CYBERSECURITY 4 TEENS

Il progetto *Cybersecurity for Teens* (CS4T) nasce nell'ambito dell'iniziativa Ludoteca del Registro .it.
L'obiettivo principale è quello di promuovere la cultura della sicurezza informatica nei giovani, molto abili dal punto di vista dell'utilizzo delle tecnologie digitali ma, spesso, non consapevoli dei possibili rischi e dunque potenziali vittime di attacchi informatici. Più nello specifico, gli obiettivi sono:

- ***Indagare e migliorare le conoscenze e i comportamenti di utilizzo della Rete Internet*** in modo da favorire l'adozione di pratiche di "igiene informatica" basate su un approccio preventivo, di conoscenza dei rischi.
- ***far acquisire ai ragazzi un curriculum verticale dedicato alla sicurezza informatica***, incentrato sulle seguenti competenze: proteggere i dispositivi; proteggere i dati personali e la privacy; riconoscere e intervenire sui rischi del cyberspazio, inteso come interazioni di persone, software e servizi per mezzo di tecnologie, dispositivi e reti ad esso connesse.

Il progetto è stato portato avanti con la collaborazione del Dipartimento di Formazione, Lingue, Intercultura, Letterature e Psicologia (FORLILPSI) dell'Università di Firenze, che si è occupato di valutare il raggiungimento degli obiettivi proposti somministrando agli studenti di un questionario al fine di rilevare le conoscenze e i comportamenti di sicurezza informatica, all'inizio e al termine del percorso di formazione stessa. La rilevazione dei dati è avvenuta in maniera anonima, con impossibilità di risalire all'identità dei singoli, nel pieno rispetto delle tutele e dei diritti riconosciuti dal Regolamento (UE) 2016/679 (come modificato dal D.lgs. n. 101/2018). I dati ricavati dalla somministrazione sono stati trattati in maniera aggregata, al fine di trarre conclusioni relativamente all'efficacia del progetto. Di seguito, sono presentati i risultati principali.

PARTECIPANTI

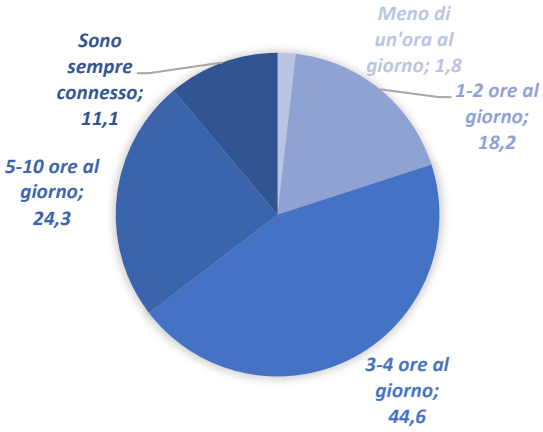
278 studenti da 3 scuole

Liceo Scientifico Statale F. Buonarroti (PISA)

IIS Da Vinci – Fascetti (PISA)

ITI Marconi (Pontedera)

26% femmine - età media 16 anni

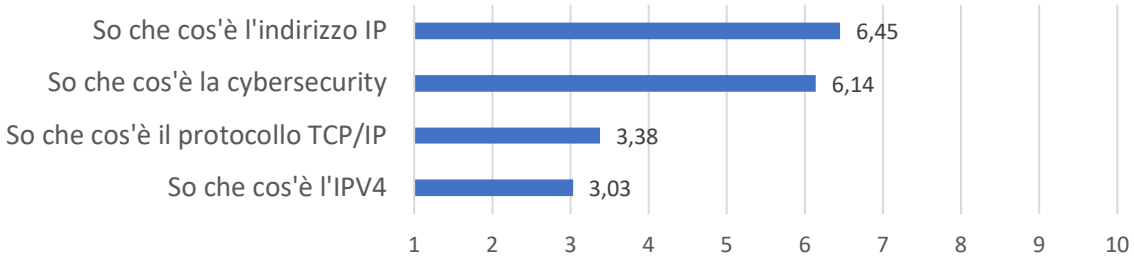


Escludendo le lezioni online, il **45%** dei partecipanti trascorre online almeno 3-4 ore al giorno, il **24%** dichiara di trascorrere online almeno 5-10 ore e **l'11%** di essere sempre connesso. Internet è usato principalmente per ***chattare con gli amici, ascoltare musica e/o guardare video online e cercare notizie o informazioni.*** Meno spesso invece, l'utilizzo di Internet riguarda attività come ***Installare un programma, Fare acquisti online e Usare linguaggi di programmazione.***

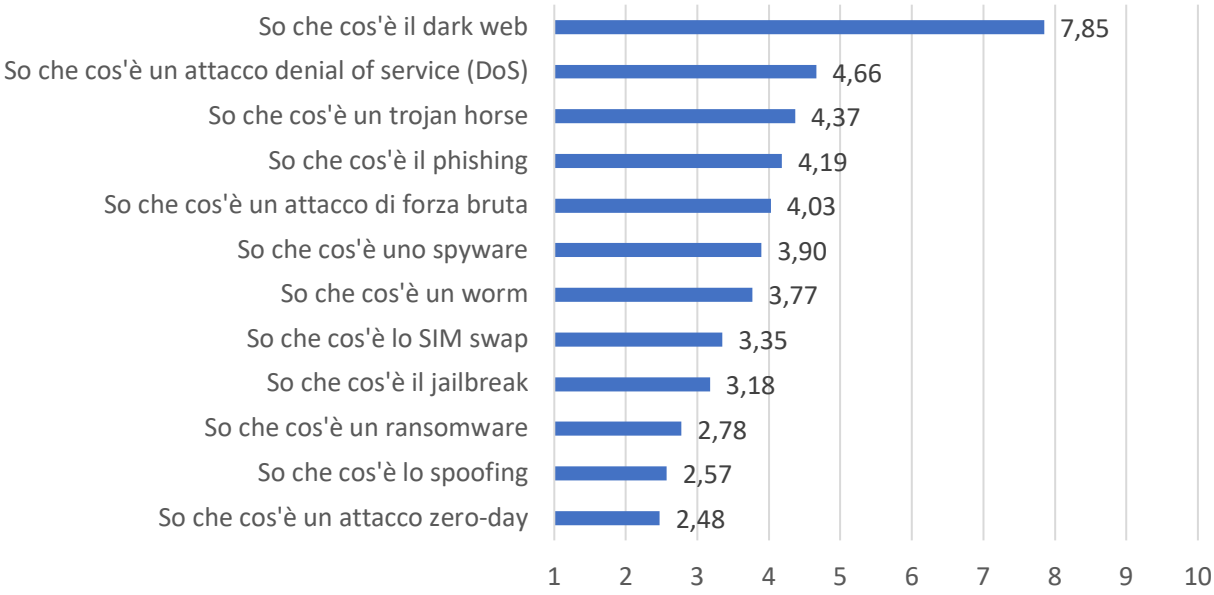
QUANTO PENSI DI CONOSCERE LA CYBERSECURITY?

Le conoscenze iniziali dei ragazzi nell'ambito della cybersecurity si collocano ad un livello ***complessivamente insufficiente***: qualche concetto ottiene una risposta media sufficiente (*es. "So che cos'è un indirizzo IP" – "So che cos'è il dark web*", ma ***la maggior parte degli argomenti sembrano essere scarsamente conosciuti*** (*es. "So che cos'è il protocollo TCP/IP" – "So che cos'è il phishing"*). Il livello medio di conoscenze nell'ambito della cybersecurity è molto diverso tra maschi e femmine: sebbene anche i maschi si assestino su un punteggio medio insufficiente *(mediamente 5 su una scala da 1 a 10)*, le femmine sembrano saperne ancora meno *(mediamente 3 su una scala da 1 a 10)*. Inoltre, questi livelli di conoscenza hanno una variabilità molto elevata: qualche studente sembra essere molto preparato, mentre altri sembrano non saperne quasi niente.

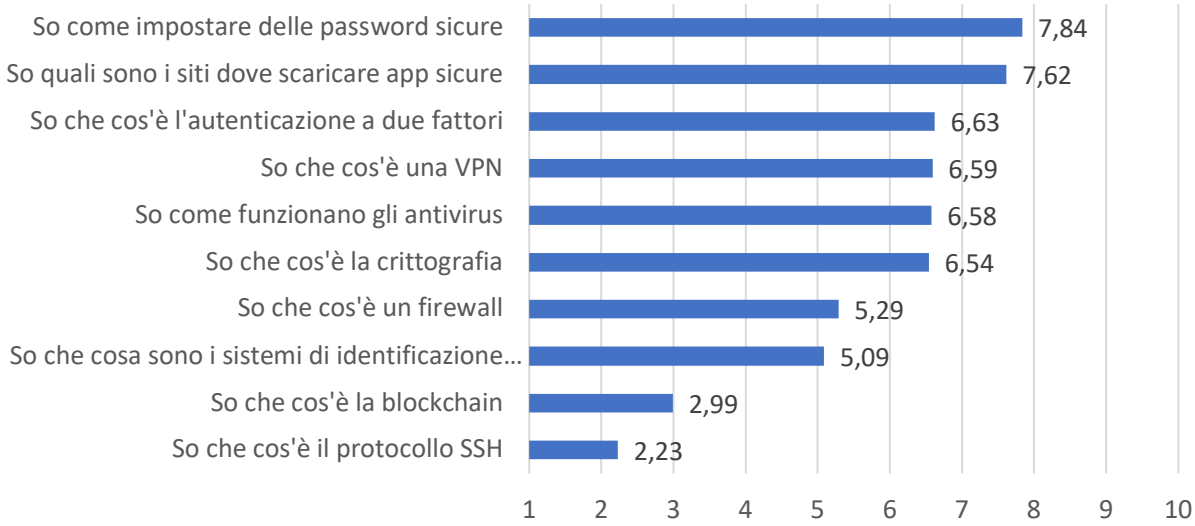
CYBERSECURITY



RISCHI



CONTROMISURE



I CONTENUTI DEL PROGETTO:

A seguito della prima rilevazione dei dati, le classi hanno partecipato a 3 incontri formativi, i primi due a stampo teorico mentre l'ultimo di tipo laboratoriale.

I contenuti affrontati nella parte teorica sono stati incentrati sulle seguenti tematiche:

	I incontro	II incontro	III incontro
Fasi	Webinar 1 + Questionario 1 cos'è la cybersecurity; superficie di attacco; minacce e vulnerabilità; cardini sicurezza; principali tipologie di attacchi informatici; contromisure tecniche (sistemi di identificazione e prevenzione intrusioni, autenticazione, crittografia) e buone pratiche.	Webinar 2 approfondimento delle buone pratiche con focus sul mobile e sui social media (gestione download app, permessi, impostazione privacy/accesso);	Webinar 3 + Laboratorio + Questionario 2 hacker, cracker, hacktivism; le professioni digitali (professioni del web con focus sul settore della cybersecurity).
Durata	3 ore	3 ore	4 ore
Periodo	Novembre/Dicembre	Gennaio/Febbraio	Marzo/Aprile

Per rendere il più interattive possibile le lezioni teoriche sono stati utilizzati diversi strumenti didattici tra cui:

- materiale video (webinar e video pillole) a cura della Ludoteca del Registro .it e dei ricercatori Unità di Ricerca Trust, Security and Privacy dello IIT-CNR;
- mappa 3D degli attacchi dell'Osservatorio di Cybersecurity dello IIT-CNR;
- Escape room a cura dell'IMT Lucca: https://anerddogma.it/94cc01e344e42fea9c4d7814302af384/
- materiale corso online: https://www.hackerhighschool.org/lessons.html#header2-10;
- app di quiz online come Kahoot, Mentimeter, Slido

Il laboratorio didattico è stato curato dai ricercatori dell'Unità di Ricerca Trust, Security and Privacy dello IIT-CNR. In questo incontro sono state fornite agli studenti nozioni più tecnico-pratiche relativamente a tre attacchi noti: phishing, la creazione di un malware e l'attacco di Denial of Service Distribuito. Allo scopo di accrescere la consapevolezza degli studenti rispetto alla pericolosità di questi attacchi e alla facilità con cui è possibile farli e anche esserne vittima, per ognuno di questi attacchi sono stati descritti strumenti specifici per la loro attuazione. È stato anche richiesto agli studenti di fare piccoli esercizi per "toccare con mano" la fattibilità di tali attacchi. Infine, sono state descritte le contromisure da mettere in atto per proteggersi dagli attacchi descritti.

EFFICACIA DEL PROGETTO

Il 91% dei ragazzi ha partecipato al progetto seguendo almeno un incontro, e ***la maggior parte di loro ha seguito l'intero percorso formativo, partecipando a tutti e tre gli incontri (85%).*** In totale, hanno preso parte al progetto CS4T, compilando i questionari sia alla prima che alla seconda rilevazione, 212 studenti.

A seguito del percorso formativo CS4T, il livello medio di conoscenze relative alla cybersecurity, ***migliora sotto tutti gli aspetti: cybersecurity in generale*** (Figura 1), ***rischi*** (Figura 2) ***e contromisure*** (Figura 3). Le femmine, che partivano da un livello di conoscenze iniziali nettamente più basso rispetto ai loro coetanei maschi, recuperano questo gap a seguito del percorso formativo e raggiungono lo stesso livello di conoscenze medio dei maschi.

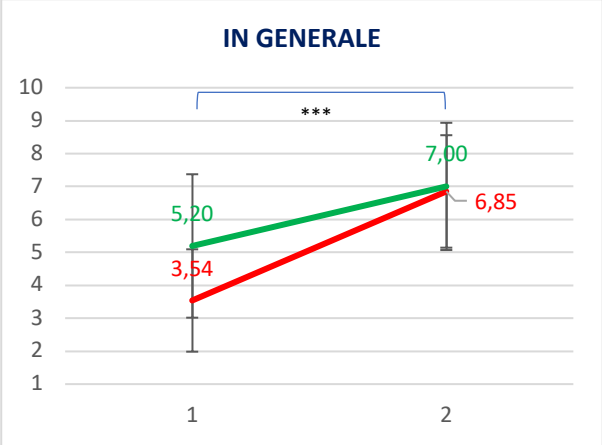


Figura 1 - Efficacia del progetto: cybersecurity

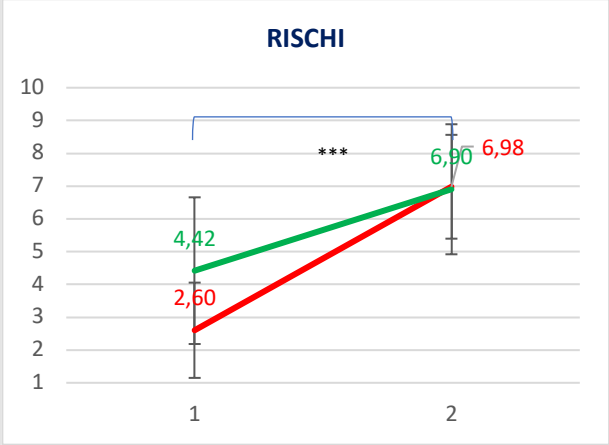


Figura 2 - Efficacia del progetto: cybersecurity (rischi)

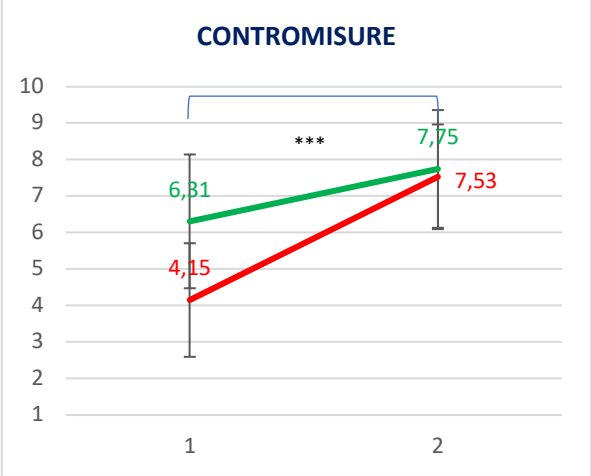
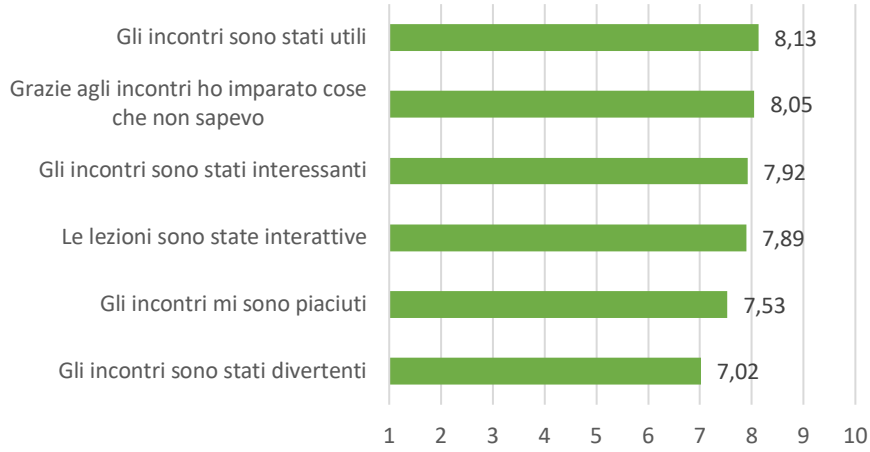


Figura 3 - Efficacia del progetto: cybersecurity – contromisure

GRADIMENTO

Il progetto CS4T ha avuto un riscontro positivo in termini di gradimento. In generale, gli incontri sono stati valutati come ***interessanti, interattivi, e divertenti.*** Alcuni dei ragazzi hanno lasciato qualche commento per esprimere la soddisfazione per il progetto, come ad esempio: ***"Fondamentale per una conoscenza sufficiente del mondo del web, grazie!".***



CONCLUSIONI

L'ampio margine di miglioramento ottenuto dai ragazzi ci conferma come questo argomento fosse da loro molto poco conosciuto, ma anche di ***grande interesse, visto l'impegno e l'attiva partecipazione*** che hanno dimostrato nel corso degli incontri. L'importanza di attività formative come quella proposta, è relativa anche alla divulgazione di certe tematiche, e in particolare nel tentativo di indirizzare i ragazzi verso il ***settore professionale della cybersecurity***: in questo campo, c'è infatti ancora carenza di esperti, e sviluppare un percorso di formazione di questo tipo può avere anche ***ricadute utili per il mercato del lavoro.***