



**CYBERSECURITY
NATIONAL LAB**

**CYBER
HIGH
SCHOOLS**



Introduzione alla Cybersicurezza

Corso di formazione per docenti delle scuole secondarie di II grado

Iniziativa formativa ID 98197

Edizione ID 146989

Presentazione

Indice

Presentazione	2
Obiettivi	2
Organizzazione.....	2
Modalità di iscrizione, erogazione e fruizione	3
Programma	3
Docenti.....	5
Costi	6
Prerequisiti.....	6
Date	6
Programma	6
Materiale didattico	7
Punti di forza.....	7

Presentazione

Il corso:

- è finalizzato a far crescere la sensibilizzazione verso le problematiche di sicurezza nell'uso di strumenti e tecnologie informatiche, attraverso un opportuno mix di lezioni, di tutoraggi e di Escape Room, fruibili da remoto
- è completamente gratuito e selezionabile tramite la piattaforma S.O.F.I.A. del Ministero dell'Istruzione e del Merito. I docenti non di ruolo, che non possono accedere alla piattaforma di cui sopra, possono registrarsi tramite un form ad hoc
- è organizzato dal *Cybersecurity Nazionale Lab*¹ del CINI² (Consorzio Interuniversitario Nazionale per l'Informatica) nell'ambito del programma *CyberHighSchools*³
- è una delle azioni del CINI *Cybersecurity National Lab* finalizzate alla attuazione della Misura #65 del "Piano di implementazione" della "*Strategia Nazionale di Cybersicurezza 2022-2026*"⁴ dell'ACN - Agenzia per la Cybersicurezza Nazionale
- è tenuto da docenti e specialisti del settore, afferenti al Laboratorio
- è fruibile in modalità remota tramite la piattaforma Teams del Laboratorio
- ha una durata complessiva di 35 ore.

Obiettivi

il corso mira a far crescere la sensibilizzazione verso le problematiche di sicurezza nell'uso di strumenti e tecnologie informatiche, attraverso un opportuno mix di lezioni, di tutoraggi e di Escape Room, fruibili da remoto.

Organizzazione

- Il corso prevede 35 ore complessive di impegno, di cui:
 - 24 h di lezione, di cui:
 - 4 h erogate on-line, tramite la piattaforma Teams
 - 20 h fruibili da remoto in modalità e-learning asincrono, tramite lezioni videoregistrate e accessibili tramite il portale <https://corso-base.cyberhighschools.it/>
 - 11 h di tutoraggio on-line.
- Il corso è organizzato in
 - Un *incontro iniziale*, della durata di 2 h, in modalità on-line live
 - 10 *moduli*: ciascun modulo viene erogato nell'arco di una settimana e include tipicamente:
 - 2 h di lezione, preregistrate e fruibili in modalità e-learning asincrona;
 - 1 h di tutoraggio, in modalità on-line live da parte del docente che ha registrato la lezione;

¹ <https://cybersecnatlab.it>

² <https://www.consorzio-cini.it>

³ <https://cyberhighschools.it>

⁴ <https://www.acn.gov.it/portale/strategia-nazionale-di-cybersicurezza>

- Alcuni moduli prevedono una esercitazione pratica sotto forma di gaming tramite una *Escape Room* in modalità on-line asincrona;
 - Un *incontro finale*, della durata di 2 h, in modalità on-line live.
- Il corso prevede, tra l'altro:
 - Questionari di gradimento, da compilarsi on line, uno per ciascun modulo⁵ e uno relativo al corso nel suo complesso⁶
 - Rilascio di un attestato di partecipazione, anche sotto forma di Open Badge⁷.

Modalità di iscrizione, erogazione e fruizione

- L'iscrizione avviene tramite la piattaforma S.O.F.I.A.⁸ del Ministero dell'Istruzione e del Merito.
- I docenti non di ruolo, che non possono accedere alla piattaforma di cui sopra, possono registrarsi tramite un form ad hoc predisposto dal Cybersecurity National Lab⁹.
- Gli incontri iniziali e finali e i tutoraggi vengono erogati on-line live, tramite la piattaforma Teams.
- Per l'ottenimento dell'attestato di partecipazione è necessario seguire almeno il 60% degli incontri on-line live tramite la piattaforma Teams.

Programma

Incontro Iniziale:

- In modalità on-line live [2 h – Paolo PRINETTO]
 - Introduzione al corso
 - Presentazione del *Cybersecurity Nazionale Lab*
 - Presentazione di *The Big Game*, la filiera di formazione e addestramento del Lab
 - Presentazione della *Escape Room*

Modulo 1 - Concetti introduttivi:

- Lezioni – in modalità preregistrata [2 h – Paolo PRINETTO]:
 - Introduzione alla sicurezza
 - Safety, Security, Dependability
 - Cybersicurezza & Cyberspazio
 - Protezione delle Informazioni
 - Attacchi - Cause e Tassonomie
 - I Pilastri della Sicurezza
- Tutoraggio on-line [1 h – Paolo PRINETTO]

⁵ <https://form.cybersecnatlab.it/index.php/579682>

⁶ <https://form.cybersecnatlab.it/index.php/175599>

⁷ <https://openbadges.org>

⁸ <https://sofia.istruzione.it>

⁹ <https://form.cybersecnatlab.it/index.php/295282>

- Materiali aggiuntivi, non coperti a lezione:
 - Security vs Safety
 - Vulnerabilità

Modulo 2 - Crittografia:

- Lezione 2 – in modalità preregistrata [2 h – Rocco DE NICOLA]
 - Introduzione e storia della crittografia
 - Crittografia simmetrica
 - Crittografia asimmetrica e scambio di chiavi
 - Steganografia e Watermarking.
- Tutoraggio on-line [1 h – Rocco DE NICOLA]

Modulo 3 – Virus, Malware e Controllo Accessi:

- Lezione 3 – in modalità preregistrata [2 h – Gabriele COSTA]
 - Virus e malware
 - Controllo degli accessi e gestione password
 - Accessi sicuri al web, cookie e sessioni
- Tutoraggio on-line [1 h – Gabriele COSTA]

Modulo 4 - Firma digitale & SPID:

- Lezione 4 – in modalità preregistrata [2 h – Francesco BUCCAFURRI]
 - Hashing, MAC e Firma Digitale
 - Identità Digitale Pubblica (SPID) & PEC
- Tutoraggio on-line [1 h – Francesco BUCCAFURRI]

Modulo 5 - Privacy & GDPR:

- Lezione 5 – in modalità preregistrata [2 h – Stefania STEFANELLI]
 - Privacy e Dati Personali
 - Gestione e protezione dei Dati Personali
 - GDPR
 - Responsabilità degli insegnanti
- Tutoraggio on-line [1 h – Stefania STEFANELLI]

Modulo 6 - Aspetti Legali ed Etici:

- Lezione 6 – in modalità preregistrata [2 h – Carlo BLENGINO]
 - Il diritto penale nella rete - I reati informatici
 - L'accesso abusivo
 - Etica e Sicurezza
- Tutoraggio on-line [1 h – Carlo BLENGINO]

Modulo 7 - Ingegneria Sociale & Incremento della Resilienza:

- Lezioni – in modalità preregistrata [2 h – Paolo PRINETTO]
 - Social Engineering – Motivazioni
 - Social Engineering – Phishing
 - Social Engineering – Altre tipologie di pesca
 - Social Engineering – Altri vettori di attacco
 - Incremento della resilienza a livello di Individuo
- Tutoraggio on-line [1 h – Paolo PRINETTO]

Modulo 8 – Open-Source Intelligence - OSINT:

- Lezioni – in modalità preregistrata [2 h – Riccardo BONAFEDE]
 - Introduzione all’OSINT
 - Tecniche e strumenti
- Tutoraggio on-line [1 h – Riccardo BONAFEDE]

Modulo 9 - Media Literacy e contrasto al discorso d’odio online: il gioco Hate Out!:

- Lezioni – in modalità preregistrata [2 h – Sylvia LIUTI]
 - Sistema dell’informazione e disordini informativi
 - Comunicazione sui social media
 - Stereotipi e discorso d’odio online
 - Discorso d’odio e libertà d’espressione
 - Il gioco Hate Out!: come giocare e come riproporlo in classe.
- Tutoraggio on-line [1 h – Sylvia LIUTI]

Modulo 10 – Come preparare esercitazioni tramite Escape Room:

- Lezioni – in modalità preregistrata [2 h – Antonio FACCIOLI]
- Tutoraggio 1 on-line [1 h – Antonio FACCIOLI]
- Tutoraggio 2 on-line [1 h – Antonio FACCIOLI]

Incontro Conclusivo:

- In modalità on-line live [2 h – Paolo PRINETTO]
 - Considerazioni conclusive
 - Analisi dell’andamento del corso
 - Attività future

Docenti

- Le lezioni e i tutoraggi sono svolti da docenti universitari e specialisti del settore, afferenti al Cybersecurity National Lab:
 - Carlo BLENGINO (Penalista)

- Riccardo BONAFEDE (Cybersecurity National Lab)
- Francesco BUCCAFURRI (Università Mediterranea di Reggio Calabria)
- Gabriele COSTA (IMT – Scuola Alti Studi Lucca)
- Rocco DE NICOLA (Cybersecurity National Lab)
- Antonio FACCIOLI (Edulife Fondazione ETS)
- Sylvia LIUTI (FORMA.Azione srl)
- Paolo PRINETTO (Cybersecurity National Lab)
- Stefania STEFANELLI (Università degli Studi di Perugia).

Costi

- Il corso viene offerto gratuitamente dal Cybersecurity National Lab del CINI ai docenti delle scuole superiori di II grado.

Prerequisiti

- Nessuno

Date

- Iscrizioni: dal 18.03.2025 al 01.04.2025
- Svolgimento del corso: dal 08.04.2025 al 16.05.2025

Programma

Il programma dettagliato degli incontri on-line live, tramite la piattaforma Teams, è il seguente:

Data	Orario	Docente	Oggetto
02/04/2025	17:00 -19:00	PRINETTO Paolo	Incontro introduttivo
08/04/2025	18:00 -19:00	PRINETTO Paolo	Tutoraggio on-line
15/04/2025	18:00 -19:00	DE NICOLA Rocco	Tutoraggio on-line
23/04/2025	18:00 -19:00	COSTA Gabriele	Tutoraggio on-line
29/04/2025	18:00 -19:00	BUCCAFURRI Francesco	Tutoraggio on-line
06/05/2025	18:00 -19:00	STEFANELLI Stefania	Tutoraggio on-line
14/05/2025	18:00 -19:00	BLENGINO Carlo	Tutoraggio on-line
21/05/2025	18:00 -19:00	PRINETTO Paolo	Tutoraggio on-line
27/05/2025	18:00-19:00	BONAFEDE Riccardo	Tutoraggio on-line
03/06/2025	18:00 -19:00	LIUTI Sylvia	Tutoraggio on-line
09/06/2025	18:00-19:00	FACCIOLI Antonio	Tutoraggio on-line
16/06/2025	16:00 -17:00	FACCIOLI Antonio	Tutoraggio on-line
16/06/2025	17:00 -19:00	PRINETTO Paolo	Incontro conclusivo

Materiale didattico

Tutto il materiale didattico relativo a ciascun modulo:

- Registrazione delle lezioni
- Copia delle slide utilizzate
- Puntatori a materiali di approfondimento
- Registrazione del tutoraggio on line

verrà reso disponibile ai partecipanti, sia durante il corso sia successivamente alla sua conclusione, tramite il portale dedicato¹⁰.

Punti di forza

- Contribuire a far crescere, nel corpo docente della scuola secondaria di II grado, la sensibilizzazione verso le problematiche di sicurezza nell'uso delle tecnologie informatiche
- Qualificazione del soggetto erogante
- Modalità di fruizione remota, supportata da docenze e tutoraggi qualitativamente significative
- Valorizzazione e diffusione dei programmi *CyberChallenge.IT*¹¹, *OliCyber*¹², *CyberTrials*¹³, *ITSCyberGame*¹⁴ e *CyberNextGen*
- Attuazione della Misura #65 del "Piano di implementazione" della "Strategia Nazionale di Cybersicurezza 2022-2026" dell'ACN - Agenzia per la Cybersicurezza Nazionale
- Partecipazione gratuita, con rilascio di un attestato di partecipazione, anche sotto forma di Open Badge
- Possibilità di accedere a tutto il materiale didattico anche successivamente alla conclusione del corso
- Possibilità di apprendere come adattare e personalizzare gli strumenti proposti durante il corso al fine di utilizzarli nelle proprie attività didattiche.

¹⁰ <https://corso-base.cyberhighschools.it/>

¹¹ <https://cyberchallenge.it>

¹² <https://olicyber.it>

¹³ <https://www.cybertrials.it>

¹⁴ <https://itscybergame.it>