Associazione
Protezione Diritti e Libertà
Privacy APS

AMBASCIATORI DI SICUREZZA INFORMATICA
&
EDUCAZIONE DIGITALE CONSAPEVOLE

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

PROGETTO FORMATIVO

PER LE SCUOLE SECONDARIE DI PRIMO E SECONDO GRADO

Anno scolastico 2025-2026

Associazione
Protezione Diritti e Libertà
Privacy APS

Moduli 1 – 9

Associazione
Protezione Diritti e Libertà
Privacy APS

Privacy e Sicurezza Online

- Modulo 4 – Patentino Digitale Durata: 2 ore

Associazione
Protezione Diritti e Libertà
Privacy APS

Obiettivi del modulo

- Capire cos’è la privacy digitale
- Conoscere le basi del GDPR
- Riconoscere rischi e minacce online
- Sviluppare comportamenti protettivi
- Imparare a impostare privacy e sicurezza sui social

Associazione
Protezione Diritti e Libertà
Privacy APS

Cos'è la privacy digitale?

- Controllo sui propri dati personali
- Decidere chi vede cosa
- Protezione di:
- identità
- foto
- opinioni
- informazioni sensibili
- Privacy ≠ "non ho niente da nascondere"

Associazione
Protezione Diritti e Libertà
Privacy APS

Che cos'è un dato personale?

- Un'informazione che identifica una persona:
- nome, cognome
- foto, video, audio
- chat e messaggi
- email, telefono
- posizione GPS
- indirizzo IP
- preferenze, like, cronologia
- Dati particolari:
- salute
- orientamento
- dati biometrici

Associazione
Protezione Diritti e Libertà
Privacy APS

Perché proteggere i dati?

- Rischi di furto d’identità
- Manipolazione
- Profilazione indesiderata
- Truffe e ricatti
- Immagine pubblica compromessa

Associazione
Protezione Diritti e Libertà
Privacy APS

Le principali minacce online

- Phishing
- Hackeraggio di account
- Truffe
- Furto d’identità

Associazione
Protezione Diritti e Libertà
Privacy APS

Phishing: come si riconosce

- Segnali di allarme:
- Messaggi con urgenza
- Link strani o accorciati
- Errori grammaticali
- Premi “troppo belli”
- Mittente sospetto
- Regola: non cliccare, non rispondere, elimina.

Associazione
Protezione Diritti e Libertà
Privacy APS

Hackeraggio di account

- Cause più comuni:
- password deboli
- stessa password ovunque
- Wi-Fi pubblico
- app o download non sicuri
- accesso lasciato aperto
- Prevenzione:
- password forti
- 2FA
- logout dai dispositivi condivisi

Associazione
Protezione Diritti e Libertà
Privacy APS

Truffe online: esempi

- Finti corrieri
- Finti premi
- Finti servizi clienti
- Finti profili social
- Truffe nel gaming (“regalami la skin”)
- “Mandami il codice…” → sempre NO

Associazione
Protezione Diritti e Libertà
Privacy APS

Furto d'identità

- Cosa può succedere:
- Creano un profilo con il tuo nome
- Usano le tue foto
- Inviando messaggi a tuo nome
- Combinano problemi reali nella tua vita
- Cosa fare:
- segnalare
- cambiare password
- attivare 2FA
- informare subito un adulto/docente

Associazione
Protezione Diritti e Libertà
Privacy APS

Sicurezza quotidiana

- 1. Password forti
- lunghe
- uniche per ogni account
- password manager consigliato
- 2. 2FA – Autenticazione a due fattori
- SMS
- app Authenticator
- chiavi fisiche
- 3. Gestione dispositivi
- blocco schermo
- aggiornamenti
- antivirus
- attenti ai Wi-Fi pubblici

Associazione
Protezione Diritti e Libertà
Privacy APS

Permessi delle app

- Controllare sempre:
- fotocamera
- microfono
- posizione
- contatti
- file
- attività in background
- Ridurre al minimo i permessi non necessari.

Associazione
Protezione Diritti e Libertà
Privacy APS

Chat e gruppi: comportamenti sicuri

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

Associazione
Protezione Diritti e Libertà
Privacy APS

Sicurezza nei social

- Impostare privacy su “solo amici”
- Controllare i tag
- Disattivare geolocalizzazione
- Attenzione alle storie: visibili anche a sconosciuti
- Non rispondere a DM sospetti

Associazione
Protezione Diritti e Libertà
Privacy APS

Sicurezza nel gaming online

- Usare nickname non riconducibili a nome reale
- Mai condividere dati personali in chat
- Non accettare regali o offerte strane
- Attenzione alle microtransazioni
- Segnalare giocatori tossici o molesti

Associazione
Protezione Diritti e Libertà
Privacy APS

Laboratorio 1:
Individua i messaggi falsi

- Analizziamo:
- 3 messaggi di phishing
- 2 truffe via social
- 1 caso di furto d’identità
- Obiettivo:
- riconoscere segnali di rischio
- proporre la risposta sicura

Associazione
Protezione Diritti e Libertà
Privacy APS

Laboratorio 2: Impostiamo la privacy

- Scegli un social (Instagram, TikTok, WhatsApp, Discord).
- Controlla e modifica:
- chi può vedere i post
- chi può scrivere DM
- chi può commentare
- gestione dei tag
- privacy delle storie
- sincronizzazione contatti
- tracking pubblicitario

Associazione
Protezione Diritti e Libertà
Privacy APS

Checklist del profilo sicuro

- Un profilo è sicuro quando:
- è privato
- ha password forte + 2FA
- ha tag controllati
- non mostra dati personali
- non ha geolocalizzazione attiva
- ha permessi app configurati correttamente

Associazione
Protezione Diritti e Libertà
Privacy APS

Obiettivi raggiunti

- Alla fine del modulo, lo studente:
- comprende il GDPR
- riconosce minacce online
- sa proteggersi da phishing e truffe
- usa password e 2FA
- configura la privacy sui social
- adotta comportamenti sicuri in chat e gaming

Associazione
Protezione Diritti e Libertà
Privacy APS

Conclusione

- “La tua sicurezza online dipende da ogni scelta che fai.”
- Proteggi te stesso, proteggi gli altri.

- ***Grazie per l'attenzione!***