questioni relative alla privacy. Ambiti chiave della proposta di regolamento sono la riservatezza delle comunicazioni, il controllo della privacy tramite consenso elettronico e Browser, i cookie.

L'ambito di applicazione del regolamento ePrivacy è ancora in discussione. Secondo alcune proposte, si applicherebbe a qualsiasi azienda che elabora dati in relazione a qualsiasi forma di servizio di comunicazione online, utilizza tecnologie di tracciamento online o si occupa di marketing diretto elettronico.





Alcuni dei più importanti e.provisions della normativa privacy ancora in discussione:

Nuovi partecipanti al mercato	<p>Il 92% degli europei afferma che è importante che la posta elettronica e i messaggi online siano mantenuti riservati. Tuttavia, l'attuale direttiva e-privacy si applica solo agli operatori di telecomunicazioni tradizionali. Le regole sulla privacy ora si applicheranno anche ai nuovi fornitori di servizi di comunicazione elettronica come WhatsApp, Facebook Messenger, Skype, Gmail, iMessage o Viber.</p>
Regole più severe	<p>Il fatto che l'attuale direttiva sia per essere aggiornata con un regolamento direttamente applicabile significa che a tutti i cittadini e alle imprese dell'UE sarà garantita la stessa protezione per le loro comunicazioni elettroniche e un insieme di norme si applicherà in tutta l'UE.</p>
Contenuto e Metadati delle Comunicazioni	<p>Si propone di garantire la riservatezza del contenuto e dei metadati (come l'ora e il luogo della chiamata) delle comunicazioni elettroniche. Sia il contenuto che i metadati delle comunicazioni elettroniche sono altamente privati e le norme proposte richiederebbero che siano resi anonimi o distrutti (a meno che tali dati non siano necessari ai fini della fatturazione) se gli utenti non acconsentono al loro trattamento.</p>
Nuove opportunità di business	<p>Ottenendo l'autorizzazione al trattamento dei dati di comunicazione (contenuti e/o metadati), gli operatori di telecomunicazioni tradizionali avranno maggiori possibilità di utilizzare i dati e fornire servizi aggiuntivi. Ad esempio, saranno in grado di produrre mappe a colori che mostrano dove si trovano le persone; tali mappe potrebbero essere utili per le autorità pubbliche e le aziende di trasporto durante la preparazione di nuovi progetti infrastrutturali.</p>
Regole per i cookie più semplici	<p>Sarebbe semplificata la cd cookie policy, che prevede che gli utenti di Internet rispondano costantemente alle richieste di autorizzazione all'uso dei cookie. Le nuove regole darebbero agli utenti un maggiore controllo sulle proprie impostazioni di navigazione fornendo un modo semplice per accettare o rifiutare i cookie persistenti e altri identificatori se la privacy è a rischio. La proposta chiarisce che non sarà più richiesto il consenso per i cookie non invasivi (come i cookie per ricordare cosa è stato aggiunto al carrello) utilizzati per garantire la comodità della navigazione online. Il consenso non sarebbe più necessario anche per i cookie utilizzati per contare i visitatori del sito web.</p>
Protezione da spam	<p>Tra le proposte fatte vi è il divieto di inviare messaggi non richiesti con tutti i mezzi di comunicazione elettronica, come e-mail o SMS se non è stata ottenuta l'autorizzazione dell'utente. Gli Stati membri possono decidere di avvalersi dell'opzione per concedere ai consumatori il diritto di rinunciare alle chiamate di telemarketing, ad esempio inserendo il proprio numero in un elenco da non chiamare. I chiamanti di marketing dovranno visualizzare il proprio numero di telefono o utilizzare un codice speciale per identificarlo come una chiamata di marketing.</p>
Applicazioni più efficaci	<p>Le autorità nazionali per la protezione dei dati avrebbero il compito di garantire il rispetto delle regole di riservatezza stabilite nel regolamento..</p>





Le sanzioni proposte per l'inadempienza sarebbero fino a 20 milioni di euro o, nel caso di un'impresa, fino al 4% del fatturato totale annuo mondiale, se superiore. Il Regolamento ePrivacy doveva originariamente entrare in vigore il 25 maggio 2018, insieme al GDPR, ma non è ancora stato adottato.

Video: The impact of the European ePrivacy regulation

<https://www.youtube.com/watch?v=Q8YFLkvEcLE>



Differenza tra regolamento e direttiva

1

Differenza tra regolamento e direttiva .

2

Contrariamente a una Direttiva UE, un Regolamento UE è un atto giuridico dell'Unione Europea che diventa immediatamente efficace come legge in tutti gli Stati membri contemporaneamente.

3

L'attuale Direttiva ePrivacy è un atto giuridico dell'Unione Europea che richiede agli Stati membri di raggiungere un determinato risultato senza dettare i mezzi per raggiungere tale risultato. Pertanto è stato recepito nelle leggi e nei regolamenti nazionali.

4

Se il regolamento ePrivacy proposto diventasse effettivo, queste leggi sarebbero sostituite e probabilmente (per ragioni di chiarezza) saranno abrogate. Il regolamento ePrivacy sarebbe autoeseguibile e non richiederebbe molte misure di attuazione.





5.2. GDPR E CCPA



Il Regolamento generale sulla protezione dei dati (GDPR) è una legge sulla privacy e sulla sicurezza relativa alla protezione dei dati personali. È considerato dato personale qualsiasi informazione che può, direttamente o indirettamente, portare all'identificazione di una persona (Goddard, 2017, p. 703). I dati personali includono informazioni relative alla posizione, etnia, sesso, dati biometrici, credenze religiose o cookie web. I dati pseudonimi possono anche essere inclusi nel contesto dei dati personali, se è facile rivelare l'identità di un individuo. Il GDPR è stato attuato e approvato dall'Unione Europea (UE), tuttavia impone obblighi alle organizzazioni di tutto il mondo a condizione che interagiscono e raccolgano dati relativi ai cittadini dell'UE (Wolford, 2019). In questo modo tutti i residenti nell'UE sono protetti dal luogo del trattamento dei dati.

Breve sguardo storico

<p>1950</p> <p>La Convenzione europea dei diritti dell'uomo ha affermato che "ognuno ha il diritto di proteggere la propria vita privata e familiare"</p>	<p>1995</p> <p>La direttiva europea sulla protezione dei dati ha implementato gli standard minimi di privacy e sicurezza dei dati</p>	<p>2000</p> <p>Molte organizzazioni finanziarie offrivano transazioni online</p>
<p>2006</p> <p>Facebook ha fatto la sua prima apparizione</p>	<p>2011</p> <p>Un utente di Google ha citato in giudizio l'azienda per aver controllato le sue e-mail</p>	<p>2016</p> <p>Il Parlamento Europeo ha messo in vigore il GDPR</p>





Penali

In caso di violazione del GDPR, le multe sono davvero alte. Ci sono due tipi di sanzioni. La prima è una multa di circa 20 milioni di euro o il 4% delle entrate globali, e la seconda è che le persone, i cui dati non sono stati protetti, hanno il diritto di chiedere un risarcimento (Wolford, 2019).



Principi di protezione dei dati (Wolford, 2019).

Il trattamento dei dati personali dovrebbe essere effettuato secondo sette principi fondamentali

- 1 Trasparenza - Legalità - Correttezza.
- 2 Limitazione delle finalità: i dati devono essere utilizzati solo per le finalità di cui l'interessato è stato informato.
- 3 Minimizzazione dei dati: dovresti raccogliere solo i dati assolutamente necessari per il tuo scopo.
- 4 Accuratezza: i dati devono essere mantenuti accurati e aggiornati.
- 5 Accuratezza: i dati devono essere mantenuti accurati e aggiornati.
- 6 Integrità e riservatezza: il trattamento dei dati deve essere condotto in modo da garantire protezione e riservatezza.
- 7 Responsabilità: La persona che elabora i dati è responsabile di dimostrare la conformità al GDPR con tutti i suddetti principi.



Consenso

È obbligatorio che gli interessati diano il loro consenso, al fine di consentire il trattamento dei loro dati. Ma cosa costituisce il consenso?

- Il consenso deve essere liberamente prestato, specifico e inequivocabile.
- Le richieste di consenso devono essere chiare, distinguibili e presentate con parole semplici.
- Gli interessati hanno il diritto di revocare il proprio consenso ogni volta che lo desiderano.
- Quando si tratta di bambini di età inferiore ai 13 anni, il permesso dei genitori è obbligatorio.
- Le prove documentali del consenso devono essere salvate.

Diritto di privacy

L'individuo, che accetta di rivelare i dati personali, ha anche il diritto alla privacy. Sono elencati di seguito (Wolford, 2019):

- Il diritto di essere informati
- Il diritto di accesso
- Il diritto alla correzione
- Il diritto alla cancellazione
- Il diritto di limitare il trattamento
- Diritto alla portabilità dei dati
- Il diritto di esprimere obiezioni
- Diritti in relazione al processo decisionale automatizzato e alla profilazione.

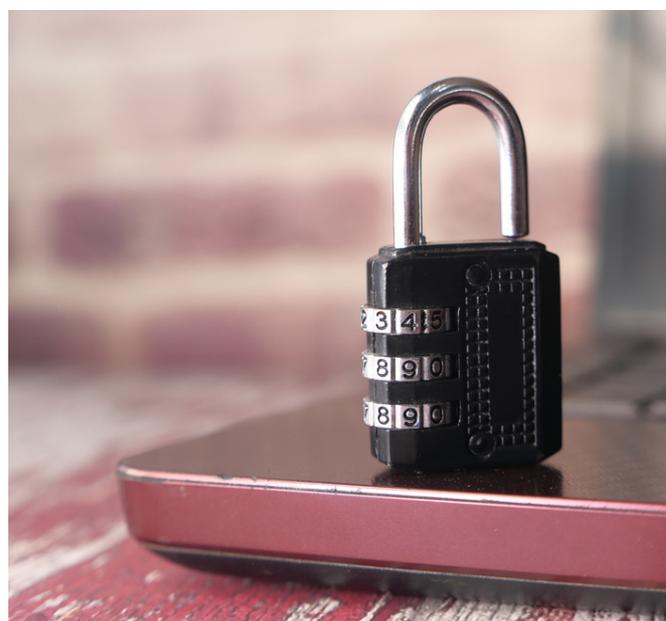
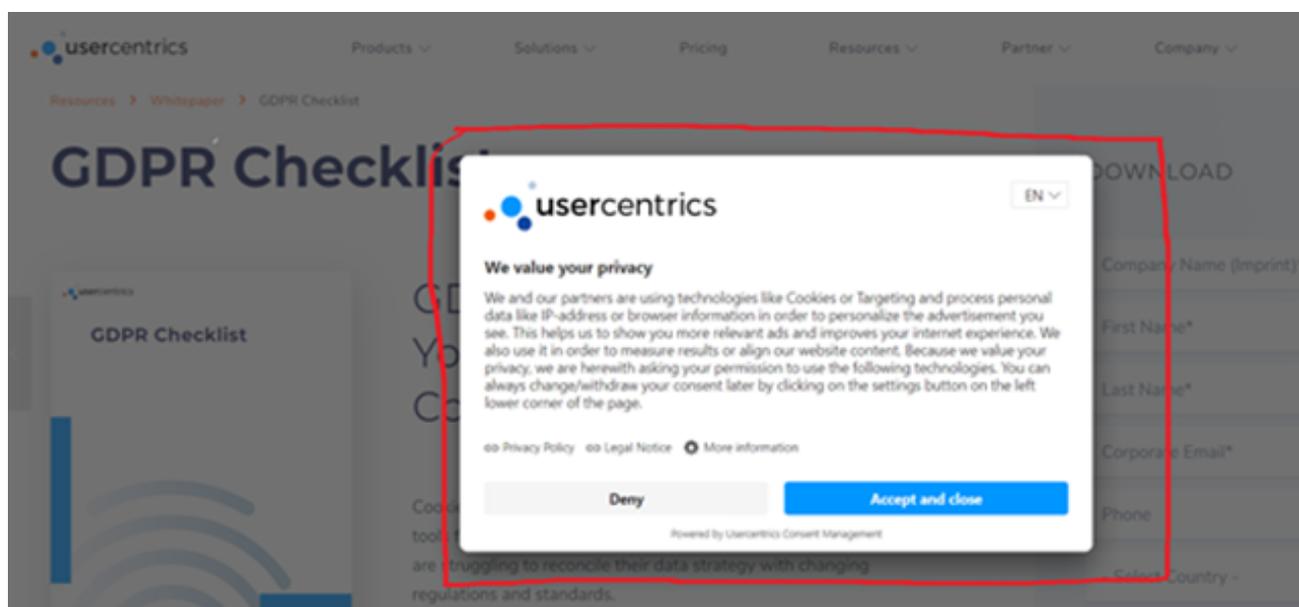


Figura 18. Un esempio di come viene richiesto l'accesso ai dati personali tramite Internet





Il California Consumer Privacy Act (CCPA) rafforza i diritti alla privacy e le tutele dei consumatori per i residenti in California. È una legge statale della California che è stata effettivamente votata nel giugno 2018 ma non è entrata in vigore fino al 1° gennaio 2020 (Cooman, 2020).

Secondo il CCPA i dati personali sono considerati tutte le informazioni che possono portare all'identificazione di un individuo (come nome, indirizzo, e-mail, numero di passaporto, codice fiscale, ecc.), informazioni commerciali (come prodotti acquistati), attività di rete elettronica, audio o dati visivi e conclusioni tratte da una qualsiasi delle suddette informazioni per creare un profilo su un consumatore che rifletta le sue preferenze.



Simile al GDPR, la nuova legge CCPA della California sancisce i diritti delle persone di ottenere informazioni dalle società tecnologiche sui dati che hanno raccolto su un particolare utente e di richiedere alle società di eliminare tutti i dati personali dell'utente.

Uno degli aspetti chiave del CCPA riguarda la vendita dei dati personali dei consumatori: il CCPA prevede che i consumatori non solo abbiano il diritto di chiedere alle aziende di rivelare quali dati su un determinato consumatore vengano raccolti per scopi commerciali, ma anche che i consumatori possano esigere che i loro dati personali non vengano venduti.

Obiettivi CCPA

- Possedere i tuoi dati personali
- Controlla i tuoi dati personali
- Proteggi i tuoi dati personali
- Ritenere responsabili le grandi aziende



Figura 19. elementi base CCPA

CCPA AND THE BOTTOM LINE

Implications for Companies Doing Business in California
Compliance with the CCPA is likely to affect the bottom line of companies who process substantial amounts of data from California consumers.

EFFECTIVE DATE	DAMAGES
<p>2020 January 1st</p> <p>Comes into force on January 1, 2020 START PLANNING NOW</p>	<p>\$100 to \$750 PER INDIVIDUAL or ACTUAL DAMAGES FOR SECURITY INCIDENTS</p>
CONSUMER RIGHTS	WHO NEEDS TO COMPLY
<p>KNOW WHAT personal information is collected about them.</p> <p>KNOW WHETHER their personal information is sold or disclosed and to whom.</p> <p>OPT OUT of the sale of their personal information.</p> <p>MORE DIFFICULT to share data if under 18.</p> <p>EASIER TO sue after breach.</p> <p></p>	<p>ALL COMPANIES THAT COLLECT personal consumer INFORMATION</p> <ul style="list-style-type: none"> • \$25M annual gross revenue • 50K+ consumer personal information • derive 50% of revenue from consumer information <p>(ALL CALIFORNIA RESIDENTS)</p> <p></p>
ATTORNEY GENERAL PENALTIES	SIGNIFICANT CHANGES REQUIRED
<p>More Authority to PURSUE VIOLATOR for damages</p> <p></p>	<p>How consumer DATA is collected, used and stored which will affect</p> <ul style="list-style-type: none"> • personal property records • products or services purchased • biometric information • geolocation data <p></p>

We recommend that companies begin acquiring an in-depth understanding of the new CCPA requirements and keep 12 month look-back of data activities because they will require significant changes in how customer data is collected, used and stored. Taking this precaution will minimize CCPA's affect to the Bottom line.

Principali differenze tra GDPR e CCPA

Sebbene GDPR e CCPA condividano punti comuni, non sono intercambiabili. Le loro differenze chiave riguardano l'ambito territoriale e l'applicazione della legge, le sanzioni - in caso di violazione - la natura e i limiti di raccolta e il fatto che il GDPR richiede una base legale per tutti i trattamenti di dati personali (A., 2021). I suddetti sono indicati nella figura seguente (A., 2021).





5.3. AUTORITÀ STATALI PER LA PROTEZIONE DEI DATI

Le autorità statali per la protezione dei dati (DPA) sono autorità pubbliche indipendenti incaricate di sovrintendere all'attuazione delle leggi sulla protezione dei dati, attraverso poteri investigativi e correttivi (Cosa sono le autorità per la protezione dei dati (DPA)? 2018).

Le DPA offrono consulenza esperta in materia di protezione dei dati e sono responsabili della gestione delle denunce presentate a causa di violazioni del Regolamento generale sulla protezione dei dati (GDPR) e delle rispettive leggi nazionali. Nel contesto del GDPR, tutti gli Stati membri dell'UE dovrebbero avere un'autorità per la protezione dei dati, che funge da mediatore tra le parti interessate all'interno di quello Stato membro (Clerck, 2019).



Autorità statali per la protezione dei dati nei paesi partner del progetto:

- Lituania: Ispettorato statale per la protezione dei dati (<https://vdai.lrv.lt/lt/>)
- Austria: Autorità austriaca per la protezione dei dati (<https://www.dsb.gv.at/>)
- Spagna: Agenzia spagnola per la protezione dei dati (<https://www.aepd.es/es>)
- Grecia: Autorità ellenica per la protezione dei dati (<https://www.dpa.gr/en>)
- Cipro: Ufficio del Commissario per la protezione dei dati personali
http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/home_en/home_en?opendocument
- Italia: Garante per la protezione dei dati personali italiano (<https://www.garanteprivacy.it>)

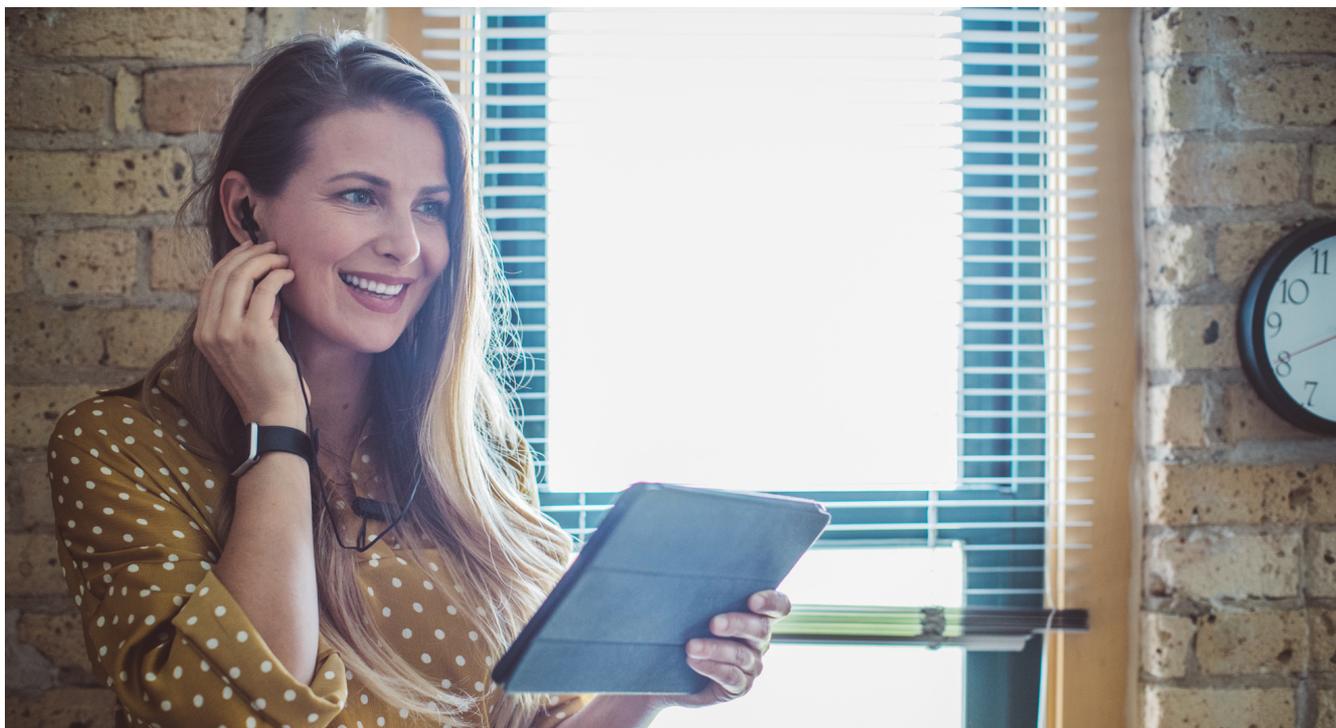


6 MODULO



FINAL WORD

6.1. EVITA LA "CRISI" DI METÀ CARRIERA - RIMANI AGGIORNATO SULLA TECNOLOGIA



La tecnologia sta diventando sempre più integrata con ogni aspetto della nostra vita ogni giorno. Molte persone condividono le loro preoccupazioni riguardo al fatto che il mondo sta cambiando così rapidamente e che potrebbero trovarsi fuori dal giro. Questo è un pensiero molto legittimo attualmente, più comune di quanto si possa supporre.

Indipendentemente dal campo in cui ti trovi, è particolarmente importante rimanere al passo con la tecnologia per influenzare la tua vita personale e professionale. La tecnologia è aumentata rapidamente negli ultimi decenni e cose che in precedenza si pensava fossero impossibili vengono rese possibili a un ritmo molto veloce.

Conoscere i progressi della tecnologia è di per sé un affascinante piacere per la mente. È anche importante familiarizzare con la nuova tecnologia, perché la vecchia tecnologia con cui sei abituato a lavorare diventerà rapidamente obsoleta. Otterrai il vantaggio in ogni campo se la tua conoscenza della tecnologia è aggiornata. Nella sezione seguente verrà presentata l'importanza di stare al passo con le nuove tendenze nello sviluppo tecnologico, necessarie per la vita di tutti i giorni.





La tecnologia ci tiene in contatto (soprattutto con la nostra famiglia e i nostri amici)

Man mano che le famiglie continuano a crescere, i membri spesso si allontanano da casa per andare a scuola, al lavoro o per perseguire le proprie famiglie. Fortunatamente, con l'aiuto della tecnologia, la comunicazione non è mai stata così facile. Che si tratti di messaggi di testo, FaceTime o Skype o uno qualsiasi dei vari siti di social media, è facile rimanere in contatto con familiari e amici da lontano. I moderni tablet, computer e telefoni cellulari hanno quasi tutti la capacità di utilizzare una qualsiasi delle suddette forme di comunicazione per mantenere la famiglia e gli amici connessi, indipendentemente da dove si trovino nel mondo.

La tecnologia ti aiuta a rimanere informato

Il modo più rapido e conveniente per conoscere ciò che sta accadendo in tutto il paese o in tutto il mondo è "fare clic" e "scorrere" sui portali di notizie su Internet. Puoi anche abbonarti al fornitore di notizie di tua scelta o scaricare l'applicazione per telefoni cellulari (nella maggior parte dei casi gratuitamente) e consentirà la notifica sugli eventi in corso che ti terranno informato.



La tecnologia migliora la tua produttività

Esistono molte app di produttività che possono aiutare a rimanere produttivi e organizzati. Ad esempio, "Evernote" è un'app di produttività che funziona come un fantastico archivio. Aiuta a tenere a bada il disordine mentale poiché organizza tutto per te.

Utilizzo dei portali del lavoro come tecnica più efficiente per la ricerca di lavoro

Abbiamo fatto molta strada dal cercare la prossima opzione di carriera negli editoriali di carriera di ogni giornale e spargere la voce sulla nostra disoccupazione in circuiti chiusi di familiari e amici sperando solo di ottenere un riferimento prima. Tuttavia, l'ultima sensazione digitale è la nostra grazia e tempo salvifico, qui le carriere sono fatte di clic. I portali di lavoro sono l'ultimo punto di riferimento per tutti coloro che cercano lavoro che stanno cercando di iniziare, interessati a un cambiamento nei percorsi di carriera o semplicemente vogliono lavorare fuori dalle loro vecchie mura o trovare un lavoro in generale.

Servizi elettronici che ti semplificano la vita (ad esempio l'online banking)

Non c'è dubbio che la digitalizzazione ha portato a una rivoluzione in materia finanziaria. L'attività bancaria online viene eseguita tramite un laptop, un tablet o un'app per telefono ora è la norma. Gli utenti della banca possono ora controllare i pagamenti in entrata e in uscita da remoto, nonché organizzare trasferimenti di denaro e pagamenti delle bollette. Al di fuori del settore bancario, altre questioni finanziarie, come l'acquisto e la vendita di valuta e azioni, possono essere trattate online. Anche il trasferimento di denaro tra conti nazionali e internazionali ha visto una grande innovazione negli ultimi anni.





6.2. GIOCHI E APP INTERATTIVI



DUOLINGO

(<https://www.duolingo.com/>) ti aiuta ad imparare una lingua straniera.

STUDYBLUE

(<https://www.studyblue.com/>) è un compagno di studio mobile progettato per aiutarti a "conquistare il tuo corso" utilizzando flashcard, note, guide allo studio e altro ancora.

TYPINGCLUB

(<https://www.typingclub.com/>) Le attività ludiche e guidate dai dati aiutano a padroneggiare le abilità di tastiera.

TED

(<https://www.ted.com/>) diffusione di pensieri intriganti o stimolanti, di solito in video di 18 minuti o meno.

YOUTUBE

(<https://www.youtube.com/>) Digita le parole "come fare" nella barra di ricerca dell'app e troverai tutto.





QUIZLET

(<https://quizlet.com/>) Il supporto flessibile allo studio supporta l'apprendimento a casa, a scuola e in viaggio.

LEARN CRYPTIC CROSSWORDS

(<https://www.learncrypticcrosswords.com/>) Impara i cruciverba criptici I cruciverba criptici non sono così criptici una volta che inizi a imparare alcuni dei metodi per risolverli. Questa app fa davvero un ottimo lavoro nello spiegare come affrontare i puzzle, mettendoti alla prova con esercizi.

ELEVATE: BRAIN TRAINING

(<https://elevateapp.com/>) Impara i cruciverba criptici I cruciverba criptici non sono così criptici una volta che inizi a imparare alcuni dei metodi per risolverli. Questa app fa davvero un ottimo lavoro nello spiegare come affrontare i puzzle, mettendoti alla prova con esercizi.

SKILLSHARE

(<https://www.skillshare.com/>) disegno, fotografia, grafica e altre discipline creative.

COURSERA

(<https://www.coursera.org/>) offre programmazione, arte e design, scienze e affari e altre materie attraverso 3.500 corsi di apprendimento online, completi di lezioni video e istruttori, con colleghi con cui chattare.

GOOGLE ARTS AND CULTURE

(<https://artsandculture.google.com/>) tour virtuali di oltre 2.000 "istituzioni culturali" in tutto il mondo, utilizzando foto, video e realtà virtuale.

Scopri di più su app e giochi interattivi:

<https://bit.ly/2KOFFiK>

<https://bit.ly/2NA3Br9>

<https://bit.ly/39b33>



Bibliografija

1. Wheeler, S. (2009, Ed) *Connected Minds, Emerging Cultures: Cybercultures in Online Learning*. Charlotte, NC: Information Age.
2. Anderson, J. (2010) *ICT Transforming Education: A Regional Guide*. Bangkok: UNESCO Publication
3. Kress, G. (2009) *Literacy in the New Media Age*. Abingdon: Routledge.
4. Van Dijk, J. (2005). *The Deepening Divide. Inequality in the Information Society*. London: Sage Publications
5. Carr, N. (2008) *Is Google Making us Stupid?* *The Atlantic*, July/August Issue Retrieved May 21, 2012, from
6. <http://www.theatlantic.com/magazine/archive/2008/07/is-google-making-us-stupid/6868/#>
7. Keen, A. (2007) *The Cult of the Amateur: How Today's Internet is Killing our Culture and Assaulting our Economy*. London: Nicholas Brealey.
8. International Society for Technology in Education (2007). *iste.nets.s: Advancing Digital Age Learning*. Iste.org/nets.
9. <http://www.newmedialiteracies.org/files/working/NMLWhitePaper.pdf>
10. Qiu, Jack Linchuan. 2018. "China's Digital Working Class and Circuits of Labor." *Communication and the Public* 3 (1): 5–18. <https://doi.org/10.1177/2057047318755529>.
11. Refine web searches: <https://support.google.com/websearch/answer/2466433?hl=en>
12. <https://ec.europa.eu/digital-single-market/en/trust-services>
13. Nika, D., Gioldasi, P., & Vitta, F. (2017). *Cyber bullying) vs cyber stalking*.
14. Olweus, D. (2012). *Cyberbullying: An overrated phenomenon?*. *European journal of developmental psychology*, 9(5), 520-538.
15. Šléglová, V., & Cerna, A. (2011). *Cyberbullying in adolescent victims: Perception and coping*.
16. *Cyberpsychology: journal of psychosocial research on cyberspace*, 5(2).
17. Slonje, R., Smith, P. K., & Frisé, A. (2013). *The nature of cyberbullying, and strategies for*
18. *prevention. Computers in human behavior*, 29(1), 26-32.
19. *Savižudybių, priskirtų patyčioms, sąrašas*. Vikipedija.
20. https://en.wikipedia.org/wiki/List_of_suicides_that_have_been_attributed_to_bullying
21. Allcott, H., & Gentzkow, M. (2017). *Social Media and Fake News in the 2016 Election*.
22. *Journal of Economic Perspectives*, 31(2), 211–236. <https://doi.org/10.1257/jep.31.2.211>
23. Bjola, C. (2018). *The Ethics of Countering Digital Propaganda*. *Ethics & International Affairs*,
24. 32(3), 305–315. <https://doi.org/10.1017/s0892679418000436>
25. *CyberWise*. (2019, August 10). *What Is Fake News?* YouTube.
26. <https://www.youtube.com/080/21670811.2017.1360143>

Bibliografia

27. How to spot fake news. n.d. [Illustration].
28. <https://www.lib.sfu.ca/help/research-assistance/fake-news#how-to-spot-fake-news-in-eight-simple-steps>
29. Spencer, S. H. (2020, February 11). Fake Coronavirus Cures, Part 2: Garlic Isn't a "Cure." FactCheck.Org.
30. <https://www.factcheck.org/2020/02/fake-coronavirus-cures-part-2-garlic-isnt-a-cure/>
31. Tandoc, E. C., Lim, Z. W., & Ling, R. (2017). Defining "Fake News." *Digital Journalism*, 6(2), 137–153. <https://doi.org/10.1080/21670811.2017.1360143>
32. Tsompanidis, G. (2018) "Translated bibliography". Propaganda from the point of view of modern international law.
33. Gainsbury, S. M. (2015). Online Gambling Addiction: The Relationship Between Internet Gambling and Disordered Gambling. *Current Addiction Reports*, 2(2), 185–193.
34. <https://doi.org/10.1007/s40429-015-0057-8>
35. Griffiths, M. (2005). A 'components' model of addiction within a biopsychosocial framework.
36. *Journal of Substance Use*, 10(4), 191–197.
37. Kuss, D. J. (2013). Internet gaming addiction: current perspectives. *Psychology research and behavior management*, 6, 125.
38. Kuss, D. J., & Griffiths, M. D. (2012). Online gaming addiction in children and adolescents: A review of empirical research. *Journal of behavioral addictions*, 1(1), 3-22.
41. 2019 is the Year of . . . CCPA? [Infographic]. (2019). *The National Law Review*. <https://www.natlawreview.com/article/2019-year-ccpa-infographic>
42. A. (2021, January 7). CCPA vs. GDPR – differences and similarities. *Data Privacy Manager*.
43. <https://dataprivacymanager.net/ccpa-vs-gdpr/>
44. Cooman, G. (2020, January 28). What is CCPA and why should it matter to you? Proxyclick.
45. <https://www.proxyclick.com/blog/what-is-ccpa-and-why-does-it-matter-to-you#DDP>
46. Goddard, M. (2017). The EU General Data Protection Regulation (GDPR): European Regulation that has a Global Impact. *International Journal of Market Research*, 59(6), 703–705. <https://doi.org/10.2501/ijmr-2017-050>
47. Wolford, B. (2019, February 13). What is GDPR, the EU's new data protection law? GDPR.Eu.
48. <https://gdpr.eu/what-is-gdpr/>
49. What are Data Protection Authorities (DPAs)? (2018, August 1). European Commission - European Commission.
50. https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-are-data-protection-authorities-dpas_en

51. Clerck, J. (2019, November 25). Supervisory authorities: consistency and Data Protection Authorities (DPAs) under GDPR. I-SCOOP.
52. <https://www.i-scoop.eu/supervisory-authorities-consistency-and-data-protection-authorities-dpas/>
53. Allcott, H., & Gentzkow, M. (2017). Socialinė žiniasklaida ir netikros naujienos 2016 m. rinkimuose. Journal of Economic Perspectives, 31 (2), 211–236.
54. <https://doi.org/10.1257/jep.31.2.211>
55. Bjola, C. (2018).
56. Kovos su skaitmenine propaganda etika. Etika ir tarptautiniai reikalai, 32 (3), 305–315. <https://doi.org/10.1017/s0892679418000436>
57. „CyberWise“. (2019 m., rugpjūčio 10 d.). Kas yra netikros naujienos? „YouTube“. https://www.youtube.com/watch?v=V4o0B6IDo50&ab_channel=CyberWise
58. Kaip aptikti netikras naujienas.
59. <https://www.lib.sfu.ca/help/research-assistance/fake-news#how-to-spot-fake-news-in-eight-simple-steps>
60. Spenceris, S. H. (2020 m., Vasario 11 d.). Netikri koronaviruso vaistai, 2 dalis: česnakai nėra „gydymas“. „FactCheck.Org“.
61. <https://www.factcheck.org/2020/02/fake-coronavirus-cures-part-2-garlic-isnt-a-cure/>
62. Tandoc, E. C., Lim, Z. W., & Ling, R. (2017). „Netikrų naujienų“ apibrėžimas. Skaitmeninė žurnalistika, 6 (2), 137–153. <https://doi.org/10.1080/21670811.2017.1360143>
63. <http://esaugumas.lt/lt/duomenu-vagystes.html>
64. Gintautas Mažeikis. Metodinis leidinys „Propaganda“. Šiauliai, 2006.
65. <https://atviri.emokymai.vu.lt/mod/book/tool/print/index.php?id=12>
66. <https://www.stuff.co.nz/technology/digital-living/68293880/japans-first-internet-fasting-camp-for-teens-a-success>
67. Julius Zaleskis. Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė (GDPR). Registrų centras, 2019.
68. https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-are-data-protection-authorities-dpas_en
69. <https://www.europarl.europa.eu/factsheets/en/home>
70. <https://researchguides.ben.edu/source-evaluation>