DOI: 10.26314/GARR-Conf21-proceedings-04

Ludoteca del Registro .it: i laboratori di cybersecurity

Giorgia Bassi, Beatrice Lami

CNR-IIT, Istituto di Informatica e Telematica

Abstract. Il contributo descrive i laboratori di cybersecurity della Ludoteca del Registro .it, progetto a cura del Registro .it, anagrafe dei domini internet italiani il cui servizio è gestito dall'Istituto di Informatica e Telematica del Cnr di Pisa

Keywords. Digital literacy, cybersecurity, educazione digitale

Introduzione

La Ludoteca del Registro .it è un progetto nato nel 2011 con l'obiettivo di diffondere la cultura digitale a partire dalle scuole primarie. Ad oggi, sono oltre 14.000 gli alunni incontrati in tutto il territorio nazionale, per un totale di circa 1400 ore di formazione.

Il progetto nasce da un dato evidente: ragazzi e bambini trascorrono buona parte della loro vita online, nella maggioranza dei casi senza gli strumenti adeguati per un utilizzo sicuro e responsabile delle risorse digitali.

Secondo la ricerca "Ipsos per Save the Children" del 2019, il 97% dei ragazzi tra gli 11 e 17 anni possiede uno smartphone connesso a Internet e il 74% dichiara di avere una percezione dei potenziali rischi. A questo si aggiunge il ruolo della famiglia, non sempre preparata a gestire la dimensione digitale della vita dei figli. Secondo la ricerca condotta da CISF (2017) su un campione rappresentativo di 4000 famiglie, il 56% dichiara di non avere protocolli condivisi per l'uso dei media digitali, il 27% non ne parla mai con i figli e il 37% non si preoccupa di quello che questi ultimi possono pubblicare online. Inoltre, nella maggior parte dei casi "a fronte di una verbalizzazione preoccupata dei rischi del digitale, si assiste a una diffusione generalizzata e non adeguatamente resa oggetto di riflessione critica" (Rivoltella 2020).

I problemi derivanti da un uso non sicuro di Internet e dei sistemi informatici possono essere molteplici, dalla diffusione di malware, alla violazione di dati al furto di identità. Fenomeni sempre più diffusi come il cyberbullismo, il grooming e il sexting implicano invece considerazioni e interventi che appartengono all'ambito delle scienze sociali, ma è evidente che gli strumenti della cybersecurity, anche in questi casi, possono rappresentare un primo passo per stimolare un atteggiamento preventivo, soprattutto per quanto riguarda la protezione dei dati personali.

1. Insegnare la cybersecurity

A partire dall'anno scolastico 2018/19, la Ludoteca del Registro .it ha avviato il progetto di

laboratori di cybersecurity per le classi primarie e secondarie di primo grado, coinvolgendo in questo primo ciclo circa 1000 bambini.

I laboratori prevedono una parte propedeutica dedicata a nozioni elementari di informatica (ad esempio: indirizzo IP, protocolli informatici, nomi a dominio) spiegate sempre attraverso attività di gruppo. Si passa quindi a introdurre la cybersecurity come insieme degli strumenti per la protezione del cyberspazio, intendendo con questo termine l'insieme dei sistemi informatici (computer e dispositivi digitali di vario tipo) e dei dati in formato digitale.

Ai bambini si spiega che la sicurezza, in generale, va intesa come un processo, non come una soluzione tecnica da usare per contrastare la minaccia quando si presenta: anche in ambito informatico, è fondamentale sviluppare un atteggiamento preventivo. A questo proposito, le immagini di una cintura di sicurezza e di uno spazzolino da denti risultano molto efficaci per introdurre il concetto di "igiene informatica", l'insieme cioè dei comportamenti da seguire quotidianamente per prevenire e minimizzare i rischi.

La difesa del cyberspazio riguarda non solo l'aspetto hardware dei dispositivi ma anche i dati in essi salvati, trasmessi e condivisi. Per introdurre il concetto di dati personali e privacy in Rete, viene mostrata l'immagine di un cartello di proprietà privata, segnale che i bambini riconoscono e che identificano come divieto di accesso all'interno di uno spazio fisico.

Argomento quello della privacy online cruciale visto che, per la cosiddetta generazione Z (i nati dalla seconda metà degli anni '90 al 2010), rappresenta un valore tutto da definire, la "self(ie) generation" vive in "un contesto di sovra esposizione di informazioni personali, si costruisce attraverso le proprietà che caratterizzano il rapporto tra relazioni e contenuti nelle proprie reti, aprendo o chiudendo le cerchie, esplorando i profili degli altri a misurarne la reputazione, dando valore a sharing e tag " (Boccia Artieri 2015).

Un concetto quindi molto labile che merita di essere chiarito già nelle classi primarie, definendo quali siano le informazioni che senza dubbio non si devono mai condividere, ovvero password, nominativi, indirizzi postali, numeri di telefono, dati bancari.

Ai bambini si spiegano quindi i principali requisiti di un sistema informatico sicuro: confidenzialità, integrità e disponibilità. La confidenzialità è la riservatezza di un messaggio (si fa l'esempio di una mail o di una chat), l'integrità è la completezza e correttezza di quel messaggio (si pone la domanda: che cosa succederebbe se al destinatario arrivassero messaggi interrotti a metà?), la disponibilità è la caratteristica di rendere quel messaggio o quell'applicazione leggibile/utilizzabile per tutto il tempo necessario.

2. Conoscere e contrastare le minacce

Il tema delle minacce e della difesa del cyberspazio è affrontato portando all'attenzione della classe esperienze e opinioni, attraverso queste domande poste alla classe: "avete mai preso un virus informatico o è capitato a qualcuno che conoscete?", "come si deve impostare una password perché sia sicura?", "avete mai sentito parlare di "hacker", "quali sono i dati che non si devono condividere su Internet?".

Attraverso il dibattito, si stimola una prima riflessione su una serie di comportamenti

a rischio: apertura e condivisione di link all'interno di messaggi che provengono da sconosciuti, scelta inadeguata di password, download applicazioni da siti non sicuri, condivisione dati personali, gestione inadeguata dei permessi delle app e delle impostazioni di accesso e privacy di account social o di applicazioni di messaggistica istantanea.

L'immagine utilizzata per approfondire il tema delle minacce e degli attacchi cyber è il cavallo di Troia che, oltre a indicare una specifica categoria di malware, permette ai bambini di riflettere soprattutto sui meccanismi di diffusione.

Quello che si evidenzia è che l'anello debole è rappresentato, proprio come nella leggenda dell'assedio di Troia, non tanto da eventuali vulnerabilità tecniche ma soprattutto dal comportamento umano che cede, per esempio, di fronte a invitanti premi o richieste da parte di persone che si fingono amici.

In questo caso, l'atteggiamento da adottare è quello di una "sana diffidenza" che deve passare anche dal confronto e dalla condivisione delle esperienze con gli adulti, spesso meno esperti da un punto di vista tecnico ma sicuramente in grado di riconoscere e gestire alcune situazioni di potenziale rischio.

Dopo una breve introduzione ai più comuni malware (virus, worm, trojan, spyware) e soprattutto ai meccanismi che permettono a questi programmi malevoli di entrare nei dispositivi (link sospetti, download da siti non ufficiali), si affronta il tema delle contromisure.

Tra queste i sistemi di autenticazione, in particolare ci si sofferma sul tema delle password, giocando con una serie di combinazioni per dimostrare l'importanza di sceglierle sempre robuste, ovvero non facili da memorizzare e diverse a seconda degli account. Introduciamo quindi altri sistemi di difesa come l'antivirus e i firewall con un breve accenno anche alla crittografia che approfondiamo nel gioco del Cifrario di Cesare, descritto nel paragrafo successivo.

3. Giocare con la sicurezza informatica

La caratteristica comune dei laboratori è quella di alternare le nozioni teoriche con attività pratiche di gioco che vedono la partecipazione attiva dei bambini. Per il dettaglio completo dei materiali utilizzati si rimanda al sito web della Ludoteca, alla pagina: https://www.ludotecaregistro.it/per-le-scuole/cybersecurity/.

Di seguito una breve descrizione di alcuni materiali utilizzati:

- Fumetto "Nabbovaldo contro i pc zombi": ambientato nella città di Internetopoli, il protagonista è Nabbovaldo, un ragazzo appassionato di Internet ma molto ingenuo che dovrà affrontare la minaccia di terribili malware.
- Gioco del "Cyber Security Quiz": tavole a fumetti ambientate nella città di Internet. Il protagonista è sempre Nabbovaldo. Ogni tavola presenta una situazione a rischio di partenza e tre possibili comportamenti che potrebbero risolverla, ma solo uno rappresenta la scelta corretta.
- Cyber bowling sulla sicurezza in Rete: i birilli da abbattere sono i comportamenti da evitare, come ad esempio non aggiornare i sistemi operativi, scegliere sempre la stessa password, scaricare app da siti non ufficiali.

Fig. 1
Il gioco a fumetti
"Cyber Security Quiz"

- Cifrario di Giulio Cesare: l'antico strumento per inviare messaggi segreti diventa lo spunto per spiegare ai bambini la confidenzialità dei dati e una tecnica di crittografia.
- Password Memory: lo sforzo mnemonico legato alla ricerca di coppie uguali di password è un'occasione per riflettere sull'importanza di sceglierle in modo adeguato.

Naturalmente, a seguito dell'emergenza da Covid-19, durante l'anno scolastico 2020/21, si è resa evidente l'importanza di adottare strumenti per la didattica a distanza e dunque alcune attività sopra ricordate sono state in parte adattate al mutato contesto di apprendimento.

4. Sviluppi futuri

Nel mese di maggio 2021 è stato pubblicato sui principali store il videogioco "Nabbovaldo e il ricatto dal cyberspazio" per dispositivi mobile e nella versione desktop. La scelta di sviluppare, all'interno di questo progetto, un videogioco educativo interamente dedicato a questo tema rappresenta un'ulteriore spinta nella diffusione di una cultura della sicurezza informatica attraverso una modalità didattica innovativa e ricca di potenzialità.

La modalità di fruizione è single-player ma è previsto un percorso specifico di utilizzo nelle classi, attraverso il supporto dei formatori della Ludoteca e degli altri strumenti e risorse del progetto. Il gioco prevede una struttura ibrida tra il percorso fisso e open world: ci si può muovere liberamente nella mappa della città, parlare con i personaggi e risolvere i mini-giochi nell'ordine che si preferisce, anche se la trama del gioco si sviluppa in quattro capitoli principali, più un epilogo.

Dal mese di febbraio 2021 inoltre è stata avviata la valutazione dell'efficacia dei laboratori in collaborazione con il Dipartimento di Formazione, Lingue, Intercultura, Letterature e Psicologia dell'Università di Firenze.

La valutazione si è svolta fino al mese di aprile 2021 mediante la somministrazione di questionari ex ante ed ex post.

Riferimenti bibliografici

Boccia Artieri G., (2015), Gli effetti sociali del Web. Forme della comunicazione e metodologie della ricerca online, Franco Angeli, Milano.

Rivoltella P. C., (2020), Nuovi alfabeti, Scholè, Brescia.

Autrici

Giorgia Bassi giorgia.bassi@iit.cnr.it

Master in Comunicazione e Multimedia, dal 2006 lavora all'Istituto di Informatica e Telematica del Cnr di Pisa in cui ha sede il Registro .it l'anagrafe dei nomi a dominio a targa .it, collaborando a progetti di comunicazione legati ai nomi a dominio. Dal 2011 cura i contenuti, la comunicazione e le attività di divulgazione della Ludoteca del Registro .it. E' referente del progetto di peer education Let's Bit! destinato agli istituti superiori.

Beatrice Lami beatrice.lami@iit.cnr.it

Laurea Magistrale in Informatica, Master in Management della Formazione. Dal 2000 lavora all'Istituto di Informatica e Telematica del Cnr di Pisa in cui ha sede il Registro .it. Si occupa di aspetti tecnici legati alla registrazione dei nomi a dominio, della formazione dedicata ai Registrar; dal 2011 è referente del progetto Ludoteca del Registro .it, di cui valida anche i contenuti tecnici. Collabora anche al progetto di peer education Let's Bit!.