

Intelligenza Prudenza Forza Gentilezza Coraggio

**Vivi
Internet,
al meglio.▲**

**Corso di sicurezza e
cittadinanza digitale**

Scuola secondaria
di secondo grado

Ti diamo il benvenuto al corso “Vivi Internet, al meglio”, una risorsa frutto della collaborazione tra Google e Fondazione Mondo Digitale, parte di un programma poliedrico progettato per fornire ai ragazzi le competenze necessarie per comportarsi in modo sicuro e responsabile online e prepararli a muoversi in sicurezza in questo mondo interconnesso.

Il corso “Vivi Internet, al meglio” offre ai docenti strumenti e metodi per insegnare le basi della sicurezza e della cittadinanza digitale in classe e quest’anno si è arricchito di nuove attività educative sui media.

Questi i cinque temi legati alla sicurezza e alla cittadinanza digitale trattati:

- **Utilizza la tecnologia con buon senso**
- **Impara a distinguere il vero dal falso**
- **Custodisci le tue informazioni personali**
- **Diffondi la gentilezza**
- **Nel dubbio parlane**

Le lezioni sono pensate per gli alunni delle scuole superiori. Ti invitiamo a sperimentare questo percorso per capire cosa funziona meglio con i tuoi studenti: potresti completare il corso dall’inizio alla fine, oppure scegliere un paio di lezioni più pertinenti in base al tuo contesto didattico.

Il corso “Vivi Internet, al meglio” fa parte di una serie più ampia di risorse tra cui video didattici per gli insegnanti, materiali da scaricare per la classe, nonché suggerimenti per famiglie e insegnanti per incoraggiare l’adozione di comportamenti sicuri online, disponibili all’indirizzo g.co/vivinternetalmeglio.

Sommario

Guida per gli insegnanti	3
Risorsa 1 Domande frequenti (FAQ)	
Lezione 01: Utilizza la tecnologia con buon senso	4
Attività 1: Quando non condividere	
Attività 2: Di chi è questo profilo?	
Attività 3: In che modo ci vedono gli altri?	
Attività 4: Mantenere la privacy	
Attività 5: Non è quello che intendevo!	
Attività 6: L'importanza del contesto	
Attività 7: Il benessere digitale	
Lezione 02: Impara a distinguere il vero dal falso	22
Attività 1: Non abboccare all'esca del phishing!	
Attività 2: Chi sei veramente?	
Attività 3: A proposito di bot	
Attività 4: È proprio vero?	
Attività 5: Disinformazione online, come individuarla	
Lezione 03: Custodisci le tue informazioni personali	51
Attività 1: Come creare una password perfetta	
Attività 2: Tienilo per te	
Lezione 04: Diffondi la gentilezza	59
Attività 1: Da testimoni a difensori	
Attività 2: Cosa fa un difensore	
Attività 3: Scherzo o bullismo?	
Attività 4: Dillo con più tatto!	
Attività 5: Usa il tono giusto	
Attività 6: Sfidare l'odio in rete	
Lezione 05: Nel dubbio parlane	77
Attività 1: Quando farsi aiutare	
Attività 2: Segnalalo, anche online	
Attività 3: Cosa significa avere coraggio?	

Domande frequenti (FAQ)

Bisogna avere un account Google per il programma “Vivi Internet, al meglio”?

No. Il programma è disponibile per chiunque visiti il sito. Non serve alcun nome utente, password o email.

A quali pagine sono disponibili le risorse?

- Per andare alla home page di “Vivi Internet, al meglio”, visita g.co/vivinternetalmeglio.
- Per il corso “Vivi Internet, al meglio”, visita g.co/peridocenti.
- Per le risorse dedicate alle famiglie, visita g.co/perlefamiglie.
- Ulteriori risorse dedicate ai tuoi studenti sono disponibili alla pagina g.co/periragazzi.

Per poter completare il programma, devo avere una formazione particolare o un’abilitazione speciale come insegnante?

No, qualunque insegnante può tenere questo corso ai propri studenti. Non è necessaria alcuna formazione extra. E poi... ogni insegnante è speciale. :)

Per quali classi è più indicato il corso “Vivi Internet, al meglio”?

L'intero programma, inclusi il corso, il gioco e le risorse sul sito web, è stato pensato per gli studenti delle scuole elementari, medie e superiori (dai 7 ai 19 anni). Infatti, a seconda del modo in cui gli insegnanti personalizzano il corso, gli argomenti possono essere utili per le classi di qualsiasi ordine e grado. Alcune attività sono più indicate per gli studenti dei primi anni, mentre altre sono più focalizzate sul comportamento degli studenti adolescenti.

Devo avere una particolare formazione in cittadinanza digitale per poter usare questo programma?

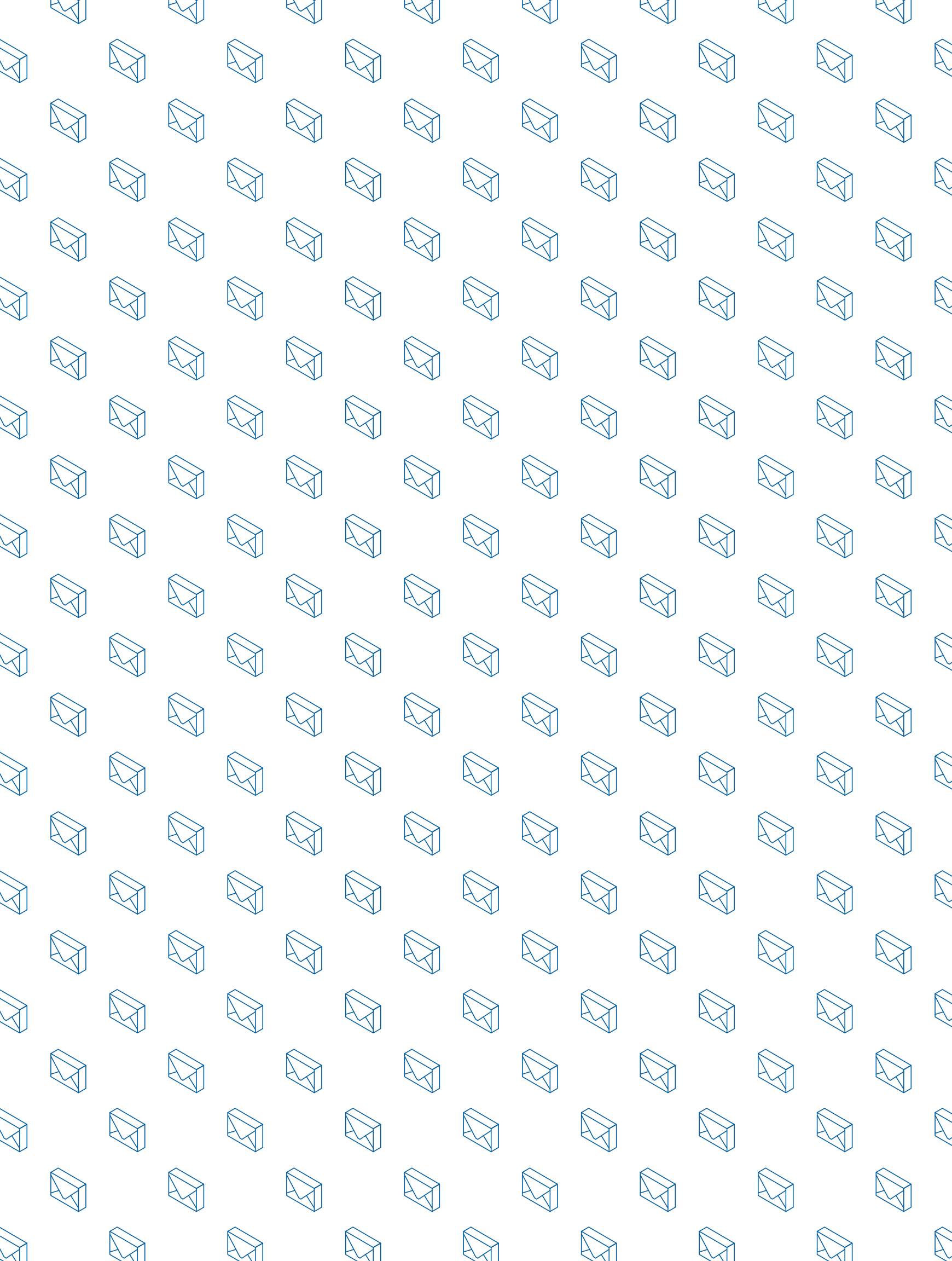
Absolutamente no. Il corso è stato pensato affinché tutti gli insegnanti possano sceglierlo e utilizzarlo con i propri alunni. Inoltre, se vuoi ripassare o saperne di più sugli argomenti relativi alla sicurezza e alla cittadinanza digitale, puoi seguire il nostro corso online per i docenti alla pagina <https://viam.mondodigitale.org/>.

Il corso “Vivi Internet, al meglio” è in linea con gli standard nazionali o regionali?

Il progetto “Vivi Internet, al meglio” è promosso dal Safer Internet Centre - Generazioni Connesse nell’ambito delle attività di sensibilizzazione ed educazione all’uso consapevole di Internet e delle nuove tecnologie.

Dove posso trovare ulteriori risorse per gli insegnanti?

Tutti i materiali di “Vivi Internet, al meglio” si trovano sulla nostra pagina delle risorse all’indirizzo g.co/peridocenti.



Utilizza la tecnologia con buon senso

Proteggiti e proteggi la tua reputazione online

Panoramica della lezione

Attività 1: **Quando non condividere**
Attività 2: **Di chi è questo profilo?**
Attività 3: **In che modo ci vedono gli altri?**
Attività 4: **Mantenere la privacy**
Attività 5: **Non è quello che intendevo!**
Attività 6: **L'importanza del contesto**
Attività 7: **Il benessere digitale**

Temi

Gli adulti sanno che alcuni errori commessi sui dispositivi digitali e su Internet in giovane età potrebbero comportare danni permanenti alla reputazione o generare ripercussioni sui comportamenti. È di grande importanza far comprendere ai ragazzi che un uso equilibrato e intelligente dei dispositivi, dei social e più in generale di Internet può rappresentare un'opportunità di crescita di apprendimento... di vero e proprio benessere digitale che può riflettersi positivamente nelle relazioni personali e nel percorso di studio.

Le attività proposte sono volte a fornire esempi concreti e spunti per intavolare dibattiti stimolanti e insegnare in classe come mantenere un buon profilo online, gestendo le impostazioni della privacy e proteggendo le proprie informazioni personali.

Obiettivi per gli studenti

- ✓ **Creare e gestire** una reputazione positiva sia online sia offline
- ✓ **Rispettare** i limiti della privacy altrui, anche se sono diversi dai propri.
- ✓ **Comprendere** il potenziale impatto di un'impronta digitale mal gestita
- ✓ **Chiedere** aiuto agli adulti qualora ci si trovi in situazioni delicate

Utilizza la tecnologia con buon senso

Vocabolario

Privacy online: un termine generico che solitamente indica la capacità di controllare quali informazioni condividi su di te online e chi può vederle.

Impronta digitale (o presenza digitale): la tua impronta digitale contiene tutte le informazioni su di te presenti online. Può includere qualsiasi cosa, dalle foto ai contenuti audio e video, dai contenuti testuali ai “mi piace” e ai commenti che pubblichi sui profili dei tuoi amici. Come una vera e propria impronta che si lascia sul terreno quando si cammina, anche quello che pubblichi online lascia un segno.

Reputazione: le idee, opinioni, impressioni o credenze che altre persone hanno su di te; qualcosa di cui non puoi avere la certezza assoluta ma che vorresti fosse positiva o buona.

Informazioni personali: tutte le informazioni che identificano una persona specifica, ad esempio il nome, l'indirizzo, il numero di telefono, il codice fiscale, l'indirizzo email ecc., sono dette informazioni personali (o sensibili). Rifletti attentamente prima di condividere questo tipo di informazioni online.

Condivisione compulsiva: il condividere troppe cose online; di solito ci si riferisce alle troppe informazioni personali o semplicemente alle troppe notizie su se stessi fornite in una determinata situazione o conversazione online.

Impostazioni: l'area di qualsiasi sito web, app, prodotto digitale e simili in cui è possibile stabilire i contenuti che condividi e definire il modo in cui viene gestito il tuo account, incluse le impostazioni per la privacy.

Stereotipo: l'immagine o l'idea di una persona, di un gruppo o di una cosa, troppo semplificata, convinzione diffusa.

Interpretare: il modo in cui una persona comprende un messaggio o il significato che ne trae.

Contesto: le informazioni che riguardano il messaggio o qualsiasi cosa vediamo che ci aiuti a comprendere meglio il messaggio. Il contesto può includere il luogo da cui è stato inviato il messaggio, l'ora in cui è apparso e da chi proviene.

Rappresentazione: un'immagine, un simbolo o una descrizione che dice molto (o esprime una verità) su una cosa, una persona o un gruppo.

Inquadratura: quando fai una foto o un video ritraendo un panorama, una persona o un oggetto, l'inquadratura è ciò che definisce la sezione fotografata o ripresa. La parte che decidi di lasciare all'esterno dell'inquadratura è ciò che l'osservatore non potrà vedere.

Quando non condividere

Le storie proposte parlano di condivisione di informazioni in rete apparentemente innocue che possono avere, al contrario, pesanti ripercussioni sull'identità digitale dei protagonisti.

Obiettivi per gli studenti



- ✓ **Capire** che alcune informazioni potrebbero avere un impatto negativo sulla reputazione e la privacy propria e di altri.
- ✓ **Ricordare** che è un diritto di tutti far sì che le proprie scelte relative alla privacy vengano rispettate.

Spunti di discussione



Perché la privacy è importante?

Sul web condividiamo informazioni in modo volontario ma non sempre consapevole delle possibili conseguenze. Con le nostre interazioni su blog e sui social network delineiamo il nostro profilo, per questo è fondamentale riconoscere e valutare quali informazioni e quali azioni online hanno un impatto maggiore sulla creazione della nostra identità digitale.

Ogni qualvolta pubblichiamo una foto, ci registriamo in un luogo tramite geolocalizzazione, commentiamo un post, decidiamo di seguire o meno una pagina, un topic, ecc., condizioniamo e alimentiamo la nostra identità digitale.

Tuttavia, le informazioni che lasciamo in rete vengono talvolta intercettate da persone che non ci conoscono affatto e potrebbero farsi un'idea sbagliata di noi, con ripercussioni negative sulla nostra vita, ora o in un futuro lontano. Una volta pubblicato qualcosa, è difficile tornare indietro.

Ricorda: una volta che qualcosa su di noi o creata da noi è online, potrebbe restarci per sempre. Immaginiamo questa impronta come un pennarello indelebile: i segni che lascia non potranno mai essere cancellati, anche se ci rendiamo conto di aver scritto qualcosa che non corrisponde esattamente a ciò che pensiamo.

Per questo la privacy è importante, e noi possiamo proteggerla condividendo solo contenuti che sappiamo con certezza di voler mostrare, e riflettendo sempre su ciò che è bene pubblicare, su chi potrebbe vedere il nostro post, su quale effetto potrebbe avere su di noi e sugli altri e quando è più opportuno non pubblicare nulla. La tutela della propria privacy è importante, la tutela della privacy degli altri è "sacra".

Di seguito riportiamo alcune domande che potrebbero aiutarti a proseguire il dibattito (gli studenti possono rivolgere queste domande anche alla propria famiglia dopo la scuola):

- Quando è giusto condividere una foto o un video di qualcun altro?
- Pensate sia possibile mantenere il controllo di quanto si è condiviso?
- Raccontare il segreto di un'altra persona, può mai essere giusto?
- E se una persona a cui teniamo molto pubblicasse qualcosa che ci fa pensare che questa persona sia in pericolo e noi decidessimo di confidarlo a qualcuno? Dovremmo avvisare questa persona e dirle cosa pensiamo prima di agire? Dovrebbe sapere che ci stiamo preoccupando per lei?

[Continua alla pagina successiva →](#)

Attività



1. Racconta ai ragazzi la seguente storia.

Angela realizza un fotomontaggio di una sua foto con un ragazzo che le piace, Nando, e invia l'immagine a Gemma, la sua migliore amica. Questa, che conosce Nando molto bene, pensando di fare un favore all'amica, pubblica la foto su un suo album dedicato agli amici del cuore su un suo account social. Nando, infuriato, scrive sotto la foto un commento carico di rabbia nei confronti delle due ragazze.

2. Cosa ha spinto i tre personaggi a comportarsi così?

Dividi ora la classe in gruppi da tre: i componenti di ogni gruppo dovranno immedesimarsi nei tre personaggi: Angela, Gemma e Nando, e provare a esprimere cosa li ha spinti a comportarsi come descritto nella storia. Poi riunisci la classe e parlatene insieme. Poni ai ragazzi le seguenti domande:

- È giusto condividere i nostri segreti con gli altri, a prescindere dal tipo di segreto?
- Quando ci confidano un segreto, in automatico ci donano il diritto di farne cosa vogliamo?
- E se Nando avesse già una fidanzata, cosa potrebbe accadere?

Da ricordare

I segreti costituiscono informazioni personali che potremmo voler tenere per noi o condividere solo con amici e parenti di cui ci fidiamo. Dopo aver condiviso un segreto, non ne abbiamo più il controllo e non sappiamo dove può andare a finire. Pertanto, dobbiamo sempre fare molta attenzione a cosa condividiamo, ancor più quando si tratta di contenuti falsi, come nel caso di un fotomontaggio. Ne abbiamo il diritto?

Quale altro genere di informazioni dovremmo proteggere con attenzione?

- L'indirizzo di casa e il numero di telefono
- L'indirizzo email
- Le password
- I nomi utente
- Tutti i file e documenti personali.

In generale, rispettare le opzioni di privacy delle altre persone è una regola sempre valida da tenere a mente e rispettare, anche laddove riteniamo si tratti di scelte che non condividiamo e che riteniamo eccessive.

Di chi è questo profilo?

In questa attività gli studenti analizzano alcune informazioni personali di personaggi di fantasia per cercare di indovinare alcune cose su di loro.

Obiettivi per gli studenti



- ✓ **Individuare** i modi in cui è possibile trovare online informazioni sulle persone.
- ✓ **Riflettere** su come nascono i pregiudizi sulle persone quando pubblicano qualcosa online.
- ✓ **Determinare** l'accuratezza delle informazioni e saper distinguere tra ipotesi, fatti e opinioni.

Spunti di discussione



Come sappiamo ciò che (apparentemente) sappiamo

Su Internet si possono trovare moltissime informazioni personali, alcune delle quali possono farci pensare o supporre delle cose su persone che potrebbero non rivelarsi vere.

Ecco alcune domande che dovremmo porci:

- Cosa possiamo imparare su una persona attraverso le sue informazioni personali?
- Cosa possiamo provare a indovinare o quali conclusioni possiamo trarre a partire da alcune informazioni personali, anche se non possiamo esserne sicuri?
- Sappiamo in che modo queste informazioni sono state originariamente raccolte? Come possiamo individuarne la fonte?

Attività



Materiale necessario:

- Informazioni raccolte online su persone fittizie o reali. Distribuisci la scheda didattica "Di chi è questo profilo?" oppure raccogli ulteriori esempi consultando i social media account di familiari o celebrità, se pertinenti per l'età. Puoi svolgere questa attività in classe o assegnarla come compito per casa da svolgere individualmente e condividere l'indomani con la classe.
- Registri della cronologia delle ricerche
- Bloc-notes o dispositivi su cui scrivere

1. Studiate il personaggio

Se decidi di usare le informazioni raccolte nella scheda didattica, mostrala alla classe tramite videoproiettore o, in alternativa, fai in modo che tutti ne abbiano una copia.

2. Scrivete una descrizione

Dividi la classe in gruppi e assegna un personaggio per gruppo. Ogni gruppo scrive una breve descrizione della persona, rispondendo alla domanda: "Chi pensi che sia questa persona?".

3. Scoprite chi è

Bene, adesso è il momento di scoprire la verità sui nostri personaggi (ricorda di non leggere le informazioni successive fintanto che tutti i gruppi non avranno completato la descrizione):

- **Serena:** si potrebbe pensare di lei che è una ragazza con una certa sensibilità, forse è di religione ebraica, ama la meditazione e il relax. Chi è davvero Serena? Una studentessa all'ultimo anno di liceo. Si trovava alla Sinagoga per un'uscita organizzata dalla scuola. Ascolta musica rilassante ogni qualvolta ha una discussione con i suoi. Le foto sono state scattate in una maxi piscina scoperta della sua città. Ama i film romantici.
- **Chiara:** si potrebbe pensare di lei che è una ragazza dall'umore piuttosto cupo, Marilyn Manson, gatti neri... Probabilmente è una ragazza dal carattere duro e ribelle. Chi è Chiara nella realtà? Una ragazza di 17 anni dolcissima, fa volontariato nei canili e per associazioni animaliste. Ha due gatti e un cane. Crede profondamente nell'importanza di manifestare per la difesa dei propri diritti. Ha tanti amici ed è molto brava in letteratura (Shakespeare è il suo scrittore preferito).

- **Mario:** guardando il suo profilo si potrebbe pensare che è un ragazzo che pensa solo allo studio, i ragazzi lo definirebbero un “classico Secchione”, che forse pratica arti marziali orientali. Chi è in realtà? Un ragazzo di 15 anni, con una passione per la tecnologia, ma con voti molto bassi nelle materie umanistiche. Ha un fratello più piccolo che gli sta sempre addosso, per questo Mario ha scelto come profilo l’ideogramma cinese della pazienza.

4. Parliamone

Quante cose hanno indovinato i ragazzi? Quante ne hanno sbagliate? Come mai? Che cosa hanno imparato da questa attività?

Da ricordare

Quando vediamo i post, i commenti e le foto di altre persone, facciamo delle supposizioni sul loro conto che spesso non sono corrette, specialmente se non le conosciamo. Succede perché le cose che vediamo online sono solo una parte dell’identità di quella persona e dei suoi interessi. Quella persona potrebbe anche fingere di essere qualcun altro, o potrebbe aver condiviso un pensiero, uno stato d’animo che provava solo nel momento in cui lo ha pubblicato. Non possiamo sapere chi è effettivamente o come si sente davvero finché non la incontriamo, e anche in quel caso ci vorrà del tempo per conoscerla!

Di chi è questo profilo?

Leggete ogni raccolta di attività online svolte dai personaggi riportate di seguito. In base a ciò che vedete qui, scrivete una breve descrizione di come pensate sia questa persona, ad esempio cosa le piace, cosa non le piace e a cosa tiene di più.

Serena



Sinagoga di Roma



Attività: ascoltando musica per meditare



Album di foto: "Tutte le sfumature dell'acqua"



Guardando "Io e Annie" di W. Allen

Status: Meditate, gente, meditate!

Chiara

Ascoltando Marilyn Manson



Foto di una manifestazione



Foto di un gatto nero



Video di sé mentre disegna dei tatuaggi tribali.

"I codardi muoiono molte volte prima di morire... attenti a voi!"

Mario



Screenshot di una porzione di codice di un'app



Nuova immagine di copertina: lo spazio



Nuova immagine di profilo: simbolo della pazienza nel Kung fu



Presso Camera mia



Guardando: Star Wars

In che modo ci vedono gli altri?

In questa attività gli studenti si confrontano su come persone diverse (genitori, insegnanti, datori di lavoro, amici o poliziotti) giudicherebbero i personaggi dell'attività precedente.

Obiettivi per gli studenti



- ✓ **Capire** i punti di vista diversi dal proprio prima di decidere se condividere o meno informazioni online.
- ✓ **Considerare** le conseguenze dell'esposizione delle informazioni personali: ciò che condividiamo diventa parte della nostra reputazione, e può durare per un lungo periodo.
- ✓ **Sviluppare** un obiettivo per creare in modo proattivo una presenza online positiva.

Spunti di discussione



Un nuovo punto di vista

La nostra impronta digitale potrebbe dire molto più di quanto vorremmo che si sapesse e le conseguenze potrebbero essere rilevanti.

Chiediamo ai ragazzi di dare un'occhiata ai profili dell'attività precedente dal punto di vista del nostro personaggio.

- Pensate che a questa persona farebbe piacere che la gente conoscesse le sue informazioni personali? Perché?
- Quali persone potrebbero volerle vedere o, al contrario, sarebbe meglio non vedessero?
- In che modo queste informazioni potrebbero essere viste da altri?
- In che modo queste informazioni potrebbero essere usate da altri?

Situazioni diverse richiedono impostazioni sulla privacy diverse. Il trucco per avere delle buone abitudini di privacy online è pensare al modo in cui le altre persone vedrebbero ciò che pubblichiamo.

Attività



Materiale necessario:

- Una copia a testa dei profili di fantasia dell'attività 2

1. Assumere un nuovo punto di vista

Dividi la classe. Ogni gruppo proverà a immedesimarsi in una delle seguenti figure:

- Genitore
- Allenatore
- Datore di lavoro
- Amico
- Poliziotto
- Pubblicitario
- Tu fra 10 anni

- Cos'è importante per te in qualità di genitore, responsabile, allenatore, amico ecc.?
- Quali conclusioni trarresti sul personaggio?
- Come useresti quelle informazioni?
- Escludi le informazioni che pensi che il nostro personaggio non voglia che tu veda.

2. Cosa emerge?

Ogni gruppo espone i propri risultati e motiva le proprie scelte relative alla privacy. Se ritieni sia il caso, questa potrebbe essere una buona opportunità per fare un gioco di ruolo.

3. Discussione di classe

Quali sono le principali cose da ricordare dopo questa attività di gruppo? Perché le informazioni che abbiamo visto potrebbero raccontare una storia incompleta? Quali pensate possano essere le conseguenze del fatto che una persona si faccia un'opinione negativa su di voi in base a ciò che ha trovato online?

Da ricordare

Persone diverse possono trarre conclusioni diverse dalle stesse informazioni. Non diamo mai per scontato di sapere cosa pensa di noi la gente online.

Mantenere la privacy

Analizzando i quattro scenari che seguono, riflettete su quale potrebbe essere la soluzione migliore in termini di privacy per ognuna delle situazioni descritte.

Obiettivi per gli studenti



- ✓ **Imparare** a valutare le preoccupazioni sulla privacy da diversi punti di vista.
- ✓ **Comprendere** come diversi scenari richiedono livelli diversi di privacy.

Spunti di discussione



Scenari relativi alla privacy: come ci dovremmo comportare?

Scenario 1: Marta lavora il pomeriggio distribuendo volantini per mettere da parte un po' di soldi, ma non vuole che le sue compagne di classe lo sappiano.

- Le altre persone hanno il diritto di saperlo?
- Dovresti essere tu a dirglielo?

Scenario 2: Uno studente manda a un compagno di scuola una poesia chiedendogli un parere, e pregandolo di non divulgarla. Questi, trovandola bellissima, l'indomani la pubblica online.

- Chi ha pubblicato online la poesia ha sbagliato?
- Come ti sentiresti se qualcuno facesse la stessa cosa con delle informazioni che volevi rimanessero private?

Scenario 3: Qualcuno scrive "Ieri sera in mezzo alla folla di piazza San Giovanni ti ho riconosciuta!"

- La ragazza voleva che tutti sapessero dove si trovasse la sera prima?
- Ci sono altre modalità per comunicare questo messaggio in modo più discreto? Magari scrivendolo in un messaggio privato o via SMS?

Scenario 4: Hai scoperto che uno studente, Luca, ha di nascosto creato un account social falso per impersonare un altro studente, Fabio, e comportarsi in maniera negativa, inserendo tutte le sue informazioni personali.

- Fabio ha il diritto di saperlo?
- Qualcuno dovrebbe farlo sapere a un insegnante o a un adulto di fiducia? Come? Cosa potrebbe succedere se nessuno lo facesse?
- Non è chiaro chi l'abbia fatto, ma tu sai chi è stato. Dovresti comunicare queste informazioni a un adulto di fiducia?

Attività



Analizza con la classe i quattro diversi scenari e parlate insieme di come, per ognuno, potrebbe essere richiesta una soluzione diversa in termini di privacy. Dividi la classe in quattro gruppi, ogni gruppo affronterà uno scenario diverso e poi parlatene tutti insieme.

Da ricordare

A seconda delle circostanze il comportamento adeguato da tenere cambia, online e offline. È sempre importante rispettare le scelte in termini di privacy delle altre persone, anche se differiscono da quelle che faremmo noi.

A volte condividendo una foto, un post, o qualsiasi altro tipo di contenuto su un sito web o su una piattaforma social, si inviano involontariamente informazioni e dettagli anche intimi della nostra vita. Per questo è opportuno valutare sempre attentamente il grado di rischio e di impatto sulla privacy nostra o altrui che qualsiasi tipo di contenuto condiviso può avere: registrazioni presso palestre, locali, scuole, immagini e informazioni della propria abitazione, foto in cui tagghiamo i presenti, ecc.

Utilizza la tecnologia con buon senso - Attività 5

Non è quello che intendevo!

Non sempre Internet presenta o ci consente di interpretare la realtà in modo coerente con la verità.

Obiettivi per gli studenti



- ✓ **Imparare** a capire l'importanza di porsi la domanda: "In che modo gli altri potrebbero vedere questo messaggio diversamente da me?"
- ✓ **Sviluppare consapevolezza** sui segnali visivi che le persone usano per comunicare.
- ✓ **Capire** che condividere qualcosa online significa fare informazione.
- ✓ **Imparare** il significato di "contesto" e "rappresentazione".

Spunti di discussione



Qualcuno ha mai mal interpretato qualcosa che abbiamo detto, fatto, scritto o pubblicato online?

Qualcuno si è mai arrabbiato o intristito e abbiamo dovuto spiegarli che non intendevamo dire quello che ha capito?

A volte quando comunichiamo sappiamo a cosa ci riferiamo, ma non è detto che gli altri ne comprendano il senso, specialmente se non ci troviamo fisicamente nello stesso posto. Ciò avviene perché le esperienze di ciascuno influenzano il modo in cui interpretiamo immagini e parole.

Ad aumentare la confusione, ci sono molti messaggi che comunichiamo senza neanche accorgercene. Diciamo alle persone chi siamo - e valutiamo chi sono loro - tramite indizi come i vestiti, l'acconciatura e persino il modo in cui camminiamo o gesticoliamo. Tutto questo viene indicato con il nome di "rappresentazione", ovvero l'espressione di qualcosa, di una persona o di un gruppo attraverso immagini, simboli, stili e parole.

Attività



Leggete insieme la seguenti storie.

Scenario 1

Paolo è un aspirante poeta oltre ad essere anche un bravo writer e nel tempo libero realizza graffiti con alcune delle sue rime. Lo fa su commissione, per privati o in spazi pubblici adibiti dal Comune a tale scopo. Sui social e sul suo canale YouTube pubblica foto e video che lo ritraggono all'opera, appeso ad un cavo, spesso di notte, da solo, senza alcun riferimento sui luoghi o sui committenti delle sue opere. Molti amici di Paolo, scherzosamente, si rivolgono a lui chiamandolo "poeta clandestino" e postando commenti del tipo "Quale altro palazzo stai per imbrattare, writer malefico?"

Immaginate ora che Paolo, terminata la scuola, stia cercando lavoro presso alcune aziende della sua città. I titolari di alcune delle aziende a cui si rivolge, visitano i suoi profili social, come spesso accade nella realtà.

Scenario 2

Andrea partecipa alla festa di fine anno della sua scuola. La serata si accende, tutti si stanno divertendo ma qualcuno comincia a fare battute pesanti decisamente fuori dagli schemi, e così anche Andrea si fa prendere la mano e inizia a dire cose che mai in nessun altro

contesto avrebbe pronunciato. L'indomani uno dei suoi compagni di classe pubblica un video realizzato durante la festa, senza alcun contesto e solo con alcuni passaggi della serata, proprio i più imbarazzanti.

Il video, in cui Andrea è riconoscibilissimo, a distanza di anni finisce in una playlist pubblica e diventa virale. In rete si scatena un passaparola su Andrea che lo pone in grande imbarazzo.

Chiedi ora ai ragazzi di riflettere sulle seguenti questioni:

Scenario 1

- Sarebbe bene che Paolo tenesse foto simili in privato? Quali impostazioni suggerireste a Paolo di modificare?
- Se sì, perché?
- I futuri datori di lavoro potrebbero essere influenzati da questi contenuti nel farsi un'opinione sul ragazzo?
- Come Paolo potrebbe contestualizzare meglio le foto sui suoi account?

Scenario 2

- Ti capita mai di dire cose che non pensi realmente? Sapresti fare un esempio?
- E se qualcuno diffondesse video che ti ritraggono mentre pronunci queste cose?
- Vi è mai capitato di pubblicare o vedere pubblicati contenuti su di voi che non riflettono la realtà?
- Come è possibile evitare al massimo che ciò accada?

Da ricordare

In qualità di creatori di contenuti multimediali, prima di pubblicare messaggi o foto online sarebbe meglio fermarsi un attimo e chiedersi: "In che modo una persona diversa da me potrebbe interpretare questo messaggio? Ho la certezza che capisca cosa voglio dire?" E dovremmo chiederci la stessa cosa prima di fare commenti ad altre persone. "Ho la certezza di capire cosa vogliono dire? Come faccio ad averla?".

Utilizza la tecnologia con buon senso - Attività 6

L'importanza del contesto

Nota per gli insegnanti:

I contenuti multimediali sono creati da persone che compiono la scelta di cosa includere e cosa escludere da quello che stanno comunicando. Questa lezione aiuta gli studenti a immaginarsi come dei creatori di contenuti ogni volta che devono decidere cosa condividere online.

Obiettivi per gli studenti



- ✓ **Immaginarsi** come creatori di contenuti multimediali.
- ✓ **Comprendere** che i creatori di contenuti multimediali scelgono cosa mostrare e cosa tenere al di fuori dell'inquadratura.
- ✓ **Capire** che condividere qualcosa online significa fare informazione.
- ✓ **Usare** il concetto di inquadratura per capire la differenza tra cosa rendere visibile e pubblico e cosa tenere al sicuro o nascosto.

Spunti di discussione



Immaginiamo la nostra comunicazione come una cornice: siamo noi a decidere cosa far rientrare all'interno dell'inquadratura (ciò che possiamo vedere), e ciò che resta all'esterno dell'inquadratura (ciò che rimane nascosto agli occhi di guarda).

Attività



Materiale necessario:

- Schede e forbici (una per studente)
- Scheda didattica "Cosa c'è nell'inquadratura?" o schermo o lavagna interattiva con le immagini proiettate

Tutti i contenuti multimediali sono il frutto di una serie di scelte da parte dei relativi creatori. Tra le scelte importanti vi sono quelle di decidere cosa includere e cosa escludere. Quando scattiamo una foto o registriamo un video, ciò che rimane all'interno e ciò che è escluso sono separati da una cornice.

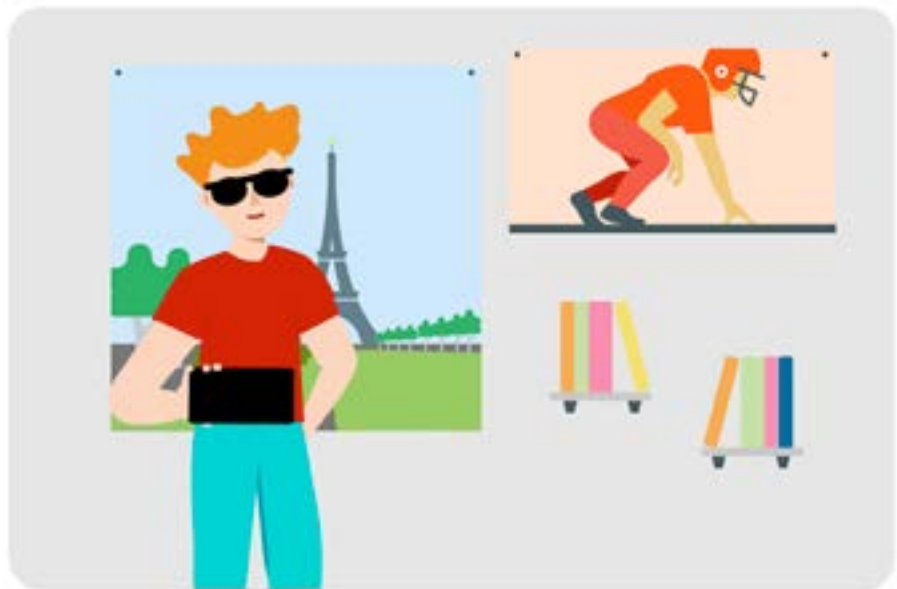
Esaminate ogni attività come classe, poi parlate dei seguenti aspetti:

1. Lo mostriamo oppure no? Mostra ai ragazzi le immagini 1A e 2A della scheda didattica "Cosa c'è nell'inquadratura" e chiedi loro di descrivere cosa vedono. Poi mostra loro le immagini 1B e 2B. Le loro descrizioni coincidono con la realtà?
2. Troppe informazioni? Le informazioni extra non sono sempre ben accette. A volte un elemento in più è causa di distrazione o non ci permette di comprendere un'immagine all'interno di un'inquadratura. Cosa accadrebbe se ogni volta che guardassimo un film, un programma TV o un video vedessimo anche le telecamere, i microfoni, i membri della troupe e tutto il set? Pensate che riusciremmo a goderci la storia allo stesso modo?
3. La decisione spetta a noi! Ogni volta che condividiamo qualcosa online, stiamo creando dei contenuti. E proprio come i produttori di un film, di un video o di un programma TV, siamo noi a decidere ciò che le persone vedranno: cosa rimarrà all'interno dell'inquadratura e cosa sarà nascosto alla vista e rimarrà ignoto agli altri.

Cosa c'è nell'inquadratura?



1A



1B



2A



2B

Il benessere digitale

Per “benessere digitale” si intende quello stato di soddisfazione e comfort che si sviluppa in relazione al modo in cui la tecnologia fa parte della propria vita. È utile offrire ai ragazzi occasioni per riflettere su tematiche legate al loro personale utilizzo della tecnologia e di Internet e su quanto questi condizionino la loro vita e le loro relazioni interpersonali.

Obiettivi per gli studenti



- ✓ **Comprendere** qual è il confine tra un uso sicuro e gratificante della tecnologia e un utilizzo esagerato e poco consapevole di quest'ultima.
- ✓ **Riflettere** su quali abitudini online hanno un impatto totalmente positivo e quali, al contrario, creano frustrazione, dipendenza, isolamento e perdita del controllo.

Spunti di discussione



Si parla spesso dei rischi e pericoli della rete, tralasciando le grandi potenzialità che può offrire dal punto di vista dell'apprendimento e dello sviluppo emotivo, sociale e cognitivo.

Attività



Materiale necessario:

- Fogli bianchi (anche riciclati) e forbici (una per studente).

Attività 1

Chiedi ai ragazzi di immedesimarsi nelle seguenti storie e di provare a individuare, sinceramente, situazioni che davvero accadono nelle loro vite:

- Durante un'attività scolastica o di formazione (compiti a casa) ti capita di essere involontariamente distratto/a da un dispositivo collegato ad Internet, e riprendere il filo di ciò che stavi facendo è più oneroso che se ti fossi alzato/a per una breve pausa, per andare al bagno o fare uno spuntino.
- Senti spesso la necessità di controllare se ci sono notifiche sul tuo telefono.
- Segui una serie tv e ti rendi conto di avere guardato troppe puntate, perdendo la concezione del tempo.
- Ti è successo almeno una volta nell'ultimo mese di ritrovarti isolato/a, non coinvolto/a nella discussione, pur essendo in gruppo, perché distratto/a da un dispositivo collegato ad Internet.
- Dimentichi il tuo smartphone a casa durante una gita di un giorno con la scuola. La cosa ti agita, ti fa sentire privo di una parte fondamentale di te e fai di tutto per poter tornare indietro a prenderlo.
- Ti capita di essera a tavola con i tuoi genitori o fratelli e di non ascoltare quello che si dice perché alle prese con il tuo smartphone.

Attività 2

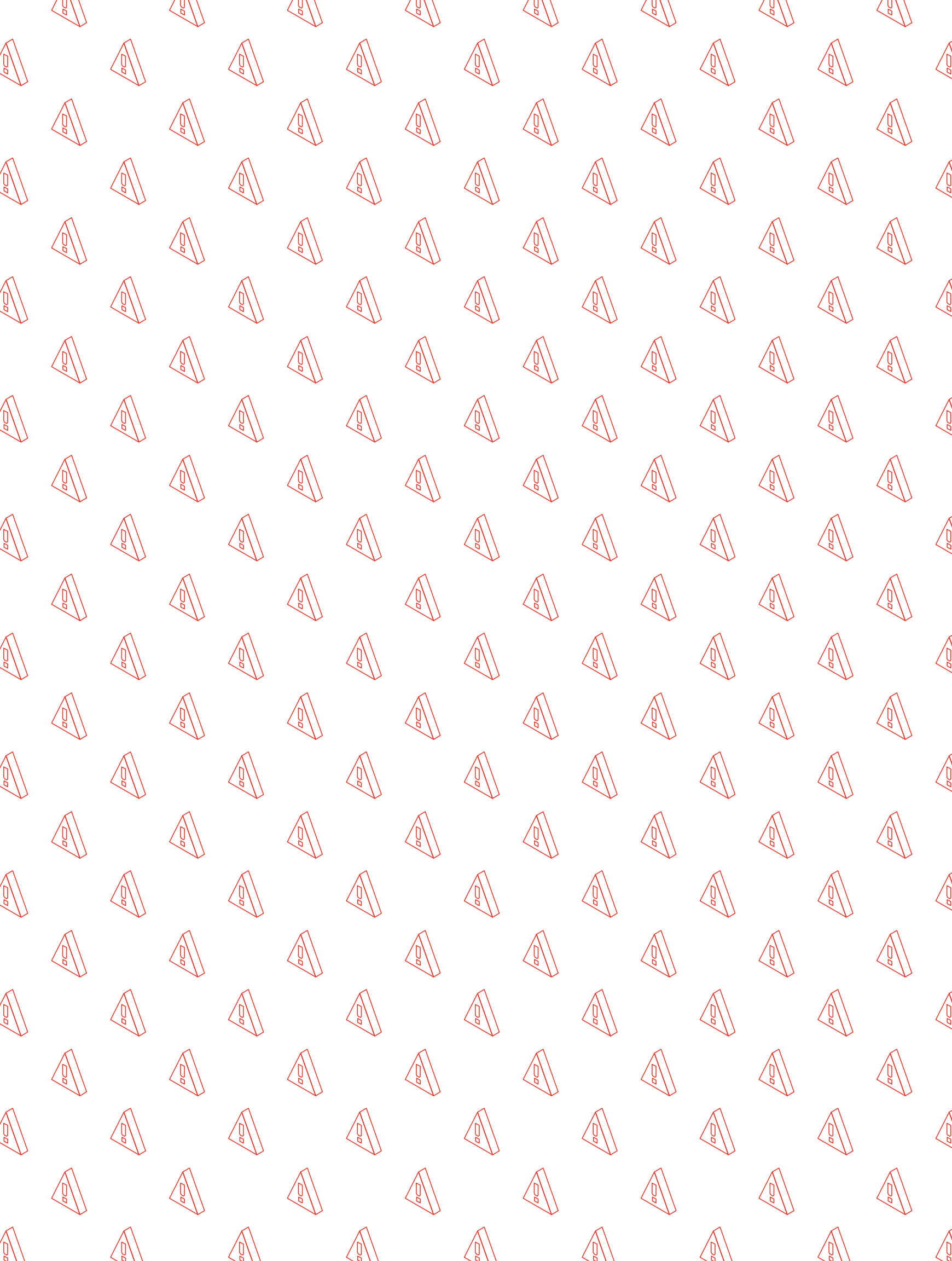
Chiedi ai ragazzi di stilare un elenco di tutte le attività online o svolte tramite dispositivi digitali che migliorano la qualità della loro vita e in che modo. Riportiamo di seguito alcuni esempi:

- Videochiamate con parenti lontani
- Uso di mappe per trovare luoghi che non si sa come raggiungere
- Contatto con le famiglie quando si è fuori casa
- Attività didattiche
- Visione di film
- Ascolto di musica
- ...

Da ricordare

Internet può essere un grande ausilio allo studio dei ragazzi per rendere l'apprendimento più appassionante: molti studenti lo utilizzano quotidianamente come un'enciclopedia in cui poter ricercare approfondimenti, in cui effettuare traduzioni o come supporto per risolvere i compiti assegnati a scuola.

È compito dei docenti aiutare gli studenti a comprendere cos'è il benessere digitale e a sviluppare un pensiero critico, accompagnandoli nel processo di sviluppo delle abilità comunicative interpersonali/interculturali di cui hanno bisogno per vivere positivamente le opportunità della rete.



Impara a distinguere il vero dal falso

Tenersi alla larga da phishing e frodi

Panoramica della lezione

Attività 1: **Non abboccare all'esca del phishing!**
Attività 2: **Chi sei veramente?**
Attività 3: **A proposito di bot**
Attività 4: **È proprio vero?**
Attività 5: **Disinformazione online, come individuarla**
Attività 6: **Sviluppare spirito critico**

Temi

È importante che i ragazzi capiscano che i contenuti che trovano online non sono necessariamente veri o affidabili, anche se talvolta sono realizzati tanto bene da sembrarlo, e che a volte potrebbe trattarsi di tentativi di rubare le loro informazioni personali. Il phishing e altri tentativi di frode online incoraggiano gli utenti di Internet di tutte le età a rispondere a esche lanciate da persone che non conoscono, o a volte anche da persone che fingono di conoscerli.

Obiettivi per gli studenti

- ✓ **Capire** che non tutto ciò che è online è necessariamente vero.
- ✓ **Comprendere** i meccanismi del phishing, perché è una minaccia e cosa fare per evitarlo.
- ✓ **Stabilire** la validità dei siti web e di altre fonti di informazioni e saper prestare attenzione alle manipolazioni, alle affermazioni infondate, alle offerte o ai premi fasulli e ad altre truffe online.

Impara a distinguere il vero dal falso

Vocabolario

Bot: detti anche “chatbot” o “assistenti virtuali”, sono dei software che funzionano online o su una rete e rispondono automaticamente alle domande, eseguono dei comandi (ad es. dare le indicazioni per raggiungere la nuova casa di un amico) oppure svolgono semplici compiti (ad es. riprodurre una canzone).

Phishing: tentativo di frode o inganno finalizzato a spingerci a condividere informazioni di accesso o altre informazioni personali online. Generalmente questi attacchi avvengono via email, tramite pubblicità o siti che sembrano quelli che usiamo abitualmente.

Spear phishing: frode di phishing in cui chi compie l'attacco usa le nostre informazioni personali per colpirci in modo mirato.

Frode: tentativo disonesto di guadagnare soldi o ottenere qualcosa di valore tramite l'inganno.

Affidabile: qualcosa di cui ci si può fidare in termini di esattezza e necessità.

Autentico: reale, genuino, onesto o vero; non falso, né copiato.

Verificabile: di cui si può provare o dimostrare che è vero o corretto.

Ingannevole: falso; un'azione o un messaggio pensati per imbrogliare, prendere in giro o confondere qualcuno.

Manipolazione: azione di qualcuno che controlla o influenza un'altra persona o situazione in maniera scorretta, disonesta o sotto minaccia. Le cose che si trovano online possono essere manipolate, ad esempio una foto modificata per farci credere che una determinata cosa non è vera.

Fraudolento: ingannare qualcuno al fine di ottenere qualcosa di valore.

Firewall: programma che protegge il computer dalla maggior parte delle frodi e degli imbrogli.

Malevolo: parole o azioni pensate appositamente per

essere crudeli o offensive. Può essere riferito anche a software dannoso con lo scopo di compromettere il dispositivo, l'account o le informazioni personali di una persona.

Catfishing: creare un'identità o un account falsi su un social network per convincere le persone a condividere le proprie informazioni personali o a credere che stiano parlando a una persona reale con un account, un profilo o una pagina legittimi.

Clickbait: contenuti, post o annunci online manipolatori pensati per catturare l'attenzione delle persone e spingerle a fare clic su un link o una pagina web, spesso per aumentare le visualizzazioni o il traffico a un sito allo scopo di guadagnare denaro.

Vlogger: una persona che è conosciuta per via della pubblicazione regolare di brevi video su un blog o un social media.

Fonte: qualcuno o qualcosa che fornisce delle informazioni.

Credibile: attendibile; chi è credibile mostra delle prove per rassicurarci del fatto che sta dicendo la verità.

Prova: fatti o esempi che dimostrano che qualcosa è vera o falsa.

Competenze: capacità o conoscenze speciali di un argomento in particolare; gli esperti hanno delle competenze.

Motivazione: la ragione per cui una persona fa qualcosa; intenzione.

Notizie ingannevoli: notizie che mentono o distorcono la realtà intenzionalmente.

Gruppo di facciata: un gruppo che finge di essere qualcosa che in realtà non è al fine di nascondere l'identità delle persone che effettivamente lo gestiscono.

Disinformazione: informazioni false o volte a ingannare.

Non abboccare all'esca del phishing!

Analizzando esempi di email e di messaggi, i ragazzi saranno in grado imparare a distinguere quelli affidabili dai tentativi di truffa.

Obiettivi per gli studenti



- ✓ **Imparare** le tecniche utilizzate per rubare le identità.
- ✓ **Analizzare** i sistemi a disposizione per prevenire i furti di identità.
- ✓ **Sapersi** rivolgere a un adulto di fiducia nel caso si pensi di essere vittima di un furto d'identità.
- ✓ **Riconoscere** gli indizi che identificano un tentativo di phishing.
- ✓ **Fare attenzione** a come e con chi si condividono le proprie informazioni personali.

Spunti di discussione



Allora che cos'è questo phishing?

Si parla di phishing quando una persona, fingendo di essere qualcuno di cui ci fidiamo, prova a rubarci informazioni come dati di accesso o altri dettagli di un nostro account via email, messaggio o tramite altre forme di comunicazione online. Le email di phishing, nonché i siti non sicuri a cui cercano di rimandarci o gli allegati che tentano di farci aprire, possono anche portare dei virus sul computer. Alcuni virus utilizzano l'elenco dei contatti per prendere di mira i nostri amici e la nostra famiglia con lo stesso attacco di phishing, talvolta anche più personalizzato. Altri tipi di frode potrebbero tentare di farci scaricare malware o software indesiderati, facendoci credere che ci sia qualcosa che non va sul nostro dispositivo.

Ricorda: un sito o una pubblicità non possono sapere se c'è qualcosa che non va nel nostro dispositivo!

Alcuni attacchi di phishing sono facilmente riconoscibili. Altri possono essere subdoli e molto convincenti, ad esempio quando un truffatore ci invia un messaggio che include alcune informazioni personali. In quest'ultimo caso si parla di spear phishing ed è molto difficile da individuare perché l'utilizzo delle nostre informazioni lo fa sembrare un messaggio di una persona che ci conosce.

Prima di fare clic su un link o inserire la password in un sito che non abbiamo mai visitato prima, è buona norma porsi delle domande su quell'email o pagina web. Ecco qualche esempio:

- Ha un aspetto professionale come altri siti web che conosciamo e di cui ci fidiamo? Il logo del prodotto o della società e i testi sono privi di errori di battitura?
- L'URL del sito corrisponde al nome e alle informazioni del prodotto o della società che stiamo cercando? Ci sono errori di battitura?
- Si aprono dei pop-up con spam?
- L'URL inizia con https:// ed è presente un lucchetto verde alla sua sinistra? (Questo significa che la connessione è sicura.)
- Cosa c'è scritto a lettere piccole? (Spesso è così che scrivono le cose più ambigue.)
- L'email o il sito offrono qualcosa che sembra troppo bella per essere vera, ad esempio la possibilità di guadagnare molti soldi? (Quasi sempre è troppo bello per essere vero.)
- Il messaggio sembra un po' strano? È come se ci conoscessero, ma non ne siamo sicuri al 100%?

Alcuni suggerimenti da condividere con la classe

Cosa fare se riescono a truffarci?

- Tanto per cominciare, non andiamo nel panico!
- Parliamone subito con i genitori, gli insegnanti o qualche altro adulto di cui ci fidiamo. Più aspettiamo, più la situazione potrebbe peggiorare.
- Cambiamo le password dei nostri account online.
- Se siamo stati vittime di una truffa, facciamolo sapere subito ad amici e conoscenti, perché potrebbero essere i prossimi a essere colpiti.
- Utilizziamo le impostazioni per segnalare il messaggio come spam, quando possibile.

Attività



Materiale necessario:

- Scheda didattica: "Esempi di phishing"

Risposte alla scheda didattica "Esempi di phishing" (pag. 25):

1. **Vero.** L'email chiede all'utente di visitare il sito web della società e di accedere al suo account autonomamente, anziché fornire un link all'interno dell'email o chiedergli di inviare la password tramite email (i link possono rimandare gli utenti a siti web malevoli).
2. **Falso.** URL sospetto e non sicuro.
3. **Falso.** Offerta sospetta in cambio di dati bancari.

1. Analizzate gli esempi in gruppo

Analizzate gli esempi riportati nella scheda didattica "Esempi di phishing" (pag. 25), si tratta di tentativi di phishing o normali comunicazioni?

2. Analizzate URL e indirizzi email

Immaginiamo un'ipotetica piattaforma di film in streaming, il cui dominio Internet (inesistente e immaginato solo ai fini del gioco) è teenmovie.it.

Pertanto, tutti gli indirizzi web (URL) o gli indirizzi email contenuti nelle email provenienti da questa piattaforma dovranno essere del tipo: teenmovie.it/login (pagina di login), xyz.teenmovie.it (URL), xyz@teenmovie.it (email).

Quali tra quelli in elenco potrebbero essere tentativi di frode? E perché?

1. db2w0assistenza@teen-movie.com
2. http://online.da.teenmovie.ru-it.update.com
3. https://titolari.teenmovie.it/portal/server.pt
4. http://kpalsveta.tr/www.teenmovie.it/index.php
5. http://login.teenmovie.access.it
6. assistenza@teenmovie.tr
7. http://80.574.215.39.teenmusic-italia.it
8. noreply@teenmovie.it
9. www.teenmovie.com.personal.login

Risposte

1. Una strana sequenza iniziale di lettere non è un buon segnale, oltre al dominio errato, il nostro dominio teniamolo sempre a mente è: teenmovie.it
2. Dominio totalmente errato (.da-it.update.com) e protocollo http non sicuro. I protocolli sicuri prevedono https
3. Il dominio teenmovie.it è corretto
4. Il dominio in questo caso è kpalsveta.tr e protocollo http non sicuro, specialmente laddove si inseriscono dati personali
5. Il dominio è access.it, ed è quindi errato
6. Indirizzo email turco (.tr non .it)
7. Il dominio è errato, inizia con indirizzo IP e dopo teenmovie ha un - italia
8. L'indirizzo è affidabile, il dominio del sender è corretto
9. Il dominio è errato è un .com e non un .it

Quali sono gli esempi che sembravano affidabili e quali quelli sospetti? C'era qualche risposta che non vi aspettavate? Se sì, perché?

3. Valutate la seguente situazione

Leggi la storia di Monia in classe. Poi chiedi ai ragazzi di rispondere individualmente alla domanda che segue.

Monia va a trovare suo padre in ufficio e mentre lui è impegnato in una riunione lei si siede alla sua postazione e inizia ad utilizzare il suo pc. Monia entra nella casella di posta personale e tra le mail in arrivo ce n'è una inviata, apparentemente, dalla sua piattaforma di video streaming (legale) preferita, che le propone due settimane di abbonamento gratuito, semplicemente scaricando un file allegato da compilare e inoltrare al mittente con i suoi dati. Monia scarica l'allegato e improvvisamente perde il controllo del computer del padre, mentre sullo schermo compare una finestra che richiede l'inserimento di una password per sbloccare il pc e accedere ai dati e ai file. La password si può ottenere effettuando il pagamento di 300 euro. Monia è terrorizzata, soprattutto perché si tratta del computer di lavoro di suo padre, in cui è custodito tantissimo materiale riservato.

Cosa avrebbe potuto fare Monia per evitare che ciò accadesse?

1. Controllare l'indirizzo email del mittente
2. Controllare che l'allegato avesse un' estensione immediatamente eseguibile (es. .exe, .bat o ancora .msi)
3. Contattare la polizia postale
4. Spegner il PC nella speranza che si resettasse
5. Staccare la corrente elettrica e non accendere il PC per i 3 giorni consecutivi
6. Scaricare un programma antivirus per rimediare

Risposte:

1. V 2. V 3. V 4. F 5. F 6.F

È buona prassi controllare sempre l'indirizzo email del mittente, ancora di più se lo scopo della mail è una richiesta di informazioni.

È bene controllare l'estensione dell'allegato prima di scaricarlo: allegati immediatamente eseguibili (es. .exe, .bat o ancora .msi) potrebbero rappresentare un tentativo di "ransomware" un tipo di virus che limita l'accesso del dispositivo che infetta, richiedendo un riscatto (ransom in Inglese) da pagare per rimuovere la limitazione. Inoltre, è sempre bene effettuare tutte le verifiche del caso prima di scaricare allegati o cliccare su link segnalati, per accertarsi della veridicità della email, oltre ad installare sul pc un buon antivirus e anti-phishing.

Non riaccendere il pc per 7 - 10 - 20 giorni non cambierà la situazione.

Scaricare un antivirus con il PC bloccato non solo sarebbe impossibile, ma tardivo.

In questa storia la tecnica di phishing usata è chiamata “baiting” e consiste nell’offrire qualcosa al fine di consentire il download di un file dannoso. Quello descritto è un caso piuttosto sofisticato, ma con un po’ di attenzione si può identificare il tentativo di frode. E nel dubbio, è sempre bene rivolgersi ad un adulto di fiducia più esperto di noi!

4. Approfondimento

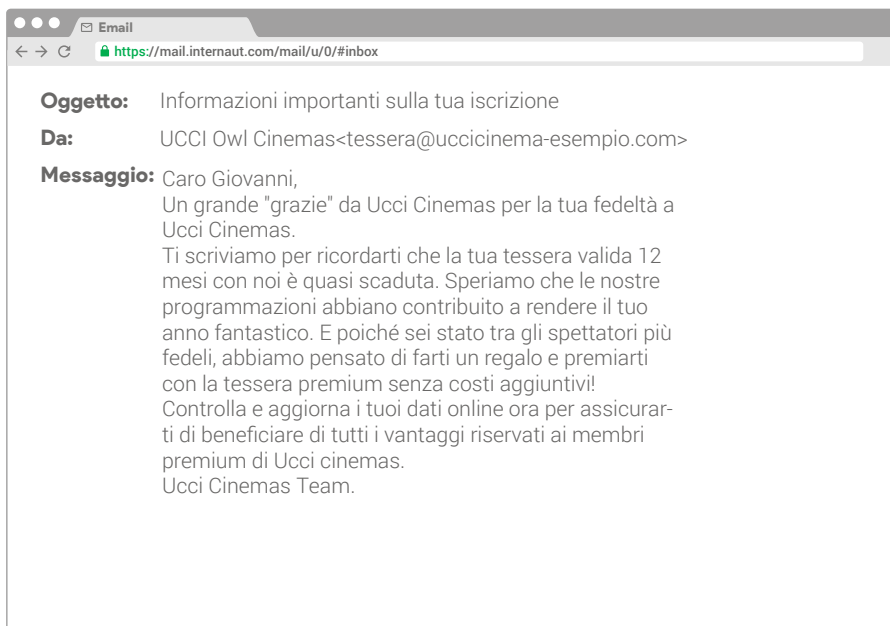
Ecco alcune ulteriori domande che dovremmo porci quando cerchiamo di capire se i messaggi o i siti che troviamo online sono autentici:

- C’è qualcosa di strano in questo messaggio? Leggendo qual è il nostro primo istinto? Notiamo qualcosa di sospetto? Offre di risolvere qualcosa che non sapevamo fosse un problema?
- Nella mail ci viene offerto qualcosa a titolo gratuito? Normalmente le offerte gratuite non sono davvero tali.
- Ci vengono richieste informazioni personali? Alcuni siti ci chiedono informazioni personali per poterci mandare altri tentativi di frode. Per esempio, i quiz o “test della personalità” potrebbero raccogliere dati per riuscire a indovinare la nostra password o sottrarci altre informazioni private. La maggior parte delle aziende reali non chiede informazioni personali via email.
- Si tratta di una catena? Le email e i post in cui ci viene chiesto di far girare il messaggio a tutti i nostri contatti possono mettere a rischio noi e altre persone. Non fateli girare a meno che non conosciate la fonte e sappiate con certezza che il messaggio è sicuro.
- Contiene parti scritte in piccolo? In fondo alla maggior parte dei documenti possiamo trovare delle note scritte con caratteri più piccoli. Questa parte di testo spesso contiene informazioni importanti scritte in piccolo di modo che non si riescano a leggere. Per esempio, potrebbe esserci un titolo in cui viene annunciato che abbiamo vinto un telefono in omaggio, ma in piccolo viene specificato che per averlo dobbiamo pagare 200 euro al mese. Anche la totale assenza di scritte in caratteri più piccoli può essere un brutto segno, prestate attenzione anche a quello.

Da ricordare

Quando siamo online, facciamo sempre attenzione agli attacchi di phishing via email, nei messaggi di testo e nei messaggi pubblicati. Nel caso in cui qualcuno riuscisse a ingannarvi, ditelo immediatamente a un adulto di cui vi fidate.

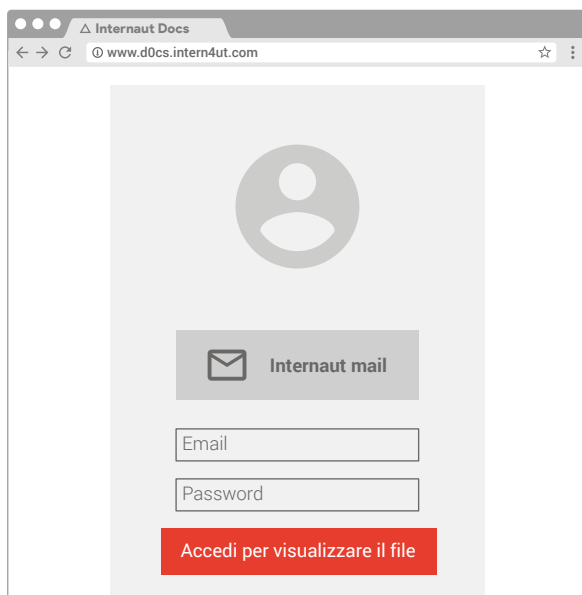
Esempi di phishing



1. Vero o falso?

Vero

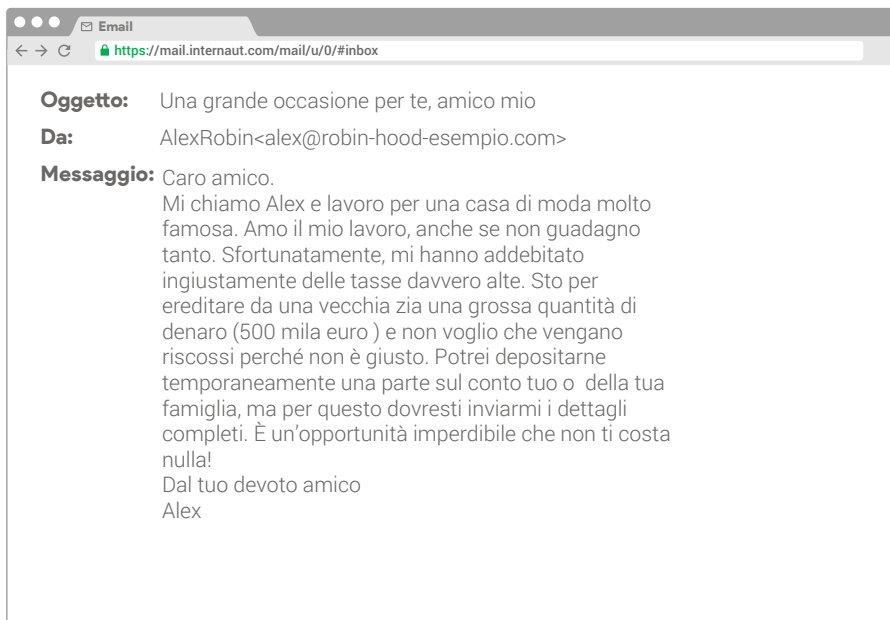
Falso



2. Vero o falso?

Vero

Falso



3. Vero o falso?

Vero

Falso

Chi sei veramente?

Gli studenti potranno ora esercitare le competenze anti-phishing, interpretando e parlando dei comportamenti da tenere di fronte a messaggi online, post, richieste di amicizia, foto e email sospetti.

Obiettivi per gli studenti



- ✓ **Capire** che le persone online potrebbero non essere chi dicono di essere.
- ✓ **Assicurarsi**, prima di parlare, che la persona con cui si sta comunicando è chi dice di essere.
- ✓ **Fare domande** o chiedere aiuto a un adulto se è difficile riuscire a capire chi è la persona con cui si sta parlando.

Spunti di discussione



Come facciamo a sapere di chi si tratta?

Quando parliamo per telefono con un amico siamo in grado di dire che è certamente la persona che dice di essere perché ne riconosciamo la voce, anche se non lo vediamo. Tuttavia, nel mondo online è un po' diverso, e può risultare più complicato essere certi che qualcuno sia realmente chi dice di essere. Nelle app e nei giochi, a volte le persone si fingono qualcun altro, per scherzo, per prendere in giro qualcuno in maniera cattiva o, peggio ancora, per rubare informazioni personali. Quando navighiamo in Internet, potrebbe capitarci che qualcuno che non conosciamo ci chieda di aggiungerlo ai contatti. La cosa più sicura da fare è non rispondere o riferirlo a un genitore o a un adulto di cui ci fidiamo. Ma se decidiamo di rispondere, è una buona idea cercare prima di scoprire qualcosa sul suo conto. Controlliamo il suo profilo, vediamo chi sono i suoi amici o cerchiamo altre informazioni che confermino la sua identità.

Ci sono tanti modi per verificare l'identità di qualcuno online. Per iniziare, ecco alcuni esempi.

Nota per gli insegnanti:

Potresti considerare di iniziare a fare un brainstorming di classe partendo dalla domanda: "Come si fa a verificare l'identità di una persona online?". Poi prosegui la conversazione con questi spunti di riflessione.

- La foto del profilo è sospetta? La foto del profilo è sfocata o non si vede bene? Oppure non c'è alcuna foto e al suo posto vi è una bitmoji o il volto del personaggio di un cartone animato? Foto di bassa qualità, bitmoji, foto di animali domestici, ecc. servono a nascondere più facilmente l'identità di una persona sui social media. Inoltre non è difficile per i truffatori rubare foto di persone reali per creare profili falsi e fingere di essere loro. Riuscite a trovare altre foto di quella persona associate allo stesso nome?
- Il nome utente contiene un nome reale? Per esempio, sui social media il nome utente combacia con il nome reale?
- Il profilo contiene una biografia? Se c'è, sembra scritta da una persona reale? Gli account falsi spesso non hanno molte informazioni nella sezione "Su di me" e quelle che ci sono potrebbero essere una serie di informazioni copiate e messe insieme a caso solo per creare un profilo falso. C'è qualcosa sul profilo che potete confermare facendo una ricerca?
- Da quanto tempo esiste questo account? L'attività che vedete combacia con le vostre

aspettative? Si tratta di un profilo nuovo o mostra un gran numero di attività? Questa persona ha amici in comune con voi come pensavate? Gli account falsi di solito non hanno molti contenuti né mostrano segni di socializzazione, post e commenti di altre persone.

Da ricordare

Siamo noi a decidere con chi parlare online. Controlliamo sempre che i nostri interlocutori siano davvero chi dichiarano di essere!

Chi sei veramente?

Scenario 1

Online, ricevi da uno sconosciuto la richiesta di seguirlo. "Ehi! Sembri una persona simpatica. Conosciamoci meglio! Puoi seguirmi? Luca"

Scenario 2

Ricevi sul cellulare un messaggio di testo da parte di qualcuno che non conosci. "Ciao, sono Carlo! Ti ricordi di me, dall'estate scorsa?"

Scenario 3

Ricevi un messaggio da parte di qualcuno che non segui. "Ehi! Adoro i tuoi post, sei TROPPO forte! Dammi il tuo numero di telefono, così possiamo parlare un po'!"

Scenario 4

In chat ti scrive qualcuno che non conosci. "Ti ho visto in corridoio oggi. 6 adorabile! Com'è il tuo indirizzo? Potremmo vederci x fare 2 chiacchiere."

Scenario 5

Ricevi un messaggio online. "Ciao, ho appena incontrato la tua amica Irene! Mi ha parlato di te, mi piacerebbe incontrarti. Dove abiti?"

Riepilogo sul phishing - Attività 2

Chi sei veramente?

Ecco cinque scenari di messaggi che chiunque potrebbe ricevere online o sul proprio telefono. Ogni scenario include un elenco di modi in cui è possibile rispondere, alcuni sono ottimi, altri un po' meno. Leggeteli e vedete se li ritenete appropriati, oppure se vi vengono in mente altre risposte. Se uno di questi scenari dovesse verificarsi realmente e non sapete come comportarvi, la cosa più semplice è non rispondere. Potete sempre ignorare o bloccare queste persone. Inoltre, parlarne con un genitore o con un insegnante non è mai una cattiva idea.

Scenario 1

Ricevi questo messaggio da qualcuno che non conosci: "Ciao! Sembri una persona simpatica. Conosciamoci meglio! Mi aggiungi alla lista dei tuoi amici? Luca." Cosa vuoi fare?

- **Ignorare Luca.** Se non lo conosci, puoi semplicemente decidere di non rispondergli.
- **"Ciao Luca. Ci conosciamo?"** Se hai dei dubbi, puoi fargli delle domande.
- **Bloccare Luca.** Se hai controllato chi è Luca e hai deciso di bloccarlo, non riceverai più i suoi messaggi. Sulla maggior parte delle piattaforme social, non saprà nemmeno che l'hai bloccato.
- **Controllare il profilo di Luca.** Fai attenzione: creare un profilo falso non è difficile! Controlla la lista degli amici di Luca e guarda con chi è connesso. La sua cerchia di amici potrebbe essere un modo per capire se è reale oppure no, specialmente se non conosci nessuno tra i suoi amici! Anche una ridotta attività sulla sua pagina indica che non si tratta di una persona reale.
- **Aggiungere Luca ai tuoi amici.** Questa non è un'opzione consigliata, a meno che tu non abbia verificato chi è insieme a un adulto di cui ti fidi.
- **Dargli informazioni personali.** Non dare mai le tue informazioni personali alle persone che non conosci.

Scenario 2

Ricevi sul cellulare un messaggio di testo da parte di qualcuno che non conosci. "Ciao, sono Carlo! Ti ricordi di me, dall'estate scorsa?" Cosa vuoi fare?

- **Bloccare Carlo.** Questa azione sarebbe considerata scortese, qualora conoscessi questa persona. Ma se non hai la certezza di aver conosciuto una persona di nome Carlo l'estate scorsa o se ti sta mandando troppi messaggi su di sé, bloccarlo potrebbe essere una buona idea.
- **Ignorare Carlo.** Se non conosci questa persona, puoi semplicemente non rispondere.
- **"Ciao Carlo. Ci conosciamo?"** Questa è un'opzione sicura se non hai la certezza di averlo incontrato e vuoi scoprire qualcosa di più. Ma non dire a Carlo dove hai trascorso l'estate scorsa!
- **"Non mi ricordo, ma possiamo comunque vederci, uno di questi giorni."** Pessima idea: non dovresti mai proporre un incontro a qualcuno che non conosci.

[Continua alla pagina successiva →](#)

Scenario 3

Ricevi un messaggio privato da parte di @surfingbird15, una persona che non segui. "Ehi! Adoro i tuoi post, sei TROPPO forte! Dammi il tuo numero di telefono, così possiamo parlare un po'!" Cosa vuoi fare?

- **Ignorare @surfingbird15.** Non devi per forza rispondere, se non vuoi farlo.
- **Bloccare @surfingbird15.** Se ritieni che questa persona sia strana e decidi di bloccarla, non saprai più nulla di lei, a meno che questa persona non crei nuovamente un altro profilo finto e ti contatti sotto falso nome.
- **"Ciao, ci conosciamo?"** Se hai dei dubbi, prima di scrivere le tue informazioni personali, ad esempio il numero di telefono, assicurati di fare delle domande.
- **"Ok, il mio numero è..."** Non farlo! Anche se hai verificato l'identità di questa persona, condividere informazioni personali sui social media non è mai una buona idea.

Scenario 4

In chat ti scrive qualcuno che non conosci. "Ti ho visto in corridoio oggi. 6 adorabile! Com'è il tuo indirizzo? Potremmo vederci x fare 2 chiacchiere." Cosa vuoi fare?

- **Ignorare.** Probabilmente si tratta di una buona scelta.
- **Bloccare questa persona.** Non esitare a farlo, se c'è qualcosa che non ti torna.
- **"Chi sei?"** Probabilmente no. Se il messaggio ti sembra vago, potrebbe essere meglio non rispondere o bloccare il mittente.
- **"Alice, sei tu? Anche tu 6 adorabile! Abito in via Roma 24."** Rispondere in questo modo non è una buona idea, anche se pensi di sapere chi ti ha scritto. Prima di scrivere a qualcuno il tuo indirizzo o altre informazioni personali, verificane l'identità, anche quando pensi che sia una persona che conosci. Non incontrare mai di persona qualcuno con cui hai avuto solo delle interazioni online.

Scenario 5

Ricevi questo messaggio: "Ciao, ho appena incontrato la tua amica Irene! Mi ha parlato di te, mi piacerebbe incontrarti. Dove abiti?" Cosa vuoi fare?

- **Ignorare.** Se non conosci questa persona, ma hai un'amica che si chiama Irene, la cosa migliore da fare è chiedere a lei prima di rispondere a questo messaggio.
- **Bloccare.** Se non conosci questa persona e non hai nessuna amica che si chiama Irene, probabilmente è meglio usare le impostazioni per bloccare questa persona e impedirle di contattarti ancora in futuro.
- **"Chi sei?"** Probabilmente non è una buona idea. Se non conosci questa persona è meglio non rispondere, almeno finché non hai sentito Irene.

A proposito di bot

Gli studenti interagiscono sempre più spesso con delle “voci” non umane provenienti da dispositivi, app e siti. Questo avviene principalmente a casa, ma sempre più frequentemente capita anche nelle scuole. A volte vengono chiamati “chatbot”, altre volte “assistenti virtuali” e spesso solo “bot”. Questa semplice attività di domande e risposte mira a far sì che la classe ragioni ad alta voce sull’interazione con i bot.

Nota per gli insegnanti:

Cerca di non mettere limiti alla discussione; questa attività è pensata per aiutare i ragazzi a sviluppare il pensiero critico, non per trarre conclusioni.

Obiettivi per gli studenti



- ✓ **Scoprire** questo tipo di tecnologia interattiva, sempre più presente nella vita degli studenti.
- ✓ **Identificare** le esperienze con i bot di vario tipo.
- ✓ **Analizzare** l'impatto che queste tecnologie possono avere sulla nostra vita, sia positivo sia negativo.

Spunti di discussione



Al giorno d’oggi sempre più persone utilizzano i bot. Avete già sentito questa parola? Alcune persone li chiamano “chatbot” o “assistenti virtuali”. Sono utilizzati per una miriade di cose, ad esempio nei videogame, per controllare il meteo, trovare risposte a delle domande, ricevere indicazioni stradali, ricevere una notifica per un promemoria, ecc. A volte hanno un nome umano, altre volte il loro nome descrive ciò che sono in grado di fare, ad esempio “Easy English” potrebbe essere un bot che invia ogni giorno una parola in inglese da imparare. I bot sono sui dispositivi mobili, online, nelle auto oppure su dispositivi speciali situati in diverse stanze della casa.

Parlate in classe delle esperienze vissute con i bot a partire dalle seguenti domande:

- Quanti di voi hanno parlato con un bot?
- Per cosa pensate siano più utili i bot (ad es. per chiedere che tempo fa, per sentire le notizie, per fare un gioco, per chiedere informazioni)?
- I bot utilizzano la cosiddetta IA, o intelligenza artificiale. In un certo senso, l’IA impara da ciò che chiediamo, quindi può aiutarci sempre meglio. Per farlo, a volte i bot “ricordano” o registrano quello che chiedete e dite. Questo vi fa riflettere su quali informazioni comunicare e quali invece tenere per voi?
- Pensate che sia come parlare a un essere umano? In che modo è simile e in che modo non lo è?
- Vi è mai capitato di scrivere a un bot con rabbia, magari lamentandovi di qualcosa?
- Se i bot potessero imparare da noi umani, secondo voi cos’è che non dovremmo dire affinché i bot non lo imparino? (Suggerimento: ripensa alle attività di “Utilizza la tecnologia con buon senso” e parla di come siano correlate a questo argomento.)

Attività



Dopo la discussione, sfruttando computer e dispositivi digitali scolastici, gli studenti (individualmente o in gruppo) cercano delle immagini di bot e delle informazioni a riguardo (inclusi articoli di giornali online). I termini di ricerca potrebbero essere “bot”, “chatbot”, “assistenti digitali” o “assistenti virtuali”. La classe stabilirà se le informazioni trovate sono valide.

Da ricordare

Il pensiero critico è uno degli “strumenti” migliori e più duraturi per far sì che il nostro uso della tecnologia sia positivo. La cosa straordinaria è che si tratta di uno strumento che migliora ogni volta che lo utilizziamo. Pensare ad alta voce insieme è un modo divertente, ma anche molto potente, di utilizzare e migliorare quello strumento.

È proprio vero?

Nota per gli insegnanti:

Oltre ad aiutare gli studenti a porsi domande analitiche per valutare la credibilità di una fonte, vogliamo anche che capiscano che l'informazione può provenire da diversi posti. Pertanto, devono applicare le loro abilità per analizzare tutti i tipi di mezzi di comunicazione. Arrivati a quel punto, saranno pronti ad analizzare categorie speciali di mezzi di comunicazione, come le notizie o i dati scientifici.

Obiettivi per gli studenti



- ✓ **Identificare** gli strumenti di cui già si è a conoscenza per capire se un'informazione è attendibile.
- ✓ **Tenere conto** di come determinate cose, quali competenza e motivazione, influiscano sulla credibilità.
- ✓ **Imparare** 4 domande da porsi per valutare la credibilità di una fonte.
- ✓ **Capire** che una fonte attendibile per un determinato argomento potrebbe non esserlo per altri.
- ✓ **Sapere** che la verifica di più fonti spesso aiuta a capire se l'informazione è attendibile o meno.

Spunti di discussione



Di seguito alcuni punti da considerare per avviare una discussione con la classe.

• Cos'è che rende qualcosa o qualcuno attendibile o affidabile

Ogni giorno prendete decisioni su ciò in cui credere e ciò in cui non credere. Il video che avete visto era vero o falso? I vostri fratelli maggiori vi stanno dicendo la verità o vi stanno prendendo in giro? Quella indiscrezione che avete sentito su un vostro amico, è vera?

Cosa fate quando cercate di capire se qualcuno dice la verità? Pensate già a questi suggerimenti?

• Cosa sapete di una persona

Ad esempio, sapete se un compagno di classe è molto bravo in qualcosa o se è sempre stato affidabile oppure se fa degli scherzi o ancora se si comporta da bullo, quindi solitamente siete in grado di capire quando è serio, quando sta scherzando o quando sta mentendo.

• Cosa sa una determinata persona di voi

Ad esempio, i vostri genitori sanno quali tipi di alimenti vi fanno venire il mal di stomaco, quindi seguite i loro consigli su cosa mangiare. Il bibliotecario della scuola conosce i vostri interessi e quali libri vi piacciono, quindi vi fidate dei suoi consigli per le vostre letture future.

• Tono di voce ed espressione del viso

Ad esempio, sapete capire se un vostro amico dice qualcosa ma intende l'opposto, se alza gli occhi al cielo e si comporta in modo strano quando vi dice che è stato un grosso sacrificio trascorrere 15 giorni a Londra per imparare l'inglese.

• La situazione

Ad esempio, quando gli amici stanno giocando e uno di loro vi prende in giro per il vostro nuovo taglio di capelli, sapete che quella è solo una battuta. Però se qualcuno a scuola dice le stesse identiche parole per mettervi a disagio davanti a tutta la classe, sapete che in quel caso si tratta di un insulto.

Quando sentiamo dire certe cose in un video, da una persona alla TV o su un sito web, non conosciamo personalmente la fonte e viceversa. Potremmo anche non sapere con certezza se crederci o meno.

Anche quando qualcuno che conosciamo ci invia un messaggio non abbiamo indizi sulla sua espressione del viso o sul suo tono di voce, quindi non possiamo avere la certezza di ciò che intende dire. È allora che dobbiamo porci delle domande.

Attività



Materiale necessario:

- Scheda didattica "Stabilire cosa è attendibile"

1. Valutare le fonti

Chiedi agli studenti di rispondere alla seguente domanda: "Se tu volessi un consiglio per una tavola da surf, chiederesti a tua madre o a tuo padre?" Oppure, in altre parole, "I tuoi genitori sono una fonte di informazioni attendibile per quanto riguarda le tavole da surf?"

Una fonte attendibile è una fonte di cui possiamo fidarci, dalla quale possiamo aspettarci di ricevere informazioni precise e pertinenti.

Chiedi poi di stilare un elenco di pro e contro come nella tabella qui sotto per spiegare i vantaggi e gli svantaggi di chiedere consiglio ai tuoi genitori rispetto a una tavola da surf.

PRO	CONTRO
I miei desiderano il meglio per me	I miei non hanno mai fatto surf
I miei genitori sono fenomenali nel reperire informazioni	I miei non sanno quale caratteristiche deve avere una tavola da surf per principianti

Se gli elenchi prodotti sono più o meno così, gli studenti hanno utilizzato due degli strumenti più comuni per decidere se una fonte è attendibile: motivazione e competenza. La "competenza" è un'abilità o una conoscenza speciale su un determinato argomento; gli esperti hanno competenza. La "motivazione" è l'intenzione di qualcuno, la ragione per cui dice o fa qualcosa.

Quale elemento dell'elenco dà informazioni sulle motivazioni dei tuoi genitori? Quali elementi dicono qualcosa sulla loro competenza? Quindi, sulla base di questa tabella di pro e contro, i tuoi genitori possono essere considerati una fonte di informazioni attendibile per la scelta della tavola da surf? Di certo, loro non potrebbero mai mentirci, ma probabilmente sarebbe meglio chiedere a qualcuno a cui importa di noi e che conosca il mondo del surf.

Papà cucina molto bene ma non sa assolutamente nulla di moda, l'allenatore conosce il basket ma non la ginnastica artistica, e la nonna sa aggiustare qualsiasi giocattolo ma non sa nulla di videogiochi. **Solo perché qualcuno è esperto in qualcosa non significa che sia esperto in tutto.**

2. I pro e i contro

Chiedi agli studenti di immaginare di voler diventare un grande calciatore o calciatrice, e di essere a caccia di buoni consigli. Chiedi di stilare degli elenchi di pro e contro per ognuno dei personaggi sotto elencati, per poter capire se si tratta di fonti attendibili oppure no:

- La nonna
- Il blog di un allenatore di basket della scuola superiore
- Il capitano della tua squadra
- Un sito web che vende scarpe da calcio e offre consigli
- Dei video che insegnano le tecniche per giocare a pallavolo

Cosa possiamo notare sui punti di forza e sui punti deboli di ciascuna fonte?

- Sa insegnare ma non ha dimestichezza con le abilità calcistiche?
- È esperto/a di calcio ma non sa come si insegna?
- I suoi consigli sembrano volermi spingere all'acquisto di qualche prodotto?
- Conosce bene il calcio ma non conosce te e non sa quali abilità dovresti migliorare?

Discussione: Chi potrebbe rappresentare una buona fonte a cui fare riferimento e perché?

Raramente la credibilità può essere al 100%. In genere tutte le fonti hanno dei punti deboli e dei punti di forza. Ecco perché le risposte migliori si ottengono rivolgendosi a più fonti e confrontando i risultati. Un film su uno tsunami ci fa vedere un'onda gigantesca, più alta di un grattacielo, che corre verso le persone sulla spiaggia. Ma gli tsunami hanno davvero questo aspetto? Un annuncio sottintende che la maggior parte degli scienziati ha i capelli scompigliati, indossa occhiali da vista spessi e camice bianco. È la verità?

3. Passaggi da considerare

Seguendo i 3 passaggi sulla scheda didattica "Stabilire cosa è attendibile", incentrati sui temi di competenza e motivazione, è possibile verificare qualsiasi fonte.

4. A caccia di fonti

Ora è il momento di fare pratica. Fai scegliere agli studenti una domanda collegata a qualcosa di cui si sta parlando in classe oppure che hanno visto online. Dovranno trovare una fonte che fornisca una risposta a quella domanda e, in piccoli gruppi, usare le domande sulla dispensa per stabilire se la fonte è attendibile o meno.

Esempi:

- *Avete bisogno di idee per il regalo di compleanno di un tuo amico. Un annuncio di un negozio locale dice che il suo strumento di ricerca, in grado di trovare tutti gli articoli offerti, può esservi utile per trovare il regalo perfetto. Può fare al caso vostro?*

- *State leggendo delle recensioni online su una nuova pizzeria e vi accorgete che tre delle sei recensioni con 5 stelle sono state scritte da persone che hanno lo stesso cognome del proprietario del locale. Altre due dicono che hanno mangiato la migliore pizza del mondo e una dice che il rapporto quantità-prezzo non è male. Ci sono anche quattordici commenti negativi. Le recensioni positive vi convincerebbero a provare la pizzeria?*
- *Un annuncio pop-up sostiene che fate parte di un piccolo gruppo di utenti selezionati per provare una speciale pillola che vi trasformerà in sirene permettendovi di respirare sott'acqua senza l'attrezzatura per le immersioni. Dovete solo pagare € 9,99 per la spedizione. Cosa fareste?*
- *Vi piacciono molto i video di un famoso vlogger perché sono divertenti, ma a volte dicono cose cattive su diversi gruppi di persone che non vorreste sentire. Continuate a seguirlo perché i video sono divertenti e molto popolari? Pensate che possa influenzare le persone?*

Da ricordare

Non dobbiamo avere paura di fare domande. Quando si pongono le domande giuste sulle fonti e sulle informazioni che esse forniscono, si ricevono informazioni migliori. Più fonti utilizziamo, meglio è. Ricordiamo che se una fonte è ottima per un argomento non significa che lo sia per tutti gli argomenti.

Stabilire cosa è attendibile

Passaggi utili per distinguere le fonti attendibili da quelle non attendibili.

Passaggio 1

Usiamo il buon senso

È una cosa logica? Ha senso?

- Se a) ciò che vedi non ha senso, b) sai per esperienza che non è vero o c) non corrisponde alle cose che sai già, allora non hai bisogno di ulteriori passaggi. La tua fonte non è attendibile, puoi starne certo.

Passaggio 2

Fai delle domande

E non delle domande qualsiasi, ma queste quattro legate alla competenza e alla motivazione:

Competenza

1. Questa fonte mi conosce o mi vuole bene (ed è importante)?

- La risposta a questa domanda dipende dall'informazione che si sta cercando. Se stiamo cercando informazioni sull'inquinamento degli oceani dovuto alle bottiglie di plastica, non importa se la fonte ci conosce. Ma un sito che ci assicura che il nuovo giocattolo in vendita ci piacerà moltissimo, per essere attendibile dovrebbe sapere quali tipi di giochi o attività ci piacciono.

2. Questa fonte conosce bene l'argomento? Come ha imparato queste cose?

- Alcune persone pensano che il modo più semplice di trovare informazioni attendibili sia chiedere a un assistente vocale digitale. Sembra che gli assistenti digitali sappiano tutto! Ma come fanno ad avere tutte quelle risposte? Utilizzano dei calcoli matematici (detti "algoritmi") per trovare le risposte.
- Per delle domande semplici che prevedono una sola risposta (ad esempio la temperatura esterna o il nome di un cantante famoso) in genere sono una fonte attendibile. Ma se la domanda è complicata, sarebbe meglio chiedere prima a una persona o a un gruppo di persone con molta esperienza, o che abbia vinto dei premi o abbia ottenuto un dottorato correlato all'argomento. Poi è possibile usare un assistente vocale per confermare l'informazione (vedi Passaggio 3 a pagina 47).

Motivazione

3. Questa fonte cosa vuole che facciamo o cosa vuole farci credere e perché?

- Questa fonte ci guadagna se seguiamo il suo consiglio? Ad esempio, pensi che un influencer guadagni una percentuale se acquisti il prodotto che indossa o di cui parla? Un atleta professionista indossa una certa marca di scarpe o una maglietta perché è pagato per farlo?
- I soldi spesso possono essere una ragione per cui vediamo il logo o il nome di un brand in un video o annuncio. Questo può influire su ciò che l'influencer o l'atleta ci stanno dicendo (e su cosa non ci sta dicendo). Probabilmente non vogliono ferirci, ma è possibile che per loro guadagnare sia più importante che darci tutte le informazioni o dirci cosa può farci bene.

[Continua alla pagina successiva →](#)

4. Chi potrebbe trarne vantaggio e chi invece esserne danneggiato se credessimo a questa fonte? Non è sempre facile capirlo. Ecco un esempio:

Immaginiamo un annuncio per un'app che ci promette di farci diventare degli studenti migliori.

- Quali sono i possibili vantaggi? Lo sviluppatore dell'app trarrebbe un vantaggio dall'acquisto dell'app perché ci guadagnerebbe dei soldi. E noi potremmo trarne vantaggio se l'app funzionasse davvero.
- Chi potrebbe essere danneggiato se credessimo all'annuncio? Potremmo sprecare dei soldi se comprassimo l'app. Potremmo anche sprecare tempo a fare pratica con le cose sbagliate e addirittura peggiorare a scuola. Oppure potremmo fidarci dell'app, che può solo tirare a indovinare le nostre esigenze, anziché chiedere aiuto a un insegnante, che effettivamente sa di cosa abbiamo bisogno.

Passaggio 3

Conferma

Altre fonti attendibili sostengono ciò che dice questa fonte? Non serve solo verificare più fonti, bensì valutarne la credibilità. Se non riusciamo a trovare una varietà di fonti attendibili che concordano con la fonte che vogliamo verificare, forse questa non è poi così degna della nostra fiducia.

- Utilizzate gli strumenti di ricerca online o la biblioteca della scuola per trovare altre fonti di informazione sull'argomento (le fonti possono essere libri, articoli di riviste, online oppure offline).
- Ripetete i passaggi 1 e 2 sulla base delle nuove informazioni che hai raccolto, poniti le stesse domande anche su queste fonti. Se vi vengono fornite le stesse informazioni sull'argomento, allora è probabile che la fonte sia attendibile.

Disinformazione online, come individuarla

È necessario mettere i ragazzi in condizione di identificare il tipo di contenuti in cui si imbattono e valutare la credibilità della fonte, affinché diventino agenti attivi del cambiamento e della lotta alla disinformazione.

Obiettivi per gli studenti



- ✓ **Identificare** gli indizi che suggeriscono che una fonte di notizie o di informazioni è ingannevole.
- ✓ **Utilizzare** domande analitiche e osservazioni attente per valutare l'attendibilità di una fonte.
- ✓ **Comprendere** l'importanza di controllare l'attendibilità di una fonte prima di condividerne il messaggio.
- ✓ **Sviluppare** l'abitudine di analizzare tutte le notizie e le informazioni, non solo gli articoli che sembrano sospetti.

Spunti di discussione



Avete mai fatto uno di quei giochi in cui bisogna individuare gli errori nascosti in una foto? A volte quando abbiamo a che fare con delle notizie succede la stessa cosa. Ci sono molte persone e gruppi di individui talmente presi da ciò in cui credono da stravolgere la realtà pur di farci arrivare a essere d'accordo con loro. Quando le informazioni distorte vengono mascherate da notizie, parliamo di disinformazione.

Alcune persone non sanno come individuare le informazioni false, ma le condividono ugualmente. È così che si diffondono. E quando le persone scelgono di fare determinate cose o di credere ad altre sulla base di quella disinformazione, cessa di esistere la capacità di parlare in modo calmo, di discutere serenamente, di capire meglio l'altro e di risolvere i problemi.

Dunque, come facciamo a distinguere tra ciò che è reale e ciò che è falso quando vediamo o sentiamo una notizia? Ci sono degli indizi che possiamo imparare a riconoscere, dei trucchetti utilizzati da chi fa disinformazione. E poi ci sono delle domande che possiamo porci per capire quali articoli non sono basati su prove concrete.

Attività



Materiale necessario:

- Scheda didattica "Identificare gli URL fasulli"

1. Prendete la scheda didattica "Identificare gli URL fasulli"

- La prima cosa da fare è guardare l'indirizzo web o l'URL del sito che ha pubblicato la notizia. Alcuni siti fasulli cercano di ingannarti scegliendo nomi che imitano un sito reale ma con qualche lieve differenza. La maggior parte delle aziende usa URL brevi, perché sono semplici da ricordare e da digitare, perciò gli URL con lettere aggiuntive o non necessarie sono spesso fasulli.
- Cerchiate tutti gli URL che pensi siano reali.
- Guardate.... Li avete individuati tutti?

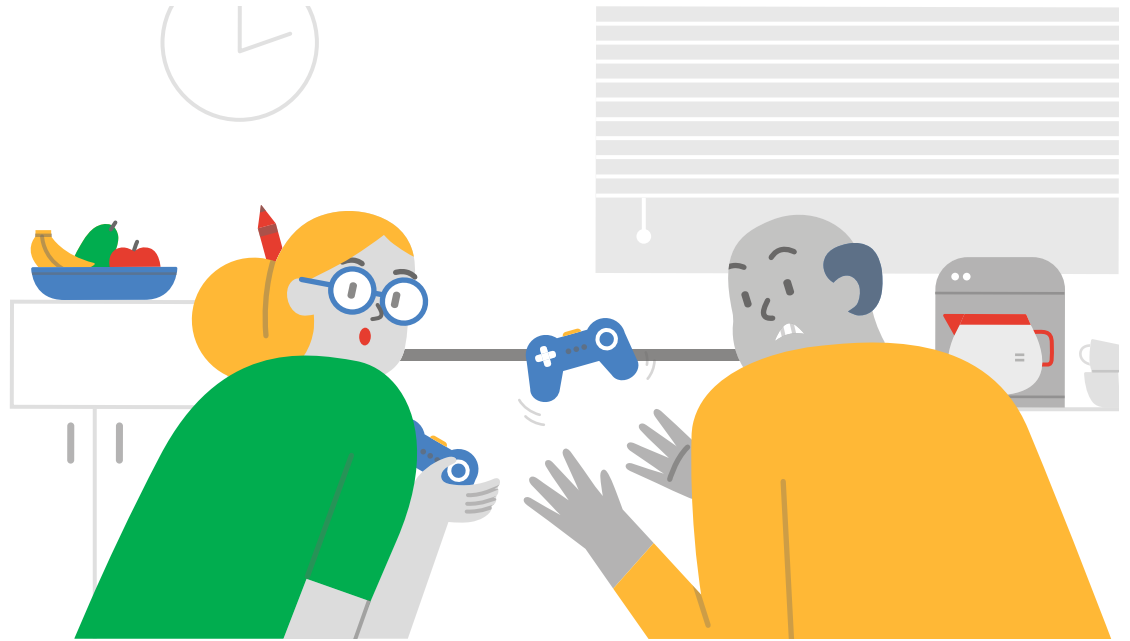
Come si fa a verificare che un URL appartenga a un sito di notizie reale? Una possibilità consiste nel cercare sul Web la testata giornalistica o l'URL. Visita la pagina About e raccogli informazioni sulla testata. Effettua una ricerca sul web con il nome del sito di notizie per verificare se altre fonti la menzionano. Se l'URL non è reale, probabilmente verranno mostrati diversi titoli che segnalano il sito come un titolo fasullo, oppure verrà fuori che il sito non è più disponibile.

2. Attenzione ai titoli

A volte le persone condividono notizie senza riportarne l'URL. In questi casi, ecco alcuni elementi a cui prestare attenzione:

- a. Un articolo inizia con l'immagine di qualcosa che potrebbe interessarci, ad esempio un cagnolino, un personaggio famoso o una strana trovata, ma quando facciamo clic, l'articolo che si apre ha poco o nulla a che vedere con l'immagine.
- b. Spesso post e notizie vengono condivisi usando formattazioni speciali come il grassetto, il MAIUSCOLO, le sottolineature o i punti esclamativi, per farci credere che quello che stiamo osservando sia importante. I veri giornalisti non fanno uso di questo tipo di formattazione.
- c. Per farci leggere una notizia, alcune persone includono nel titolo parole quali "sconvolgente", "sorprendente" o "scandaloso". Sanno che parole come queste ci incuriosiscono. Ma i giornalisti veri lasciano che la notizia parli da sé. Raccontano la notizia e ci lasciano stabilire se è sconvolgente o sorprendente.

Osservate questa immagine e il titolo



La scioccante verità su cosa fanno i docenti terminate le lezioni

Senza proseguire oltre, cosa pensate ci sia scritto nell'articolo? Perché lo pensate? Che prova avete?

[Continua alla pagina successiva →](#)

Ecco la notizia: “(2019) - Un recente sondaggio dell'Università della Terra di Mezzo ha rivelato che l'86% degli insegnanti, dopo il lavoro, fa quello che fanno tutti. Fa delle commissioni, prepara la cena, trascorre del tempo con la famiglia, sbriga le faccende domestiche e si prepara per il giorno successivo. Ma di recente, molti insegnanti hanno iniziato a fare qualcosa di inaspettato.

Un decennio fa, a causa dei problemi economici, molti Stati hanno tagliato i fondi per l'istruzione. Ciò ha comportato il blocco degli aumenti di stipendio per gli insegnanti. Poiché lo stipendio basso non permette di coprire tutte le spese principali, molti insegnanti adesso hanno un secondo lavoro. In alcune zone del paese hanno persino scioperato per chiedere un aumento di stipendio e riuscire così a lasciare il secondo lavoro e dedicare più tempo ai propri studenti.”

....come vi aspettavate che fosse? Pensate che....? Che prova avete?

3. Attenzione alle fonti

Quando analizziamo le notizie, ci sono degli indizi che possono venirci in aiuto, ma spesso non sono sufficienti. A volte le notizie vere usano alcune tecniche per attirare la nostra attenzione, e questo potrebbe farci pensare che siano false. Viceversa, alcune fonti false riescono a copiare talmente bene quelle vere che è difficile riuscire a distinguerle. Non è facile capire la differenza. Leggi i nomi delle testate di seguito: quali pensi siano reali e quali fittizi?

- TG Italia
- RaiNews24
- L'Osservatore italiano
- World News
- Daily Report
- Bollettino settimanale
- Notizie24

In realtà, solo RaiNews24 è reale. Come scoprirlo? Possiamo cominciare facendo una ricerca web del nome della testata. Vediamo dove appare al di fuori del sito web della testata. Se viene mostrato su Wikipedia o in un articolo su una rivista o sul sito di un giornale, probabilmente si tratta di una testata reale. Ma è bene leggere sempre questi articoli! Magari ci dicono che si tratta di una testata falsa.

4. Mettetevi alla prova

Trovate una notizia sulla vostra scuola, sulla vostra città, su una dieta di tendenza o un'altra notizia che vi interessa. Seguite i 3 passaggi sulla scheda didattica "Stabilire cosa è attendibile" e i nuovi trucchetti che hai imparato per capire se la notizia è vera o ingannevole.

Passaggio 1

Usate il buon senso

Ponetevi la domanda: è logico? Ha senso?

A volte l'inganno è palese. Se vedete un titolo del tipo MATRIMONIO SPAZIALE: VIP SPOSA UN ALIENO IN SEGRETO, la logica vi dirà probabilmente che non si tratta di una notizia reale.

Altre volte invece non è così scontato. Se: a) ciò che vedete non ha senso b) sapete che non è vero per tua esperienza, oppure c) non combacia con le notizie di cui siete a conoscenza, la vostra fonte probabilmente è fasulla.

Passaggio 2

Ponetevi le domande relative a motivazione e competenza (pag. 41)

Passaggio 3

Verificate

Ponetevi la domanda: altre fonti attendibili sostengono ciò che dice questa fonte?

Chi altri sta riportando questa notizia? Quali altre notizie include il sito? Le notizie offrono tutte la stessa prospettiva o ci sono vari punti di vista? Se non si trovano più fonti affidabili che trattano la stessa notizia, sarebbe corretto essere scettici nei confronti di quella fonte.

Da ricordare

Adesso che sapete come utilizzare i trucchi e le domande da porvi per individuare le informazioni false, potete usare l'osservazione attenta e la capacità d'indagine nella vita di tutti i giorni. Potete analizzare tutte le informazioni che trovate online e condividere i risultati con amici e parenti. Potete davvero essere cittadini intelligenti, rispettosi e rispettabili!

Identificare gli URL fasulli

Vero o falso?

Cerchia la risposta corretta.

tgcom24.mediaset.it	Vero	Falso
rainews24.if	Vero	Falso
larepubblica.it	Vero	Falso
rainews24.italia.com	Vero	Falso
tg24.sky.it	Vero	Falso
rainews24.it	Vero	Falso
corriereufficiale.it	Vero	Falso
la7.com.tg	Vero	Falso
ilmessaggero.it	Vero	Falso
corriere.it	Vero	Falso
larepubblica.com.co	Vero	Falso
rainews.notizie/finanza	Vero	Falso
tg.la7.it	Vero	Falso
tgcom24.mesiaset.com	Vero	Falso

Soluzioni

Vero

rainews24.it
tg24.sky.it
tg.la7.it
corriere.it
ilmessaggero.it
tgcom24.mediaset.it

Falso

rainews24.if
rainews24.italia.com
la7.com.tg
corriereufficiale.it
rainews.notizie/finanza
larepubblica.it
larepubblica.com.co
tgcom24.mesiaset.com

Impara a distinguere il vero dal falso - Attività 6

Sviluppare spirito critico

Il dibattito è una metodologia molto efficace, non solo per quanto riguarda l'ambito delle competenze cognitive, ma anche di quelle relazionali.

Obiettivi per gli studenti



- ✓ **Lavorare** in gruppo.
- ✓ **Partecipare** attivamente.
- ✓ **Sostenere** il proprio punto di vista.
- ✓ **Ascoltare** e dialogare con gli altri gestendo la propria emotività.
- ✓ **Coinvolgere** e convincere l'audience.

Spunti di discussione



Il dibattito come metodo educativo è molto efficace perché non solo impegna i partecipanti ad approfondire il tema da trattare, ma li stimola a ricercare ulteriori informazioni e fonti a sostegno dei diversi argomenti. Attraverso il dialogo, il confronto e la ricerca attiva, la pratica del dibattito favorisce il miglioramento delle capacità argomentative e la comprensione critica dei giovani.

Attività



1. Titolo attività

- Dividi la classe in gruppi di lavoro omogenei dal punto di vista numerico e individua un mediatore.
- Assegna un tema.
- Ogni gruppo raccoglie dati a supporto delle proprie argomentazioni.
- Aprite un dibattito in classe guidato dal mediatore.

Da ricordare

La fase della valutazione tra pari è un importante momento finalizzato al miglioramento delle conoscenze e competenze e al coinvolgimento attivo degli studenti, che possono così passare per una costruzione autonoma di senso anziché subire passivamente.

Regole della buona informazione

1. Diffidate dai titoli altisonanti, usati per attrarre l'attenzione degli utenti e che spesso nascondono informazioni poco attendibili.
2. Leggete tutta la notizia e non fermatevi al titolo, in quanto i titoli rispecchiano solo parzialmente il contenuto di una notizia.
3. Fate una ricerca sulla fonte per verificarne l'attendibilità.
4. Eseguite un controllo incrociato e confrontate più fonti giornalistiche.
5. Controllate che l'URL sia corretto e che sia presente il protocollo di sicurezza https.
6. Fate attenzione alla formattazione di una pagina web: refusi e layout inusuali spesso segnalano contenuti di bassa qualità.
7. Verificate data e località di una notizia: potrebbe trattarsi di un contenuto datato o di un evento avvenuto in luoghi geografici diversi da quelli descritti.
8. Fate attenzione alle foto e ai video e verificate l'autenticità delle foto.
9. Assicuratevi che la notizia riportata non sia uno scherzo.
10. Rifletti prima di condividere o commentare una notizia facendola così diffondere.



Custodisci le tue informazioni personali

Alcuni dati reali su privacy e sicurezza

Panoramica della lezione

Attività 1: **Come creare una password perfetta**

Attività 2: **Tienilo per te**

Temi

Non sempre sono sufficienti o del tutto corrette le misure che adottiamo per garantire la nostra sicurezza online. Tenere al sicuro le informazioni personali e difendere la propria privacy nella forma più adeguata implica il porsi delle domande e, acquisendo nuove conoscenze, trovare le risposte più adatte.

Obiettivi per gli studenti

- ✓ **Imparare** l'importanza della privacy e il suo legame con la sicurezza online.
- ✓ **Esercitarsi** a creare password efficaci.
- ✓ **Scoprire** gli strumenti e le impostazioni per proteggersi da hacker e altre minacce.

Come creare una password perfetta

Gli studenti imparano a creare una password efficace e a mantenerla segreta.

Obiettivi per gli studenti



- ✓ **Riconoscere** l'importanza di non condividere le password, tranne che con genitori o tutori.
- ✓ **Capire** l'importanza del blocco schermo per proteggere i dispositivi.
- ✓ **Imparare** a creare password difficili da indovinare ma facili da ricordare.
- ✓ **Scegliere** impostazioni sulla sicurezza adeguate relativamente all'accesso, tra cui la verifica a due fattori.

Spunti di discussione



Meglio prevenire che curare

La rivoluzione digitale degli ultimi anni ha consentito ai ragazzi di accedere a informazioni e servizi online, e di comunicare con amici, compagni, insegnanti in qualsiasi parte del mondo.

Tuttavia gli stessi strumenti potrebbero permettere anche ad hacker e malintenzionati di rubare informazioni e usarle per danneggiare i nostri dispositivi, le nostre relazioni o la nostra reputazione. Adottando semplici ma importanti misure come usare il blocco schermo sui nostri dispositivi, fare attenzione alle informazioni personali che inseriamo che potrebbero andare perse o venire rubate e, soprattutto, scegliere delle password efficaci, possiamo proteggere la nostra privacy e la nostra reputazione.

È vero, siamo sommersi da codici, chiavi segrete di accesso a social network, email, piattaforme di musica o film in streaming, videogame, e per questo spesso utilizziamo la stessa password, certi che nessuno potrà mai scoprirla. Basti pensare che nel 2019 e per il sesto anno di fila, la password più usata al mondo è stata «123456». Difficile?

Altre password inefficaci possono essere il proprio nome scritto per intero, la propria data di nascita, il proprio numero di telefono e altre informazioni personali a cui altri potrebbero risalire.

Attività



Materiale necessario:

- Dispositivi dotati di connessione a Internet (uno a testa o uno per ogni gruppo di studenti)
- Una lavagna o un proiettore
- Scheda didattica: "Linee guida per creare password efficaci"

1. Leggete in classe la seguente storia

Diego, come rappresentante di classe, è stato incaricato di creare un account di posta su Gmail a cui tutti i compagni di classe potranno accedere e dove i loro insegnanti potranno inviare mail con materiale e suggerimenti. Diego, al momento di scegliere la password utilizza quella usata solitamente per i suoi account personali, per differenziarla aggiunge solo l'anno corrente e la condivide con i suoi compagni di gruppo.

Dopo una settimana nota che la sua immagine, su uno dei profili social è cambiata. Si tratta di una foto piuttosto imbarazzante che lo ritrae ad una festa, lui è certo di non averla mai usata come immagine del profilo. Prova ad accedervi senza riuscirci. Qualcuno ha eseguito l'accesso e cambiato la password. Si preoccupa perché quella è anche la password di altri account tra cui quello di posta elettronica.

Cosa dovrebbe fare a questo punto Diego? Riflettete sulle possibili azioni da intraprendere.

- Attivare su tutti i siti dove dispone di un account la verifica in due passaggi, laddove possibile? (Abilitare la verifica in due passaggi è ormai possibile su tutti gli account di posta elettronica e sui canali social, oltre che su moltissimi siti di e-commerce.)
- Verificare sulla pagina di assistenza del provider di posta l'esistenza di un metodo di recupero password alternativo? (Anche senza aver abilitato l'autenticazione a due fattori, sugli account di posta elettronica è quasi sempre possibile recuperare la password tramite un'apposita procedura di recupero che prevede l'inserimento di dati come password precedenti, risposte di sicurezza, data di creazione dell'account, ecc.)
- Cancellare o chiudere i suoi account e profili con password simili a quella violata? (Non occorre cancellare gli altri account; è sufficiente modificare le password e abilitare l'autenticazione a due fattori dove possibile.)
- Modificare in maniera sostanziale le password simili a quella hackerata usate per accedere ad altri account? (Non è bene utilizzare la stessa password, sebbene leggermente modificata, per registrarsi su diversi siti. Questa prassi agli hacker o ai malintenzionati è ben nota.)
- Aprire un nuovo account e rinunciare subito ad accedere al vecchio? (Creare un nuovo account e rinunciare al recupero del vecchio è davvero l'extrema ratio, da considerare solo quando è risultato impossibile recuperare la password del vecchio. È meglio fare tutti i tentativi di recupero possibili quando si ha la certezza di avere email con dati sensibili, copie di documenti, fotografie personali.)

2. Create password efficaci

Dividi la classe in coppie. Ogni coppia avrà a disposizione 60 secondi per creare una password. (Opzione sfida: gli studenti condividono degli indizi con la classe per vedere quante informazioni sul contesto sono necessarie per poter fare un'ipotesi corretta sulla password).

3. Confrontate le password

Due squadre alla volta scriveranno la propria password alla lavagna.

4. Ai voti!

Per ogni coppia di password la classe voterà e stabilirà qual è la più sicura.

Linee guida per creare password efficaci

Ecco alcuni suggerimenti per creare password che permetteranno di mantenere le nostre informazioni al sicuro.

Linee guida

Le password efficaci si basano su una frase o un enunciato descrittivi che sono semplici da ricordare e difficili da indovinare per gli altri e includono una combinazione di lettere, numeri e simboli. Ecco alcuni suggerimenti per creare password che permetteranno di mantenere le nostre informazioni al sicuro.

Crea acronimi a partire da una frase semplice, ma ben rappresentativa della tua identità.

Es. *Mia madre è veterinaria e ha 3 gatti* - Potrebbe diventare - **MmEVeH3g**

Costruisci una frase-password: realizza un'unica stringa a partire da una frase composta e poco prevedibile, ad esempio eliminando gli spazi e aggiungendo numeri e/o lettere maiuscole all'inizio di ogni parola.

Es. *Come cadono le foglie* - Potrebbe trasformarsi in - **C0meCadon0LeF0glie**

Es. *Pizza 5 stagioni* - Potrebbe trasformarsi in - **Pizza.5.Stagioni**

Prendi la tua solita password e aggiungi caratteri extra alla fine (si chiama padding)

Es. *Come cadono le foglie* - Potrebbe diventare - **ComeCadonoLeFoglie+10** oppure **Come,Cadono,le,Foglie,10**

Potresti creare una password adottando tutte queste pratiche contemporaneamente.

MmEV.H3g.<3Pizza.5.Stagioni_

Mia madre
è veterinaria

Ha 3 gatti

Ama la pizza 5 stagioni

Questa tipologia di password risulta particolarmente difficile da violare e riprodurre.

Le password mediamente efficaci sono abbastanza sicure e un software dannoso non dovrebbe riuscire a indovinarle facilmente, ma qualcuno che ti conosce potrebbe riuscirci.

Le password poco efficaci contengono solitamente informazioni personali, ad esempio il nome di un animale domestico, un software può facilmente eseguirne il crack e chi ti conosce le può indovinare con semplicità (ad es. "Proprio Nome+data di nascita" o "nome dell'animale domestico").

Cosa fare

- Usa una password diversa per ognuno dei tuoi account importanti.
- Usa almeno otto caratteri. Creane una che sia più lunga possibile (l'importante è che la ricordi!).
- Usa combinazioni di lettere (maiuscole e minuscole), numeri e simboli.
- Fa' in modo che le password siano facili da ricordare, così non dovrai scriverle ed eviterai altri rischi.
- Modifica immediatamente la password se hai la certezza o credi che qualcuno la sappia, al di là di un adulto di cui ti fidi.
- Usa sempre blocchi schermo efficaci sul tuo dispositivo. Imposta i dispositivi in modo che si blocchino automaticamente qualora finiscano nelle mani sbagliate.

Prendi in considerazione l'uso di un gestore delle password, ad esempio quello integrato nel browser, per ricordarti le password. In questo modo potrai usare password univoche per ogni tuo account e non dovrai ricordarle tutte.

Cosa non fare

- Non usare informazioni personali (nome, indirizzo, email, numero di telefono, cognome di tua madre da nubile, date di nascita e così via) o parole di uso comune nella tua password.
- Non usare una password facile da indovinare, come il tuo soprannome, il solo nome della tua scuola, la tua squadra del cuore, il nome del tuo fidanzato/fidanzata, una fila di numeri (del tipo 123456) o simili. E, ovviamente, non usare la parola "password"!
- Non condividere la tua password con nessuno a parte i tuoi genitori o i tuoi tutori.
- Non scrivere mai le tue password in posti in cui qualcuno potrebbe trovarle.

Tienilo per te

Utilizzando un dispositivo scolastico, prova a spiegare alla classe quali sono e dove trovare le impostazioni sulla sicurezza da modificare.

Obiettivi per gli studenti



- ✓ **Personalizzare** le impostazioni sulla privacy dei vari servizi online utilizzati.
- ✓ **Decidere** quali informazioni condividere sui siti e i servizi online utilizzati.
- ✓ **Imparare** cosa sono l'autenticazione a due fattori e la verifica in due passaggi e quando è opportuno usarle.

Spunti di discussione



Privacy equivale a sicurezza

Privacy online e sicurezza online vanno di pari passo. Quasi tutti i software e le app offrono la possibilità di controllare le informazioni che condividi e in che modo lo fai.

Quando usiamo un'app o un sito, cerchiamo opzioni tipo "Il mio account" o "Impostazioni". È lì che possiamo trovare le impostazioni sulla privacy e di sicurezza che ci consentiranno di decidere:

- Quali informazioni rendere visibili sul nostro profilo
- Chi può vedere i nostri post, foto, video e gli altri contenuti che condividiamo.

Impariamo a usare queste impostazioni e ricordiamo sempre che mantenendole aggiornate, potremo proteggere più facilmente la nostra privacy e la nostra sicurezza. È importante sapere che, nel caso dei ragazzi, sono i genitori o tutori i responsabili di queste decisioni.

Attività



Materiale necessario:

- Un dispositivo scolastico collegato a un proiettore in grado di mostrare alla classe un esempio di account impostato in modo appropriato (ad es., un indirizzo email temporaneo o un account su un sito web)

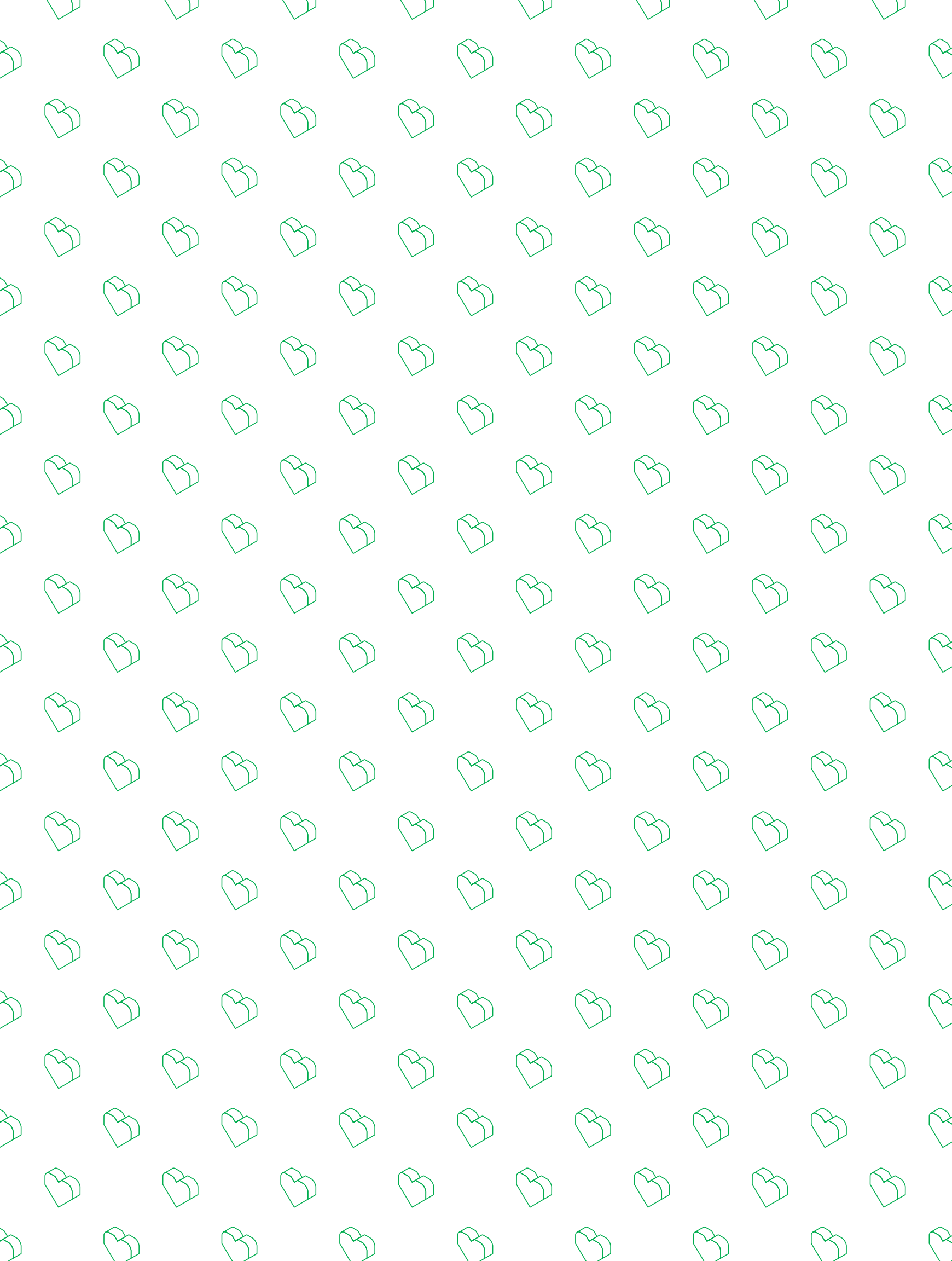
Collega il pc, tablet o smartphone della scuola al proiettore. Vai alla pagina delle impostazioni di questa app per vedere quali sono le opzioni attive. Chiedi ai ragazzi di dirti dove devi cliccare per:

- Modificare la password
- Scorrere le impostazioni di condivisione, posizione ecc. e capire quali fanno al caso tuo
- Ricevere una notifica quando qualcuno prova ad accedere al tuo account da un dispositivo sconosciuto
- Rendere il tuo profilo online, inclusi foto e video, visibile solo a parenti e amici che scegli tu
- Attivare l'autenticazione a due fattori o la verifica in due passaggi
- Impostare le informazioni di recupero nel caso in cui non riuscissi più ad accedere al tuo account.

Da ricordare

È bene ricordare che l'impostazione di sicurezza più importante è nella nostra testa: siamo noi a scegliere quante informazioni personali condividere, quando e con chi.

Scegliere una password efficace diversa per ogni account importante è un ottimo primo passo. Adesso bisogna imparare a ricordare le proprie password e mantenerle riservate.



Diffondi la gentilezza

La forza della positività online

Panoramica della lezione

Attività 1: **Da testimoni a difensori**

Attività 2: **Cosa fa un difensore**

Attività 3: **Scherzo o bullismo?**

Attività 4: **Dillo con più tatto!**

Attività 5: **Usa il tono giusto**

Attività 6: **Sfidare l'odio in rete**

Temi

Il mondo digitale crea nuove sfide e opportunità di interazione sociale, per i ragazzi e per tutti noi. L'apparente garanzia di anonimato e l'assenza di una relazione faccia a faccia in rete può incoraggiare comportamenti negativi e atti di bullismo che tuttavia lasciano tracce indelebili. Allo stesso modo Internet può diventare un amplificatore di gentilezza. Per questo è importante comunicare con cortesia ed empatia, anche in risposta a eventuali comportamenti negativi e offensivi, per costruire relazioni sane e ridurre il senso di isolamento che può sfociare in episodi di bullismo, depressione, difficoltà scolastiche o altri problemi. È compito degli adulti insegnare ai più giovani a costruire relazioni positive anche in rete, e incoraggiarli a chiedere aiuto e uscire dal silenzio in caso di episodi di violenza o di odio, offline e online.

Queste attività incoraggiano gli studenti a interagire in modo positivo fin dalle prime esperienze online e insegnano loro a gestire i potenziali comportamenti negativi.

Obiettivi per gli studenti

- ✓ **Definire** cosa significa essere positivi e comportarsi in modo positivo, sia online che offline.
- ✓ **Mettere** in pratica comportamenti positivi durante la comunicazione online.
- ✓ **Identificare** le situazioni in cui è necessario consultare un adulto di cui ci si fida.

Diffondi la gentilezza

Vocabolario

Bullismo: comportamento intenzionalmente scorretto, in genere ripetuto. La persona che viene presa di mira spesso ha difficoltà a difendersi.

Cyberbullismo: bullismo che si verifica online o attraverso i dispositivi digitali.

Molestia: un termine più generico rispetto a bullismo che può assumere varie forme: infastidire, intimidire, umiliare, assillare ecc. e che può avvenire anche online.

Conflitto: una discussione o un disaccordo che non necessariamente si ripete.

Aggressore: la persona che mette in atto la molestia o l'episodio di bullismo; sebbene a volte venga definito "bullo", gli esperti di prevenzione del bullismo suggeriscono di non etichettare mai così questo genere di persona.

Vittima: la persona che subisce un episodio di bullismo o che viene perseguitata.

Testimone: il testimone di una molestia o di un episodio di bullismo che si rende conto della situazione ma sceglie di non intervenire.

Difensore: il testimone di una molestia o di un episodio di bullismo che sostiene l'obiettivo privatamente o pubblicamente, a volte cercando anche di fermare e/o segnalare la situazione a cui ha assistito.

Amplificare: aumentare o ampliare la partecipazione o l'impatto.

Esclusione: una forma di molestia o bullismo che avviene online e offline; spesso detta "esclusione sociale".

Blocco: un modo per terminare tutte le interazioni con un'altra persona online, impedendole di accedere al proprio profilo, inviare messaggi, vedere i propri post ecc. senza che ne sia a conoscenza (non sempre è una scelta ideale in situazioni di bullismo in cui il bersaglio vuole sapere cosa sta dicendo l'aggressore o quando l'atto di bullismo si conclude).

Disattivazione delle notifiche: meno definitiva del blocco, la disattivazione delle notifiche è un modo per non vedere più i post, i commenti ecc. di una persona sul proprio feed di social media quando quel tipo di comunicazione diventa fastidiosa. La persona non riceverà alcun avviso e il proprio profilo non verrà disattivato per l'aggressore (inutile in casi di bullismo).

Anonimo: una persona sconosciuta o senza nome, qualcuno online di cui non si conosce il nome né l'identità.

Trolling: pubblicare o commentare online in modo deliberatamente crudele, offensivo o provocatorio.

Segnalare una molestia: utilizzare gli strumenti o il sistema online di un social media per segnalare una molestia, un atto di bullismo, minacce e altri contenuti pericolosi che in genere violano i termini di servizio del servizio o gli standard della community.

Didascalia: testo che accompagna un'immagine e fornisce informazioni su ciò che è ritratto nell'immagine.

Contesto: informazioni aggiuntive su una fotografia o altre informazioni che ci aiutano a capire meglio cosa stiamo vedendo. Il contesto può includere informazioni quali il luogo in cui è stata scattata la foto, l'orario di invio di un messaggio, la situazione in cui si trovava il mittente ecc.

Da testimoni a difensori

Vittime, autori e testimoni di atti di cyberbullismo spesso nascondono l'accaduto, e per genitori e insegnanti è difficile individuare il problema. Spesso è proprio a causa dell'omertà che lo circonda, che il bullismo riesce a trovare terreno fertile per crescere e perpetrarsi. Per questo è importante far comprendere ai ragazzi che nel caso in cui si trovassero a osservare episodi di bullismo, prendendo le difese della vittima potrebbero contribuire a stroncarli sul nascere.

Obiettivi per gli studenti



- ✓ **Identificare** situazioni di molestie o bullismo online.
- ✓ **Valutare** cosa significa avere il ruolo di testimone o di difensore online.
- ✓ **Imparare** strategie specifiche per rispondere agli episodi di bullismo a cui si potrebbe assistere.
- ✓ **Capire** come comportarsi nel caso in cui si subissero delle molestie.

Spunti di discussione



Perché è importante essere gentili?

È importante ricordare a noi stessi che dietro a ogni nome utente e dietro a ogni avatar c'è una persona reale, che prova sentimenti reali e che dobbiamo trattare come vorremmo essere trattati noi. Quando si verificano episodi di bullismo, il più delle volte sono coinvolte quattro figure:

- C'è l'aggressore, o la persona che si comporta da bullo.
- C'è la vittima, o la persona che subisce l'episodio di bullismo.
- Ci sono i testimoni, ovvero coloro che osservano ciò che sta accadendo.
- E poi ci sono i difensori, coloro che assistono all'episodio e cercano di intervenire in modo positivo.

Ecco alcune cose che possiamo fare se ci capita di essere vittime di bullismo o di altri comportamenti scorretti online:

Se sono la vittima, posso:

- Evitare di rispondere
- Bloccare la persona
- Segnalare la persona a un genitore, insegnante, fratello o qualcun altro di cui mi fido e utilizzare gli strumenti di segnalazione dell'app o del servizio per segnalare il post, il commento o la fotografia molesti.

Se ti ritrovi a essere testimone di un episodio di molestia o bullismo, puoi intervenire e segnalare il comportamento scorretto. A volte i testimoni non cercano di fermare l'atto di bullismo né di aiutare la vittima, ma quando lo fanno si comportano da difensori. Puoi scegliere di essere un difensore, astenendoti dal supportare il comportamento scorretto e facendoti portavoce di gentilezza e positività. Piccoli gesti di gentilezza possono fare una grande differenza online. In questo modo puoi evitare la diffusione della negatività, e la crudeltà e il dolore che ne conseguono.

Se sono un testimone, posso intervenire...

- Trovando un modo di essere gentile o sostenendo la persona vittima della molestia
- Richiamando il comportamento scorretto in un commento o in una risposta (ricorda di

richiamare il comportamento, non la persona), se mi sento a mio agio e penso che non ci siano rischi nel farlo.

- Decidendo di non aiutare l'aggressore, non promuovendo il bullismo né peggiorando la situazione con la condivisione del post o del commento molesto online.
- Convincendo un gruppo di amici a essere gentili, pubblicando tantissimi commenti carini sulla persona vittima di bullismo (ma niente di cattivo nei confronti dell'aggressore, perché si vuole dare il buon esempio, non vendicarsi), innescando una reazione a catena di positività.
- Segnalando la molestia. Posso riferirlo a una persona in grado di aiutarmi, ad esempio un genitore, un insegnante o un consulente scolastico.

Attività



Materiale necessario:

- Scheda didattica: "Da testimoni a difensori"

Risposte della scheda didattica "Da testimoni a difensori":

Scenario 1: T, D, T (perché non aiuta durante l'episodio), D, D

Scenario 2: D, T, D, D

Scenario 3: D, D, T, T, D

Scenario 4: Sei tu a stabilire le risposte!

1. Leggete gli scenari e suddividete le risposte per categoria

Dopo aver discusso dei ruoli, distribuisce la scheda didattica e concede agli studenti 15 minuti per leggere i tre scenari e assegnare ogni risposta a una categoria. Se c'è abbastanza tempo, chiedi loro di creare un quarto scenario tutti insieme.

2. Parlate della risposta

Prima o al termine della discussione, chiedi agli studenti se sanno dirti perché può essere una buona idea avere dei difensori sia a scuola sia online.

3. Parlate degli scenari difficili da suddividere per categorie

Se c'è abbastanza tempo, chiedi agli studenti se qualche risposta è stata difficile da categorizzare e perché. Avvia una discussione a riguardo.

Da ricordare

Difendere qualcuno che viene attaccato, segnalare i contenuti offensivi, ignorare le provocazioni per evitare che si amplifichino... Sono molte le strategie che possiamo adottare, a seconda della situazione in cui ci troviamo. Con un po' di gentilezza, tutti noi possiamo fare la differenza e risolvere una situazione spiacevole.

Da testimoni a difensori

Adesso sappiamo che un semplice testimone può sfruttare le proprie potenzialità per fare del bene e difendere chi ha bisogno di aiuto in un episodio di bullismo. Di seguito sono riportati tre scenari di esempio di atteggiamenti di bullismo o molestia online. Proponi alla classe di creare anche un quarto scenario verificatosi con persone reali e inventare delle risposte che prevedano azioni sia da “testimone” sia da “difensore”.

Ciascuno dei tre scenari proposti è accompagnato da un elenco di risposte. Chiedi agli studenti di leggere ogni risposta e stabilire se si tratta di qualcosa che farebbe un testimone o un difensore: possono inserire la “T” per “testimone” e la “D” per “difensore” nella casella bianca accanto a ogni frase. Se c’è abbastanza tempo, parlate insieme delle risposte per le quali è stato più difficile decidere e perché.

Scenario 1

Una tua amica ha lasciato il telefono nella palestra della scuola. Qualcuno l’ha trovato e ha inviato un messaggio molto cattivo su un’altra studentessa a un gruppo di persone della sua classe, poi ha rimesso il telefono dov’era. La studentessa vittima della molestia ha detto alla tua amica che inviando quel messaggio si è comportata in modo scorretto, anche se non è stata lei a inviarlo. Nessuno sa chi ha inviato il messaggio molesto. Tu...

- ☐ Ti senti triste per la tua amica ma non fai nulla perché nessuno sa chi sia l’autore di questa cattiveria.
- ☐ Vai a cercare la vittima e le chiedi come si sente e come puoi esserle d’aiuto.
- ☐ Diffondi cattiveria condividendo il messaggio molesto con altri amici.
- ☐ Tu e la tua amica chiedete a tutta la squadra di pubblicare dei complimenti sulla persona vittima di molestia.
- ☐ Tu e la tua amica segnalate l’incidente in maniera anonima al vostro preside, dicendogli che tutti devono essere a conoscenza delle prassi per tenere al sicuro e bloccare il proprio telefono.

Scenario 2

Per un progetto scolastico la tua insegnante ha creato un canale YouTube con video di alcuni studenti che raccontano di viaggi fatti in luoghi lontani. Sotto uno di questi video cominciano a comparire commenti cattivi e offensivi da parte di alcuni studenti della scuola. L’insegnante non se n’è ancora accorto. Tu...

- ☐ Lasci un commento sotto i commenti negativi scrivendo cose come: “Finiamola con queste offese!”.
- ☐ Ignori la situazione fino a che non interviene l’insegnante.
- ☐ Chiedi ad altri studenti di pubblicare commenti positivi e complimenti sullo studente preso di mira.
- ☐ Dici all’insegnante che si stanno verificando comportamenti scorretti sul canale dedicato al progetto.

Scenario 3

Un gruppo di amici gioca spesso online a un particolare gioco. Di solito la chat del gioco è usata principalmente per parlare di ciò che avviene durante le partite. A volte si crea un ambiente ostile, ma nella maggior parte dei casi si tratta di sana rivalità tra amici, nulla di realmente offensivo. Stavolta, però, un giocatore inizia a dire cose molto cattive su uno dei tuoi amici che sta giocando insieme a voi, e non ha intenzione di smettere. Continua anche il giorno successivo. Tu...

- ☐ Richiami il tuo amico dicendogli che non ti piace più di quanto non piaccia a lui e gli chiedi cosa pensa che dovrete fare.
- ☐ Chiami tutti quelli che conosci che giocano con voi (assicurandoti che il vostro amico sappia che lo state facendo) per vedere se si riesce a trovare un accordo e si decida di smettere di comportarsi in modo scorretto.
- ☐ Decidi di aspettare e vedere se il giocatore la smette, poi forse farai qualcosa.
- ☐ Abbandoni il gioco per un po'.
- ☐ Consulti le regole della community del gioco e, se il bullismo non è contemplato, segnali il comportamento scorretto tramite il sistema di segnalazione del gioco.

Scenario 4

Crea uno scenario verosimile con la classe, basandoti su una situazione raccontata da qualcuno, poi inventa delle risposte da "testimone" e "difensore" per dimostrare che adesso è a tutti perfettamente chiaro di cosa si sta parlando.

Cosa fa un difensore

Spesso gli studenti vogliono aiutare le vittime di bullismo ma non sanno cosa fare. Questa attività mostra loro le possibilità che hanno a disposizione, esempi di come comportarsi, e offre loro un'opportunità per creare risposte positive da zero.

Obiettivi per gli studenti



- ✓ **Capire** che essere difensori è una scelta possibile.
- ✓ **Imparare** che ci sono diversi modi per intervenire ed essere difensori in una determinata situazione.
- ✓ **Scegliere** come rispondere tra diverse opzioni che si ritengono sicure e adeguate.
- ✓ **Creare** la propria risposta alla situazione.

Spunti di discussione



Quando vediamo che qualcuno si comporta in modo scorretto nei confronti di un'altra persona online, provocandole imbarazzo escludendola, prendendola in giro, mancandole di rispetto, ferendo i suoi sentimenti ecc. abbiamo sempre delle opzioni. In primo luogo, possiamo decidere di essere dei difensori, anziché semplici testimoni, e aiutare la vittima. In secondo luogo, se decidiamo di essere dei difensori, abbiamo la possibilità di scegliere che tipo di azione intraprendere.

La cosa più importante da tenere a mente è che una persona che è stata presa di mira ha bisogno anche solo di essere ascoltata, se è triste, e di sapere che qualcuno si preoccupa per lei.

Non tutti, però, si sentono a proprio agio nel difendere qualcuno pubblicamente, che sia online o a scuola. Ma è bene farlo quando ce la sentiamo. Possiamo:

- Richiamare il comportamento scorretto (non la persona), dicendo che non è una cosa carina.
- Dire qualcosa di carino sulla vittima in un post o commento.
- Chiedere anche agli amici di fare complimenti online alla vittima.
- Offline, puoi invitare la persona a uscire con te durante la pausa o sedersi a mensa insieme a te.

Se non te la senti, non fa niente. Puoi sempre sostenere la vittima privatamente. Puoi...

- Chiederle come sta tramite SMS o messaggio privato.
- Dirle qualcosa di gentile o di carino in un post, commento o messaggio privato in forma anonima (se utilizzi dei mezzi che ti consentono di mantenere l'anonimato).
- Dirle che ci sei se ha voglia di parlare dopo la scuola.
- Nel corso di una conversazione, di persona o al telefono, puoi dirle che pensi che quel comportamento scorretto sia stato inaccettabile e chiederle se se la sente di parlare di quello che è successo.

Non importa in che modo scegliamo di essere difensori, se tramite segnalazione, pubblica o privata. Possiamo anche segnalare un episodio di bullismo tramite l'interfaccia di un sito web o di un'applicazione, oppure parlarne con un adulto di cui ci fidiamo.

Cosa fa un difensore

Di cosa si tratta? Dopo aver creato i gruppi, ciascun gruppo decide in che modo comportarsi da “difensore” nelle seguenti situazioni. Poi confrontatevi sulle diverse azioni possibili da intraprendere in difesa della vittima.

Situazione 1

Uno studente pubblica un video di se stesso che canta una canzone di un famoso artista pop. Altri studenti iniziano a pubblicare commenti cattivi sotto il video. Cosa fai per sostenere lo studente che ha pubblicato il video? Pensa ad alcune delle soluzioni discusse in precedenza oppure formula una risposta con il tuo gruppo.

Situazione 2

Uno studente invia a un altro studente lo screenshot di un commento pubblicato dal tuo amico e lo fa apparire come una buffonata. Lo screenshot viene condiviso e ripubblicato e a scuola diventa virale. Cosa faresti per sostenere lo studente autore del commento condiviso sotto forma di screenshot? Scegli una delle idee di cui abbiamo parlato insieme oppure formula una tua risposta.

Situazione 3

Scopri che uno studente della tua scuola ha creato un account di social media fasullo con il nome di un altro studente e pubblica foto e meme che affermano cattiverie su altri studenti, insegnanti e sulla scuola in generale. Cosa decidi di fare per supportare lo studente la cui identità è stata rubata in modo scorretto? Prendi in considerazione alcune delle idee discusse in precedenza oppure formula una risposta tutta tua.

Un'azione può fare la differenza?

Leggete insieme la seguente storia e provate a ipotizzare differenti epiloghi con e senza l'intervento o meno dei difensori e di un adulto.

Storia 1 - Lucia ha 15 anni e frequenta il secondo anno di scuola superiore. È affetta da vitiligine, e ha grandi macchie chiare su tutto il corpo e anche sul viso. È sempre stata molto timida, ma va molto bene a scuola e piace ai professori. Un compagno di classe comincia a inviarle messaggi contenenti offese: “Ma ti guardi allo specchio prima di uscire di casa?”, “Ciao Pierrot?!” “Vuoi un po' di latte detergente?”. Lucia all'inizio cerca di non badarci troppo, ma con il passare del tempo comincia a sentirsi inadeguata e a soffrire. Trova la forza di mostrare i messaggi a sua sorella, ma lei le dice di ignorarli. Ma Lucia ormai ha paura di comparire in classe e comincia ad assentarsi, all'insaputa dei genitori.

Riportiamo di seguito due possibili epiloghi da condividere con la classe dopo aver ascoltato le loro considerazioni.

Finale 1: il professore, per via delle assenze ripetute di Lucia, contatta la famiglia della ragazza. Capisce che Lucia è vittima di cyberbullismo, dunque organizza una riunione a scuola con gli altri docenti e con uno psicologo per parlarne, e organizza lo stesso incontro in classe con gli allievi per dar vita ad un dibattito. Organizza attività sportive e lavori di gruppo che richiedono collaborazione e che esaltano le caratteristiche fisiche più diverse. Lucia decide di aprirsi con il professore e di seguire un percorso con una psicoterapeuta. Il bullo non chiederà mai scusa, ma capirà di aver provocato una grande sofferenza alla compagna di scuola.

Finale 2: Lucia non solo smette di andare a scuola ma non esce più di casa. Si rifiuta di parlare con i suoi genitori e tanto meno con un medico. È depressa. Si lascia bocciare. Tutto va a rotoli, i suoi rapporti, la scuola... e lei non ne può davvero più.

Nota per l'insegnante:

Il bullismo è un fenomeno sociale. Se un ragazzo compie atti di bullismo la colpa non è di un singolo individuo, ma è l'intero sistema familiare e educativo ad aver fallito. È responsabilità e onere di tutti farsene carico e intervenire: genitori, insegnanti, scuola, adulti in genere, classe dirigente.

Scherzo o bullismo?

In genere gli atti di bullismo si distinguono per:

- obiettivo, ovvero l'intenzione di offendere o arrecare danno, fisico o morale alla vittima;
- persistenza nel tempo, in quanto si tratta di azioni ripetute e con una certa frequenza;
- asimmetria nella relazione, poiché in molti casi c'è uno squilibrio nel "potere" e nella "forza" tra la vittima e il bullo.

È di grandissima importanza saper riconoscere le varie declinazioni in cui il bullismo può verificarsi con altre forme di interazione tra pari (divergenze di opinioni, scherzi, discussioni).

Obiettivi per gli studenti



- ✓ Riflettere sui rischi che si corrono adottando alcuni comportamenti.

Spunti di discussione



Esistono diverse forme di bullismo, offline oppure online, e talvolta sono sottili e difficili da riconoscere e, dunque, contrastare (vedi l'esclusione):

- **Flaming** (da flame, fiamma): invio di messaggi offensivi mirati ad innescare battaglie verbali online (ad esempio su una piattaforma di gaming online).
- **Harassment** (molestia): simile al Flaming, si verifica in caso di invio reiterato di messaggi denigratori finalizzati a ferire qualcuno.
- **Cyberstalking** (persecuzione telematica): l'artefice dell'aggressione non si limita più a offese, ma perseguita la sua vittima con vere e proprie minacce, tanto da farle temere per la propria sicurezza fisica.
- **Denigrazione**: diffusione di pettegolezzi o immagini imbarazzanti sulla vittima allo scopo di ridicolizzarla e danneggiarne la reputazione.
- **Sostituzione dell'identità**: il cyberbullo riesce ad accedere all'account della vittima e fingersi questa persona, inviando messaggi ai suoi contatti e a nome suo, allo scopo di rovinarne la reputazione.
- **Trickery** (raggiro): il cyberbullo diffonde informazioni personali della vittima ottenute con l'inganno, ad esempio condividendo registrazioni di confidenze o chat o minacciando di farlo qualora questa non accetti di esaudire le sue richieste.
- **Esclusione**: la vittima viene esclusa da liste di gruppi online o piattaforme di gioco interattive. Infatti, oggi la leadership di un adolescente è dettata anche dai suoi amici online, non solo da quelli reali, e l'esclusione costituisce una vera e propria punizione volta a ledere la popolarità della vittima.
- **Cyberbashing o Happy Slapping** (letteralmente "schiaffeggio allegro"): la forma più estrema di cyberbullismo che consiste nella ripresa di atti di violenza nei confronti della vittima e la successiva condivisione del video sulle piattaforme social. Costituisce un comportamento criminale.

Attività



1. Scherzo o bullismo?

Chiedi alla classe di provare a stabilire se gli esempi della scheda didattica “Scherzo o bullismo?” costituiscono uno scherzo o un atto di cyberbullismo.

2. Cosa emerge dalle risposte?

Aperte un dibattito sulle risposte emerse.

Risposte scheda didattica “Scherzo o bullismo?”

Caso 1: cyberbullismo - La diffusione, in questo caso via una chat di gruppo, di contenuti denigratori, fotografie o commenti offensivi, costituisce cyberbullismo.

Caso 2: cyberbullismo - Riprendere di nascosto una persona e diffondere a sua insaputa o contro la sua volontà il video costituisce cyberbullismo e violazione della privacy.

Caso 3: scherzo - I ragazzi sono cugini e sui social continuano a chiamarsi con appellativi che usano nella vita reale, sebbene poco ortodossi. Tuttavia, se non c'è intenzione di ledere l'onore di una persona, non si tratta di cyberbullismo. Ma è bene ricordare che essere gentili è sempre un comportamento positivo, specialmente in rete, dove ogni parola scritta lascia un segno indelebile.

Caso 4: reato - I due ragazzi sono amici e facilmente la “vittima” intuirà o verrà a sapere che si è trattato di uno scherzo.

Da ricordare

Scherzi tra adolescenti e bullismo: qual è la differenza? Il confine tra uno scherzo “innocente” e un atto di bullismo è ben definito?

Una presa in giro – un insulto, un soprannome, ecc. – diventa bullismo quando è continuativa nel tempo, unidirezionale, intenzionale e lesiva nei confronti di una persona. Non si tratta di bullismo, invece, quando una frase, un nomignolo, ecc, rappresentano una manifestazione di affetto, basata sul reciproco riconoscimento, o un modo per sdrammatizzare una situazione. E quando questo accade, tutti si divertono!

Scherzo o bullismo?

1. Insulti inviati ripetutamente in una chat di gruppo ad una persona sono da considerarsi uno scherzo?
2. Due ragazzi riprendono di nascosto una loro amica, molto timida e riservata, mentre sta canticchiando nel giardino della scuola durante la ricreazione, e diffondono il video online. Siamo in presenza di un atto di cyberbullismo?
3. Due cugini si prendono spesso in giro e si scambiano le medesime battute anche online, utilizzando attributi spesso poco gentili. Questo atteggiamento è ascrivibile a cyberbullismo?
4. Un ragazzo invia un messaggio privato al suo migliore amico fingendosi il professore di matematica che gli comunica il voto all'ultimo compito: un bel 2. È cyberbullismo?

Diffondi la gentilezza - Attività 4

Dillo con più tatto!

Riformulando i commenti offensivi o aggressivi si può imparare a trasformare un'interazione negativa in una positiva.

Obiettivi per gli studenti



- ✓ **Esprimere** ciò che si pensa e si prova in maniera positiva ed efficace.
- ✓ **Reagire** agli stimoli negativi in modo costruttivo e civile.

Spunti di discussione



Trasformare la negatività in positività

I ragazzi sono esposti a ogni sorta di contenuto online e alcuni di questi includono messaggi negativi che promuovono comportamenti scorretti. Poni i seguenti interrogativi alla classe:

- Avete mai assistito, o qualcuno che conoscete ha mai assistito, a comportamenti negativi sul Web? Come vi hanno fatto sentire?
- È mai capitato che qualcuno sul Web fosse inaspettatamente gentile con voi (o con qualcuno che conoscete)? Come vi ha fatto sentire?
- Quali semplici rimedi possiamo adottare per trasformare le interazioni negative in positive?
- Possiamo reagire alle emozioni negative in modo costruttivo, riformulando i commenti ostili e facendo più attenzione al tono che utilizziamo durante la comunicazione online.

Attività



Materiale necessario:

- Scheda didattica: "Dillo con più tatto!"

1. Leggete i commenti

Leggi l'elenco di commenti negativi.

2. Scrivete una versione diversa

Ogni studente dovrà inventare due tipi di risposta a questi commenti. Per aiutare gli studenti poni loro le seguenti domande:

- In che modo avreste potuto esprimere lo stesso concetto, o uno simile, in maniera più costruttiva?
- Se uno dei vostri compagni facesse un commento di questo tipo, in che modo potreste intervenire per offrire un contributo positivo alla conversazione?

Nota per gli insegnanti:

Completare un esempio tutti insieme potrebbe essere un buon metodo per assicurarsi che gli alunni riescano a pensare in modo corretto e indipendente.

3. Condividete le risposte

Leggete ad alta voce le risposte per entrambe le situazioni.

Da ricordare

Reagire positivamente a uno stimolo negativo può rendere la conversazione più interessante e più divertente, ed è molto meglio che dover aggiustare una situazione complicata generata da un commento spiacevole.

Dillo con più tatto!

Leggi i commenti riportati di seguito. Dopo ogni commento, parlane con il resto della classe.

- In che modo avresti potuto esprimere lo stesso concetto, o uno simile, in maniera più costruttiva?
- Se uno dei tuoi compagni facesse un commento di questo tipo, in che modo potresti intervenire per offrire un contributo positivo alla conversazione?

Usa gli spazi sotto ai commenti per annotare le tue idee.

Ahah, Stefano è l'unico della classe che non farà una festa di 18 anni seria!

La festa di sabato è a tema anni '80, ma diciamo a Laura che il tema sono gli anni '50 :).

Mi spiace, non penso che tu possa venire alla mia festa. Non hai abbastanza stile!

Senza offesa, tu e lo sport avete litigato.

È tremenda, ma chi le ha fatto credere di saper cantare??

Puoi partecipare al nostro gruppo solo se mi dai i dati di accesso del tuo account.

Sono l'unico qui a pensare che Susanna sembra una vecchia strega?



Usa il tono giusto

È importante saper interpretare le emozioni dietro ad alcuni messaggi di testo per esercitare il pensiero critico ed evitare malintesi o conflitti negli scambi online.

Obiettivi per gli studenti



- ✓ **Prendere la decisione giusta** quando si sceglie come e cosa comunicare e se comunicarlo o meno.
- ✓ **Riconoscere** le situazioni in cui è meglio aspettare e comunicare di persona con un compagno anziché inviargli subito un messaggio.

Spunti di discussione



Ci è mai capitato che un nostro messaggio venisse frainteso? Ad esempio, è mai successo di scrivere una battuta a un nostro amico e che questi non capisse l'intenzione scherzosa, percependola come una cattiveria da parte nostra?

Ci è mai capitato di fraintendere qualcuno via messaggio o in chat? Cosa abbiamo fatto per chiarire l'equivoco? Cosa avremmo potuto fare in modo diverso?

Attività



Materiale necessario:

- Esempi di messaggi di testo scritti alla lavagna o proiettati

1. Esaminate i messaggi

Date un'occhiata a questi esempi di messaggi. Probabilmente anche i ragazzi avranno degli ottimi esempi da aggiungere, quindi scrivetene alcuni alla lavagna per poi parlarne.

- "Ammazza!"
- "Vedi tu"
- "Come non ti sopporto!"
- "CHIAMAMI IMMEDIATAMENTE"
- "Oooooook"

2. Leggete i messaggi ad alta voce

Ora leggete ad alta voce tutti i messaggi, usando ogni volta un tono di voce diverso.

Notate qualcosa? In che modo possono essere interpretati questi messaggi? In che modo chi ha scritto quei messaggi potrebbe comunicare meglio ciò che intendeva realmente?

Può essere difficile capire cosa prova qualcuno dalla lettura di un messaggio. Scegliere con attenzione quale strumento si usa per comunicare è importante, così come non dare troppo peso a quello che viene detto online. E se non si ha la certezza di ciò che l'altra persona voleva dire, meglio scoprirlo parlandole di persona o al telefono.

Da ricordare

È facile che si creino malintesi

I giovani usano diversi tipi di comunicazione per vari tipi di interazione; tuttavia, i messaggi via chat possono essere interpretati in modo diverso da come accadrebbe di persona o parlando al telefono.

Sfidare l'odio in rete

Un particolare tipo di comunicazione che si serve di parole, espressioni o elementi non verbali aventi come fine ultimo quello di esprimere e diffondere odio ed intolleranza, nonché di incitare al pregiudizio e alla paura verso un soggetto o un gruppo di persone ascrivibili alle caratteristiche sopra elencate, può essere definito "hate speech".

Obiettivi per gli studenti



- ✓ **Riflettere** sulle conseguenze dei discorsi di odio online.
- ✓ **Valutare** in che modo contrastare l'odio in rete.

Spunti di discussione



Le parole che usiamo hanno un peso: esse possono ferire, emarginare, generare odio, discriminare. Le espressioni e azioni verbali che incitano all'odio e alla violenza, specialmente se rivolte ad un gruppo, o un singolo ad esso appartenente, e basate su caratteristiche etnico-razziali, politico-religiose, di orientamento sessuale, ecc. ricadono nella definizione di "hate speech", o "discorsi di incitamento all'odio". Spesso i discorsi ostili e violenti raggiungono una tale forza da trasformarsi in istigazione, diventando per qualcuno una sorta di lasciapassare per agire con violenza contro il bersaglio scelto.

Nota per l'insegnante:

Nelle attività che seguono alcuni ragazzi potrebbero esprimere opinioni forti e contrarie agli obiettivi pedagogici e didattici prefissati. In ogni caso, è bene ascoltarli pazientemente e spronarli ad esempio ad analizzare e riconsiderare certi pregiudizi, ma senza rimproverarli o ammonirli, perché ciò produrrebbe molto probabilmente l'effetto contrario.

Attività



1. Prova a porre ai tuoi studenti le seguenti domande e discutatene insieme.

- Un'opinione negativa genera necessariamente un discorso di odio?
- Un commento negativo diretto a un individuo e non a un gruppo o a una categoria, produce effetti diversi?
- Cosa trasforma un'opinione negativa in un commento di odio?
- Il diritto ad esprimere la propria opinione prevale sulla possibilità di ferire i sentimenti di qualcuno?

È buona prassi, ancora di più in rete, chiedersi a chi si sta parlando, a chi può arrivare quel messaggio e come può essere interpretato. La tolleranza nasce dalla capacità di sviluppare senso critico e di comprendere che un fatto circostanziato e provato non può essere trasformato in un concetto universale.

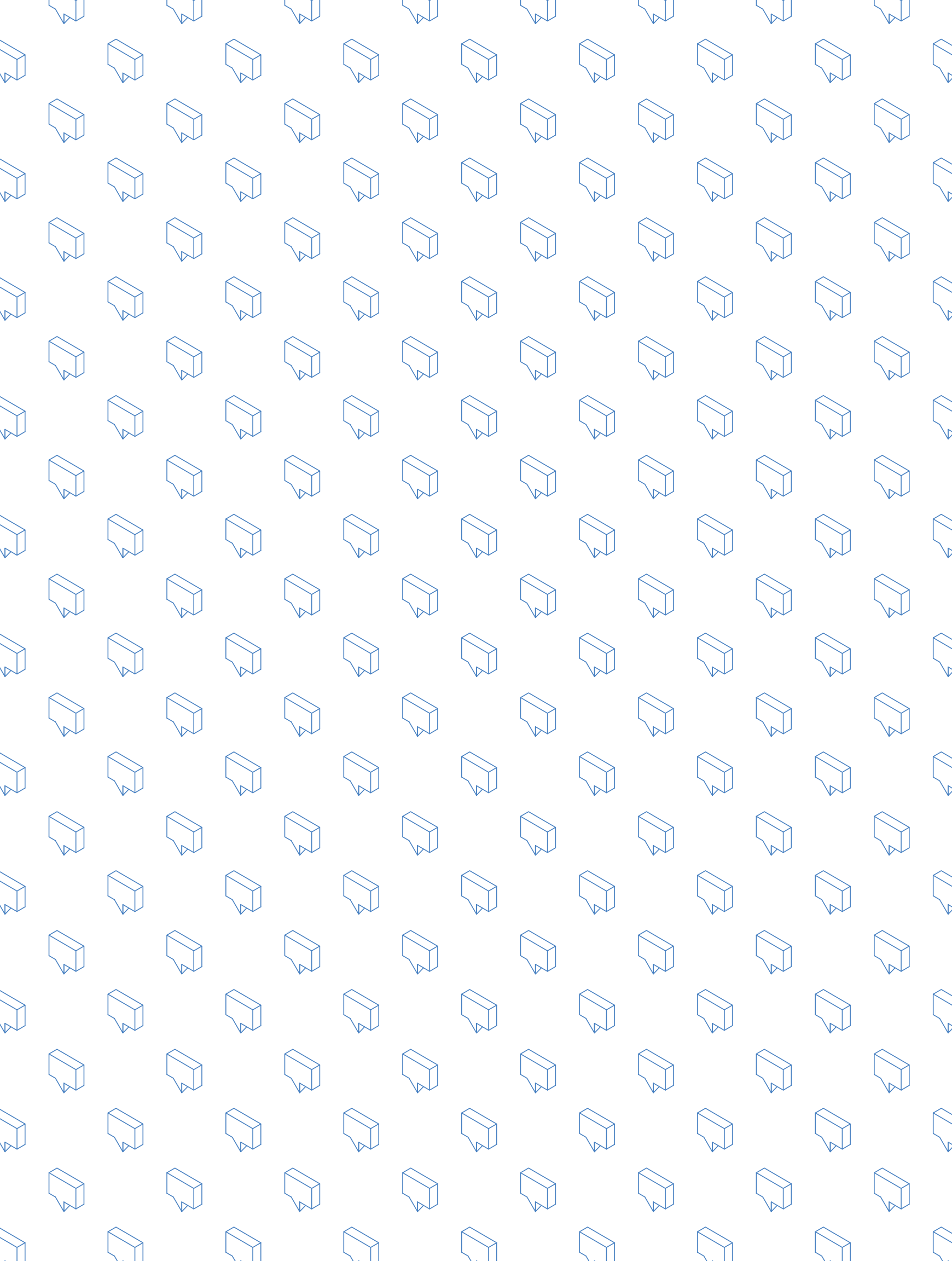
2. Chiedi ai ragazzi di individuare tra le frasi seguenti quelle che possono costituire esempi di incitamento all'odio.

- Potrebbero formare le classi sulla base del rendimento. Ne gioverebbero tutti e i ragazzi più bravi non sarebbero rallentati.
- I miei genitori affittano solo agli italiani perché vogliono che la casa sia tenuta sempre pulita.

- Le ragazze indiane hanno tutte i capelli nero corvino liscissimi. Possono risparmiare tanti soldi in tinte e pieghe!
- I miei genitori dicono sempre che le persone dell'est dell'Europa lavorano senza sosta dalla mattina alla sera, sono molto bravi nei traslochi e nel montaggio di mobili. Ecco perché i ragazzi romeni e albanesi della mia classe non hanno buoni voti: di sicuro i genitori li fanno lavorare togliendo tempo allo studio.

Da ricordare

Le parole sono potenti: possono fare male e provocare sofferenza, con conseguenze anche molto gravi. Ma non possiamo reagire a quel dolore punendo chi parla. Optiamo per un'altra strada, difendiamo la libertà di parola, ma educiamo al rispetto ed alla gentilezza. E ricordiamo che le parole possono fare male, sì, ma possono anche guarire.



Nel dubbio parlane

Definire e promuovere il comportamento del vivere Internet con coraggio

Panoramica della lezione

Attività 1: **Quando farsi aiutare**
Attività 2: **Segnalalo, anche online**
Attività 3: **Cosa significa avere coraggio?**

Temi

È importante che i ragazzi capiscano di non essere da soli quando vedono dei contenuti online che li mettono a disagio, specialmente se loro o altri possono farsi del male. Non dovrebbero mai esitare nel chiedere aiuto a qualcuno di cui si fidano. Inoltre, è bene che conoscano i diversi modi di essere coraggiosi e di intraprendere un'azione.

Obiettivi per gli studenti

- ✓ **Comprendere** in quali situazioni è opportuno farsi aiutare o parlarne apertamente con un adulto.
- ✓ **Considerare** in che modo possiamo essere coraggiosi e perché è importante coinvolgere gli adulti.

Nel dubbio parlane

Vocabolario

Coraggioso: audace; non per forza senza timore, perché le persone sono molto coraggiose quando hanno paura o sono nervose, ma intraprendono comunque delle azioni positive.

Account compromesso: un account online di cui si è impadronito qualcun altro e del quale non si ha più il controllo totale.

Agency dello studente: l'agency dello studente è la capacità di agire o di apportare un cambiamento; include la protezione o la difesa di se stessi e degli altri; spesso è considerata come una parte fondamentale del senso civico.

Fiducia: forte convinzione che qualcosa o qualcuno sia affidabile, veritiero o capace.

Quando farsi aiutare

Un consiglio che appare con costanza in queste lezioni è: se gli studenti incappano in qualcosa che li mette a disagio o peggio ancora, incoraggiali a fare una segnalazione, a essere coraggiosi e a parlarne con qualcuno di cui si fidano e che possa aiutarli, ad esempio tu, il direttore o un genitore. Di seguito troverai un ulteriore elenco di situazioni in cui “parlarne” può essere molto utile.

Note per gli insegnanti:

1. *Da generazioni ai ragazzi viene detto che non si deve “fare la spia”, che ormai è diventata una norma sociale, ma è importante far capire loro la differenza tra “raccontare” qualcosa e chiedere aiuto. Aiuta i tuoi studenti a capire che cercare aiuto quando succedono cose spiacevoli online non significa “fare la spia”: significa farsi aiutare o cercare di aiutare i propri compagni se viene fatto loro del male.*
2. *Promuovi una comunicazione aperta in classe e ricorda agli studenti che sei sempre a loro disposizione se hanno bisogno di supporto in merito all’agency dello studente e a come fare una segnalazione adeguata.*

Obiettivi per gli studenti



- ✓ **Riconoscere** che cercare aiuto per sé e per gli altri è segno di forza.
- ✓ **Pensare insieme e ad alta voce** a situazioni per le quali può davvero essere d’aiuto sfogarsi.

Spunti di discussione



Ecco un elenco di situazioni in cui si potrebbe incappare online. Chiedi ai ragazzi di individuare eventuali episodi vissuti personalmente tra quelli menzionati e di raccontare come si sono comportati a riguardo.

Da ricordare

A volte non sembra, ma essere in grado di chiedere aiuto quando non si è sicuri di qualcosa è un atto di coraggio. Se aiuta noi stessi o qualcun altro a riprendersi da una situazione dolorosa o a evitare che una cosa brutta succeda, allora parlare è un atto di coraggio e di intelligenza al tempo stesso.

Argomenti di discussione



1. Chiedi ai ragazzi di leggere l'elenco che segue in silenzio, ognuno per conto proprio e di pensare ad eventuali situazioni simili vissute e al modo in cui hanno reagito:

- Come vi comportereste?
- Vi è mai capitato?
- Se sì, avreste voluto chiedere aiuto a un adulto? L'avete chiesto?
- Se no, perché?

Situazioni:

- Avevi la sensazione che il tuo account fosse stato compromesso. (Spunto di discussione: cosa puoi fare per aumentare la sicurezza del tuo account?)
- Avevi bisogno di aiuto per ricordare una password.
- Non avevi la certezza che si trattasse di una truffa o hai pensato che ti avessero truffato. (Spunto di discussione: quali sono i possibili indizi per identificare una truffa?)
- Qualcuno online ti stava parlando di argomenti che ti mettevano a disagio.
- Hai ricevuto un messaggio o un commento strano da parte di un estraneo. (Spunto di discussione: quand'è che qualcosa si può definire strana?)
- Volevi parlare di qualcosa che qualcuno ha detto online e che era molto gentile o molto cattiva.
- Temevi di aver condiviso accidentalmente qualcosa che non avresti dovuto condividere.
- Hai visto che un tuo compagno si comportava in maniera offensiva nei confronti di un altro studente online.
- Hai visto qualcuno minacciare di far partire una lite o fare del male a qualcuno.
- Qualcuno ha pubblicato un profilo finto di un altro studente.
- Eri in apprensione per un altro studente per via di qualcosa che altri hanno pubblicato o inviato. (Spunto di discussione: a volte è difficile rischiare di turbare i propri amici, ma non è più importante preoccuparsi della loro sicurezza e del loro benessere?)

2. Chiedi ai ragazzi, volontariamente, di condividere le proprie esperienze, cosa hanno (o non hanno) fatto e perché. Se uno studente ha già scelto un argomento di cui discutere, i compagni a seguire dovranno scegliere situazioni diverse.

Nota per gli insegnanti:

Avere la possibilità di organizzare un'assemblea di studenti o un gruppo di lavoro nella scuola (o una scuola media/superiore del tuo quartiere) può essere un modo molto efficace di sviluppare l'agency degli studenti sull'argomento. Se esiste già un'assemblea o un gruppo di tutoraggio nella tua scuola, fai in modo che i tutor spieghino gli scenari analizzati in precedenza agli studenti e condividano le loro esperienze di supporto.

Segnalalo, anche online

Utilizzando un dispositivo scolastico, mostra alla classe diversi tipi di contenuti: decidete insieme se segnalarli e discutete del perché sarebbe giusto o sbagliato.

Obiettivi per gli studenti



- ✓ **Essere** a conoscenza degli strumenti online per la segnalazione di molestie.
- ✓ **Valutare** quando utilizzarli.
- ✓ **Parlare** del perché e del quando segnalare una molestia.

Spunti di discussione



Quando la cattiveria e altri contenuti inappropriati fanno capolino online, possiamo agire in diversi modi. Nell'ultima attività abbiamo parlato dell'azione più importante: parlare con qualcuno di fiducia. Un'altra opzione è quella di segnalare i contenuti all'interno dell'app o del servizio in cui li abbiamo trovati, il che può facilitarne l'eliminazione.

È importante abituarsi a utilizzare questi strumenti di segnalazione online. Gli studenti dovrebbero prendere l'abitudine di fare degli screenshot delle conversazioni o delle attività che ritengono dannose o sospette prima di utilizzare l'opzione di blocco e gli strumenti di segnalazione (che potrebbero rendere impossibile l'accesso al registro delle attività). In questo modo possono assicurarsi che gli adulti abbiano modo di verificare cosa è successo e aiutarli a risolvere la situazione.

Attività



Materiale necessario:

Scheda didattica: "Segnalalo, anche online"

1. Come segnalare un problema?

Utilizzate i dispositivi digitali a disposizione della classe. Chiedi ai ragazzi di indicarti gli strumenti per la segnalazione di contenuti o comportamenti inappropriati in almeno tre account collegati alla scuola: ad esempio sito web, email, chat...

2. Leggete i sette scenari presenti sulla scheda didattica.

3. Dovreste segnalarli?

Chiedi agli studenti di alzare la mano se pensano di dover segnalare i contenuti; poi chiedi di alzare la mano se pensano di non doverlo fare.

4. Se sì, perché?

Chiedi a uno degli studenti che la segnalerebbe di spiegare alla classe perché lo farebbe, e chiedi a un altro studente tra quelli che non la segnalerebbero, di fare lo stesso.

Nota: difficilmente c'è una sola risposta o un solo approccio giusto. Assicurati che la classe ne sia consapevole prima di dare il via alla discussione.

Da ricordare

La maggior parte delle app e dei servizi hanno degli strumenti per segnalare e/o bloccare i contenuti inappropriati e utilizzandoli potremmo aiutare le persone coinvolte, la loro comunità e le piattaforme stesse. Prima di bloccare o segnalare i contenuti inappropriati, è consigliabile fare uno screenshot in modo da avere una prova tangibile di quella situazione.

Segnalalo, anche online

Leggete gli scenari qui sotto e chiedi ai ragazzi di alzare la mano se ritengono si tratti di una situazione che segnalerebbero nell'app o servizio in cui l'hanno riscontrata. Poi chiedi loro di spiegare perché la segnalerebbero (o perché no) e perché hanno scelto di comportarsi in quel modo.

Nota: tutti dovrebbero essere consapevoli del fatto che difficilmente esiste una scelta giusta da fare, ed è per questo che è utile parlarne. Nessuno dovrebbe sentirsi in torto per la scelta che ha fatto. Persino gli adulti a volte non sanno quando o come fare una segnalazione.

Situazione 1

Uno studente pubblica una foto di gruppo su un account pubblico e tu non ti piaci per niente in quello scatto. Segnali quella foto oppure no? Come puoi rispondere?

Situazione 2

Qualcuno crea un account di uno studente che conosci utilizzando il suo nome e la sua foto. Trasforma la foto in un meme e disegna dei baffi o altri tratti del viso particolari, facendo diventare quella foto una presa in giro. Segnali quell'account oppure no?

Situazione 3

Uno studente crea un account utilizzando il nome della scuola come nome utente e pubblica foto degli studenti con commenti di cui tutti vengono a conoscenza. Alcuni sono commenti cattivi, altri sono complimenti. Segnali i commenti cattivi, l'intero account o entrambi?

Situazione 4

Qualcuno pubblica molti commenti cattivi su uno studente senza utilizzare il suo vero nome, ma tu pensi di aver capito di chi si tratta. Segnali quei commenti oppure no?

Situazione 5

Ti accorgi che uno studente ha lasciato un commento online dicendo che domani litigherà con un altro studente alla ricreazione. Segnali quel commento online oppure no? Il mattino dopo lo riferisci a un insegnante o al preside, oppure no? O fai entrambe le cose?

Situazione 6

Stai giocando online con gli amici e qualcuno (che non è tra i giocatori) inizia a chattare con te. Non dice cose cattive, né altro, ma non lo conosci. Lo ignori o lo segnali?

Cosa significa avere coraggio

Chiedi agli studenti di scegliere una persona che ritengono abbia fatto qualcosa di coraggioso. Invitali a pensare più approfonditamente alla loro scelta, e a capire da cosa scaturisce l'idea che si tratti di un atto di coraggio.

Nota per gli insegnanti:

Sappiamo tutti che le opinioni delle persone possono essere influenzate dai mezzi di comunicazione. Quindi, per aiutare gli studenti a esserne consapevoli, potrebbe essere utile "sfogarsi", parlare tutti insieme di come ciò avviene. Ecco alcune cose importanti da tenere a mente:

1. Le nostre idee sono plasmate da tutto quello che vediamo, ascoltiamo e leggiamo.
2. Interpretiamo quello che vediamo attraverso la lente delle nostre esperienze, pertanto possiamo trarre messaggi diversi dagli stessi mezzi di comunicazione.
3. Impariamo tanto dalle immagini quanto dalle parole, a volte anche più.
4. L'educazione ai media aiuta a contrastare gli stereotipi aiutandoci a prendere consapevolezza dei modelli e a metterli in discussione, in particolare la ripetizione. Ad esempio, vedendo soltanto eroi di sesso maschile, potremmo farci l'idea che gli uomini diventino eroi più facilmente, anche se nessuno dice mai alle donne che non possono essere eroine (anche l'assenza di informazioni è qualcosa di cui tenere conto).

Obiettivi per gli studenti



- ✓ **Pensare** a cosa significa essere coraggiosi, anche online.
- ✓ **Individuare** le fonti delle nostre idee relative a cosa significa essere coraggiosi.
- ✓ **Prendere** l'abitudine di chiedersi: "Cosa stanno tralasciando?"

Spunti di discussione



Quando i ragazzi pensano al coraggio, chi hanno in mente?

I mezzi di comunicazione per esigenze economiche, puntano a conquistare il più possibile la nostra attenzione. Così ci presentano le forme di coraggio più drammatiche e più ricche di azione. Questo giustifica il perché molti studenti hanno scelto supereroi, paramedici e soldati. Questi possono essere degli ottimi esempi, certo, ma non sono gli unici! Quali altri esempi di coraggio ci sono?

Cosa vuol dire, dunque, essere coraggiosi?

1. Invita i ragazzi a pensare ad una persona che conoscono e che considerano coraggiosa. Chiedi loro di spiegare alla classe i motivi dietro le loro scelte.

- Che cosa ha reso coraggiosa la persona che è stata scelta?
- C'erano differenze tra i tipi di atti di coraggio compiuti dalle persone reali e quelli generalmente compiuti dai personaggi dei mezzi di comunicazione? Se sì, quali?

Riflettete insieme sui seguenti punti:

- Qualcuno ha nominato una persona che ha salvato altri da un pericolo fisico?
- Qualcuno ha nominato una persona che si è fatta avanti per qualcun altro che era vittima di bullismo? La maggior parte delle persone concorda sul fatto che salvare qualcuno dal farsi male fisicamente sia un atto di coraggio.

- E se invece si riesce a evitare che i sentimenti di una persona vengano feriti, oppure si mostra gentilezza o sostegno nei suoi confronti nel caso in cui i suoi sentimenti siano già stati feriti, non si tratta anche in questo caso di un “salvataggio”? Non è un atto di coraggio?

2. Quando i ragazzi pensano alla parola “coraggioso”, immaginano un uomo/ragazzo o una donna/ragazza? Che aspetto ha il coraggio delle donne/ragazze? È diverso da quello degli uomini/ragazzi? Cosa li induce a pensarla così?

Da ricordare

Avere coraggio significa correre dei rischi per aiutare qualcuno, in vari modi. I mezzi di comunicazione possono plasmare il modo in cui intendiamo l'essere coraggiosi, ma non sempre mostrano tutte le possibilità. Può essere utile chiedersi: “Cosa stanno tralasciando?”. Quando siamo online dobbiamo anche pensare di correre dei rischi per “salvare” qualcuno, ad esempio per evitare che i suoi sentimenti vengano feriti. Tutti possiamo scegliere di essere coraggiosi.

