BRICKS
FUORI NUMERO

A scuola di sicurezza informatica

a cura di:
Giorgia Bassi, Beatrice Lami

Sicurezza, Educazione digitale

L'importanza dell'educazione digitale

Bambini e ragazzi vivono oggi un rapporto spontaneo con il digitale che si manifesta soprattutto in una abilità tecnica. Sul fronte della consapevolezza c'è invece ancora molta strada da fare.
La generazione Z (i nati tra la seconda metà degli anni '90 e la fine degli anni 2000) non possiede infatti gli strumenti adeguati per sfruttare le risorse del digitale in modo critico e sicuro, questo ovviamente per un naturale difetto di maturità, anche se, secondo la ricerca "Ipsos per Save the Children" del 2019, il 74% dei ragazzi tra gli 11 e 17 anni dichiara di avere una percezione dei potenziali rischi.
Per supportare mondo scolastico e famiglie in un'azione di educazione digitale, il Registro .it, anagrafe dei domini a targa .it, ha creato nel 2011 il progetto Ludoteca del Registro .it, con l'obiettivo di diffondere la cultura digitale a partire dalle classi delle scuole primarie.
Ad oggi, sono oltre 11.000 i bambini incontrati in tutto il territorio nazionale, per un totale di circa 1.100 ore di formazione.
Durante i laboratori, gli alunni sono coinvolti in un percorso ludico didattico dedicato alla Rete Internet, per spiegare che cos'è, come funziona e come usarla in sicurezza.

Figura 1 - Laboratori di sicurezza informatica

Insegnare la sicurezza informatica

Le lezioni nelle classi primarie prevedono sempre una parte introduttiva dedicata ad alcune nozioni elementari di informatica, per spiegare, ad esempio, il linguaggio binario e la trasmissione a pacchetto dei dati. Su queste basi, si introducono i temi della sicurezza informatica, che ha lo scopo di proteggere i sistemi informatici e i dati in formato digitale.
L'aspetto che si evidenzia è che, anche nel mondo digitale, è meglio prevenire le minacce anziché ricorrere a contromisure tempestive, questo grazie soprattutto ad alcuni comportamenti quotidiani. 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 delle regole da seguire per minimizzare i rischi del cyberspazio.
Altro punto fondamentale è chiarire quale sia il bene più importante da difendere quando siamo su Internet e utilizziamo le tecnologie digitali.
Si parla, infatti, di dati ma non tutti i dati hanno la stessa importanza. 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, ci aiuta a introdurre il concetto di privacy.
Il passaggio successivo è, attraverso questa metafora, farli riflettere sul perché sia necessario identificare una "proprietà privata" anche nel mondo digitale.

Aspetto questo per niente scontato visto che la *privacy* rappresenta per questa generazione un valore tutto da definire, come afferma il sociologo Boccia Artieri 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* (…)".
Un concetto quindi molto labile che merita di essere affrontato già nelle classi primarie, chiarendo intanto quali siano le informazioni che senza dubbio non si devono mai condividere, ovvero *password*, nominativi, indirizzi postali, numeri di telefono, dati bancari.

Conoscere e prevenire le minacce

Una volta messi a fuoco "i beni" da difendere, si introducono altri due concetti cruciali della sicurezza informatica: vulnerabilità e minaccia. Per la prima usiamo l'immagine di una bicicletta lasciata senza catena e lucchetto, esposta quindi con alta probabilità al rischio di un furto.
L'immagine utilizzata per introdurre il tema delle minacce è invece il cavallo di Troia che, oltre a indicare una specifica categoria di *malware*, fa riflettere i bambini soprattutto sui meccanismi di inganno. Quello che si evidenzia è che l'anello debole è rappresentato, proprio come nella leggenda dell'assedio di Troia, non tanto da eventuali vulnerabilità dei dispositivi ma 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, ai bambini spieghiamo che l'atteggiamento migliore è quello di una sana "diffidenza" che deve passare anche dal confronto e dalla condivisione delle esperienze, a cominciare da amici, familiari o utenti più esperti.
A conclusione di questa parte introduttiva, si passa alla condivisione di buone pratiche da adottare per prevenire possibili minacce.
Parliamo quindi di "autenticazione", un'operazione fondamentale per garantire la "confidenzialità" dei dati quando accediamo a un sito o usiamo un'app, perché tramite l'operazione di *login* ci identifichiamo.

Per rendere l'autenticazione sicura raccomandiamo ai bambini di scegliere password "robuste", non facili da memorizzare e quindi di minimo otto caratteri, alfanumeriche, con almeno un carattere speciale e soprattutto diverse per ogni *account*.

Anche la sicurezza delle app richiede un approfondimento specifico, pensando soprattutto all'uso che ne fanno bambini e adolescenti sui loro smartphone: una fruizione rapida e quindi poco attenta alle conseguenze. In questo caso, questi sono i principali consigli:

- scaricare le app solo da store ufficiali,
- cercare di ottimizzare le impostazioni di privacy e sicurezza,
- fare attenzione a concedere i permessi di accesso a funzioni come il microfono, la videocamera, l'accesso ai contatti della rubrica.

Questo sul fronte della prevenzione. Per imparare a difendersi dalle minacce nel momento in cui si presentano una raccomandazione importante è, per esempio, non cliccare su *link* che arrivano da sconosciuti con messaggi di premi o richieste di modifica delle *password* dei nostri account.

Giocare con la sicurezza informatica

A partire da queste basi teoriche, proponiamo le attività laboratoriali che prevedono questi giochi di gruppi, svolti con materiali tradizionali (tavole, cartelloni, lavagna):

- Gioco del "Cyber Security Quiz": tavole a fumetti ambientate nella città di Internet. Il protagonista è Nabbovaldo, un ragazzo che affronta la vita *online* con troppa disinvoltura. Ogni tavola presenta una situazione a rischio di partenza e tre possibili comportamenti che potrebbero risolverla, ma solo uno rappresenta la scelta corretta dal punto di vista della sicurezza.

- *Cyber bowling* sulla sicurezza in Rete, dove 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.
- Cifrario di Giulio Cesare: l'antico strumento per inviare messaggi segreti diventa lo spunto per spiegare ai bambini la confidenzialità dei dati e dunque la crittografia.
- *Password memory*: il classico gioco di abbinamento di carte identiche, in questo caso raffiguranti elementi tecnologici o password. Lo sforzo mnemonico legato alla ricerca di coppie uguali di password è un'occasione per riflettere sull'importanza di sceglierle in modo adeguato.

Conclusioni

I laboratori dedicati alla sicurezza informatica continueranno per tutto l'anno scolastico 2020/21 anche in modalità di didattica a distanza a causa dell'improvvisa emergenza sanitaria da COVID-19. Alla luce di questo nuovo contesto, si è dovuto naturalmente ripensare alle modalità di svolgimento di alcune attività, penalizzando in parte il livello di interattività delle esperienze.

L'utilizzo di una nuova piattaforma Moodle della Ludoteca permetterà però di attivare percorsi formativi sulla sicurezza informatica basati sul modello della *flipped classroom*, naturalmente con il supporto dell'insegnante.

Per i prossimi mesi è previsto anche il lancio del videogioco "Nabbovaldo e la furia dei ramsomware", un'avventura a livelli ambientata a Internetopoli, la città di Internet, tutta dedicata alle tematiche della sicurezza informatica.

Giorgia Bassi

giorgia.bassi@iit.cnr.it
Affiliazione: Istituto di Informatica e Telematica (CNR)

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. Ha collaborato anche al progetto Let's Bit! il cui obiettivo è coinvolgere gli studenti delle superiori come educatori della Rete nelle classi primarie.

Beatrice Lami

beatrice.lami@iit.cnr.it
Istituto di Informatica e Telematica (CNR)

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. Ha collaborato anche al progetto Let's Bit! il cui obiettivo è coinvolgere gli studenti delle superiori come educatori della Rete nelle classi primarie.