

Educare alla cyber sicurezza con il gioco

Giorgia Bassi¹ e Beatrice Lami¹

¹ Istituto di Informatica e Telematica, Consiglio Nazionale delle Ricerche – Registro .it.
giorgia.bassi@iit.cnr.it, beatrice.lami@iit.cnr.it

Abstract

Il presente articolo descrive alcune metodologie e strumenti didattici utilizzati nell'ambito del progetto di educazione digitale Ludoteca del Registro .it, con un focus sui laboratori dedicati alla sicurezza informatica. Il progetto Ludoteca del Registro .it è a cura di Registro .it, l'anagrafe dei domini con estensione .it gestita dall'Istituto di Informatica e Telematica del Cnr.

1 Introduzione

Nell'era digitale bambini e adolescenti sono sempre più connessi e accedono quotidianamente a piattaforme, siti, social network per informarsi, comunicare o semplicemente trascorrere momenti di svago. Questa crescente interazione con il mondo digitale da un lato offre alle giovani generazioni innumerevoli opportunità, ma allo stesso tempo comporta una serie di rischi, legati soprattutto alla gestione dei dati.

L'indagine pubblicata da Save the Children in occasione del Safer Internet Day 2024 evidenzia una diminuzione dell'età media del primo accesso alla Rete e un aumento del tempo medio trascorso online dai più giovani, specialmente dopo la pandemia. Dalla stessa ricerca emerge che il 13,5% degli adolescenti italiani di 11, 13 e 15 anni fa un uso problematico dei social media, mentre il 24% è a rischio di sviluppare una dipendenza da videogiochi.

Il rapporto "EU Kids Online Italy" del 2017 evidenzia che la percentuale di ragazzi italiani che dichiara di aver vissuto esperienze negative su internet è raddoppiata rispetto al 2010 e al 2013. In particolare, tra i bambini di 9-10 anni, la percentuale è aumentata dal 3% al 13%.

Tali dati mettono in evidenza l'esposizione sempre più pervasiva a pericoli che riguardano la sfera sociale (cyberbullismo, dipendenza) ma che derivano spesso da un utilizzo non sicuro dei dispositivi, e dunque a una scarsa tutela dei propri dati e privacy online.

L'obiettivo del progetto Ludoteca del Registro .it, nato nel 2011 per iniziativa del Registro .it, parte proprio da questa premessa: proporre attività di cybersecurity education a partire dalla fascia di età dei 11-13 anni, cercando di stimolare in loro un uso critico e consapevole del digitale, partendo anche da conoscenze tecniche.

2 Competenze digitali e cybersecurity

La Ludoteca opera nel campo della cultura digitale dal 2011, promuovendo l’uso consapevole della Rete attraverso laboratori nelle classi di tutti gli ordini e gradi.

In ambito formativo, oggi prevale l’idea di una “didattica per competenze”, intendendo con quest’ultimo termine l’insieme delle conoscenze, abilità e attitudini applicabili a uno specifico contesto. Per quanto riguarda le competenze digitali, il riferimento teorico è il framework europeo *DigComp* (oggi giunto alla versione 2.2), che individua queste cinque aree di interesse: alfabetizzazione dei dati, comunicazione e collaborazione, creazione di contenuti digitali, sicurezza, problem solving.

Inserita all’interno di questa cornice teorica, l’attività della Ludoteca copre, in parte, l’area delle competenze legate all’alfabetizzazione dei dati (come navigare e gestire le informazioni online) e della sicurezza. Per insegnare a bambini e ragazzi, futuri cittadini digitali, come muoversi all’interno del cyberspazio, evitando i rischi, la Ludoteca propone da anni percorsi formativi dedicati alla conoscenza dei rischi ma anche all’acquisizione di un “saper fare” o abilità con cui riconoscerli e contrastarli, sviluppando un’attitudine alla prevenzione che è propria della cosiddetta “igiene informatica”.

L’impegno nell’ambito della cybersecurity education ha alla base la ferma convinzione che per agire sull’anello debole della sicurezza dei sistemi informatici, ovvero l’utente, sia necessario intervenire con campagne di sensibilizzazione ma anche con programmi formativi, già a partire dalle scuole primarie e secondarie di primo grado.

2.1 Game based learning

Per diffondere le competenze digitali e, in particolare, le buone pratiche di sicurezza informatica in modo coinvolgente per gli alunni delle primarie e secondarie di primo grado, si è cercato di lavorare molto sugli strumenti didattici, optando per soluzioni che aumentassero il più possibile il livello di interazione. Da qui la scelta di adottare strumenti e metodologie “game base learning”, con attività e giochi di gruppo da svolgere in classe con il supporto di risorse didattiche specifiche. Già a partire dall’anno scolastico 2018/19, sono stati proposti nelle classi di scuole secondarie di primo grado i seguenti giochi “unplugged”, privi cioè di supporti tecnologici:

- Gioco Cifrario di Cesare: ispirato al metodo di cifratura utilizzato dal celebre condottiero romano per inviare messaggi segreti. Il gioco prevede l’utilizzo di un manufatto costruito come una doppia rotella su cui è riportato l’alfabeto e su cui è possibile mettere in atto il meccanismo di sostituzione monoalfabetica. Rappresenta un valido strumento per introdurre il concetto di “confidenzialità” dei dati e dei messaggi e al tempo stesso per spiegare le tecniche di crittografia.
- Gioco Carte Memory: classico gioco con carte, per allenare la memoria facendo le varie accoppiate. Questo gioco stimola la riflessione sull’importanza di gestire le password con attenzione, evidenziando il diverso livello di robustezza.
- Gioco acronimo: partendo dal testo di una canzone famosa, i gruppi considerano solo le prime lettere delle varie parole che compongono la frase e da questo primo insieme di lettere creano una password robusta ma facilmente memorizzabile.
- Cruciverba: il classico cruciverba con definizioni su alcune nozioni di cyber sicurezza e di informatica di base (come ad esempio backup, file, app, malware, hacker, antivirus).
- Gioco Cyber Quiz: gioco di gruppo basato su tavole a fumetti in cui viene presentata una possibile situazione di rischio online e tre possibili finali: solo uno di questi rappresenta il comportamento corretto in un’ottica di igiene informatica.
- Gioco Prima pensa poi condividi: gioco che prevede l’utilizzo di carte che riportano su un lato varie tipologie di informazioni personali (ad esempio: indirizzo di casa, numero carta di

credito, band preferita, colore preferito), sull’altro le argomentazioni per cui è opportuno o meno non condividerle online.



Figure 1 Gioco unplugged

2.2 Il videogioco Nabbovaldo: storytelling e metafore

La scelta di sviluppare, all’interno di questo progetto, un videogioco educativo sulla cybersecurity rappresenta un’ulteriore spinta nella diffusione della cultura della sicurezza informatica attraverso una modalità innovativa e ricca di potenzialità.

Il videogioco “Nabbovaldo e il ricatto dal cyberspazio” è single player ed è concepito come un’avventura in quattro capitoli, come un libro, e si sviluppa attraverso una storia avvincente.

Il protagonista è Nabbovaldo (crasi tra Nabbo, nel gergo online “novellino” e Marcovaldo, dall’omonimo romanzo di formazione di Calvino), un giovane tuttofare che vive e lavora a Internetopoli, dal carattere ingenuo e che nel corso dell’avventura impara a difendersi dalle insidie dell’online. Ciascun personaggio è caratterizzato da un nome che richiama aspetti della cultura digitale, ad esempio, in riferimento ai social network Troll, Heater Hater, e Fint Flamer. Tra di loro, Carla Cospira spicca come una donna incline a vedere cospirazioni ovunque: nevrotica e credulona, indossa uno scolapasta in testa e crede a teorie come le scie chimiche o il mostro di Loch Ness.

In ogni capitolo, il giocatore aiuta Nabbovaldo a completare missioni e minigiochi legati alla sicurezza informatica. Quando un misterioso pacco consegnato alla casa di Linda rilascia un “ransomware” (malware che mette sotto sequestro i dispositivi, liberandoli solo con un riscatto) che ne blocca l’ingresso, Nabbovaldo è costretto a trovare una soluzione, rivolgendosi senza successo a vari esperti.

La trama si intensifica quando altre case sono infestate dal ransomware, spingendo Nabbo e Linda a indagare sul colpevole. Dopo vari tentativi, il giocatore scopre che dietro a tutto c’è un piano diabolico orchestrato dai gatti di Internetopoli, guidati dalla gattara robotica Kitty Kathy, per trasformare Internet in un mondo dominato dai felini. Solo chi riuscirà ad arrivare all’epilogo saprà se i nostri eroi riusciranno a salvare la rete da questo disastro.

La storia si dipana attraverso quattro capitoli, vari Ambienti di Internetopoli e l’attivazione dei Dialoghi che introducono nozioni e concetti importanti relativi soprattutto ad alcune buone pratiche di cybersecurity (impostazioni password, gestione di messaggi da sconosciuti, utilizzo dati sui social network). Lo storytelling permette dunque di mantenere viva l’attenzione e il coinvolgimento, veicolando contenuti educativi e nozioni tecniche.

Gli scenari in cui si muovono i personaggi sono coloratissimi e caratterizzati da una grafica molto originale e sono costruiti anche con un ricco uso di metafore.

Il lucchetto sulla porta di Linda è una metafora dell'attacco informatico ransomware che mette sotto sequestro i dispositivi impedendo agli utenti di accedervi e, ancora, la doppia casa di Mr. D richiama all'utilità di fare il back up dei propri dati.



Figure 2 Nabbovaldo e la metafora del ransomware

Lo storytelling e l'uso delle metafore nella didattica esercitano un'influenza positiva sul processo di apprendimento, poiché coinvolgono gli alunni/e a livello emotivo e facilitano la comprensione dei concetti, rendendoli più semplici da ricordare. Attraverso le narrazioni, i contenuti educativi vengono inquadrati in storie che favoriscono una comprensione più profonda e aiutano a sviluppare un legame empatico con ciò che stanno studiando (Arsena, 2023).

Inoltre, l'uso della metafora, nella didattica e in generale nel campo della divulgazione, ha dimostrato di poter migliorare la comprensione di concetti complessi, rendendoli accessibili attraverso il collegamento a esperienze quotidiane o contesti familiari. Lakoff e Núñez sostengono che le metafore sono strumenti cognitivi fondamentali per il ragionamento scientifico - matematico, poiché permettono di comprendere concetti astratti attraverso elementi del nostro sistema senso-motorio (Sbaragli, 2016).

Anche nei laboratori unplugged (v. par. 2.1) spesso si utilizza la metafora per introdurre concetti legati alla sicurezza: l'immagine della cintura di sicurezza di un'automobile introduce l'idea della prevenzione come conoscenza dei rischi; il cavallo di Troia non solo si riferisce a un malware specifico, ma serve a far capire che spesso l'insidia, anche in Rete, si nasconde dietro qualcosa di apparentemente innocuo o allettante; un cartello di "proprietà privata" viene mostrato per introdurre il concetto di uno spazio in cui non si può entrare proprio come la nostra privacy online; e ancora le chiavi di casa che servono a spiegare le password, uniche e da non consegnare mai a sconosciuti.

3 La valutazione dell'efficacia dei lab sul videogioco

A conclusione di questa pubblicazione, si riportano i dati del progetto di valutazione dell'efficacia dei laboratori sul videogioco Nabbovaldo, svolti nelle classi secondarie di primo grado. La valutazione è stata svolta in collaborazione con il Dipartimento di Formazione, Lingue, Intercultura, Letterature e Psicologia (FORLILPSI) dell'Università di Firenze.

I dati di seguito riportati si riferiscono all'anno scolastico 2022/23 e riguardano sia classi sperimentali, che hanno cioè partecipato ai laboratori, sia classi di controllo, per un totale di 204 alunni.

I risultati sono il frutto di una rilevazione svolta attraverso la somministrazione di questionari agli alunni prima e dopo i lab, finalizzati a misurare le conoscenze e competenze in ambito di sicurezza informatica.

A seguito del percorso formativo, il livello medio di conoscenze relative alla Rete Internet, sono migliorate sia per quanto riguarda le conoscenze generali (Figura sotto a sinistra) che quelle più specifiche (Figura sotto a destra). Le femmine (segmento rosso), per quanto riguarda le conoscenze più specifiche, recuperano il gap nei confronti dei loro coetanei maschi (segmento verde) e, a seguito del percorso formativo, raggiungono il loro stesso livello medio di conoscenze

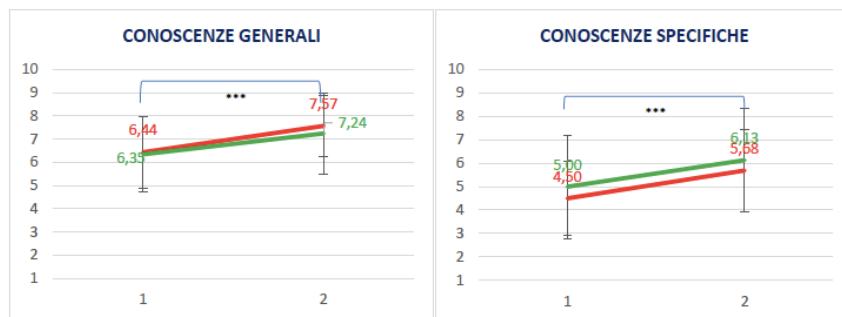


Figura 3 Livello di conoscenze

Inoltre, dalla valutazione emerge che il 60% degli alunni che ha partecipato al progetto ha giocato al videogioco e, per la maggior parte, da casa e non in compagnia. In generale, il videogioco è stato valutato utile e con meccaniche di gioco facili da comprendere e una grafica originale.



Figura 4 Gradimento videogioco

4 Sviluppi futuri

Lanciato nel 2019, il videogioco *Nabbovaldo e il ricatto dal cyberspazio* è il principale strumento della Ludoteca per educare alla cybersecurity i ragazzi in età tra 10-13 anni, tra le fasce oggi più esposte ai cyber rischi. Il videogioco è stato portato nelle classi a partire dall'anno scolastico 2020/21, coinvolgendo ad oggi circa 800 studenti.

Per operare in stretta sinergia con il corpo docente, è stata realizzata una Guida per insegnanti, per dare loro la possibilità di svolgere percorsi di approfondimento specifici in classe.

La necessità di “formare i formatori” rappresenta del resto una priorità futura del progetto Ludoteca che mira a una scalabilità di tutte le risorse. Il videogioco Nabbovaldo e tutti gli strumenti didattici della Ludoteca sulla cybersecurity convergono anche nel progetto europeo Erasmus Plus *SuperCyberKids! (SCK)*, partito a fine 2023 con la partecipazione di altri cinque partner internazionali. L’obiettivo del progetto è sviluppare e testare un framework educativo completo, basato sulle competenze di sicurezza informatica, attraverso una piattaforma *game-based learning* di risorse

educative per gli insegnanti. A breve, nel mese di marzo, partirà la fase pilota che in Italia prevede l'utilizzo di *Nabbovaldo* e di altre risorse della Ludoteca, partirà a breve con una sessione di formazione per gli insegnanti, per dare loro alcune basi di sicurezza e far acquisire metodologie e strumenti per l'utilizzo della piattaforma.

References

- Lughi, G. (2006). *Cultura dei nuovi media: teorie, strumenti, immaginario*, Voronkov, A. (2004). *EasyChair conference system*. Milano Guerini
- Arsena, A. (2023). *La lezione con storytelling digitale: per una narratività relazionale ed inclusiva attraverso la Rete* Annali online della Didattica e della Formazione Docente” Vol. 15, n. 26/2023, pp. 3-16 – ISSN 2038-1034
- Sbaragli S. (2016), *L'importanza della metafora in matematica e nella sua didattica*. In Iori M. (Ed.). Mathematics and Mathematics Education. International Conference, October 8, 2016, University of Bologna (Italy), 459-464.