

SALONE DELL'ORIENTAMENTO 2026

#BREAK THE PATTERN

CORSO DI LAURE MAGISTRALE

CYBERSECURITY ENGINEERING



**Politecnico
di Torino**



Programma:

Importanza della Cybersecurity oggi

Prof. Cataldo Basile, Referente del CdS

Descrizione del piano di studi e degli orientamenti

Fulvio Valenza, Referente Orientamento

Descrizione attività complementari

Claudia Passaro e Debora Bini

Studentesse II anno CdLM in Cybersecurity Engineering

Q&A

**SCOPRI IL CORSO
DI STUDIO a.a.26/27**



Importanza della Cybersecurity oggi

Prof. Cataldo Basile

Referente del CdLM in Cybersecurity Engineering



**Politecnico
di Torino**





Politecnico di Torino

Cybersecurity

competenze di grande rilevanza

Transizione digitale

- banche, assicurazioni, pubblica amministrazione
- grandi aziende e commercio elettronico
- SPID e identità digitale

Veicoli sempre più connessi

- e guida autonoma

Industria 4.0 e 5.0

- fabbriche intelligenti in cui le macchine si coordinano autonomamente

Infrastrutture critiche

Metaverso

- l'ultima frontiera della digitalizzazione...

Cybercrime 1,3% del PIL globale

- per il WEF 10.5 "triloni" di dollari nel 2025

Economia digitale. Un report sulla cyber sicurezza evidenzia l'aumento delle intrusioni

Grandi aziende italiane nel mirino degli hacker

Nel 2017 speso poco più di un miliardo per la difesa

Enrico Netti
Hacker all'attacco con ransomware, massive phishing e spear phishing. Sono queste le più comuni tipologie di tentativi che hanno colpito grandi società italiane nel 2016. Offensive che negli ultimi tempi hanno avuto una risonanza quasi duotriennale (cacio) e Netconsulting 3 con il patrocinio tra gli altri, della Presidenza del Consiglio dei ministri, che sarà presentato domani a Milano. Ne emerge un quadro confortante, a conferma di come la sicurezza non sia affrontata in modo adeguato dalle grandi aziende quotate che compongono il panel

GLOSSARIO
Spear phishing
Indica un sofisticato e particolare tipo di phishing realizzato mediante l'invio di email profilate e targettizzate per una specifica

cederle 22 milioni di spese nel 2016 che, secondo una stima, quest'anno diventeranno 1,05 miliardi (+9%). Non molto e così Lezzi suggerisce al governo di privilegiare, anche in un'ottica di Iskra 2.0, gli appalti per le aziende che investono in servizi continuativi di auditing, simulazione di attacco, monitoraggio.



Global Cybercrime Damage Costs:

- **\$6 Trillion USD a Year. ***
- **\$500 Billion a Month.**
- **\$115.4 Billion a Week.**
- **\$16.4 Billion a Day.**
- **\$684.9 Million an Hour.**
- **\$11.4 Million a Minute.**
- **\$190,000 a Second.**



ALL FIGURES ARE
PREDICTED BY 2021

* SOURCE: CYBERSECURITY VENTURES



**CYBERSECURITY
VENTURES**



Politecnico
di Torino

Cybersecurity

competenze di grande rilevanza

Difesa e sicurezza nazionale

- guerra in Ucraina si combatte anche con armi cyber
- attaccati siti governativi e di importanti società energetiche
- terrorismo, traffico di armi e droga...

Impatto anche in ambito militare

- definizione di forze armate "cyber"
 - oltre alle tradizionali terra, aria, acqua

Agenzia per la Cybersicurezza Nazionale

- definizione del perimetro nazionale
- reazione agli attacchi meno "educate"

I numeri del cyber conflitto

Se le immagini dei palazzi residenziali sventrati dai missili e i cadaveri per le strade ci restituiscono l'orrore dell'invasione russa e dei crimini compiuti ai danni dei civili, altrettanto distruttivi sono stati gli attacchi cyber. Passati in sordina, dopo le prime, convulse settimane di guerra, ma non per questo sospesi. Anzi. **Nel 2022 in Ucraina sono stati registrati 4.500 cyber attacchi.** Il triplo rispetto al 2021 (1.400), più di cinque volte quelli del 2020, secondo i dati forniti a *Wired* dal Centro nazionale ucraino di coordinamento della sicurezza informatica.

La Difesa arruola cyber militari, al via il primo bando: ecco chi può partecipare

Si tratta di 21 posti da Sottotenente di Vascello nel Corpo del Genio della Marina, da impiegare nei domini cyber e spazio della Difesa. Crosetto: unificare settori Spazio e Cyber

24 gennaio 2023 • Articolo aggiornato il 25 gennaio, ore 10:00





Servono **VERI** esperti in cybersecurity

grave **carezza di competenze** in ambito cybersecurity

- 100'000 persone (secondo alcuni esperti) solo in Italia
- milioni a livello globale

le competenze dei laureati in Ingegneria Informatica non adeguate alla Cybersecurity

- ambito multidisciplinare (ibrido)
- potenziare **ambiti giuridico, sociale ed economico**
- fornire ulteriori **competenze di dominio** rispetto a lauree a più ampio spettro

- non è possibile fornirle nell'ambito dell'attuale laurea magistrale in ingegneria informatica

ENISA (European Network and Information Security Agency) sottolinea l'importanza delle università e della formazione universitaria

- **Skill Framework**

- <https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles>



Servono **VERI** esperti in cybersecurity

grave **carezza di competenze** in ambito cybersecurity

- 100'000 persone (secondo alcuni esperti) solo in Italia
- milioni a livello globale

le competenze dei laureati in Ingegneria Informatica non adeguate alla Cybersecurity

competenze multidisciplinaria (ibrida)

L'interesse verso la cybersecurity è destinato a rimanere molto alto per i prossimi anni



CdLM in Cybersecurity Engineering @ PoliTO

compatibilità con **Curricula ECSO** (European Cybersecurity Organization)

- uno dei primi in EU
- profili e ruoli professionali chiari a livello EU
 - copre insegnamenti e argomenti riconosciuti a livello comunitario
 - è *chiaramente un corso di laurea magistrale di tipo ingegneristico*
 - dà competenze indispensabili in area economica, sociale e giuridica



forte connessione con gli **standard internazionali**

- progettato a partire da framework di risk management del NIST
- forte enfasi dell'interdisciplinarietà per creare i 'profili ibridi'
 - richiesti dal mercato del lavoro interamente in lingua inglese





Principali profili professionali proposti



Cybersecurity Analyst

valuta lo stato di sicurezza di un sistema informativo, monitora e risponde agli incidenti, svolge analisi forensi

Cybersecurity Designer

pianifica, progetta ed implementa le misure di protezione che servono a garantire un appropriato livello di sicurezza



Cybersecurity Legal, Policy and Compliance Officer

valuta la conformità delle soluzioni di sicurezza con gli standard quadri legali e aspetti normativi, valuta requisiti legali/strategie o contratti aziendali

Cryptography expert

definisce o sviluppa applicazioni e programmi crittografici di base ed avanzati



Descrizione del piano di studi e degli orientamenti

Fulvio Valenza

Referente Orientamento CdLM Cybersecurity Engineering



**Politecnico
di Torino**





Caratteristiche del corso di Laurea

- ❑ Erogato in **Lingua inglese**
 - ❑ Imparerai attraverso **lezioni frontali, esercitazioni in aula** e in **laboratori informatici**, con attività condotte in modo autonomo o organizzate in gruppi di lavoro.
- ❑ Formato da **4 diversi Orientamenti** relativi alle principali figure professionali:
 - ❑ **Cyber Designer**
 - ❑ **Cryptography expert**
 - ❑ **Cyber Analyst**
 - ❑ **Cyber Legal & Compliance Officer**
- ❑ **Interclasse: LM-32 (Ingegneria Informatica) e LM-66 (Cybersecurity)**
- ❑ Possibilità di scegliere come esame finale **solo Tesi** oppure **Tesi+Tirocinio**



Interclasse LM-32 e LM-66

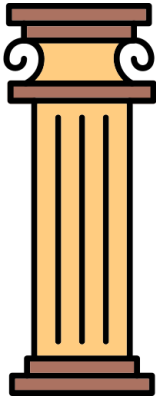
- ❑ La cybersecurity è un **dominio complesso** che richiede competenze tecnologiche avanzate e interdisciplinari
- ❑ Il CdLM fornisce **basi tecnologiche** nel campo dell'Ingegneria Informatica ed **conoscenze interdisciplinari** nel campo giuridico, economico e sociale
- ❑ Il CdLM è di tipo **interclasse**, coprendo gli obiettivi formativi sia della classe di laurea magistrale in **Ingegneria Informatica** (LM-32) sia di quella in **Sicurezza Informatica** (LM-66).

Unico Piano di Studi, diviso in 4 Orientamenti
ma possibilità di scegliere se **Laurearsi come LM-32 o LM-66**



Basi del piano di studio

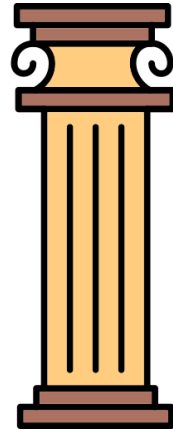
Piano di studio Cybersecurity



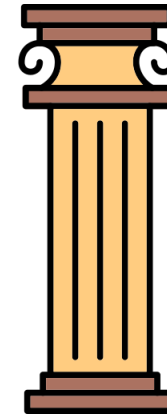
Interdisciplinarietà



LM32 & LM66



Conformità



Innovazione





Cosa imparerai

Aree di Apprendimento

Computer Science

Cybersecurity
Protection

Cybersecurity
Monitoring

Cryptography

Legal and
Regulatory

Governance

Cosa potrai fare dopo

Orientamenti



Cryptography expert



**Cyber Legal &
Compliance Officer**



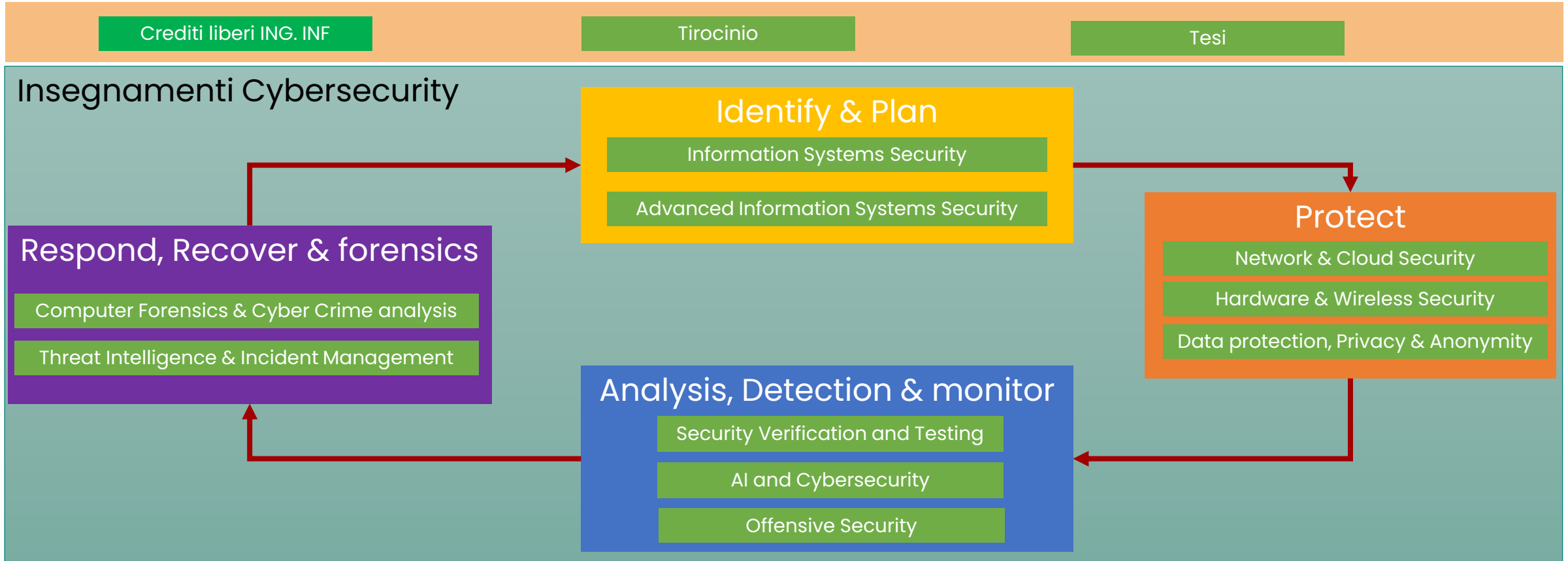
Cyber Designer



Cyber Analyst



Architettura del piano di studio



Insegnamenti MAT

- Cryptography
- Advanced Cryptography
- Post-Quantum Cryptography

Insegnamenti GES

- Cybersecurity laws and regulations
- Corporate cybersecurity evaluation

Insegnamenti ING. INF

- Computer Architectures & Operating systems
- Computer Networks & Cloud technologies
- Web Application



Primo anno

(Comune a tutti gli Orientamenti)

Nome	CFU	Periodo
Computer architectures and operating systems	8	1
Information Systems Security	8	1
Corso di Base a scelta	6	1 o 2
Networks & Cloud Technology and Security	12	1 + 2
Web applications	8	2
Cryptography	6	2
Hardware & Wireless Security	12	2





Secondo anno (6 Corsi)

Ambito Giuridico, Economico Sociale (GES)

Ambito Matematico (MAT)

Ambito Cybersecurity (CYBER)



	Analyst	Designer	Officer	Cryptography
Obbligatori	1 GES			
	1 CYBER	1 CYBER	1 CYBER	1 MAT
Caratterizzanti	2 CYBER	2 CYBER	2 GES	1 MAT
A scelta	1 CYBER o MAT	1 CYBER o MAT	2 CYBER o 1 CYBER + 1 MAT	2 CYBER
	1 GES	1 GES		1 GES



Secondo anno: **Cyber Analyst**

Nome	CFU	Periodo	
Security Verification and Testing	8	1	
Cybersecurity laws and regulations	6	1	
AI and Cybersecurity	6	1	
Advanced Cryptography	6	1	1 su 3
Advanced Information Systems Security	8	1	
Data protection, Privacy and Anonymity	6	1	
<hr/>			
Computer Forensics and cyber crime analysis	8	2	1 su 2
Technology and Innovation Management in Cybersecurity	6	2	
Threat Intelligence and Incident Management	6	2	
Tesi oppure Tirocinio+Tesi	22	2	



Secondo anno: **Cyber Designer**

Nome	CFU	Periodo	
Advanced Information Systems Security	8	1	
Cybersecurity laws and regulations	6	1	
Data protection, Privacy and Anonymity	6	1	
Advanced Cryptography	6	1	1 su 3
Security Verification and Testing	8	1	
AI and Cybersecurity	6	1	
<hr/>			
Computer Forensics and cyber crime analysis	8	2	1 su 2
Technology and Innovation Management in Cybersecurity	6	2	
Offensive Security	6	2	
Tesi oppure Tirocinio+Tesi	22	2	



Secondo anno: **Cryptography expert**



Nome	CFU	Periodo	
Cybersecurity laws and regulations	6	1	
Advanced Cryptography	6	1	
Security Verification and Testing	8	1	1 SU 2
Advanced Information Systems Security	8	1	
AI and Cybersecurity	6	1	1 SU 2
Data protection, Privacy and Anonymity	6	1	
Computer Forensics and cyber crime analysis	8	2	1 SU 2
Technology and Innovation Management in Cybersecurity	6	2	
Post-quantum Cryptography	6	2	
Tesi oppure Tirocinio+Tesi	22	2	



Secondo anno: **Cyber Legal & Compliance Officer**

Nome	CFU	Periodo	
Cybersecurity laws and regulations	6	1	
Data protection, Privacy and Anonymity	6	1	
Security Verification and Testing	8	1	2 su 4
Advanced Information Systems Security	8	1	
AI and Cybersecurity	6	1	
Advanced Cryptography	6	1	
<hr/>			
Computer Forensics and cyber crime analysis	8	2	
Technology and Innovation Management in Cybersecurity	6	2	
Tesi oppure Tirocinio+Tesi	22	2	



Tesi e Tirocino

- ❑ La prova finale può essere composta
 - ❑ **Tesi di 22 CFU**
 - ❑ **Tirocinio Formativo 10 CFU + Tesi da 12 CFU**

- ❑ Le attività di Tesi possono essere condotte al Politecnico di Torino, anche presso altri enti o aziende, in Italia o all'estero

- ❑ Le attività di Tirocinio Formativo costituiscono **un'occasione per svolgere esperienze lavorative e di formazione** presso aziende del settore



Percorsi di mobilità

- **15** Erasmus+ Mobility programmes
- **6** Double Degree programmes
- **9** Extra-UE Mobility programmes
- **2** percorsi si Erasmus Italiano

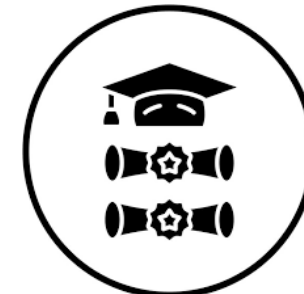
Laurea Magistrale CYBERSECURITY ENGINEERING Seleziona uno o più tipi di mobilità...



Erasmus+



unite!





Twin track master programme

Nell'ambito del programma **Twin Track** studenti immatricolati al Corso di Studi in **Cybersecurity Engineering** hanno la possibilità di conseguire la **seconda Laurea Magistrale in Ingegneria Informatica** o in **Ingegneria Matematica** con un solo anno in più



Twin track Cybersecurity Engineering & Ingegneria Informatica

Il percorso è strutturato come segue:

- 1° anno in **Cybersecurity Engineering**
- 2° anno in **Cybersecurity Engineering + Tesi**
- 3° anno con insegnamenti caratteristici del corso di **Ingegneria Informatica + Tesi**

Twin Track Cybersecurity Engineering & Ingegneria Matematica

Il percorso è strutturato come segue:

- 1° anno in **Cybersecurity Engineering**
- 2° anno in **Cybersecurity Engineering + Tesi**
- 3° anno con insegnamenti caratteristici del corso di **Ingegneria Matematica + Tesi**



**Politecnico
di Torino**



Descrizione attività complementari

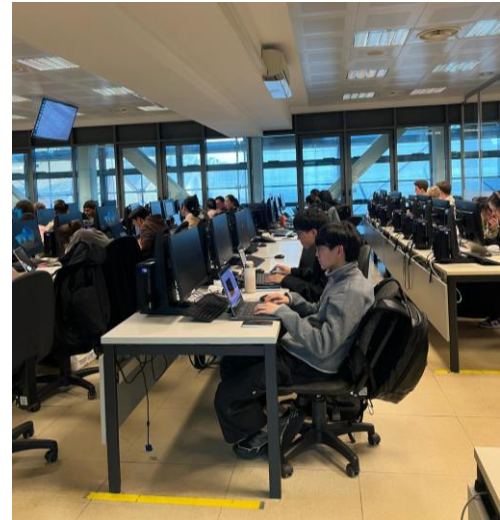
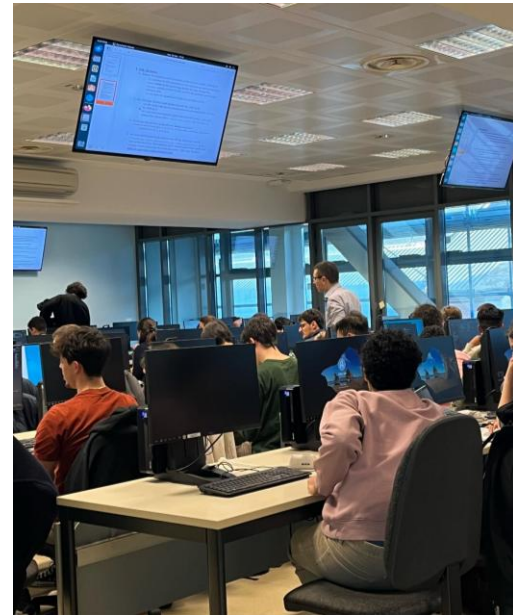
Claudia Passaro e Debora Bini

Studentesse II anno CdLM in Cybersecurity
Engineering



Laboratori

- ❑ Attività pratiche guidate da docenti nei laboratori informatici
- ❑ Esercitazioni **hands-on**
- ❑ Applicazione dei concetti teorici attraverso casi di studio
- ❑ Lavoro individuale e di gruppo per stimolare sia l'autonomia che la collaborazione



Punto di forza
Suggerito
dagli studenti





Politecnico
di Torino

Seminari



<ESCAPE>
EXPLAIN CYBERSECURITY WITH AN APERITIF

- ❑ Seminari su tematiche di cybersecurity particolarmente rilevanti
- ❑ Tenuti da Professori Internazionali ed Esperti di Settore
- ❑ Al termine di ciascun seminario, è prevista una discussione informale con un aperitivo





Visita e attività esperienziali

- ❑ Esplorazione di **ambienti lavorativi reali** per comprendere il funzionamento quotidiano delle strutture di cybersecurity
- ❑ Confronto con **professionisti del settore**
- ❑ Comprensione pratica delle dinamiche all'interno di strutture operative (es. **SOC**)
- ❑ Opportunità di vedere **tecnologie all'avanguardia in azione**
- ❑ Scoperta **futuri sbocchi lavorativi**





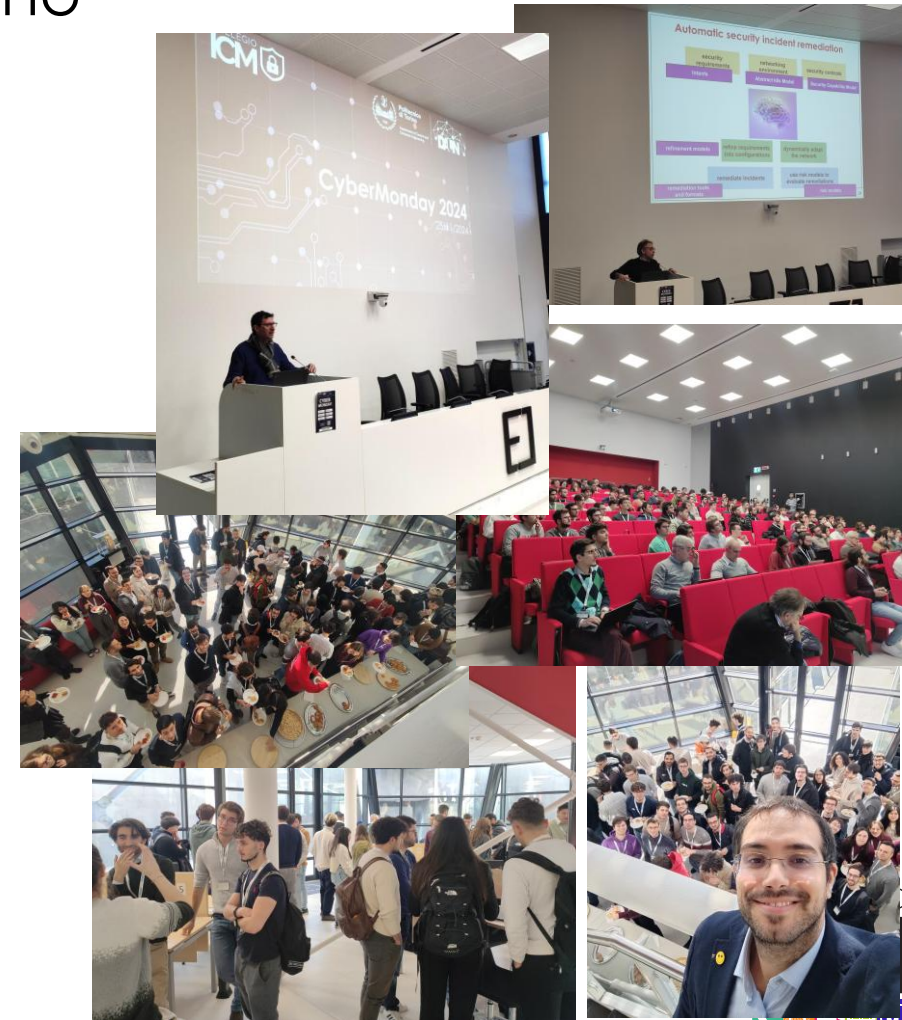
Politecnico
di Torino

CyberMonday



Giornata dedicata al Corso di Laurea, dove vengono presentate:

- ❑ Le **attività di ricerca** all'interno del Politecnico
- ❑ Le **possibilità di tesi e di tirocinio**
 - ❑ in università, all'estero o in azienda
- ❑ Le **attività di mobilità**
 - ❑ progetto Erasmus+, doppia laurea, tesi
- ❑ I **percorsi di dottorato e master** dopo la laurea





Politecnico
di Torino

CyberAcademy

Corsi extra-curricolari tenuti da aziende esperte del settore su **tecnologie** legate alla Cybersecurity

- ❑ Certificazioni **gratuite** riconosciute a livello internazionale
- ❑ Riconoscimento di **CFU extra-curricolare**
- ❑ Accesso a **materiali formativi esclusivi** (video, libri, tutorial)





Cyberchallenge.IT

programma nazionale di addestramento in cybersecurity per formare **ethical hacker**

- ❑ progetto per la valorizzazione delle eccellenze del Ministero dell'Istruzione
- ❑ @Polito: scelti 20(+5) studenti (16-24 anni)
 - ❑ 72h di addestramento
 - ❑ prova finale individuale nazionale (jeopardy)
 - ❑ prova a squadre Attacco-Difesa
 - ❑ scelti i rappresentanti di **TeamItaly**
- ❑ riconoscimento di **CFU extra-curricolari**





Politecnico
di Torino

Team studenteschi: **pwnthem0le**



Team studentesco di **Ethical Hacking**

<https://twitter.com/pwnthem0le>

<https://pwnthem0le.polito.it/>

Le principali attività sono:

- ❑ partecipazione a competizioni **Capture The Flag (CTF)**
 - ❑ anche in presenza a Las Vegas, Grenoble, Abu Dhabi, ...
- ❑ **formazione interna**, *talk su offensive security e presentazioni*
- ❑ organizzazione di eventi sulla sicurezza informatica
 - ❑ **m0leCon Computer Security Conference and CTF**
www.m0lecon.it
<https://www.youtube.com/@pwnthem0le/videos>





Politecnico di Torino

Pagina linkedin



CdLM Cybersecurity Engineering - Polito



Politecnico di Torino

229.348 follower
1m •

🎓 Al #PoliTO le prime lauree in Cybersecurity in Italia: 36 studenti e studentesse hanno concluso oggi il Corso di laurea magistrale in Cybersecurity Engineering, uno dei percorsi più innovativi e apprezzati dell'offerta formativa dell'Ateneo.

Il corso, erogato in lingua inglese, offre quattro diversi orientamenti e si distingue per l'unicità e la varietà delle sue proposte, improntata agli aspetti tecnologici e ingegneristici e capace di integrare anche competenze trasversali.

📝 Con circa 250 nuovi iscritti previsti per il prossimo anno accademico, il Corso di Cybersecurity Engineering contribuisce a formare una massa critica di professionisti qualificati di rilievo nel panorama nazionale e internazionale, dove la domanda di professionisti legati alla cybersicurezza è in grande aumento

Scopri di più leggendo il #PoliFlash ➡ https://lnkd.in/d_uZHwvF

Collegio ICM



👍👍👍 Tu e 855 altre persone

5 commenti · 39 diffusioni post

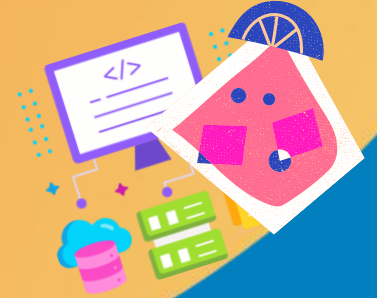




Politecnico
di Torino



#TOMORROW STARTS TODAY



Aperitivo di Benvenuto

Venerdì **27 Marzo** 2026

H. **17:30**

2° piano Dipartimento **DAUIN**, **Corso Castelfidardo 34/d** (ingresso lato MixTo)

Occasione perfetta per fare nuove conoscenze, scoprire i laboratori del collegio ICM ed incontrare i docenti dei relativi corsi di studio!



Politecnico
di Torino

SALONE DELL'ORIENTAMENTO 2026

Sito:



Piano di Studi:



Telegram:



Politecnico
di Torino

