Together for Tomorrow!
Enabling People

CRESCERE CITTADINI DIGITALI

Guida all'insegnamento dell'Educazione Civica Digitale

SAMSUNG

Cari insegnanti, cari genitori...

Samsung è da sempre attenta al tema dell'educazione, e si pone l'obiettivo di guidare la comunità a un corretto utilizzo delle tecnologie che ogni giorno porta nelle case degli italiani.

Questi mesi hanno portato anche le generazioni più giovani ad utilizzare strumenti come smartphone e tablet e a vivere una dimensione sociale e relazionale sempre più digitale. Per alcuni di loro si è trattato della "prima volta", altri utilizzano la tecnologia quotidianamente, alcuni di loro anche eccessivamente e spesso in modo poco consapevole. Per tutti loro, ma anche per noi adulti, risulta fondamentale imparare ad utilizzare la tecnologia in maniera responsabile, sicura, sostenibile e rispettosa dell'altro.

È da questa premessa che nasce il progetto "Crescere cittadini digitali", un vero e proprio libro didattico rivolto agli insegnanti e agli studenti, ma anche ai genitori e alla cittadinanza intera.

Riteniamo che anche aziende come Samsung debbano fare la loro parte in questo processo di evangelizzazione e di conoscenza. Non a caso, Samsung Italia, agendo da cittadino italiano, non misura i suoi successi solo in base ai risultati di business, ma anche rispetto al proprio contributo verso la comunità e alla capacità di facilitare e arricchire la vita delle persone.

Attraverso "Crescere cittadini digitali" auspichiamo di poter offrire un ulteriore momento di formazione e arricchimento alle generazioni future, perché sappiamo che i giovani di oggi saranno gli innovatori di domani, e cerchiamo di fornire loro tutti gli strumenti, le conoscenze, la creatività e l'empatia necessarie per prosperare in un futuro guidato dalla tecnologia.

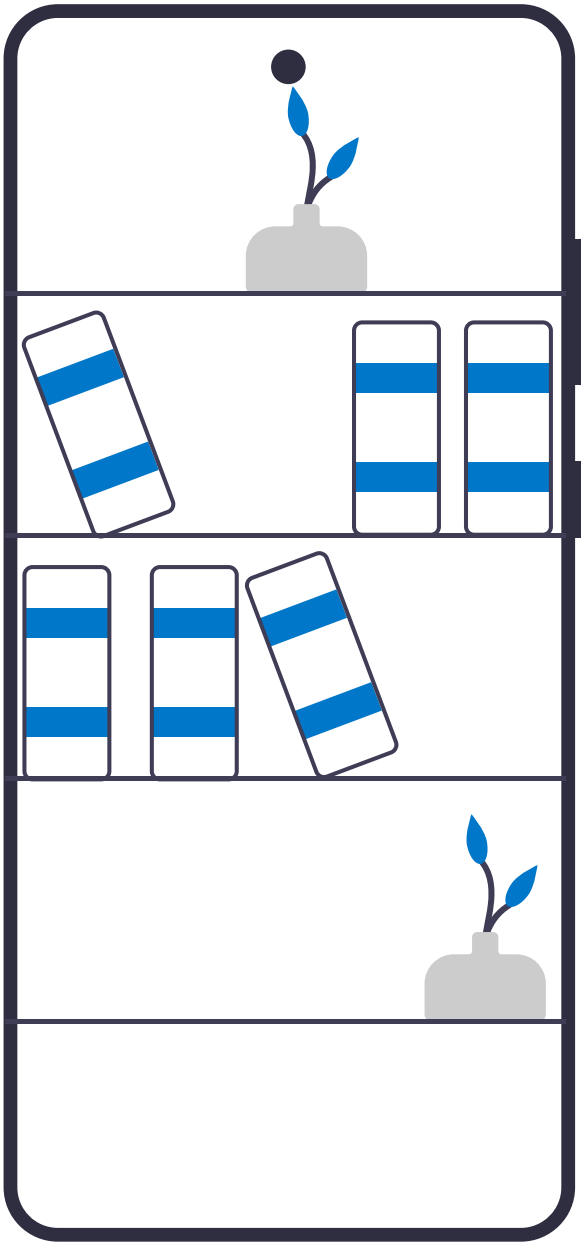
Anastasia Buda,
Corporate Citizenship Manager,
Samsung Electronics Italia SpA

Si ringraziano:
Giovanni Barina, Davide Bigoni, Paola Brovelli, Laura Castelnuovo, Vito Fortunato, Cristina Guatteri, Anna Rosetti, Ji Sun Yu, Carolina Borella, Claudia Cottica, Chiara Luchini, Marco Peluso, Angela Francolino, Producer Support Team Marketing Specialist, Erion Compliance Organization S.c.a.r.l. Fabrizia Gasperini Producer Support Team Manager, Erion Compliance Organization S.c.a.r.l.

Together for Tomorrow!
Enabling People

CRESCERE CITTADINI DIGITALI

Guida all'insegnamento dell'Educazione Civica Digitale



Lezione 0
Introduzione

SAMSUNG

Parola all'On. Massimiliano Capitanio

Massimiliano Capitanio è un giornalista e politico italiano. Nato il 12 giugno 1974 a Vimercate e cresciuto a Concorezzo (MB), si è laureato in Lettere e filosofia, con indirizzo in Comunicazione sociale alla Cattolica di Milano con 110 e lode. Dopo la laurea ha frequentato e concluso un corso di perfezionamento in Management delle pubbliche amministrazioni (MAP) presso la SDA Bocconi. Iscritto alla Lega Nord Lega Lombarda a metà degli anni Novanta, ha partecipato alla fondazione del Movimento giovani padani, divenendo responsabile federale di quello studentesco. È autore di libri e giornalista professionista, con una lunga carriera nelle redazioni di diversi giornali. Nel 2009 viene scelto come responsabile stampa e poi capo segreteria dell'assessorato alle Politiche sociali della Provincia di Milano. Dal 2013 al 2018 è stato vicedirettore dell'ufficio stampa del Consiglio regionale della Lombardia. Eletto deputato con la Lega nel 2018, è membro della IX Commissione parlamentare trasporti, poste e telecomunicazioni della Camera dei deputati e Segretario della Commissione parlamentare per l'indirizzo generale e la vigilanza dei servizi radiotelevisivi. Sempre dal 2018 è tesoriere del gruppo parlamentare della Lega alla Camera dei deputati.

Nella sua attività parlamentare è molto attento alle tematiche legate al mondo digitale e dell'innovazione ed anche all'ambito educativo/scolastico. **È stato il promotore e primo firmatario della legge 92 del 2019 che ha reintrodotto l'educazione civica obbligatoria e curricolare nelle scuole italiane.**

Crescere Cittadini Digitali

Era il 1958 quando Aldo Moro, allora ministro dell'Istruzione, introdusse a scuola l'ora di educazione civica. Lo statista, poi assassinato dalle Brigate Rosse, aveva un sogno: "pulire il futuro" ai giovani. La nuova materia doveva servire proprio a quello: aiutare bambini e ragazzi a crescere nella conoscenza delle regole e nel rispetto delle leggi, coltivando insieme a insegnanti e genitori i valori della responsabilità, della partecipazione, del volontariato. La base di partenza non può che essere la nostra Costituzione, che riassume nei suoi articoli tutte le "educazioni" irrinunciabili: alla legalità, all'ambiente, alla salute, alla bellezza, nel senso più ampio del termine. Oggi, però, c'è un'altra educazione che non è più rimanda-

bile: quella alla cittadinanza digitale. Essere "nativi digitali" non sempre equivale a conoscere regole, pericoli o anche opportunità di quell'universo racchiuso nei nostri smartphone e fatto di applicazioni, giochi, comunicazioni, immagini.

Quando il Parlamento italiano, praticamente all'unanimità, ha approvato la legge 92 del 2019, lo ha fatto nella convinzione che questi temi debbano essere al centro del nostro cammino di formazione.

"Crescere cittadini digitali", come suggerisce questo interessante ciclo di lezioni, vuol dire imparare a maneggiare con responsabilità il cellulare e tutti i nostri device. Secondo l'Osservatorio nazionale sull'adolescenza il 46% degli 11-13enni resta attaccato allo smartphone al massimo due ore mentre il 44% dei giovani tra 14 e 18 anni arriva a stare al telefono anche sei ore al giorno. Un arco di tempo, a volte infinito, dove è in gioco la nostra privacy, la nostra identità, la nostra sicurezza, la nostra salute. Non solo la nostra, ma anche quella dei nostri compagni di classe e dell'ambiente che ci circonda. Esserne più consapevoli ci aiuterà a crescere cittadini più consapevoli. E forse migliori.

On. Massimiliano Capitanio

Obiettivi formativi

- Introdurre il concetto di Educazione Civica Digitale, spiegare come mai è un tema rilevante non solo per i ragazzi (nativi digitali), ma anche per docenti e genitori (immigrati digitali).

- Spiegare gli obiettivi del percorso formativo proposto in questa serie di lezioni.

Indice lezione

Capitolo 1: Cittadini digitali

Questa serie di lezioni affronta i temi propri dell'Educazione Civica Digitale, approfondendo il concetto di cittadinanza digitale attraverso cinque aree tematiche che contraddistinguono il nostro ruolo di cittadini consapevoli e responsabili del web.

Perché si parla di cittadinanza digitale?

Si parla di cittadinanza digitale perché l'ecosistema digitale si è evoluto a tal punto da essere diventato uno dei luoghi, e per tante persone, uno dei principali, che abitiamo nella nostra quotidianità.

E non solo è un posto a cui accediamo per svolgere delle attività individuali, come effettuare delle ricerche, lavorare o guardare un film in streaming, ma sempre più è anche un luogo dove svolgiamo attività di relazione con altri individui e attraverso il quale comunichiamo con loro.

Infine, è anche uno dei modi che abbiamo per relazionarci con lo Stato, attraverso l'identità digitale e tutti i servizi a cui questa ci permette di accedere.
Il concetto fondamentale da cui partire per intraprendere questo percorso è che Internet è ormai molto più che un mezzo: è uno spazio che abitiamo, e che utilizziamo quotidianamente per esercitare la nostra libertà di espressione e di pensiero.
In quest'ottica, come la cittadinanza definisce la nostra appartenenza a uno Stato per permetterci di godere dei diritti e per ricordarci che siamo soggetti a dei doveri, allo stesso modo dobbiamo "navigare" nell'ecosistema digitale consapevoli che si tratta di un ambiente dove noi siamo presenti in quanto cittadini che si mettono in relazione con gli altri e con lo Stato secondo un sistema "normato", e che questo stesso sistema ci tutela e ci fornisce delle garanzie.

In quanto cittadini digitali infatti abbiamo dei diritti come la privacy, la libertà di espressione e la tutela della persona, e siamo tenuti a rispettare delle buone norme comportamentali e ad osservare delle regole.

Sembra tutto piuttosto lineare, ma il mondo del digitale è diverso dal mondo reale, si basa su meccanismi differenti, che spesso disorientano, ed evolve molto in fretta. È difficile comportarsi da cittadini consapevoli e responsabili se non si conosce a fondo l'ecosistema in cui si agisce, se non ne si conoscono i limiti e le potenzialità.

Per poter vivere da cittadini digitali, dobbiamo conoscere innanzitutto il sistema di cui siamo parte, con le sue implicazioni in termini di diritti e doveri e intendendo il nostro ruolo di cittadini digitali sia come individui che si mettono in relazione con gli altri in uno spazio "normato", sia come individui che hanno la possibilità di esprimere legalmente la propria individualità attraverso i mezzi digitali.

Tutti, giovani e adulti, nativi e immigrati digitali, dobbiamo acquisire piena consapevolezza di come funziona l'ecosistema digitale in tutte le sue sfumature. E i giovani, che più facilmente entrano in contatto con il mondo al di là dello schermo, hanno bisogno di una guida per poterlo navigare in sicurezza e per poterlo sfruttare al meglio.

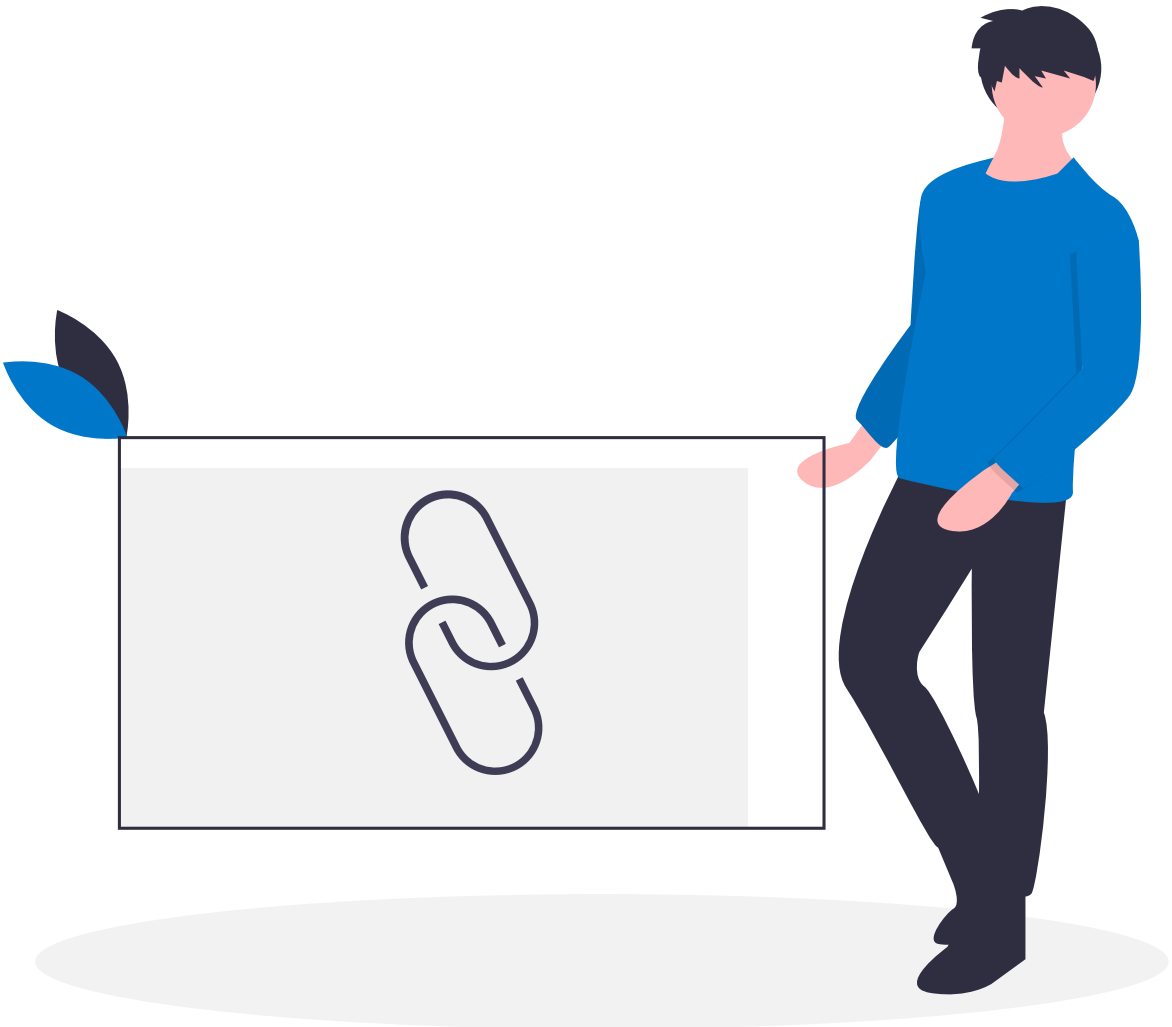
Con questa serie di lezioni si vuole supportare i docenti affinché possano guidare gli studenti in un percorso formativo che li porti ad acquisire consapevolezza del funzionamento del web e delle implicazioni della presenza degli individui online e che li aiuti ad appropriarsi dei mezzi digitali e diventare fruitori di Internet critici e responsabili, allontanandosi dal ruolo di consumatori passivi che ne subiscono inconsapevolmente gli effetti.

Link e informazioni utili

- Agenzia per l'Italia Digitale
  https://www.agid.gov.it/it

- DigComp 2.1 - Il quadro di riferimento per le competenze digitali dei cittadini
  https://www.agid.gov.it/sites/default/files/repository_files/digcomp2-1_ita.pdf

- Linee guida del Ministero dell'Istruzione per l'insegnamento dell'Educazione Civica
  https://www.miur.gov.it/web/guest/-/inviate-alle-scuole-le-linee-guida-per-l-insegnamento-dell-educazione-civica-azzolina-studio-della-costituzione-sviluppo-sostenibile-cittadinanza-digi



Capitolo 2: Lezioni e obiettivi formativi

Educazione Civica Digitale è un percorso che si compone delle seguenti lezioni:

- Lezione 1: **Identità digitale**
- Lezione 2: **Galateo del digitale**
- Lezione 3: **Sicurezza digitale**
- Lezione 4: **Contenuti digitali**
- Lezione 5: **Sostenibilità digitale**

Le lezioni sono state pensate come supporto al docente, perché possa approfondire i temi legati all'Educazione Civica Digitale, possa avere un supporto didattico e una guida a come trattare i temi in classe con i propri alunni.
Ogni lezione si compone di un'introduzione redatta da un esperto del tema specifico, di una prima parte teorica suddivisa in capitoli e di una seconda parte pratica, con proposte di esercizi e attività da svolgere in classe inerenti al tema trattato in ciascuna lezione.

Vediamo di seguito gli obiettivi formativi di ciascuna lezione.

1. Lezione 1: Identità digitale

- Definire le "norme" comportamentali del cittadino digitale.
- Approfondire temi legati al comportamento del cittadino digitale con particolare attenzione al tema dei dati personali e della privacy.
- Approfondire il tema del cyberbullismo fornendo indicazioni sia sull'entità che sulla portata del fenomeno.
- Sensibilizzare alla prospettiva legale dei reati online.

2. Lezione 2: Galateo del digitale

- Approfondire temi legati al comportamento del cittadino digitale con particolare attenzione a spazi virtuali come i social media.
- Introdurre il tema della netiquette

3. Lezione 3: Sicurezza digitale

- Sensibilizzare sulla quantità di dati che creiamo e sul valore che questi hanno.
- Approfondire il tema della sicurezza online, sia dal punto di vista della prevenzione (impostazioni smartphone, geolocalizzazione) che dei pericoli in cui si può incorrere (frode informatica, phishing, cyber-criminalità, ransomware, ecc.).
- Introdurre il tema dei pagamenti digitali (modalità di pagamento, come avvengono, ecc.).

4. Lezione 4: Contenuti digitali

- Apprendere come riconoscere fonti e contenuti attendibili da quelli non, sensibilizzare sull'importanza di sviluppare senso critico verso quello che si trova online.
- Ragionare sul tema dell'Information Disorder e delle Fake News.
- Definire cos'è il copyright e come utilizzare i testi che si trovano online per lavori personali (ricerche, tesi, ecc.) e suggerire strumenti utili.

5. Lezione 5: Sostenibilità digitale

- Fornire una panoramica su dispositivi e connessioni in Italia e nel mondo.
- Introdurre il tema dello smaltimento della tecnologia (dove finiscono i device).
- Introdurre il tema dell'impatto della trasformazione digitale sull'ambiente.

ATTIVITÀ CON LA CLASSE

Attività 1 - Quiz!

- Materiale necessario: possibilità di proiettare
- Obiettivo: sviluppare senso di responsabilità e spirito critico nell'utilizzo degli strumenti del web

Nel mare digitale non ci siamo solo noi. Non nuotiamo mai da soli, neanche quando leggiamo un contenuto (c'è sempre qualcuno che l'ha scritto e pubblicato). Qualunque sia il nostro livello di conoscenza del web e degli strumenti, quindi, ci sono regole da rispettare per poter godere di tutti i benefici. Esattamente come accade offline. Due parole: **spirito critico** e **responsabilità**. Scopriamo quanto ne sapete con un quiz!

◊ *Viene proiettato/condiviso un quiz, a cui gli studenti rispondono per alzata di mano con la massima sincerità. I ragazzi hanno un massimo di 5 secondi per rispondere. L'insegnante aiuta a tirare le somme per dare una risposta condivisa dalla classe.*

Esempi di domanda a risposta multipla:

IDENTITÀ DIGITALE
"Cosa significa la parola SPID?"
A – Sistema Pubblico di Identità Digitale
B – Sistema Privato di Identità Digitale
C – Scuola di Preparazione all'Istruzione Digitale

Risposta corretta: A. È un sistema pubblico e gratuito che permette ai cittadini di accedere ai servizi online delle Pubbliche Amministrazioni e dei soggetti privati con un'unica Identità Digitale.

In alternativa:
"L'altro giorno ho fatto una gita in montagna con la mia famiglia. È stato divertente, ho voglia di raccontarlo ai miei amici sui social!"
A – Descrivo tutti i luoghi che abbiamo visto, magari qualcuno vuole visitarli
B – Pubblico la foto della vetta taggando i miei fratelli: è stato un bel traguardo e va premiato
C – Descrivo tutto il percorso che abbiamo fatto, da casa al rifugio. È stato lungo e va documentato!

Risposta corretta: A. Per descrivere un'esperienza che abbiamo fatto e che racconta qualcosa di noi, non è necessario entrare nel dettaglio della nostra vita privata indicando per esempio dove abitiamo e chi sono i nostri famigliari.

GALATEO DIGITALE
"Ogni volta che scrivo qualcosa sui social, un mio contatto interviene pubblicando messaggi provocatori, irritanti e senza senso. Questo tipo di azione ha un nome, quale?"
A – Flaming
B – Trolling
C – Harassment

Risposta corretta: B. Sono tutte forme di cyberbullismo con sfumature diverse: l'"harassment" (in italiano "molestia") porta a causare paure e disagio in una persona con azioni, parole e comportamenti ripetuti; il "Flaming" invece è l'offesa, pura e gratuita, fatta sui social e spesso volgare.

ATTIVITÀ CON LA CLASSE

SICUREZZA DIGITALE

"Ricevo dalla mia banca un messaggio con una richiesta di inviare i miei dati sensibili via posta elettronica. Cosa significa?"

A – È una normale procedura delle banche, che mensilmente contattano i clienti per controllare che i dati siano corretti

B – Accade di solito quando c'è un grave problema con un account da risolvere al più presto

C – Qualcuno sta cercando di rubare i miei dati per accedere al mio conto bancario e carta di credito

Risposta corretta: C. È un tipico messaggio di "phishing", dall'inglese «to fish», «pescare», perché la vittima viene «presa all'amo» dal truffatore che cerca di spacciarsi per qualcun altro

CONTENUTI DIGITALI

"Su Internet vedo girare una foto che fa molto discutere. Qual è la mia prima reazione?"

A – Se sono in tanti a pubblicarla, sarà vera

B – Mi fido delle riviste online che l'hanno pubblicata

C – Preferisco scoprire da dove viene

Risposta corretta: C. Non basta fidarsi, occorre risalire sempre alle fonti facendo qualche ricerca in più.

SOSTENIBILITÀ DIGITALE

"Quando il mio telefonino non funziona più, dove lo butto?"

A – Nel bidone dell'indifferenziata

B – Nell'isola ecologica

C – Lo smonto cercando di differenziare le diverse parti

Risposta corretta: B. Trattandosi di rifiuti elettronici, i cellulari vanno smaltiti nelle **isole ecologiche** e negli appositi centri RAEE presenti nei vari comuni italiani. In un certo senso anche la risposta C è corretta perché è esattamente quello che succede nelle fabbriche di riciclaggio, ma è un lavoro che può fare solo il personale specializzato.

Il quiz è un'occasione per portare gli studenti a riflettere sulle azioni che compiono quotidianamente e spontaneamente quando navigano. Vengono affrontati 5 argomenti - **identità, galateo, sicurezza, contenuti e sostenibilità** - per arrivare al concetto di Educazione Civica Digitale. Segue un brainstorming per provare a rispondere ad alcune domande: cosa significa per voi Educazione Civica Digitale? Perché è importante oggi? È importante solo per noi o anche per i nostri familiari?

ATTIVITÀ CON LA CLASSE

Attività 2 - Gioco ATTIVO/PASSIVO

- Materiale necessario: due fogli e due penne per ogni studente
- Obiettivo: rendere gli studenti consapevoli della quantità di azioni, attive e passive, che compiamo ogni giorno navigando online

Dividiamo la classe in due squadre. A una squadra viene dato il compito di scrivere sul foglio un elenco di azioni attive che possiamo compiere sul web (es. scrivere un messaggio, pubblicare un video o una foto, fare una ricerca, ecc.) e all'altra un elenco di azioni passive (es. leggere le notizie, ricevere un messaggio o una foto, ecc.). Le due squadre hanno pochi minuti di tempo, l'obiettivo è scrivere quante più azioni possibili. A tempo scaduto, i due elenchi vengono consegnati all'insegnante che legge tutte le azioni e decreta la squadra "vincitrice".

Con questo esercizio abbiamo visto che navigando online ci sono cose che decidiamo di fare, e cose che non possiamo controllare. Per questo è importante saper fare delle scelte:

- Come fruitori attivi (es. scegliere bene le parole e le foto che decidiamo di pubblicare, informarsi prima di scrivere su argomenti che non conosciamo, usare un linguaggio corretto, chiedere prima di postare foto di qualcun altro, ecc.)
- Come fruitori passivi (es. essere sempre critici, per esempio quando leggiamo le notizie o vediamo una foto "acchiappaclic", impostare comandi che ci permettano di decidere se pubblicare o meno una foto scelta da altri, ecc.)

Modalità Didattica a Distanza

- Chiedere a ogni studente di prendere un foglio e piegarlo a metà. Viene dato il compito di scrivere su una metà un'azione attiva e sull'altra metà un'azione passiva. Gli studenti hanno pochi minuti di tempo, al termine dei quali saranno chiamati a condividere a voce quello che hanno scritto.

Together for Tomorrow!
Enabling People

CRESCERE CITTADINI DIGITALI

Guida all'insegnamento dell'Educazione Civica Digitale

Lezione 1
Identità Digitale

SAMSUNG

Parola all'esperto: Barbara Volpi

Psicologa, psicoterapeuta, PhD in Psicologia Dinamica e Clinica Sapienza-Roma. Collabora con il Dipartimento di Psicologia Dinamica e Clinica della Sapienza. È autrice di numerose pubblicazioni, articoli di ricerca e interventi sulla genitorialità e sull'educazione digitale in tutto il territorio nazionale.

Tra le sue recenti pubblicazioni:

B. Volpi [2021], Docenti Digitali. Insegnare e sviluppare nuove competenze nell'era di internet, Il Mulino;

B. Volpi [2017] Genitori Digitali. Crescere i propri figli nell'era di internet;

B. Volpi [2014], Gli adolescenti e la rete, Carocci [2° rist. 2021].

Identità digitale: che cos'è?

L'identità digitale è l'insieme delle informazioni e dei dati che l'utente immette in rete sia per accedere a determinati siti o per poter usufruire di determinate applicazioni, sia come tracce di sé che lascia o che altri lasciano senza la sua autorizzazione nella navigazione come foto, video, contenuti che possono essere raccolti per determinare l'identificazione di una persona. Navigando in rete lasciamo orme digitali [digital footprint] che determinano di riflesso la nostra conformazione identitaria sia in forma di dati personali come nome cognome, indirizzo di residenza, codice fiscale, numero di telefono, sia sotto forma di gusti personali, hobbies, desiderata che possono essere proliferati orientando le nostre stesse scelte comportamentali.

L'identità digitale è il nostro biglietto da visita con il quale gli altri possono trovarci in rete, conoscere i nostri gusti, le nostre preferenze, visionare le nostre azioni e i nostri comportamenti, arrivare a conoscere i nostri dati personali con i rischi ed i pericoli che ne possono derivare.

Identità Digitale: perché parlarne

Nella società del riflesso delle identità sugli screen il promuovere e tutelare l'identità digitale di ciascuno di noi è uno dei tasselli cardine dell'educazione digitale e della tutela del benessere digitale delle nuove generazioni. Gli obiettivi educativi della società attuale nella riconfigurazione digitale devono orientarsi alla tutela della privacy della vita privata e delle relazioni interpersonali e al controllo e al monitoraggio dei propri dati personali all'interno della rete nel rispetto dei suoi diritti e della sua dignità personale.

L'input e l'output con il quale attiviamo le nostre azioni in rete non è mai indelebile ma lascia sempre traccia del nostro percorso. Un po' come le serie Tv che riassumono nelle puntate successive quanto emerso in quelle precedenti facendoci comprendere a che punto della nostra conformazione identitaria siamo arrivati.

Oggi nel 2020 non ha più molto senso parlare della distinzione tra mondo reale e mondo virtuale in quanto siamo tutti inseriti in un e-life costante in cui il dentro e il fuori lo schermo ha riconfigurato e riconfigura incessantemente la nostra società. L'ormai datata distinzione tra immigrati e nativi digitali viene superata dalla considerazione generale che TUTTI, bambini e grandi, tecnologicamente abili o meno, sono a tutti gli effetti cittadini digitali con il diritto e il dovere di utilizzare con competenza la tecnologia che anche se invisibile (basti pensare all'Internet of Things) orienta i nostri comportamenti in tutte le sfere del vivere quotidiano (dal lavoro alle relazioni sociali, all'apprendimento). Compito della società è quello di orientare i cittadini verso la costruzione di una cittadinanza digitale responsabile e consapevole avvalendosi di un percorso di educazione digitale o "screen education" che parte dall'infanzia fino all'età adulta lungo una traiettoria educativa che tiene conto dei bisogni e della capacità di acquisizione nelle diverse fasce del ciclo vitale.

I genitori devono essere consapevoli che immettere le foto del loro bambino in rete è un primo tassello della costituzione dell'identità digitale del proprio figlio prima ancora che lui stesso ne sia consapevole.

Quel che accade dentro lo screen e tra gli screen non appartiene solo allo spazio digitale ma di riflesso, nell'interconnessione costante tra il dentro e il fuori lo schermo, si rispecchia nella vita quotidiana agendo da amplificatore del disagio qualora in rete vengano immessi dati personali e agiti espressivi poco

edificanti. Nella nuova scrittura digitale che segue le sue regole espressive nulla viene dimenticato e ogni passo è segnalato per comprendere i passi procedurali di una società in profonda e rapida trasformazione. Le linee guida preventive per arginare il disagio in rete mettono in evidenza l'azione capillare dell'attenzione dapprima genitoriale, poi della scuola e solo in ultimo degli adolescenti come dimensione primaria per strutturare con competenza e dare valore alla propria identità digitale e per rispettare quella dell'altro.

In questa prospettiva il bambino sin da piccolo deve essere indirizzato verso la protezione dei suoi dati personali e non può essere lasciato da solo con lo schermo in mano prima ancora di essere pervenuto ad una distinzione tra ciò che vede nello screen e ciò che è parte del suo ambiente di vita. Prima infatti di arrivare a fenomeni di derisione e di scherno che in rete si diffondono in modo epidemico assumendo il profilo identitario del cyberbullismo occorre sensibilizzare i bambini e i ragazzi a mantenere viva l'attenzione e la riflessione sulle azioni azionate da touch impulsivi e poco riflessivi. Sin da piccoli i bambini devono essere sollecitati a parlare in famiglia delle loro attività con i device, sia a casa che a scuola. Parlare delle esperienze digitali è il primo passo preventivo per agire con consapevolezza, spirito critico e valore etico in rete.

Attenzione alla protezione dei dati personali, alla privacy che non è solo relativa al nome e al cognome ma anche agli agiti che lasciano tracce di sé nel digitale, così come all'invio di screenshot per testimoniare con dati alla mano il tradimento di turno, vuoi che sia dell'amico che del fallimento di una relazione sentimentale. Prima di arrivare a commettere reati in rete, a creare profili falsi per ingannare l'altro, ad entrare senza l'autorizzazione nei profili dell'altro per immettervi foto o notizie che ledono la reputazione e l'immagine personale commettendo dei veri e profili reati punibili per la legge, occorre attivare una rete di sensibilizzazione tesa alla prevenzione del disagio e al corretto comportamento in rete a partire dalla tutela e della protezione della nostra identità digitale così tanto importante nella società attuale. Se siamo vittime di attacchi diretti alla nostra identità digitale, se diveniamo il bersaglio mediatico di diffamazioni, minacce e insulti in rete dobbiamo sapere che ogni comportamento sia il nostro che quello dell'altro può essere tracciato, ricostruito e denunciato. Abbiamo il dovere di segnalare di essere stati vittime e il diritto di essere tutelati e di far cancellare l'attacco alla nostra identità. Abbiamo il diritto all'oblio, a cancellare tracce che noi non abbiamo prodotto e che testimoniano l'altra faccia della medaglia di agiti criminali che come società responsabile ed eticamente fondata dobbiamo punire aiutando la persona offesa a riconfigurare la sua vera identità nella rete.

D'altra parte nella costruzione di una società di alto valore etico occorre strutturare un percorso di rieducazione per i soggetti che hanno violato le buone prassi di condotta digitale tendendo conto, soprattutto per i minori, delle implicazioni psicologiche dei diversi acting out.

Barbara Volpi

Obiettivi formativi

- Definire le “norme” comportamentali del cittadino digitale
- Approfondire temi legati al comportamento del cittadino digitale con particolare attenzione al tema dei dati personali e della privacy
- Approfondire il tema del cyberbullismo fornendo indicazioni sia sull’entità che sulla portata del fenomeno
- Sensibilizzare alla prospettiva legale dei reati online

Indice lezione

Capitolo 1: Orme digitali e cookie

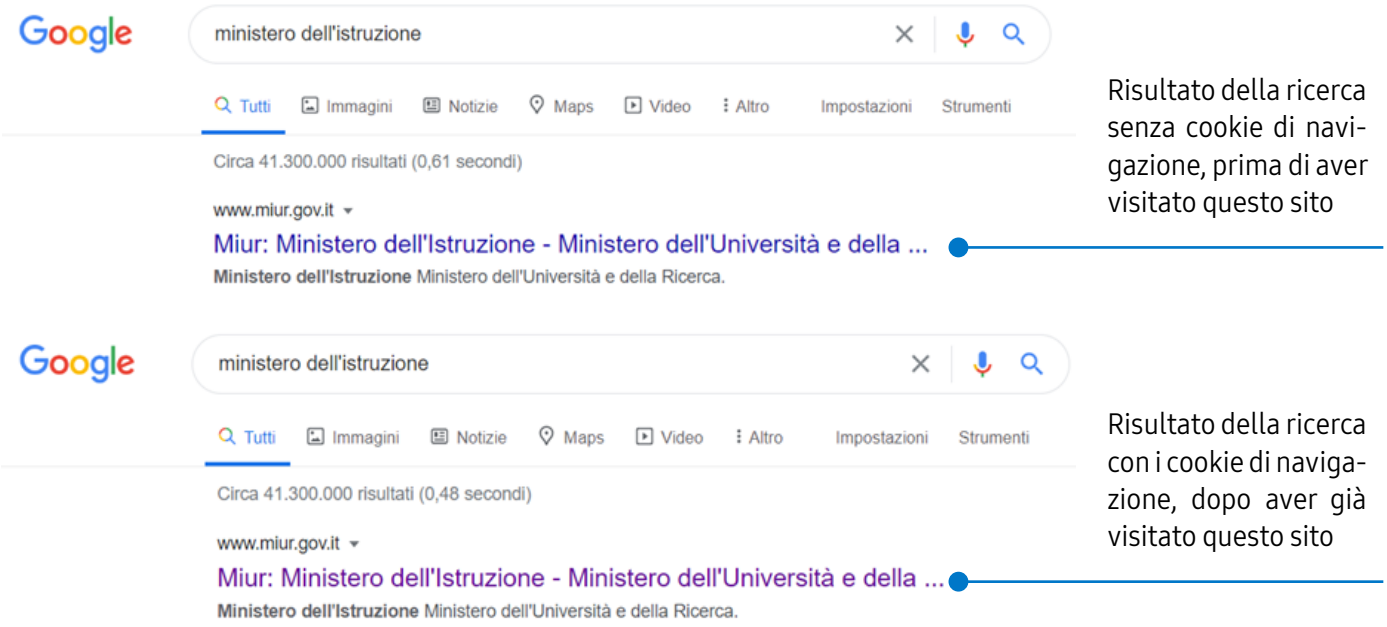
In quanto cittadini digitali dobbiamo essere consapevoli che, anche online, abbiamo una nostra identità che ci definisce, che lascia delle tracce nei vari "movimenti" che facciamo e che è rintracciabile sulla base di una serie di informazioni che ci identificano.

I cookie

Quando navighiamo in rete, lasciamo infatti delle tracce del nostro passaggio che servono a migliorare la nostra esperienza di navigazione e a raccogliere dati sui nostri interessi e sulle nostre preferenze.
Queste orme digitali prendono il nome di "cookie".

I cookie sono dei file che vengono creati automaticamente quando visitiamo dei siti web e che vengono salvati dal nostro browser, cioè il programma che utilizziamo per navigare su Internet (ad es. Google Chrome). Questi file memorizzano i dati della nostra navigazione e tengono traccia delle nostre attività, generando una sorta di codice identificativo anonimo che viene associato all'utente.

Se, ad esempio, facciamo una ricerca Google e apriamo uno dei risultati, facendo la stessa ricerca dallo stesso dispositivo e dallo stesso browser tempo dopo, nella pagina dei risultati vedremo in viola il risultato che avevamo già aperto.



Risultato della ricerca senza cookie di navigazione, prima di aver visitato questo sito

Risultato della ricerca con i cookie di navigazione, dopo aver già visitato questo sito

Ciò significa che la prima volta che abbiamo aperto il sito "www.miur.gov.it" è stato creato un cookie che ha memorizzato questa attività. La volta successiva, quindi, quel sito ci viene presentato in cima all'elenco dei risultati ed è contrassegnato con il colore viola, ad indicare che abbiamo già visitato quel sito e che quindi è probabilmente ciò che stiamo cercando.

I cookie, quindi, da un lato migliorano la nostra esperienza online, permettendoci di salvare le nostre preferenze e di trovare più facilmente le informazioni che stiamo cercando, ma dall'altro raccolgono i nostri dati per fini commerciali e pubblicitari.

Esistono infatti due macro-tipologie di cookie:

- Cookie tecnici, che servono ad ottimizzare la navigazione e sono necessari per il corretto funzionamento dei siti web
- Cookie di profilazione, che servono a creare un profilo dell'utente sulla base dei suoi interessi e che sono utilizzati per attività di marketing e pubblicità. Vi sarà sicuramente capitato di cercare un prodotto online e di visualizzare poi, per un certo periodo di tempo, moltissime pubblicità relative a quello stesso prodotto: questo è reso possibile proprio dai cookie di profilazione.

Dal 2015, secondo la legge italiana ed europea, tutti i siti che utilizzano cookie di profilazione sono obbligati ad informarne l'utente, che potrà scegliere se accettarli o meno. Quando apriamo un sito, infatti, vediamo comparire in primo piano un banner che ci informa sull'utilizzo dei cookie e ci permette di accettare o meno l'utilizzo di quelli relativi ai fini pubblicitari: questi cookie non sono necessari per il funzionamento del sito, quindi se decidiamo di rifiutarli potremo comunque navigare senza limitazioni. Se non clicchiamo sul banner, ma continuiamo a visitare il sito, accettiamo implicitamente l'informativa.

Capitolo 2: Dati e privacy

Le "orme" attraverso la navigazione in rete sono di fatto dati personali. Cosa sono questi dati nello specifico? Perché è così importante comprendere come vengono tracciati e trattati?

Dati personali

Iniziamo cercando di capire quali sono le varie tipologie di dati che tutti i giorni girano sul web. I dati presenti online vengono raggruppati in due macro-categorie:

- I dati non personali
- I dati personali

Vengono considerati **dati non personali** tutti quei dati che non possono essere collegati a una persona identificata o identificabile. Le informazioni di questo tipo includono per esempio i dati meteorologici, i dati prodotti da dispositivi industriali, i dati relativi al monitoraggio di strutture o di processi e, in generale, tutti quei dati generati da dispositivi.

I **dati personali** costituiscono qualsiasi informazione relativa a una persona fisica identificata o identificabile, incluse quindi quelle informazioni che conducono all'interessato solo indirettamente, o effettuando controlli incrociati. Sono dati personali il nome, il codice fiscale, la voce, l'impronta digitale, gli indirizzi IP (Internet Protocol address), i cookie e i dati di geolocalizzazione, i dati telefonici, gli account, i dati sulle opinioni politiche ecc. Per la legge italiana ed europea, i dati personali possono riferirsi solamente a una persona fisica, non a una persona giuridica, come per esempio un'azienda.

I dati personali a loro volta si differenziano per tipologia ed è prevista una tutela maggiore per quei dati che possono essere utilizzati per discriminare gli individui, i cosiddetti dati particolari (o come venivano chiamati una volta, dati sensibili).

Vediamo nel dettaglio quali tipologie di dati costituiscono i dati personali:

- **Dati identificativi**, ovvero quei dati che permettono l'identificazione diretta, come i dati anagrafici, o indiretta, come un numero di identificazione, dell'interessato. Fanno parte di questa categoria nome e cognome, indirizzo di casa, indirizzo mail, numero di passaporto, numero di telefono, indirizzo IP del proprio computer, dati di geolocalizzazione, numero di targa ecc.

- **Dati particolari (sensibili)** sono dati soggetti a trattamento speciale, ovvero quelli che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, i dati genetici e i dati biometrici (es. l'impronta digitale, la forma fisica della mano, del volto, dell'iride o della retina), i dati relativi alla salute, i dati relativi all'orientamento e alla vita sessuale della persona e i dati giudiziari.

L'utilizzo dei dati personali è dettagliatamente regolamentato dalla normativa europea.

Secondo la Carta dei diritti fondamentali dell'Unione europea, infatti, il diritto alla protezione dei dati personali è un diritto fondamentale dell'individuo e il 25 maggio 2018 in tutti i paesi dell'UE è entrata in vigore una nuova importante normativa, frutto del lavoro di diversi anni all'interno dell'UE, denominata General Data Protection Regulation (GDPR), Regolamento Generale sulla Protezione dei Dati.

Si tratta di un passo molto importante che ha rafforzato la protezione dei dati personali di cittadini e residenti UE.

Ma perché è così importante proteggere questi dati?

Proteggere i propri dati

I dati che immettiamo ogni giorno in Internet sono tantissimi. Quando utilizziamo la posta elettronica, effettuiamo delle ricerche su Google o ci muoviamo all'interno di una pagina web veniamo costantemente monitorati (le impronte di cui si parlava prima). Tutti questi dati, anche se apparentemente non ci sembrano "preziosi", hanno in realtà un importante valore economico.

Le tracce che lasciamo, incluse quelle sulla nostra mobilità, vengono raccolte e permettono a chi ha ottenuto il dato di "profilare" ognuno di noi, di avere quindi un quadro abbastanza chiaro di quello che ci interessa, dei luoghi virtuali e fisici che frequentiamo e di tanti altri aspetti che possono interessare chi usa Internet per pubblicizzare i propri prodotti o servizi, o per influenzare il pubblico.

La profilazione, infatti, determina il tipo di contenuti che visualizziamo online. Questo può tornarci molto utile quando siamo alla ricerca di qualcosa di particolare, o quando vogliamo ritrovare velocemente una pagina che avevamo già visitato, perché in quel caso il web ci verrà in aiuto proponendoci suggerimenti che potrebbero facilitare il nostro lavoro (pensiamo a quando si cerca un paio di scarpe su un motore di ricerca e si visualizzano poi annunci di scarpe per giorni e giorni).

Talvolta, però, la profilazione fa sì che le notizie e le informazioni che troviamo online siano "filtrate" dal tipo di utente che siamo, influenzandoci quindi nelle nostre opinioni e scelte. Basti pensare al caso di Cambridge Analytica, la società che ha raccolto senza consenso esplicito i dati personali di milioni di account Facebook per rivenderli a scopo di propaganda politica. Uno scandalo che ha reso chiaro a tutti come sfruttando i dati personali e le informazioni condivise sui social sia possibile influenzare le decisione di milioni di persone.

Non è necessario che questi dati vengano considerati tutti assieme per avere valore: sapere anche solo la fascia d'età, il sesso di una persona, il paese in cui vive e quali sono le ricerche che effettua su Google sono informazioni sufficienti per essere utilizzate.

Per questo motivo è importante che ognuno di noi sia consapevole di quello che accade mentre naviga in Internet, e che adotti delle misure per tu-

telare la propria privacy, ovvero la riservatezza dei priori dati personali.

Vediamo assieme alcune misure che possiamo adottare:

- Quando ci iscriviamo a un servizio o creiamo un account, leggiamo l'informativa privacy e aiutiamo i più giovani a capire di cosa si tratta. Leggendo le varie informative noteremo che non sono tutte uguali, e impareremo a identificare quali sono gli aspetti a cui prestare attenzione. Ogni informativa infatti è composta più o meno dagli stessi elementi, che dovrebbero aiutare gli utenti a capire diversi aspetti, tra cui chi eroga il servizio e detiene i dati, quali sono esattamente i dati che detiene, per quanto tempo e con quali finalità, come fare per cancellare i propri dati ecc.

- Impariamo a distinguere i motori di ricerca: ognuno ha la propria policy in termini di dati che vengono raccolti. Firefox e Qwant, ad esempio, sono motori di ricerca che non profilano le informazioni degli utenti.

Link e informazioni utili

- Il 28 gennaio viene celebrata la giornata europea della protezione dei dati personali, per sensibilizzare e promuovere l'importanza della privacy e della protezione dei dati

- Garante per la protezione dei dati personali
  www.garanteprivacy.it/

- Link Google per verificare quali informazioni relative alla nostra identità e alle nostre attività sono tracciate per decidere se eliminarle o meno
  https://myaccount.google.com/dashboard

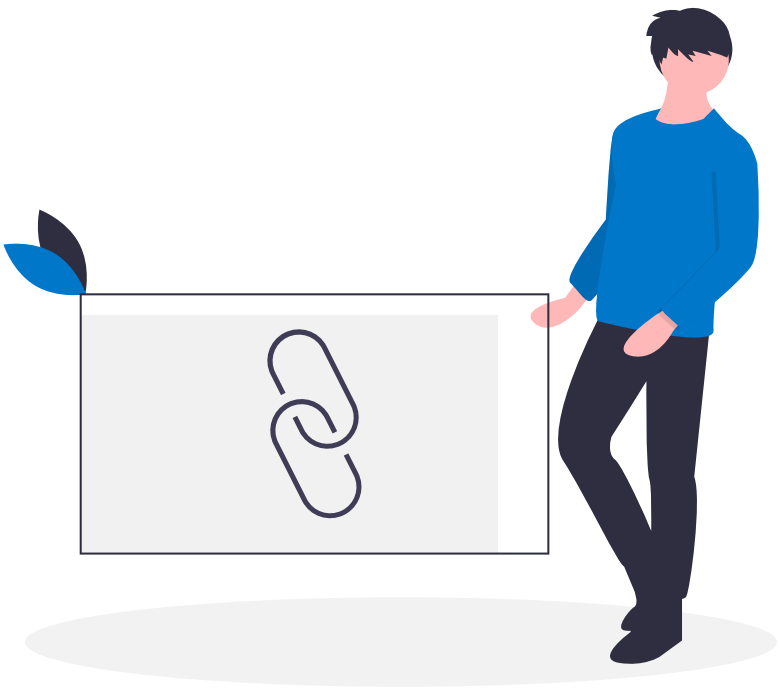
- Link Facebook per modificare le impostazioni sulla privacy
  https://it-it.facebook.com/help/325807937506242

- Link Instagram per modificare le impostazioni sulla privacy
  https://www.facebook.com/help/instagram/116024195217477/

- Modulo Google per richiedere di far rimuovere dai risultati delle ricerche i contenuti ritenuti lesivi (che non vengono quindi più indicizzati)
  https://www.google.com/webmasters/tools/legal-removal-request?complaint_type=rtbf&visit_id=637369701910557419-3025121284&rd=1

- Modulo per il Reclamo al Garante per la protezione dei dati personali
  https://www.garanteprivacy.it/modulistica-e-servizi-online/reclamo

- Altri link utili:
  www.garanteinfanzia.org
  www.agcom.it
  www.commisariatodips.it
  www.miur.gov.it
  www.famiglia.governo.it
  www.generazioniconnesse.it



Capitolo 3: Cyberbullismo

Un aspetto fondamentale legato alla nostra presenza online riguarda il comportamento che adottiamo nei confronti degli altri utenti. Non avere davanti una persona fisica porta spesso le persone a comportarsi in modi che, nella vita reale, non prenderebbero neanche in considerazione. Lo schermo, in questi casi, per molti funge da barriera, ma in quanto utenti e cittadini digitali dobbiamo ricordarci che i nostri comportamenti sul web hanno lo stesso valore di quelli che adottiamo offline.

Con lo sviluppo del mondo digitale si è sviluppato anche il fenomeno, di cui ormai abbiamo tutti sentito parlare, del cyberbullismo, ovvero di tutti quegli atteggiamenti che avvengono online e che costituiscono episodi di bullismo.

Non so chi è stato ma i miei genitori si sono rivolti alla Polizia Postale per identificare il colpevole. Non sono riuscita più ad entrare nel mio profilo di Instagram, la password non era più quella ma il profilo era attivo.
Hanno iniziato a pubblicare mie foto e video di me fuori dalla scuola deridendomi facendo credere che fossi io a farlo quando invece non sapevo nulla di nulla. Mi hanno seguito, mi hanno fotografato e hanno pubblicato tutto a mia insaputa.
È stato difficile anche farlo capire ai miei che inizialmente non mi credevano ma poi hanno visto in tempo reale un video pubblicato quando ero davanti a loro e avevano il mio telefono in mano.

La legge italiana

La Legge 29 maggio 2017 n. 71 prevede delle misure di contrasto del fenomeno del cyberbullismo lo definisce come *"qualunque forma di pressione, aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione, furto d'identità, alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati personali in danno di minorenni, realizzata per via telematica, nonché la diffusione di contenuti on line aventi ad oggetto anche uno o più componenti della famiglia del minore il cui scopo intenzionale e predominante sia quello di isolare un minore o un gruppo di minori ponendo in atto un serio abuso, un attacco dannoso, o la loro messa in ridicolo".*

Pertanto possono essere sanzionate penalmente le singole condotte di cyberbullismo qualora ricadano nelle fattispecie di reato (quali minaccia, estorsione, sostituzione di persona).
Uno screenshot, una foto ritoccata, un video. Il cyberbullismo può iniziare da un'azione semplice, una di quelle che tutti noi compiamo ogni giorno. Proviamo a pensare a qual è la differenza tra una presa in giro tra amici e un'aggressione online. Nel primo caso si tratta di una interazione tra amici che utilizzano espressioni scherzose in maniera affettuosa senza l'intento di far soffrire qualcuno. Nel secondo caso invece si tratta di episodi in cui una o più persone rivolgono scherzi e battute contro una persona sola con l'intenzione di farle del male ed emarginarla dal gruppo, stabilendo una relazione che tra le parti che non è alla pari.

Qualche dato

Secondo un'indagine conoscitiva effettuata su bullismo e cyberbullismo dall'ISTAT[1], il cyberbullismo riguarda il 22,2% di tutte le vittime di bullismo.
Secondo l'indagine, tra i ragazzi di età compresa tra gli 11 e 17 anni che utilizzano quotidianamente il cellulare (85,8% del totale), ben il 22,2% riferisce di essere stato vittima di cyberbullismo.

Dall'indagine emergono anche due aspetti interessanti:

- **Le ragazze sono più colpite dei ragazzi.** Il 7,1% delle ragazze 11-17enni che hanno accesso a Internet o possiedono uno smartphone ha subito episodi ricorrenti di cyberbullismo, contro il 4,6% dei ragazzi. Questa differenza è probabilmente dovuta anche al fatto che le ragazze di questa età utilizzano il cellulare in maniera maggiore rispetto ai propri coetanei (l'88% delle ragazze usa il cellulare tutti i giorni, contro l'84% dei ragazzi).
- **I giovani sono più colpiti degli adolescenti.** Il 7% dei bambini tra 11 e 13 anni ha subito episodi ricorrenti, contro il 5,2% dei i ragazzi di età compresa tra i 14 e i 17 anni.

Varie forme di cyberbullismo

Come abbiamo visto il fenomeno del cyberbullismo si basa su alcune condizioni: l'intenzionalità, la persistenza nel tempo, l'asimmetria nella relazione e il mezzo telematico. Le forme con cui si manifesta questo fenomeno però sono molteplici. Gli esperti hanno identificato le seguenti modalità:

- **Cyberstalking (cyber-persecuzione)** Consiste nel molestare e denigrare ossessivamente una persona online per incutere paura e terrore generando in essa una sensazione di insicurezza e facendola temere per la propria incolumità.

SMS anonimo:

Te la farò pagare. Hai ancora pochi giorni e poi finalmente sarà finita.
Ti voglio MORTO.

- **Exclusion (esclusione)** Consiste nell'escludere deliberatamente e senza motivo una persona da un gruppo online per ferirla.

In chat:

Dai, di questo parliamone nell'altra chat che qui non sanno neanche cosa vuol dire!

- **Exposure o outing (rivelazioni)** Consiste nel diffondere online le informazioni confidate spontaneamente da un compagno.

Chat di classe:

Perché, non lo sapevate che Matteo è follemente innamorato di Greta? Guardate qua, le manda anche sue foto in Direct!

Screenshot chat privata

1 ISTAT, Commissione parlamentare per l'infanzia e l'adolescenza, Indagine conoscitiva su bullismo e cyberbullismo (2019) https://www.istat.it/it/archivio/228976

- **Harassment (molestie)** Consiste nell'inviare in maniera ossessiva e ripetuta messaggi contenenti insulti a una singola persona, che causano disagio emotivo e psichico.

SMS anonimo:
Ti odio, anzi ti odiano tutti. Sei un'inutilità e faresti meglio a sparire!

- **Flaming (dall'inglese flame, fiamma)** Consiste nell'inviare messaggi offensivi e/o volgari online al fine di danneggiare gratuitamente una persona, solitamente su social network, forum e siti di discussione online.

Chat tra giocatori che stanno giocando online live:
- Niko97 sei un pivello, neanche mia nonna gioca così male
- Sì Niko97 fuori di qui!
- Non farti rivedere!

- **Happy slapping (dall'inglese, schiaffeggio allegro)** Consiste nel molestare fisicamente qualcuno con l'obiettivo di riprendere l'aggressione e di pubblicare il video sul web.

Riprendendo un ragazzo mentre viene picchiato da un gruppo:
Dai bello, fai un sorriso per i tuoi fan, fai vedere come sanguini bene!

- **Trolling** Consiste nel disturbare le conversazioni altrui online pubblicando messaggi provocatori o senza senso.

Commenti ripetuti a un post pubblico:
- Stai zitto, i vaccini sono una truffa!
- Basta vaccini, basta casta!

- **Masquerade (sostituzione di persona) o identity theft (furto d'identità)** Consiste nel rubare l'identità di una persona con l'obiettivo di pubblicare a suo nome contenuti volgari.

Post Facebook sulla bacheca di una ragazza, scritto a sua insaputa da compagni che le hanno rubato la password dal diario:
Ciao, sono brava in tutto, se mi volete chiamatemi (+39 555 1234 567)

- **Denigration (denigrazione)** Consiste nel divulgare nella rete notizie sulla vittima, allo scopo di danneggiarne la reputazione o le amicizie. Colpisce generalmente aspetti centrali della personalità del soggetto come l'orientamento sessuale, l'appartenenza etnica, difetti fisici, difficoltà scolastiche e situazioni familiari.

Mailing list della scuola:
Oggetto: Sorpresa
Testo: Eccolo qui il più gay della scuola
Allegati: foto di un compagno di scuola con il suo ragazzo

- **Trickery (inganno)** Consiste nel conquistare la fiducia di una persona per ottenere informazioni private e/o imbarazzanti con la finalità di renderle pubbliche.

Chat privata:
Ma quindi vai dallo psicologo? Perché? Dai raccontami, di me puoi fidarti!

Abbiamo visto che in moltissimi casi le forme di cyberbullismo riguardano la condivisione non autorizzata di informazioni, vere o false, relative alla vittima. Riguardo a questo è interessante sottolineare che secondo le statistiche lo strumento principale del cyberbullismo sono le foto.

Secondo i dati riportati dall'Indagine Telefono Azzurro e DoxaKids, rispetto ai ragazzi intervistati:

- Il 30% ha dichiarato di aver trovato online proprie foto non autorizzate
- Il 20% ha dichiarato di aver trovato online proprie foto imbarazzanti
- Il 15% ha dichiarato di aver trovato online propri video non autorizzati
- Il 10% ha dichiarato di aver trovato online propri video imbarazzanti

Cosa fare

Come abbiamo visto, il cyberbullismo può assumere diverse forme e non è solo evitando di mettere in atto in prima persona comportamenti violenti che il problema può essere eliminato.

Nel cyberbullismo la responsabilità può essere estesa e condivisa anche da chi "semplicemente" visiona un video e decide di inoltrarlo ad altri, ride o rimane indifferente. In questo senso il ruolo del gruppo assume nel bullismo elettronico un'importanza ancora più evidente e delicata.

L'astante o spettatore che frequenta i siti e fruisce delle immagini, diventa uno "strumento" fondamentale per lo scopo del cyberbullo e assume un ruolo di responsabilità attiva nei confronti delle vittime anche se, paradossalmente, non le conosce affatto.

Quando vediamo situazioni anomale, ma non ne parliamo o non denunciamo il fatto perché non ci sembrano affari nostri, diventiamo complici di atti di cyberbullismo. Lo stesso vale quando ci rendiamo conto che una persona a noi vicina viene bersagliata e prendiamo parte allo scherzo per non sentirci esclusi.

Per combattere il cyberbullismo possiamo:

- evitare di diffondere screenshot, foto o video intimi, denigratori o imbarazzanti, nostri e di persone che conosciamo;
- non partecipare a chat o pagine Facebook aperte esclusivamente per bersagliare qualcuno;
- parlare con un docente o con un nostro famigliare se ci sembra di vivere o di assistere a una situazione anomala;
- far caso ai comportamenti e alle reazioni dei compagni più sensibili e avvicinarli o avvertire qualcuno se ci sembra che si stiano isolando;
- non praticare mai hate speech sui social e ignorare o segnalare chi utilizza un linguaggio aggressivo.

Un'associazione italiana no profit, Parole Ostili, ha pubblicato il Manifesto della comunicazione non ostile, per rendere i rapporti più distesi nella vita e online. Consideriamo sempre che ogni contenuto condiviso online può avere forti impatti anche nella vita reale di ogni giorno.

Seguire le 10 regole del manifesto può aiutarci a lavorare contro l'hate speech, non solo evitando in prima persona di usare linguaggi e metodi comunicativi aggressivi e violenti, ma anche promuovendo uno stile di comunicazione più positivo centrato sull'importanza del rispetto della dignità dell'altro.

È possibile trovare il manifesto a questo link.
http://paroleostili.com/manifesto/

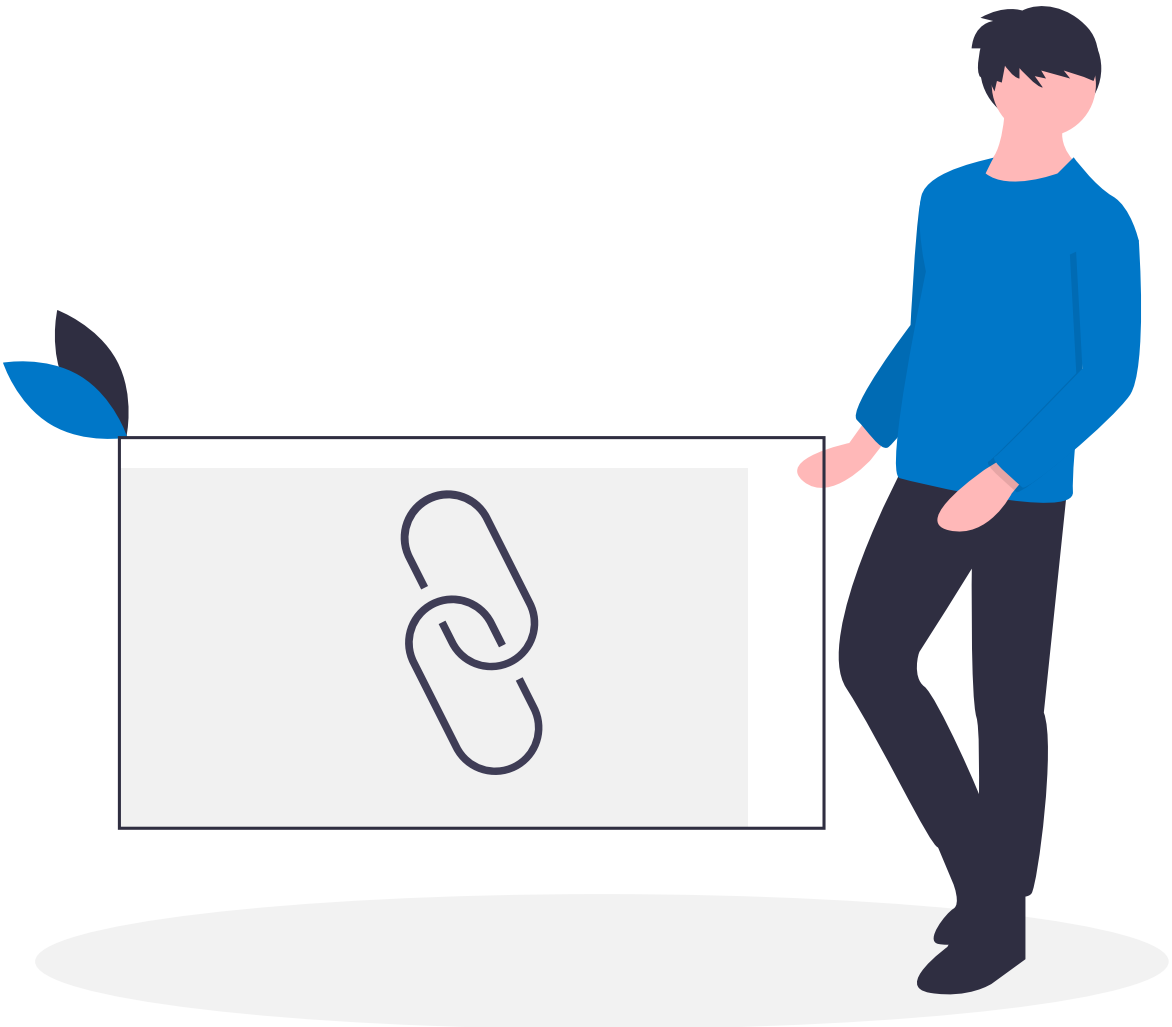
Link e informazioni utili

- Il Servizio del Dipartimento per le Politiche della Famiglia-Presidenza del Consiglio dei Ministri ha istituito un numero verde attivo o 24 ore su 24, il **114**, per dare supporto e soluzioni alle vittime di bullismo e di cyberbullismo.

- Ogni secondo giorno della seconda settimana di febbraio (9 febbraio 2021 il prossimo) si celebra il 'Safer Internet Day', una giornata istituita per fare appello alla gentilezza e per ricordare che, a livello mondiale, **1 studente su 3** è stato vittima di cyberbullismo .
  www.saferinternetday.org

- Indagine conoscitiva su bullismo e cyberbullismo dell'ISTAT:
  www.istat.it/it/archivio/228976

- Indagine Telefono Azzurro e DoxaKids 2020:
  https://azzurro.it/wp-content/uploads/2020/02/Dossier-Doxa_2020_web_singole.pdf



Capitolo 4: Prospettiva legale

La Legge 71/2017, oltre ad aver introdotto per la prima volta la definizione di "cyberbullismo", ha anche indicato alcune misure per il suo contrasto. Tra queste, le misure di maggior rilievo sono le seguenti:

- Ciascun minore ultraquattordicenne (o soggetto esercente la responsabilità del minore) che sia stato vittima di atti di cyberbullismo può inoltrare al titolare del trattamento o al gestore del sito internet o del social media un'istanza per l'oscuramento, la rimozione o il blocco dei contenuti. Entro 24 ore, il gestore deve provvedere. In mancanza, l'interessato può rivolgere analoga richiesta al Garante per la protezione dei dati personali, che rimuoverà i contenuti entro 48 ore (art. 2 L. 71/2017);
- Il dirigente scolastico che venga a conoscenza di atti di cyberbullismo informa tempestivamente i genitori dei minori coinvolti. I regolamenti scolastici dovranno prevedere esplicite sanzioni disciplinari, commisurate alla gravità degli atti compiuti (art. 5 L. 71/2017);
- Per i minori autori di atti di cyberbullismo, fra i 14 e i 18 anni, fino a che non intervenga una denuncia per i reati di cui agli articoli 594, 595 e 612 del codice penale, può essere applicata la c.d. "procedura di ammonimento": il questore convoca il minore insieme ad almeno un genitore per un ammonimento formale, che può avvenire anche in forma scritta (art. 7 L. 71/2017).

Si osservi che la Legge 71/2017 non ha introdotto una fattispecie autonoma di reato per atti di cyberbullismo, limitandosi a prevedere misure per il suo contrasto. Nondimeno, le condotte alla base delle varie forme di cyberbullismo (pressione, aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione, furto d'identità, alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati personali) possono configurare fattispecie perseguibili penalmente, punite finanche con la reclusione.

Così, ad esempio, flaming, denigration e masquerade possono configurare atti di diffamazione puniti, ex art. 595 cod. pen., con la reclusione fino a due anni, ovvero con la multa fino a 2.065 euro.

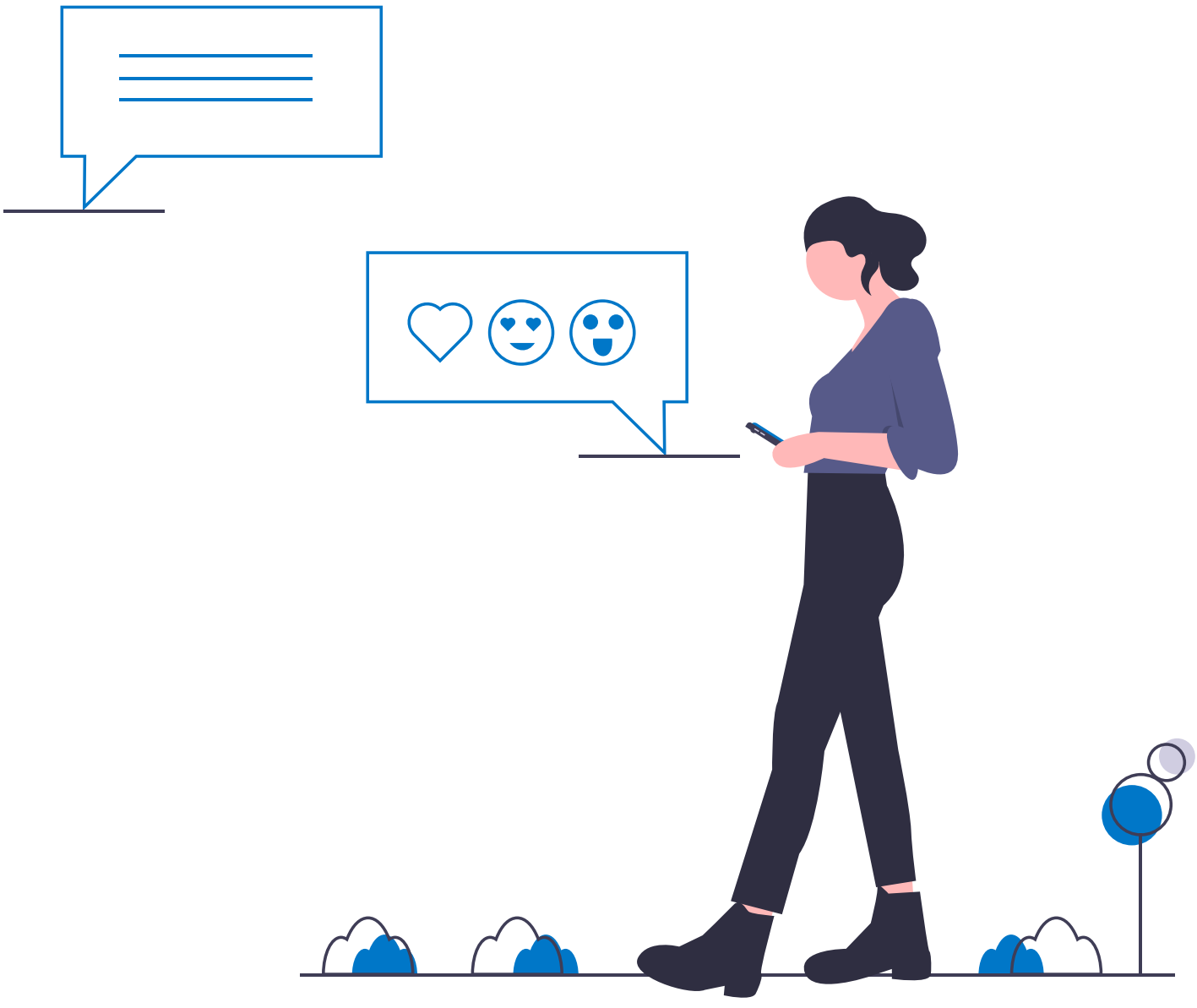
Flaming e masquerade possono astrattamente arrivare ad integrare il reato di minaccia di cui all'art. 612 cod. pen. (punito con la multa fino a euro 1.032).

L'exposure e il trickery (ove quest'ultimo sia finalizzato alla diffusione dei dati personali) sono sanzionati dall'art. 167 del D.lgs. 196/2003 con la reclusione da sei a diciotto mesi, laddove vengano diffusi dati della vittima senza il suo consenso e da tale condotta derivi un danno alla persona offesa (occorre tuttavia osservare che la tutela è in questo caso indebolita dall'esigenza di un profitto per l'agente: raramente il cyberbullo agisce per profitto, mirando piuttosto all'umiliazione della vittima).

Il cyberstalking (le cui condotte sono costituite materialmente da molestie) rientra nell'ambito del reato di atti persecutori ex art. 612 bis cod. pen. *"è punito con la reclusione da sei mesi a quattro anni chiunque, con condotte reiterate, minaccia o molesta taluno in modo da cagionare un perdurante e grave stato di ansia o di paura ovvero da ingenerare un fondato timore per l'incolumità propria o di un prossimo congiunto o di persona al medesimo legata da relazione affettiva ovvero da costringere lo stesso ad alterare le proprie abitudini di vita".* Laddove l'ipotesi non comporti veri e propri atti persecutori, potrebbe comunque essere integrata la contravvenzione di molestie ex art. 660 cod. pen.

Occorre a questo proposito ricordare che se il colpevole è un minore con meno di 14 anni, esiste una esclusione totale di imputabilità, cioè non si è perseguibili. Per chi, invece, ha più di 14 anni ma meno di 18, le pene sono ridotte.

Sul piano civile, l'autore degli atti di cyberbullismo – indipendentemente dal fatto che questi si qualifichino come reato – può certamente essere chiamato al risarcimento dei danni causati alla vittima.



ATTIVITÀ CON LA CLASSE

Attività 1 - I soliti ignoti

- Materiale necessario: due fogli e due pennarelli
- Obiettivo: rendere gli studenti consapevoli della quantità di azioni che compiamo per costruire la nostra identità digitale

La nostra reputazione digitale è nelle nostre mani dal primo accesso online e ogni impronta concorre a formarla e caratterizzarla. Ma come si costruisce un'identità digitale?
Sulla falsariga del gioco "I soliti ignoti", i ragazzi vengono stimolati a indovinare quante identità possiamo avere nel mondo digitale. Vengono chiamati due volontari, maschio e femmina, che si posizionano davanti alla classe. Prima di alzarsi avranno scritto su un foglio il loro nome virtuale – es. Marco e Anna – da attaccare addosso con lo scotch. L'insegnante elenca informazioni sui loro gusti e hobby (es. guarda film di fantascienza, il suo animale preferito è il gatto, è fan di Billie Eilish..) e i compagni devono indovinare, per alzata di mano, a chi piace cosa. In questa fase emerge il fatto che le informazioni sono generiche, dicono qualcosa di loro senza metterne a rischio la privacy. Successivamente l'insegnante condivide con la classe informazioni sui due personaggi (es. abita in Corso Como 25, va nella tal scuola, ha due sorelle di nome...) e invita gli studenti a riflettere sull'opportunità di condividere questo tipo di informazioni, sul concetto di privacy e dell'importanza e delicatezza del dato.

Modalità Didattica a Distanza
L'attività si può svolgere allo stesso modo anche a distanza, scegliendo due volontari che scrivono i loro nomi virtuali su un foglio da piegare e posizionare davanti allo schermo (oppure da attaccare addosso con lo scotch) in modo che tutti i compagni vedano.

ATTIVITÀ CON LA CLASSE

Attività 2 - L'identikit del cyberbullismo

- Materiale necessario: stampe
- Obiettivo: scoprire le diverse sfaccettature che può assumere il fenomeno dandogli un nome preciso. Rispondere alla domanda: "cosa potrei fare se mi trovassi in questa situazione?".

Dopo un breve brainstorming (il dibattito può essere ravvivato da frasi/domande stimolo fornite dall'insegnante) riguardo i possibili tratti che possono caratterizzare il fenomeno del cyberbullismo, si divide la classe in due squadre. Ad ogni squadra verranno consegnati diversi bigliettini prestampati con su scritto dei termini e altri contenenti una spiegazione. La squadra dovrà trovare la giusta associazione stilando così un vero e proprio identikit che aiuta a riconoscere le situazioni in cui si può parlare di cyberbullismo.

FLAMING	Offesa pura e gratuita, spesso volgare, per "tappare la bocca" della vittima e ricoprirla di insulti, con lo scopo magari di far ridere gli altri
HARASSMENT	Dall'inglese "molestia", è l'invio ripetuto di messaggi dal contenuto offensivo mirati a ferire una determinata persona e causarle un evidente disagio sia emotivo che psichico
TROLLING	Un "troll", nel gergo di Internet, è un soggetto che interagisce con gli altri tramite messaggi provocatori, irritanti, fuori tema o semplicemente senza senso per disturbare la comunicazione e fomentare gli animi
CYBERSTALKING	Rivolgere a qualcuno minacce, molestie e violenze con lo scopo di incutere nella vittima terrore e paura per la propria incolumità fisica
EXPOSURE/OUTING	Ottenere la fiducia di qualcuno con l'inganno per poi diffondere, pubblicare e condividere in rete le sue informazioni private, rivelandone i segreti
EXCLUSION	Escludere intenzionalmente qualcuno da un gruppo su un social network con l'obiettivo di provocargli un sentimento di emarginazione
DENIGRATION	Insultare o diffamare qualcuno online con pettegolezzi, menzogne e commenti crudeli, offensivi e denigratori per danneggiare gratuitamente e con cattiveria la sua reputazione
TRICKERY	Conquistare la fiducia di una persona per ottenere informazioni private e/o imbarazzanti con la finalità di renderle pubbliche
HAPPY SLAPPING	Molestare fisicamente qualcuno con l'obiettivo di riprendere l'aggressione e di pubblicare il video sul web
MASQUERADE/IDENTITY THEFT	L'aggressore si sostituisce alla vittima, utilizzando le sue informazioni personali per crearsi un profilo fittizio da cui spedire messaggi o pubblicare contenuti deplorevoli con lo scopo di danneggiarne l'immagine

Modalità Didattica a Distanza
Proiettare la tabella con le dieci parole e definizioni senza rispettare la corrispondenza parola-definizione. Gli studenti provano a fare delle ipotesi di associazione e condividono a voce o via chat quelli che secondo loro sono i reali abbinamenti.

Si può concludere con una riflessione sulle differenze tra il bullismo offline e il cyberbullismo. Cosa cambia?
Esempio: assenza di limiti spazio-temporali, maggiore visibilità, apparente anonimato del bullo...

Together for Tomorrow!
Enabling People

CRESCERE CITTADINI DIGITALI

Guida all'insegnamento dell'Educazione Civica Digitale

Lezione 2
Galateo del Digitale

SAMSUNG

Parola all'esperto: Antonio Deruda

Docente e consulente di comunicazione con vent'anni di esperienza professionale. È professore a contratto di "Teorie e tecniche dei linguaggi pubblicitari" e di "Psicologia della comunicazione e neuromarketing". Insegna comunicazione digitale nei corsi di specializzazione della SIOI, dell'Export Academy dell'ICE e della Scuola Nazionale dell'Amministrazione. È autore di due libri sulla diplomazia digitale.

La rivoluzione di Internet

Nell'ottobre del 1971 il giovane ricercatore americano Ray Tomlinson invia la prima email della storia. Poco dopo nascono le prime mailing list e i gruppi di discussione, nel 1980 fanno il loro debutto le emoticon, nel 1991 va online il primo sito web e nel 1996 nasce Sixdegrees.com, il precursore di tutti i social media. Sono le tappe principali di un lungo percorso che ha cambiato il nostro modo di vivere, di lavorare, di comunicare e di relazionarci con gli altri. La chiamiamo "rivoluzione di Internet" e la sperimentiamo ogni giorno, eppure ancora fatichiamo a comprenderne la portata e soprattutto a capire come comportarci nel nuovo universo digitale.

Cosa succede quando inviamo un'email a una persona, quando postiamo la foto di una festa con i nostri amici o quando critichiamo il video di uno sconosciuto? Il più delle volte la risposta è che non conosciamo veramente le conseguenze di questi gesti quotidiani. Siamo sempre più tecnologici, ma sempre meno consapevoli delle azioni che compiamo online. Sempre più immersi in nuove relazioni, ma sempre meno rispettosi degli altri. Sempre più comunicatori, ma sempre meno empatici. Ogni minuto nel mondo vengono scambiati 142 milioni di messaggi su WhatsApp, postate 147 mila foto su Facebook e caricate 500 ore di video su YouTube. Numeri da capogiro, che spesso ci fanno perdere il senso del nostro stare

online. Navighiamo nel web e consumiamo contenuti in modo superficiale, commentiamo e reagiamo con impulsività.

L'obiettivo di questa lezione sul Galateo Digitale è quello di lanciare un duplice invito. Uscire dal vortice di una Rete vissuta con frenesia e riflettere su quelle regole di base che possono aiutarci a comportarci in modo più consapevole e civile nelle nostre esistenze digitali.
Non inviare email indesiderate, rispettare gli argomenti in un forum di discussione, stemperare i toni di una discussione online con l'uso di un'emoji, chiedere il permesso prima di postare la foto di un'amica, fermarsi prima di scrivere un commento che potrebbe ferire un'altra persona. Piccole attenzioni che possono avere un impatto enorme, anche nel contrastare il diffondersi di patologie legate a un uso distorto della Rete e a una difficoltà di relazionarsi con gli altri online. Isolamento sociale, non accettazione di sé, bisogno morboso di apprezzamento da parte degli altri. Sono fenomeni in crescita che riguardano soprattutto i più giovani e che colpiscono in una fase delicata della crescita, lasciando spesso ferite interiori che il tempo non riesce a rimarginare.

Negli ultimi anni le piattaforme online hanno sviluppato una maggiore sensibilità verso queste problematiche e attuato misure per cercare di contrastarle. Da un più scrupoloso monitoraggio dei contenuti fino al blocco degli account che violano le norme. Sono passi avanti, ma non ancora sufficienti. La vera soluzione risiede in realtà nei nostri comportamenti. È solo attraverso l'educazione alle nuove tecnologie, la conoscenza delle regole del galateo digitale e la consapevolezza degli effetti delle nostre azioni online che possiamo rendere la Rete un luogo sicuro, inclusivo e ricco di opportunità di crescita per tutti.

Antonio Deruda

Obiettivi formativi

- Approfondire temi legati al comportamento del cittadino digitale con particolare attenzione a spazi virtuali come i social media

- Introdurre il tema della netiquette

Indice lezione

1. Rischi dei social media
2. Linguaggio corretto e rispetto dell'opinione altrui
3. Condividere contenuti
4. Attività con la classe

Capitolo 1: Rischi dei Social Media

La tecnologia digitale ha generato cose meravigliose: costruito relazioni, reso accessibili informazioni a un numero enorme di persone, creato nuove professioni e opportunità. Ha permesso alle persone di superare le distanze fisiche, di entrare in contatto con i propri cari e di esprimere pubblicamente le proprie opinioni.

Questi effetti presentano tuttavia anche un lato "oscuro": milioni di persone sono ancora poco consapevoli degli impatti negativi che la tecnologia digitale, se non utilizzata responsabilmente, può generare.

I rischi legati a una "non educazione" digitale:

- **Isolamento.** L'uso delle tecnologie digitali non è la causa diretta di disturbi associati all'isolamento sociale, ma a volte può favorire una più rapida diffusione di alcune patologie. Esiste infatti uno stretto legame tra salute mentale e utilizzo distorto dei social media. Per alcune persone i social media aiutano a colmare un vuoto relazionale nella vita reale, ma spesso si trasformano in un rifugio dalle pressioni del contesto sociale. Ci si abitua a vivere in un universo fatto solo di rapporti virtuali.

- **Non accettazione di sé.** L'uso distorto dei social media ha favorito anche altre patologie, come ad esempio la dismorfia. Si tratta di una condizione psicologica per cui le persone si concentrano su una o più caratteristiche del proprio aspetto esteriore, notando difetti che agli altri appaiono minimi o inesistenti. Può colpire chiunque, ma è più frequente negli adolescenti e nei giovani, e può causare ulteriori problemi come senso di angoscia, ansia e depressione. Recenti studi hanno rilevato che molti adolescenti ambiscono ad assomigliare a canoni di bellezza irrealistici, rappresentati nei loro selfie e in quelli dei loro influencer, grazie all'uso dei sempre più diffusi filtri. È stata definita la "dismorfia da Snapchat" (una delle prime piattaforme con i filtri) e viene esasperata quando l'adolescente riceve sui propri profili commenti e insulti denigratori che talvolta possono portare la vittima a sentirsi colpevole per la propria condizione.

- **Bisogno di riconoscimento.** Siamo esseri sociali e, in quanto tali, il nostro imperativo biologico primario è quello di connetterci con gli altri. Questa dinamica può però diventare rischiosa quando si associa a un eccessivo bisogno di approvazione sociale. La spasmodica ricerca del giudizio degli altri può farci perdere oggettività e autostima.

Sui social media tendiamo a costruire le nostre vite intorno a un'idea di perfezione percepita perché veniamo ricompensati attraverso segnali emotivi a brevissimo termine: un cuore, un like, uno smile. Questi segnali li confondiamo con la verità oggettiva. Fatichiamo a comprendere che si tratta di una popolarità finta, fragile, che in realtà ci lascia un senso di vuoto ancora più grande. Entriamo in un circolo vizioso, che ci porta a pensare: che cosa devo fare? Quanto devo cambiare per ottenere popolarità, ammirazione e stima da parte degli altri? Una stima che siamo in grado di misurare solo attraverso un pugno di like.

Questo esagerato bisogno di riconoscimento esterno colpisce in particolar modo le persone più fragili, più introverse, quelle con una bassa autostima o ancora troppo giovani per essersi costruite una propria autostima. Non a caso si è registrato negli ultimi anni un aumento vertiginoso tra giovani adolescenti e preadolescenti di ansia e de-

pressione (+189% i ricoveri ospedalieri per autolesionismo negli USA nelle preadolescenti rispetto al 2009) e di suicidi (+151% nelle preadolescenti e +70% nelle adolescenti rispetto alla media nel decennio 2001-2009, sempre negli USA)*.

Emerge dunque quanto sia importante essere digitalmente educati, consapevoli di quanto ogni nostra azione, commento o like abbiano un impatto su noi stessi e sugli altri e di quanto fondamentale sia il rispetto nei confronti di tutti.

*Fonte: Centers for disease control and preventions https://www.cdc.gov/

Capitolo 2: Linguaggio corretto e rispetto dell'opinione altrui

Con "netiquette" o "galateo digitale" si intende la serie di regole di comportamento quando si interagisce su Internet in spazi virtuali pubblici come forum, chat, social media oppure tramite email. Non c'è nessuna legge che imponga il rispetto di queste regole. Se una persona viola la netiquette non commette alcun reato, ma può essere giudicata negativamente e percepita come non rispettosa dell'altro.

Per sintetizzare la netiquette si usa spesso l'acronimo T.H.I.N.K.: prima di scrivere o socializzare, PENSA. Si applica, ovviamente con sfumature diverse, a tutti gli strumenti di comunicazione digitale (email, messaggistica istantanea, social media):

- **True**: quello che sto scrivendo o condividendo è vero? (vedi approfondimento Lezione 4)
- **Helpful**: è utile al mio interlocutore?
- **Inspiring**: offre uno spunto in una conversazione?
- **Necessary**: è necessario?
- **Kind**: è "gentile"?

Il principio fondamentale della netiquette è lo stesso che sta alla base del "viver civile", ovvero evitare di essere scortesi e maleducati. Partendo da questo principio, nel 1995 la Internet Engineering Task Force, organismo internazionale interessato all'evoluzione di Internet, ha redatto alcune regole con lo scopo di rendere l'esperienza del web la migliore possibile per chiunque, tenendo conto della peculiarità del mezzo tecnico a cui si applicano.

Secondo queste regole è educato:

- compilare correttamente il campo "oggetto" delle email in modo da far comprendere al destinatario l'argomento del messaggio e permettergli di attribuirgli la giusta importanza;
- curare la grammatica e la forma dei messaggi, per rendere più agevole la lettura e la comprensione del testo scritto;
- in caso di errori grammaticali da parte degli altri, evitare di attaccarli pubblicamente per quello che può essere un semplice errore di digitazione;
- evitare di essere intolleranti nei confronti di chi commette errori in una lingua straniera;
- evitare di scrivere in MAIUSCOLO: questo tipo di carattere è associato ad un tono di prepotenza e arroganza che equivale al gridare;
- evitare di inviare messaggi SPAM (pubblicitari, indesiderati);
- evitare di inviare email a tutti i propri contatti, rendendo visibili gli indirizzi di tutti gli utenti (esiste la funzione "inviare in copia nascosta" proprio per garantire la privacy degli utenti in queste situazioni. Se si invia una mail non privata a più destinatari lasciando in chiaro gli indirizzi email si stanno violando le normative sulla privacy);
- evitare, in situazioni diverse da quella appena citata, di inserire persone in copia nascosta: è poco elegante e, se si ha piacere che qualcuno che non è tra i destinatari sia aggiornato su quello che stiamo scrivendo, è meglio inserirlo in copia, magari, per la prima volta, presentandolo ai destinatari.
- cercare di non andare "fuori tema", inserendo nella chat o nel gruppo argomenti che non c'entrano nulla con le finalità per il quale il gruppo è stato creato;
- evitare di alimentare discussioni all'interno di un gruppo: nel caso di un diverbio di opinioni, è preferibile continuare la conversazione privatamente, senza coinvolgere e mettere in imbarazzo gli altri componenti del gruppo;
- non pubblicare, senza l'esplicito permesso

dell'autore, il contenuto di messaggi di posta elettronica, o di chat private;
- evitare di pubblicare foto che potrebbero mettere in imbarazzo altre persone;
- evitare qualsiasi tipo di discriminazione sociale (razziale, politica, sessuale, religiosa, ecc.).

Negli ultimi anni molte aziende hanno redatto dei documenti dedicati alle regole del galateo online, rivolti sia ai propri dipendenti che alle persone con le quali interagiscono online. Ecco alcuni esempi virtuosi di aziende che hanno introdotto una loro netiquette sui social media:

- IKEA
  www.facebook.com/IKEAItalia/app/208195102528120
- LA GAZZETTA DELLO SPORT
  www.facebook.com/LaGazzettaDelloSport/app/200170090317334
- VODAFONE
  www.facebook.com/vodafoneit/app/462397810604918

La prossemica nella comunicazione online

La prossemica è l'insieme degli elementi fisici attraverso i quali ci relazioniamo con gli altri: i gesti, i sorrisi, il tono di voce, i movimenti del volto e del corpo.

Comunicare online e attraverso i social media risulta certamente facile, veloce, informale e divertente. Ma mancano ovviamente tutti gli elementi della prossemica. È infatti impossibile stabilire con esattezza il tono di un messaggio veicolato attraverso la Rete. Questo aumenta in maniera esponenziale il rischio di fraintendimenti. Uno stesso commento può essere inteso in senso letterale o al contrario in senso ironico.

Pensiamo a un amico che, a commento di un nostro racconto su qualcosa che ci è appena accaduto, scrive la frase "Bella storia interessante!". Senza l'aiuto dell'intonazione, non è semplice capire se il nostro amico ci sta prendendo in giro o se è rimasto realmente colpito dalla nostra avventura. L'ironia è una forma di linguaggio figurato, così come la metafora o l'iperbole: per comprendere il significato realmente inteso dal parlante, chi riceve il messaggio deve comprendere quale sia l'intenzione comunicativa che va oltre le parole.

Per aiutare una corretta comprensione del messaggio, risulta particolarmente importante utilizzare bene la punteggiatura e gli emoticon. I puntini di sospensione, soprattutto se ripetuti, comunicano per esempio l'idea di poca chiarezza, di vaghezza, di "non detto". I punti esclamativi, invece, possono essere utilizzati per esprimere entusiasmo o per rafforzare dei concetti. Ma possono essere fraintesi. Se stiamo scherzando, è bene utilizzare una faccina sorridente per chiarire il nostro intento. Gli emoticon, usati con moderazione, possono infatti aiutarci ad aggiungere empatia a un messaggio che, in quanto virtuale, può risultare freddo o poco chiaro.

Capitolo 3: Condividere contenuti

Nonostante l'apparente facilità con la quale gli strumenti digitali ci permettono di comunicare, condividere e socializzare, molti sono i danni che possiamo causare agli altri con un atteggiamento di superficialità e mancanza di rispetto. Quello che possiamo definire una sorta di "disimpegno morale".

Non sempre ovviamente i danni sono voluti: spesso feriamo l'altro per semplice disattenzione, senza alcuna premeditazione. Per questo è bene considerare attentamente quello che si scrive, cercando di evitare anche le situazioni di fraintendimento.

Quali contenuti condividere

Abbiamo affrontato nella Lezione 1 il tema del cyberbullismo. Non è necessario sfociare in episodi estremi per parlare di non rispetto dell'altro sui social media. Oltre al linguaggio più corretto da utilizzare (netiquette), merita un approfondimento il tema della condivisione: è corretto o non corretto pubblicare foto o contenuti che riguardano o coinvolgono una terza persona?

Chi pubblica sul proprio profilo o su quello di altri la foto di un soggetto di cui non ha ricevuto l'autorizzazione, commette un reato. La legge sulla privacy, infatti, punisce con la reclusione fino a tre anni l'illecito trattamento di dati personali sul web. Quando queste immagini sono di carattere "intimo", si commette il reato più grave di stalking. Questo si applica a tutti i casi di diffusione non autorizzata di fotografie o video su WhatsApp, Snapchat, Facebook o YouTube.

Questi sono alcuni esempi di foto che non possiamo pubblicare su Facebook senza l'autorizzazione dei soggetti interessati:

- un'immagine in cui una persona sia riconoscibile e visibile da un pubblico indistinto e non controllabile: è violazione della privacy;
- un'immagine che mostra il volto di un minore, visibile da un pubblico indistinto e non controllabile, in questo caso senza l'autorizzazione dei genitori;
- un'immagine che ritrae una persona isolata dal contesto (per esempio una persona che appare sullo sfondo);
- un'immagine che ritrae una persona anche in una porzione piccola della foto (ripresa da lontano) ma con il volto riconoscibile (prevale il concetto della riconoscibilità rispetto a quello della dimensione dell'immagine).

Indipendentemente dai risvolti legali, anche quando esiste un rapporto di amicizia o confidenza con la persona oggetto della foto, raccomandiamo che le si chieda sempre un permesso preventivo alla pubblicazione.

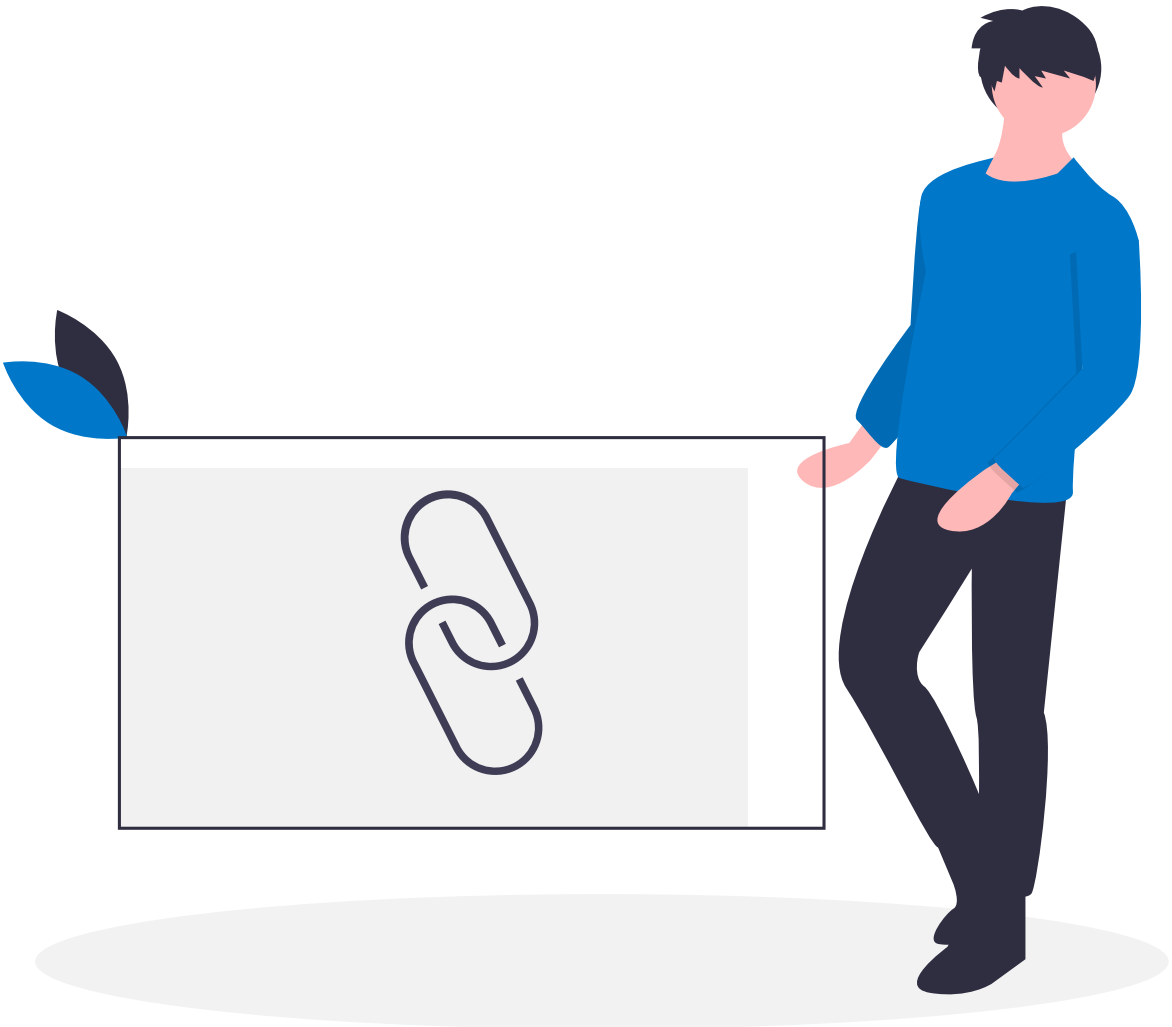
Qualora invece qualcuno abbia postato immagini nostre senza chiederci il consenso, abbiamo tutti i diritti di chiedere l'immediata rimozione del contenuto e di intraprendere vie legali qualora la richiesta non venisse immediatamente assolta.

Link e informazioni utili

- Linee guida della community di Instagram
  https://help.instagram.com/477434105621119

- Linee guida della community di Facebook
  https://www.facebook.com/help/477434105621119

- Linee guida della community di Tik Tok
  https://www.tiktok.com/community-guidelines?lang=en



ATTIVITÀ CON LA CLASSE

Attività 1 - Buone maniere Online

- Materiale necessario: possibilità di proiettare
- Obiettivo: rendere gli studenti consapevoli dei comportamenti corretti da tenere sul web e di come riconoscere quelli scorretti

Come nella quotidianità ci troviamo di fronte a diverse situazioni che richiedono un certo comportamento, anche online c'è bisogno di darsi alcune regole per non risultare inopportuni. Vengono fornite delle frasi, immagini o situazioni che rappresentano dei comportamenti che seguono il galateo digitale e altre completamente sbagliate (in alcuni casi molto riconoscibili, in altri meno)

Esempio 1: Importanza dell'oggetto delle mail

Cosa capisci leggendo l'oggetto di questa mail?

- La la laaa
- Regolamento Concorso Canoro

◊ *L'oggetto delle mail deve contenere lo scopo del messaggio, in questo caso il riepilogo del regolamento di un concorso canoro. La prima può anche essere una frase scherzosa, ma se non c'è confidenza con gli interlocutori meglio risparmiare le battute.*

Esempio 2: Parla come chatti

Cosa significano queste due frasi?

- No, non capisci.
- No, non capisci 😅

◊ *Nel mondo digitale, il contesto è quasi sempre informale ma la punteggiatura segue spesso regole diverse. Essendo del tutto assenti il tono, la cadenza, i gesti, i sorrisi, per evitare fraintendimenti possiamo usare le emoji (con moderazione). Il punto fermo invece non indica solo la fine di una frase: viene a volte caricato con un significato spiacevole, come il desiderio di chiudere.*

Esempio 3: Rispetto della privacy altrui

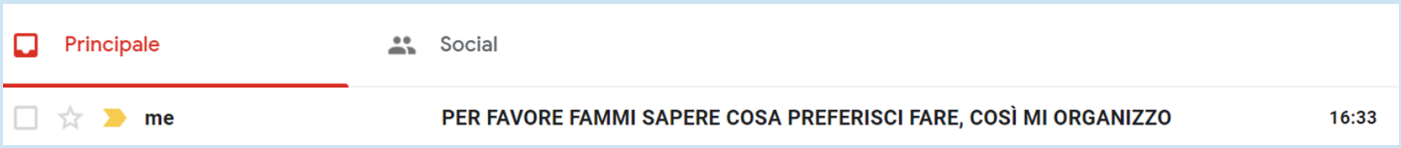
Ho una foto divertentissima di me con i miei amici. Non facciamo niente di particolare, ma a noi fa tantissimo ridere. Faccio bene a condividerla sui social?

◊ *Risposte libere dei ragazzi. Qualcuno potrebbe dire che se la foto non è compromettente non c'è nulla di male, al massimo ci facciamo tutti una bella risata. In realtà non è così, perchè una foto pubblicata oggi rimane per sempre ed è giusto che i diretti interessati siano liberi di scegliere se condividerla o meno. Per questo bisogna SEMPRE chiedere il consenso.*

ATTIVITÀ CON LA CLASSE

Esempio 4: L'importanza di non scrivere messaggi in maiuscolo

PER FAVORE FAMMI SAPERE COSA PREFERISCI FARE, COSÌ MI ORGANIZZO



Questa frase, che appare all'interno di una email, va bene scritta così?

- Sì, perchè il messaggio è chiaro: il maiuscolo permette di capire bene qual è l'obiettivo
- No, perchè più che un favore sembra un'imposizione

◊ *Il problema in questo caso non è il contenuto in sé, che è chiaro, ma il modo in cui viene veicolato. Il maiuscolo è da evitare perchè sembra che il messaggio venga urlato, e non detto, all'interlocutore*

Esempio 5: Le idee si possono discutere, le persone si devono rispettare

Capita a tutti di non essere d'accordo con qualcuno. A voi quando è capitato l'ultima volta? Stavate discutendo di persona oppure via chat? Quali sono state le vostre reazioni?

◊ *Lasciare che gli studenti raccontino le loro esperienze. Può essere utile evocare una discussione recente avvenuta in classe. Per stimolare le risposte, dovrebbero emergere le seguenti domande:*

- Ti è mai capitato di insultare qualcuno in rete? E di persona? Cosa gli/le hai detto?
- Quando discuti con qualcuno, ascolti/leggi attentamente quello che dice/scrive?
- Prima di rispondere, pensi bene alle parole che vuoi usare?
- Ti è mai capitato di rimanere in silenzio perchè non avevi più nulla da dire?

Attività 2 - Gruppo Regalo

- Materiale necessario: un foglio e una penna per ogni studente
- Obiettivo: rendere gli studenti consapevoli dell'importanza dell'uso delle parole sui social anche nell'esprimere idee diverse

Chiedere agli studenti di creare dei gruppi di 4 persone. I gruppi devono darsi un nome relativo al motivo per cui sono tutti insieme, esattamente come accadrebbe sui social, in questo caso la scelta del regalo di compleanno per il compagno o la compagna che fa gli anni (l'insegnante affida a ogni gruppo il nome, cercando possibilmente di scegliere una persona che conoscono poco).
Per esempio, un gruppo si chiamerà "Regalo Giulia", un altro "Regalo Marco" e così via. I membri di ogni gruppo scrivono su un foglio il primo regalo che viene in mente, con una regola: usare il foglio come se fosse lo schermo del cellulare ed esprimersi come farebbero in chat. In questo modo ogni foglio contiene i riquadri relativi al numero di messaggi che si scambieranno.

ATTIVITÀ CON LA CLASSE

MESSAGGIO 1. Ognuno scrive il regalo che farebbe
I membri del gruppo leggono ai compagni quello che hanno scritto. È probabile che siano state fatte scelte diverse: da questo momento in poi ognuno dovrà criticare la scelta degli altri e difendere la propria. Tutto esclusivamente "via chat", senza parlare (tranne quando leggono i messaggi ad alta voce, momento che viene stabilito dal docente)

MESSAGGIO 2. Ognuno critica le scelte degli altri.
I membri del gruppo leggono poi ai compagni quello che hanno scritto. Adesso devono rispondere alle critiche che sono state mosse.

MESSAGGIO 3. Ognuno risponde alle critiche difendendo la propria scelta.
Di nuovo vengono letti i messaggi e si risponde un'ultima volta. Ogni membro ha la possibilità di chiudere la conversazione come meglio crede - cercando un compromesso, rimanendo sulla sua posizione, chiedendo di risentirsi dopo qualche giorno...

MESSAGGIO 4. Ognuno prova a chiudere la conversazione

Alla fine dell'attività, l'insegnante chiede ai gruppi se sono riusciti a trovare il regalo, le loro impressioni sulla modalità con cui hanno interagito, e di rileggere i propri messaggi: sul telefonino avrebbero scritto le stesse cose? Quello che dovrebbe emergere è che in questa occasione hanno avuto più tempo per pensare a cosa scrivere, per difendere la propria idea, per esprimerla scegliendo bene le parole. I concetti sono gli stessi, sia su carta che via chat e possiamo sempre scegliere come usare le parole, anche quando i messaggi sono istantanei.

Modalità Didattica a Distanza
Anziché creare 4 gruppi distinti, è l'intero gruppo classe a formare il Gruppo Regalo, per esempio con il nome "Regalo Giulia".

- Nella Fase 1 ognuno scrive in chat il regalo che farebbe.
- Nella Fase 2 ognuno sceglie un'opzione diversa dalla propria e la critica apertamente via chat; nessuno parla, il compito è scrivere soltanto ascoltando le indicazioni dell'insegnante.
- Nella Fase 3 chi è stato criticato risponde provando a difendere la sua scelta.
- Nella Fase 4 ognuno deve trovare un modo per chiudere la conversazione.

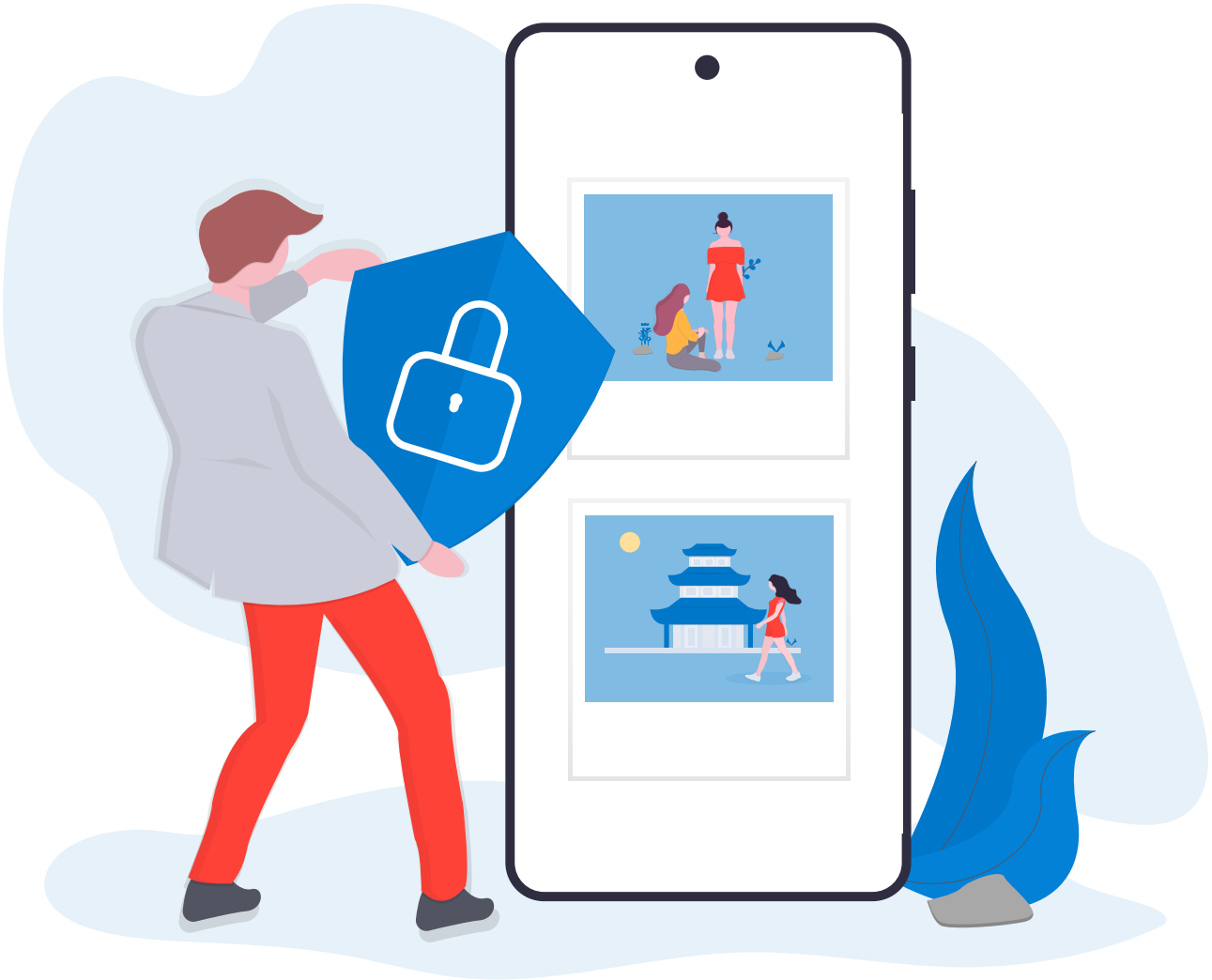
◊ In questo caso quello che dovrebbe emergere è che, essendo una situazione "monitorata" dall'insegnante, gli studenti hanno soppesato bene le parole. Sarebbe stato così se fossero stati da soli?

Together for Tomorrow!
Enabling People

CRESCERE CITTADINI DIGITALI

Guida all'insegnamento dell'Educazione Civica Digitale

Lezione 3
Sicurezza Digitale



SAMSUNG

Parola all'esperto: Riccardo Meggiato

Riccardo Meggiato è uno dei massimi esperti in sicurezza digitale, ethical hacking, investigazioni informatiche e digital forensics. Fondatore del laboratorio di informatica forense Meggiatolab, co-fondatore di una startup nel campo dei software di ricerca medica, e di una software house specializzata nello sviluppo di videogame, ha all'attivo oltre trentacinque libri best-seller; scrive su testate quali Wired, Rolling Stone, Panorama, Corriere.it e GQ; è head of content di Rolling Stone Arcade e tiene conferenze in tutta Europa, parlando di sicurezza, futuro e tecnologie software. Non si fa mai mancare un paio di ore di studio al giorno e un'ora di palestra. Lavora sette giorni su sette e dorme quattro ore a notte, e questo spiega tutto.

L'oscuro potere di un clic

Sono le 4 del mattino, state dormendo profondamente e, di punto in bianco, suona il citofono. È la Polizia, che vi comunica che siete indagati per alcuni, grossi, reati informatici, tra cui il sabotaggio di una centrale energetica e diversi furti di carte di credito. Non avete fatto nulla di tutto questo, eppure vi trovate catapultati nel bel mezzo di un incubo molto peggiore di quello che vi stava rovinando il sonno solo pochi minuti prima.

Com'è potuto succedere?

Con un clic, ma per capire meglio questa storia occorre fare un salto indietro di una settimana.

Era un venerdì pomeriggio, stavate già pregustando l'imminente weekend di fronte al vostro notebook aziendale e, tra un documento e l'altro da controllare, ecco arrivare una e-mail dal vostro boss: vi chiede di dare priorità alla compilazione del modulo in allegato e che si aspetta tutto per le 17, prima della vostra uscita, anzi fuga, dall'ufficio. Tra l'essere sollevati per l'improvviso diversivo alla solita monotonia, e l'essere un po' arrabbiati per un'aggiunta che rischia di compromettere la vostra storica puntualità alla cena del venerdì, con gli amici del Fantacalcio, decidete di aprire il modulo, un banale foglio Excel, e mettervi subito al lavoro. Ok che vi portate sempre appresso il notebook, ma "il lavoro lo si lascia in ufficio": la vostra fidanzata, su questo, è stata chiara. In realtà ci sono pochissime voci da compilare e tutto sommato vi sentite quasi in colpa per aver inveito contro il boss.

Comunque, portate a termine il lavoro e, addirittura prima delle 17, lo inviate insieme a tutto il resto.

Spegnete il notebook, lo chiudete e riponete nello zaino, e mentre state per prendere la porta dell'ufficio arriva proprio il boss a salutarvi. Ricambiate e gli dite che avete mandato tutto, modulo compreso. Lui alza il sopracciglio e vi chiede a quale modulo vi riferite e a nulla valgono le spiegazioni successive. Pare proprio che lui quella e-mail non ve l'abbia mai mandata. Poco importa, ora è tempo di weekend, fate spallucce, superate il capo e via, verso il meritato riposo.

Ora, invece, è tempo del vostro incubo reale, perché siamo tornati a quella notte e a tutto quel che sta succedendo. A proposito, ci chiedevamo: cosa è successo? In realtà, una cosa molto semplice. Ricordate il modulo? Non ve l'aveva spedito il vostro boss, ma un cyber-criminale che, al suo interno, aveva nascosto un malware, cioè un software con fini malevoli capace di trasformare il notebook in un così detto "zombie". In pratica, un computer asservito al volere del criminale. Così, mentre voi lo utilizzavate per il vostro lavoro, il criminale lo usava per le sue attività illegali, senza che ve ne poteste accorgere. E una volta beccato, in realtà, gli investigatori sono risaliti al vostro PC.

Non si tratta di fantascienza: secondo un report di WatchGuard Technologies, nel secondo trimestre del 2020 il 70% degli attacchi informatici era basato sull'utilizzo di malware "zero day", cioè malware che sfruttano i punti deboli sconosciuti di computer e smartphone. E gli esiti sono quelli che abbiamo visto in questo esempio, ma la varietà di situazioni in cui si rischia di incappare è molto più estesa. Si va dal furto dal vostro conto a quello dal conto dell'azienda per cui lavorate, dal ritrovarsi invischiati in traffici di droga in cui non c'entrate nulla, al vedersi bloccato non solo il vostro notebook ma tutta la rete aziendale, con conseguente richiesta di riscatto da parte dei criminali per sbloccare tutto. E il punto di partenza potrebbe essere proprio l'apertura di un banale allegato, oppure un clic a un link, l'inserimento di certe informazioni in alcuni moduli online, o l'utilizzo di una rete Wi-Fi poco protetta. Le attività criminali nel mondo informatico, così come le tecniche per sferrarle, sono così varie che a elencarle ci girerebbe la testa. La buona notizia, però, è che per difendersi, e limitare o evitare i danni, non serve chissà quale fatica. Giusto alcune accortezze di base. Un po' come ricordarsi di chiudere a chiave la porta di casa quando si esce, mettere il lucchetto alla bici o nascondere il portafoglio in una tasca quando si passeggia. Perché, mai come ora, la criminalità digitale deve fare più paura di quella del mondo reale. In questo booklet, per fortuna, trovate ottimi suggerimenti per difendervi.

Riccardo Meggiato

Obiettivi formativi

- Sensibilizzare sulla quantità di dati che creiamo e sul valore che questi hanno.
- Approfondire il tema della sicurezza online, sia dal punto di vista della prevenzione (impostazioni smartphone, geolocalizzazione) che dei pericoli in cui si può incorrere (frode informatica, phishing, cyber-criminalità, ransomware, ecc.).
- Introdurre il tema dei pagamenti digitali (modalità di pagamento, come avvengono, ecc.).

Indice lezione

Capitolo 1: Sicurezza dei device

I nostri dati sono ovunque

I nostri dispositivi sono pieni di informazioni che ci riguardano, dai dati anagrafici a quelli sulla nostra vita, su ciò che ci interessa e sulle nostre abitudini. Pensate a quante cose si possono scoprire di una persona semplicemente accedendo al suo smartphone:

- Accedendo alla posta elettronica si può risalire a tutti i documenti allegati che abbiamo inviato per e-mail almeno una volta, tra i quali ci potrebbero essere Carta d'Identità e tessera sanitaria, magari anche il contratto di lavoro, quello di affitto o di acquisto della nostra casa con l'indirizzo di residenza, il libretto universitario o il registro scolastico, solo per citarne alcuni.
- Accedendo ai social network si può risalire ai nostri interessi, luoghi che frequentiamo (presenti anche sul dispositivo se abbiamo attivato la geolocalizzazione), il network di amici e le nostre abitudini.
- Il dispositivo contiene le nostre foto, video e tutti i contatti della rubrica, che potrebbero diventare a loro volta vittime di frodi.
- Le applicazioni contengono informazioni come gli estremi delle nostre carte di credito e dei sistemi di pagamento che utilizziamo online, le password e tanto altro ancora.

Sono solo alcuni esempi di tutto quello a cui è possibile risalire sull'identità e sulla vita di una persona, semplicemente accedendo al suo dispositivo personale. Proteggere questi dati è importantissimo e dobbiamo abituarci a prestare particolare attenzione a questo aspetto del mondo digitale.

Mettere in sicurezza i dispositivi

Prima di parlare di come mettere in sicurezza i dati online, è bene ricordarsi che anche i dispositivi permettono di impostare delle procedure di sicurezza che aiutano a proteggere i nostri dati, sia quelli online che quelli salvati sui dispositivi (come fotografie, video e documenti).
Per esempio, i computer consentono di bloccare lo schermo con delle password e i dispositivi mobili di bloccare lo schermo con codici numerici, password, con delle sequenze (le così dette "gesture") o con l'impronta digitale.

Vediamo nel dettaglio come proteggere i nostri dispositivi mobili come smartphone e tablet:

1. **Proteggi i tuoi dati con un blocco schermo sicuro:**
   Imposta un PIN o una password complessi e difficili da indovinare, oppure usa un blocco biometrico, come l'impronta digitale.

2. **Nascondi le informazioni più importanti:**
   Attiva Area Personale, una "cassaforte" a cui si accede con password o impronta digitale in cui puoi salvare i file più importanti e le app più sensibili, come quella della banca.

3. **Registra l'impronta digitale:**
   Con l'impronta digitale puoi accedere rapidamente a siti e app senza inserire le credenziali.

4. **Rintraccia il tuo dispositivo:**
   Se perdi un telefono o un tablet è ormai possibile individuarlo, bloccarlo o resettarlo anche da remoto. Se si tratta di dispositivi Android in cui è stato aggiunto un Account Google al dispositivo, il servizio "Trova il mio dispositivo" è automaticamente attivo. Per verificare vai su Impostazioni > Sicurezza > Trova il mio dispositivo. Per i dispositivi iOS, invece, Apple mette a disposizione la funzione "Dov'è", attivabile in questo modo: Impostazioni > Account e password > iCloud > Dov'è.

Capitolo 2: Sicurezza online

La mole di dati generata online è impressionante e tutti noi abbiamo una grandissima quantità di informazioni personali in rete. È fondamentale, quindi, tenere al sicuro queste informazioni, attraverso alcune accortezze e l'utilizzo di un sistema efficace di password.

Le password

Prestare attenzione alle password che si utilizzano è importantissimo per proteggere i propri dati personali. Ecco alcune regole generali:

- Mai utilizzare la stessa password per più di un sito, meglio inventarsene una nuova per ogni sito e servizio a cui ci si iscrive.
- Utilizzare password complesse, di almeno 12 caratteri, contenenti lettere, numeri, maiuscole e, dove consentito, caratteri speciali, difficili da crackare.
- Sostituire periodicamente le password: alcune aziende, per esempio, le fanno cambiare a tutti i dipendenti ogni 75-90 giorni. In altre aziende ancora, gli IT manager provvedono a programmare cambi periodici automatici.
- Utilizzare un tool per gestire le password (password manager) e non rischiare di dimenticarle.
- Rafforzare la sicurezza della password, utilizzando le domande di sicurezza o la cosiddetta verifica in due passaggi, che include un codice numerico da inviare sul telefono per rendere più difficoltoso l'accesso all'account da un nuovo device.
- È anche buona norma ricordarsi di effettuare il log out dai siti che richiedono l'inserimento delle proprie credenziali, se si utilizza un dispositivo condiviso o che può essere raggiunto da altri.
- Non condividere mai e per nessuna ragione le proprie password: una persona fidata oggi, potrebbe diventare inaffidabile domani. E nel frattempo potremmo esserci scordati di quali password le abbiamo consegnato.

Antivirus

Per evitare di contrarre malware navigando su Internet, oppure aprendo e-mail che sembrano innocue, occorre avere sempre un antivirus aggiornato e in funzione sui propri device. Evitate, invece, di installarne due come consigliato anche da alcuni esperti: rischierebbero di andare in conflitto tra loro, perdendo entrambi di efficacia. Anche aggiornare i propri software e sistemi aiuta a mantenere i propri dati personali al sicuro.

La posta elettronica

La casella di posta elettronica è uno degli strumenti più utilizzati ogni giorno e uno degli aggregatori di dati personali più importanti. Nei nostri scambi di e-mail abbiamo dati bancari, documenti personali, estratti conto, risultati di esami e tutto ciò che riguarda la nostra vita. È indispensabile, quindi, porre in sicurezza le nostre caselle ed evitare di mettere in pericolo le informazioni che ci riguardano.

La prima cosa da fare per non correre rischi è evitare di aprire allegati sospetti o di cliccare su link contenuti nel corpo del messaggio, soprattutto se questo proviene da un mittente non attendibile.

In ogni caso, quando non si è sicuri dell'identità del mittente, meglio verificarla e, se si tratta di un nostro conoscente, contattarlo in altro modo per assicurarsi che il messaggio provenga dal suo indirizzo.

I profili social

Anche mantenere un discreto livello di privacy sui propri profili social è di certo un buon metodo per proteggere i propri dati. È importante selezionare bene i contatti, prestare attenzione a chi si aggiunge al proprio network, controllare e restringere la privacy di alcuni contenuti pubblicati, limitandone l'accesso ad amici o gruppi, e non pubblicare mai informazioni personali come numero di telefono o indirizzo e-mail.

Facebook e Instagram, per esempio, offrono una serie di opzioni personalizzabili per modificare le impostazioni sulla privacy di ciascun profilo: prendersi cura di questo aspetto è molto importante. Inoltre, mantenere privati i contenuti del proprio profilo scoraggia i cyber-criminali dal rubare la nostra identità e le nostre foto.

Capitolo 3: Frode informatica

Frodi informatiche

Oltre a proteggere i nostri dispositivi, dobbiamo fare attenzione anche a quando navighiamo online: in rete, infatti, si può cadere vittime di malware, truffe e messaggi ingannevoli ed è quindi importante conoscere le principali tecniche che i malintenzionati usano per attaccare online.

Per aggirare antivirus e sistemi di sicurezza, sono state sviluppate delle tecniche per lo studio e la manipolazione dei comportamenti delle persone con lo scopo di raccogliere informazioni confidenziali. L'insieme di queste tecniche prende il nome di **"Ingegneria sociale"**.

I principali metodi che rientrano nell'ingegneria sociale sono:

- **Phishing:** consiste nell'ingannare la vittima a condividere i propri dati tramite l'invio di messaggi o e-mail ingannevoli
- **Vishing:** è la versione telefonica del phishing
- **Pretexting:** consiste nel fingere di essere entità considerate affidabili (banca, posta, pubbliche amministrazioni...) sfruttando dei dati sull'utente che già si conoscono (data di nascita, indirizzo di residenza...) per spingerlo a divulgare informazioni confidenziali
- **Baiting:** consiste nell'utilizzare un'esca (come una chiavetta USB, contenente un malware, che viene lasciata incustodita) per stimolare la curiosità della vittima e indurla a raccogliere l'oggetto, che una volta inserito in un PC diventerà un punto di accesso per i sistemi aziendali.

Queste tecniche sono particolarmente insidiose perché cercano di ingannarci, cercando di indurci a fidarci di chi ci sta contattando. Il phishing, in particolare, esiste ormai da molti anni ma rimane uno degli attacchi più efficaci. Vediamolo nel dettaglio.

Phishing

Parliamo di phishing (da «to fish», «pescare», perché la vittima viene «presa all'amo» dal truffatore) quando qualcuno cerca di rubarci l'identità o i dati per accedere ai nostri conti bancari, carta di credito o per altre operazioni criminali, e generalmente lo fa spacciandosi per qualcun altro. Un tipico messaggio di phishing arriva via e-mail e sembra provenire da una banca o da un'organizzazione conosciuta che, solitamente, segnala un grave problema tecnico da risolvere al più presto. Il messaggio generalmente chiederà di cliccare su un link, che conduce a un modulo dove inserire i nostri dati bancari o personali, induce a installare un malware, o addirittura a rispondere direttamente coi nostri dati, password o codici di accesso.

Qualunque messaggio che richieda l'inserimento di dati personali, password o codici di accesso, pena la cancellazione di un account o il blocco di un conto, va immediatamente segnalato e cestinato.

Ricordiamoci che le banche o le compagnie telefoniche non inviano mai una richiesta sollecita di inviare i nostri dati sensibili via posta elettronica.

I messaggi provenienti da mittenti sconosciuti e contenenti link sospetti e pulsanti che invitano a cliccare su dei link per compiere delle azioni, come "Verifica subito", "Vai al sito" ecc.; e anche gravi errori ortografici, sono probabilmente tentativi di phishing che vanno segnalati.

Inoltre, i messaggi di phishing contengono spesso errori grammaticali, a volte i loghi delle organizzazioni sono riprodotti male e invitano sempre a cliccare per risolvere il problema immediatamente, pena la chiusura o disattivazione del nostro account. Non è difficile riconoscerli, basta fare attenzione.

Come riconoscere i messaggi ingannevoli?

Le immagini di seguito contengono esempi di phishing via SMS e via e-mail:

Numero di telefono sconosciuto.

Il messaggio arriva da un numero di telefono che non abbiamo salvato in rubrica. Bisogna fare sempre molta attenzione ai messaggi che riceviamo da numeri sconosciuti.

Link sconosciuto.

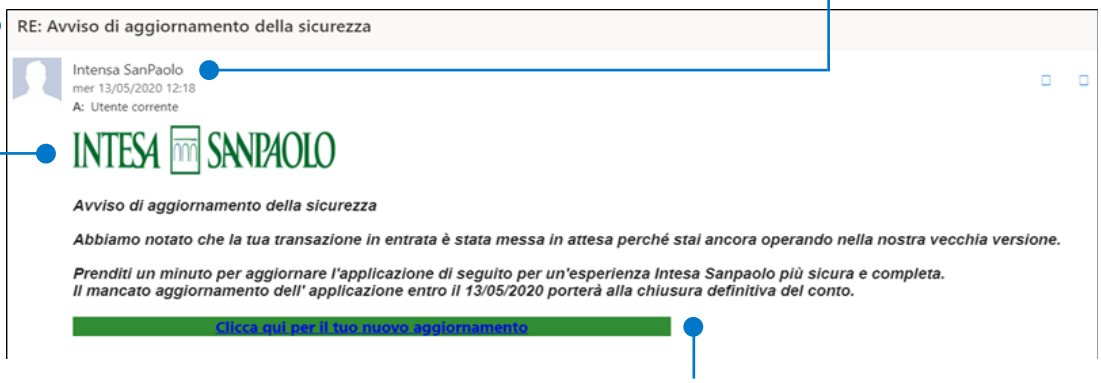
Il link non porta a nessun sito di banche o altre istituzioni note. Non bisogna mai cliccare su link sconosciuti perché potrebbero portare a pagine dannose.

Contenuto generico.

Nel messaggio non viene specificato chi è il mittente, né di che tipo di conto si tratta. Inoltre, non vengono dati dettagli sul motivo della presunta sospensione del conto.

Oggetto sospetto.
In questo caso, l'oggetto dell'e-mail è strutturato come risposta a un messaggio ("RE:"). Se non abbiamo inviato nessuna e-mail a questo mittente, il messaggio è falso.

Mittente sconosciuto.
Il mittente in questo caso appare come "Intensa SanPaolo", che non è il nome corretto della banca.



Logo non corretto.
Il logo non rispetta le proporzioni di quello reale della banca.

Canale non ufficiale.
L'e-mail suggerisce di cliccare sul link per aggiornare l'app: gli aggiornamenti avvengono sempre e solo attraverso gli store ufficiali, per cui questo link non è affidabile.

Per riconoscere le e-mail maligne, ci sono alcuni suggerimenti da ricordare:

1. **Verificare il mittente:** prima di aprire il messaggio, dobbiamo controllare da chi arriva e fare molta attenzione in caso di mittenti sconosciuti.
2. **Leggere l'oggetto:** se l'oggetto della e-mail non è chiaro, è molto generico, o è scritto in inglese, potrebbe trattarsi di una e-mail maligna.
3. **Non dare mai dati personali:** a volte l'indirizzo può sembrare affidabile, ma se vengono richiesti dei dati (password, numeri di carta di credito, ecc.), non bisogna mai fornirli. Nessuna banca o ente ufficiale raccoglie i dati via e-mail.
4. **Non scaricare gli allegati:** in caso di mittente sconosciuto, bisogna evitare di scaricare gli allegati. Se invece conosciamo il mittente, possiamo verificare con lui/lei che l'e-mail sia vera e l'allegato non pericoloso.
5. **Non aprire i link:** un link è un rimando ad un sito Internet e potrebbe portare a pagine web maligne. Prima di aprirli, è sempre meglio verificare con il mittente, se conosciuto, o non aprirli se il mittente è sconosciuto.
6. **"Capire" le e-mail:** una e-mail andrebbe sempre letta con attenzione. Richieste strane o non coerenti con un mittente che di solito adotta un altro stile o parla di altri contenuti potrebbero essere indicative di una e-mail truffaldina.
7. **Il trucco del reply:** le e-mail malevole, in genere, sono fatte per convincerci a cliccare su un link o scaricare un allegato, ma non per ricevere le nostre risposte. Così, se facciamo un reply a una e-mail sospetta, e riceviamo un errore di invio o ricezione perché l'indirizzo del destinatario sembra essere inesistente, potremmo avere la conferma di essere di fronte a una trappola digitale.

In generale, banche, poste, pubbliche amministrazioni ed entità simili comunicano sempre attraverso i loro canali ufficiali e non chiedono mai di inserire o confermare dati personali, password o numeri di carta di credito via e-mail o SMS. In caso di dubbi, è meglio contattare il presunto mittente del messaggio attraverso i canali ufficiali e verificare che la richiesta sia reale.

Le truffe si possono anche basare su finte vincite, con e-mail che parlano di premi o somme di denaro: queste e-mail vanno sempre ignorate e cancellate.

Capitolo 4: Pagamenti digitali

Per evitare di cadere vittime dei tentativi di frode appena visti è bene imparare come funzionano le transazioni e i pagamenti digitali, in modo da prendere confidenza coi vari metodi e riconoscere subito eventuali tentativi di frode.

I metodi di pagamento

Sono molti i metodi di pagamento riconosciuti e accettati in Italia, alcuni più tradizionali e in uso ormai da secoli, come il contante, e altri di più recente introduzione, come le carte di credito: queste ultime rientrano nella categoria dei cosiddetti "pagamenti digitali".

Per "pagamenti digitali" si intendono tutti quei pagamenti effettuati con strumenti di pagamento elettronici, come appunto le carte di credito. I pagamenti digitali offrono molti vantaggi rispetto alle forme di pagamento tradizionali: possono più facilmente essere tracciati, per esempio per motivi fiscali, possono essere bloccati in caso di furto e danno la possibilità di ottenere più facilmente rimborsi in caso di reso del prodotto o di truffe. Usando pagamenti digitali, inoltre, non dovremo preoccuparci di cambiare la valuta se andiamo all'estero, poiché il cambio è gestito automaticamente dal circuito di pagamento.

I "circuiti" sono società che gestiscono le richieste e le autorizzazioni di pagamento che avvengono in modalità elettronica, mettendo in comunicazione il POS (cioè il lettore delle carte di pagamento, presente ormai in tutti i negozi) con la banca o l'istituto che ha emesso la carta. Esempi di circuiti di pagamento tra i più diffusi sono Visa e MasterCard.

Tra le modalità di pagamento digitale rientrano:

- le carte di credito, debito o prepagate, che vengono utilizzate con i tradizionali POS oppure per gli acquisti online
- i pagamenti effettuati con lo smartphone, attraverso siti web, app e mobile wallet

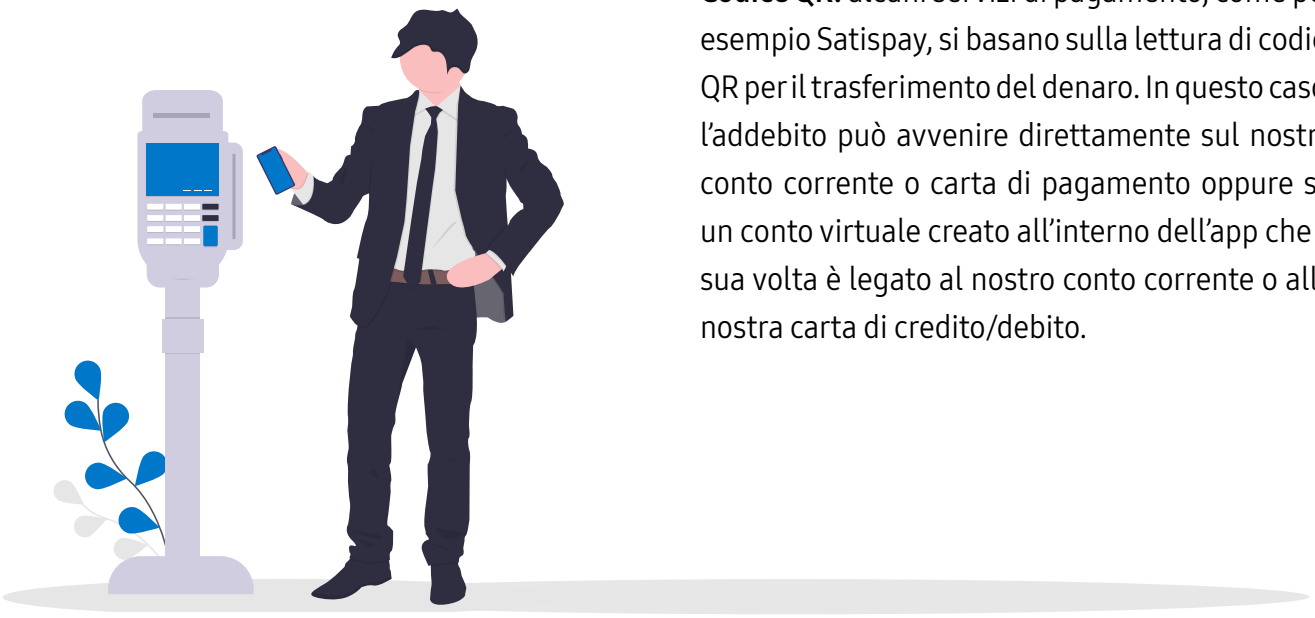
I *mobile wallet (o e-wallet)* sono portafogli digitali che vengono creati e gestiti sullo smartphone e possono contenere, oltre alle carte di pagamento, anche carte fedeltà, carte di imbarco, biglietti dei trasporti pubblici e molto altro.

Pagare con lo smartphone

Ci sono diverse modalità di pagamento con lo smartphone, che si raggruppano in:

- **Mobile Remote Payment:** sono tutti quei pagamenti digitali effettuati tramite lo smartphone da remoto, cioè non presso un punto vendita. Rientrano in questa categoria le transazioni eseguite attraverso app per lo shopping online, per i pagamenti di bollettini, ricariche telefoniche o biglietti dei trasporti pubblici.

- **Mobile Proximity Payment:** sono i pagamenti che avvengono presso un punto vendita e che sono effettuati con l'uso dello smartphone. Questa tipologia è sempre più diffusa come sostituto dei pagamenti tradizionali in contanti o con carte di pagamento fisiche. È una categoria molto vasta, che include modalità di pagamento basate su diverse tecnologie:



  - **NFC (Near-Field Communication):** è una tecnologia che consente lo scambio immediato e sicuro di dati da un dispositivo a un altro (nel caso dei pagamenti, dallo smartphone al POS) a una distanza molto ravvicinata. Su questa tecnologia si basano le app di pagamento più diffuse, come Samsung Pay, Apple Pay o Google Pay: queste app consentono di creare una "versione digitale" della nostra carta di pagamento sullo smartphone. Aprendo l'app, e avvicinando il telefono al POS, potremo concludere il pagamento proprio come si fa con le carte fisiche. Per verificare la nostra identità, queste app utilizzano un PIN oppure un metodo di riconoscimento biometrico, come le impronte digitali o il riconoscimento del viso. Le app di questo tipo addebitano il costo sulla carta di pagamento che abbiamo scelto di digitalizzare.

  - **Codice QR:** alcuni servizi di pagamento, come per esempio Satispay, si basano sulla lettura di codici QR per il trasferimento del denaro. In questo caso, l'addebito può avvenire direttamente sul nostro conto corrente o carta di pagamento oppure su un conto virtuale creato all'interno dell'app che a sua volta è legato al nostro conto corrente o alla nostra carta di credito/debito.

- **Peer-to-peer Payment:** spesso abbreviato in P2P, si tratta dello scambio di denaro tra privati. Ci sono molte soluzioni che consentono di trasferire soldi ai nostri amici in modalità digitale, gratuitamente e in tempo reale. Alcune di queste app si appoggiano direttamente al conto corrente, mentre altre consentono di creare un conto virtuale prepagato che possiamo ricaricare quando necessario, ma hanno tutte in comune un'estrema semplicità di utilizzo: ci basterà infatti avere il numero di telefono o l'indirizzo e-mail della persona a cui vogliamo inviare il denaro per completare il trasferimento. Alcune delle app più diffuse che offrono questa funzionalità sono PayPal, Circle, Jiffy e Satispay e sono molto utili, per esempio, per dividere un conto al ristorante o per raccogliere quote per un regalo di gruppo.

Sicurezza nei pagamenti digitali

Esiste una normativa europea che regola i pagamenti digitali e garantisce che tutte le app e le piattaforme che offrono servizi di pagamento seguano dei criteri molto rigidi di sicurezza. Questa normativa, entrata in vigore nel Gennaio 2018, si chiama Payment Services Directive 2 (Direttiva dei Sistemi di Pagamento 2) o PSD2 e sostituisce la precedente PSD del 2007.

La principale novità introdotta nell'ambito della sicurezza riguarda l'obbligo di adottare nuovi e più sicuri sistemi di autenticazione basati sulla Strong Customer Authentication (Autenticazione forte del cliente o SCA). Questo sistema serve a identificarci in modo univoco quando utilizziamo i pagamenti digitali, per evitare che altre persone possano utilizzarli a nostro nome o a nostra insaputa.
In caso di transazioni non autorizzate, poi, è possibile chiedere un rimborso al circuito di pagamento che, se verificherà un uso illecito della nostra carta, ci potrà restituire la somma addebitata. Possiamo facilmente tenere sotto controllo le transazioni abilitando i messaggi di notifica: questo servizio ci invia un SMS, un'e-mail oppure una notifica via app ogni volta che utilizziamo i nostri mezzi di pagamento digitali, permettendoci di avere sempre le spese sotto controllo ed essere informati tempestivamente in caso di spese non autorizzate. Le carte, inoltre, possono facilmente essere bloccate in qualunque momento, telefonando alla nostra banca.

Se dovessimo invece perdere lo smartphone, o ci venisse rubato, è possibile bloccarlo e cancellare da remoto i nostri dati grazie ai servizi di localizzazione dei dispositivi (come Find my mobile o Find my iPhone): in questo modo, nessun altro potrà usare i nostri strumenti di pagamento digitale dal nostro smartphone.
Queste operazioni non sono invece possibili per i contanti, che non possono in alcun modo essere bloccati o rintracciati.

Dove si può pagare con gli strumenti digitali?

È possibile utilizzare le carte di pagamento fisiche presso tutte le attività commerciali che sono dotate di POS, cioè lo strumento necessario per leggere le carte. Nel caso in cui il POS sia abilitato al pagamento *contactless* (cioè appoggiando la carta al lettore) è anche possibile pagare attraverso le app basate su tecnologia NFC che digitalizzano le nostre carte di pagamento (Samsung Pay, Apple Pay, Google Pay, ecc.).

Già dal 2014, in tutta Italia, è obbligatorio per negozi, ristoranti, hotel e tutte le attività commerciali dotarsi di POS, anche se non tutti si sono adeguati. I POS, comunque, soprattutto quelli contactless, sono ormai molto diffusi e questo ci permette di utilizzare i nostri strumenti di pagamento digitali quasi ovunque.

Accettare pagamenti non basati sulle carte di credito o debito (per esempio Satispay) è invece una scelta dell'esercente, ma molti stanno adeguando anche a questi metodi.
In alcuni casi è addirittura obbligatorio usare pagamenti digitali: per pagamenti superiori a 2.000€, infatti, dal 1 luglio 2020 è vietato utilizzare i contanti.

ATTIVITÀ CON LA CLASSE

Attività 1 - Oggetti dimenticati

- Materiale necessario: connessione a Internet, possibilità di proiettare
- Obiettivo: rendere gli studenti consapevoli dell'importanza di tutelare i propri dati

Vengono proiettate le immagini di oggetti e luoghi che trent'anni fa erano utilizzati per le stesse azioni di oggi (un walkman, un telefono a cornetta, una cartina geografica, una console Nintendo, una macchina Polaroid, una cabina telefonica, una macchina da scrivere, una cinepresa, un videoregistratore, uno stereo portatile...).
Gli oggetti sono disponibili su www.conservethesound.de

- Viene chiesto agli studenti di individuare gli oggetti che trent'anni fa permettevano di compiere determinate azioni: per esempio, con quale di questi oggetti si ascoltava la musica? Come ci si orientava per strada? Con cosa si giocava? Probabilmente non riconosceranno gran parte degli oggetti. L'attività permette di spiegare che fino a non molto tempo fa molte azioni erano delegate a oggetti singoli analogici, mentre oggi vengono racchiuse tutte in formato digitale all'interno di un unico oggetto, il telefonino.
- Ma cosa sarebbe successo trent'anni fa se avessi perso il walkman, il Nintendo o la cartina geografica? Si perdeva solamente un oggetto, mentre oggi si perde qualcosa di molto più prezioso: i nostri dati. Accade per esempio se rubano il mio account Spotify o Netflix, o quello della Playstation. Oppure posso condividere informazioni sui miei spostamenti mentre uso Google Maps, se è impostata la geolocalizzazione.
- Un account è l'insieme di dati identificativi di un utente che gli/le consentono l'accesso a un servizio telematico. Viene chiesto agli studenti quali dati andrebbero persi se venissero rubati gli account digitali di Netflix, Spotify, o altre applicazioni che permettono di compiere le azioni descritte nel primo esercizio. Si scoprirà che potrebbero essere messi a rischio la casella email, il profilo Facebook con contatti e informazioni personali, fino ai dati di pagamento della carta di credito associata all'account. Anche il furto di un account Playstation potrebbe permettere al ladro di accedere al profilo personale dell'utente per poterlo gestire a proprio piacimento, effettuando il download di giochi con la carta di credito a esso collegata.
- Poiché i dispositivi tecnologici di oggi non sono semplici oggetti ma racchiudono in un certo senso la nostra vita, è importante proteggere i propri dati e prendere provvedimenti per impedire l'accesso di utenti indesiderati. Una buona pratica è uscire dal proprio account sui tutti i dispositivi che non vengono solitamente utilizzati. Il sistema del Centro Assistenza invia solitamente un'email ogni volta che rileva un accesso sospetto da un nuovo dispositivo: se non riconosci l'accesso, cambia subito la password.

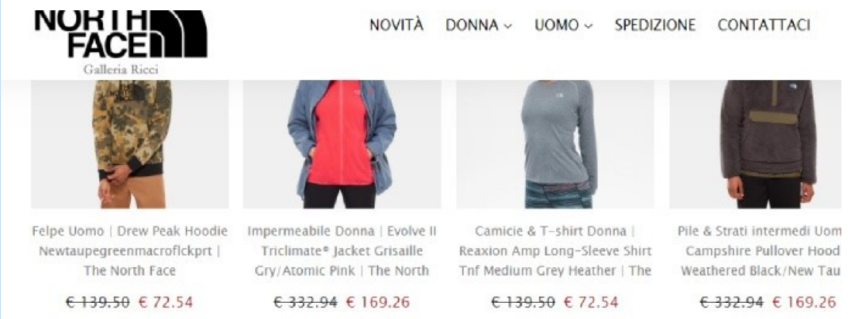
ATTIVITÀ CON LA CLASSE

Attività 2 - Non ci casco!

- Materiale necessario: possibilità di proiettare
- Obiettivo: fornire agli studenti strumenti su come riconoscere truffe online

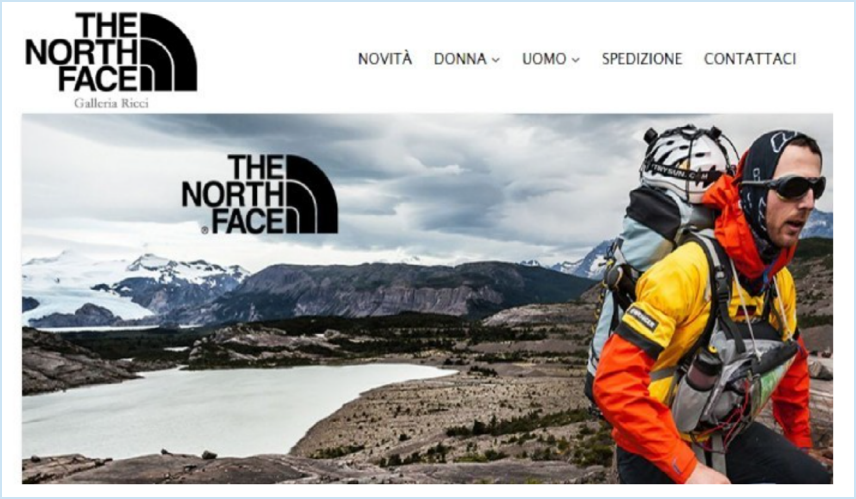
Esistono purtroppo molte notizie riguardanti falsi negozi online, che rubano i soldi dei clienti e spariscono nel nulla dopo averli attirati con recensioni false e annunci pubblicitari offrendo prezzi stracciati (anche del 60% rispetto al prezzo originale di listino). Di solito il sito truffa è costruito bene ed è spesso molto simile a quello originale. Per questo è facile caderci!

Ma come si fa a capire se un sito è una truffa?
L'insegnante proietta un esempio di sito truffa www.galleriaricci.it (senza svelare che si tratta di un fake) chiedendo agli studenti di osservare se c'è qualcosa che non quadra e se acquisterebbero o meno dal sito.



Il sito presenta capi d'abbigliamento costosi a prezzi veramente bassi. Inoltre il protocollo HTTPS nella URL è assente. Ma non finisce qui...ci sono altre differenze!

Consiglio n°1: controlla il dominio e diffida dei siti che propongono prodotti costosi a prezzi stracciatissimi

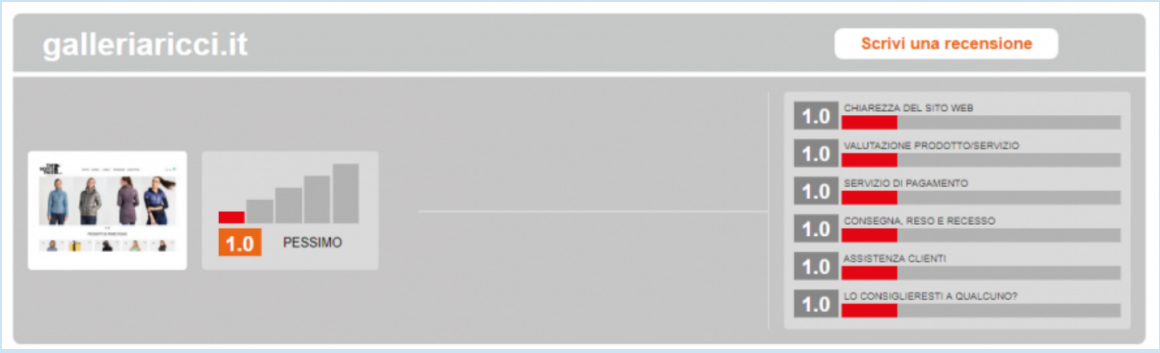


Il negozio online fasullo presenta il nome di un brand insieme al nome di una galleria d'arte moderna... ma vende capi d'abbigliamento!

Consiglio n°2: verifica nome del sito e corrispondenza dei prodotti

ATTIVITÀ CON LA CLASSE

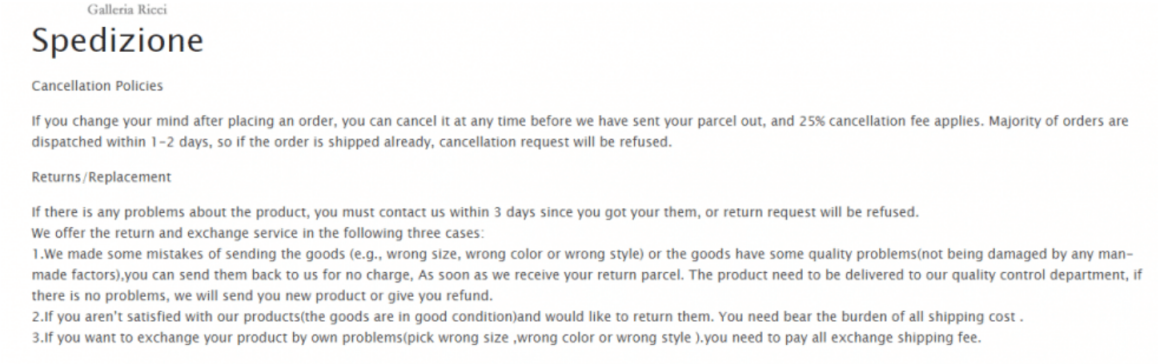
Osserviamo adesso la seguente tabella: cosa notate?



Consiglio n° 3: leggi sempre le recensioni sul negozio
Questa è la cosa più semplice: spesso i siti truffa sono pressoché sconosciuti (se non fosse per gli annunci online), quindi mancano le recensioni oppure sono poche e pessime.

Consiglio n° 4: verifica sempre che sul sito sia presente una partita IVA reale
I siti truffa scrivono spesso sul sito una partita IVA inventata o appartenente ad un'altra azienda. Ma come scoprirlo? Basta verificarlo sul sito ufficiale dell'**Agenzia delle Entrate:**
https://telematici.agenziaentrate.gov.it/VerificaPIVA/Scegli.do?parameter=verificaPiva

Per l'ultimo consiglio, leggiamo cosa ci dice la pagina dedicata alle policy di spedizione...


Galleria Ricci

Spedizione

Cancellation Policies

If you change your mind after placing an order, you can cancel it at any time before we have sent your parcel out, and 25% cancellation fee applies. Majority of orders are dispatched within 1~2 days, so if the order is shipped already, cancellation request will be refused.

Returns/Replacement

If there is any problems about the product, you must contact us within 3 days since you got your them, or return request will be refused.
We offer the return and exchange service in the following three cases:
1.We made some mistakes of sending the goods (e.g., wrong size, wrong color or wrong style) or the goods have some quality problems(not being damaged by any man-made factors),you can send them back to us for no charge, As soon as we receive your return parcel. The product need to be delivered to our quality control department, if there is no problems, we will send you new product or give you refund.
2.If you aren't satisfied with our products(the goods are in good condition)and would like to return them. You need bear the burden of all shipping cost .
3.If you want to exchange your product by own problems(pick wrong size ,wrong color or wrong style).you need to pay all exchange shipping fee.

Il titolo è in italiano e la descrizione in inglese!

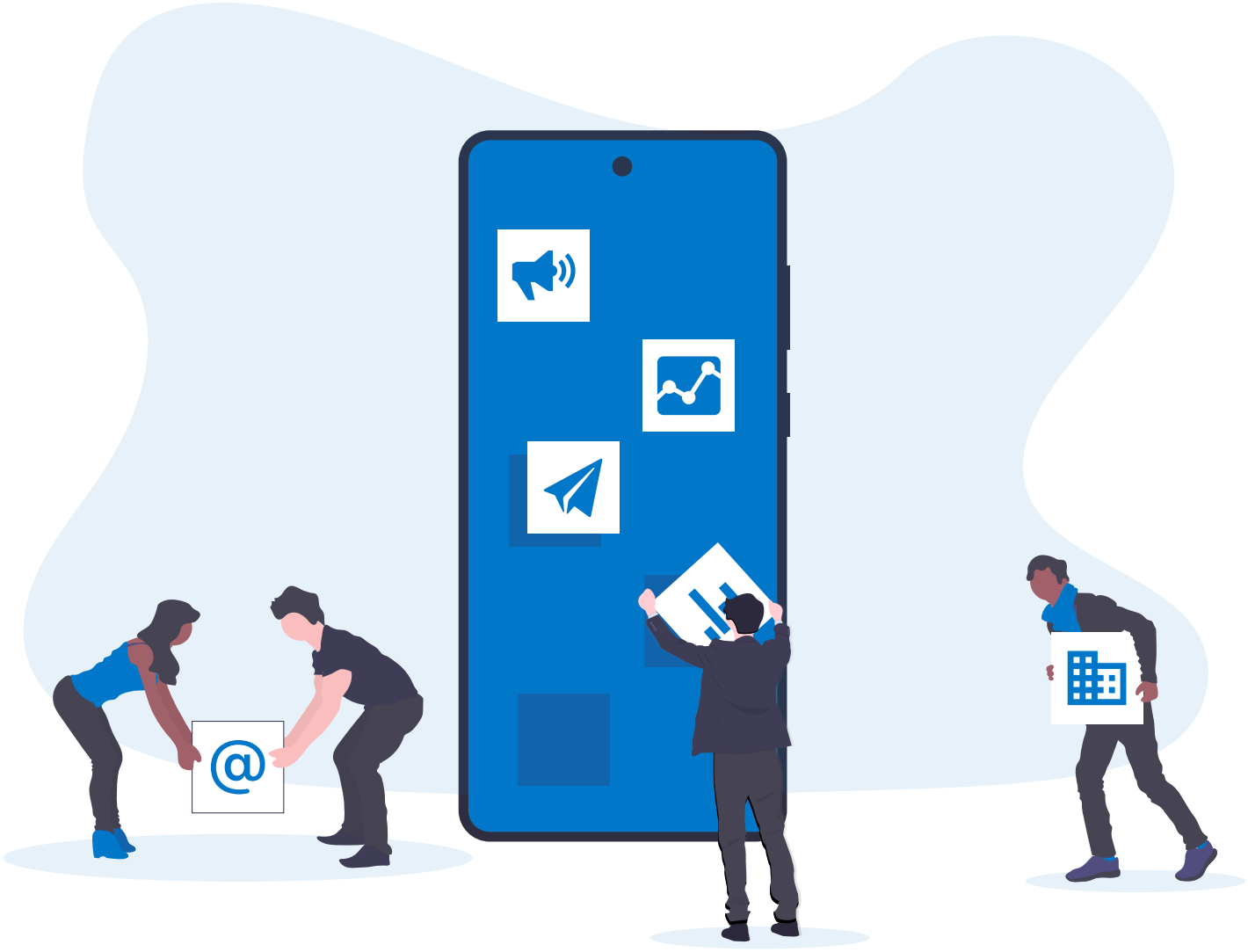
Consiglio n° 5: verifica che la grammatica dei contenuti sia corretta
In generale controllare se i testi presentano errori grammaticali o se sono tradotti solo in parte.

Together for Tomorrow!
Enabling People

CRESCERE CITTADINI DIGITALI

Guida all'insegnamento dell'Educazione Civica Digitale

Lezione 4
Contenuti Digitali



SAMSUNG

Parola all'esperto: Michelangelo Coltelli

Nato nel 1972, si è occupato di web come consulente informatico fin dai primi anni di Internet. Dal 1993 fino ai primi anni 2000 ha insegnato a privati l'uso della rete e realizzato siti per piccole aziende, trasformando quella che era una passione in un lavoro. Nel 2012, Michelangelo è tornato in rete aprendo quella che poi è diventato BUTAC. Un blog che si occupa di corretta informazione. In questi ultimi 8 anni è stato anche consulente per la Camera dei deputati nel progetto Basta Bufale, consulente della Federazione Nazionale degli Ordini dei Medici, Chirurghi e Odontoiatri. Inoltre, Michelangelo ha collaborato col CICAP, di cui è socio da diversi anni.

Orientarsi in rete

Imparare a districarsi nel web è diventata una delle doti di maggiore importanza nella società attuale. Quasi tutto è diventato accessibile via internet, e sulla rete transita la maggior parte delle informazioni che solo in un secondo tempo raggiungono gli utenti tramite altri media. La tv, la radio, la carta stampata, sono sempre un passo indietro rispetto alla velocità con cui le informazioni si diffondono tramite la rete.
Internet sta lentamente diventando il luogo dove è obbligatorio esserci. L'agenzia delle entrate, l'INPS, i comuni, tutti vogliono che noi usiamo la Rete per tutte quelle cose burocratiche che online possono essere semplificate.
A parte singole iniziative, fino ad oggi non era mai esistito nel piano studi nazionali un vero approccio alla rete web che metta in guardia dai pericoli nascosti di cui internet negli ultimi anni si è riempita. E ai docenti che dovrebbero insegnare questi concetti non era mai stato dato il "manuale delle istruzioni" per farlo: è in questo vuoto che si inserisce il progetto come quello che avete in mano.

La rete, le echo chamber e i pregiudizi

Le bufale, o Fake News come le vogliamo chiamare oggi, esistono da sempre. Non sono un problema nato con Internet, anzi, i primi anni della rete chi la usava erano per lo più accademici e studiosi, molto attenti a come la stessa veniva usata. Il problema è stato quando il grande pubblico è arrivato e ha cominciato ad usarla e abusarne sempre di più. Prima

con i sistemi di messaggistica, poi con i veri e propri social network. Un piccolo appunto che ritengo importante fare: i social network sono tutti quei luoghi dove è possibile aggregare più persone. Quindi non solo Facebook, Instagram, Twitter o TikTok ma anche Whatsapp, Telegram e tutti quei servizi di messaggistica che ci permettono di comunicare con più persone nello stesso momento. Le reti sociali purtroppo ci hanno ingabbiato in quelle che sono definite echo chamber, come succede anche nella vita al di fuori della rete.

Se siamo tifosi di una squadra di calcio è ovvio che cercheremo informazioni su di essa, se siamo appassionati di medioevo cercheremo informazioni su quel periodo storico, facilmente anche le persone che frequentiamo sono collegate in qualche modo ai nostri interessi e passioni. Sui social succede lo stesso, ci iscriviamo a gruppi e pagine seguendo lo stesso percorso. Il problema è che dal vivo le contaminazioni avvengono più facilmente. Online, invece, a dirigere tutto ci sono algoritmi, che in base a quelle che sono le nostre preferenze ci mostreranno sempre soggetti e gruppi che siano in qualche modo collegati. Questo, invece che ampliare il nostro orizzonte della conoscenza, lo limita. Ci chiudiamo a riccio all'interno di gruppi dove tutti la pensano più o meno come noi. Ci diamo ragione a vicenda. E questo è terreno fertile perché un certo tipo di disinformazione attecchisca e diventi virale.

Information disorder

Ci siamo abituati (e anche in questo manuale lo usiamo) a leggere spesso il termine Fake News: è immediato, identifica subito di cosa stiamo parlando. Ma non basta. Secondo l'Unione Europa e uno studio del 2017 il termine è diventato riduttivo. Oggi si parla di infodemia, ma il termine corretto per identificare il problema attuale è Information Disorder, Disturbo dell'Informazione. Quasi una malattia. L'ecosistema dell'informazione capillare è malato, e la malattia, il disturbo che lo affligge, ha una sola cura davvero funzionante: il nostro spirito critico.

Il termine Fake News è diventato riduttivo perché spesso i contenuti distorti a cui siamo esposti non sono neppure definibili falsi, manipolati magari, decontestualizzati, ma non falsi come invece il termine ci farebbe pensare. Per questo è importante approfondire, per questo è basilare verificare ogni informazione che leggiamo, prima di passarla a nostra volta ad altri a noi connessi.
La rete è disseminata di siti web che si spacciano per quello che non sono, influencer che diffondono informazione partigiana per portare acqua al proprio mulino. Districarsi in questo labirinto è davvero complesso.

Lo spirito critico

Purtroppo però in questo labirinto d'informazioni dobbiamo starci, quasi tutto ormai è più facile online. Dal verificare il saldo del proprio conto corrente al prenotare un volo per le nostre vacanze. Ma per poter navigare la Rete in sicurezza è fondamentale aver imparato a distinguere ciò che è rilevante e affidabile da ciò che invece può creare confusione. Affinare il proprio spirito critico per saper effettuare questa scelta è difficile senza l'aiuto di chi conosce questi meccanismi, ed è per questo che un manuale come quello che avete in mano diventa fondamentale. Imparare a riconoscere i nostri limiti, rendersi conto che tutti, ma proprio tutti siamo vittima dei nostri stessi pregiudizi è importante per saper distinguere tra fonti più o meno affidabili.

Troppe informazioni in troppo poco tempo

L'utente, grazie alla rete, è raggiunto da un quantitativo di informazioni impressionante (quell'infodemia di cui parlavamo poco sopra). Prima dell'avvento di Internet al massimo si leggeva un quotidiano, si guardava un telegiornale. Oggi l'informazione ci arriva 24 ore su 24, ovunque ci troviamo siamo in grado

di accedervi senza attendere che una redazione abbia masticato quei contenuti e li abbia resi fruibili a tutti, facendo una prima scrematura tra quanto fosse rilevante e quanto invece non lo fosse.

Nel 2015 Umberto Eco si pronunciò così:
"La tv aveva promosso lo scemo del villaggio rispetto al quale lo spettatore si sentiva superiore. Il dramma di Internet è che ha promosso lo scemo del villaggio a portatore di verità... I giornali dovrebbero dedicare almeno due pagine all'analisi critica dei siti, così come i professori dovrebbero insegnare ai ragazzi a utilizzare i siti per fare i temi. Saper copiare è una virtù ma bisogna paragonare le informazioni per capire se sono attendibili o meno."

Quell'analisi critica sui giornali non c'è, ed oggi purtroppo è diventato fondamentale invece farla. Oggi le stesse redazioni che un tempo effettuavano quel minimo di selezione dell'informazione hanno, spesso, smesso del tutto di farlo. Anche per loro il quantitativo di informazioni da verificare è troppo ed è diventato ingestibile. Anche loro, per restare a galla, per non arrivare ultimi nella gara a chi racconta la notizia, hanno smesso di verificare tante delle informazioni che poi passano al lettore. Mal che vada, quando sono colti in fallo, cancellano dai loro siti la notizia sbagliata. Questo purtroppo genera ancora più confusione nel lettore finale, che magari legge la notizia errata, la ricerca quando si rende conto che c'era qualcosa che non andava e invece che trovarne smentita non la trova più.
Tutto questo contribuisce al Disturbo dell'Informazione di cui oggi i cittadini digitali sono vittime.

Michelangelo Coltelli

Referenze:

La Stampa: Umberto Eco – Con i social la parola a legioni d'imbecilli: https://www.lastampa.it/cultura/2015/06/11/news/umberto-eco-con-i-social-parola-a-legioni-di-imbecilli-1.35250428

Council of Europe: Information Disorder: https://www.coe.int/en/web/freedom-expression/information-disorder

FirstDraft: Understand the landscape of information disorder: https://firstdraftnews.org/training/information-disorder/

Obiettivi formativi

- Apprendere come riconoscere fonti e contenuti attendibili da quelli non, sensibilizzare sull'importanza di sviluppare senso critico verso quello che si trova online.

- Ragionare sul tema dell'Information Disorder e delle Fake News.

- Definire cos'è il copyright e come utilizzare i testi che si trovano online per lavori personali (ricerche, tesi, ecc.) e suggerire strumenti utili.

Indice lezione

Capitolo 1: Reputazione di siti e fonti

Un mare di informazioni

Internet ha indubbiamente cambiato il modo in cui le persone ricercano e reperiscono le informazioni di cui hanno bisogno, dalle notizie di attualità alle ricette di cucina, alle ricerche di storia. Secondo un rapporto dell'Autorità per le Garanzie nelle Comunicazioni italiana (AGCOM), oggi Internet è la principale fonte di informazione per più di un quarto della popolazione italiana, mentre le riviste e i quotidiani lo sono solamente per il 17%.
Grazie a Internet il mondo si è fatto più piccolo, per tutti quelli che hanno accesso alla rete oggi è possibile ricevere informazioni in tempo reale.

In rete si trova tutto e il contrario di tutto, perdersi è molto facile. Vanificare il vantaggio di uno strumento così potente però è facile. Sapere usare i motori di ricerca e poter distinguere tra siti più o meno affidabili è basilare per non perdersi. Internet, a differenza dei giornali e della televisione, favorisce il rapporto diretto fra fonti e pubblico, ma questo implica che la responsabilità di determinare l'affidabilità di un'informazione spetti direttamente all'utente, non alla testata o alla rete televisiva, che basano la propria attività su una reputazione che bene o male devono cercare di mantenere.

Navigare consapevolmente

Per essere effettivamente utile e vantaggioso ai lettori, il web deve essere "navigato" consapevolmente. Bisogna adottare un atteggiamento attivo e consapevole per poter definire la qualità delle informazioni che vengono reperite e per poter definire delle gerarchie tra le varie fonti.
Come ben sappiamo, l'immediatezza della comunicazione digitale porta continuamente a un proliferare di informazioni false o non verificate, condivise ugualmente da moltissime persone sulla scia dell'emotività. Istintivamente, infatti, tendiamo a fidarci più facilmente delle opinioni che confermano ciò in cui crediamo. Inoltre, per verificare la veridicità di una notizia ci vogliono tempo e competenze, e non tutti hanno sempre la possibilità e la voglia di farlo.
Pensiamo ad esempio a quante volte è stata smentita la morte già annunciata di un personaggio famoso o la falsa credenza che la terra sia piatta. In gergo giornalistico si parla di «bufale» o «fake news», notizie false, la cui circolazione spopola sui social, specialmente su Facebook, proprio a causa della tendenza degli utenti a condividere impulsivamente i contenuti, magari leggendo solo i titoli o affidandosi alle immagini, senza verificarne l'attendibilità.
Tuttavia, attraverso la rete è quasi sempre possibile effettuare delle verifiche per controllare l'attendibilità delle notizie e per svelare informazioni false o comunque non verificate.
Vediamo nel dettaglio come si presentano le "fake news" e quali sono i comportamenti che ci aiutano ad avere un atteggiamento critico e consapevole verso le informazioni che reperiamo online.

Capitolo 2: Information Disorder e Fake News

Secondo l'Enciclopedia Treccani con "fake news" si intendono *"informazioni in parte o del tutto non corrispondenti al vero, divulgate intenzionalmente (quando chi diffonde la notizia sa che è falsa) o inintenzionalmente (quando chi diffonde la notizia non si è accorto che è falsa) attraverso il Web, i media o le tecnologie digitali di comunicazione, e caratterizzate da un'apparente plausibilità, ovvero dal fatto che sono verosimili, sembrano quasi vere, a maggior ragione quando vengono create per alimentare delle aspettative dell'opinione pubblica o alcuni pregiudizi".*

Secondo uno studio del 2017 fatto su richiesta dell'Unione Europea oggi possiamo distinguere due macrocategorie di "fake news" che vanno a esplicitare le due definizioni "intenzionali e inintenzionali". Le due macrocategorie sono la *misinformation* ("misinformazione") e la *malinformation* ("malinformazione").

MISINFORMAZIONE: Notizie false o distorte, create in buonafede, ma che presentano comunque rischi per il lettore finale. In questa categoria ricadono ad esempio quegli articoli che ci raccontano di nuove scoperte scientifiche basandosi su un singolo studio magari neppure revisionato. Il giornalista, non essendo scienziato, si fida dell'agenzia che ha riportato la notizia, senza approfondire e passando così un'informazione incompleta al lettore finale.

MALINFORMAZIONE: Notizie false o distorte create in malafede. Partendo magari da un fondo di verità si sceglie di raccontare solo una parte della notizia, quella che meglio rappresenta i propri bias (pregiudizi). Questo fa si che l'informazione finale che arriva al lettore sia distorta in un modo tale da non rappresentare più la notizia iniziale. Questo tipo di disinformazione è molto pericolosa perché particolarmente difficile da riconoscere.

Si tratta quindi di notizie:

- in cui la verità che viene presentata è o distorta, o completamente assente;
- che vengono diffuse su canali digitali e social (Facebook, Twitter, quotidiani e riviste online, blog ecc.);
- che spesso si basano su desideri o pregiudizi comuni.

Un'altra caratteristica delle notizie false è che queste si diffondono molto più velocemente delle notizie vere e, soprattutto, raggiungono molte più persone. Una ricerca condotta dal MIT in collaborazione con Twitter e pubblicata sulla rivista Science nel 2018 ha infatti appurato che le falsità viaggiano più lontano, più velocemente, più in profondità e più ampiamente della verità in tutte le categorie di informazioni. Una notizia vera, per raggiungere 1500 utenti, impiega 60 ore. Una notizia falsa, per raggiungere lo stesso numero di utenti, ne impiega 19.

Le notizie false raggiungono circa il 35 per cento di persone in più rispetto alle notizie vere, e un aspetto interessante di questa analisi è che è stato appurato anche che le notizie false e le notizie vere vengono condivise in egual misura dagli algoritmi, i cosiddetti bot. Questo significa che a condividere maggiormente le notizie false sono solo le persone.

Le motivazioni che spingono gli utenti a condividere più facilmente notizie false sono principalmente due:

- l'impatto emotivo che suscitano queste notizie (che spesso confermano i nostri pregiudizi, in inglese *bias*)
- l'interesse per la novità.

Prendiamo per esempio il caso della diffusione del virus COVID-19: la quantità di notizie false sul tema sono tantissime. Dagli articoli che sostengono che il virus non esista, a quelli che propongono cure e rimedi di ogni tipo per sconfiggerlo. Non è difficile capire perché le persone si interessino a chi sostiene queste cose: piacerebbe a tutti che fosse sufficiente assumere tante vitamine per essere immuni al COVID-19, o che bastasse un po' di vino per prevenire il Coronavirus.

Le fake news, quindi, interessano di più delle notizie vere perché indirizzano le paure e i desideri delle persone e perché rappresentano delle novità, che vengono presentate come scoperte o informazioni dell'ultima ora.

Perché esistono?

I motivi che spingono persone e siti a creare notizie false o non verificate sono molteplici.
Uno dei principali è sicuramente legato al traffico che si genera su pagine e siti di questo tipo. Più traffico viene generato su una pagina web, più gli inserzionisti sono disposti a pagare gli spazi pubblicitari che acquistano sulle pagine di quel sito. Questo è il motivo per cui vengono create tante notizie false clamorose: la gente è attratta, legge e condivide tantissimo. Questo porta a un ritorno economico per il blog, il giornale o la rivista che ha pubblicato la notizia.
Un altro motivo riguarda la possibilità di influenzare le decisioni altrui. Basti pensare a quanto le notizie possono influenzare la nostra opinione su una persona, su un avvenimento o su un partito politico. E questo potrebbe avere delle conseguenze su come poi ci comportiamo, su chi riteniamo meritevole della nostra fiducia e su chi votiamo.
Ovviamente, c'è anche chi vuole trovare un modo facile per attirare l'attenzione, o chi ha come obiettivo preciso quello di mettere qualcuno in cattiva luce.

Per esempio, nel 2016, durante la campagna elettorale per le elezioni presidenziali americane, un gruppo di complottisti sostenne che alcune email dell'account di posta elettronica della responsabile della campagna elettore della candidata Hillary Clinton collegassero esponenti del partito democratico (rappresentato dalla Clinton) e alcuni ristoranti statunitensi a un presunto caso di traffico di esseri umani e abuso di minori.

Questa teoria del complotto, rinominata "Pizzagate", si è ampiamente diffusa sui più popolari social, siti e forum americani e ha raccolto un seguito sempre più diffuso, nonostante la notizia fosse stata screditata da indagini condotte da diverse testate giornalistiche. Secondo diversi sondaggi condotti durante le elezioni, il 17% degli elettori della Clinton credeva che la notizia fosse vera, così come il 46% degli elettori del suo rivale, Trump. Tra questi ultimi anche un uomo del Nord Carolina, che si è recato in una delle pizzerie citate dai complottisti e ha aperto il fuoco con un fucile, fortunatamente senza provocare feriti. Una Fake News che, oltre a mettere personaggi pubblici in cattiva luce, ha rischiato di avere conseguenze davvero drammatiche.

Alcuni esempi di Fake News

Proviamo ad analizzare un po'più nel dettaglio alcuni esempi di notizie false, per capire assieme come vengono costruite e come le immagini vengono spesso utilizzate in maniera fuorviante."

Il flash mob

15 marzo 2020

Meravigliosa Italia. Le splendide foto del flash mob con le luci dei cellulari puntate verso il cielo

In questo caso la foto è vera, ed è vero anche che il 15 marzo del 2020 si è tenuto un flash mob. Ma le luci che si vedono nella foto ovviamente non sono quelle dei cellulari puntati in alto durante l'evento. Si tratta invece di un'immagine satellitare, scattata dagli astronauti che si trovavano sulla Stazione Spaziale Internazionale nel 2015. Attraverso una ricerca per immagini si può risalire alle pubblicazioni originali della fotografia.

Venezia ghiacciata

6 dicembre 2016

Venezia ghiacciata per il freddo, prima volta nella storia!

Il 6 dicembre 2016 esce questa notizia, ma la foto è in realtà l'opera di un artista americano che ha unito alcune immagini di Venezia con quelle di un lago ghiacciato della Siberia. È stata diffusa associandole una notizia falsa per attirare i lettori e ottenere più clic.

Filippo di Edimburgo

"Filippo è morto", l'indiscrezione choc sul marito della Regina Elisabetta sconvolge il Regno Unito


PEOPLE | FAMIGLIE REALI

"Filippo è morto", l'indiscrezione choc sul marito della regina Elisabetta sconvolge il Regno Unito

26 marzo 2020

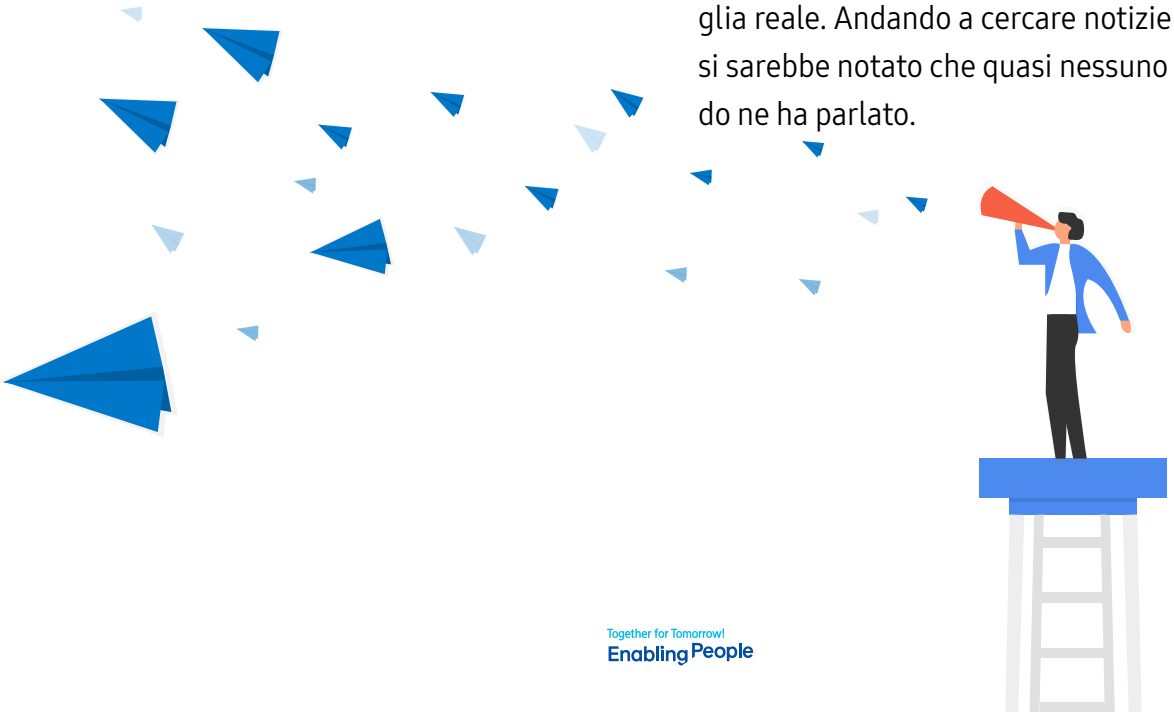
Condividi 13 1 0 7

La regina Elisabetta II e il principe consorte Filippo d'Edimburgo: fotostoria di un amore reale

Foto | Video

Il 26 marzo 2020 è uscita questa notizia sulla presunta morte del Principe Filippo, marito della Regina Elisabetta II.

Ma il Principe Filippo, sebbene 98enne, non è certo morto. Per capire se la notizia di cui si è parlato moltissimo sui media italiani nel mese di marzo era vera o falsa si poteva provare a cercare informazioni da fonti «più vicine» alla monarchia inglese, come gli organi di stampa ufficiali della famiglia reale. Andando a cercare notizie simili, infatti, si sarebbe notato che quasi nessuno in quel periodo ne ha parlato.



Come riconoscere le notizie false

Abbiamo visto in questi esempi alcuni suggerimenti per identificare notizie false, ma ci sono diversi metodi per riconoscere siti o articoli "sospetti". Quali sono?

Vediamo alcuni suggerimenti per imparare a riconoscere fonti, notizie e autori potenzialmente poco attendibili.

- **La fonte:** è importantissimo controllare il tipo di sito su cui è pubblicata la notizia ed eventualmente cercare riscontro in siti fidati come www.ansa.it, ww.corriere.it, www.repubblica.it, www.ilpost.it ecc. Controllando più testate è possibile effettuare delle verifiche incrociate, cercando di risalire alle modalità con cui si è diffusa un'informazione e ai soggetti che l'hanno accreditata. Spesso infatti le testate citano il quotidiano o la rivista che per prima ha dato la notizia. Se, per esempio, si tratta di una notizia sanitaria, il sito del Ministero della Salute sarà molto più affidabile del blog di un personaggio famoso. O se un articolo di Repubblica cita dei dati sulla diffusione delle tecnologie tra la popolazione italiana presi da un report dell'ISTAT, e questi dati sono leggermente diversi da quelli del report, dobbiamo essere in grado di identificare il report ISTAT come la fonte originale e primaria del dato, che può essere stato arrotondato o semplificato dal giornalista di Repubblica per rendere l'articolo più leggibile per il lettore.

- **URL:** l'url è la sequenza di caratteri che identifica univocamente l'indirizzo di una risorsa in Internet. È bene prestare attenzione a questo elemento perché eventuali errori di battitura e nomi "strani" possono essere indizi per identificare siti poco attendibili, soprattutto quando sono simili ad altri siti di informazione famosi e certificati, come «iNews24» o «DirettaNews, che non sono vere testate giornalistiche, ma hanno lo scopo di ingannare gli utenti con nomi simili a testate importanti per portare le persone a cliccare sui link solo per generare traffico.

- **L'autore:** si può verificare chi è attraverso una ricerca sul web. Se, per esempio, un autore sostiene di essere un professore universitario, il suo nome dovrebbe comparire sul sito dell'università. Se stiamo leggendo un articolo sull'inquinamento delle acque e scopriamo che l'autore scrive abitualmente su siti e riviste di settore e viene spesso citato da importanti testate giornalistiche probabilmente potremo dare un certo livello di attendibilità alle sue parole.

- **Il layout grafico:** solitamente siti e blog che propongono contenuti di alta qualità presentano anche una struttura e una grafica curate, senza errori di battitura. Un layout troppo semplice, testi ricchi di errori grammaticali, pagine piene di pubblicità e poca coerenza grafica sono segnali d'allarme.

- **I titoli delle notizie:** attenzione ai "titoli-esca", conosciuti anche come clickbait, che spingono a cliccare sul link promettendo grandi scoop (ma mai esplicitati nel titolo): servono solo a generare traffico. Titoli a effetto come «Non immaginerete mai cosa nasconde questa immagine!» sono esche: nel titolo non si svela nulla dell'articolo, semplicemente perché non c'è nessun contenuto. Anche banner come «Clicca qui per sapere come vincere un'automobile!» non sono affidabili: aprire link del genere può addirittura portare a scaricare un virus.

- **La ricerca inversa sui motori di ricerca:** dati e immagini possono sempre essere verificati cercando sui motori di ricerca. Per esempio, basta utilizzare la ricerca per immagini su Google caricando una foto per esaminare tutti i siti dov'è stata pubblicata. Attraverso questa ricerca è possibile anche risalire alle date di pubblicazione, utili per controllare se immagine e testo corrispondono (o se, per esempio, la stessa foto scattata durante un momento di protesta viene riutilizzata anni dopo per mostrare delle piazze più piene di quanto in realtà non fossero). Oltre alle immagini, la ricerca inversa permette anche di verificare se una citazione è stata presa dal suo contesto reale o se è stata estrapolata e inserita in un contesto diverso, assumendo quindi un significato differente.

- **La spunta blu degli account verificati:** sui profili social di personaggi e pagine verificate è presente una spunta blu che garantisce l'autenticità dell'account. Per capire se un autore o una fonte non nota sono attendibili si può provare a cercare il nome dell'autore o del sito sui vari social e verificare se hanno o meno la spunta (attenzione: non tutti ce l'hanno, non basta solo l'assenza della spunta a rendere un sito non affidabile).

Prestare attenzione a questi elementi aiuta a scovare le informazioni potenzialmente non veritiere e a fare delle verifiche per poter determinare se l'informazione è vera o falsa.

In generale, navigando sul web è bene mantenere un atteggiamento critico, ma è anche importante fidarsi dell'informazione quando questa è di qualità o proviene da fonti dirette (come un report pubblicato da un ente di ricerca, o un'intervista di un esperto).

Navigando in Internet è quindi importante:

- Farsi sempre delle domande
- Usare la testa, essere critici e fidarsi di quello che si è imparato e di quello che si sa di non sapere! Bisogna essere disposti a riconoscere quando non si sa qualcosa e a mettersi a cercare delle prove.
- Imparare a restare col dubbio di qualcosa: è meglio essere insicuri piuttosto che arrivare a conclusioni affrettate e iniziare a diffondere notizie non completamente verificate.

Ecco alcuni link utili per indagare notizie sospette:

Google Images permette, inserendo l'indirizzo URL di un'immagine o caricandola dal dispositivo, di fare una ricerca di foto simili e dei relativi siti di origine: www.google.it/imghp?hl=it

Foto Forensics è un sito che analizza le immagini e riconosce se sono presenti dei fotomontaggi: https://fotoforensics.com/

Factcheckers è una piattaforma interamente dedicata a come riconoscere le fake news: http://factcheckers.it/guida/

Capitolo 3: Il diritto d'autore (Copyright)

Se si deve fare una ricerca scolastica Internet è sicuramente un mezzo comodo e veloce per raccogliere informazioni. Ovviamente, Internet non contiene tutte le informazioni specifiche e dettagliate che può contenere per esempio una biblioteca universitaria, ma quasi sempre è possibile trovare quello che ci serve per svolgere una ricerca scolastica, o per organizzare l'itinerario di un bel viaggio.

Quando vogliamo utilizzare informazioni reperite in Internet, però, dobbiamo tenere presente che ci sono delle norme precise da rispettare in merito alla possibilità di riprodurre i contenuti che troviamo.
Anche le opere (testi, immagini, video, musica, audio, ecc.) che vengono pubblicate in Internet infatti godono del diritto d'autore, o copyright in inglese, ovvero quel diritto che tutela le creazioni di un artista e, in generale, qualunque opera d'ingegno, cioè opera originale.

Come funziona il copyright

Il diritto d'autore determina che tutte le opere sufficientemente nuove e originali appartengano a chi le ha create. Per la legge italiana e per quella di molti altri stati, quindi, in mancanza di altre indicazioni l'autore di un'opera ne è proprietario. Il diritto decade dopo 70 anni dalla morte dell'autore e, a quel punto, l'opera diventa di pubblico dominio. Per le fotografie, invece, il diritto decade dopo 20 anni dalla produzione della foto, a meno che non si tratti di un'immagine creativa. In quel caso, il diritto d'autore dura 70 anni come per i testi.

Attenzione a non farsi confondere dal simbolo del copyright: spesso immagini, loghi, testi ecc. presentano il simbolo © del copyright. Questo simbolo viene usato per indicare la presenza di copyright, ma, come abbiamo visto, non è assolutamente necessario per determinare che il contenuto in questione gode di protezione.

Che ci sia il simbolo o meno, immagini, testi e altri tipi di contenuti che si reperiscono online vanno utilizzati seguendo dei criteri. Per non rischiare di incorrere in violazioni del copyright è bene osservare alcune accortezze che ci permettono di utilizzare i materiali che reperiamo online in sicurezza e rispettando il lavoro altrui.

Vediamole assieme:

- **Riproduzione:** non è possibile copiare integralmente un articolo, né copiarne alcune parti senza specificare chi è l'autore di tali contenuti. Lo stesso vale per le immagini: è possibile riutilizzare solo le immagini che sono esplicitamente messe a disposizione del pubblico senza il permesso dell'autore. Lo stesso vale per le tracce musicali, i video ecc.

- **Citazioni:** se si desidera riportare un testo, si può fare nella forma della citazione, ovvero esplicitando che si tratta di un contenuto prodotto da qualcun altro, e indicando chi è l'autore e da dove proviene il brano. È bene evidenziare anche graficamente che si tratta di una citazione utilizzando le virgolette e il corsivo. Le citazioni vanno utilizzate comunque con parsimonia, e deve essere chiaro che il testo citato non ci appartiene. Le citazioni inoltre devono essere funzionali al nostro contenuto, vanno quindi intervallate con nostri commenti e osservazioni.

- **Fonti:** se si utilizza una citazione, è necessario sempre inserire la fonte da cui è stata estrapolata. Questo serve anche a contestualizzare le parole dell'autore: la stessa frase utilizzata in ambiti diversi può cambiare radicalmente di significato. Possiamo inserire le fonti anche per spiegare da dove provengono delle idee che magari noi abbiamo rielaborato, in modo da esplicitare che si tratta di un concetto preso da quel determinato autore o da quella determinata opera.

- **Link:** se si sta svolgendo un lavoro online, è possibile anche linkare pagine o fonti. In questo caso possiamo agire liberamente: se linkiamo un articolo perché secondo noi è interessante per l'argomento che stiamo trattando possiamo tranquillamente farlo. L'importante è non riportare sul nostro sito i contenuti che abbiamo trovato, "copiandoli" dal sito originale. Questo è molto importante quando si lavora online: indicare autore e fonte non ci permette di riportare interamente le opere degli altri. Se vogliamo riportare un articolo bisogna usare dei link esterni, non copiarne il contenuto.

Creative Commons

Se un autore vuole rendere il proprio materiale liberamente utilizzabile o modificabile da parte del pubblico senza che quest'ultimo rischi di violare il diritto d'autore può decidere di attribuire alla propria opera una delle varie licenze Creative Commons.

Queste licenze d'uso, in base alla tipologia di licenza, permettono da parte del pubblico diverse tipologie di utilizzo delle opere. Eccone alcune:

- riproduzione libera dell'opera per qualsiasi fini
- riproduzione libera dell'opera per fini non commerciali
- riproduzione dell'opera purché se ne citi l'autore
- riproduzione e modifica dell'opera (che quindi può essere liberamente alterata)

Le opere coperte da queste licenze solitamente presentano questo logo:

Esistono alcuni siti che propongono contenuti protetti da queste licenze e facilmente utilizzabili dal pubblico. Eccone alcuni:

Foto e video

- www.unsplash.com
- www.pexels.com
- www.pixabay.com
- www.stockfootageforfree.com
- www.freepd.com

Musica

- www.freemusicarchive.org

Attenzione: per essere sicuri delle modalità con cui si possono utilizzare questi materiali è bene sempre verificare il tipo di licenza su ciascun sito.

Per riassumere

Se stiamo svolgendo una ricerca per la scuola e abbiamo deciso di utilizzare Internet come mezzo per reperire informazioni dobbiamo ricordarci di seguire alcuni passaggi.

Dopo aver identificato un'opera, quindi un'immagine che vogliamo inserire nella nostra presentazione o un testo che spiega bene un concetto che vogliamo esporre, dobbiamo procedere ponendoci alcune domande che ci aiutano a capire se e come possiamo utilizzare l'opera.

Possiamo utilizzare liberamente l'opera se:

1. Si tratta di un'opera di pubblico dominio, quindi un'opera i cui diritti d'autore sono scaduti (creata più di 70 anni fa se si tratta di un testo o di un'immagine creativa e 20 anni se si tratta di una semplice fotografia)
2. Si tratta di un'opera per cui la legge dispone che non ci sia il diritto d'autore (opere non d'ingegno)

Possiamo utilizzare l'opera seguendo delle condizioni particolari se:

1. Si intende utilizzare l'opera per fini che godono di eccezioni (per esempio i fini didattici)
2. L'opera detiene una licenza come le licenze Creative Commons o proviene da una piattaforma che definisce particolari condizioni di utilizzo

Se l'opera non rientra in nessuno dei casi precedenti, non siamo autorizzati a riprodurre l'opera se non facendone espressa richiesta all'autore, che dovrà fornirci la licenza per l'utilizzo sulla base di un compenso.

ATTIVITÀ CON LA CLASSE

Attività 1 - Vero o falso?

Le fake news sono sempre esistite, si sono modificate nel tempo e con loro gli strumenti di diffusione. Gli studenti vengono sottoposti a un quiz con immagini e devono indovinare se corrispondono a notizie vere o false. Quali domande dovrebbero porsi? Quali strumenti possono utilizzare? Come si riconosce una fake news?

Attività 2 - Cos'è un copyright

- Materiale necessario: possibilità di proiettare, cassa da collegare allo schermo
- Obiettivo: rendere gli studenti consapevoli di cosa sia il diritto d'autore sul web

L'insegnante mostra alcune opere e chiede agli studenti se li utilizzerebbero (per esempio come citazione sui social, come colonna sonora di un video, come logo di un progetto...). In alcuni casi i contributi possono essere utilizzati, in altri no perché protetti da copyright. Viene introdotto il tema delle licenze "CREATIVE COMMONS" - tutte quelle composizioni scritte, prodotte e cedute da autori a patto di apparire nei crediti della produzione multimediale.

Opera d'arte

L'insegnate mostra questa immagine senza dire titolo e autore e chiede agli studenti se secondo loro è protetta da copyright o meno.

La Monna Lisa di Leonardo Da Vinci risale al 1503-1504, ma in questo caso si tratta dell'opera L.H.O.O.Q. di Marcel Duchamps del 1919. Sono trascorsi 101 anni dalla realizzazione, ma l'artista è morto solo nel 1968: l'opera sarà libera da diritti d'autore solo nel 2038.

Brani musicali

L'insegnante fa ascoltare agli studenti 3 diversi brani, chiedendo di riconoscere titolo/autore e capire se è una musica riutilizzabile o meno.

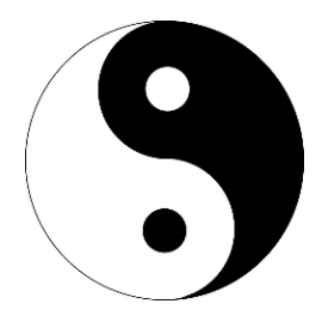
1. "Bella Storia" di Fedez. È una canzone del 2020, quindi coperta da copyright.
2. "We are the Champions" dei Queen. Brano scritto da Freddie Mercury nel 1977. Sono passati 43 anni dalla pubblicazione, ma Freddie Mercury è morto nel 1991: bisognerà aspettare altri 41 anni prima che il brano non sia più coperto da diritti.
3. "Sinfonia n.5", composta nel 1765 da Mozart, il quale è morto nel 1791. Brano libero da copyright.

ATTIVITÀ CON LA CLASSE

Logo
L'insegnate chiede agli studenti se potrebbero utilizzare questi due loghi per un progetto.

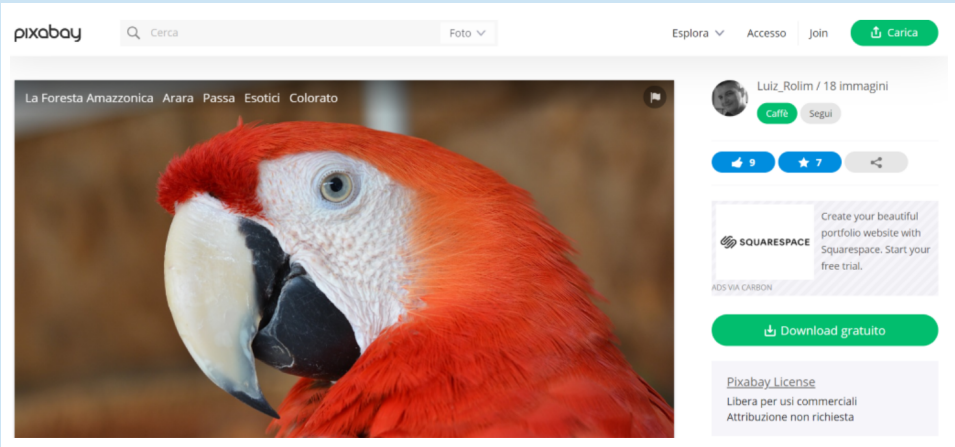
Nel primo caso la risposta dovrebbe essere no, trattandosi del logo della Nike ("Swoosh"), facilmente riconoscibile, nato nel 1971.

E questo simbolo?



Anche se lo vediamo rappresentato graficamente, lo Yin e Yang fa parte della cultura tradizionale e nella filosofia cinese e ha quindi origini molto antiche. Tutti possono usarlo, infatti lo ritroviamo praticamente ovunque.

Fotografia
Passiamo adesso a una fotografia. È possibile usare la seguente immagine all'interno di una ricerca sulla Foresta Amazzonica?



Viene mostrata questa immagine oppure una a scelta tratta dalla banca dati https://pixabay.com
Gli studenti possono riconoscere che è una immagine utilizzabile osservando il sito di provenienza e l'indicazione sulla licenza di utilizzo.

ATTIVITÀ CON LA CLASSE

Citazione di un testo

Infine, viene proposta agli studenti una citazione senza nominare l'autore - Gio Evan, scrittore, poeta e cantautore contemporaneo:

"Ogni volta che rispondi con delicatezza all'arroganza, stai insegnando al mondo la più grande delle rivoluzioni"

Il suo autore sarà ancora vivente? È un Instagram Poet, contemporaneo, quindi da citare sempre se vogliamo usare la sua frase sui social o in contesti commerciali.

E l'autore di questa frase? *"La vita non può essere scritta: la vita può essere soltanto vissuta"*

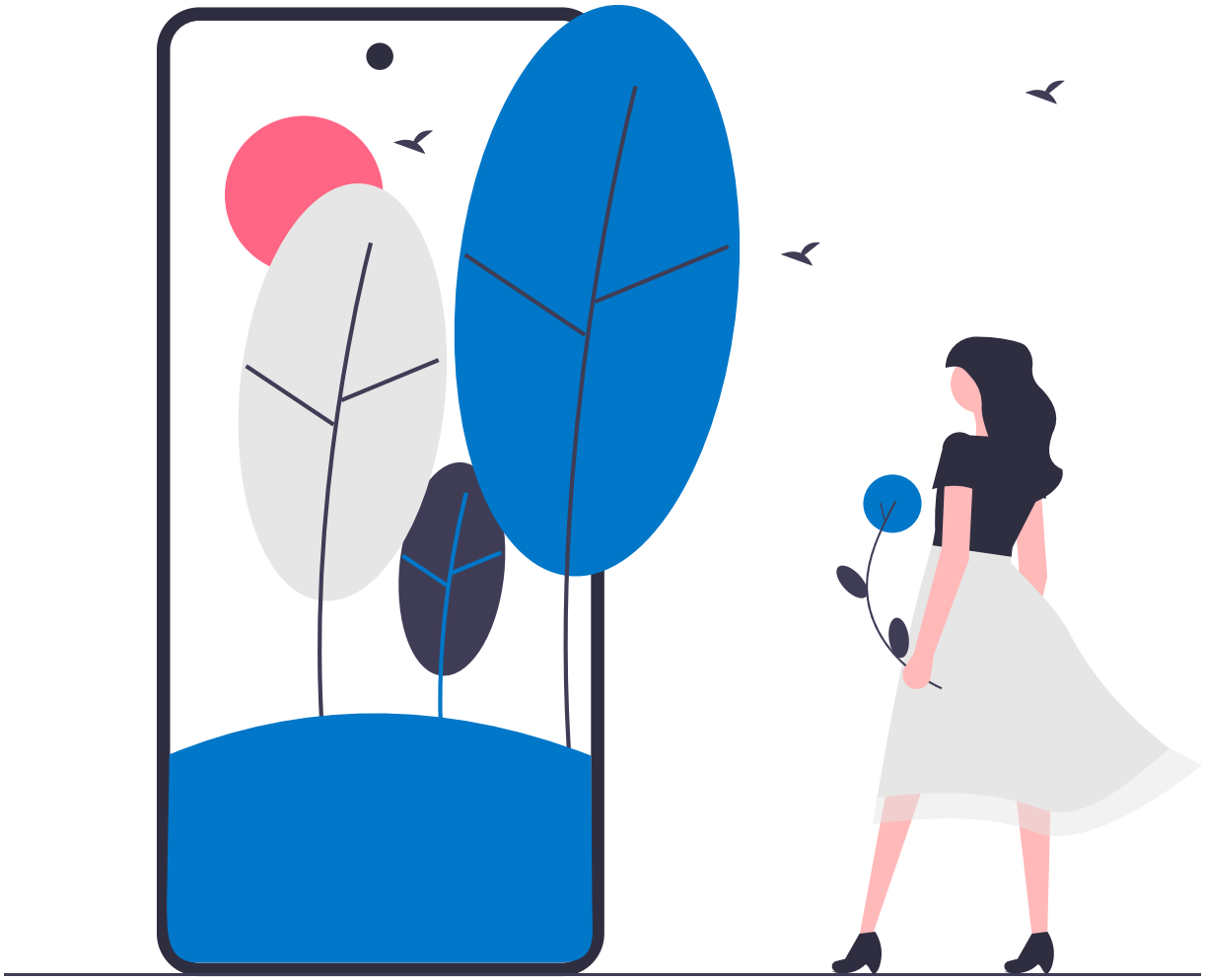
La frase appartiene al poeta Oscar Wilde. Le sue poesie si trovano un po' dappertutto perché i diritti patrimoniali non possono essere rivendicati dagli eredi essendo trascorsi più di 70 anni dalla sua morte. Questo però non significa che non debba essere citato: permangono comunque i diritti morali, quelli cioè che riguardano l'attribuzione della paternità (provenienza) di un'opera al suo creatore.

Together for Tomorrow!
Enabling People

CRESCERE CITTADINI DIGITALI

Guida all'insegnamento dell'Educazione Civica Digitale

Lezione 5
Sostenibilità Digitale



SAMSUNG

Parola all'esperto: Simone Molteni

Direttore scientifico di LifeGate, fondatore nel 2001 di Impatto Zero®, il primo progetto al mondo contro i cambiamenti climatici, è stato direttore editoriale di Expo Milano 2015, nel cda di ENEA, CESI Ricerche, ERSE, nel comitato per l'Ecolabel e l'Ecoaudit della Commissione Europea. Tra i riconoscimenti significativi: il premio svizzero-americano "Venture Leaders", la nomina ad Ambasciatore NETS per il coaching di start-up ad alto contenuto tecnologico, il premio Rotary alla professionalità, l'onorificenza "Paul Harris Fellow".

Digitale e sostenibile

Il mondo digitale ha sicuramente molto a che vedere con la sostenibilità del nostro stile di vita per tantissime ragioni. Il rapporto è duplice: da una parte il digitale aggiunge un problema al pianeta, dall'altro ci offre una serie di soluzioni particolarmente efficaci per alleggerire il nostro impatto sugli ecosistemi che abitiamo.

La parte problematica è la più semplice da capire: stiamo accumulando montagne di strumenti (smartphone, TV, laptop, ecc.) che potenzialmente sono molto inquinanti se non smaltiti correttamente. Come se non bastasse, tutte le funzioni che questi strumenti ci offrono usano moltissima energia per funzionare. Non è solo quella che vediamo noi, caricando per esempio il nostro cellulare. Ogni volta che guardiamo una serie tv in streaming accendiamo una catena di consumo energetico che inizia nel nostro salotto e finisce a chilometri di distanza, coinvolgendo in particolare i mega data center in cui risiedono i contenuti.

In un mondo ideale in cui l'energia elettrica viene prodotta esclusivamente da fonti rinnovabili non sarebbe un grande problema, ma ad oggi quest'energia richiede combustibili fossili e quindi genera molti problemi per l'equilibrio del pianeta, primo fra tutti il riscaldamento globale.

Ma il digitale racchiude anche un mondo di soluzioni incredibilmente utili a migliorare la nostra sostenibilità. Partendo dagli esempi più semplici, ragioniamo sull'archiviazione digitale di documenti cartacei importanti, di cui sia richiesta la conservazione per lunghi periodi. Ci sono quantità enormi di archivi di questo tipo, sono indispensabili anche se verranno usati pochissimo. Una tecnologia che permette di dematerializzare questi archivi (spostando i contenuti su dischi fissi o su cloud) non consente solo di risparmiare carta, inchiostro, colla ed energia (per stampare e rilegare questi documenti), ma anche di evitare tutto ciò che serve per mantenere gli immobili necessari a contenere questa mole di documenti: tipicamente questi uffici vengono illuminati, scaldati d'inverno e raffrescati d'estate.

La dematerializzazione possibile grazie al digitale tocca molti altri settori come la musica, il cinema e i trasporti (evitati) grazie alle video-conferenze.
Ma i benefici più grandi e ancora inesplorati nel campo della sostenibilità sono quelli legati all'Intelligenza Artificiale. Immaginate quanto spreco di materie prime e di energia si può evitare riuscendo a prevedere comportamenti complessi come i menù che verranno richiesti a un grande ristorante. Oppure ottimizzando i flussi di energia e di traffico in una città facendola diventare connessa e veramente smart. Oppure applicandola alle nuove tecniche dell'agricoltura di precisione, che deve integrare e digerire molti dati dinamici (tra cui la meteorologia) per capire quanta acqua e fertilizzanti siano effettivamente necessari in ogni ettaro di terreno agricolo da coltivare.

C'è un altro aspetto in cui la tecnologia può avere due facce. Mi riferisco al fenomeno del "digital divide". I mezzi tecnologici e informatici consentono di accedere a un nuovo mondo di conoscenze e di risorse. Si tratta di una nuova forma di alfabetizzazione che deve ampliare le possibilità offerte a tutti di apprendere e di creare. Il pericolo nascosto, e che dobbiamo combattere, è che l'accesso al digitale si trasformi in una barriera che isola alcune fasce di popolazione (penso agli anziani) e costituisca un ulteriore divario tra ricchi e poveri.

Come ogni tecnologia, dunque, il digitale potrà aiutarci o ostacolarci nella nostra ricerca di sostenibilità: tutto dipende dall'uso che ne faremo.

Simone Molteni

Obiettivi formativi

- Fornire una panoramica su dispositivi e connessioni in Italia e nel mondo.
- Introdurre il tema dello smaltimento della tecnologia (dove finiscono i gli apparecchi elettronici).
- Introdurre il tema dell'impatto della trasformazione digitale sull'ambiente.

Indice lezione

Capitolo 1: Riciclo della tecnologia

Ormai le nostre case sono piene di apparecchiature elettriche ed elettroniche (AEE). Se una volta c'erano il frigorifero, il forno, la televisione, la lavatrice, il frullatore e il fon, oggi oltre a questi elettrodomestici, ci sono almeno un cellulare, un computer e delle cuffie per ogni componente della famiglia. Più un modem e uno o due tablet.

Non serve fare tanti calcoli per rendersi conto che gli oggetti elettronici nelle nostre case sono sempre di più e tanti hanno appena iniziato a diffondersi, come i monopattini elettrici, gli auricolari bluetooth, gli smartwatch, i droni, le e-bike ecc.

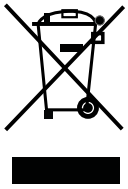
Naturalmente, tutti questi oggetti hanno un ciclo di vita che comprende la produzione, l'uso e, a un certo punto, a fine vita diventano rifiuti.

I RAEE

Tutti questi rifiuti vengono chiamati RAEE, rifiuti di apparecchiature elettriche ed elettroniche.

I RAEE si suddividono in cinque raggruppamenti in base alla tipologia di apparecchiatura ivi ricompresa:

- **R1 - Freddo e Clima** Per esempio frigoriferi, congelatori, condizionatori ecc.
- **R2 - Grandi Bianchi** Per esempio lavatrici, lavastoviglie, forni, piani cottura economici, ecc.
- **R3 - TV e Monitor** Per esempio schermi di vecchie TV con il tubo catodico, moderni schermi TV a LED e al Plasma, monitor per PC ecc.
- **R4 - Informatica, elettronica di consumo, piccoli elettrodomestici, apparecchi di illuminazione** Per esempio cellulari e smartphone, computer, tastiere, mouse, videoregistratori, impianti stereo, ferri da stiro, trapani, frullatori, aspirapolvere, plafoniere ecc.
- **R5 - Sorgenti luminose** Per esempio lampade al neon, lampade a risparmio energetico, lampade che contengono gas ecc.



Tutti i RAEE possiedono questo simbolo che sta a indicare che l'oggetto non deve essere smaltito come rifiuto indifferenziato ma attraverso canali di raccolta differenziati.

Nel 2019, in tutto il pianeta, sono stati prodotti 53,6 milioni di tonnellate di rifiuti elettronici, con un aumento del 21% rispetto al 2014. Un aumento del 21% in soli 5 anni è davvero notevole, soprattutto considerando che si tratta di un trend che certo non si arresterà nei prossimi anni.
Purtroppo però, di queste quasi 54 milioni di tonnellate, solo il 17% è stato raccolto e riciclato correttamente.

Anche la raccolta dei RAEE cresce velocemente: in Italia nel 2019 sono state raccolte oltre 340 mila tonnellate di RAEE, il 10% in più rispetto al 2018, e quasi il 50% in più rispetto al 2014!

Ma come si smaltiscono e si riciclano i RAEE?

Il riciclo dei RAEE

Tutti, in casa, abbiamo un cassetto pieno di apparecchi rotti o dismessi: dai vecchi cellulari alle cuffie che gracchiano, dalle chiavette con poca memoria a vecchi mp3. Spesso, non sapendo dove buttarli, decidiamo di accantonarli in casa.

In realtà i RAEE possono essere riciclati mediamente per oltre il 90% del loro peso. Dal processo di riciclo dei RAEE è possibile recuperare diversi materiali, tra cui plastica, ferro, alluminio e vetro.

Trattandosi di rifiuti che possono contenere sostanze inquinanti (come i clorofluorocarburi – gas un tempo impiegati per la realizzazione di materie plastiche) o tossiche (come il mercurio), per essere correttamente gestiti i RAEE devono essere lavorati in impianti di trattamento specializzati, in grado di separare le varie componenti o materiali, prestando attenzione alle sostanze pericolose.

Una corretta gestione permette non solo di evitare la dispersione di inquinanti, ma garantisce anche il riciclo di materiali che possono essere preziosi, rari o in esaurimento, evitando così di sottrarre materie prime vergini e ricorrere all'utilizzo delle miniere.

Cosa possiamo fare per smaltire correttamente i RAEE?

Se abbiamo un RAEE da smaltire abbiamo diverse possibilità:

- Possiamo portarlo alle isole ecologiche del nostro comune, oppure cercare sul sito Raccolta-RAEE.it il centro di raccolta più vicino.

- Se si tratta di un rifiuto ingombrante, come un frigorifero o una lavatrice, spesso l'azienda che gestisce la raccolta dei rifiuti del nostro comune offre il ritiro a domicilio.

- Se si tratta di un prodotto di piccole dimensioni (massimo 25 cm), possiamo portare il rifiuto in un negozio con una superficie di vendita di AEE superiore a 400 mq. Per legge, infatti, questi negozi devono effettuare il ritiro gratuito "1 contro 0" dei RAEE di piccole dimensioni, ovvero devono offrire il servizio di ritiro del RAEE senza obbligo di acquisto di un nuovo prodotto con le stesse funzionalità.

- Se vogliamo fare una sostituzione, possiamo chiedere al negoziante che ci venderà il prodotto nuovo di effettuare il ritiro dell'usato. In fase di acquisto infatti il negoziante è sempre obbligato a offrire il ritiro del RAEE, secondo la modalità detta "1 contro 1".

In ogni caso, è importante seguire queste indicazioni:

- non buttare mai i RAEE assieme ai rifiuti della raccolta "indifferenziata" o nel bidone del "secco";

- non accumulare i RAEE nei cassetti o in cantina: possiamo metterli da parte per brevi periodi in attesa di effettuare una corretta raccolta differenziata ma, trattandosi di apparecchiature con un alto tasso di materiali riciclabili e a volte con componenti inquinanti, vanno sempre correttamente smaltite in breve tempo.

Tuttavia, oltre a imparare a smaltire correttamente i RAEE, dovremmo adottare degli atteggiamenti e delle abitudini che vadano a ridurre il problema della produzione di rifiuti di questo tipo alla fonte.

I rifiuti elettronici sono infatti la tipologia di rifiuti domestici in più rapida crescita al mondo, alimentato principalmente da maggiori tassi di consumo di apparecchiature elettriche ed elettroniche e da tecnologie che cambiano sempre più velocemente.

Per combattere questa crescita possiamo agire in tre modi diversi, riassumibili nelle tre R:

- **Ridurre**, ovvero diminuire in primo luogo la quantità di prodotti AEE che acquistiamo, cercando di non averne in surplus rispetto alle nostre reali necessità;

- **Riutilizzare**, ovvero continuare a utilizzare i prodotti finché sono efficaci, in modo da sfruttarne a pieno il potenziale, e facendoli riparare quando si rompono;

- **Riciclare**, ovvero effettuare correttamente la raccolta differenziata e far sì che le componenti dei RAEE possano essere trattate e trasformate in materie prime da utilizzare per nuovi prodotti.

Link e informazioni utili

- Report *The Global E-Waste Monitor 2020*
  http://ewastemonitor.info/

- Strumento per trovare il punto raccolta RAEE più vicino
  https://www.cdcraee.it/SearchCdR.pub_do?fromArea=0

- Sito di RAEE Italia
  www.raeeitalia.it/it/

- Approfondimenti e statistiche sul mondo RAEE
  www.erionpervoi.it

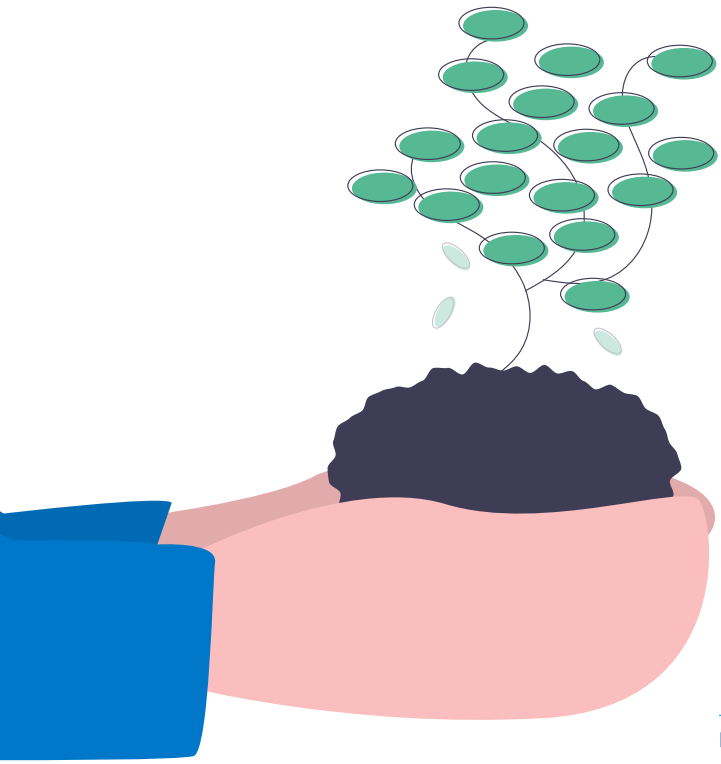
Capitolo 2: Risparmio di energia e digitalizzazione

L'impatto ambientale della digitalizzazione non riguarda solo la produzione di sempre più rifiuti di apparecchiature elettriche ed elettroniche, ma anche il consumo di energia richiesto dalle tecnologie.

Produrre e far funzionare i dispositivi, infatti, richiede grandi quantità di energia.

Tra i cellulari, i piccoli oggetti connessi, i grandi impianti dell'industria 4.0, la quantità di dati che ogni giorno viene generata, trasportata e immagazzinata, la diffusione dello streaming, spesso in HD o in risoluzioni maggiori, e tutta una serie di altri aspetti legati allo sviluppo delle tecnologie digitali, l'energia che viene consumata dall'industria ICT (Information and Communication Technologies), ovvero delle tecnologie dell'informazione e della comunicazione, cresce circa del 9% l'anno.

Basti pensare che una "libreria" di server che occupa lo spazio di un box doccia ha bisogno, per funzionare, di più energia di un'intera casa.



Come mai questa crescita?
Le ragioni alla base di questa forte crescita sono diverse, ma sono riassumibili in quattro motivazioni principali:

- la crescita del numero degli smartphone (circa 11% l'anno dal 2017 a oggi) e della ricchezza e complessità delle funzionalità offerte;
- la crescita di dispositivi connessi (come smart-watch, elettrodomestici intelligenti ecc.);
- lo sviluppo dell'Internet delle Cose (IoT) a livello industriale, che contribuirà ad aumentare il numero totale di dispositivi connessi da 8,4 miliardi nel 2017 a 20 miliardi nel 2020;
- l'esplosione del traffico dati sulle reti, che negli ultimi anni è cresciuto di oltre il 25% l'anno.

L'impatto sull'ambiente

Perché preoccuparci del consumo di tutta questa energia?
Questa crescita nel consumo di energia, a sua volta, fa sì che l'incidenza che hanno le tecnologie digitali sulle emissioni globali di gas serra, che oggi corrisponde al 3,7% del totale, sia cresciuta del 50% rispetto al 2013, quando era del 2,5%.
Si stima che, se l'industria ICT dovesse continuare a crescere con gli stessi ritmi, entro il 2025 raggiungerebbe l'8% del totale delle emissioni di gas serra.

Cosa possiamo fare per contribuire a ridurre il consumo di energia?

Innanzitutto, dobbiamo avere consapevolezza dell'impatto che le nostre abitudini hanno sull'ambiente.

Ci sono diversi strumenti che ci permettono di comprendere l'impatto delle nostre azioni sull'ambiente: carbonfootprint è uno di questi. Basta compilare un questionario in cui inseriamo alcuni dati relativi a diversi aspetti della nostra vita per sapere qual è la nostra impronta ecologica di un anno.

Avere dei dati in mano ci permette di definire piccoli obiettivi che possiamo perseguire nel corso del tempo, calcolando progressivamente la nostra impronta e verificando se ci sono dei miglioramenti.

Per abbassare la nostra impronta possiamo partire seguendo alcuni piccoli accorgimenti che ci permettono di ridurre il nostro consumo di energia, come:

- scollegare i dispositivi anche quando sono in stand-by;
- scaricare i contenuti invece che guardarli in streaming (guardare un video online in streaming per un'ora a settimana richiede la stessa energia necessaria a due frigoriferi nello stesso arco di tempo);
- ridurre la luminosità del monitor;
- cambiare le impostazioni dei pc in "sleep mode" quando facciamo delle pause (in questa modalità consumano 2-5 watt contro i 15-60 normali);
- cancellare l'iscrizione alle newsletter che non interessano ed evitare di inoltrare mail inutili, specialmente se con allegati pesanti e soprattutto se le indirizziamo a molte persone (ricorda che ogni mail emette in media 10 grammi di CO_2).

Link e informazioni utili

- Strumento online per calcolare l'impronta di carbonio individuale
  www.carbonfootprint.com/calculator.aspx

- Ecosia, il motore di ricerca che utilizza i ricavi derivanti dalle ricerche per piantare alberi
  www.ecosia.org/

ATTIVITÀ CON LA CLASSE

Attività 1 - Come è fatto uno smartphone?

- Materiale necessario: possibilità di proiettare
- Obiettivo: arrivare a una maggiore consapevolezza dell'impatto che la realizzazione di un apparecchio elettronico ha sull'ambiente

Di cosa è fatto uno smartphone? Segue brainstorming e viene proiettata la tavola periodica degli elementi. Lo scopo è individuare gli elementi necessari per produrre l'apparecchio: silicio, rame, stagno, argento (i più noti) ma anche ossigeno, arsenico, fosforo, litio e piombo. Inoltre, l'industria elettronica, in particolare quella di smartphone e pc, non può prescindere dalle "terre rare" (gruppo di elementi della tavola periodica la cui rarità è dovuta non tanto alla scarsa disponibilità sul pianeta, quanto all'enorme difficoltà di lavorazione ed estrazione del minerale, molto laboriosa e altamente inquinante).

Attività 2 - Riciclometro

- Materiale necessario: fogli e penne, connessione Internet al sito https://erionpervoi.it/it/gioca/riciclometro/
- Obiettivo: arrivare a una maggiore consapevolezza sul concetto di sostenibilità digitale, identificando come i diversi oggetti della casa possono avere un impatto sul risparmio energetico

L'insegnante chiede alla classe di dividersi in gruppi, ciascuno corrispondente ad un ambiente della casa (es. cucina, bagno, salotto, camera da letto). Utilizzando il "riciclometro" sul sito https://erionpervoi.it/it/gioca/riciclometro/ gli studenti devono identificare gli oggetti solitamente presenti nell'ambiente di casa assegnato e calcolare sia il potenziale complessivo di energia risparmiata in seguito ad un corretto riciclo dei RAEE, sia individuare il singolo oggetto che può avere l'impatto maggiore.

Modalità Didattica a Distanza
Anziché creare gruppi distinti, è l'intero gruppo classe a esplorare insieme all'insegnante, stanza dopo stanza, gli ambienti della casa utilizzando il Riciclometro in autonomia.

◊ Oltre al corretto riciclo, come è possibile ridurre il consumo di energia degli elettrodomestici e device tecnologici presenti in casa? L'insegnante apre con gli studenti una discussione sui piccoli gesti che si possono mettere in pratica per ridurre il consumo energetico in casa (es. spegnere il televisore e il computer senza tenerli in stand-by, collegare i caricatori alla corrente solo quando devono essere utilizzati, spegnere la luce quando si esce da una stanza, ecc.).

SAMSUNG

Together for Tomorrow!
Enabling People

A cura di Samsung Electronics Italia SpA

Con il contributo di:
On. Massimiliano Capitanio

E di:
Michelangelo Coltelli, Antonio Deruda, Riccardo Meggiato,
Simone Molteni, Barbara Volpi

Testi di:
Anastasia Buda, Corporate Citizenship Manager, Samsung Electronics Italia SpA,
Claudia Cottica, Chiara Luchini