Associazione protezione diritti e libertà privacy APS

IL PATENTINO DIGITALE PER STUDENTI

Viviamo in un tempo in cui la vita reale e quella digitale non sono più separate: comunicazione, studio, relazioni, creatività, informazione e sicurezza passano ogni giorno attraverso smartphone, piattaforme, app e intelligenze artificiali. Per questo la scuola ha il compito non solo di insegnare ad usare gli strumenti digitali, ma soprattutto di educare a viverli con consapevolezza, responsabilità e autonomia.

Il Patentino Digitale nasce con questa finalità: offrire agli studenti un percorso formativo strutturato, completo e coinvolgente, che permetta loro di diventare cittadini digitali competenti, consapevoli dei rischi e capaci di cogliere le opportunità del mondo online.

Il percorso è articolato in 3 macroaree (Web reputation; I meccanismi di funzionamento; Disinformazione ed hatespeech) e 9 argomenti generali , ognuno pensato per sviluppare competenze fondamentali per la vita digitale contemporanea:

Web Reputation

- *Identità digitale*
- *Privacy e sicurezza*
- *Salute e benessere digitale*

I meccanismi di funzionamento

- *Competenze digitali*
- *Intelligenza Artificiale a scuola*
- *Sviluppo del senso critico*

Disinformazione e Hatespeech

- *Aspetti giuridici*
- *Utilizzo responsabile dei social media*
- *Rischio delle interazioni online*

Modulo AGCOM

Una certificazione che educa a scegliere

Il Patentino Digitale non è un semplice corso: è un percorso educativo che aiuta gli studenti a diventare:

- più consapevoli nel pubblicare
- più critici nel leggere
- più sicuri nel navigare
- più rispettosi nelle relazioni online
- più responsabili nella gestione del digitale
- più attenti alla propria salute digitale

Si tratta di un investimento formativo che prepara i ragazzi non solo alla cittadinanza digitale, ma anche allo studio universitario, al mondo del lavoro e alla società dell'informazione in cui vivranno da adulti.

Un percorso che unisce competenze, etica e sicurezza

Con il Patentino Digitale, la scuola offre ai propri studenti un'educazione completa che integra:

- competenze digitali
- identità e consapevolezza
- sicurezza online
- responsabilità legale
- benessere psicologico
- cittadinanza e diritti

È il primo passo verso una vera alfabetizzazione digitale integrale.

90's
TEMI PRINCIPALI

Competenze digitali (2 ore)

Obiettivi
- Comprendere cosa significa “competenza digitale” secondo DigComp 3.0
- Riconoscere le 5 aree: alfabetizzazione, comunicazione, creazione, sicurezza, problem solving.
- Applicare le competenze informazionali e cruciali per la vita nello spazio digitale.

Contenuti
- Differenza tra abilità digitale e competenza digitale.
- Ricerca consapevole delle informazioni: attendibilità, autorità, bias delle fonti.
- Introduzione alle IA generative e all’uso critico.

Laboratorio
- Valutazione di tre siti web, individuazione di fonti affidabili e manipolate.
- Creazione personale del profilo di competenza digitale.

Intelligenza Artificiale a scuola: uso consapevole e responsabile (2 ore)

Contenuti:
- Come funzionano le IA generative.
- Cosa si può fare e cosa non si può fare.
- Rischi, etica, plagio, copyright.
- Applicazioni utili nello studio.
- Prime regole del “AI Digital Citizenship”.

Perché funziona:
✓ iper-attuale
✓ richiesto dalle Linee guida MIM sull’IA nella scuola
✓ prepara gli studenti al mondo universitario e del lavoro

Identità digitale (2 ore)

Obiettivi
- Capire cosa significa possedere un’identità digitale.
- Riconoscere i rischi legati a oversharing, reputazione online, tracciabilità.
- Collegare identità digitale, libertà e responsabilità.

Contenuti
- Identità reale, digitale, percepita.
- Carbon footprint digitale: dati attivi e passivi.
- Deepfake, doppi digitali, impersonation.
- Costruzione dell’identità nell’era dei social.

Laboratorio
- “La mia impronta digitale”: ricostruzione delle proprie tracce (educativo e guidato).
- Revisione del proprio profilo social: cosa comunica davvero?

90's
TEMI PRINCIPALI

Privacy e sicurezza – Interazioni online (2 ore)

- Obiettivi
- Conoscere le basi del GDPR in modo semplice.
- Saper riconoscere rischi e minacce online.
- Sviluppare comportamenti protettivi.
- Contenuti
- Che cos'è un dato personale?
- Rischi: phishing, hackeraggio di account, truffe, furto d'identità.
- Sicurezza quotidiana: 2FA, password manager, gestione dispositivi.
- Comportamenti sicuri in chat, gruppi, gaming.
- Laboratorio
- Analisi di messaggi fittizi: phishing, truffe.
- Impostazione della privacy su un social.

Aspetti giuridici (2 ore)

Obiettivi

- Conoscere i reati digitali e le responsabilità dei minori.
- Saper distinguere cosa è lecito e cosa non lo è.
- Comprendere la normativa sulla tutela dei minori.

Contenuti

- Cyberbullismo (Legge 71/2017).
- Diffamazione, minacce, revenge porn (612-ter).
- Condivisione di immagini altrui senza consenso.
- Età minima social e Termini di Servizio.
- Responsabilità penale, civile e scolastica.

Laboratorio

- Role-play "È reato o non lo è?".
- Analisi di casi reali (anonimizzati).

Sviluppo del senso critico (2 ore)

- Obiettivi
- Saper analizzare contenuti online con spirito critico.
- Conoscere bias cognitivi, distorsioni e manipolazioni digitali.
- Riconoscere fake news, clickbait, deepfake.
- Contenuti
- Algoritmi e bolle informative.
- Polarizzazione, echo chambers.
- Disinformazione, misinformazione.
- Fact-checking: strumenti essenziali.
- Laboratorio
- Fact-checking di un video o post virale.
- Analisi di un deepfake.
- Il Rapporto Dialettico (Conflittuale) tra IA e Privacy:

90's
LA CHIAVE DI LETTURA

Utilizzo responsabile dei social media (2 ore)

Obiettivi
- Promuovere uno stile comunicativo sano e non aggressivo.
- Capire conseguenze psicologiche, sociali e legali dell'uso scorretto dei social.
- Favorire un'identità digitale consapevole.

Contenuti
- Linguaggio, tono, netiquette.
- Hate speech, body shaming, cyberbullismo.
- Oscillazioni emotive legate ai social.
- Gestione del tempo e delle notifiche.

Laboratorio
- Realizzazione della Carta dello Studente Digitale.
- Creazione di esempi di post responsabili.

Rischio delle interazioni online (2 ore)

Obiettivi
- Riconoscere situazioni a rischio e strategie di protezione.
- Conoscere i meccanismi di manipolazione e adescamento.
- Sapere come chiedere aiuto.

Contenuti
- Grooming, sexting, sextortion.
- Challenge pericolose, comportamenti a rischio.
- Gaming online: toxic behavior, acquisti inconsapevoli.
- Psicologia dell'inganno e della manipolazione.

Laboratorio
- Analisi di casi reali di rischio (protetti).
- Simulazione di conversazioni sospette per imparare a riconoscerle.

Salute e benessere digitale (2 ore)

- Obiettivi
- Favorire un equilibrio tra vita online e offline.
- Conoscere le dipendenze digitali.
- Promuovere il benessere psicologico e fisico.
- Contenuti
- FOMO, dipendenze, doomscrolling.
- Sonno, postura, vista, attività fisica.
- Regole 20-20-20 e netiquette psicologica.
- LifeComp e autoconsapevolezza digitale.
- Laboratorio
- Creazione del proprio Piano personale di Benessere Digitale.
- Monitoraggio per una settimana (facoltativo).

10) AGCOM (2 ore)

I MODULI IN DETTAGLIO

Competenze digitali *(2 ore)*

Guida completa agli argomenti

1. Che cosa significa “competenza digitale” secondo DigComp 3.0

Cosa devono capire gli studenti

- La competenza digitale non è “essere bravi con i telefoni”.
- È un insieme di capacità: conoscenze + abilità + atteggiamenti.
- Le competenze digitali servono per:
  - studiare
  - comunicare
  - lavorare
  - orientarsi online
  - proteggersi dai rischi
  - partecipare alla vita civica digitale

Punti chiave da spiegare

- La competenza digitale è trasversale: riguarda tutte le materie.
- È un’abilità critica come leggere, scrivere, contare.
- È parte integrante della cittadinanza digitale prevista per legge.

2. Le 5 aree del DigComp 3.0

1) Alfabetizzazione su informazioni e dati

- Come cercare correttamente sul web.
- Come valutare l’attendibilità di una fonte.
- Capire cosa sono i “bias”, le percezioni, le manipolazioni.

2) Comunicazione e collaborazione

- Come usare gli strumenti digitali per comunicare in modo corretto.
- Netiquette, comportamento nei gruppi, rispetto online.
- Condivisione sicura di materiali e informazioni.

3) Creazione di contenuti digitali

- Scrivere, creare presentazioni, video, slide.
- Capire cos’è il copyright e cosa non si può copiare.
- Uso corretto di strumenti e applicazioni.

4) Sicurezza digitale

- Protezione dei dati personali.
- Privacy, password, autenticazione a due fattori.
- Riconoscere truffe, phishing, tentativi di manipolazione.

5) Problem solving digitale

- Risolvere problemi tecnici di base.
- Cercare soluzioni online

Saper valutare qual è lo strumento giusto per un compito.

3. Differenza tra abilità digitale e competenza digitale

Abilità digitale = saper usare uno strumento
(es. “So aprire TikTok”, “So usare Instagram”, “So accendere un PC”)
Competenza digitale = saper usare lo strumento in modo consapevole, critico, efficace e sicuro
(es. “So verificare una notizia”, “So creare un documento condiviso”, “So proteggermi online”)
Esempi concreti da spiegare agli studenti

- Abilità: “So installare un’app”
- Competenza: “Capisco a quali dati sto dando accesso”
- Abilità: “So fare uno screenshot”
- Competenza: “So che non posso diffonderlo se contiene dati sensibili”

I MODULI IN DETTAGLIO

4. Ricerca consapevole delle informazioni online

Cosa devono imparare gli studenti

- Digitare parole chiave in modo efficace.
- Capire perché Google non mostra gli stessi risultati a tutti.
- Valutare autorità, attendibilità, datazione delle fonti.
- Distinguere informazioni affidabili da contenuti manipolati.

Strumenti e criteri da presentare

- Metodo CRAAP (Currency, Relevance, Authority, Accuracy, Purpose).
- Confronto tra più fonti.
- Verifica delle immagini (Reverse Image Search).
- Attenzione a titoli sensazionalistici e “fake experts”.

5. Introduzione alle IA generative e al loro uso critico

Cosa spiegare

- Che cos’è un modello di IA generativa.
- Perché può sbagliare (hallucinations).
- Perché bisogna verificare ciò che produce.
- Quando può essere utile nello studio:
  - riassunti
  - mappe concettuali
  - revisione testi
  - brainstorming

Regola fondamentale

L’IA aiuta, ma non sostituisce il pensiero critico.

6. Laboratorio operativo (1 ora)

Attività 1 – Valutazione di tre siti web

- Attività 1 – Valutazione di tre siti web
- Gli studenti analizzano tre pagine scelte dal docente:
- una affidabile
- una moderatamente attendibile
- una manipolata / poco credibile
- Cosa devono riconoscere:
- linguaggio
- finalità del sito
- fonte delle informazioni
- eventuali manipolazioni
- pubblicità e tracciamento
- data e autore
- Output
- Una tabella comparativa delle tre pagine.

90's I MODULI IN DETTAGLIO

Attività 2 – Creazione del profilo di competenza digitale

Gli studenti compilano un autoritratto digitale, rispondendo a domande come:

- Cosa so fare davvero online?
- In cosa mi sento insicuro?
- Come proteggono i miei dati?
- So distinguere una fonte attendibile?
- Come uso i social per informarmi?
- So creare contenuti utili o presentazioni efficaci?

Risultato finale

Ogni studente crea:

✓ un'autovalutazione

✓ una lista di competenze da migliorare

✓ un impegno personale per il percorso

7. Obiettivi finali raggiunti dal modulo

Alla fine delle 2 ore lo studente deve:

- aver chiaro cosa sono le competenze digitali
- conoscere le 5 aree del DigComp 3.0
- saper valutare informazioni online
- comprendere opportunità e limiti delle IA generative
- saper riflettere sul proprio livello di cittadinanza digitale
- essere pronto per i moduli successivi del Patentino

I MODULI IN DETTAGLIO

INTELLIGENZA ARTIFICIALE A SCUOLA (2 ore)

Guida completa agli argomenti

1. Che cosa sono le IA generative

Concetti chiave da far capire agli studenti

- L'IA generativa non pensa, ma elabora pattern statistici.
- Genera testi, immagini, audio, video a partire da enormi quantità di dati.
- È una tecnologia "predittiva": calcola la parola (o il pixel) più probabile.

Cosa NON è

- Non è "magia".
- Non ha emozioni, esperienze, desideri.
- Non ha coscienza.

Esempi pratici da mostrare (se possibile)

- ChatGPT (testo)
- DALL·E / Midjourney (immagini)
- Suno / Udio (musica)
- Sora / Luma (video)

Obiettivo formativo

Aiutare gli studenti a vedere l'IA come uno strumento, non come un'autorità assoluta.

2. Cosa si può fare con l'IA (in modo utile e responsabile)

Usi permessi e consigliati

- Riassunti di contenuti complessi.
- Spiegazioni alternative degli argomenti scolastici.
- Mappe concettuali e schemi.
- Brainstorming per idee e progetti.
- Esercitazioni personalizzate (quiz, domande, flashcards).
- Simulazioni (interviste, dialoghi, role-play).
- Supporto alla scrittura (non sostitutivo del pensiero critico).

Usi particolarmente utili a scuola

- Preparare verifiche orali.
- Spiegare concetti difficili con parole più semplici.
- Allenarsi su problemi di matematica o logica.
- Migliorare testi, presentazioni, relazioni.

L'IA deve essere usata per cap

3. Cosa NON si può fare con l'IA generativa

Azioni vietate (etica, sicurezza, linee guida MIM)

- Inserire dati personali propri o altrui.
- Caricare foto di minori o persone riconoscibili.
- Usare l'IA per generare contenuti di violenza o discriminazione.
- Delegare all'IA compiti scolastici senza propria revisione.
- Aggirare verifiche, esami o consegne scolastiche.
- Diffondere deepfake o contenuti manipolati.

Azioni scorrette sul piano didattico

- Farsi fare un tema dall'IA senza rielaborarlo.
- Consegnare materiali generati senza dichiararlo.
- Usare l'IA per evitare lo sforzo cognitivo.

Impatto disciplinare

- Plagio → valutazione insufficiente.
- Violazioni privacy → segnalazione.
- Diffamazione / bullismo digitale → sanzioni disciplinari o legali.

90's I MODULI IN DETTAGLIO

4. Rischi dell'intelligenza artificiale

Rischi cognitivi

- "Allucinazioni": l'IA può inventare fatti e citazioni.
- Dipendenza: rischio di smettere di ragionare autonomamente.
- Bassa qualità informativa dei contenuti generati.

Rischi psicologici

- Manipolazione: contenuti personalizzati e persuasivi.
- Dipendenza emotiva (percezione dell'IA "amica").
- Confronto irrealistico con modelli generati.

Rischi sociali

- Deepfake, falsificazioni, disinformazione.
- Bullismo assistito da IA (es. foto false).
- Furto d'identità e impersonation.

Rischi legali

- Violazione del copyright.
- Diffusione di contenuti illegittimi.
- Trattamento scorretto di dati personali.

5. Etica dell'IA: principi da dare agli studenti

Principi europei (semplificati per studenti)

1. Trasparenza → dire quando si usa l'IA.
2. Controllo umano → decidiamo noi, non l'IA.
3. Affidabilità → verificare informazioni.
4. Privacy → non inserire dati personali.
5. Non danno → non usare l'IA per creare contenuti che feriscono.

Domande etiche da porsi sempre

- "Questo contenuto può danneggiare qualcuno?"
- "È rispettoso?"
- "Sto manipolando la percezione degli altri?"
- "Sono sicuro che l'informazione sia corretta?"

6. Plagio e copyright nell'era dell'IA

Cos'è plagio

- Presentare come proprio un contenuto generato da IA.
- Utilizzare testi altrui senza citare.
- Copiare immagini o video protetti.

Cos'è accettabile

- Usare l'IA come supporto, ma dichiarandolo.
- Riformulare contenuti generati.
- Usare immagini create per uso personale non commerciale (a seconda delle licenze).

Conclusione per gli studenti

"L'IA è un aiuto, non un sostituto della tua creatività."

90's I MODULI IN DETTAGLIO

7. Applicazioni utili nello studio

Testo e studio
- Riassunti personalizzati
- Spiegazioni passo-passo
- Mappe concettuali
- Glossari
- Ricerche simulate

Lingue straniere
- Traduzioni guidate
- Pronuncia assistita
- Dialoghi interattivi
- Correzione grammaticale

Matematica e scienze
- Spiegazione di esercizi
- Passaggi ragionati
- Generazione di test personalizzati

Organizzazione
- Pianificazione studio
- Promemoria
- Schede di ripasso

8. Prime regole del "AI Digital Citizenship"

1. Non condividere dati personali
Né tuoi né altrui.
2. Verifica sempre ciò che l'IA produce
Almeno con 2 fonti.
3. Dichiara se hai usato l'IA
Trasparenza = correttezza.
4. Non usare l'IA per ingannare
No plagio, no scorciatoie, no deepfake.
5. Mantieni il controllo umano
Tu prendi le decisioni finali.
6. Rispetta le persone
Anche quelle a cui l'IA può far male.
7. Pensa al futuro
Ciò che generi rimane online per anni

9. Perché questo modulo è fondamentale

Per gli studenti

- Capiscono uno strumento che useranno ovunque.
- Sviluppano competenze richieste in università e lavoro.
- Imparano a proteggersi da rischi e manipolazioni.

Per la scuola
- Risponde alle Linee guida MIM sull'IA.
- Collega Educazione Civica, competenze digitali, media literacy.
- Riduce plagio, scorciatoie e uso improprio.

Per la società digitale
- Aumenta consapevolezza e responsabilità.
- Riduce rischi e comportamenti scorretti.
- Promuove cittadinanza digitale attiva.

I MODULI IN DETTAGLIO

IDENTITÀ DIGITALE (2 ORE)

Guida completa agli argomenti

1. Cos'è l'identità digitale

Concetti chiave da far comprendere

- L'identità digitale è tutto ciò che ti rappresenta online:
  - informazioni
  - foto e video
  - commenti
  - profili social
  - cronologia di ricerca
  - tracce di comportamento
- Non coincide né con il nome né con un singolo profilo: è complessa e multipla.

Cosa devono capire gli studenti

- Ogni azione digitale forma o modifica la loro identità online.
- Parte dell'identità digitale sfugge al nostro controllo diretto.
- La nostra identità non è statica: evolve nel tempo, come nella vita reale.

2. Identità reale, digitale e percepita

Identità reale

- Chi siamo davvero: valori, comportamenti, storia personale.

Identità digitale

- Come appariamo online attraverso ciò che pubblichiamo (o che altri pubblicano su di noi).

Identità percepita

- Come gli altri ci vedono sul web: immagine costruita dagli altri.

Punti da evidenziare agli studenti

- Le tre identità spesso non coincidono.
- Online, anche piccole azioni possono influenzare la percezione degli altri.
- L'identità percepita ha un impatto reale su:
  - relazioni
  - opportunità scolastiche/professionali
  - reputazione

3. Oversharing e reputazione online

Oversharing = Condividere troppo

- foto intime
- informazioni personali
- opinioni impulsive
- sfoghi emotivi
- geolocalizzazione
- routine quotidiana

Perché è un problema

- Rimane online per anni (anche se cancellato).
- Può essere salvato, inoltrato, estratto dal contesto.
- Crea un'immagine distorta o vulnerabile.
- Incide su future selezioni universitarie e lavorative.

Reputazione online

- È il "curriculum invisibile" che ci segue.
- Si costruisce in modo attivo (post, commenti) e passivo (quello che gli altri pubblicano).
- Si può migliorare, ma non controllare del tutto.

90's I MODULI IN DETTAGLIO

4. Tracciabilità: tutto ciò che facciamo lascia un segno

Cosa si traccia online?

- ricerche
- preferenze
- like, commenti
- tempo trascorso su contenuti
- posizione e movimenti
- interazioni con app, siti e piattaforme
- voce, volto, movimenti (nei sistemi di IA)

Perché è importante?

- Modella quello che vediamo (algoritmi).
- Viene usato per personalizzare la pubblicità.
- Può essere sfruttato per profiling, manipolazioni, frodi.

5. Carbon footprint digitale: dati attivi e passivi

Dati attivi

Quelli che decidiamo di lasciare:

- foto
- post
- commenti
- informazioni nei profili

Dati passivi

Quelli raccolti senza che ce ne accorgiamo:

- indirizzo IP
- cronologia
- cookie
- dati dei sensori dello smartphone
- metadati delle foto

Messaggio centrale agli studenti

“Stai lasciando più tracce di quante immagini.”

6. Deepfake, doppi digitali e impersonation

Deepfake

- Video o audio generati artificialmente che sembrano veri.
- Rischi: bullismo, manipolazioni, fake news, ricatti.

Doppio digitale

- Avatar, profili secondari, versioni alternative di sé.
- Opportunità: creatività, privacy.
- Rischi: identità frammentata, comportamenti impropri.

Impersonation

- Qualcuno si finge te:
  - account fake
  - clonazione del profilo
  - furto di identità

Cosa devono imparare gli studenti

- A riconoscere segnali sospetti.
- A denunciare subito furti di identità.
- A proteggere foto e informazioni.

90's I MODULI IN DETTAGLIO

7. Costruire l'identità nell'era dei social

Come si forma l'identità online?

- contenuti pubblicati
- commenti lasciati
- community a cui apparteniamo
- pagine che seguiamo
- conversazioni in cui interveniamo

The "Highlight Effect"

I social mostrano solo momenti migliori → confronti tossici.

The "Echo Effect"

Gli algoritmi ci mostrano solo contenuti simili ai nostri gusti → identità rinforzata ma distorta.

Educazione al sé digitale

- Curare la propria presenza.
- Essere autentici ma non vulnerabili.
- Pubblicare pensando alle conseguenze.

8. Laboratorio 1 – "La mia impronta digitale"

Obiettivo

Rendere visibile ciò che normalmente è invisibile.

Passaggi

1. Lavoro individuale:
   - "Quali tracce ho lasciato online negli ultimi 12 mesi?"
   - Ricerca del proprio nome (solo se il docente ritiene opportuno).
2. Analisi guidata:
   - Che immagine restituisce?
   - Cosa non vorrei fosse visibile?
   - Cosa posso migliorare?

Output

Una mappa personale dell'identità digitale attuale.

9. Laboratorio 2 – Revisione del proprio profilo social

Cosa analizzare

- username
- bio e descrizione
- foto profilo
- post pubblici
- storie in evidenza
- commenti lasciati
- privacy attiva o passiva
- tag di altri utenti

Domande guida

- "Cosa comunica davvero questo profilo su di me?"
- "È coerente con chi sono?"
- "Sto mostrando troppo?"
- "Quali parti vorrei migliorare o nascondere?"

Attività conclusiva

Creazione della checklist del profilo sicuro e consapevole.

90's I MODULI IN DETTAGLIO

10. Obiettivi finali raggiunti dal modulo

Alla fine delle 2 ore lo studente:

- comprende cosa significa identità digitale
- riconosce rischi e opportunità
- sa distinguere identità reale / digitale / percepita
- conosce i rischi di deepfake, duplicazioni e furti di identità
- sa valutare la propria impronta digitale
- sa migliorare il proprio profilo social in modo sicuro e responsabile

I MODULI IN DETTAGLIO

PRIVACY E SICUREZZA: INTERAZIONI ONLINE (2 ORE)

Guida completa agli argomenti

1. Che cos'è la privacy digitale?

Cosa devono imparare gli studenti

- La privacy non è "non avere nulla da nascondere".
- La privacy è il diritto a controllare i propri dati.
- Decidere chi può vedere che cosa.
- Proteggere se stessi, la famiglia, i compagni.

Principi fondamentali

- Minimizzazione dei dati: fornire solo ciò che è necessario.
- Consenso consapevole: sapere cosa si accetta.
- Trasparenza: capire come vengono usati i dati.
- Controllo: poter modificare o cancellare i dati.

2. Che cos'è un dato personale? (GDPR spiegato semplice)

Definizione base

Un dato personale è qualunque informazione che identifica una persona.

Esempi concreti, comprensibili per gli studenti

- Nome, cognome
- Foto, audio, video
- Numero di telefono
- Email
- Chat e messaggi
- Indirizzo IP
- Geolocalizzazione
- Preferenze (like, tempo sui social)
- Dati scolastici (voti, assenze)

Dati "particolari" (ancora più delicati)

- salute
- orientamento
- opinioni
- dati biometrici (volto, impronta)

Messaggio chiave

"Ogni click rivela qualcosa su di te."

3. Rischi principali online

a) Phishing

Tentativo di rubare dati con messaggi falsi:

- finti link
- email allarmistiche ("il tuo account sarà chiuso")
- premi sospetti

Segnali da individuare:

- errori di ortografia
- indirizzi strani
- richieste urgenti
- link accorciati o sospetti

b) Hackeraggio di account

Come avviene:

- password deboli
- password uguali per tutto
- app non sicure
- accesso lasciato su device condivisi
- Wi-Fi pubblico

c) Truffe

- Esempi:
- "Hai vinto un iPhone!"
- "Invia il codice per confermare l'ordine"
- Finti corrieri
- Finti profili su social o gaming
- Truffe sentimentali

d) Furto d'identità

- Qualcuno si finge te online
- Crea profili falsi
- Usa le tue foto
- Entra nei tuoi account
- Compie atti illegali a tuo nome

Rischi reali

- danni reputazionali
- problemi scolastici
- bullismo digitale
- responsabilità legali

I MODULI IN DETTAGLIO

4. Sicurezza quotidiana: cosa fare ogni giorno

1. 2FA – Autenticazione a due fattori

La protezione più efficace:

- codice via SMS
- app dedicata (Google Authenticator)
- chiavi fisiche
- notifiche push

2. Password manager

Permette di creare e conservare password sicure:

- combinazioni lunghe
- difficili da indovinare
- diverse per ogni account

3. Gestione dei dispositivi

- blocco schermo
- aggiornamenti regolari
- antivirus (se necessario)
- evitare Wi-Fi pubblici
- niente download da siti strani

4. Pulizia digitale

- disattivare app inutili
- chiudere accessi ai dispositivi condivisi
- cancellare periodicamente la cronologia
- controllare permessi delle app

5. Comportamenti sicuri nelle interazioni online

a) Chat e gruppi

- Non condividere dati personali
- Non inviare foto personali o intime
- Non inoltrare contenuti di altri senza consenso
- Segnalare comportamenti aggressivi o sospetti
- Chiedere il permesso prima di aggiungere qualcuno in un gruppo

b) Social

- Account privati (non pubblici)
- Controllo dei tag
- Niente geolocalizzazione
- Attenzione a storie e live: visibili anche a sconosciuti
- Non rispondere a messaggi sospetti o provocatori

c) Gaming online

- Nickname non riconducibili a dati personali
- No chat vocali con sconosciuti senza cautela
- Attenti alle richieste di:
  - scambi strani
  - regali
  - codici
  - informazioni personali
- Evitare microtransazioni senza consenso dei genitori
- Segnalare giocatori tossici o molesti

I MODULI IN DETTAGLIO

6. Laboratorio 1 – Analisi di messaggi: phishing e truffe

Attività

Il docente presenta:

- 3 messaggi fittizi di phishing
- 2 truffe via social
- 1 esempio di furto d'identità

Obiettivo

Gli studenti devono:

- individuare i segnali di rischio
- spiegare perché il messaggio è sospetto
- proporre la risposta più sicura ("non apro", "non rispondo", "segnalo")

7. Laboratorio 2 – Impostazione della privacy su un social

Passaggi

1. Scegliere un social (Instagram, TikTok, WhatsApp, Discord).
2. Rivedere insieme tutte le sezioni privacy:
   - chi può vedere i contenuti
   - chi può mandare DM
   - chi può commentare
   - gestione tag
   - storie
   - tracking pubblicitario
   - sincronizzazione contatti
3. Attivare la configurazione più sicura possibile.

Output per lo studente

- screenshot delle impostazioni corrette
- checklist finale del profilo sicuro

8. Obiettivi raggiunti dal modulo

Alla fine delle 2 ore lo studente:

- conosce il GDPR in modo semplice
- sa riconoscere le principali minacce online
- usa strumenti di sicurezza (password, 2FA, permessi)
- applica comportamenti corretti in chat, social e gaming
- sa configurare correttamente la privacy del proprio profilo
- riconosce phishing e truffe

I MODULI IN DETTAGLIO

ASPETTI GIURIDICI (2 ORE)

Guida completa agli argomenti

1. Perché studiare gli aspetti giuridici del digitale?

Cosa devono capire gli studenti

- Online valgono le stesse leggi del mondo reale, più alcune regole specifiche.
- Ciò che pubblichiamo può avere conseguenze reali, legali e disciplinari.
- Anche i minori possono commettere reati digitali.
- La conoscenza delle norme non serve a "fare paura", ma a prevenire danni e tutelare sé stessi e gli altri.

2. Cyberbullismo – Legge 71/2017

Cos'è il cyberbullismo

Qualsiasi comportamento aggressivo online contro una persona:

- insulti
- minacce
- diffusione di foto
- derisione
- esclusioni dai gruppi
- profili falsi per prendere in giro
- diffusioni di video umilianti

Cosa prevede la Legge 71/2017

- La vittima può chiedere la rimozione dei contenuti.
- La scuola deve attivare procedure interne di tutela.
- Gli autori (anche minori) devono essere ammoniti dalle autorità.
- Possibili responsabilità civili dei genitori.

Messaggio chiave

Online nulla "è uno scherzo": può diventare reato.

3. Reati digitali principali

a) Diffamazione (art. 595 c.p.)

Diffondere contenuti che danneggiano la reputazione di una persona.

Online è considerata aggravata.

Esempi scolastici:

- Post offensivi su un compagno.
- Meme che ridicolizzano una persona reale.
- Commenti denigratori.

b) Minacce (art. 612 c.p.)

Far temere un male ingiusto e grave a qualcuno.

Valgono anche messaggi, chat, vocali.

Esempi:

- "Se non fai X ti rovino".
- "Domani a scuola ti faccio vedere io".

c) Revenge porn / Diffusione illecita di immagini (art. 612-ter c.p.)

Diffondere o inviare immagini intime senza consenso, anche se ricevute volontariamente.

Perché è grave:

- colpisce soprattutto minori
- è punito severamente
- le immagini si diffondono velocemente
- causa danni psicologici enormi

Anche inoltrare un contenuto intimo senza consenso è reato.

d) Condivisione di immagini altrui senza consenso

Anche immagini non intime:

- foto di compagni
- foto di insegnanti
- screenshot di chat
- audio, vocali, video scolastici

Violazione della privacy + possibili reati + sanzioni scolastiche.

I MODULI IN DETTAGLIO

4. Età minima per i social e Termini di Servizio

Età minima generale in UE

13 anni (GDPR – consenso digitale)

Ma ogni piattaforma può alzare l'età:

- TikTok → 13 anni (con limitazioni fino ai 18)
- Instagram → 13 anni
- YouTube → 13 anni
- WhatsApp → 13 anni
- Discord → 13 anni

Perché esiste l'età minima?

- Per proteggere i minori da contenuti rischiosi
- Per limitare raccolta dati
- Per ridurre grooming, adescamento, bullismo

Termini di Servizio (TOS)

Ogni piattaforma stabilisce:

- cosa è consentito pubblicare
- cosa è vietato
- le sanzioni in caso di violazione

Molti studenti accettano i TOS senza leggerli → rischio altissimo.

5. Responsabilità: penale, civile e scolastica

Responsabilità penale

- Alcuni reati possono essere compiuti anche dai minori
- Prima dei 14 anni non c'è responsabilità penale, ma:
  - può intervenire il tribunale dei minori
  - possono esserci ammonimenti
- Dai 14 ai 18 anni → responsabilità penale con attenuanti

Responsabilità civile

- I genitori rispondono dei danni causati dai figli minori
- Risarcimento economico in caso di:
  - offese
  - condivisione di contenuti
  - danni alla reputazione
  - atti di bullismo o cyberbullismo

Responsabilità scolastica

Le scuole possono applicare sanzioni disciplinari:

- richiamo scritto
- sospensione
- attività riparative
- coinvolgimento del Garante privacy se necessario

6. Come distinguere ciò che è lecito da ciò che non lo è

Lecito

✓ commentare in modo rispettoso
✓ esprimere opinioni senza insultare
✓ condividere contenuti creati da sé
✓ usare app e social nel rispetto dei TOS

Non lecito

✗ insultare, minacciare, ridicolizzare
✗ condividere foto di altri senza consenso
✗ violare la privacy di compagni/professore
✗ creare profili falsi
✗ usare l'IA per creare deepfake di persone reali
✗ diffondere contenuti intimi
✗ accedere ad account non propri

Il confine tra "scherzo" e "reato" online è molto più sottile.

7. Laboratorio 1 – Role-play "È reato o non lo è?"

Attività

Il docente presenta 6 scenari realistici:

1. Screenshot di un compagno preso in giro
2. Foto del prof pubblicata in un meme
3. Commenti insultanti in un gruppo
4. Profilo fake per ridicolizzare un amico
5. Inoltro di una foto intima ricevuta privatamente
6. Messaggio minaccioso in una chat di classe

Gli studenti devono:

- discutere
- classificare: lecito / illecito / reato
- motivare le loro scelte

I MODULI IN DETTAGLIO

8. Laboratorio 2 – Analisi di casi reali

Obiettivo
Rendere concreta la legge attraverso storie vere (anonime).
Esempi di casi (descritti senza nomi)

- video umiliante diffuso in classe
- minacce in chat scolastica
- ragazza la cui foto privata è stata inoltrata
- profilo fake creato per deridere un compagno
- audio manipolato tramite IA

Gli studenti devono individuare:

- quale reato è stato commesso
- quali conseguenze ci sono state
- come si poteva evitare

9. Obiettivi finali raggiunti dal modulo

Alla fine delle 2 ore lo studente:

- conosce i reati digitali più comuni
- sa distinguere comportamento scorretto da comportamento illecito
- comprende le responsabilità personali e dei genitori
- conosce i propri diritti e doveri online
- è più prudente nel pubblicare, condividere e commentare
- sa riconoscere situazioni da segnalare

I MODULI IN DETTAGLIO

SVILUPPO DEL SENSO CRITICO (2 ORE)

Guida completa agli argomenti

1. Perché serve il senso critico nel mondo digitale

Cosa devono capire gli studenti

- Online non vediamo la realtà, ma una selezione della realtà.
- Non tutte le informazioni sono vere, neutrali o complete.
- Per orientarsi serve saper analizzare, confrontare, dubitare.
- Il senso critico è una competenza fondamentale nel XXI secolo, utile:
  - a scuola
  - nella vita sociale
  - nel lavoro
  - nella partecipazione civica

Messaggio chiave

"Non credere a tutto ciò che vedi online. Nemmeno se sembra vero."

2. Algoritmi e bolle informative

Cosa sono gli algoritmi?

- Regole che decidono cosa vedere prima o dopo.
- Non mostrano tutto: selezionano contenuti per noi.
- Influenzano le nostre preferenze, emozioni e opinioni.

Esempi pratici

- Perché su Instagram vedo sempre gli stessi tipi di post.
- Perché su TikTok ricevo video simili ai miei ultimi like.

Bolle informative (filter bubbles)

- Ogni studente vede una versione diversa del mondo.
- I contenuti che confermano le nostre idee vengono mostrati di più.
- Altre opinioni vengono nascoste.
- Questo ci fa credere che "tutti la pensino come noi".

Echo chambers (camere dell'eco)

- Ci circondiamo (online) di persone che dicono ciò che vogliamo sentire.
- Le opinioni si rinforzano, diventano estreme.
- Le differenze vengono amplificate.

Effetto sugli studenti

- Si diventa meno aperti
- Si discute meno
- Si litiga di più
- Si cade più facilmente nella disinformazione

3. Disinformazione, misinformazione e manipolazione

Disinformazione

- Informazioni false create per manipolare.
- Ha uno scopo: politica, soldi, odio.

Misinformazione

- Informazioni false diffuse per errore.
- Le condividiamo perché sembrano vere.

Malinformazione

- Informazioni vere usate per danneggiare.
- (es. screenshot fuori contesto)

Tecniche comuni di manipolazione

- Titoli emotivi ("shock", "scandalo")
- Immagini alterate
- Dati inventati o estratti dal contesto
- Bot e account falsi
- Video ritagliati in modo ingannevole
- Foto con angolazioni "strategiche"

I MODULI IN DETTAGLIO

4. Fake news, clickbait e deepfake

Fake news

- Contenuti deliberatamente falsi o manipolati
- Sembrano notizie reali, ma non lo sono

Clickbait

- Titoli esagerati per farci cliccare
- Spesso promettono qualcosa che il contenuto non conferma
- Alimentano disinformazione e curiosità tossica

Esempi:

- "Non crederai a ciò che è successo dopo…"
- "Shock in Italia: nessuno te lo dirà!"

Deepfake

- Video, audio o foto creati artificialmente per sembrare veri
- Molto pericolosi perché credibili e virali
- Possibili usi per:
  - bullismo
  - ricatti
  - propaganda
  - discredito verso persone reali

Gli studenti devono imparare a dubitare anche dei video "perfetti".

5. Come sviluppare il senso critico: 5 domande essenziali

1. Chi ha creato questo contenuto?
È affidabile? È una fonte nota?
2. Qual è lo scopo?
Informare, vendere, manipolare, intrattenere?
3. È supportato da prove?
Fonti, dati, link verificabili.
4. È emotivo o neutro?
Se punta a far arrabbiare o spaventare → probabilmente manipola.
5. È troppo bello (o troppo brutto) per essere vero?
Attenzione a contenuti estremi.

6. Fact-checking: strumenti essenziali

Siti utili (adatti agli studenti)

- Facta.news
- Pagella Politica
- BUTAC
- Open – Fact Checking
- Google Fact Check Explorer

Strumenti tecnici

- Reverse Image Search (Google Immagini)
- Tineye (per verificare immagini rubate)
- InVID (per verificare video)
- Whois (per vedere proprietà di un sito)

Metodi rapidi

- Confrontare più fonti
- Verificare data e autore
- Cercare la notizia in giornali affidabili
- Analizzare commenti e contesto

7. Laboratorio 1 – Fact-checking di un post virale

Attività

1. Scegliere un post virale visto dagli studenti (o fornito dal docente)
2. Analizzare:
   - chi lo ha pubblicato
   - quali fonti cita
   - se le immagini sono autentiche
   - se il titolo è clickbait
3. Verificare con:
   - Google Immagini
   - siti di verifica
   - confronto fonti

Obiettivo

Capire se il contenuto è:

- vero
- falso
- parzialmente vero
- manipolato

I MODULI IN DETTAGLIO

8. Laboratorio 2 – Analisi di un deepfake

Attività

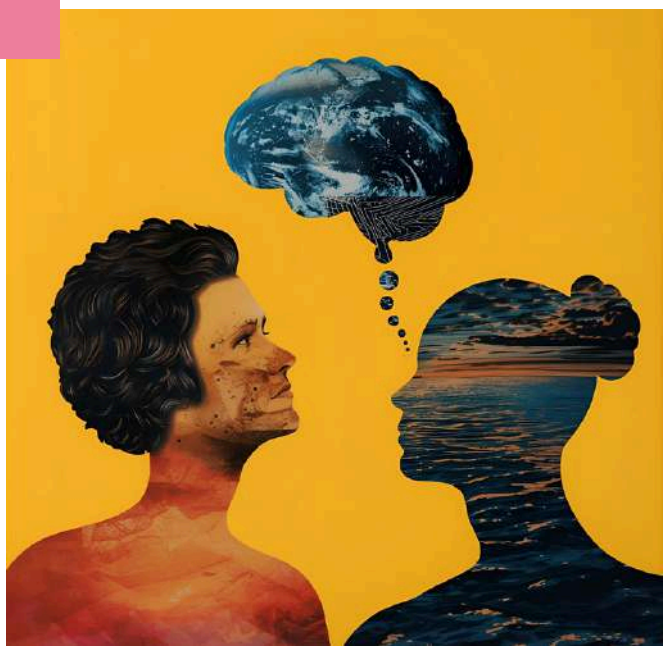
Il docente mostra un deepfake sicuro e appropriato.

Gli studenti devono individuare:

- movimenti anomali
- labiale non coerente
- ombre irreali
- audio "robotico"
- sfondi fossili o distorsioni

Obiettivo del laboratorio

- Sviluppare attenzione ai dettagli
- Aumentare la consapevolezza del rischio
- Capire che anche ciò che vediamo può essere manipolato



9. Obiettivi finali raggiunti dal modulo

Alla fine delle 2 ore lo studente:

- analizza contenuti online con occhio critico
- conosce bias, bolle informative e manipolazioni
- riconosce fake news, clickbait e deepfake
- sa verificare informazioni con strumenti concreti
- comprende il funzionamento degli algoritmi
- è meno influenzabile dai contenuti manipolatori

I MODULI IN DETTAGLIO

UTILIZZO RESPONSABILE DEI SOCIAL MEDIA (2 ORE)

Guida completa agli argomenti

1. Perché parlare di “uso responsabile” dei social?

Cosa devono capire gli studenti

- I social non sono solo intrattenimento: plasmano identità, relazioni e comportamenti.
- Ogni contenuto può restare online per anni.
- I social sono progettati per trattenere l’attenzione → servono consapevolezza e regole.
- Un uso scorretto può generare rischi psicologici, sociali, legali.

Messaggio chiave

“I social amplificano ciò che fai. Se li usi bene, amplificano opportunità. Se li usi male, amplificano rischi.”

2. Linguaggio digitale e Netiquette

Cos’è la netiquette?

Il codice di comportamento online che aiuta a:

- comunicare in modo chiaro
- evitare conflitti
- rispettare gli altri
- prevenire fraintendimenti

Principi essenziali

- pensare prima di inviare
- evitare aggressività, sarcasmo, insulti
- rispettare opinioni diverse
- non usare i social per sfogarsi
- evitare le “guerre di commenti”

Esempi di buona comunicazione

- commenti costruttivi
- domande rispettose
- tono cortese
- evitare MAIUSCOLE (percepite come urla)

3. Effetti psicologici dei social media

Aspetti positivi

- creatività
- connessione con coetanei
- scoperta di talenti
- opportunità di espressione

Aspetti negativi

- confronti continui (“highlight effect”)
- ansia da prestazione digitale
- FOMO (paura di essere esclusi)
- dipendenza da like e notifiche
- ricerca costante di approvazione
- sleep procrastination (uso dei social fino a notte)

4. Comportamenti a rischio sui social

Esempi concreti

- oversharing (condivisione eccessiva)
- post impulsivi
- “screenshottare” chat private
- pubblicazione di contenuti impropri
- partecipazione a challenge pericolose
- commenti aggressivi o provocatori
- flirt eccessivo con sconosciuti

Ogni comportamento crea un’impronta digitale.

I MODULI IN DETTAGLIO

5. Pubblicare con consapevolezza

Tre domande d'oro:

1. "Mi rappresenta?"
2. "Posso pentirmi di questo contenuto tra 1 anno?"
3. "Cosa penseranno compagni, docenti, familiari, futuri selezionatori?"

Tipologie di contenuti da evitare:

- foto intime o a rischio
- foto di terzi senza consenso
- contenuti a sfondo violento o discriminatorio
- screenshot di valutazioni scolastiche
- informazioni personali (indirizzo, scuola, routine)

"Ciò che metti online può essere usato contro di te, anche senza cattiveria."

6. Gestione di privacy e sicurezza sui social

Impostazioni fondamentali

- account privato
- approvazione dei tag
- controllo commenti
- disattivazione geolocalizzazione
- limitazione dei DM
- gestione delle liste di amici

Consigli pratici

- non accettare richieste da sconosciuti
- evitare di pubblicare in tempo reale spostamenti
- controllare chi può vedere le storie
- non fare live in luoghi sensibili (scuola, casa, palestra)

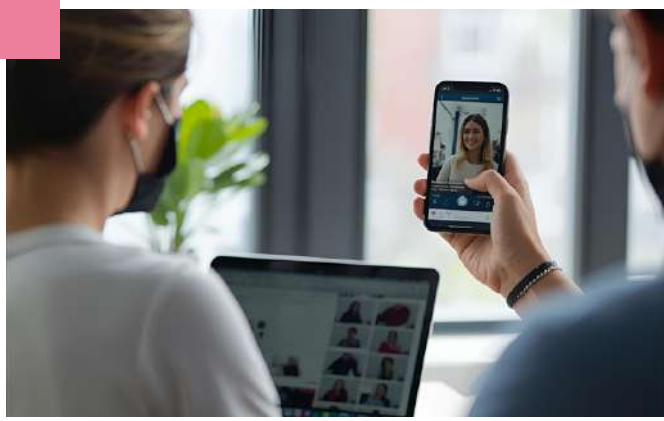
7. Influencer, pubblicità nascosta e modelli irrealistici

Cosa devono sapere gli studenti

- molti contenuti sono sponsorizzati
- molti influencer mostrano solo "il lato bello"
- spesso non dichiarano la pubblicità
- i corpi e le vite rappresentate non sono reali
- i filtri creano standard estetici distorti

Rischi:

- insoddisfazione corporea
- dipendenza dal confronto
- compulsione all'acquisto
- percezione distorta della realtà



8. Algoritmi nei social: perché vediamo ciò che vediamo

Gli algoritmi scelgono in base a:

- interessi
- tempo trascorso sui contenuti
- profili seguiti
- interazioni (like, commenti, salvataggi)
- comportamenti simili di persone simili

Conseguenze:

- contenuti ripetitivi
- rafforzamento di opinioni (echo chamber)
- dipendenza da stimoli emozionali
- invisibilità di punti di vista diversi

9. Cyberetiquette nei gruppi e nelle chat

Regole fondamentali

- non condividere screenshot senza consenso
- non diffondere audio o foto private
- evitare discussioni infinite
- rispettare silenzio e orari
- evitare spam
- non ridicolizzare compagni
- non usare chat per esclusioni sociali

Esempi da gestire con attenzione

- gruppi di classe
- gruppi gaming
- server Discord
- chat "parallele" di gossip

90's I MODULI IN DETTAGLIO

10. Relazioni online: rispetto e confini

Relazioni sane

- comunicazione chiara
- consensi espliciti
- rispetto dei confini
- niente pressioni emotive o intime
- interazione rispettosa

Segnali di allarme

- richieste di foto
- gelosia digitale
- controllo degli accessi
- manipolazione ("se mi volessi bene…")
- messaggi ossessivi

11. Il ruolo dei social nella reputazione digitale

Come si forma la reputazione

- ciò che pubblichi
- ciò che commenti
- ciò che gli altri pubblicano su di te
- gruppi a cui partecipi
- comportamenti problematici

Importante per:

- scuola
- università
- tirocinio
- lavoro
- relazioni personali

12. Laboratorio – Parte 1: Revisione dei propri social

Attività

Gli studenti analizzano:

- foto profilo
- bio
- post pubblici
- tag ricevuti
- commenti lasciati
- privacy attiva
- storie in evidenza

Domanda chiave:

"Questo profilo rappresenta la persona che voglio essere?"

13. Laboratorio – Parte 2: Creazione della "Carta dello Studente Digitale"

Gli studenti elaborano un breve documento con:

- le 10 regole personali di buon uso dei social
- le proprie "zone critiche" (cose da evitare)
- strategie per gestire emozioni digitali (FOMO, confronti tossici)
- limiti personali (orari, notifiche, contenuti da evitare)

14. Obiettivi finali raggiunti dal modulo

Alla fine delle 2 ore lo studente:

- usa i social con consapevolezza e tutela della privacy
- riconosce i comportamenti rischiosi
- comunica online in modo rispettoso
- conosce le basi della reputazione digitale
- gestisce i social senza dipendenza emotiva
- migliora il proprio profilo digitale

I MODULI IN DETTAGLIO

RISCHIO DELLE INTERAZIONI ONLINE (2 ORE)

Guida completa agli argomenti

1. Perché parlare di rischi nelle interazioni online

Cosa devono capire gli studenti

- Non tutte le persone online sono ciò che dicono di essere.
- Le interazioni digitali possono diventare rischiose senza accorgercene.
- I comportamenti digitali possono avere conseguenze psicologiche, relazionali e legali.
- Il rischio non è "colpa" della vittima: è responsabilità degli adulti insegnare la prevenzione.

Messaggio chiave

"La prevenzione è più forte del pericolo."

2. Grooming: cos'è e come funziona

Grooming

Il processo con cui un adulto manipola un minore per ottenere:

- fiducia
- segreti
- foto/video privati
- incontri

Le 6 fasi tipiche (semplificate per studenti)

1. Contatto – "Ciao, come va?"
2. Costruzione del rapporto – "Abbiamo gli stessi interessi"
3. Isolamento – "Non dirlo ai tuoi amici/genitori"
4. Normalizzazione – "È normale tra persone che si vogliono bene"
5. Richieste inappropriate – foto, video, confidenze intime
6. Ricatto/controllo – "Se non fai questo, invio tutto a tutti"

Segnali da riconoscere

- persona sempre disponibile
- messaggi segreti o notturni
- richieste di privacy
- complimenti eccessivi o strani
- domande personali insistenti

3. Sexting e Sextortion

Sexting

Condivisione volontaria di contenuti intimi:

- foto
- video
- messaggi

Rischi

- diffusione non consensuale
- screenshot
- perdita di controllo dei contenuti
- ricatti (sextortion)

Sextortion

Ricatto basato su immagini intime.

Come funziona

- minaccia di pubblicare contenuti
- richiesta di soldi, foto, favore
- pressione emotiva e psicologica

Segnali

- richieste improvvise
- minacce velate
- profilo anonimo o appena creato
- aumento improvviso del controllo nei messaggi

Cosa fare

- non farsi intimorire
- non pagare
- salvare prove
- parlare subito con adulto/docente
- denunciare

90's I MODULI IN DETTAGLIO

4. Challenge pericolose e comportamenti a rischio

Tipologie

- fisiche (soffocamento, autolesionismo)
- sociali (umiliazione pubblica)
- rischi invisibili (sfide alimentate dagli algoritmi)

Perché catturano gli adolescenti

- bisogno di approvazione
- pressione del gruppo
- viralità
- ricerca di visibilità

Segnali di pericolo

- contenuti estremi o rischiosi
- "Non provate a farlo a casa"
- sfide che richiedono dolore, paura o rischio fisico
- commenti che incitano

5. Gaming online: rischi nascosti

Toxic behavior

- insulti
- umiliazioni
- esclusioni
- pressioni a comportarsi in un certo modo

Effetti

- stress
- rabbia
- burnout
- isolamento

Acquisti inconsapevoli / loot box

Rischi:

- spesa non voluta
- dipendenza da microtransazioni
- rischio simile al gioco d'azzardo

Interazioni con sconosciuti

Rischi:

- grooming
- bullismo
- richieste di "regali"
- ricatti
- pressioni per foto/video

6. Psicologia dell'inganno e manipolazione

Come agiscono gli ingannatori

- sfruttano emozioni forti: paura, vergogna, rabbia
- promettono segretezza
- alternano gentilezza e minacce
- manipolano autostima e bisogno di approvazione
- isolano la vittima

I meccanismi più comuni

- "Solo tu mi capisci"
- "Fidati di me"
- "Non dire niente a nessuno"
- "Se non lo fai vuol dire che non ci tieni"
- "Ti succederà qualcosa"

Strategie per proteggersi

- tagliare subito il contatto
- non farsi convincere da complimenti eccessivi
- ascoltare i segnali di disagio
- chiedere aiuto senza paura

7. Come chiedere aiuto in modo sicuro

A chi rivolgersi

- genitori
- docenti
- referente bullismo
- psicologo scolastico
- adulti di riferimento
- forze dell'ordine (se necessario)

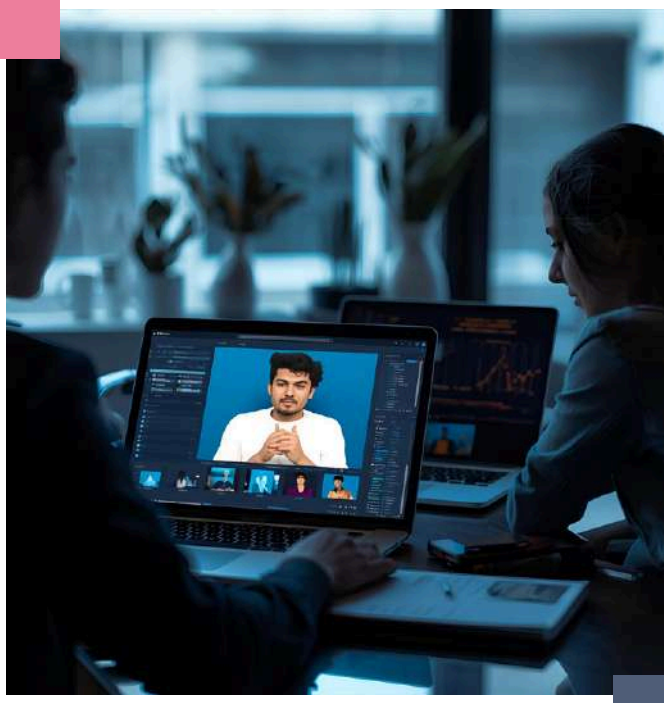
Perché chiedere aiuto

- non è colpa della vittima
- non si è soli
- casi risolti → protezione immediata
- il silenzio peggiora la situazione

Frasi guida per gli studenti

- "Ho bisogno di parlarti di qualcosa di importante."
- "Mi sento a disagio per dei messaggi ricevuti."
- "Credo di essere in una situazione rischiosa."

I MODULI IN DETTAGLIO



8. Laboratorio 1 – Analisi di casi reali (protetti)

Attività

Il docente presenta casi anonimizzati, su:

- grooming
- sexting diffuso
- ricatto digitale
- challenge pericolosa
- comportamenti tossici nel gaming

Obiettivi

- individuare il rischio
- capire come evitarlo
- riconoscere cosa ha permesso la manipolazione
- proporre la risposta corretta

9. Laboratorio 2 – Simulazione di conversazioni sospette

Modalità

Gli studenti analizzano messaggi fittizi per identificare:

- complimenti strani
- richieste inappropriate
- domande personali
- pressione psicologica
- tentativi di manipolazione
- segnali di grooming o ricatto

Obiettivi

- riconoscere immediatamente segnali di rischio
- allenare la risposta protettiva (“non rispondo”, “blocco”, “segnalo”)
- sviluppare sicurezza nell’auto-protezione

10. Obiettivi finali raggiunti dal modulo

Alla fine delle 2 ore lo studente:

- riconosce grooming, sexting, sextortion
- conosce i rischi delle challenge e dei comportamenti a rischio
- gestisce in modo consapevole le interazioni nel gaming
- sa riconoscere manipolazione e inganno
- conosce strategie di protezione
- sa a chi chiedere aiuto
- sviluppa forza, consapevolezza e autonomia

I MODULI IN DETTAGLIO

SALUTE E BENESSERE DIGITALE (2 ORE)

Guida completa agli argomenti

1. Perché il benessere digitale è fondamentale

Cosa devono capire gli studenti

- Il digitale non è "neutro": influenza corpo, mente, emozioni.
- Senza equilibrio si rischiano stress, dipendenze e calo del benessere generale.
- La salute digitale riguarda:
  - tempo online
  - posture
  - sonno
  - gestione emotiva
  - relazione con gli altri
  - consapevolezza di sé

Messaggio chiave

"Il digitale deve migliorare la vita, non sostituirla."

2. FOMO, dipendenze e doomscrolling

FOMO (Fear Of Missing Out)

- Paura di essere esclusi
- Ansia da notifiche
- Controllo compulsivo dei social
- Conseguenze: stress, bassa autostima, difficoltà a concentrarsi

Dipendenze digitali

Segnali:

- impossibilità di "staccare"
- irritazione quando si è offline
- uso compulsivo di social, gaming o messaggistica
- alterazione del ritmo del sonno
- calo scolastico o sociale

Cause:

- dopamina
- gratificazione immediata
- notifiche disegnate per "agganciare"
- pressione del gruppo

Doomscrolling

- Scorrere contenuti negativi senza riuscire a smettere
- Porta a:
  - ansia
  - pessimismo
  - insonnia
  - difficoltà di concentrazione

I MODULI IN DETTAGLIO

3. Sonno, postura, vista, attività fisica

Sonno

Problemi:

- esposizione a luce blu → ritarda il sonno
- uso del telefono a letto
- notifiche notturne
- binge-watching serale

Consigli:

- stop schermi 1 ora prima di dormire
- niente device in camera
- modalità "notte" attiva
- routine costante

Vista

Rischi:

- affaticamento visivo
- secchezza oculare
- mal di testa

Regola d'oro:

✓ Regola 20-20-20

Ogni 20 minuti → guarda 20 secondi → a 20 piedi (6 metri)

Postura

Errori comuni:

- testa piegata sul telefono
- spalle curve
- gambe accavallate per ore
- posizione rigida

Soluzioni:

- schermo all'altezza degli occhi
- pause ogni 30-40 minuti
- stretching leggero
- seduta ergonomica

Attività fisica

- contrasta lo stress
- migliora umore e concentrazione
- riduce tensioni da postura
- bilancia il tempo online

Minimo raccomandato:

- 30 minuti al giorno di movimento leggero o moderato

4. Benessere psicologico: la netiquette emotiva

La netiquette psicologica riguarda:

- come gestiamo emozioni online
- come reagiamo ai contenuti
- come trattiamo gli altri

Regole:

- evitare confronti tossici
- non inseguire like o approvazioni
- limitare contenuti negativi
- evitare discussioni infinite
- imparare a riconoscere manipolazioni emotive

5. LifeComp e autoconsapevolezza digitale

Cosa è la LifeComp

Il quadro europeo delle competenze per la vita personale, sociale e professionale.

Tre aree:

1. Personal – autoconsapevolezza, gestione delle emozioni
2. Social – empatia, collaborazione, rispetto
3. Learning to learn – motivazione, autonomia, organizzazione

Collegamento con il digitale

- gestire il proprio tempo online
- riconoscere emozioni generate dai social
- comunicare con empatia
- prendere decisioni consapevoli
- autoregolare impulsi e dipendenze digitali

90's I MODULI IN DETTAGLIO

6. Come costruire un equilibrio online/offline

Strategie pratiche

- notifiche disattivate per app non essenziali
- limiti di tempo per social e gaming
- routine di studio senza telefono
- zone “no digital” (tavola, camera, bagno)
- praticare hobby offline
- pause regolari
- routine mattina/sera senza schermi

Check personale

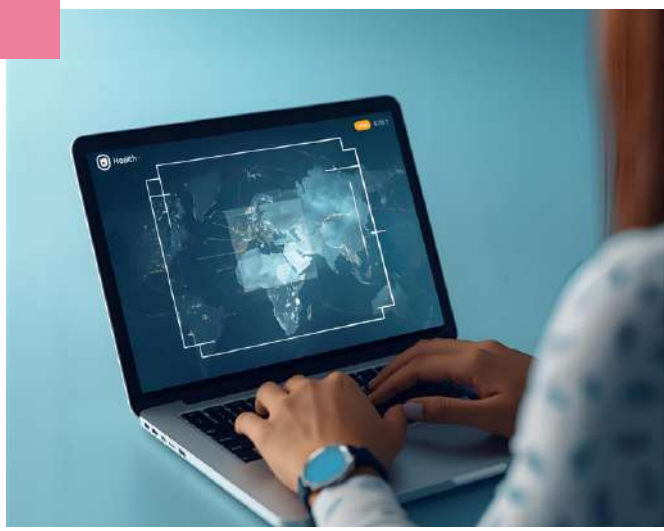
Chiediti:

- quanto tempo passo ogni giorno sui social?
- come mi sento dopo una sessione lunga?
- sto dormendo bene?
- sto trascurando amici o attività?
- il digitale mi aggiunge stress?

7. Laboratorio 1 – Piano personale di Benessere Digitale

Gli studenti creano un piano personalizzato con:

- obiettivi (es. “meno notifiche”, “stop telefono dopo le 22”)
- limiti (minuti giornalieri di social/gaming)
- strategie (routine, zone no-digital, orari)
- indicatori di benessere (sonno, concentrazione, umore)
- attività offline preferite
- segnali di allarme da monitorare



8. Laboratorio 2 – Monitoraggio (facoltativo)

Per una settimana gli studenti possono:

- monitorare il tempo di utilizzo dello smartphone
- annotare emozioni post-utilizzo
- verificare miglioramenti nel sonno
- controllare posture e pause
- valutare l’efficacia delle strategie adottate

Obiettivo:

- aumentare autoconsapevolezza
- correggere abitudini
- consolidare equilibrio e benessere

9. Obiettivi finali raggiunti dal modulo

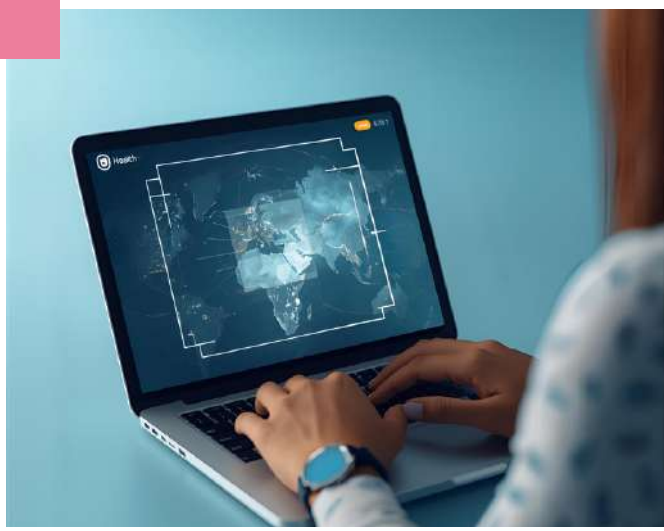
Alla fine delle 2 ore lo studente:

- conosce i rischi per la salute digitale
- riconosce segnali di dipendenza
- gestisce FOMO, notifiche e uso compulsivo
- pratica la regola 20-20-20
- costruisce equilibrio tra online e offline
- sviluppa autoconsapevolezza e controllo
- crea un proprio piano di benessere digitale

I MODULI IN DETTAGLIO

MODULO 10 – AGCOM (2 ORE)

Guida completa agli argomenti



10. Laboratorio 1

90's

I MODULI IN DETTAGLIO

Calendario attività

WEB REPUTATION

1. ***Martedì 03 marzo 2026, ore 10:00 - 12:00*** *- Identità digitale*
2. ***Martedì 10 marzo 2026, ore 10:00 - 12:00****- Privacy e sicurezza*
3. ***Martedì 17 marzo 2026, ore 10:00 - 12:00*** *- Salute e benessere digitale*

I MECCANISMI DI FUNZIONAMENTO

1. ***Martedì 24 marzo 2026, ore 10:00 - 12:00*** *- Competenze digitali*
2. ***Martedì 31 marzo 2026, ore 10:00 - 12:00*** *- Intelligenza artificiale a scuola*
3. ***Martedì 14 aprile 2026, ore 10:00 - 12:00*** *- Sviluppo del senso critico*

DISINFORMAZIONE E HATE SPEECH

1. ***Martedì 21 aprile 2026, ore 10:00 - 12:00*** *- Aspetti giuridici*
2. ***Martedì 28 aprile 2026, ore 10:00 - 12:00*** *- Utilizzo responsabile dei social media*
3. ***Martedì 05 maggio 2026, ore 10:00 - 12:00*** *- Rischio delle interazioni online*

CORECOM

1. ***Martedì 12 maggio 2026, ore 10:00 - 12:00***

Forrmatori:

- ***Alfonso Benevento****, Giornalista, Saggista, Esperto in I.A. e robotica educativa, consulente sull'innovazione digitale - Comitato Scientifico Associazione Protezione Diritti e Libertà Privacy APS*
- ***Antonio Carmine Didona,*** *Consulente in materia di privacy - Data Protection Officer - Socio Associazione Protezione Diritti e Libertà Privacy APS*
- ***Luca Di Leo, Consulente in materia di privacy - Data Protection Officer - Vice Presidente Associazione Protezione Diritti e Libertà Privacy APS***
- ***Gloria Paci****, Consulente in materia di privacy - Data Protection Officer - Presidente Associazione Protezione Diritti e Libertà Privacy APS*

I MODULI IN DETTAGLIO

GIUGNO

EVENTO DI CHIUSURA IN PRESENZA (CONSEGNA DEI PATENTINI DIGITALI)

La data e il format saranno concordati con il Co.Re.Com. cosí come i relatori e gli ospiti da invitare (rappresentanti istituzionali, giornalisti e altre categorie).

MODALITÀ DI EROGAZIONE DEI MODULI

Mista: sincrona e asincrona

MATERIALI

Schede pedagogiche per i docenti al fine dell'utilizzo per le UDA; Materiale in formato digitale per gli studenti

DESTINATARI

Studenti delle scuole secondarie di primo e secondo grado

I MODULI IN DETTAGLIO

GIUGNO

FORMATORI

(Si prega di notare che la lista non é da considerarsi definitiva in quanto puó essere soggetta a cambiamenti in base alla disponibilitá degli stessi)

REPORTISTICA FINALE DEL PERCORSO

- **Un Report finale verrá inviato al Co.re.com. a cura dell' Associazione Protezione Diritti e Libertá Privacy APS, documentando:**
- **Quante scuole hanno partecipato;**
- **Quanti studenti hanno partecipato per singola scuola;**
- **Quanti studenti hanno completato il percorso;**
- **Risultati dell'apprendimento: punteggi dei test/tassi di successo)**
- **Feedback degli studenti: Le opinioni raccolte tramite sondaggi sulla rilevanza, l'efficacia e l'utilità del corso.**
- **Raggiungimento degli obiettivi, le lezioni apprese, le aree di miglioramento**