



PROVINCIA AUTONOMA DI TRENTO



Servizio istruzione
Ufficio per le politiche di inclusione e cittadinanza

Soggetto istituzionale del Tavolo

POLIZIA DI STATO – Centro Operativo per la sicurezza Cibernetica “Trentino – Alto Adige”
Via Vannetti n. 15 – 38122 TRENTO

E-Mail: dipps503.0000@pecps.poliziadistato.it

Referente organizzativo

Funzionario Economico Finanziario MACHEDA Dott.ssa Caterina Rosa
e-mail: caterina.macheda@interno.it

Tel. 0461 260917

Articolazione e presenza sul territorio provinciale

Il Centro Operativo per la Sicurezza Cibernetica Trentino - Alto Adige, con sede a Trento, riveste competenza su tutto il territorio della Regione Trentino Alto - Adige, nel cui ambito opera unitamente alla dipendente Sezione Operativa per la Sicurezza Cibernetica di Bolzano.

Illustrazione della proposta educativa

➤ Prima proposta online:

“Capire, prevenire, agire: un dialogo contro bullismo e cyberbullismo”

Da realizzarsi in modalità online con gli alunni della scuola primaria delle classi 4^a e 5^a, con gli studenti della scuola secondaria di primo grado e del biennio della scuola secondaria di secondo grado.

L’obiettivo degli incontri da remoto, è quello di aumentare la consapevolezza dei rischi di un utilizzo inappropriato della rete e dei moderni strumenti di comunicazione digitale e far riflettere gli studenti sulle responsabilità personali, di diversa natura, sollecitandone lo sviluppo di empatia e solidarietà nei confronti di chi subisce atti di bullismo e cyberbullismo nonché coinvolgendo gli studenti ad elaborare collegamenti concettuali sui temi della giustizia, del rispetto e dell’inclusione.

➤ Seconda proposta in presenza:

“Cybersecurity: difendersi nel mondo digitale”

Rivolta agli studenti della scuola secondaria di secondo grado - ultimo triennio- incontri, da tenersi in presenza, presso istituti scolastici da individuarsi congiuntamente al Dipartimento

Istruzione e Cultura della Provincia autonoma di Trento.

Argomenti trattati:

- introduzione alla sicurezza informatica;
- principali minacce informatiche;
- buone pratiche di sicurezza;
- gestione delle password;
- phishing e social engineering;
- protezione dei dispositivi;
- navigazione sicura su internet;
- politiche aziendali di sicurezza informatica;
- gestione degli incidenti di sicurezza.