

AMBASCIATORI DI SICUREZZA INFORMATICA & EDUCAZIONE DIGITALE CONSAPEVOLE

***Il Patentino Digitale: navigare il futuro online con
consapevolezza e responsabilità!***

PROGETTO FORMATIVO

***PER LE SCUOLE SECONDARIE
DI PRIMO E SECONDO GRADO***

Anno scolastico 2025-2026

Moduli 1 – 9

© [2025] [Associazione protezione diritti e libertà privacy APS].
Tutti i diritti di traduzione, riproduzione e adattamento, totale o parziale, con qualsiasi mezzo, sono riservati per tutti i Paesi.
Ogni utilizzo non autorizzato del presente documento costituisce violazione del diritto d'autore (L. 22 aprile 1941, n. 633 e successive modifiche)

Identità Digitale

- Modulo 3 – Patentino Digitale Durata: 2 ore

Obiettivi del Modulo

- Capire cos'è l'identità digitale
- Riconoscere i rischi di oversharing e tracciabilità
- Comprendere come nasce la reputazione online
- Collegare identità digitale, libertà, responsabilità
- Saper leggere e migliorare la propria presenza online

Cos'è l'identità digitale?

- L'insieme di tutto ciò che ci rappresenta online
- Un'identità multipla e in continua evoluzione
- Foto, post, commenti, cronologie, preferenze
- Anche ciò che altri pubblicano su di noi
- È un'estensione della nostra identità reale

Tre livelli di identità

- Identità reale
- Chi siamo davvero
- Identità digitale
- Chi sembriamo online
- Identità percepita
- Come gli altri interpretano ciò che vedono
- Le tre identità raramente coincidono.

Oversharing

- Cos'è?
- Condividere troppo su di sé
- Rischi:
 - Perdita di controllo dei contenuti
 - Estraniamento dal contesto originale
 - Diffusione incontrollata
 - Vulnerabilità emotiva e relazionale
 - Impatto sul futuro (scuola, università, lavoro)

Reputazione online

- È il curriculum invisibile che ci accompagna
- Si costruisce nel tempo (post, commenti, tag)
- Non dipende solo da noi: anche dagli altri
- Può influenzare:
- relazioni
- opportunità accademiche
- selezioni lavorative

Tracciabilità: nulla scompare davvero

- Cosa viene tracciato:
- ricerche
- click, like, tempo di visualizzazione
- movimenti e posizione
- cronologie e cookie
- dati dei sensori dello smartphone
- interazioni con app e piattaforme
- Ogni azione lascia un'impronta digitale.

Carbon footprint digitale

- Dati attivi
- Quelli che scegliamo di fornire(es. foto, nome, descrizione, post)
- Dati passivi
- Quelli raccolti automaticamente(es. IP, geolocalizzazione, metadati)
- Lasciamo più tracce di quelle che crediamo.

Deepfake

- Foto, audio o video generati con IA
- Sembrano reali ma non lo sono
- Rischi principali:
 - bullismo
 - fake news
 - ricatti
 - reputazione danneggiata

Doppi digitali e profili falsi

- Avatar, account secondari, identità alternative
- Doppi digitali:
- Profili falsi:
- Qualcuno si finge te
- Clone del profilo
- Impersonation
- Cosa fare:
- Segnalare
- Cambiare password
- Attivare 2FA
- Informare un adulto o docente

Costruzione dell'identità nell'era dei social

- Le nostre identità nascono dalle interazioni
- I social mostrano solo frammenti (“highlight effect”)
- Gli algoritmi rinforzano interessi e opinioni
- Identità digitale = narrazione continua
- Online costruiamo una versione di noi stessi.

Pubblicare con consapevolezza

- Domande da porsi sempre:
- Perché sto pubblicando questo?
- Quali conseguenze potrebbe avere?
- Chi può vederlo oggi?
- Chi potrà vederlo fra 5 anni?
- Sto rispettando la mia privacy e quella altrui?

Laboratorio 1: La mia impronta digitale

- Obiettivi:
- Rendere visibili le tracce digitali
- Riflettere sulla propria presenza online
- Attività:
- Elenca tutte le tue attività digitali recenti
- Cerca tracce pubbliche del tuo nome (se autorizzato)
- Identifica:
- cosa ti rappresenta bene
- cosa NON ti rappresenta
- cosa andrebbe sistemato o rimosso



Associazione
Protezione Diritti e Libertà
Privacy APS

Laboratorio 2: Revisione del profilo social

- Cosa controllare:
- Username e bio
- Foto profilo
- Post pubblici
- Commenti lasciati
- Storie in evidenza
- Tag da parte di altri
- Impostazioni privacy
- Domanda chiave:
- “Cosa comunica davvero questo profilo su di me?”

Checklist del profilo consapevole

- Un profilo è sicuro quando:
- Mostra solo ciò che voglio che rappresenti me
- Non rivela troppe informazioni personali
- Ha privacy configurata correttamente
- Non contiene contenuti impulsivi o rischiosi
- I tag da parte di altri sono gestiti
- Non mostra dati sensibili o situazioni compromettenti

Obiettivi raggiunti

- Alla fine del modulo, lo studente:
- Comprende i meccanismi dell'identità digitale
- Conosce rischi e opportunità
- Sa distinguere identità reale/digitale/percepita
- Sa riconoscere deepfake e impersonation
- Sa migliorare il proprio profilo social
- Ha maggiore consapevolezza nella pubblicazione

Conclusione

- “La tua identità digitale parla anche quando tu non lo fai.”

• ***Grazie per l'attenzione!***