Formazione esperienziale proposte per la sicurezza digitale

Formazione esperienziale proposte per la sicurezza digitale 2019

Book · April 2019

CITATIONS
0

READS
7

2 authors:

Alessio Surian
University of Padova
62 PUBLICATIONS **62** CITATIONS
SEE PROFILE

Daniela Frison
University of Florence
21 PUBLICATIONS **18** CITATIONS
SEE PROFILE

OPEN LEARNING

Alessio Surian, Daniela Frison

FORMAZIONE ESPERIENZIALE

Proposte per la sicurezza digitale

Pensa MultiMedia

OPEN LEARNING

collana diretta

da Luciano Galliani

18

I volumi di questa collana sono sottoposti
a un sistema di *double blind referee*

Alessio Surian, Daniela Frison

FORMAZIONE ESPERIENZIALE

Proposte per la sicurezza digitale

Pensa MultiMedia

Volume pubblicato con il contributo
del Dipartimento di Filosofia, Sociologia, Pedagogia e Psicologia Applicata
dell'Università degli Studi di Padova
Progetto PRAT *Edu4Sec – Effective Education for Improving Datasecurity Awereness*

ISBN volume 978-88-6760-629-0
ISSN collana 2284-4155

73100 Lecce • Via Arturo Maria Caprioli, 8 • Tel. 0832.230435
25038 Rovato (BS) • Via Cesare Cantù, 25 • Tel. 030.5310994
www.pensamultimedia.it • info@pensamultimedia.it

Indice

Introduzione
Quali azioni formative su dati digitali e sicurezza?

di *Alessio Surian*

Dal 2004 la Commissione europea ha istituito la giornata della Sicurezza in Internet, "Safer Internet Day" (SID). Cresce la consapevolezza dell'importanza di promuovere un utilizzo più informato e responsabile delle tecnologie legate ad internet, in particolare negli ambiti in cui si studia e lavora. Ciò comporta, da un lato, un adeguamento e aggiornamento delle normative e della loro attuazione, per esempio in relazione al recente

Regolamento Generale sulla Protezione dei Dati Personali (GDPR). Comporta anche, un atteggiamento attento e critico da parte di chi usa Internet e le tecnologie digitali.

Questo testo intende sostenere chi si propone di introdurre, nei percorsi di chi studia e chi lavora, momenti formativi che possano fornire un lessico di base ed occasioni di aggiornamento in merito ai principali comportamenti da monitorare, ai fattori di rischio, ai comportamenti da adottare per prevenire ed intervenire su questioni di data security. Più in generale, offre dati, riflessioni e proposte formative per fare i conti con la nostra "intelligenza digitale", soprattutto nel nostro rapporto con Internet, e con la nostra consapevolezza in materia di privacy e sicurezza informatica.

I contributi sono articolati in cinque capitoli.

Il primo capitolo propone di legare i temi delle competenze digitali e relative ad Internet, ed in particolare della sicurezza digitale, con quelli della formazione, soprattutto in chiave esperienziale e trasformativa. Da un punto di vista educativo, l'idea chiave è innestare percorsi di maggiore consapevolezza a partire dai comportamenti quotidiani di chi usa Internet e di sviluppare maggiore consapevolezza dal punto di vista della sicurezza dei dati in accordo con i contesti specifici le aspirazioni degli utenti.

Nel secondo capitolo, Giuseppe Cascavilla e Mauro Conti offrono una mappa per orientarsi rispetto alle informazioni a disposizione e alle questioni chiave relative alla data security. L'elenco delle possibili minacce è piuttosto lungo e la loro

dinamica evolutiva è marcatamente accelerata, ma l'intento degli autori non è quello di creare ansia, quanto piuttosto di aiutare a identificare gli elementi utili ad sviluppare modalità di rapporto con la rete e con i dati che generino consapevolezza e, quando necessario, cautela. Ci consegnano un invito piuttosto diretto: siamo sollecitati a imparare a prenderci cura personalmente della sicurezza dei nostri dati con piccoli gesti quotidiani; allo stesso tempo, siamo chiamati ad interagire con i governi e l'apparato legislativo per far sì che si rafforzino i diritti dei cittadini e le misure di prevenzione e sicurezza.

Il terzo capitolo è dedicato al progetto Edu4Sec che fra il 2017 e il 2018 ha affrontato questi temi con una ricerca-azione che, da un lato, ha raccolto dati rispetto alle conoscenze di studenti e lavoratori e, dall'altro, ha realizzato alcuni interventi formativi in collaborazione con scuole secondarie ed imprese del territorio veneto. Si tratta, in particolare di percorsi di formazione esperienziale tesi a mettere in evidenza come ogni cittadino possa essere messo in grado di identificare aree di rischio rispetto ai comportamenti digitali e in rete, sia di ambito quotidiano, sia in ambiti specifici come compiere acquisti o fare prenotazioni, sia nell'ambito di operazioni saltuarie.

Nel quarto capitolo viene offerta a titolo di esempio una traccia (micro-progettazione) di intervento formativo e vengono presentate alcune proposte di attività da poter svolgere in contesti formativi e le raggruppa secondo quattro domande e ambiti di lavoro: costruire un lessico condiviso; esplorare le opinioni e conoscenze dei partecipanti; individuare e condividere le esperienze pregresse; sperimentare.

Infine, il quinto capitolo prova ad indicare dove reperire risorse ed approfondimenti in merito a questi temi, sia a livello nazionale, sia internazionale.

1.

Promuovere consapevolezza in merito alla data security: conoscenze da costruire e decostruire

di *Alessio Surian*

Nei comportamenti quotidiani, sociali, lavorativi, attraversiamo frequentemente, oltre allo spazio fisico, anche il "cyber" spazio, quello che ci vede variamente connessi a persone, applicazioni e programmi software soprattutto tramite collegamenti Internet. Ognuno di questi collegamenti può essere potenzialmente sia una fonte di condivisione e collaborazione, sia di minacce ed intrusioni nella nostra vita. Gli studenti delle scuole superiori sembrano intuire la forte tensione fra aspetti positivi e problematici. Ci raccontano: "Queste tecnologie 'tolgono' le relazioni, ci si trova meno […]

Ma ci sono i lati positivi: sei in contatto con persone distanti […] Preoccupa che il mondo si trasferisca nel web: ci sono tante informazioni su Internet, troppe rispetto a quel che una persona può riuscire a captare".

Queste dinamiche sono in rapida evoluzione e trasformano anche i riferimenti legislativi nazionali e internazionali. Ad agosto 2018 è stato approvato il testo definitivo del decreto di armonizzazione dell'ordinamento italiano al Regolamento (UE) n. 679/2016, conosciuto come *GDPR, General Data Protection Regulation*. I temi del nuovo decreto rimandano a regole deontologiche, codici di condotta, misure di salvaguardia, provvedimento sulle autorizzazioni generali e nuovi provvedimenti previsti nella nuova normativa. In sintesi: il lavoro "attuativo" da fare è ancora molto per ottenere un quadro normativo completo della disciplina della protezione dei dati personali in Italia. Ma non è questione soltanto di leggi, normative e buone pratiche tecniche e tecnologiche. La sfida riguarda anche le narrazioni e gli immaginari che fanno i conti con questi cambiamenti, anche sul piano antropologico, e la misura in cui possano venire costruiti dalla società, in modo orizzontale, innescando attenzione e riflessione sui significati delle tecnologie digitali, dell'intelligenza artificiale e dei ruoli che assume e/o vogliamo assegnargli.

L'ambito della *cybersecurity* si traduce in una costellazione di temi: la distinzione fra tecnologie aperte, free, protette da copyright, la costruzione collettiva delle conoscenze, l'accesso ai dati, l'identità digitale, la privacy, l'Agenda digitale… Sono temi che sollecitano abilità specifiche e capacità di riflessione che tenga insieme conoscenze complesse.

Se, da un lato, sono sempre più necessarie competenze specifiche, e quindi specialisti, per creare sistemi informatici che funzionino in modo da "proteggere" il cyber spazio, dall'altro è importante che i concetti chiave alla base di tale competenze possano essere condivisi in modo generativo con l'insieme della popolazione, in modo da migliorare rapidamente il grado di consapevolezza e il tipo di atteggiamenti utili a prevenire inconvenienti e minacce in rete.

In questa prospettiva, il tema della data security ha un ruolo chiave nell'identificare le principali aree legate ai rischi in ambito digitale e legati ad Internet. È un tema che richiede, in particolare, percorsi di formazione esperienziale che mettano in grado tutti i cittadini di identificare con facilità tali aree sia in relazione ai comportamenti quotidiani, sia nell'ambito di attività specifiche (dagli acquisti, alle prenotazioni e registrazioni), sia nell'ambito di comportamenti saltuari.

In questo ambito è tanto più importante pensare in modo sistemico ed evitare, per esempio, di tradurre in modo semplicistico l'idea del dato "sicuro" in dato "chiuso". La storia di Salvatore Iaconesi e Oriana Persico, la sua compagna, è emblematica. Iaconesi prese la decisione di interpretare il suo cancro al cervello come un'occasione per umanizzare la figura del paziente: rese tutto il materiale clinico che lo riguardava disponibile in forma open source. Come ha fatto? I dati clinici prodotti e "chiusi" in file dicom, formato leggibile solamente dai software ospedalieri, sono stati "hackerati" e convertito da Iaconesi in file html e jpg per poi venire condivisi con la comunità online che ha risposto al suo invito per fare della cura della malattia non anche un processo creativo, artistico e spirituale. Queste esperienze positive ci ricordano che anche a livello europeo ed internazionale incontriamo programmi significativi che investono nella capacità delle arti di sollecitare i processi della ricerca, dell'industria, della tecnologia e della società, dal programma STARTS della Commissione Europea, a quello riguardo le arti del CERN alle iniziative di Ars Electronica, per citare solo tre esempi.

Coordinato da Yana Toom, il recente "Rapporto del Parlamento Europeo sull'educazione nell'era: sfide, opportunità e lezioni per lo sviluppo delle politiche dell'Unione europea" (2018), nel testo della mozione che verrà presentata al Parlamento, afferma (al punto R) che programmi di insegnamento sulla cybersecurity dovranno essere introdotti nei curricula educativi e della formazione professionale.

Le prospettive formative in questo ambito traggono vantaggio dal partire dai comportamenti quotidiani degli "utenti" digitali e di Internet, ma deve necessariamente anche fare i conti con comportamenti e abitudini inconsapevoli dal punto di vista della sicurezza dei dati: si tratta quindi sia di "costruire" conoscenze, atteggiamenti e comportamenti d'accordo con le esigenze e le aspirazioni degli utenti, sia di "decostruire" conoscenze, atteggiamenti e comportamenti dettati da mancate percezioni o percezioni poco pertinenti riguardo alle situazioni di rischio.

La sperimentazione condotta grazie al progetto 2017-2018 Edu4SEC indica una maggiore efficacia alla proposta formativa sulla sicurezza dei dati digitali quando viene inserita nella più ampia cornice delle capacità legate all'uso di Internet, cioè in merito all'operatività, alle abilità di navigazione, di creazione di contenuti, che riguardano la mobilità ed i contatti e le informazioni sociali e pubbliche. È stato quindi individuato uno strumento di rilevamento di tali competenze già validato a livello europeo che è stato adattato, testato e validato anche a livello italiano per poter integrare gli strumenti di progetto in modo da dare consistenza alla proposta formativa Edu4SEC. Nel sito di <www.dyaloghi.com>[1] viene messo a disposizione il "Questionario sulle competenze online", adattamento validato dell'*Internet Skills Scale (ISS)*.

1 Dyaloghi è uno spin-off dell'Università di Padova nato dalla collaborazione tra gli autori e colleghi e colleghe dell'Università di Padova e altri che operano sul territorio in ambito educativo e formativo. Dyaloghi ha nella propria mission la promozione di una cultura della *data security* nei contesti scolastici e organizzativi e l'allestimento di proposte formative esperienziali su questo e altri ambiti di studio e ricerca in ambito educativo (www.dyaloghi.com).

2.

Cybersecurity: uno stato dell'arte

di *Giuseppe Cascavilla, Mauro Conti*

Cosa è la *cybersecurity*? Perché l'Europa e gli altri paesi impiegano risorse notevoli nel processo di aggiornamento e investimenti continui per garantire una sempre maggiore sicurezza dei nostri dati personali? Cosa è il GDPR di cui tanto si parla negli ultimi mesi e per cui abbiamo ricevuto tante e-mail dai vari siti dove siamo iscritti? L'Italia come sta rispondendo? Queste sono solo alcune delle domande che probabilmente molti di noi si pongono o dovrebbero porsi.

La *cybersecurity* o *sicurezza informatica* è quel ramo dell'informatica che si occupa di analizzare e prevenire le minacce informatiche, di valutare il rischio derivante dall'utilizzo di strumenti informatici, di trovare soluzioni al fine di proteggere i nostri dati da possibili attacchi che potrebbero provocare danni diretti o indiretti. La cybersecurity è dunque qualcosa che deve essere gestita solo da scienziati esperti e disinteressarsene? Decisamente no.

È ora di vedere la *cybersecurity* come un pilastro fondamentale della nostra vita 4.0, digitale, interconnessa in ogni momento e in ogni luogo, sempre più presente nella vita quotidiana di imprese e cittadini. Bisogna prendere consapevolezza che la cybersecurity è fatta di piccoli gesti quotidiani. La sicurezza è data anche dall'uso di password efficaci, sufficientemente complesse da scoprire, ma al tempo stesso abbastanza facili da memorizzare, oppure utilizzare sistemi di memorizzazione automatica. Inoltre, è importante usare password diverse per ogni sito internet in cui ci iscriviamo. Evitiamo di scrivere le nostre password su post-it attaccati al monitor dell'ufficio e lasciati alla mercé di occhi indiscreti. Dopo aver visitato qualsiasi sito internet ricordiamoci di fare sempre il *Log-Out*, così da chiudere completamente la sessione di lavoro. Fare attenzione ai siti web che visitiamo ed alle app che installiamo sui nostri dispositivi mobili. Piccoli accorgimenti quotidiani che possono migliorare di molto la sicurezza dei nostri dati personali ed evitare spiacevoli incidenti.

2.1 Cybersecurity: l'Europa e l'Italia

La cybersecurity e la sicurezza dei nostri dati (data security) però non dipende solo dalle nostre buone o cattive abitudini quotidiane, ma deve essere garantita anche dai vari servizi che utilizziamo online. Ad oggi un grande passo in avanti è stato fatto dall'Unione Europea con una serie di norme e direttive. La direttiva *NIS - Network and Information Security*, il primo passo in ambito cybersecurity che ha l'obiettivo di rafforzare la sicurezza e la resilienza informatica all'interno del vecchio continente. Operatori di servizi essenziali e operatori di servizi digitali dovranno adottare misure tecniche e organizzative adeguate alla gestione dei rischi e alla prevenzione degli incidenti informatici (Tosoni, 2018).

Il *GDPR - General data protection regulation*, è il nuovo regolamento europeo sulla privacy dei dati personali. Le aziende che offrono servizi informatici devono garantire sistemi di protezioni adeguati per i nostri dati personali e privati (Longo & Natale, 2018). La *direttiva 680* è molto simile al GDPR, ma in questo caso il testo prescrive che i dati siano conservati solo per il tempo necessario al conseguimento delle finalità per le quali sono trattati, sottoposti a esame periodico per verificarne l'effettiva necessità di conservazione e cancellati o anonimizzati una volta terminato tale termine (Troiano, 2018). Infine, l'*elDAS*, acronimo di electronic *IDentification, Authentication and trust Services*, è il regolamento europeo che disciplina la firma elettronica, i trasferimenti di denaro e altri tipi di transazioni elettroniche nel mercato unico europeo. Questo regolamento permesso di creare degli standard unici per la nostra firma elettronica e i certificati digitali, consentendo di sostituire documenti cartacei con equivalenti digitali e che hanno lo stesso valore legale e sono riconosciuti ufficialmente in tutti i paesi dell'Unione europea (Arcella, 2017).

E l'Italia? Un'ottima notizia è che non siamo rimasti indietro. Col decreto Gentiloni si è anche l'Italia ha fatto un grande passo avanti in ambito di sicurezza informatica. È stato approvato un programma nazionale per la cybersecurity in più fasi. Il provvedimento ha rafforzato il ruolo del *CISR - Comitato Interministeriale per la Sicurezza della Repubblica* che ha il compito di emanare direttive con l'obiettivo di innalzare il livello della sicurezza informatica in Italia. Si è fondato il *Nucleo Sicurezza Cibernetica* (NSC) che assicurerà una risposta coordinata agli eventi cibernetici per la sicurezza nazionale in collaborazione con tutte le strutture dei ministeri competenti in materia.

Siamo dunque finalmente al sicuro? La risposta è NO. Le minacce informatiche continuano a evolversi, a modificarsi e diventare sempre più insidiose. Resta importantissimo iniziare a prendere coscienza del fatto che dobbiamo diventare parte attiva di questa vita digitale. Dobbiamo imparare a prenderci cura perso-

nalmente della sicurezza dei nostri dati con piccoli gesti quotidiani, supportati da governi e leggi in materia che rafforzino i nostri diritti e le misure di sicurezza.

2.2 Cybersecurity: le minacce

Le elezioni presidenziali negli Stati Uniti d'America del novembre 2016 hanno dato il via ad un ampio dibattito sulla cybersecurity. La possibilità che hacker russi siano riusciti a pilotare le elezioni sottraendo documenti riservati e password di account e-mail private del Partito Democratico è ancora fonte di discussione e ad oggi sono ancora in corso indagini e accertamenti. Sembra fantascienza, e probabilmente qualcuno si domanderà se è realmente possibile manipolare il voto degli elettori o addirittura il pensiero dell'elettore attraverso tecniche di hacking. La risposta è sì, è effettivamente possibile *influenzare* il pensiero di una persona. La tecnica usata è quella delle *fake news.* Pubblicando e-mail personali imbarazzanti o focalizzando l'attenzione dei votanti su alcuni topic sensibili quali la razza o i diritti LGBTQ è possibile influenzare il pensiero di una persona. Un altro metodo per manipolare il voto è fondamentalmente quello di *hackerare* le macchine e i computer che registrano i dati e dunque modificarli.

2.3 Quali minacce informatiche aspettarsi per i prossimi anni?

Le minacce informatiche sono in continua evoluzione e con loro i metodi diventano sempre più subdoli ed efficaci per poter rubare dati personali e privati. Vediamo qui di seguito una breve descrizione delle minacce più comuni.

Fake News. Le recenti statistiche mostrano che il 23% degli italiani ha condiviso in rete notizie poi rivelatesi *fake*, di cui il 12% raramente, l'8% alcune volte e il 3% spesso. Ma chi sono le persone digitali più "credulone"? Tra i più giovani abbiamo ragazzi tra i 25 e 34 anni che hanno considerato per il 63% delle *fake news* vere, di cui il 18% di questi l'ha condivisa. A salire anagraficamente troviamo i 35/44enni. Il 49% ha creduto vere le *fake news* e le hanno condivise il 15% di loro, e ancora tra i 45/54 anni il 52% considera vere le notizie false e il 14% le condivide (Il Sole 24 Ore, 2018). Le *Fake News* nascono in rete e grazie anche ai media nazionali posso avere una diffusione molto più ampia anche tra coloro che non usano la rete.

Ma come possiamo difenderci dalle *Fake News*? I big del web si stanno già dando da fare per arginare il problema. Google ha implementato il tag *Fact*

Check proprio per segnalare che la notizia è verificata (si veda il link https://developers.google.com/search/docs/data-types/factcheck). Facebook ha implementato nuovi algoritmi per rimuovere automaticamente le *Fake News* (si veda il link https://newsroom.fb.com/news/2018/06/increasing-our-efforts-to-fight-false-news/). Sulla stessa strada anche Twitter e il blocco istantaneo della *Fake News* una volta identificata come falsa. E noi, cosa possiamo fare? Un semplice piccolo sforzo in più: verifichiamo sempre la fonte dell'informazione che stiamo per condividere online.

Ransomware. WannaCry e Petya sono stati solamente un assaggio di quello che un attacco ransomware può generare. I due attacchi hacker hanno colpito centinaia di migliaia di aziende, privati cittadini e università e hanno prodotto danni per diversi milioni di euro. Questi ransomware, sfruttando una vulnerabilità dei sistemi Windows, bloccano, criptano e rinominano con l'estensione WCRY tutti i file del PC della vittima e infine richiedono un riscatto in bitcoin per poter rilasciare la chiave di decifratura dei dati. L'unica protezione possibile per questo tipo di attacchi è mantenere il PC regolarmente aggiornato e fare un backup dei nostri dati su hard disk esterni.

Phishing. Il phishing è un tipo di truffa che mira a raccogliere le informazioni degli utenti attraverso e-mail "particolari" o e-mail truffa. Solitamente gli attacchi phishing vengono effettuati attraverso l'invio di messaggi di posta elettronica che si spacciano per servizi autorevoli come la Posta, le Banche o i Ministeri. Gli hacker riescono a ricostruire il form e la grafica utilizzata da questi enti e inviano e-mail truffaldine che un utente poco attento non riesce a riconoscere. In questo modo l'utente ignaro fornisce ai pirati informatici i propri dati personali, come il numero di conto corrente o la password per entrare su Facebook. Per difenderci da questo tipo di truffa l'unica soluzione possibile è mantenere un livello di attenzione *alto*. Controlliamo sempre che il mittente della e-mail sia verificato e ben riconoscibile, leggiamo con attenzione cosa ci viene richiesto nella mail (nessun ente come Poste Italiane o la nostra Banca ci chiederà mai di condividere password o codici tramite mail), infine, se non siamo convinti della mail, segniamola come *SPAM*, così che il sistema provvederà a non recapitarci ulteriori e-mail dallo stesso mittente.

Il Furto di Identità. Per i cyber ladri, le informazioni personali valgono oro: nome, indirizzo mail, numero di telefono, password consentono ai truffatori di creare gravi danni al nostro conto in banca, alle nostre cartelle cliniche, alla nostra assicurazione sanitaria e persino alle prospettive di lavoro. Cos'è il furto d'identità?

Il cyber ladro, ruba il numero della carta d'identità, del bancomat, della carta di credito, della tessera telefonica, etc., per commettere frodi. L'obiettivo, dunque, è quello di ottenere indebitamente le informazioni personali di un soggetto al fine di sostituirsi in tutto o in parte allo stesso e compiere azioni illecite in suo nome. Azioni che possono spaziare dall'ottenere credito in banca al compiere azioni illecite online o al compromettere la reputazione della vittima. Cosa possiamo fare e come possiamo difenderci, dunque? Utilizziamo password complesse, limitiamo ciò che condividiamo online, facciamo attenzione quando si forniscono le informazioni personali, controlliamo periodicamente il nostro estratto conto e i nostri movimenti bancari.

Download di materiale pirata. Il 90\% dei siti pirati più famosi è pieno di link a malware o software indesiderati; più del 60\% di questi link mette gli utenti a rischio di truffe *scam*. Il mondo della pirateria non è un ambiente sicuro per i computer e i suoi utenti. Non bisogna illudersi: la gratuità dei contenuti illegali ha un prezzo che non tutti possono permettersi, come ad esempio minare la nostra sicurezza. I pericoli, secondo *Intelligent Content Protection*, si possono nascondere nei tasti *download*, *play* o anche in quei link apparentemente innocui che portano a servizi di download manager. Da lì in poi si può anche incappare in *rootkits* e *ransomware*. La cosiddetta categoria dei *Potentially Unwanted Programmes* è vasta e include software più o meno pericolosi. In sintesi, per non rischiare meglio evitare scorciatoie illegali.

Cyberbullismo. Secondo il rapporto Istat sul bullismo tra i giovanissimi, il 5,9% dei giovani denuncia di avere subito atti di cyberbullismo. A farne le spese sono soprattutto le ragazze: 7,1% rispetto al 4,6% dei maschi. Il cyberbullismo è la forma di bullismo attuato attraverso la rete, con l'invio di messaggi offensivi, immagini umilianti diffuse via mail, chat o sui social network. Gli autori, i cosiddetti "bulli" o il cosiddetto "branco", sono persone che la vittima conosce o ha conosciuto spesso a scuola, o nel quartiere dove vive o in un'associazione.

Attraverso offese, minacce o ricatti il bullo inizia un processo di pressione psicologica sulla vittima che porterà la stessa a una perdita graduale di fiducia in sé stesso e a sviluppare stati di ansia e depressione. Ma come possiamo proteggere i nostri ragazzi? I giovani si possono proteggere dal cyberbullismo insegnando loro a trattare i dati privati propri e altrui in modo critico e con la massima sensibilità. Chiunque fornisca indicazioni personali o pubblichi immagini su blog, reti sociali o forum si rende un potenziale bersaglio. Ci si può proteggere mantenendo sempre un comportamento rispettoso (netiquette) sia dentro che fuori la rete, evitando di postare dati e informazioni sensibili e personali sul proprio profilo (ad

esempio, foto imbarazzanti o troppo discinte). I genitori e le scuole possono sostenere i bambini e i giovani dando loro consigli e discutendo sulle conseguenze dei loro comportamenti in rete, cercando di insegnare il rispetto della protezione dei propri dati personali e sensibili.

Acquisti Online. Negli ultimi tempi il volume degli affari generati dal Web shopping è cresciuto in maniera esponenziale. Tuttavia, in Rete, la piena tutela del consumatore appare difficile da raggiungere, soprattutto se si decide di comprare all'estero dove vige una normativa differente. Ma quali possono essere le minacce derivanti dallo shopping online dove spesso troviamo offerte "incredibili"? Potrebbe suonarci strano, ma il detto *non è tutto oro quel che luccica* è una esatta definizione dello shopping online. I pericoli a cui ci esponiamo sono molteplici e diversi. Entrando nello specifico possiamo trovarci ad acquistare *merci contraffatte*. Merci che vengono vendute come originale e a prezzi super convenienti, ma per poi risultare di scarsissima qualità. Il problema della *clonazione della carta di credito* utilizzando siti fasulli con merce che non verrà mai spedita. Come non ricordare la truffa sugli occhiali Ray-Ban venduti a poco prezzo e dove l'unico scopo era quello di rubare i codici dei padroni delle carte di credito ignari della truffa. Gli store stranieri con merce con prezzi molto vantaggiosi. Prestiamo attenzione agli store stranieri in quanto ci si potrebbe trovare di fronte a problemi relativi alla garanzia sui prodotti (non tutte le nazioni offrono gli stessi periodi di copertura) oppure semplicemente tempi molto lunghi per la consegna della merce. In alcuni casi, se ci affidiamo a store cinesi, potrebbe capitare che il nostro pacco venga bloccato in dogana in quanto non conforme ai criteri di sicurezza. Il periodo per il *recesso del prodotto*. Controlliamo sempre che lo store al quale stiamo affidando i nostri acquisti, permetta di restituire il prodotto acquistato nel caso in cui non ci soddisfi (è un diritto dell'acquirente). Le recensioni, inoltre, sono un ottimo strumento per capire quali sono stati i problemi riscontrati da altri acquirenti prima di noi. Quali sono i punti di forza e l'affidabilità del sito. E permettono di farci un'idea più generale sul prodotto che stiamo acquistando. In questo caso, un ottimo strumento è il sito internet *TrustPilot* (https://-business.trustpilot.com/). Inserendo il sito internet dello store dove stiamo acquistando i nostri prodotti, TrustPilot ci darà un'idea generale dell'affidabilità del sito basandosi sui commenti lasciati da acquirenti precedenti.

3.

Il progetto Edu4Sec. Effective Education for Improving Data Security Awareness: una proposta di attività formative per la scuola secondaria di secondo grado

di *Daniela Frison*

3.1 Data Security: un costrutto non solo tecnologico

Promuovere la *data security,* educando alla consapevolezza circa i rischi che si possono correre in rete: questo è l'obiettivo del progetto *Edu4Sec – Effective Education for Improving Data Security Awareness*. Come raggiungerlo? Come educare bambini, ragazzi, adulti alla percezione del rischio? Come invitarli a porvi attenzione? A riconoscerlo? In particolare, quando sono gli strumenti che quotidianamente maneggiano per comunicare, giocare, relazionarsi con i pari, fare acquisti, ad essere portatori di questo rischio.

La cosiddetta *data security* può essere definita come quel ramo dell'informatica che si occupa della protezione dei dati sensibili, personali o aziendali, attraverso lo sviluppo di strategie e strumenti per la rilevazione di minacce informatiche o accessi non autorizzati. Negli ultimi anni molti sforzi sono stati compiuti nella direzione di comprendere sempre meglio le ragioni e le modalità delle violazioni. Va evidenziato tuttavia, come la *data security* sia stata osservata soprattutto come un problema di natura tecnologica a cui ricercare soluzioni tecnologiche, identificando le vulnerabilità dei sistemi informatici (Ruighaver, Maynard, & Chang, 2007; Waly, Tassabehji, & Kamala, 2012). Ciò motiva la notevole letteratura internazionale che guarda alla *data security* da un punto di vista informatico e le più limitate, ma sempre in aumento, risorse che guardano ad essa da una prospettiva olistica che attribuisce rilevanza alle credenze e ai comportamenti degli utenti (Waly, Tassabehji, & Kamala, 2012). Questo secondo approccio ha spostato l'attenzione dalla "sola" *data security* – intesa in termini di gestione e protezione dei dati digitali – alla *data security awareness*, attribuendo centralità alla

consapevolezza e ancor prima ai comportamenti dei molteplici utenti della rete, riconosciuti come attori protagonisti delle performance di sicurezza (Albrechtsen & Hovden, 2010). In particolare, si è data via via maggiore importanza all'identificazione dei fattori che possono influenzare gli attacchi informatici a scapito di singoli utenti e di organizzazioni, al fine di rintracciare gli elementi centrali di una formazione efficace per incoraggiare *data security awareness*, riconoscendo che "il problema della sicurezza riguarda le persone, non solo le tecnologie" (Waly, Tassabehji, & Kamala 2012, p. 1270). Precisamente, la sicurezza dei cyber-comportamenti riguarda, a livello nazionale, quel 65,3% di persone, dai 6 anni in su, che si sono connesse alla rete negli ultimi 12 mesi, rappresentato per oltre il 92% da 15-24enni, con una crescita significativa anche tra i 55-59enni (dal 62,7% del 2016 al 68,2% del 2017), come evidenzia il *report ISTAT 2017 Cittadini, imprese e nuove tecnologie*. Il report evidenzia inoltre che, in un anno, gli internauti che hanno effettuato acquisti online sono passati dal 50,5% al 53,0%. Secondo dati Eurostat risalenti al 2016, l'82% dei cittadini dell'UE ha utilizzato Internet almeno una volta nei tre mesi precedenti all'indagine e il 79 % lo utilizza regolarmente (almeno una volta a settimana) a casa, al lavoro o altrove (Eurostat, 2018). Volendo dunque puntare il riflettore sugli adolescenti e giovani che utilizzano la rete quotidianamente, come possiamo promuovere consapevolezza rispetto ai rischi che si possono correre in rete? Come possiamo educare e sensibilizzare gli utenti all'uso corretto delle tecnologie informatiche fornendo strumenti per prevenire e ridurre un'eventuale divulgazione involontaria di dati sensibili?

3.2 Il progetto Edu4Sec: incoraggiare una cultura della Data Security

Formare alla *Data Security* e incoraggiare consapevolezza in merito ad essa e alle conseguenze dei propri comportamenti sono gli obiettivi del sopra citato *Progetto Edu4Sec – Effective Education for Improving Data Security Awareness* attivato nel 2016 presso l'Università di Padova a partire dalla collaborazione tra il Dipartimento di Filosofia, Sociologia, Pedagogia e Psicologia Applicata e il Dipartimento di Matematica (Cascavilla, Conti, Frison, & Surian, 2017; Frison & Surian, 2018).

Il progetto ha coinvolto in particolare due tipologie di target: studenti della scuola secondaria di secondo grado e personale di piccole e medie imprese del territorio veneto. Questa pubblicazione si rivolge espressamente al primo gruppo e intende offrire ad insegnanti ed animatori digitali spunti metodologici, tecniche, attività e risorse per sviluppare entro il contesto scolastico scambi di esperienze, informazioni e riflessioni in merito alla *data security*. Le risorse qui proposte ri-

prendono nei confronti degli alunni degli istituti coinvolti, al fine di incoraggiare una cultura della *data security,* Edu4Sec si è proposto i seguenti obiettivi:

- favorire la conoscenza dei rischi che si possono correre in rete;
- favorire e valorizzare la condivisione delle «cyber-esperienze» vissute dagli alunni e l'apprendimento tra pari;
- fornire ai docenti informazioni, materiali e una proposta formativa da sviluppare e replicare in autonomia.

3.3 Edu4Sec: una proposta in-formativa

In questa direzione sono stati progettati e sperimentati con oltre 250 allievi di tre Istituti di secondo grado superiore del territorio padovano, 5 moduli formativi su temi ritenuti centrali in materia di *data security* e al contempo considerati "vicini" all'esperienza quotidiana dei partecipanti[1]:

- *Internet: rischi e pericoli*: quest'area tematica ha inteso evidenziare gli aspetti più oscuri del web, cercando di fornire strumenti essenziali per potersi difendere in rete e viaggiare in tutta sicurezza nel World Wide Web.
- *e-Commerce: shopping in sicurezza*: con riferimento ai rischi derivanti dallo shopping online e a come evitare acquisti indesiderati o truffe online. Questo modulo ha voluto offrire strumenti essenziali e di facile utilizzo per poter capire l'affidabilità di un sito di e-commerce e conoscere i diritti dell'acquirente in caso di merce errata, non conforme a quella nel sito o semplicemente indesiderata.
- *Password: la nostra difesa*: con riferimento alle problematiche derivanti dalla scelta di una password inappropriata e poco sicura e i rischi che potrebbero insorgere. Quest'area si è posta l'obiettivo di mostrare quali sono i criteri alla base della scelta di una password che possa essere definita sicura.
- *Smartphone: sono veramente smart?*: Questo modulo ha inteso evidenziare i pericoli derivanti da una tecnologia che, se usata in modo improprio, potrebbe portare a seri pericoli per la persona (Conti et al., 2015), esponendo in maniera chiara e attraverso esempi pratici le minacce derivanti da una app male-

1 Le aree tematiche e i contenuti sono stati definiti e messi a punto dal Dipartimento di Matematica dell'Università di Padova, partner del progetto Edu4Sec, grazie alla collaborazione con il prof. Mauro Conti e il dott. Giuseppe Cascavilla.

vola o da un utilizzo improprio dello smartphone seguite dai possibili rimedi per evitare eventuali fuoriuscite di informazioni private.
- *Social Network: privacy & security*: con riferimento ad esempi concreti sulle varie problematiche relative alla privacy e alla sicurezza dei propri dati derivanti da un uso incauto dei social networks. Questo ultimo modulo è stato progetto per esplorare ed identificare i comportamenti da seguire nei social network al fine di evitare problemi relativi alla privacy.

Da un punto di vista tecnico e di contenuto, i moduli hanno riproposto e sviluppato le tematiche più attuali e comuni a workshop e percorsi formativi sulla *data security*, che la letteratura scientifica (per lo più focalizzata su percorsi rivolti agli adulti che lavorano nelle organizzazioni) suddivide principalmente in due tipologie: primo, campagne di sensibilizzazione e promozione della consapevolezza dei rischi mediante poster, articoli, sessioni informative e, secondo, vere e proprie sessioni di formazione miranti a fornire ai destinatari un set di informazioni e conoscenze la cui comprensione e acquisizione viene testata al termine del percorso (Korpela, 2015; Wilson & Hash, 2003).

Numerosi sono gli studi e le ricerche volte ad indagare l'efficacia di queste strategie in-formative e alcuni autori hanno cercato di identificare i fattori chiave che possono condurre al fallimento di un programma di formazione: tra questi un limitato coinvolgimento attivo dei partecipanti durante le sessioni formative oltre alla mancanza di materiali appropriati (Bada & Sasse, 2014).

Oltre a questi fattori, sono stati identificati altri due elementi critici particolarmente interessanti dalla prospettiva del progetto Edu4Sec.

Il primo è la mancata definizione di chi siano effettivamente gli utenti a rischio a cui rivolgere le opportunità in-formative: chi sono le persone "giuste" da formare? All'interno di un'organizzazione, ad esempio, al fine di intercettare casi di *phishing,* potrebbe risultare maggiormente proficuo partire con la formazione del personale tecnico-amministrativo più impegnato nel monitoraggio, nella lettura e nella selezione delle e-mail, anziché partire da figure dirigenziali invece più coinvolte in attività di leadership e di relazione e meno presenti di fronte al proprio personal computer. La tempestività nell'individuazione di una mail sospetta è da ritenersi possa essere maggiormente garantita dai primi. Nell'implementazione di un percorso formativo è dunque fondamentale chiedersi *chi* coinvolgere e quali possano essere i *pericoli* a cui il target individuato sia più esposto e i *rischi* che possa maggiormente correre (Korpela, 2015).

Un secondo elemento ritenuto cruciale per la riuscita o al contrario il fallimento di un percorso formativo sulla *data security* è il livello di comprensione e conoscenza da parte di progettisti e formatori di come la sicurezza informatica

possa essere effettivamente appresa dagli utenti finali (Korpela, 2015). Quali sono le strategie, le attività, i materiali più idonei per *facilitare* l'apprendimento? Da un punto di vista metodologico, quali teorie e modelli di apprendimento possono risultare più appropriati a guidare la progettazione di un percorso formativo sulla *data security* per un determinato gruppo target? È implicita in questa domanda una premessa metodologica di estrema importanza: che la cosiddetta strategia *one-size-fits-all* non sia ritenuta la più adatta al design di percorso informativi e tanto meno formativi sulla *data security*. Il progetto Edu4sec, al contrario, si è orientato verso una progettazione sartoriale di percorsi pensati ad hoc per target e secondo obiettivi specifici volti a proporre esperienze di apprendimento il più possibile personalizzate e costruite su misura per i destinatari. Questo volume nasce dunque con la finalità di offrire ad insegnanti, animatori digitali, educatori extrascolastici e tutti coloro che intendano incoraggiare negli adolescenti e nei giovani adulti una riflessione sui cyber-rischi, un menabò da personalizzare e adattare ai contesti d'uso e agli utenti di riferimento.

3.4 Edu4Sec: le premesse metodologiche

Prima di introdurre la sezione dedicata alla presentazione dei metodi e delle tecniche sperimentate nel corso del progetto Edu4Sec e delle loro possibili varianti, è fondamentale illustrare le teorie e i modelli di apprendimento che ne hanno sostenuto la progettazione.

3.4.1 Verso un apprendimento esperienziale

Tra le premesse metodologiche che hanno guidato il design dei moduli Edu4sec vi è il riconoscimento, imprescindibile, del *valore dell'esperienza*. Le tecnologie, i social network e, più in generale, la rete costituiscono, spesso contemporaneamente, oggetto e contesto delle esperienze degli adolescenti. Momenti importanti e tempi rilevanti della loro quotidianità e delle loro esperienze di vita si svolgono *online*. E l'*online* è divenuto ormai un'estensione tutt'altro che *virtuale,* quanto piuttosto *reale*, effettiva e tangibile, dell'*offline*. Calvani parla infatti di una nuova condizione antropologica che vede l'esistenza delle persone svolgersi "in alternanza tra un *real world* e un *e-world* immanente a quello fisico, con continue trasposizioni dall'uno all'altro" (2017, p. 17). Non intendiamo qui entrare nel merito del valore e del contributo pedagogico delle tecnologie e del loro uso nelle istituzioni educative, rimandando per questa riflessione ad altri contributi ad essa specificamente dedicati (Bonaiuti, Calvani, Menichetti, & Vivanet, 2017).

Partiamo dal presupposto che esse pervadono la vita quotidiana[2], fin dalla più tenera età (è immagine ormai sempre più comune l'utilizzo di uno smartphone o di un tablet per mostrare video musicali o cartoni animati a bambini della fascia di età 0-3!) e incidono fortemente sull'organizzazione delle più comuni attività giornaliere (la gestione del tempo e degli impegni, la comunicazione e le relazioni con persone vicine o anche molto lontane, gli acquisti e così via). In questa riorganizzazione della quotidianità, chiunque abbia accesso alla rete per gli scopi più disparati è potenzialmente esposto a dei rischi legati alla perdita di dati personali sensibili o alla loro diffusione inconsapevole. La portata del fenomeno è tale da aver alimentato lo sviluppo delle cosiddette *Cyber Sciences* ossia un insieme di discipline che coinvolgono tecnologie, persone e processi e che sono orientate a stabilire e a promuovere delle "operazioni sicure" in presenza di rischi e pericoli (Sobiesk, et al., 2015). Esse riguardano la creazione, l'analisi e la sperimentazione di sistemi operativi sicuri e lo studio delle strategie mirate a mitigare i rischi includendo aspetti di carattere normativo, politico, legati al fattore umano, alla gestione dei rischi e alla messa in atto di comportamenti etici (Sobiesk, et al., 2015). Se è dunque indubbio, ormai, che una parte importante della nostra quotidianità si svolga nel cyberspazio e siamo piuttosto consapevoli che in esso avvengano interazioni, transazioni e in generale relazioni che si basano e determinano la diffusione di informazioni personali sensibili, non siamo altrettanto consapevoli dei fattori che regolano i nostri comportamenti in rete né di come "funzionino" i pericoli della rete e di come affrontarli. Partono da questo presupposto tutte le sperimentazioni e gli studi che fin dagli anni Novanta si sono occupati di *information security awareness* (Mathieson, 1991) riconoscendo come l'aumento della consapevolezza possa ridurre i cosiddetti *user-related faults* (Swain & Guttman, 1983) e constatando che la sola conoscenza delle linee guida per adottare dei comportamenti "sicuri" in rete non garantisce la sicurezza, poiché spesso gli utenti conoscono le "regole" ma non le applicano (Warman, 1992). Se la conoscenza delle buone norme di comportamento virtuale non è dunque sufficiente a motivare gli utenti ad applicarle e dunque a proteggerli dai cyber-pericoli, cosa può incoraggiarne l'applicazione?

Gli attacchi messi a segno e riportati dai media possono aver fatto leva sull'incapacità degli utenti di riconoscerli e di immaginare quali possano essere le

2 Il sopra citato report Eurostat (2018) ci ricorda che nel 2016 la quota delle famiglie dell'UE-28 con accesso a Internet ha raggiunto l'85 %, con un aumento di 30 punti percentuali rispetto al 2007. Sempre con riferimento all'UE-28, all'inizio del 2016 oltre quattro persone su cinque (82 %), di età compresa tra 16 e 74 anni, utilizzavano Internet.

conseguenze di un intervento pirata, un'incapacità, potremmo dire, di "capirli" e quindi di mettere in atto una serie di azioni di prevenzione e protezione. Da un punto di vista psico-cognitivo, come evidenzia Munari, osservare (e dunque riconoscere!) e capire "sono due processi intimamente e indissolubilmente legati: non osserviamo, anzi, *neppure vediamo ciò che non capiamo*[3]; e simmetricamente, per poter osservare dobbiamo aver capito" (2010, p. 24). Se non conosciamo né comprendiamo le strategie messe in atto da hacker e malintenzionati della rete, non saremo in grado di ri-conoscerle una volta che saremo noi ad esserne coinvolti in prima persona.

Il *valore dell'esperienza*, sopracitato come premessa metodologica del progetto Edu4Sec è da intendersi dunque in una duplice accezione: esperienza come conoscenza acquisita mediante gli eventi di cui siamo già stati protagonisti (e come abbiamo visto gli eventi *online* si alternano a quelli *offline* con assidua frequenza) ed esperienza come sperimentazione attiva, manipolazione e conoscenza diretta di nuovi eventi, concetti, problemi legati alla *data security*. Un primo riferimento metodologico rimanda dunque al modello dell'*apprendimento esperienziale* (Kolb, 1984; Kolb, Boyatzis, & Mainemelis, 1999) che vede il processo di apprendimento realizzarsi attraverso l'azione e la sperimentazione di situazioni di cui il soggetto è attivo protagonista e in cui viene coinvolto da un punto di vista fisico, cognitivo ed emotivo. Noto, soprattutto nell'ambito dell'apprendimento degli adulti, è il cosiddetto *learning circle* tracciato da Kolb (1984) che ha attribuito all'apprendimento esperienziale una forma ciclica che ha inizio con un'esperienza concreta, passando per forme di osservazione riflessiva e concettualizzazione astratta, e giungere infine ad una sperimentazione attiva che nutrendo nuovamente l'esperienza concreta darà il via ad un nuovo ciclo. Gli autori che come Kolb si sono interessati all'apprendimento dall'esperienza[4] si sono ispirati ai precedenti lavori di Piaget, Lewin e Dewey e hanno valorizzato il ruolo dell'esperienza stessa e della riflessione nella creazione e comprensione di idee e concetti a partire dalle osservazioni condotte (Merriam, Caffarella, & Bamgartner, 2007). Da un punto di vista metodologico, questo approccio messo in valore al fine di orientare la progettazione di interventi formativi rivolti agli adulti, offre stimoli interessanti per la progettazione formativa di attività e tecniche da proporsi anche al nostro target ossia gli studenti della scuola secondaria di secondo grado. Non

3 Corsivo dell'autrice.

4 Boud, Walker, Jarvis, ecc. per un approfondimento si rimanda al capitolo dedicato all'apprendimento esperienziale da Francesca Bracci nel suo volume (2017). *L'apprendimento Adulto. Metodologie didattiche ed esperienze trasformative*. Milano: Unicopli.

va dimenticato, infatti, che il *learning by doing* teorizzato e sperimentato da John Dewey tra fine Ottocento e primi del Novecento rimanda proprio ad un apprendimento ottenuto con il fare, un "formarsi nell'azione" mediante "un'interrotto esercizio dell'osservazione, dell'ingegno, dell'immaginazione costruttiva" (1949, p. 5) da proporsi e attuarsi nella scuola.

Incoraggiare *data security awareness* mediante un approccio esperienziale sostiene la proposta di *learning game* o di attività ludico-metaforiche che favoriscano l'"immersione" nel problema, tema o concetto oggetto di lavoro e/o formazione e la sua sperimentazione e manipolazione attiva e che stimolino l'osservazione e riflessione sull'esperienza vissuta mediante domande chiave e stimoli riflessivi, discussioni di gruppo, storytelling secondo le indicazioni metodologiche che seguiranno (Fedeli, 2011, 2012).

3.4.2 Verso un apprendimento situato

Il riferimento ad un *apprendimento esperienziale* si collega fortemente anche ad un *apprendimento situato* (Fabbri, 2007; Lave & Wenger, 1991; Wenger, 1998), che evidenzia la dimensione contestuale dell'apprendimento. Come ha evidenziato Bracci (2017) gli autori che hanno riflettuto sul ruolo dell'esperienza nel processo di apprendimento si sono chiesti non solo che cosa porti ad apprendere dall'esperienza stessa ma anche quale importanza assuma il contesto in cui essa si realizza. Secondo questo approccio, a giocare un ruolo significativo nel processo di apprendimento non sono esclusivamente le esperienze concrete con cui il soggetto si interfaccia ma anche la comunità sociale con cui ed in cui interagisce poiché l'apprendimento è una pratica sociale e non un atto individuale. Sul tema della *data security* appare pertinente stabilire connessioni tra apprendimento ed esperienze che gli studenti sviluppano nella loro vita quotidiana nel gruppo dei pari, in famiglia, a scuola e, in generale, nelle comunità di cui sono parte. Guardare all'apprendimento da questa prospettiva invita a favorire in aula situazioni il più possibile vicine ai contesti quotidiani degli studenti: situazioni "autentiche" non solo in quanto riferite a problemi "reali", ma autentiche nelle relazioni che le caratterizzano, che tengano conto delle situazioni a cui gli allievi prendono parte (Bracci & Romano, 2018). Si ispirano a questo approccio *role play*, casi studio, simulazioni, scenari che riprendano e ripropongano casi di attacchi e violazioni realmente accaduti e riportati dai media, il più possibile vicini all'esperienza quotidiana dei destinatari.

3.4.3 Verso un apprendimento cooperativo

Il terzo approccio preso qui in considerazione rimanda all'*apprendimento cooperativo* e all'*apprendimento tra pari* (Comoglio, 1996; Johnson & Johnson, 1987) una metodologia didattica diffusasi nel contesto americano a partire dagli anni Sessanta del secolo scorso e in quello nazionale dalla fine degli anni Ottanta. Il *Cooperative Learning* si riferisce ad un insieme di principi e tecniche secondo i quali gli studenti dedicano molto del loro tempo in classe al lavoro in piccoli gruppi, di 4-6 persone, ottenendo riconoscimenti, ricompense e voti basati su prestazioni scolastiche di gruppo (Slavin, 1991). Gli studenti sono invitati a lavorare insieme in modo strutturato per migliorare reciprocamente il loro apprendimento. Questo approccio può essere adattato a qualsiasi tipo di compito o, materia, con obiettivi che intersechino l'imparare a relazionarsi e a lavorare in contesti complessi ed eterogenei, come spesso richiesto dalla società e dall'organizzazione del lavoro contemporanea (Comoglio, 1996; Slavin, 1991).

Esperienza, contestualizzazione e cooperazione risultano dunque le tre parole chiave che hanno guidato la progettazione della proposta formativa presentata in questo volume, linea guida per una personalizzazione che insegnanti, educatori e animatori digitali sono invitati a perseguire con riferimento ai loro setting professionali.

4.

Metodi, tecniche e attività per promuovere data security awareness

di *Daniela Frison, Alessio Surian**

Questo capitolo presenta le principali tecniche e attività proposte agli studenti delle scuole secondarie di secondo grado coinvolte nel progetto Edu4Sec. Ad esse ne verranno aggiunte altre, sulla base degli obiettivi di apprendimento che riteniamo possano essere perseguiti in aula e dei metodi che a nostro avviso sono più coerenti con le teorie e i modelli di apprendimento illustrati nel capitolo precedente (apprendimento esperienziale e situato, apprendimento cooperativo e tra pari).

Le strategie qui presentate, in particolare, si baseranno su alcuni elementi chiave che riteniamo vadano incoraggiati e salvaguardati in ciascuna tecnica.

Primo fra tutti, una *partecipazione attiva e concreta* che parte da un approccio alla conoscenza come costruzione: "una conoscenza costruita attivamente e continuamente durante tutto il processo educativo […] d'interazione tra le persone e con diversi oggetti", come evidenzia Ligorio (2003, p. 15). Non apprendiamo dunque per assorbimento, per mera trasmissione di informazioni e di saperi da un esperto ad un novizio, apprendiamo piuttosto mediante processi di interpretazione, di riflessione e di analisi di ciò che incontriamo. La conoscenza emerge dunque dall'interazione con il mondo fisico e sociale e le tecniche qui proposte intendono promuovere un'immersione in casi reali, la simulazione di interazioni con le tecnologie e con i pericoli della rete, l'elaborazione di piste di soluzione e strategie di prevenzione.

* Daniela Frison ha redatto i §§ 4.1 e 4.2; Alessio Surian ha redatto i §§ 4.3 e 4.4.

Perciò, il secondo elemento portante delle tecniche qui presentate è dato da un *approccio induttivo ed esperienziale*, che prenda il via dai casi riportati dai media o vissuti e sperimentati in prima persona dai partecipanti, vicini alle loro esperienze quotidiane per attivare processi di riflessione e di analisi e incoraggiare il processo di *concettualizzazione astratta* messo in evidenza dal ciclo dell'*apprendimento esperienziale* esplorato nel capitolo precedente.

Il terzo elemento enfatizzato dalle tecniche descritte poggia su un approccio alla conoscenza come processo sociale, di partecipazione ed appartenenza ad un gruppo e ad una comunità. L'apprendimento non è né un atto esclusivamente cognitivo, né un atto esclusivamente individuale. Come evidenzia sempre Ligorio (2003), riprendendo l'approccio situato all'apprendimento, teorizzato da Lave e Wenger (1991), "si impara partecipando a varie forme di attività e pratiche culturali" (p. 19). Elementi chiave sono quindi l'attenzione alle dinamiche di gruppo, a come favorire ascolto e collaborazione e, in questa prospettiva, alla *funzione facilitatrice* del docente. Si tratta di far progressivamente crescere nel gruppo la consapevolezza dei contributi individuali e collettivi ad un equilibrio in constante evoluzione fra attenzione per i contenuti ed i compiti formativi e per le relazioni all'interno del gruppo. Farle evolvere positivamente richiede sia un riconoscimento delle specificità dei singoli e delle potenzialità ed esigenze del gruppo, sia la capacità di contribuire con modalità comunicative che privilegino gli aspetti propositivi ed incoraggianti. La dimensione del "riconoscimento" richiede attenzione per le aspirazioni e per le esperienze ed i vissuti quotidiani di chi partecipa ai processi di apprendimento, così come per la possibilità di condividerli e renderli complementari con quelli degli altri partecipanti.

4.1 Obiettivo 1: Costruire un lessico condiviso

Nell'ambito del Progetto Edu4Sec e dei moduli formativi realizzati presso gli istituti scolastici coinvolti, sono stati rilevati dati in merito alle conoscenze, alle abitudini e ai comportamenti adottati in rete dai partecipanti. La sperimentazione ha coinvolto 251 allievi e mediante somministrazione di un questionario autocompilato abbiamo potuto rilevare, ad esempio, che il 42,19% dei partecipanti non conosceva il termine *phishing* e il fenomeno ad esso correlato ("non so cosa sia il *phishing*") prima dell'intervento formativo. È inoltre emerso come molti altri fenomeni legati alla *data security* e ai pericoli che si possono correre in rete (virus e malware ad esempio) non fossero familiari agli studenti coinvolti.

Uno degli obiettivi principali dei moduli formativi è stata dunque la costru-

zione di un lessico condiviso che, primo, valorizzasse le esperienze e le conoscenze precedenti degli allievi e le collocasse entro una cornice di riferimento e di significato e, secondo, avvicinasse i partecipanti a termini specialistici legati alla *data security*. La *data security*, infatti, è caratterizzata da una terminologia di matrice anglofona che pur essendo stata coniata nel settore informatico, è entrata a far parte della quotidianità di un pubblico sempre più vasto ed indifferenziato (organizzazioni e persone che vi operano ma anche privati che si connettono dalle loro abitazioni con i loro device personali) che ne subisce le ricadute in termini di rischi e pericoli concreti pur senza saperli *nominare.* Con l'obiettivo dunque di *dare un nome* a fenomeni che possiamo incontrare nel corso delle nostre navigazioni, presentiamo di seguito una serie di tecniche e attività che possono essere proposte agli studenti.

4.1.1 Glossario: quali sono i termini chiave in materia di *data security*?

Descrizione del metodo/tecnica

Tecnicamente un glossario è una raccolta di vocaboli, generalmente poco noti o non di uso comune, che per questo necessitano di spiegazione. Il glossario li riporta in genere in ordine alfabetico e seguiti dal significato o da altri commenti e osservazioni.

La costruzione di un glossario può risultare utile per rintracciare e chiarire i termini chiave della *data security* e, in particolare, una descrizione delle possibili ricadute concrete nelle nostre attività *online*.

Ad esempio, se parlo di *malware*, che cosa intendo? È sinonimo di virus? Come si può incappare in un *malware* e come invece lo si può evitare? Cosa può accadere al nostro computer e ai nostri dati se ne veniamo colpiti? E così via. L'esplorazione di un termine, del suo significato e la sua traduzione nelle conseguenze reali di cui è portatore, contribuisce a rendere *visibile* un fenomeno prima del tutto sconosciuto, celato dietro termini per lo più anglofoni e di uso specialistico.

Per far sì che la costruzione del glossario enfatizzi gli aspetti metodologici sopra citati, è consigliabile allestirla come un *compito autentico* che, come evidenzia Tessaro (2014) riprendendo i tratti principali messi in luce da Glatthorn (1999), si fonda sull'impostazione costruttivista precedentemente introdotta. I compiti autentici "sono problemi complessi, aperti, che gli studenti affrontano per apprendere ad usare nel reale di vita e di studio le conoscenze, le abilità e le capacità personali, e per dimostrare in tal modo la competenza acquisita" (p. 79). La costruzione del glossario come compito autentico può essere allestita come attività collaborativa, da realizzarsi in gruppo. La classe può essere suddivisa in gruppi di

3-4 alunni e ciascun gruppo può contribuire all'esplorazione e definizione di alcuni termini. Ciascun gruppo contribuirà così alla messa a punto del glossario.

Obiettivi di apprendimento

Mediante questa attività, i partecipanti saranno in grado di:

- Conoscere i termini chiave della *data security* e il relativo significato
- Tradurre i termini chiave e il relativo significato in ricadute concrete che riguardano le comuni attività online
- Trasferire dei termini e dei concetti astratti in rischi e problemi concreti

Svolgimento

Al fine di allestire l'attività come compito autentico, anziché fornire agli allievi un elenco di termini da esplorare e definire, è possibile partire da una lista di casi reali, riportati dai media o dai siti di settore. È preferibile scegliere articoli in cui termini collegati alla *data security* e poco noti siano numerosi. Le tappe di sviluppo dell'attività sono dunque le seguenti:

1. suddividere gli studenti in gruppi di 4/5;
2. proporre a ciascun gruppo una serie di articoli che contengano numerosi termini tecnici. Gli articoli dovranno essere suddivisi per aree tematiche, ad esempio le medesime proposte dal progetto Edu4Sec (*Internet: rischi e pericoli, e-Commerce: shopping in sicurezza, Password: la nostra difesa, Smartphone: sono veramente smart?* e *Social Network: privacy & security*) e ciascun gruppo dovrà occuparsi di un'area;
3. invitare i gruppi ad analizzare gli articoli (4 o 5 per gruppo, in base alla complessità dell'articolo e al numero di termini tecnici riportati) e ad individuare i termini tecnici (20 minuti);
4. invitare i gruppi a riportare ogni termine tecnico in un post-it e ad affiggere i post-it su una parete dedicata. Evidenziare eventuali termini in comune e attribuirli al gruppo più coerente per area tematica evitando così ripetizioni;
5. a questo punto l'attività può essere svolta secondo diverse modalità. Mediante l'uso di cartelloni, ad esempio riportando ogni termine tecnico e il relativo significato in cartoncini formato A5 che poi verranno affissi, oppure può essere svolta online, mediante la risorsa *Glossario* della piattaforma *Moodle*. In tal caso l'attività dovrà essere condotta presso l'aula informatica dell'istituto. Ciò renderà anche più agevole la ricerca di informazioni da parte degli allievi al fine di definire e contestualizzare i termini di loro competenza. Di aiuto, è la condivisione di una griglia da seguire per la definizione dei termini. Ad esempio: Malware. Cos'è? Come agisce e chi colpisce? Cenni storici (quando, come, da chi è stato creato, chi ha attaccato…). Come potrebbe colpire noi

stessi in relazione alle attività che siamo soliti condurre online? Questo ultimo punto favorisce il perseguimento dell'ultimo obiettivo di apprendimento sopra enunciato ossia trasferire dei termini e dei concetti astratti in rischi e problemi concreti. Se l'attività di ricerca viene svolta in aula informatica, può avere una durata di almeno 40 minuti, altrimenti l'attività di ricerca può essere svolta a casa e i termini con le relative definizioni riconsegnati in occasione della lezione successiva;

- per favorire il lavoro di gruppo e la condivisione tra gruppi, è possibile, una volta avvenuta la condivisione in plenaria o effettuata la proiezione del glossario completo, richiedere ad ogni gruppo di analizzare le definizioni elaborate da un altro gruppo e completare/ampliare i punti relativi ai rischi e ai problemi concreti collegati al termine, a partire dai propri casi analizzati.

Materiali necessari

- Casi, articoli specialistici
- Post-it rettangolari, pennarelli, cartelloni, cartoncini o post-it formato A5
- Eventuale disponibilità dell'aula informatica
- Predisposizione della risorsa *Glossario* all'interno della piattaforma *Moodle* dell'istituto

Risorse utili

Si riporta qui l'esempio dell'articolo Valentini, A. (2018). *Cybersecurity: Come difendersi dalle quattro principali minacce informatiche* reperibile al link http://cybersecurity.startupitalia.eu/61347-20180716-cybersecurity-difendersi-dalle-quattro-principali-minacce-informatiche

Di seguito si riportano i link ad alcuni glossari reperibili online a cui ispirarsi:

- il glossario messo a disposizione dal Progetto *Generazioni Connesse* coordinato dal MIUR è reperibile al link https://www.generazioniconnesse.it/site/it/glossario/;
- il glossario messo a disposizione dalla National Initiative for Cybersecurity Careers and Studies (NICCS), US è reperibile al link https://niccs.uscert.gov/glossary;
- il glossario messo a disposizione dalla NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia, è reperibile al link https://ccdcoe.org/cyber-definitions.html.

Al fine di reperire casi da proporre agli studenti, si invita a consultare:

- la rivista ICT Security Magazine alla sezione Notizie al link https://www.ict-securitymagazine.com/argomenti/notizie/;

4.1.2 La mappa delle parole chiave in materia di *data security*

Descrizione del metodo/tecnica

Una variante del glossario prevede l'identificazione dei termini chiave e la loro collocazione all'interno di una *mappa concettuale* (Cañas, et al., 2003; Novak, 1990; Novak, 2001; Novak, Bob Gowin, & Johansen, 1983). La mappa concettuale è una rappresentazione visiva e grafica che raffigura relazioni tra fatti, termini e concetti e che viene proposta in ambito educativo e formativo per supportare il processo di apprendimento. La sua elaborazione consente infatti di organizzare le informazioni e puntare l'attenzione non tanto sui singoli elementi quanto più sulle relazioni tra essi, incoraggiando un'attribuzione di senso più complessiva ed un approccio reticolare alle conoscenze. La mappa concettuale, ideata nel 1972 da Novak e dal suo gruppo di ricerca presso la Cornell University (US) è ormai uno strumento piuttosto noto e diffuso presso le scuole di ogni ordine e grado. Tuttavia, tale strumento viene spesso adottato e suggerito agli allievi per favorire l'organizzazione delle conoscenze nello studio individuale (ad es. per mettere a fuoco gli elementi salienti di un capitolo o di una unità di apprendimento o di un'area tematica e così via). In questo caso si intende adottare la mappa concettuale a supporto di un'attività di gruppo. Le ricadute positive di un uso collaborativo delle mappe concettuali sono state messe in evidenza da numerosi studi, come sottolineano Cañas e colleghi (2003). L'elaborazione collettiva delle mappe promuove infatti il dibattito, il confronto e i processi di interrogazione a partire da una maggiore interazione tra gli studenti (Cañas et al., 2003). Gli obiettivi di apprendimento rimangono i medesimi del glossario.

Obiettivi di apprendimento

Mediante questa attività, i partecipanti saranno in grado di:

- conoscere i termini chiave della *data security* e il relativo significato;
- tradurre i termini chiave e il relativo significato in ricadute concrete che riguardano le comuni attività online;
- trasferire dei termini e dei concetti astratti in rischi e problemi concreti.

Svolgimento

Rispetto all'attività precedente, che partiva da una suddivisione dei termini per aree tematiche e proseguiva con un approfondimento degli stessi, la costruzione della mappa delle parole chiave procede in direzione opposta. Essa parte dell'esplorazione e successivo approfondimento dei termini per proseguire con la loro organizzazione per aree tematiche (le ramificazioni della mappa concettuale). Il punto di partenza rimane il medesimo e consiste nella distribuzione di una lista di casi reali, riportati dai media o dai siti di settore che contengano preferibilmente numerosi termini tecnici collegati alla *data security*.

Le tappe di sviluppo dell'attività sono dunque le seguenti:

1. suddividere gli studenti in gruppi di 4/5;
2. proporre a ciascun gruppo una serie di articoli che contengano numerosi termini tecnici. Anziché essere rigidamente suddivisi per aree tematiche, come nel caso del glossario, gli articoli, pur coprendo i numerosi ambiti di interesse della *data security*, potranno essere distribuiti in modo meno strutturato, ma non del tutto casuale. Sarà infatti importante che ogni gruppo abbia a disposizione articoli che convergano verso una medesima area tematica rendendo possibile al gruppo la sua individuazione (ad esempio, come detto per il Glossario, le medesime proposte dal progetto Edu4Sec);
3. invitare i gruppi ad analizzare gli articoli (4 o 5 per gruppo, in base alla complessità dell'articolo e al numero di termini tecnici riportati) e ad individuare i termini tecnici (almeno 20 minuti);
4. invitare i gruppi a riportare ogni termine tecnico in un post-it e ad affiggere i post-it su una parete dedicata (una sezione per ciascun gruppo). Il gruppo, con il supporto del docente che ricoprirà il ruolo di facilitatore, potrà manipolare i post-it e riflettere sui termini chiave al fine di individuare le aree tematiche di riferimento. I post-it che rimarranno esclusi dalle aree tematiche rintracciate potranno essere affissi nelle sessioni di altri gruppi (che avranno dunque esplorato altre aree tematiche). In questo modo ciascun gruppo dovrà interagire con il lavoro degli altri gruppi;
5. pur essendo disponili in rete numerosi software che consentono gratuitamente l'elaborazione di mappe digitali graficamente curate[1], riteniamo che in questo caso sia preferibile l'elaborazione di una mappa cartacea. Se gli spazi lo con-

1 Ad esempio: *Coggle, Imindq, FreeMind, MindMapple, Text2mindmap* e molti altri accessibili gratuitamente, alcuni dei quali possono essere usati anche in forma collaborativa ossia unendo il lavoro di soggetti multipli che contribuiscono online a sviluppare i nodi della mappa (una mappa in modalità wiki dunque, con riferimento ad un contenuto digitale scritto in forma collaborativa da una comunità di utenti).

sentono, la mappa potrà essere di grandi dimensioni (pari ad una parete o a parte di essa) e tutti i gruppi potranno alimentare il proprio nodo e affiggere ogni termine tecnico e il relativo significato mediante l'uso di cartoncini formato A5 (o A4, dipende dalle dimensioni). Anche in questo caso sarà utile la condivisione di una griglia da seguire per la definizione dei termini (vedasi esempio riportato con riferimento al Glossario).

Materiali necessari

- Casi, articoli specialistici
- Post-it rettangolari, pennarelli, cartelloni, scotch, cartoncini o post-it formato A5
- Eventuale disponibilità dell'aula informatica

Risorse utili

Si rinvia alle risorse indicate al paragrafo precedente.

4.1.3 *Diamond Ranking*: quali sono i *cyber attack* più diffusi?

Descrizione del metodo/tecnica

La Diamond Ranking (letteralmente, ordinamento a diamante) (d'ora in avanti DR) è una tecnica che può essere proposta per l'analisi di concetti, parole chiave, problemi legati alla *data security* e per favorire la discussione e il confronto al fine di stabilire un ordinamento di questi concetti sulla base di un criterio classificatore (ad esempio, la frequenza degli attacchi o il livello di pericolo, ecc.).

Obiettivi di apprendimento

Mediante questa attività, i partecipanti saranno in grado di:

- Conoscere la terminologia relativa a determinate aree tematiche inerenti la *data security* (ad es. rischi e pericoli relativi ai social network, al commercio online, ecc.).
- Formulare ipotesi di ordinamento sulla base criterio di classificazione (livello di frequenza, probabilità di essere colpiti, livello di pericolo, ecc.)
- Collegare i pericoli e i rischi alle proprie esperienze quotidiane

Svolgimento

La DR può essere utilizzata in due modi:

- Come tecnica di esplorazione di concetti/termini nuovi e/o complessi
- Come tecnica per favorire il *brainstorming* a partire dalle proprie conoscenze pregresse

Nel primo caso, come tecnica di esplorazione di concetti/termini nuovi e/o complessi, può essere proposta come segue:

1. suddividere gli studenti in gruppi di 4/5;
2. fornire a ciascun gruppo una domanda chiara collegata ai rischi e ai pericoli che si possono correre in rete. Ad. es. Quali sono a vostro avviso i cyber attack più diffusi?
   Quali sono i pericoli a cui possiamo essere esposti quando acquistiamo online?
   Quali sono i rischi che possiamo correre quando utilizziamo i social network?
   Coerentemente con la domanda, fornire 9 elementi da classificare (ad esempio, per la prima domanda proporre un elenco di tipologie di minacce e attacchi online) invitando i membri a discuterne e a stabilire un ranking di gruppo (10 minuti);
3. richiedere la condivisione in plenaria e favorire il confronto tra le diverse classificazioni (ad es. capita che un rischio ritenuto molto alto da un gruppo possa essere ritenuto invece molto baso da un altro gruppo, a partire da questi casi è possibile stimolare ulteriormente il confronto e indagare le *premesse implicite* che hanno guidato le scelte dei gruppi);
4. mostrare una classificazione ufficiale a partire da una statistica aggiornata, un articolo, un sito o una rivista di settore.

Nel secondo caso, come tecnica per favorire il *brainstorming*, può essere proposta come segue:

1. suddividere gli studenti in gruppi di 4/5;
2. proporre una domanda chiara e che stimoli la riflessione e la connessione con le esperienze che essi possono già aver vissuto;
3. incoraggiare il *brainstorming* e favorire la discussione e la condivisione delle idee emergenti nel gruppo (5/7 minuti);
4. distribuire lo schema della DR e chiedere ai partecipanti di decidere quali sono i 9 rischi che intendono inserirvi e classificare da un livello molto alto a un livello molto basso. Osservando lo schema è possibile notare che i livelli sono 6: molto alto, alto, medio, basso, molto basso. Questo passaggio è piuttosto complesso poiché richiede processi di condivisione, negoziazione e presa di decisione (10 minuti);
5. richiedere la condivisione in plenaria e favorire il confronto sui principali rischi/pericoli emersi.
   Questa seconda versione è più complessa e può essere proposta a gruppi che hanno già esplorato precedentemente tematiche relative alla *data security*.

Variante: è possibile far lavorare i gruppi tutti su uno stesso problema da classificare e quindi a partire dalla medesima domanda oppure fornire 4-5 temi differenti (ad esempio, i pericoli più probabili che si possono correre in riferimento ai 5 moduli proposti dal progetto Edu4Sec e precedentemente descritti).

Materiali necessari

Sia per la versione 1) che per la versione 2) è necessario 1 schema DR per ciascun gruppo, da riprodurre in formato A3. Online è possibile trovarne diverse versioni solo da stampare (Figura 1).

Per la versione 1) è necessario predisporre 9 cartoncini (delle stesse dimensioni dei riquadri della DR) contenenti i 9 rischi che il gruppo dovrà collocare nella posizione desiderata.

Si riportano qui alcuni esempi:

Acquisti online: Quali sono i rischi più diffusi?

Livello di rischio (1, 2, 3, 4, 5) e nome del rischio:
1 Recensioni fake
2 Applicazione di costi aggiuntivi
2 Merci contraffatte
3 Mancata consegna
3 Phishing
3 Pharming
4 Furto d'identità
4 Sniffing
5 Vishing

Descrizione dei rischi:

- Recensioni fake
- Applicazione di costi aggiuntivi
- Merci contraffatte
- Mancata consegna della merce acquistata
- *Phishing*: storpiatura della parola inglese che significa "pescare". Strategia che si avvale di un messaggio e-mail in apparenza proveniente da un istituto di credito o da una società che fornisce servizi online mirato a pescare, per l'appunto, i dati d'accesso dei riceventi che, rispondendo al messaggio e seguendone le istruzioni, inseriscono i loro dati in un sito fittizio.
- *Pharming*: è una ulteriore tecnica fraudolenta che sempre più spesso si sta ac-

compagnando al *phishing*. La truffa consiste nel realizzare pagine web identiche a siti noti già esistenti (banche, assicurazioni, poste, ecc.) in modo che l'utente sia convinto di trovarsi, ad esempio, nel sito della propria banca e indotto a compiere le ordinarie transazioni sul proprio conto. Una volta digitate le credenziali di accesso esse potranno essere recuperate e utilizzate a fini fraudolenti.

Furto d'identità

- *Sniffing*: è così chiamata l'attività di intercettazione passiva dei dati che transitano in una rete telematica per intercettare informazioni sensibili come le credenziali di accesso ad un determinato servizio.
- *Vishing*: è l'ultima evoluzione del *phishing* legato all'utilizzo del Voip, ovvero le telefonate via internet.

Fonte: https://www.ecc-netitalia.it.

Password: Quali sono gli errori più diffusi?
Livello di errore (1, 2, 3, 4, 5) e nome dell'errore:
1 Dimenticare di inserire caratteri speciali
2 Scarsa frequenza di aggiornamento
2 Password fra loro uguali o simili
3 Basso numero di caratteri nella password
3 Lasciare le proprie password scritte
3 Utilizzare dati personali
4 Usare una parola del dizionario
4 Permettere ai siti che memorizzino le password
5 Usare terminologia Hacker

Descrizione degli errori:

- Dimenticare di inserire caratteri speciali: I caratteri speciali sono fondamentali per generare delle password sicure, poiché rendono molto più lenta l'individuazione della password da parte di hacker.
- Scarsa frequenza di aggiornamento
- Password fra loro uguali o simili
- Basso numero di caratteri nella password: Maggiore è il numero di caratteri della password, specie se alfanumerici e includendo anche i caratteri speciali, maggiore sarà la sua "forza"; una buona password ha almeno 8 caratteri, meglio se 12 o 16.
- Lasciare le proprie password scritte
- Utilizzare dati personali facilmente rintracciabili

- Utilizzare una parola presente nel dizionario, di uso comune
- Permettere ai siti che memorizzino le password
- Usare terminologia Hacker: molti elenchi usati dai programmi di decodifica delle password, fanno parte della terminologia LEET.

Fonti: https://support.apple.com/it-it/HT201579

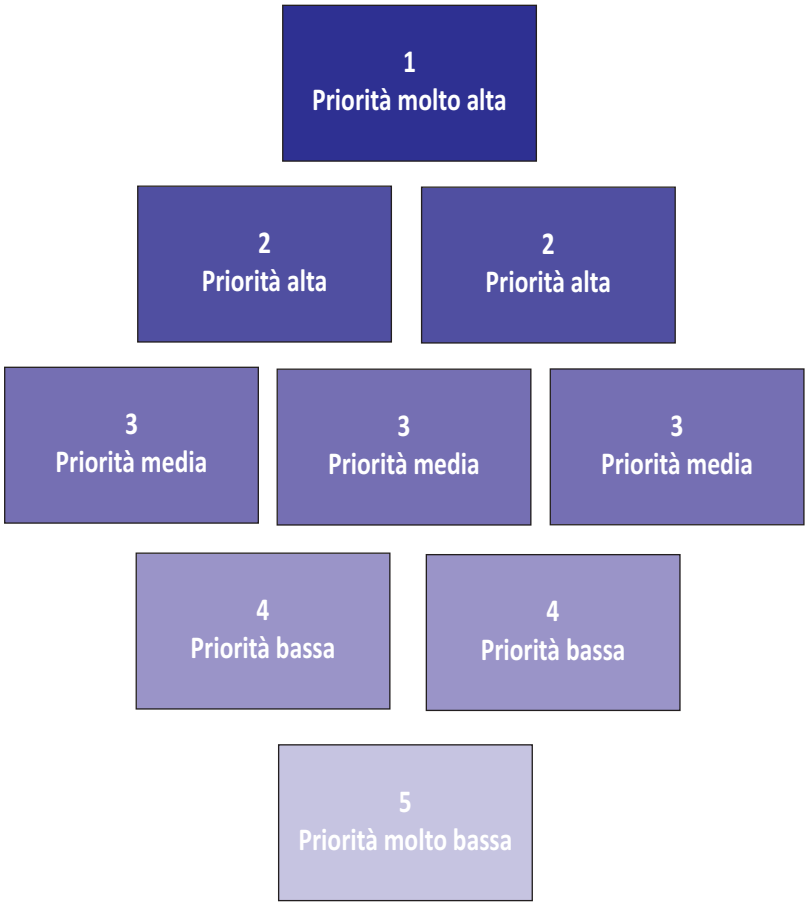


Figura 1 – Diamond Ranking

Risorse utili

Al fine di rintracciare classificazioni ufficiali a partire da statistiche aggiornate, articoli, siti o riviste di settore invitiamo a consultare:

- articoli e documenti messi a disposizione dal Centro Europeo Consumatori e dagli altri Centri Europei della rete ECC-Net per migliorare la tutela dei consumatori nel Mercato Unico Europeo, al link https://www.ecc-netitalia.it/it/ in particolare per quanto riguarda l'area tematica E-commerce al link https://www.ecc-netitalia.it/it/area-tematica/e-commerce;
- articolo e documenti messi a disposizione dal sito della Polizia di Stato, ad esempio http://www.poliziadistato.it/articolo/17734-Rischi_e_pericoli_del_-web_come_difendersi/;
- i report messi a disposizione da IBM Security per quanto riguarda i cyber attack. Il report 2018 è reperibile al link https://www.ibm.com/security/data-breach/threat-intelligence;
- relativamente alla creazione di password "sicure" è possibile consultare i servizi di assistenza di Google https://support.google.com/accounts/answer-/32040?hl=en o di Apple https://support.apple.com/kb/PH25256?viewlocale=en_US&locale=en_U;
- anche i siti di software antivirus offrono interessanti statistiche o indicazioni per la sicurezza in rete. Ad esempio per quanto riguarda i rischi collegati all'uso dello smartphone: https://www.kaspersky.com/resource-center/threats/top-seven-mobile-security-threats-smart-phones-tablets-and-mobile-internet-devices-what-the-future-has-in-store.

Le fonti e le notizie reperibili in rete possono essere innumerevoli e sempre estremamente aggiornate, si invita a porre attenzione all'attendibilità affidandosi a centri di ricerca pubblici o privati o testate online di rilievo.

4.1.4 Il decalogo del cybernauta: consigli per navigare sicuri

Descrizione del metodo/tecnica

L'attività qui presentata può essere proposta a seguito di una delle attività precedenti (in particolare il glossario e la mappa delle parole chiave). Si tratta infatti della definizione di un decalogo di comportamenti da seguire per una navigazione "sicura" che può essere stilato a partire dall'esplorazione dei termini chiave, oltre che dei rischi e pericoli che essi veicolano, promossa dalle attività sopra citate.

Erano gli anni Novanta quando veniva elaborato quello che tuttora rimane il più importante e riconosciuto documento ufficiale sulla *netiquette*, neologismo che

scaturisce dalla fusione dei termini inglesi *net(work)*, rete e *(e)tiquette*, ossia etichetta, galateo, a significare quindi un *galateo della rete*. Il documento RFC 1855[2] del 1995 in cui viene pubblicata in forma definitiva la *netiquette* contiene tutte le regole ufficialmente riconosciute dai cittadini della rete per il suo buon uso. Essa fa esplicito riferimento anche a comportamenti di violazione della sicurezza e della privacy in rete. Con un focus specifico su questi aspetti, quali sono le 10 norme di comportamento da seguire per navigare sicuri? Gli allievi possono definirle e stabilirne una classificazione a partire dagli output del glossario o della mappa delle parole chiave.

Obiettivi di apprendimento

- Tradurre i concetti chiave precedentemente esplorati in comportamenti da agire in rete per navigare "sicuri".

Svolgimento

Le tappe di sviluppo dell'attività sono dunque le seguenti:

1. suddividere gli studenti in gruppi di 4/5;
2. invitare i gruppi a riprendere e analizzare gli output del glossario o della mappa delle parole chiave (5 minuti);
3. invitare ciascun gruppo a tradurre i termini chiave e i relativi rischi e pericoli ad essi connessi in comportamenti da adottare nelle proprie attività online per favorire una navigazione "sicura". I comportamenti devono poi essere trasferiti per ordine di importanza decrescente ne *Il decalogo del Cybernauta: consigli per navigare sicuri*. Anche in questo caso si tratta di un'attività da svolgersi in gruppo che mette in azione abilità di riflessione, negoziazione e problem solving per giungere ad una versione condivisa del decalogo (40 minuti);
4. a questo punto l'attività può essere svolta secondo diverse modalità. Ancora una volta potrà essere previsto l'uso di cartelloni e pennarelli per l'elaborazione di un decalogo cartaceo. Altrimenti, l'attività potrà essere svolta sempre in modalità collaborativa online mediante *Padlet*, un'applicazione gratuita che permette di creare bacheche virtuali condivise tra utenti, molto usata in ambito didattico anche grazie alle sue caratteristiche estremamente *user-friendly*[3] (Frison, Tino, & Fedeli, 2019). Tra i formati offerti da *Padlet* è efficace per la messa a punto del decalogo il formato "serie" che ottimizza i contenuti in un output verticale, da leggere dall'alto verso il basso. Nel caso in cui si decida di proporre l'uso di *Padlet*, l'attività dovrà essere condotta presso l'aula informatica dell'istituto o mediante il supporto di tablet.

2 Reperibile online al link https://tools.ietf.org/html/rfc1855.
3 Altre applicazioni simili a Padlet sono: Linoit, Netboard e Wakelet.

Materiali necessari

- Output delle attività precedenti (glossario o mappa delle parole chiave)
- Cartelloni e pennarelli
  o, in alternativa
- Disponibilità dell'aula informatica
- Predisposizione di un *Padlet* con formato "serie" al link https://padlet.com/

Risorse utili

Si rinvia alle risorse indicate ai paragrafi precedenti.

4.2 Obiettivo 2: Esplorare le rappresentazioni e le pre-conoscenze

Come precedentemente evidenziato, le tecniche e le attività qui proposte sono ispirate ad un modello di *apprendimento induttivo ed esperienziale* che intende valorizzare le pre-conoscenze dei partecipanti e collegare nuove conoscenze ad eventi e fenomeni vicini alle loro esperienze quotidiane per attivare processi di riflessione e di analisi e favorire nuove connessioni. A tal fine, il modulo formativo sulla *data security* può aprirsi con attività e tecniche mirate a rilevare tali preconoscenze o ad esplorare le rappresentazioni e le *premesse implicite* che guidano le abitudini e i comportamenti che i partecipanti agiscono in rete.

4.2.1 *Quiz & clickers*

Descrizione del metodo/tecnica

Il *Piano Nazionale Scuola Digitale*[4] pubblicato dal MIUR nel 2015 sottolinea il contributo della tecnologia per una innovazione della didattica. Viene sottolineato infatti che "l'educazione nell'era digitale non deve porre al centro la tecnologia, ma i nuovi modelli di interazione didattica che la utilizzano" (PNSD, 2015, p. 28) al fine di "passare da una didattica unicamente "trasmissiva" a una didattica attiva, promuovendo ambienti digitali flessibili" (p. 41) attraverso le tecnologie digitali e la rete. Il PNSD è orientato inoltre alla promozione di politiche attive per il BYOD (*Bring Your Own Device*), in collaborazione con le famiglie e gli enti locali, a sostegno dell'utilizzo di dispositivi elettronici personali durante le attività didattiche.

4 Si tratta del documento di indirizzo del Ministero dell'Istruzione, dell'Università e della Ricerca per il lancio di una strategia di innovazione della scuola italiana nonchè documento pilastro de La Buona Scuola (Legge 107/2015).

Si colloca dunque entro questo framework, la proposta in aula di *Student Response System* (SRS) e di *Game-based Student Response System* (GSRS) grazie all'utilizzo degli smartphone degli allievi. A tale proposito, la letteratura presenta numerose esperienze e studi riferiti alla didattica universitaria (Bonaiuti & Ricciu, 2007; Cheong et al., 2013; Poirier, & Feldman, 2007; Ranieri, Bruni, & Raffaghelli, 2018; Wang, 2015) e all'introduzione di elementi di *gamification* per innovarla ossia l'uso di aspetti e dinamiche proprie del gioco in contesti educativi e di apprendimento, non di gioco (Deterding et al., 2011). È ormai piuttosto comune in ambito didattico il riferimento ai *serious games*, termine introdotto da Rejeski nel 2002 con riferimento a giochi progettati e sviluppati secondo obiettivi educativi che incorporano una dinamica pedagogica e formativa nell'esperienza di gioco (Cheong et al., 2013; Stokes, 2005). Meno diffusa, tuttavia, appare la letteratura scientifica riferita all'introduzione di strategie *Bring Your Own Device* e di *Student Response System* nella scuola secondaria di secondo grado nel contesto nazionale, mentre appare più nutrita a livello internazionale (Bruff, 2014).

Nel caso specifico del progetto Edu4Sec gli SRS sono stati proposti in fase di avvio del modulo formativo per indagare le conoscenze pregresse dei partecipanti in materia di *data security*. Precisamente, è stato proposto *Kahoot!*, una piattaforma gratuita basata sulla *gamification* che consente di creare in modo semplice e divertente questionari, test, quiz e verifiche. Nel caso specifico *Kahoot!* è stato adottato per elaborare e proporre un quiz. Grazie ad un'interfaccia gradevole e colorata, alla musica di accompagnamento allo svolgimento dell'attività e alla dinamica di competizione prevista dalla piattaforma, che prevede l'assegnazione di punti in base alle risposte esatte e alla velocità di risposta e la proiezione di una classifica a fine quiz, *Kahoot!* consente di sondare le conoscenze pregresse dei partecipanti in modo divertente e dinamico e di rilevare i concetti che risultano meno noti e vicini alle conoscenze e alle esperienze del gruppo classe. Il risultato del quiz consentirà dunque al docente di comprendere su quali aspetti soffermarsi maggiormente, poiché *Kahoot!* permette di visualizzare immediatamente i risultati per ciascuna risposta evidenziando in rosso le risposte errate e in verde le risposte sbagliate. È dunque di immediata rilevazione il livello di conoscenza del gruppo classe per ciascuna risposta.

Vale qui la pena sottolineare che l'obiettivo dell'attività non è in alcun modo valutativo. Essa piuttosto mira ad introdurre nuovi concetti e problematiche collegate alla *data security*, attivando le preconoscenze degli studenti e favorendo un "aggancio" alle loro esperienze come *cybercitizen.*

Obiettivi di apprendimento

- Riflettere sulle proprie preconoscenze ed esperienze pregresse in materia di *data security*
- Esplorare nuovi concetti/termini/problemi in materia di *data security*

Svolgimento

Le tappe di sviluppo dell'attività sono le seguenti:

1. innanzitutto, è necessario prevedere con anticipo (e verificare o richiedere le necessarie autorizzazioni da parte del Dirigente e delle famiglie) l'uso dei dispositivi da parte degli allievi (modalità BYOD);
2. è possibile proporre un quiz già disponibile online in versione pubblica o elaborarne uno ad hoc. Suggeriamo di non proporre più di 5-6 domande;
3. il quiz verrà proposto in apertura del modulo, secondo una modalità esperienziale ed induttiva, che favorisca l'introduzione di nuovi concetti a partire da una riflessione sulle conoscenze e le esperienze pregresse degli allievi. Una volta lanciato il quiz, i partecipanti vi accedono mediante un codice di accesso (*game pin*) e l'inserimento di un nickname. Proiettate tutte le domande e raccolte le risposte del gruppo classe, il sistema provvede a visualizzarle in un grafico a barre, mettendone in evidenza la frequenza per ciascuna categoria di riposta (è possibile prevedere da un minimo di 2 ad un massimo di 4 opzioni di risposta). Come sopra anticipato, in questa fase, domanda per domanda, il docente ha l'opportunità di commentare i risultati;
4. potrà seguire una sessione frontale di approfondimento dei temi introdotti dalle domande.

Materiali necessari

Per la predisposizione del quiz è necessario connettersi alla pagina "docente" al link https://create.kahoot.it/login.

Risorse utili

Per la formulazione delle domande si può fare riferimento alle risorse precedente indicate o a quelle riportate alla sezione *Risorse Chiave*.

Il quiz *Kahoot!* elaborato nell'ambito del progetto Edu4Sec è pubblico e disponibile al link https://play.kahoot.it/#/k/83656308-0fa2-4c73-8bf8-117d6cc880fc.

4.2.2 Barometro

Descrizione del metodo/tecnica

Un'altra attività che consente di esplorare le esperienze pregresse e le rappresentazioni degli studenti in merito a concetti e problematiche relative alla *data security* è il *barometro*. Una delle difficoltà delle attività di gruppo è, com'è noto, la promozione dello scambio e della partecipazione di tutti i membri oltre che l'avvio di un confronto proficuo e generativo a cui tutti si sentano legittimati a prendere parte, soprattutto quando la tematica sia piuttosto critica e possa assumere risvolti personali. La tecnica del barometro consente una partecipazione *indiretta* alla discussione e può risultare particolarmente proficua per facilitare l'emersione di opinioni e la narrazione di esperienze e per favorirne l'esplicitazione all'interno del gruppo. L'attività prende infatti avvio con una presa di posizione fisica: è attraverso la posizione che il soggetto assume all'interno di uno spazio definito che esprime la propria opinione in merito ad una tematica, anziché esplicitandola a parole, in modo diretto[5]. Si tratta a tutti gli effetti di una versione "fisica" delle domande di grado di accordo o in generale di giudizio e posizionamento con scale continue che possiamo ritrovare all'interno di un questionario.

L'attività, di seguito illustrata più nel dettaglio, può così essere particolarmente efficace:

- in fase di introduzione della tematica, per esplorare le rappresentazioni e le opinioni dei partecipanti in merito al fenomeno indagato e successivamente approfondirlo;
- nel corso delle attività, per favorire un momento di rottura rispetto a quelle precedentemente svolte e "spezzare" una tradizionale dinamica frontale;
  al termine, come opportunità di sintesi.

Obiettivi di apprendimento

- Riflettere sulle proprie preconoscenze ed esperienze pregresse in materia di *data security*
- Esplorare nuovi concetti/termini/problemi in materia di *data security*

5 Per un approfondimento di tecniche di mediazione da proporre nella ricerca e nella formazione si rimanda a Frison, D. (2014). Dialogare con le immagini. L'uso delle immagini nella ricerca e nella formazione esperienziale. In M. Fedeli, L. Frontani, & L. Mengato (a cura di) *Experiential Learning - Metodi, Tecniche e Strumenti per il Debriefing* (pp. 73-86). Milano: Franco Angeli e Frison, D. (2016). L'intervista mediata: evoluzioni dell'intervista cognitivo-critica piagetiana. *Journal of Educational, Cultural and Psychological Studie*s, 13, 191-209.

Svolgimento

Le tappe di sviluppo dell'attività sono le seguenti:

1. Prevedere un tema da introdurre mediante l'attività del barometro, ad esempio *L'uso di Smartphone e Social Network*.
2. Invitare gli studenti ad alzarsi e a schierarsi a seconda del grado di accordo o disaccordo* con la posizione che viene presentata, ad es.:
   - Se non ti mostri sei uno sfigato
   - La reputazione digitale? I millennials sanno come gestirla
   - Smartphone a scuola: meglio vietarlo
   - Quando posto sono consapevole dei rischi che corro
   - Penso sempre prima di postare un contenuto
   - …

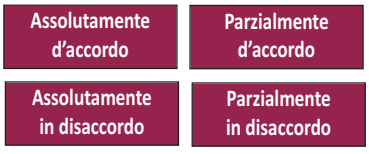
   * **Completamente I in disaccordo** ——————— **I Completamente d'accordo**

3. Variante: anziché chiedere il grado accordo o disaccordo è possibile invitare gli studenti ad alzarsi e a schierarsi posizionandosi fisicamente in uno di 4 angoli dell'aula, che rappresentano diversi gradi di accordo o diverse opzioni di risposta*:
   - Se non ti mostri sei uno sfigato
   - La reputazione digitale? I millennials sanno come gestirla
   - Smartphone a scuola: meglio vietarlo
   - Quando posto sono consapevole dei rischi che corro
   - Penso sempre prima di postare un contenuto
   - …

   ***Opzione a)**

   Opzione b)

4. La presa di posizione nello spazio definito è solo il punto di partenza dell'attività. L'abilità dell'insegnante risiede nell'invitare e sollecitare i partecipanti a motivare la propria posizione e ad esplicitare opinioni ed eventuali esperienze pregresse. Al termine del momento di condivisione e di discussione, è utile in-

vitare gli allievi a riflettere sulla posizione inizialmente scelta e a valutare se intendano modificarla, a partire dalle narrazioni emerse, ad esempio riducendo il loro grado di completo accordo o disaccordo nei confronti dell'item proposto.

5. Potrà seguire una sessione frontale di approfondimento dei temi introdotti dal barometro.

Materiali necessari

Questa tecnica non necessita di particolari materiali.

Risorse utili

Per la formulazione delle domande si può fare riferimento alle risorse precedente indicate o a quelle riportate alla sezione *Risorse Chiave*.

4.2.3 Dibattito

Descrizione del metodo/tecnica

Un'altra attività che consente di esplorare le esperienze pregresse e le rappresentazioni degli studenti in merito a concetti e problematiche relative alla *data security* è il dibattito, "un'interazione dialogica regolata, in cui più interlocutori suddivisi per squadre con punti di vista incompatibili tentano di fare aderire una giuria e il pubblico alla propria posizione coinvolgendoli mediante argomenti" (Cattaneo & De Conti, 2018, p. 56). La letteratura scientifica mette particolarmente in evidenza il valore del dibattito nello sviluppo della competenza verbale e non verbale oltre che come attività che favorisce l'inclusione (Cattaneo & De Conti, 2018; De Conti & Giangrande, 2017). Nel contesto preso qui in considerazione, il dibattito viene proposto ancora una volta come attività introduttiva rispetto all'approfondimento di un'area tematica inerente la *data security*. Esso consente al gruppo classe di prendere coscienza, mediante il processo di esplicitazione, dei possibili risvolti del fenomeno e all'insegnante-moderatore di raccogliere rappresentazioni, eventi, esperienze a cui ancorare il successivo momento di approfondimento frontale.

Obiettivi di apprendimento

- Riflettere sulle proprie preconoscenze ed esperienze pregresse in materia di *data security*
- Esplorare nuovi concetti/termini/problemi in materia di *data security*

Svolgimento

Le tappe di sviluppo dell'attività sono le seguenti:

1. prevedere un tema da introdurre mediante l'attività del dibattito. Riprendiamo qui gli esempi già adottati per l'esplorazione della tematica sviluppata mediante l'attività del barometro: l*'uso di Smartphone e Social Network;*
2. suddividere gli studenti in gruppi di 4-5 e chiedere a due gruppi di dibattere: un gruppo sarà a favore e l'altro sarà contro e dovranno portare le loro argomentazioni a seconda della posizione da sostenere. Di seguito alcuni esempi:
   - Se non ti mostri sei uno sfigato
   - La reputazione digitale? I millennials sanno come gestirla
   - Smartphone a scuola: meglio vietarlo
   - Smartphone alla scuola primaria: assolutamente non regalate uno smartphone a vostro figlio
   - …
3. tempi: circa 5 minuti per dibattito o fino ad esaurimento se il dibattito è molto acceso;
4. potrà seguire una sessione frontale di approfondimento dei temi introdotti dal barometro.

Materiali necessari

Questa tecnica non necessita di particolari materiali.

Risorse utili

Per la formulazione delle domande si può fare riferimento alle risorse precedente indicate o a quelle riportate alla sezione *Risorse Chiave*.

4.2.4 Proposta di questionari pre- e post-intervento

Descrizione del metodo/tecnica

Nel caso del progetto Edu4Sec, ciascun intervento in aula è stato anticipato dalla somministrazione di un questionario auto-compilato da parte degli alunni coinvolti volto a rilevare, ex-ante, conoscenze e abitudini di comportamento in rete. Il medesimo questionario è stato somministrato ex-post, al fine di rilevare nuovamente le conoscenze dei partecipanti sulle tematiche proposte e le intenzioni/previsioni di comportamento a seguito della partecipazione al modulo formativo. I questionari, somministrati mediante *Google Moduli*, hanno proposto sia domande aperte sia domande chiuse a scelta multipla ad una sola risposta o a più risposte, proponendo batterie di domande collegate alle aree tematiche pre-

viste: *Io e le Password, Io e Facebook, Io e i Social, Io e Internet, Io e le app, Io e gli acquisti online*.

Obiettivi di apprendimento

- Riflettere sulle proprie preconoscenze ed esperienze pregresse in materia di *data security*
- Esplorare nuovi concetti/termini/problemi in materia di *data security*

Materiali necessari

- Disponibilità dell'aula informatica
- I questionari pre- e post-intervento elaborati nell'ambito del progetto Edu4Sec sono disponibili in appendice. Gli autori, previo contatto, ne mettono a disposizione la versione compilabile online mediante Google Moduli. I dati rilevati vengono raccolti e analizzati dagli autori del presente volume che si impegnano a condividerli, in forma anonima e aggregata, con i docenti di riferimento degli istituti e delle classi coinvolte nella somministrazione.

4.3 Obiettivo 3: Esplorare e condividere le esperienze pregresse

Le seguenti attività sono pensate per sollecitare, nei percorsi formativi sulla data security, ambienti favorevoli allo scambio e alla collaborazione che permettano ai partecipanti di riconoscersi al contempo diversi, vulnerabili, capaci, creativi. Si tratta di tecniche mirate a valorizzare la dimensione individuale della memoria, aiutando l'introspezione e la riflessione anche in funzione di una condivisione fra pari delle proprie esperienze all'interno di un clima di rispetto, ascolto attivo, basi per poter dar vita a processi di interazione, scambio e co-costruzione di idee e proposte.

4.3.1 Storytelling di Gruppo

Descrizione del metodo/tecnica

Questa modalità di lavoro favorisce l'attenzione per l'esperienza e la narrazione incoraggiando l'ascolto reciproco nel rievocare eventi dei percorsi individuali sui cui riflettere collettivamente. Si tratta di fornire alcuni elementi di riferimento che diano la possibilità di strutturare le proprie narrazioni in modo accessibile anche al resto del gruppo.

Obiettivi di apprendimento

Esercitare pensiero narrativo, introspezione e feedback in funzione dello sviluppo di pensiero analitico e critico sui nostri comportamenti in ambito digitale.

Svolgimento

I partecipanti vengono invitati a condividere una o più esperienze personali che permettano di esplorare e ripensare i propri comportamenti in ambito digitale. Per ricordare le esperienze in chiave narrativa vengono suggeriti i seguenti cinque passi.

Condividere storie in cinque passi:

1. Create un ambiente di ascolto e fiducia reciproca. Per narrare è utile pensare a chi ci ascolta, che cosa possa rendere interessante e accessibile agli altri quanto abbiamo da dire. In un gruppo che si conosce poco, è utile una fase di mutua presentazione. In un gruppo che già si conosce può essere utile chiarire, dando spazio ad ogni partecipante, che non c'è un solo modo di rapportarsi con il mondo digitale e vale la pena, soprattutto ad inizio percorso, ascoltare quali mezzi, modalità e tempi caratterizzino l'esperienza di ciascuna persona. Possono tornare utili brevi esercizi per favorire l'ascolto reciproco.
2. Introducete un ragionamento sull'opportunità se sia il caso che ogni partecipante o solo alcuni si offrano di condividere le proprie narrazioni e se queste vadano preparate individualmente o in gruppi di lavoro. I motivi per preparare solo alcune storie possono essere legati ai tempi, quando non consentono una completa circolarità, o ad un consenso nel gruppo che sia opportuno ascoltare solo chi sente di avere già qualcosa da raccontare.
3. Sollecitate una riflessione su come raccontare. Offrite a titolo di esempio alcuni elementi narrativi che possano rendere le storie interessanti e rilevanti per quante più persone possibile. Per esempio: Chiarire qual è il tema/problema chiave della narrazione in modo da focalizzare attenzione e commenti su questo aspetto "centrale" e magari trovare un titolo che generi aspettative adeguate. Rendere la storia interessante provando a cercare un inizio, un momento centrale e un finale (che può anche essere aperto/interrogativo) che richiamino l'attenzione e scandiscano i tempi della narrazione. Come in un testo teatrale, provate a chiarire elementi di contesto utili e chi siano i personaggi chiave e chi sia a creare problemi e chi abbia le potenzialità/capacità per risolverli.
4. Incoraggiate i partecipanti a prendersi cura dello spazio e del momento narrativo. Chi facilita/guida gli altri in questo spazio-tempo? Questo riguarda sia il far sentire tutti benvenuti al momento narrativo, sia prestare attenzione alla

motivazione individuale e collettiva a costruire storie, narrare, ascoltare, sia alla consapevolezza di ogni partecipante rispetto alle fasi del processo. Richiede attenzione e rispetto per i tempi (e le possibilità di renderli flessibili) e per il grado di circolarità (contributi da parte di ogni partecipante) che è possibile innescare complessivamente e nelle singole fasi del processo.

5. Aiutate i partecipanti a vedere le narrazioni come processi relazionali in cui è importante offrire commenti, porre domande, esplicitare emozioni e scoperte. È importante saper distinguere tempi e modi di domande e commenti di verifica (che permettono di meglio comprendere la storia mentre viene raccontata) da feedback che restituiscono a chi narra l'impatto che la storia ha avuto su chi l'ha ascoltata. In questa fase è importante lasciare spazio a tutti, non dare per scontato che tutti recepiamo la narrazione nello stesso modo e quindi provare a porgere i propri commenti come vissuti individuali, senza cercare di interpretare senso o sentimenti collettivi. Ed è importante "celebrare" lo sforzo narrativo di chi si è messo in gioco cercando di riconoscerne le qualità.

Materiali necessari

Può essere utile condividere il testo (o una sua versione semplificata) dei Cinque passi.

4.3.2 Think-pair-share

Descrizione del metodo/tecnica

L'attività invita i partecipanti a confrontarsi con problemi su cui produrre una varietà di risposte lavorando a coppie e in piccoli gruppi, favorendo quindi i contributi di ogni persona.

Obiettivi di apprendimento

- Promuovere la collaborazione.
- Promuovere ascolto attivo e pensiero critico attraverso la produzione di idee diverse e la loro condivisione.

Svolgimento

L'attività è strutturata in tre momenti:

1. I partecipanti vengono invitati a formare coppie (*pair*).
2. Alle coppie viene assegnato un problema da risolvere e viene dato un tempo limite per pensarci (*think*), produrre (e possibilmente scrivere) una o più ri-

sposte. Le coppie lavorano sul problema e su come presentare la propria o le proprie risposte.

3. Le risposte vengono condivise (*share*) con gli altri partecipanti.

Variante:

Una tappa intermedia fra il secondo e il terzo momento, chiamata in inglese *Timed-Pair-Square* è quella di cominciare a condividere e ricevere feedback sulle proprie risposte da un'altra coppia. Qualche volta, se il tempo non consente la condivisione in plenaria, l'attività in classe può anche terminare qui.

Materiali necessari

Non è indispensabile alcun materiale, ma può essere utile predisporre lo spazio per agevolare il lavoro a coppie e in piccoli gruppi.

Può essere utile mettere a disposizione fogli e pennarelli per la fase di elaborazione e presentazione delle risposte.

Risorse utili

Possono contribuire a migliorare la partecipazione a questa attività esercizi sull'ascolto attivo e su come fare in modo che entrambe le persone abbiano modo di contribuire al lavoro di analisi del problema, elaborazione delle risposte e loro presentazione.

4.3.3 Role-play di un'esperienza

Descrizione del metodo/tecnica

Si tratta di coinvolgere i partecipanti a dar vita a brevi simulazioni in cui, a gruppi, assumano il ruolo di "attori", a partire da un nucleo narrativo/problematico.

Obiettivi di apprendimento

Sviluppo delle capacità comunicative

Sviluppo dell'ascolto attivo e dell'attenzione per le ragioni degli altri

Svolgimento

In particolare, per approfondire l'uso di smartphone e reti sociali, può essere utile suddividere gli studenti in gruppi di 3/4/5 chiedendo di dar vita a role-play. Quando un gruppo mette in scena la propria narrazione gli altri partecipanti svolgono il ruolo di "osservatori" dei contenuti e dei processi.

Istruzioni per l'uso:

1. *Preparazione*: può essere utile "riscaldare" l'attenzione dei partecipanti informandoli in anticipo dei temi al centro del role-play perché si possano preparare e abbiano tempo per raccogliere ed elaborare informazioni e materiali.
2. *Introduzione e riscaldamento*: all'inizio dell'attività, può aiutare coinvolgere i partecipanti in esercizi di riscaldamento, per esempio condurre brevi interviste, in modo da invogliarli ed avvicinarli ad assumere il ruolo di qualcun altro.
3. *Scelta degli attori*.
4. *Role-play*

   Fase in gruppi: i partecipanti si dividono in piccoli gruppi (di 3-5 persone) e all'interno di questi gruppi vengono loro assegnati (o hanno loro stessi preparato in precedenza) uno scenario problematico che dovranno sviluppare poi di fronte al resto del gruppo e che prevede ruoli diversi e un tempo indicativo (breve) di presentazione.

   Fase in plenaria: i gruppi a turno presentano il proprio role-play; durante le rappresentazioni dei gruppi, se lo si ritiene utile, chi conduce l'attività può intervenire proponendo varianti come l'intervista o l'inversione dei ruoli, per sbloccare o sviluppare le situazioni rappresentate.
5. *Ascolto e riflessione*

   Fase di ascolto: spazio per chi ha osservato (e poi chi ha interpretato il role-play) per condividere emozioni;

   Fase di riflessione: spazio per chi ha osservato (e poi chi ha interpretato il role-play) per commentare, scambiare feed-back e trarre elementi di comprensione rispetto al tema/problema del role-play.

Materiali necessari

Può essere utile fornire ai partecipanti una *lista di temi* che siano da spunto per mettere in scena un episodio (reale o inventato), per esempio:

- Come gestire la reputazione digitale
- L'uso dello smartphone a scuola
- L'uso dello smartphone con gli amici

Può essere utile fornire a ciascun gruppo una breve *scheda* per strutturare il proprio role-play, per esempio:

- Titolo del role-play
- Ruoli
- Breve descrizione
- Tema problematico

4.4 Obiettivo 4: Sperimentare

Le seguenti due proposte formative hanno natura diversa. In entrambi i casi si tratta di momenti formativi "impegnativi" che possono essere programmati nel momento in cui il percorso formativo generale è già a buon punto ed ha costituito un lessico e una modalità sana riguardo alle relazioni interpersonali, oppure all'inizio del percorso nei casi in cui esista già questa fiducia nel gruppo e nel suo potenziale riguardo al misurarsi con sfide complesse.

Nel primo caso si tratta di segnalare l'ambito delle simulazioni, degli scenari, dei serious game come archivi vivi in grado di fornire contesti di sperimentazione ludica su sfide impegnative che caratterizzano le nostre società. Non, quindi, un'attività già confezionata, ma alcune indicazioni su dove reperire materiali utili e come metterli a tema nell'ambito di processi formativi.

Nel secondo caso, si tratta di dar fiducia al gruppo con cui si lavora ed invitarlo a generare idee e proposte su problemi sentiti dal gruppo stesso, innescando processi creativi nel misurarsi con problemi attuali.

4.4.1 Simulazioni

Descrizione del metodo/tecnica

Simulazioni (e giochi basati su scenari) contribuiscono a valorizzare la natura relazionale dell'esperienza umana e a sperimentare e riconoscere elementi chiave di scenari che riteniamo problematici nella nostra vita. In questo spazio si favorisce la consapevolezza del gioco e della simulazione in quanto via metaforica all'apprendimento comprendente sia aspetti cognitivi, sia comportamentali, affettivi e relazionali, verso l'ambiente esterno nel suo complesso e verso il gruppo o i gruppi in cui si è inseriti in maniera specifica. Come per il role-play, il senso educativo dell'esplorare insieme simulazioni e scenari sta nell'abilità del legare questa esperienza ai momenti e processi di ascolto e riflessione (*debriefing*) soprattutto nella parte finale dell'attività.

Obiettivi di apprendimento

- Sviluppo delle capacità comunicative
- Sviluppo delle capacità interpretative
- Sviluppo dell'ascolto attivo e dell'attenzione per le ragioni degli altri

Svolgimento

La costruzione di scenari e i giochi di simulazione hanno in comune il saper disegnare un contesto, ipotizzarne uno sviluppo temporale e l'identificazione di alcuni

attori e variabili chiave. Lo scopo è quello dell'invitare a "mettersi in gioco" di fronte a temi di rilievo per la nostra vita. Scenari e simulazioni ci invitano ad apprendere dall'esperienza diretta all'interno di una realtà semplificata, simbolizzata.

Arnaldo Cecchini definisce il gioco di simulazione (e indirettamente il far evolvere uno scenario) come la valutazione degli effetti di decisioni (*simulation*) prese attraverso l'assunzione di ruoli (*role*), sottoposti a un insieme di regole (cioè a un *game*).

La simulazione richiama le dinamiche teatrali, vuole essere ludica, ma più strutturata del role-play. Può essere realizzata con supporti più o meno strutturati (per esempio attraverso percorsi "guidati" da un mazzo di carte e/o tabelloni predisposti in precedenza). L'articolo di Hendrix, Al-Sherbaz, e Bloom (2016), riportato qui sotto presenta una sintesi della letteratura in inglese su questi temi (in particolare nell'ambito dei "*serious game*" da cui si possono trarre spunti o adattare contesti e scenari simulativi.

Materiali necessari

Scheda: Ascolto, riflessione e *debriefing* in tre fasi

1. Fase 1: la descrizione: al termine dell'attività di scenario o simulazione, tutti i partecipanti, possibilmente disposti in cerchio, sono invitati ad esprimersi e ad ascoltarsi reciprocamente, soprattutto in relazione alle emozioni provate, in un clima di rispetto che evita giudizi e commenti critici.
2. Fase 2: analogia e analisi: collettivamente si cerca di ricostruire gli elementi chiave, l'eventuale modello e le loro implicazioni per le questioni affrontate durante la simulazione e per la nostra vita quotidiana.
3. Fase 3: applicazione: i partecipanti sono incoraggiati ad interrogarsi sui possibile apprendimenti: cosa ho scoperto personalmente? In che modo queste scoperte mi sollecitano a modificare i miei comportamenti?

Risorse utili

Hendrix, M., Al-Sherbaz, A., & Bloom, V. (2016). *Game Based Cyber Security Training: are Serious Games suitable for cyber security training? International Journal of Serious Games, 3*(1), 53-61. DOI: 10.17083/ijsg.v3i1.107

4.4.2 Problem solving di gruppo

Descrizione del metodo/tecnica

Questa attività incoraggia a discutere e trasformare sfide e problemi in gruppo, rispondendo innanzitutto a due temi: quello della collaborazione e quello del sol-

lecitare pensiero creativo e divergente. A differenza del pensiero convergente (la modalità del cercare la risposta più adeguata ad un problema), il pensiero divergente sollecita molteplici soluzioni, ognuna adeguata a modo suo perché prende in considerazione piani di lettura diversi del problema.

Obiettivi di apprendimento

- Favorire la creatività e il pensiero divergente
- Favorire l'ascolto di punti di vista diversi
- Sviluppare la collaborazione fra pari

Svolgimento

Offrire una soluzione di gruppo significa soprattutto mettersi nelle condizioni di poter cambiare punto di vista, cioè essere in grado di vedere le cose da un'altra angolazione per capire e verificare i pro e i contro dei diversi modi per affrontare e trasformare o risolvere un problema. L'idea è quella di incoraggiare una varietà di proposte da parte di tutti i partecipanti nel contesto di un ambiente collaborativo che ispiri a pensare in modo creativo. Come fare? Ecco due esempi:

1. Diciamolo con in post-it (o con Padlet):
   Dopo aver presentato o invitato a presentare un problema, distribuiamo a tutti i presenti post-it su cui scrivere la propria proposta di trasformazione / soluzione del problema.
   Di fatto, si tratta di un brainstorming e quindi il tempo di produzione delle idee va tenuto relativamente contenuto, incoraggiando i partecipanti ad essere creativi.
   I post-it vanno quindi appesi al muro / ad un ampio foglio dove possano essere visionati collettivamente e quindi letti, commentati e raggruppati riflettendo sulle implicazioni di ciascuna proposta.
2. Dimmelo con il role-play:
   Seguendo le indicazioni fornite per il role-play (si veda paragrafo 4.3.3), uno o più gruppi sono invitati a rappresentare la situazione problematica e alcuni possibili scenari che suggeriscano come affrontare la sfida e raccogliere osservazioni e commenti da parte di tutti i partecipanti.
   In entrambi i casi è utile favorire un ambiente che non abbia fretta di identificare la soluzione e che permetta a tutti di esprimersi, di ascoltarsi e di osservare similitudini e divergenze fra le proposte andandone a capire le motivazioni e le implicazioni da diversi punti di vista.

Materiali necessari

Post-it o fogli che sia possibile appendere nel caso del primo esempio.

4.5 Una proposta di micro-progettazione

di *Alessio Surian e Daniela Frison*

A partire dagli input metodologici forniti e dalle attività e tecniche descritte, presentiamo di seguito una proposta di micro-progettazione di moduli formativi della durata di 2 ore, con articolazione di tempi, contenuti, metodo/tecnica/attività e strumenti/materiali necessari per la sua realizzazione, da adattare o rimodulare a seconda del gruppo e delle tempistiche effettive a disposizione.

TEMPI (2 h)	CONTENUTI	METODO / TECNICA / ATTIVITÀ	STRUMENTI / MATERIALI
0-15'	**Breve introduzione e questionario pre-intervento**		Questionario su google moduli Tablet/PC/Smartphone Connessione internet e condivisione del link di accesso al questionario
15'- 45'	**Modulo "Internet: rischi e pericoli"**	Diamond Ranking Activity Mini-lezione	Istruzioni per DR Slide di presentazione
45'-65'	**Modulo "E-commerce: acquisti in sicurezza"**	Mini-Lezione	Slide presentazione[6]
65'-80'	**Modulo "Password: la nostra difesa"**	Quiz Presentazione	Kahoot "Password" Slide presentazione
80'-110'	**Moduli "Smartphone" "Social Network"**	Role-play o Dibattito o Barometro Mini-Lezione	Istruzioni per Role Play, Dibattito o Barometro Slide presentazione
110'-120'	**Conclusioni e questionario post-intervento**		Questionario su google moduli

6 Come per i questionari, anche le presentazioni Edu4Sec possono essere rese disponibili ad animatori digitali e quanti interessati.

5.

Il progetto Edu4Sec: i risultati emersi

di *Daniela Frison, Alessio Surian*

5.1 L'avvio del Progetto Edu4Sec: un'esplorazione delle esperienze d'uso delle tecnologie

I moduli formativi sopra presentati sono stati progettati e proposti ad oltre 250 studenti e studentesse di scuola secondaria di secondo grado. Precisamente, nel corso degli Anni Scolastici 2016/2017 e 2017/2018 sono stati coinvolti nel progetto Edu4Sec tre istituti superiori di secondo grado del territorio di Padova e provincia, raggiungendo 12 classi per un totale di 256 studenti.

Il progetto si è proposto: primo, di allestire un'offerta in-formativa che potesse essere poi replicata, ampliata e personalizzata da altri docenti e istituti scolastici del territorio nazionale, a partire dalla sperimentazione qui descritta e, secondo, di indagare se un approccio "gamificato" ai contenuti proposti potesse favorire l'acquisizione di conoscenze e pratiche di data security.

Considerate le peculiarità del contesto scolastico e l'impossibilità di controllare tutti i fattori che ne caratterizzano la complessità educativa, è stato messo a punto un disegno di ricerca quasi-sperimentale a due gruppi (Campbell & Stanley, 2015; Trinchero, 2002) con identificazione di un gruppo sperimentale (GS) e di un gruppo di controllo (GC) definiti secondo un campionamento di comodo basato sull'identificazione di classi simili per anno e tipologia (tradizionale o digitale). L'adozione di un campione di comodo ha consentito la realizzazione degli interventi nel rispetto delle tempistiche riconosciute come più opportune dagli animatori digitali.

Prima di mettere a punto e condurre le attività nelle classi e finalizzare la micro-progettazione precedentemente illustrata, sono stati condotti 3 focus-group preliminari, al fine di esplorare le abitudini di comportamento ed eventuali nodi critici relativi all'uso delle tecnologie da parte degli studenti e allestire su

tale quadro di riferimento la progettazione di dettaglio degli interventi. Il focus-group ha così facilitato l'emersione dei temi più vicini agli studenti in materia di *data security*.

Sono stati realizzati e co-condotti 3 focus group della durata media di 100 minuti. Gli incontri hanno coinvolto 3 gruppi di studenti e studentesse, per un totale di 39 soggetti delle classi III e IV sempre digitali e tradizionali.

Gli incontri[1] hanno inteso esplorare le tematiche successivamente declinate e approfondite nei moduli formativi:

- le esperienze d'uso delle tecnologie, sia in ambito scolastico che extrascolastico;
- la gestione della *privacy* nella condivisione delle informazioni sui social network (abitudini e motivazioni);
- gli acquisti online e le modalità di pagamento adottate;
- la creazione e la gestione delle password (modalità e abitudini);
- l'utilizzo della e-mail;
- l'utilizzo delle reti Wi-Fi pubbliche;
- più in generale, comportamenti e situazioni critiche vissute in rete.

Dalla prima esplorazione mediante i focus group, è emerso che *i dispositivi più utilizzati* dai gruppi coinvolti sono: il tablet (25), seguito dal pc (22) e, infine, dallo smartphone (30). Smartphone e tablet, secondo le testimonianze raccolte, permetterebbero un accesso immediato alle informazioni che accelera i tempi di ricerca e ne facilita le modalità. Sono *device* più comodi e versatili rispetto al computer, adottato per ricerche e attività più complesse e strutturate, quali ad esempio l'elaborazione di testi scritti, la preparazione di presentazioni e l'esecuzione di compiti di programmazione. Con particolare riferimento alle classi digitali, emerge come questi dispositivi vengano spesso utilizzati a scuola, insieme alle Lavagne Interattive Multimediali (3), per effettuare ricerche, elaborare documenti e presentazioni, progettare ed elaborare lavori di gruppo. Oltre all'ambito scolastico, i dispositivi indicati vengono utilizzati per lo svago e il tempo libero.

Con riferimento ai *social network*, emerge dai focus group come essi vengano utilizzati "in ogni momento della giornata", al risveglio per controllare eventuali aggiornamenti, durante il giorno, sia a scuola che a casa e, infine, la sera, prima di addormentarsi. In prevalenza, ci si connette ai social mediante lo smartphone.

1 Si ringrazia per la co-conduzione dei focus group il dott. Angelo Canal che ha svolto nell'ambito del progetto Edu4Sec la propria tesi di laurea magistrale presso l'Università degli Studi di Padova, Corso di Studi in Management dei Servizi Educativi e Formazione Continua.

In ordine, Facebook (34), Instagram (25) e Snapchat (20) risultano i social più utilizzati per condividere immagini, mentre WhatsApp (30) risulta l'applicazione più utilizzata per la messaggistica. Per quanto riguarda invece la posta elettronica, essa è riservata allo scambio e all'elaborazione di compiti scolastici, ad esempio nel caso dell'elaborazione di ricerche, condivisione di presentazioni e condivisione di appunti. Solo una minoranza cita servizi come Google Drive o Dropbox per la gestione dei propri file online. Facebook è utilizzato dalla totalità degli studenti e delle studentesse coinvolti nei focus group, nella maggior parte dei casi dall'inizio delle scuole superiori, per una minoranza già dalla scuola media di primo grado. La maggior parte degli intervistati dichiara di avere un profilo "chiuso" (25) e di condividere quindi foto ed informazioni solamente con i propri "amici". Tuttavia, si condividono in prevalenza contenuti proposti da altri, più che inserire informazioni ed immagini personali. Nonostante dai focus-group emerga una netta preferenza per il mantenimento di profili chiusi, gli studenti e le studentesse coinvolte riportano di effettuare spesso, per comodità, l'accesso ad altri siti o applicazioni tramite uno dei profili social utilizzati, con il rischio di condividere anche informazioni personali, consapevolezza che pare non emergere durante le discussioni esplorative.

Uno degli aspetti più interessanti emersi durante i focus-group riguarda gli *acquisti online,* tema inizialmente non considerato ai fini della progettazione dei moduli formativi. Tra coloro che acquistano in rete, gli intervistati hanno aperto la strada agli acquisti in rete, mai praticati prima all'interno del nucleo familiare (12); solo un numero minimo (4) ha proseguito una pratica già adottata dai genitori. Emerge come gli acquisti vengano solitamente effettuati via computer, soprattutto se si tratta di acquisti importanti, mentre per prodotti poco costosi o relativi ad applicazioni e videogiochi vengono utilizzati anche il tablet o lo smartphone. Gli intervistati che riferiscono di acquistare in rete, segnalano di controllare sempre che il sito permetta il rimborso nel caso di merce scadente o diversa da quanto riportato nella scheda di descrizione del prodotto. Contemporaneamente, segnalano di prestare molta attenzione alle recensioni degli altri acquirenti, soprattutto nel caso si apprestino ad effettuare l'acquisto da siti poco noti. Per quanto riguarda le modalità di pagamento, alcuni (4) segnalano l'uso di una carta prepagata (4). Tuttavia, dopo esperienze di merce danneggiata o di mancata consegna, alcuni dei presenti evidenziano di prediligere il pagamento alla consegna (3), dove possibile.

I focus group hanno inteso indagare anche eventuali *situazioni critiche* rispetto all'uso dei *device*. Fra le criticità più frequenti emerse, gli studenti riferiscono l'attivazione di banner pubblicitari e "pagine indesiderate che si aprono da sole" (10). Citano, inoltre, la necessità di verificare il profilo degli utenti da cui vengono con-

tattati via social network, preferendo stringere "amicizia" con persone note (28). Con riferimento a tale criticità, alcuni (10) segnalano di aver modificato le impostazioni del profilo, rendendolo privato dopo averlo inizialmente mantenuto pubblico. Per quanto riguarda, inoltre, la gestione dei *tag*, la maggior parte degli studenti (25) ne verifica i contenuti prima di renderli visibili nella propria bacheca.

Con riferimento alla *creazione e gestione delle password*, l'esplorazione mediante focus-group ha evidenziato come, circa un terzo dei partecipanti utilizzi la medesima password per tutti i propri profili (12). Si tratta, per alcuni (8) di password molto semplici e intuitive, che vengono salvate nello smartphone per non dimenticarle (8) e che rimandano a dati personali, quali nome, cognome e data di nascita (6). Alcuni ammettono, inoltre, di non aver mai modificato la password dei propri profili dal momento dell'attivazione (7).

Maggiore appare la consapevolezza circa il rischio rappresentato da *virus e malware*. La totalità dei presenti ha affermato di possedere un antivirus nel proprio pc, quasi sempre nella versione gratuita. Gli intervistati hanno segnalato numerose criticità a riguardo, riportando numerose esperienze, dal rallentamento della macchina, fino ad un caso di *Crypto Locker*[2].

Per quanto riguarda la *connessione a reti Wi-Fi pubbliche*, è emerso che vengono utilizzate in prevalenza per accedere ai social network, ma vengono accuratamente evitate per fare acquisti o accedere alla propria casella di posta elettronica. Vengono percepite come maggiormente sicure le reti che richiedono una registrazione (8) ed evitate le reti aperte.

I nodi emersi dai focus-group hanno così orientato la messa a punto dei moduli formativi, progettati al fine di incoraggiare nei partecipanti una riflessione sui contenuti risultati particolarmente critici, per la rilevanza rivestita nelle abitudini d'uso degli studenti o per la distorta o ridotta percezione del rischio rilevata.

5.2 L'articolazione degli interventi formativi del progetto Edu4Sec

Come anticipato, hanno preso parte alla sperimentazione 12 classi (Tabella 1). Il gruppo sperimentale era composto di 6 classi, 2 per ogni istituto per un totale di 116 studenti coinvolti e il gruppo di controllo di altre 6 classi, 2 per ogni istituto per un totale di 140 studenti coinvolti che hanno beneficiato ciascuno di un intervento formativo della durata di 2 ore scolastiche ossia una durata media di

2 Ricordiamo che si tratta di un *malware* che agisce criptando i dati della vittima, richiedendo un pagamento per la decriptazione.

105 minuti (per approfondimenti sul disegno sperimentale si rimanda a Frison & Surian, 2018).

Interventi realizzati	n. 12
Istituti coinvolti:	n. 3
Classi coinvolte	n. 12 così ripartite: Seconde n. 1 Terze n. 7 Quarte n. 4
Interventi Gruppo Sperimentale	n. 6 (2 per ognuno dei 3 Istituti)
Interventi Gruppo di Controllo	n. 6 (2 per ognuno dei 3 Istituti)
Durata media degli interventi	105 minuti
Studenti coinvolti	n. 256 così riparti: - 140 GS - 116 GC

Tabella 1. Sintesi degli interventi realizzati

I moduli formativi proposti hanno sviluppato le aree tematiche sopra illustrate:

- *Internet: rischi e pericoli*
- *e-Commerce: shopping in sicurezza*
- *Password: la nostra difesa*
- *Smartphone: sono veramente smart?*
- *Social Network: privacy & security*.

Per ogni modulo è stata prevista una presentazione frontale, per quanto possibile contenuta, intercalata da attività e tecniche di "manipolazione" di concetti chiave a partire da una rielaborazione delle loro esperienze in materia di gestione delle password, scelta e download di applicazioni, uso delle reti sociali, ecc. Secondo un approccio induttivo, inoltre, le attività hanno, di norma, anticipato la presentazione dei contenuti più teorici al fine di promuovere la problematizzazione dei concetti proposti e favorire un ancoraggio all'esperienza personale.

Al gruppo sperimentale è stato proposto un intervento che ha previsto le medesime attività e tecniche e, oltre a esse, l'inserimento di elementi di *gamification* (Detering, Dixon, Khaled & Nacke, 2011; Cheong et al., 2013; Kapp, 2012).

Più precisamente, entrambi i gruppi hanno beneficiato di interventi che hanno previsto l'ausilio di presentazioni e attività di gruppo (attività di *decision making* di gruppo e *role-play*). Oltre a ciò, nelle classi afferenti al gruppo sperimentale, l'intervento ha previsto un *Learning Game* focalizzato sull'e-commerce (in Figura 1) e un quiz *Kahoot* sulla gestione delle password (come indicato nella proposta di micro-progettazione precedentemente presentata) (Frison & Surian 2018).

Figura 1 – Schermata di Login del Learning Game dedicato all'E-commerce

Le cinque sezioni tematiche sopra menzionate, sono state seguite da una sezione conclusiva dedicata al tema *Io e l'incontro di oggi*, che ha inteso indagare i temi di nuova conoscenza e le attività/tematiche che, secondo l'opinione degli studenti coinvolti, sono risultate maggiormente coinvolgenti.

5.3 Lo strumento d'indagine

Ciascun intervento formativo è stato anticipato dalla somministrazione di un questionario auto-compilato da parte dei partecipanti volto a rilevare, ex-ante, dati anagrafici, conoscenze e abitudini di comportamento degli studenti coinvolti. Il questionario è stato somministrato anche ex-post, al fine di rilevare nuovamente le conoscenze dei partecipanti sulle tematiche proposte e le intenzioni/previsioni di comportamento dopo la partecipazione al modulo. I questionari, somministrati mediante Google Moduli, hanno proposto sia domande aperte sia domande chiuse a scelta multipla, ad una sola risposta o a più risposte, proponendo batterie di domande collegate alle aree tematiche proposte.

Si riportano di seguito alcune informazioni introduttive sul campione di comodo considerato, composto per il 44,92% da studenti che afferiscono a classi digitali e per il 55,08% a classi tradizionali (Tabella 2).

	GS Ex ante	GS Ex post	GC Ex ante	GC Ex post
M	56	71	91	107
F	84	39	25	28
Classe "tradizionale" - CT	69	54	72	94
Classe Digitale - CD	71	56	44	41
Istituto Tecnico Commerciale - ITC	45	39	38	42
Istituto Tecnico Industriale - ITI	50	41	44	63
Liceo Scienze Applicate - LSA	0	0	13	11
Liceo Scientifico - LS	24	21	21	19
Liceo Scienze Umane - LSU	21	9	0	0
Totale	140	110	116	135

Tabella 2. Ripartizione rispondenti per classe di appartenenza e gruppo

La variazione nel numero di questionari raccolti ex-ante ed ex-post per gruppo, sperimentale (140 ex-ante e 110 ex-post) e di controllo (116 ex-ante e 135 ex-post) è da imputarsi a problemi tecnici incontrati dagli studenti nell'accesso a Google Moduli mediante il loro account Google (ad es. difficoltà nel recupero della password di accesso o indirizzo e-mail errato e mancato recapito del link per la compilazione del questionario). In altri casi, inoltre, si è trattato di mancata compilazione del questionario che, ove le tempistiche lo hanno concesso, è stato proposto in aula prima dell'avvio del modulo formativo ed immediatamente dopo la sua conclusione; dove invece i tempi erano troppo stretti (ad esempio intervento formativo di 100 minuti), il link al questionario è stato trasmesso via e-mail e la compilazione è stata sollecitata dagli animatori digitali il giorno antecedente l'intervento. In questi casi, il questionario non è stato compilato dalla totalità degli studenti coinvolti.

Tra i dati socio-anagrafici richiesti in apertura di questionario, è stata indagata la tipologia di dispositivi posseduti dai rispondenti oltre che il dispositivo maggiormente utilizzato, così come era stato inizialmente esplorato mediante i focus-

group condotti. Lo smartphone risulta in assoluto il dispositivo più utilizzato, segnalato dal 75,39%, e seguito dal PC, segnalato dal 15,93% dei rispondenti. Oltre a Smartphone e PC, il 44,14%, con riferimento al proprio nucleo familiare, dichiara di possedere Tablet, Smart TV e Console e il 28, 13% di possedere i medesimi dispositivi (Smartphone, PC, Tablet, Console) fatta eccezione per la Smart TV.

5.4 Risultati

5.4.1 Sezione "Io e le password"

Con riferimento alle password utilizzate abitualmente e alle strategie adottate per la loro gestione, è stato indagato come esse vengano scelte dai rispondenti (con riferimento a quali criteri), quali siano le strategie messe in atto per ricordarle e la relativa frequenza di aggiornamento. Vengono riportate di seguito, in tabella 3, le strategie di gestione maggiormente citate dalla totalità dei rispondenti. Tra esse emergono l'annotazione delle password su un foglio e l'utilizzo di una medesima password o di password molto simili per facilitarne la memorizzazione e il recupero. I rispondenti evidenziano, inoltre, come spesso le password adottate siano di semplice strutturazione, con riferimento a nomi e numeri significativi quali date di nascita o eventi importanti della vita personale. Le strategie menzionate sono le medesime per GS e GC.

	GESTIONE PSW %
Le scrivo su un foglio	20,00%
Uso nomi o numeri significativi	19,29%
Uso password uguali o simili	15,71%
Uso password semplici	12,14%
Le ricordo a memoria	12,14%
Uso caratteri speciali	3,57%

Tabella 3 – Strategie di gestione delle password, gruppo complessivo

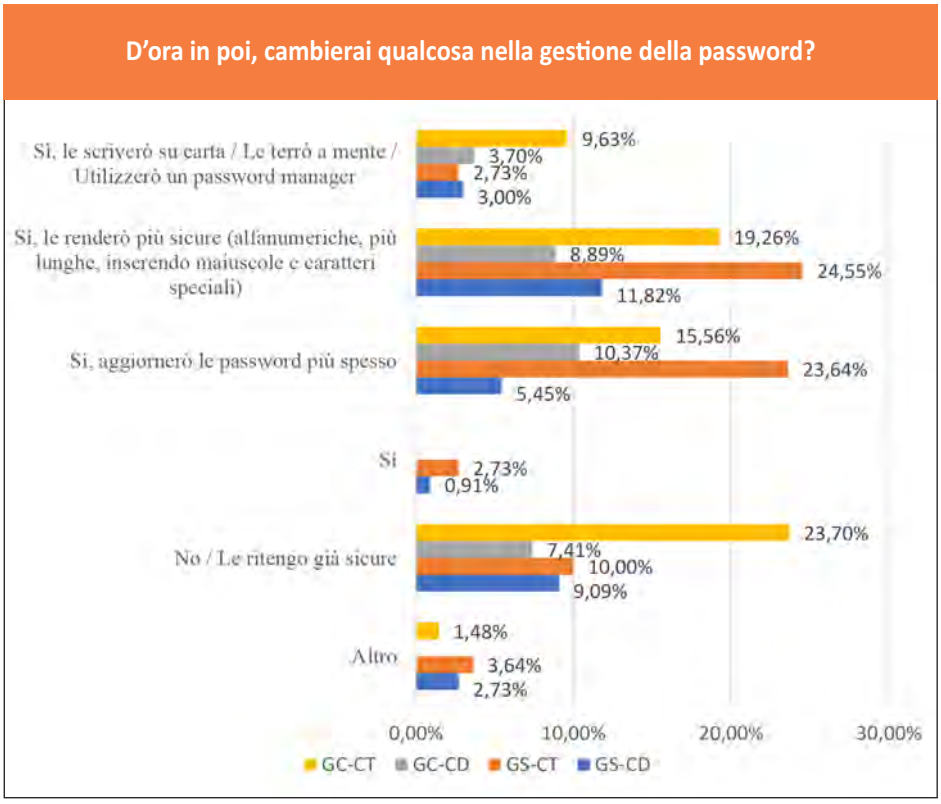


Grafico 1 – Cambiamenti nella gestione delle password, post-intervento, gruppo di controllo/sperimentale, classe digitale/tradizionale

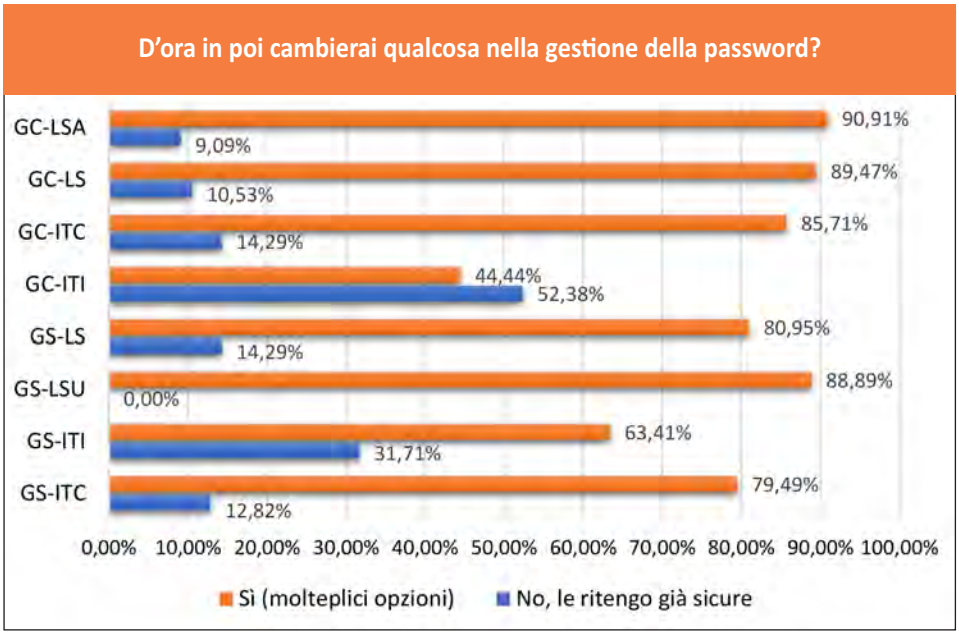


Grafico 2 – Cambiamenti nella gestione delle password, post-intervento, gruppo di controllo/sperimentale, per istituto

Dopo l'esplorazione delle abitudini in merito alla gestione delle password, il modulo *Password: la nostra difesa* mostra agli studenti come costruire una password appropriata oltre a fornire evidenza degli eventuali rischi connessi all'utilizzo di password non sicure. Relativamente all'impostazione delle password, il grafico 1 evidenzia come siano soprattutto gli studenti delle classi tradizionali a dichiararsi intenzionati ad apportare cambiamenti al fine di renderle più sicure. Ciò riguarda sia il GS, con il quale l'argomento "password" è stato sviluppato mediante l'integrazione delle slides con un quiz Kahoot (Figura 1), che il GC, che ha invece beneficiato della sola presentazione frontale.

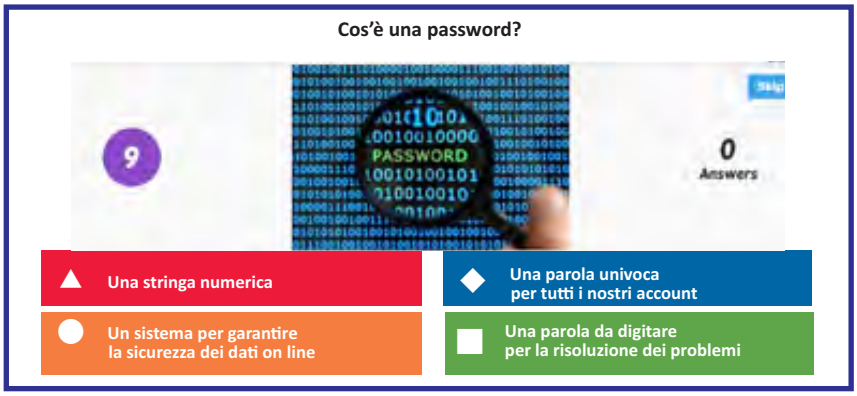


Figura 1 – Quiz Kahoot modulo Password: la nostra difesa

La percezione di un buon livello di sicurezza delle proprie password, che non richiedono dunque di essere modificate, riguarda soprattutto gli studenti dell'ITI (peraltro iscritti all'indirizzo informatico e dunque già in possesso di una serie di conoscenze a riguardo previste dal loro curricolo) e i membri delle classi digitali.

5.4.2 "Io e Facebook", "Io e i Social"

La batteria successiva, ha indagato la presenza e l'attività dei rispondenti nei social network. In particolare, è stata indagata la tipologia di informazioni condivise su Facebook e altri social, le strategie di gestione della privacy e la percezione di sicurezza dei propri profili. Così come per le password, ex-post, è stata verificata l'intenzione dei partecipanti di apportare o meno modifiche.

Innanzitutto, il 73,05% dei rispondenti possiede un profilo Facebook. Di questi, il 76,85% lo ritiene "sicuro" ("Pensa al tuo profilo Facebook: a tuo avviso, quanto è sicuro?") ad un livello 3 o 4 (dove 1 = per nulla sicuro e 4 = assolutamente sicuro) nonostante ben il 63,10% non verifichi i post in cui è taggato consentendo una pubblicazione immediata nella propria bacheca, priva di verifica, effettuata invece dal 25,13% dei rispondenti.

Oltre alla sicurezza del profilo Facebook, a tutti gli studenti coinvolti è stato chiesto quanto ritenessero sicuri i loro social in generale e i loro device dai rischi di Phishing o dalle minacce legate al download di applicazioni. A riguardo, la maggioranza sia del GC che del GS si attesta intorno ad un livello di sicurezza percepita pari a 3 per tutti i punti sopra indicati. Come evidenziato dalla tabella

4, inoltre, il 40,11% degli alunni coinvolti posta foto, video e in generale notizie dalla rete; a queste informazioni, il 41,71% dei rispondenti aggiunge la pubblicazione di stati in bacheca e della propria posizione.

	TIPOLOGIA POST %
Stati in bacheca / Foto / Video / Posizione / Notizie dalla rete	41,71%
Foto / Video / Notizie dalla rete	40,11%
Non pubblico nulla	6,95%
Non lo uso più	5,88%
Posizione / Foto / Video / Notizie dalla rete	2,67%

Tabella 4 – Tipologia di informazioni postate, gruppo complessivo

Precisamente, il 73,68% degli appartenenti al GS e il 70,27% degli appartenenti al GC che si dichiarano intenzionati ad apportare modifiche, segnalano di voler trasformare il proprio profilo da pubblico a privato, di voler impostare il controllo tag e di voler verificare le proprie impostazioni di privacy per rendersi conto di chi abbia accesso ai propri dati (profilo pubblico, amici, amici degli amici, ecc.), informazione non nota al momento dell'intervento formativo. Chi invece afferma di non essere intenzionato ad apportare modifiche (il 54,22% del GS e il 64,42% del GC, vedasi grafico 3), lo fa esplicitando le seguenti motivazioni:

"Non ne ho bisogno / Non mi interessa / Non condivido cose personali" per il 22,73% del GC e il 22,2% del GS e "Lo ritengo già sicuro / Ho già impostato tutti i livelli di sicurezza possibili", per il 72,73% del GC e il 60,00% del GS.

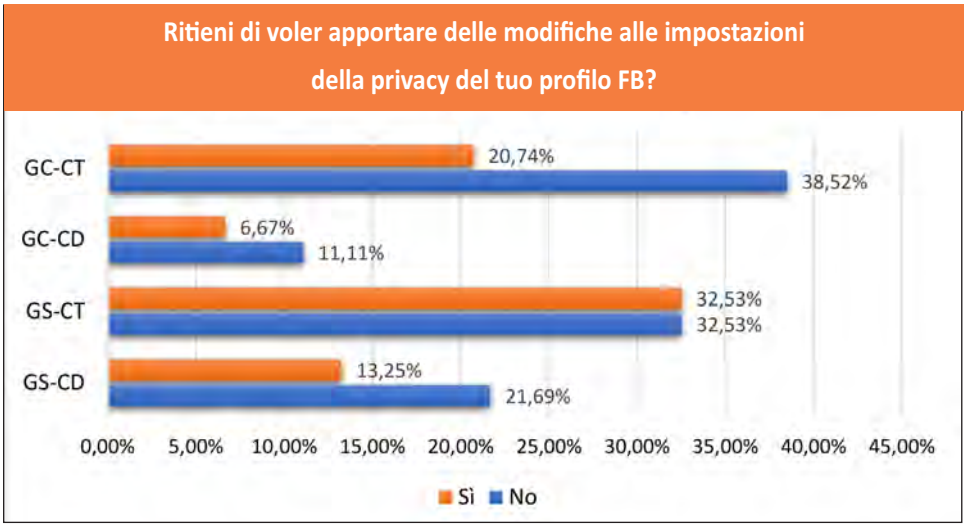


Grafico 3 – Apporto di modifiche al proprio profilo Facebook, post-intervento, gruppo di controllo/sperimentale, classe digitale/tradizionale

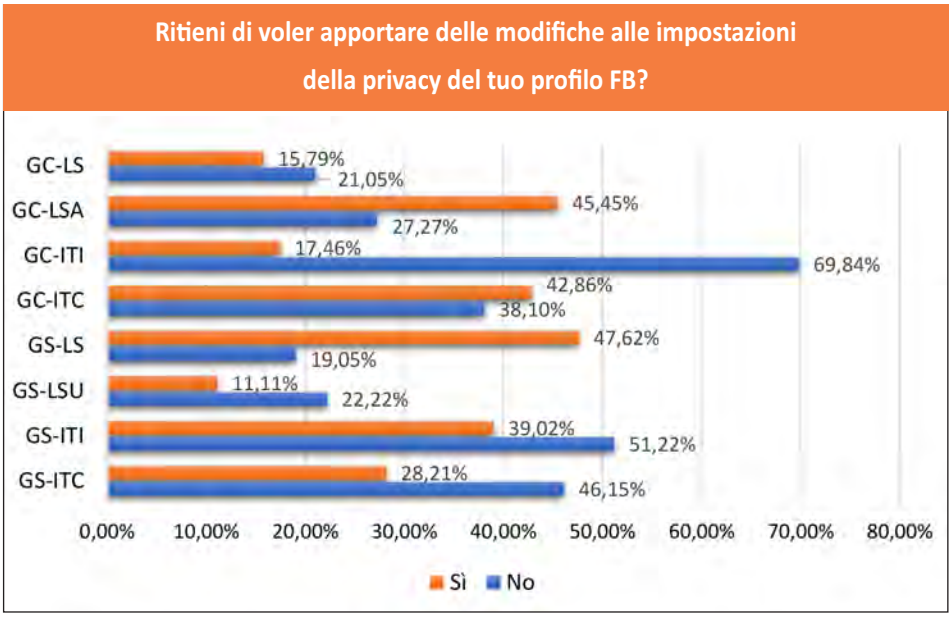


Grafico 4 – Apporto di modifiche al proprio profilo Facebook, post-intervento, gruppo di controllo/sperimentale, per istituto

Anche per Facebook, così come per le password, emerge come siano soprattutto gli studenti delle classi tradizionali ad esprimersi in favore di possibili cambiamenti al proprio profilo, rispetto alla classe digitali e come, ancora una volta, gli studenti dell'ITI si confermino i maggiori "esperti".

Sempre relativamente ai social network, il 98,44% dei rispondenti totali possiede un profilo in altri social (es. Telegram, Twitter, WhatsApp, Instagram, Snapchat, ecc.) oltre a Facebook e l'82% di essi ritiene i propri profili "sicuri" ad un livello 3 o 4 (dove 1 = per nulla sicuro e 4 = assolutamente sicuro). Chi si dichiara non intenzionato ad apportare modifiche ai propri profili social (vedasi grafico 5) segnala le medesime motivazioni relative al profilo Facebook: "Non mi interessa" per il 5,21% del GC e "Non mi interessa / Non condivido cose personali" per il 20% del GS e "Lo ritengo già sicuro / Ho già impostato tutti i livelli di sicurezza possibili", per il 90,63% del GC e il 61,22% del GS.

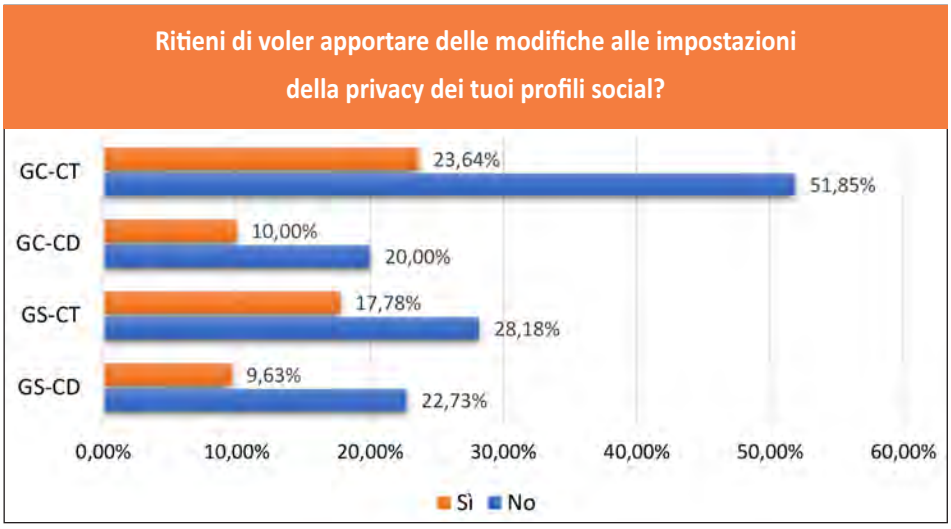


Grafico 5 – Apporto di modifiche ad altri profili social, post-intervento, gruppo di controllo/sperimentale, classe digitale/tradizionale

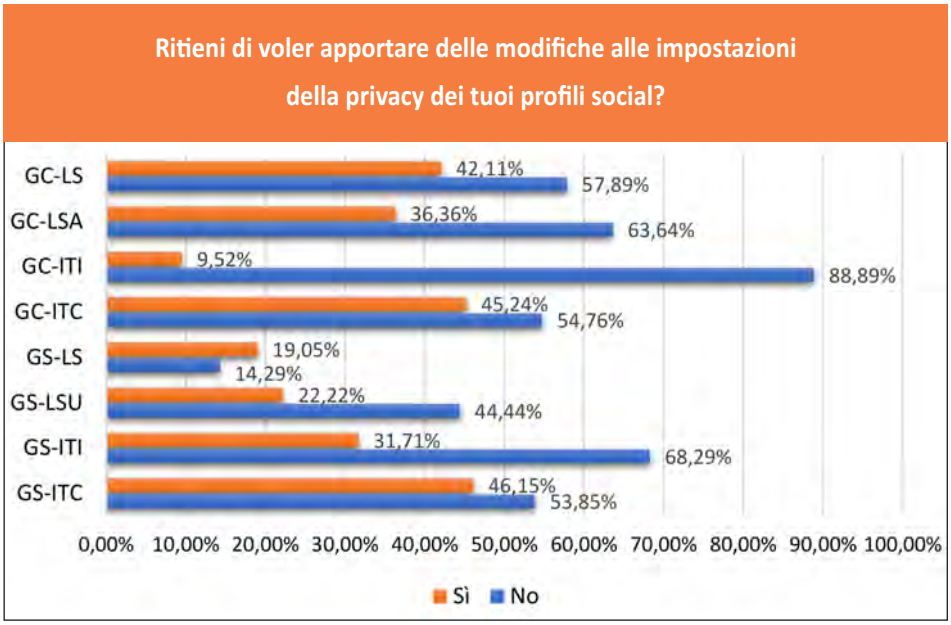


Grafico 6 – Apporto di modifiche ad altri profili social, post-intervento, gruppo di controllo/sperimentale, per istituto

Viene replicata nuovamente la distribuzione percentuale relativa ai profili Facebook, con un maggior orientamento all'apporto di modifiche da parte delle classi tradizionali in rapporto a quelle digitali. Emerge tuttavia, come relativamente all'uso dei social, gli studenti si sentano "sicuri" e ritengano, per la maggioranza, che i loro profili non necessitino di un potenziamento delle impostazioni di privacy. Potremmo dunque trovarci, da un lato, di fronte ad un gruppo composto prevalentemente da "esperti", abili e consapevoli utilizzatori dei social network, che hanno accuratamente messo a punto il loro profilo proteggendolo, per quanto possibile, da sguardi indesiderati. Ma potrebbe anche trattarsi di un gruppo di fruitori che, abitando quotidianamente l'ambiente social, lo percepiscono così conosciuto e familiare (e dunque "sicuro") da viverlo in maniera indifferente ed inconsapevole, senza adottare alcuna precauzione contro i rischi che potrebbero incontrare. La data security e i rischi ad essa connessi potrebbero così riguardare soprattutto gli users più inesperti, che in quanto tali, ignorano completamente le possibili fonti e forme di "infortunio", o, al contrario, gli utilizzatori più esperti che si muovono nel cyberspazio con maggior disinvoltura, proprio come accade nel caso degli infortuni sul luogo di lavoro laddove l'eccessiva familiarità con l'ambiente e gli strumenti di lavoro diviene fattore di rischio anziché di protezione.

5.4.3 "Io e Internet"

Proseguendo con il questionario, la terza batteria di domande ha indagato il fenomeno del *phishing*, tematica che si è rivelata in generale poco nota al gruppo di studenti coinvolto. Precisamente, è stato indagato quanto questo fenomeno risultasse noto e quali fossero i casi di *phishing* accaduti agli studenti o alla loro cerchia di amici e familiari. Alla domanda "Sei mai stato vittima personalmente di episodi di phishing su Internet?" i partecipanti hanno risposto mettendo in evidenza che il 42,19% di essi non era a conoscenza del fenomeno ("non so cosa sia il phishing") prima dell'intervento formativo.

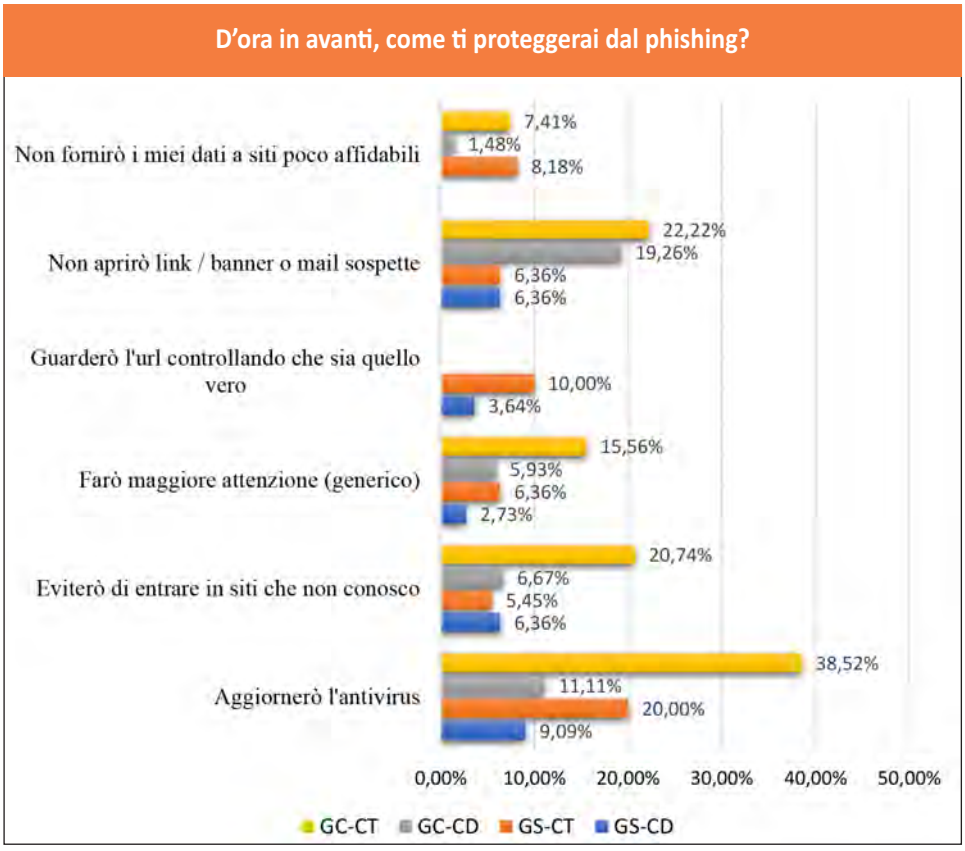


Grafico 7 – Esempi di strategie di protezione dal phishing, post-intervento, gruppo di controllo/sperimentale, classe digitale/tradizionale

Il modulo è stato strutturato a partire dall'attività *Diamond Ranking* (si veda il paragrafo 4.1.3.) finalizzata a sollecitare la discussione e il confronto rispetto a posizioni e idee differenti all'interno del gruppo in merito ai rischi connessi alla rete. A fronte dell'intervento formativo, emerge dal grafico 7 come gli studenti, invitati a riflettere sulle modalità di protezione dal *phishing*, abbiano ripreso quanto evidenziato nel corso del modulo. Il grafico evidenzia inoltre come, ancora una volta, siano soprattutto gli studenti delle classi tradizionali ad orientarsi verso strategie di protezione. A tale proposito si consideri che, dal punto di vista metodologico, la domanda proposta era aperta e le risposte raccolte sono state categorizzate ex-post. Si può dunque rilevare come alcuni studenti, in particolare quelli delle classi tradizionali, abbiano dichiarato di voler attivare più strategie di protezione contemporaneamente.

5.4.4 "Io e le app"

La quarta batteria proposta ha riguardato le applicazioni utilizzate dai rispondenti e i loro comportamenti a riguardo, ad esempio in merito alla lettura delle note informative prima di effettuarne il download e delle recensioni. Relativamente alle app, pre-intervento, il 28,13% le ritiene una minaccia per i propri dispositivi ad un livello 3 o 4 (dove 1 = per nulla sicuro e 4 = moltissimo). Ciò significa che per oltre un 70%, esse non costituiscono una minaccia. Post-intervento, la percentuale di rispondenti che non ritengono le app una minaccia (livello 1-2) passa dal 71,88% al 62% e alla richiesta di elementi concreti a cui prestare attenzione al download di nuove applicazioni, gli studenti dichiarano di voler approfondire maggiormente sia le recensioni che i permessi richiesti per l'installazione (grafico 8), in particolare, ancora una volta, gli studenti delle classi tradizionali.

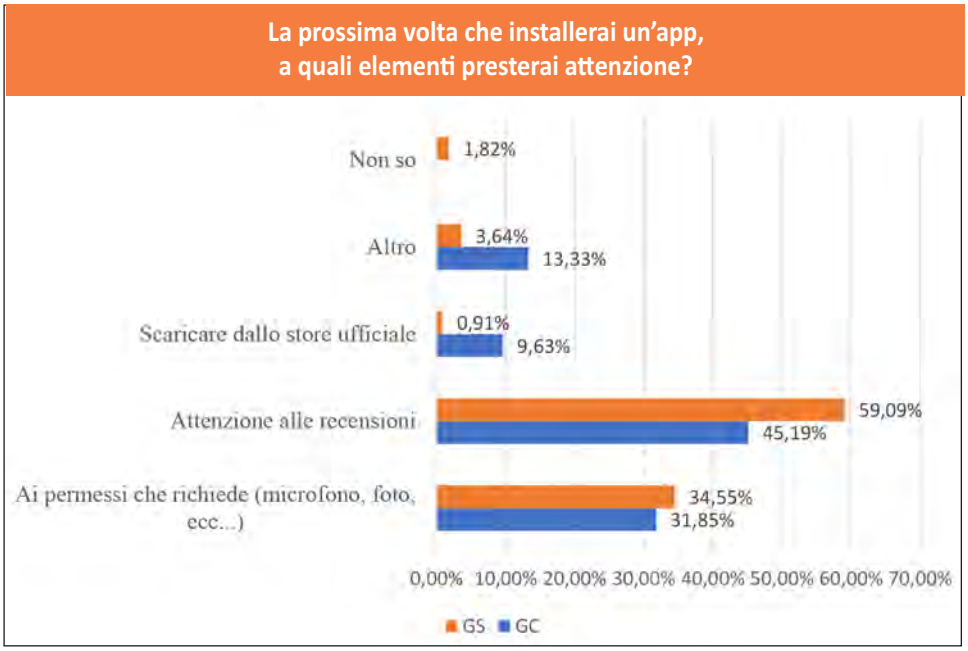


Grafico 8 – Elementi concreti a cui prestare attenzione al download di nuove applicazioni, post-intervento, gruppo di controllo/sperimentale

5.4.5 "Io e gli acquisti online"

L'ultima batteria proposta ha indagato un'ulteriore area tematica inserita nel percorso formativo a seguito di quanto emerso dai focus group condotti in fase di avvio negli istituti coinvolti: "*e-Commerce: shopping in sicurezza*". Il modulo ha inteso affrontare il problema degli acquisti online ricorrendo ad esempi concreti relativi a situazioni di rischio e, al contempo, a strategie di shopping sicuro. Questo modulo è stato preceduto, per il gruppo sperimentale, da un *Learning Game* strutturato come un quiz a livelli che richiedeva, per poter accedere alle parti successive, il completamento di tutte le precedenti, visualizzando il punteggio ottenuto e favorendo così una propositiva competizione fra i vari studenti.

Il questionario pre-intervento ha esplorato le abitudini di acquisto ed in particolare le modalità di pagamento maggiormente utilizzate dal gruppo.

Il grafico 9 mostra la frequenza degli acquisti online con riferimento al campione di studenti presi qui in considerazione: a fronte di un 28% che non si è ancora avvicinato allo shopping online, il 57% dei rispondenti effettua acquisti in rete da 1 a 3 volte al mese. Di questi, il 61,62% lo fa utilizzando un account PayPal o una carta prepagata mentre il 15,14% dichiara di utilizzare direttamente

una carta di credito collegata ad un conto proprio o dei propri genitori. Il 7,03% adotta entrambe le strategie (Paypal o prepagata, carta di credito).

Il grafico 10 mostra le intenzioni di comportamento dei rispondenti che affermano di voler porre maggiore attenzione alle modalità di pagamento e, più in generale, al sito in cui effettuare l'acquisto, per verificarne affidabilità, recensioni, ecc. GC e GS risultano perfettamente allineati.

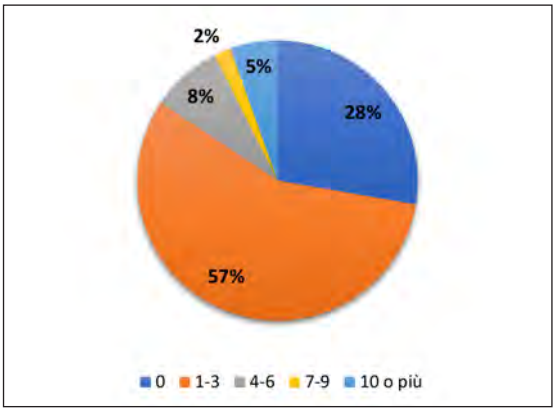


Grafico 9 – Frequenza mensile degli acquisti online, gruppo complessivo

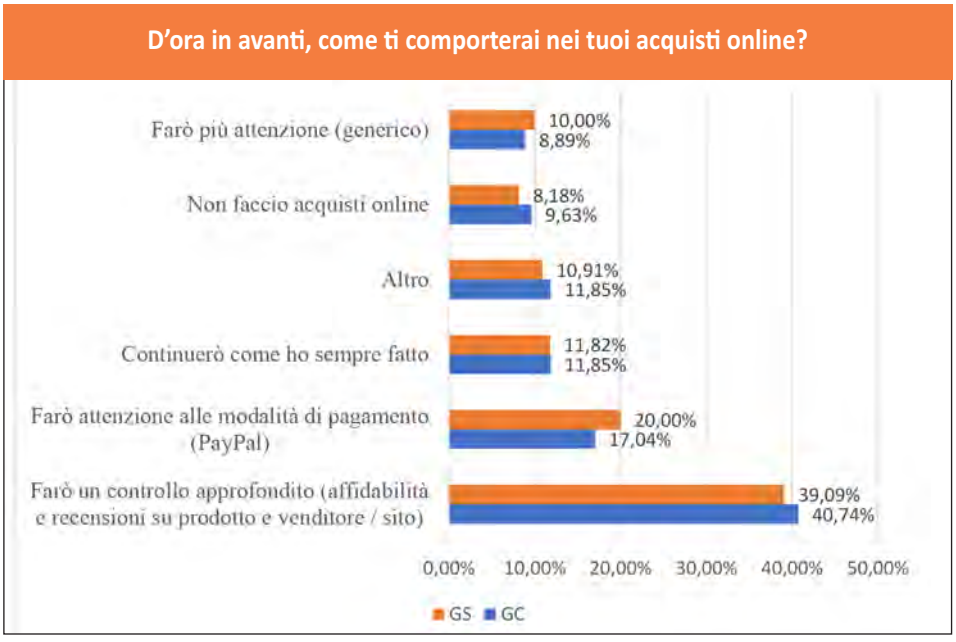


Grafico 10 – Intenzioni di comportamento negli acquisti online, post-intervento, gruppo di controllo/sperimentale

5.4.6 "Io e l'incontro di oggi"

Al termine delle domande specifiche sui contenuti del modulo, il questionario ha proposto agli studenti coinvolti due domande conclusive volte ad indagare attività/momenti ritenuti maggiormente coinvolgenti e nuove conoscenze. Osservando il grafico 11, è immediato il riferimento dei partecipanti ai momenti dedicati al confronto e allo scambio con i compagni (role-play, attività di decision making di gruppo, "attività" in generale ecc.). Per il solo GS, è possibile ritrovare il riferimento al quiz Kahoot, estremamente coinvolgente grazie alla dinamica di *gamification* (musica, interfaccia accattivante, sfida) citato in particolare dagli studenti delle classi tradizionali. In merito alle nuove conoscenze, i partecipanti riferiscono in particolare del *phishing* (circa il 33% del GS e il 25% del GC) e dei molteplici virus e malware citati durante l'intervento (30% del GS e 20% del GC).

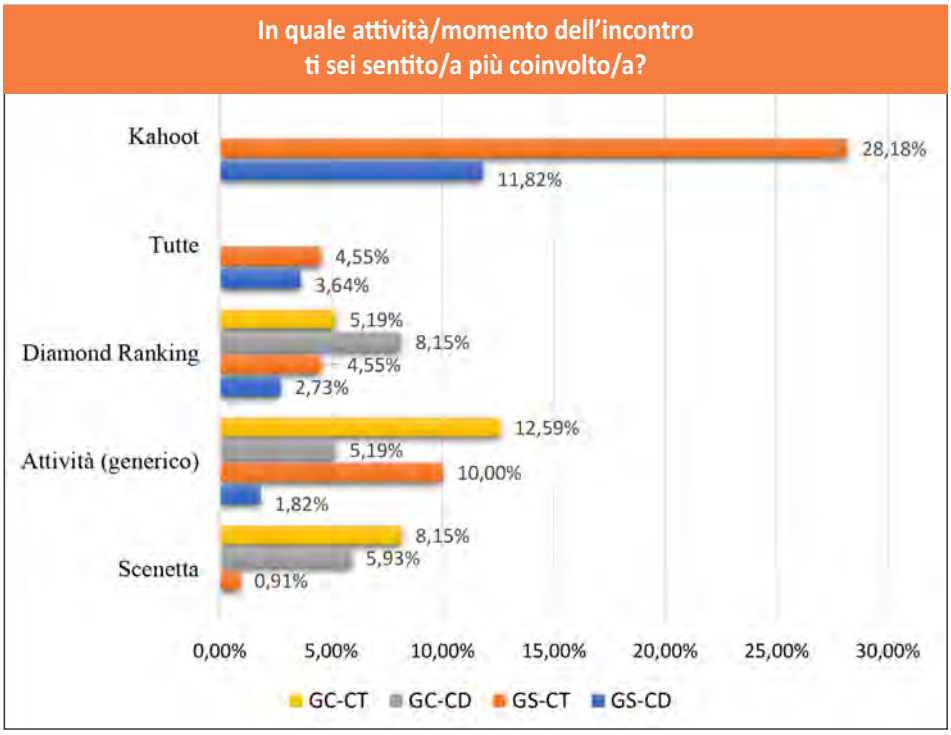


Grafico 11 – Attività/momento di maggior coinvolgimento, post-intervento, gruppo di controllo/sperimentale, classe digitale/tradizionale

5.5 Conclusioni

I dati qui presentanti intendono fornire un'ulteriore indicazione in merito alla proposta di attività formative che insegnanti e animatori digitali potrebbero allestire nei propri contesti scolastici di riferimento e alla tipologia di riflessioni che la somministrazione degli strumenti d'indagine ex-ante ed ex-post sviluppati nel corso del progetto Edu4Sec possono consentire qualora adottati. È evidente come un limite importante del modulo offerto – e dunque, da un punto di vista di ricerca, anche dei dati raccolti – è legato alla durata dell'intervento. 100-120 minuti costituiscono uno spazio limitato per mettere a fuoco e sollecitare cambiamenti in merito a percezioni e comportamenti, spesso inconsapevoli, ma consolidati dall'abitudine quotidiana e dalla familiarità con gli ambienti virtuali. Invitiamo, dunque, come autori, alla luce dell'esperienza condotta, di integrare tali riflessioni, e con esse gli strumenti proposti, all'interno di percorsi più complessi e prolungati che favoriscono l'attivazione di un dialogo proficuo e generativo tra insegnanti e studenti a sostegno di una cultura della *data security* più efficace e ancorata alle molteplici esperienze, dirette e indirette, patrimonio delle classi.

6.

Risorse chiave

di *Daniela Frison, Alessio Surian*

Vengono presentate qui di seguito alcune risorse utili (in continuo aggiornamento attraverso il sito online www.dyaloghi.com), raggruppate per siti web, blog, video.

6.1 Siti web

CampusLab – Agenzia Formativa, Servizi per il Lavoro e Agenzia di Sviluppo per la Promozione del Territorio. *Sicurezza integrata: un'azione di prevenzione per i ragazzi su fenomeni di bullismo e i rischi collegati all'uso di Internet e dei social network*.
Online http://www.campuslab.eu/picopdm-als0057

Cisco Systems. Cisco Cybersecurity Reports.
Online https://www.cisco.com/c/en/us/products/security/security-reports.html

CIS-Sapienza & Laboratorio Nazionale di Cyber Security. *Framework Nazionale per la CyberSecurity.*
Online http://www.cybersecurityframework.it/

Commissariato di P.S. online. *Sportello per la sicurezza degli utenti del web*.
Online http://www.commissariatodips.it/

Confederazione Svizzera. *Giovani e media. Piattaforma nazionale per la promozione delle competenze mediali*.
Online http://www.giovaniemedia.ch/it/home.html

Consorzio Interuniversitario Nazionale per l'Informatica. *Laboratorio Nazionale di Cybersecurity.*
Online https://www.consorzio-cini.it/index.php/it/lab-cyber-security

European Union Agency for Network and Information Security.
Online https://www.enisa.europa.eu/about-enisa

IBM. IBM Security.
Online https://www.ibm.com/security

Microsoft. *Ischool. Il futuro della scuola*.
Online http://ischool.startupitalia.eu/

MIUR, Ministero per l'Istruzione, l'Università e la Ricerca. *Generazioni Connesse. Safer Internet Centre*.
Online http://www.generazioniconnesse.it/site/it/home-page/

Network Digital 360. *Agenda Digitale*.
Online https://www.agendadigitale.eu/

Network Digital 360. *Cybersecurity360*.
Online https://www.cybersecurity360.it/

Polizia Postale e delle Comunicazioni. *Una vita da social*.
Online https://www.facebook.com/unavitadasocial/

Presidenza del Consiglio dei Ministri. *Agenzia per l'Italia digitale*.
Online http://www.agid.gov.it/agenda-digitale

Progetto Mowgli Naviga In Rete.
Online https://sites.google.com/site/mowglinavigainrete/progetto

Project Net Children Go Mobile.
Online http://netchildrengomobile.eu/PROJECT/

Save the Children. *Che genere di tecnologie? Ragazze e digitale tra opportunità e rischi*.
Online https://www.savethechildren.it/cosa-facciamo/pubblicazioni/che-genere-di-tecnologie-ragazze-e-digitale-tra-opportunit%C3%A0-e-rischi

Università degli Studi di Milano-Bicocca. Dipartimento di Sociologia e ricerca sociale. *Benessere digitale. Formazione e ricerca sulla qualità della vita iperconnessa*.
Online http://www.benesseredigitale.eu/

6.2 Blog

Digital Education Lab. La scuola di educazione digitale. *Blog*.
Online https://www.digitaleducationlab.it/blog/

Repubblica.it. *Osservatorio Cyberbullismo*.
Online http://osservatorio-cyberbullismo.blogautore.repubblica.it/

Save the Children. *Blog e Notizie*.
Online https://www.savethechildren.it/blog-notizie

Startup Italia. *Cybersecurity.*
Online http://cybersecurity.startupitalia.eu/blog

6.3 Video

Garante per la protezione dei dati personali. *Canale Youtube*.
Online https://www.youtube.com/user/videogaranteprivacy

Garante per la protezione dei dati personali (2013). Fatti smart! Tutela la tua privacy su smartphone e tablet.
Online https://www.youtube.com/watch?v=6eF-mwKhrVo&feature=youtu.be+-modulo+smatphone

Garante per la protezione dei dati personali (2016). *App-rova di privacy. I suggerimenti del Garante privacy per un uso consapevole delle app*.
Online https://www.youtube.com/watch?v=MopODAPI5HY

Geracitano, D. & Pilato, S. (2016). Pensa prima di postare.
Online https://www.youtube.com/watch?v=uRxvd8W1qDo&feature=share

Portale giovani protagonisti in Liguria (2013). Come tutelare la privacy sui social network: il video tutorial del Garante dei dati personali.
Online https://www.youtube.com/watch?v=By1mRm-AOmg
Safe Internet Banking. Dave Campaign.
Online https://www.safeinternetbanking.be/en/dave-campaign

Appendice

Questionario Pre-Intervento

Il questionario è stato elaborato nell'ambito del Progetto EDU4SEC - Effective Education for Improving Data Security Awareness è un progetto dell'Università degli Studi di Padova, nato da un gruppo di ricercatori di Pedagogia e Matematica, interessati al tema della data security e alla promozione di comportamenti cosiddetti "sicuri" in rete.

Ti ringraziamo in anticipo della tua collaborazione e ti chiediamo di compilare il seguente questionario relativo a questi temi. Ti invitiamo a rispondere a tutte le domande con la massima sincerità. Tieni presente che non ci sono risposte "giuste" o "sbagliate", ma è importante che tu attinga alla tua personale esperienza quotidiana.

La compilazione ti richiederà all'incirca 5 minuti.

Il questionario è anonimizzato e le informazioni rilevate saranno analizzate esclusivamente in forma aggregata (senza riferimento alla singola persona che ha risposto) a fini statistici e per scopi di ricerca.

Grazie della tua collaborazione, ci stai aiutando a comprendere meglio i comportamenti in materia di data security!

Alcune Informazioni

1. Quale Istituto frequenti?*[1]

- ☐ Istituto Tecnico Commerciale
- ☐ Istituto Tecnico Industriale Settore Tecnologico
- ☐ Liceo Scientifico
- ☐ Liceo Classico
- ☐ Liceo Linguistico
- ☐ Liceo Artistico

1 Gli item contrassegnati da * sono obbligatori.

- ☐ Liceo delle Scienze Applicate
- ☐ Liceo delle Scienze Umane
- ☐ Istituto Professionale Agrario
- ☐ Istituto Professionale per l'Industria e l'Artigianato
- ☐ Istituto Professionale Alberghiero
- ☐ Istituto Tecnico per Geometri
- ☐ Altro:_____

2. Sesso: *
- ☐ Maschio
- ☐ Femmina

3. Età (in cifre): *_____

4. Che tipologia di classe frequenti? *
- ☐ Classe tradizionale
- ☐ Classe digitale

5. A quale anno sei iscritto/a? *
- ☐ Primo
- ☐ Secondo
- ☐ Terzo
- ☐ Quarto
- ☐ Quinto

6. Di quanti membri è composta la tua famiglia? (In cifre) * _____

7. Quanti fratelli e/o sorelle hai? (In cifre) * _____

8. Di che tipo di dispositivi dispone la tua famiglia? *
- ☐ Seleziona tutte le voci applicabili.
- ☐ Smartphone
- ☐ PC
- ☐ Tablet
- ☐ Smart TV
- ☐ Console (es. Wii, WiiU, XboX, PlayStation..)
- ☐ Altro: _____

9. Di quanti dispositivi, considerando quelli indicati sopra, dispone la tua famiglia? Considera anche quelli dei tuoi fratelli/sorelle.
(In cifre) * _____

10. Quanto tempo al giorno trascorri in rete, all'incirca? (In cifre, in ore o frazioni di ora, es. 0,5 ore, 1,5 ore, ecc.) * _____

11. Qual è il dispositivo che utilizzi maggiormente per andare in rete? *

12. Qual è l'eta dei tuoi genitori? Madre (In cifre) * _____

13. Qual è l'eta dei tuoi genitori? Padre (In cifre) * _____

14. Qual è la professione dei tuoi genitori? Madre * _____

15. Qual è la professione dei tuoi genitori? Padre * _____

Sezione Io e le Password

16. Scrivi un esempio di password come di solito la usi (ti invitiamo a non scrivere una password che stai utilizzando al momento) * _____

17. Ora, riscrivi la stessa password cercando di aumentarne la sicurezza. Quali strategie hai utilizzato per renderla più sicura? *
_____

18. Come gestisci le tue password? Fai degli esempi concreti (es. per sceglierle, per ricordarle, per aggiornarle, ecc.) *
_____

Sezione Io e i Social

19. Hai un profilo Facebook? *
☐ Sì
☐ No Passa alla domanda 24.

20. Pensa al tuo profilo Facebook: a tuo avviso, quanto è sicuro? Dove 1 è Per nulla sicuro e 4 è Assolutamente sicuro *
☐ 1
☐ 2
☐ 3
☐ 4

21. Che tipo di informazioni posti? *
Seleziona tutte le voci applicabili

- ☐ Stati in bacheca
- ☐ Posizione (luogo in cui ti trovi)
- ☐ Selfie
- ☐ Foto personali
- ☐ Video personali
- ☐ Recensioni
- ☐ Foto degli amici
- ☐ Notizie dalla rete
- ☐ Video dalla rete
- ☐ Altro: _____

22. Chi può vedere le informazioni che posti? *

- ☐ Tutti
- ☐ Amici e amici di amici
- ☐ Solo i miei amici
- ☐ Solo alcune persone fra i miei amici
- ☐ Non saprei
- ☐ Altro: _____

23. Quando vieni taggato in un post (video, stato, ecc.): *

- ☐ I post in cui sei taggato compaiono automaticamente in bacheca
- ☐ Devi dare il consenso alla pubblicazione dei post prima che appaiano in bacheca
- ☐ Non saprei
- ☐ Altro: _____

24. Possiedi un profilo in altri social (es. Telegram, Twitter, WhatsApp, Instagram, Snapchat, ...)? *

- ☐ Si
- ☐ No Passa alla domanda 28.

25. Pensa ai tuoi profili social: a tuo avviso quanto sono sicuri? *
Dove 1 è Per nulla sicuro e 4 è Assolutamente sicuro *

- ☐ 1
- ☐ 2
- ☐ 3
- ☐ 4

26. Che tipo di informazioni condividi? Fai degli esempi concreti *

_____

27. Chi può avere accesso alle informazioni che condividi tramite questi profili? *

- ☐ Tutti
- ☐ Amici e amici di amici
- ☐ Solo i miei amici
- ☐ Solo alcune persone fra i miei amici
- ☐ Non saprei
- ☐ Altro: _____

Io e Internet

28. Sei mai stato vittima personalmente di episodi di phishing su Internet? *

- ☐ Si Passa alla domanda 29.
- ☐ vNon io personalmente, ma un membro della mia famiglia Passa alla domanda 30.
- ☐ Non io personalmente, ma un mio compagno di classe / amico Passa alla domanda 30.
- ☐ No, né io né alcuna persona che io conosca Passa alla domanda 31.
- ☐ Non so cosa sia il phishing Passa alla domanda 33.

29. Puoi farci un esempio concreto di un episodio in cui sei stato vittima di phishing? *

30. Puoi raccontarci cosa è successo? *

_____

31. Secondo te, il dispositivo che più utilizzi per andare in rete quanto è protetto dal rischio di phishing? Dove 1 è Per nulla protetto e 4 è Assolutamente protetto *

- ☐ 1
- ☐ 2
- ☐ 3
- ☐ 4

32. Come ti proteggi dal phishing? Fai degli esempi concreti *
_____

Sezione Io e le app

33. All'incirca, quante applicazioni (app) hai installato nel dispositivo che utilizzi maggiormente? (In cifre) * _____

34. Quali app utilizzi maggiormente? *
- ☐ Seleziona tutte le voci applicabili.
- ☐ WhatsApp
- ☐ Telegram
- ☐ Instagram
- ☐ Facebook
- ☐ Gmail
- ☐ Twitter
- ☐ Snapchat
- ☐ SmartChat
- ☐ AskUs
- ☐ We Heart it
- ☐ Altro: _____

35. Quanto, secondo te, le app possono risultare una minaccia per i tuoi dispositivi? * Dove 1 è Per nulla e 4 è Moltissimo *
- ☐ 1
- ☐ 2
- ☐ 3
- ☐ 4

36. Solitamente quando installi una app, leggi le note informative prima di effettuare il download? *
- ☐ Si, sempre
- ☐ Si, a volte
- ☐ Raramente
- ☐ No, mai Passa alla domanda 38.

37. A quali aspetti delle note informative presti attenzione? Fai degli esempi concreti * _____

38. Quando installi una app, leggi le recensioni fatte da altri utenti su quell'applicazione? *

- ☐ Si, sempre
- ☐ Si, a volte
- ☐ Raramente
- ☐ No, mai Passa alla domanda 40.

39. A quali aspetti delle recensioni presti attenzione? Fai degli esempi concreti * _____

40. Da dove scarichi le app? *

- ☐ Seleziona tutte le voci applicabili.
- ☐ Store ufficiali
- ☐ Siti internet
- ☐ Altro: _____

41. Ti è capitato di scaricare app da store non ufficiali? *

- ☐ No, mai
- ☐ Si, una volta
- ☐ Si, più di una volta
- ☐ Si, sempre

42. Ti è mai capitato di rifiutare l'installazione di una app? *

- ☐ Si
- ☐ No Passa alla domanda 44.

43. Per quale motivo hai rifiutato l'installazione dell'app? Fai degli esempi concreti * _____

Sezione Io e gli acquisti online

44. All'incirca, quante volte al mese fai acquisti online? (In cifre)* _____

45. Cosa acquisti di solito? *

- ☐ Seleziona tutte le voci applicabili.
- ☐ Musica
- ☐ Videogiochi
- ☐ Dispositivi multimediali (es. console, pc, tv, videocamera, fotocamera, ecc.)

- ☐ Componentistica per pc e console (es. joystick, mouse, adattatori, componenti hardware...)
- ☐ E-book ad uso scolastico
- ☐ E-book per svago
- ☐ Libri formato cartaceo ad uso scolastico
- ☐ Libri formato cartaceo per svago
- ☐ Abbigliamento e accessori personali
- ☐ Biglietti per mezzi di trasporto (pullman, treno, aereo,…)
- ☐ Biglietti per eventi (concerti, teatro...)
- ☐ Prenotazioni alberghi
- ☐ Abbonamenti online (radio, tv, giornali...)
- ☐ Altro: _____

46. Come effettui il pagamento? Puoi indicare anche più di un'opzione *

- ☐ Seleziona tutte le voci applicabili.
- ☐ Utilizzo un account PayPal o una carta prepagata/ricaricabile
- ☐ Utilizzo una carta collegata direttamente al mio conto (o a quello dei miei genitori)
- ☐ Pago in contrassegno (in contanti alla consegna)
- ☐ Pago a mezzo bonifico bancario
- ☐ Altro: _____

47. Nel caso utilizzi modalità diverse (es. a volte in contrassegno, a volte con carta di credito, ecc.), in base a quali criteri scegli la modalità di pagamento? (Se non utilizzi modalità di pagamento diverse, lascia vuota questa risposta e clicca su "Invia")

Questionario Post -Intervento

Alla fine di questo intervento formativo, ti invitiamo nuovamente a rispondere al questionario. Vorremmo, infatti, capire quanto il nostro intervento sia stato efficace e come possiamo migliorarlo affinché questa esperienza con la tua scuola possa essere estesa ad altre scuole del territorio. La compilazione ti richiederà all'incirca 5 minuti.

Grazie ancora della tua collaborazione!

Sezione Io e le Password

1. Scrivi un esempio di password sicura (ti invitiamo a non scrivere una password che stai utilizzando al momento) *

_____

2. A quali elementi hai prestato attenzione nello scrivere questo esempio di password sicura? Fai degli esempi concreti *

_____

3. D'ora in poi cambierai qualcosa nella gestione delle tue password (es. per sceglierle, per ricordarle, per aggiornarle, ecc.)? Fai degli esempi concreti * _____

Sezione Io e i Social

4. Hai un profilo Facebook? *

☐ Sì
☐ No Passa alla domanda 9.

5. Pensa al tuo profilo Facebook: a tuo avviso, quanto è sicuro? Dove 1 è Per nulla sicuro e 4 è Assolutamente sicuro *

☐ 1
☐ 2
☐ 3
☐ 4

6. Ritieni di voler apportare delle modifiche alle impostazioni della privacy del tuo profilo? *

☐ Si Passa alla domanda 7.
☐ No Passa alla domanda 8.

7. Quali modifiche vuoi apportare? Per quali motivi? Fai degli esempi concreti * _____

9. Possiedi un profilo in altri social (es. Telegram, Twitter, WhatsApp, Instagram, Snapchat, ..)? *

☐ Si
☐ No Passa alla domanda 14.

10. Pensa ai tuoi profili social: a tuo avviso, quanto sono sicuri? Dove 1 è Per nulla sicuri e 4 è Assolutamente sicuri *

☐ 1
☐ 2
☐ 3
☐ 4

11. Ritieni di voler apportare delle modifiche alle impostazioni della privacy dei tuoi profili?

☐ Si Passa alla domanda 12.
☐ No Passa alla domanda 13.

12. Quali modifiche vuoi apportare? Per quali motivi? Fai degli esempi concreti * _____

13. Per quali motivi ritieni di non apportare modifiche alle impostazioni di privacy del tuo profilo? * _____

14. Dopo quanto appreso questa mattina, ritieni di avere qualcosa da aggiungere su eventuali episodi di phishing di cui sei stato vittima tu o un tuo conoscente / amico / familiare? Fai degli esempi concreti * _____

15. Secondo te, il dispositivo che più utilizzi per andare in rete quanto è protetto dal rischio di phishing? * Dove 1 è Per nulla protetto e 4 è Assolutamente protetto *

☐ 1
☐ 2
☐ 3
☐ 4

16. Come ti proteggerai dal rischio di phishing? Fai degli esempi concreti * _____

Sezione Io e le app

17. Quanto, secondo te, le app possono risultare una minaccia per i tuoi dispositivi? Dove 1 è Per nulla e 4 è Moltissimo *

- ☐ 1
- ☐ 2
- ☐ 3
- ☐ 4

18. La prossima volta che installerai un'app, a quali elementi presterai attenzione? Fai degli esempi concreti * _____

Io e gli acquisti online

19. D'ora in avanti, come ti comporterai nei tuoi acquisti online? Fai degli esempi concreti * _____

Sezione Io e l'incontro di oggi

20. In quale attività/momento dell'incontro ti sei sentito/a più coinvolto/a? Fai degli esempi concreti* _____

21. C'è qualcosa che hai imparato e di cui assolutamente non avevi mai sentito parlare? Cosa? Fai degli esempi concreti *

_____

Riferimenti bibliografici

Albrechtsen, E., & Hovden, J. (2010). Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. *Computers & Security, 29*(4), 432-445.

Arcella, R. (2017). *Firme digitali: che cosa cambia con eIDAS*. Online https://www.cspt.pro/pct/firme-digitali-che-cosa-cambia-con-eidas-di-roberto-arcella/

Bada, M., & Sasse, A. (2014). Cyber security awareness campaigns: Why do they fail to change behaviour?. Global Cyber Security Capacity Centre, University of Oxford: Oxford, UK. Consultabile all'indirizzo http://discovery.ucl.ac.uk/-1468954/1/Awareness%20CampaignsDraftWorkingPaper.pdf

Bonaiuti, G., Calvani, A., Menichetti, L., & Vivanet, G. (2017). *Le tecnologie educative*. Roma: Carocci.

Bonaiuti, G., & Ricciu, R. (2017). Mobile devices to increase attention and improve learning. *Form@re - Open Journal per la formazione in rete, 17*(1), 190-203. Consultabile all'indirizzo http://www.fupress.net/index.php/-formare/article/view/20470/19074

Bracci, F. (2017*). L'apprendimento adulto. Metodologie didattiche ed esperienze trasformative*. Milano: Unicopli.

Bracci, F., & Romano, A. (2018). Educare al pensiero critico e creativo. In C. Tino & D. Frison (eds.), *Employability skills. Riflessioni e strategie per la scuola secondaria* (pp. 96-108). Milano: Pearson Academy.

Bruff, D. (2014*). Classroom response system ('clickers') bibliography*. Retrieved form https://cft.vanderbilt.edu/docs/classroom-response-system-clickers-bibliography/

Burattin, A., Cascavilla, G., & Conti, M. (2014). Socialspy: Browsing (supposedly) hidden information in online social networks. *International Conference on Risks and Security of Internet and Systems*, 83-99.

Calvani, A. (2017). Mente e media. Quale interazione cognitiva per apprendere.

In G. Bonaiuti, A. Calvani, L. Menichetti, e G. Vivanet, *Le tecnologie educative* (pp. 17-45). Roma: Carocci.

Cañas, A. J., Coffey, J. W., Carnot, M. J., Feltovich, P., Hoffman, R. R., Feltovich, J., & Novak, J. D. (2003). *A summary of literature pertaining to the use of concept mapping techniques and technologies for education and performance support*. Consultabile all'indirizzo https://eventos.unipampa.edu.br/seminario-docente/files/2011/03/Oficina-9-A-Summary-of-Literature-Pertaining-to-the-Use-of-Concept.pdf

Cascavilla, G., Conti, M., Frison, D., & Surian, A. (2017). Data Security Awareness: metodi e strumenti per promuoverla nella scuola secondaria. Il caso del progetto Edu4Sec. *MEDIA EDUCATION – Studi, ricerche, buone pratiche, 8*(2), 276-284

Cattaneo, N. A., & De Conti, M. (2018). Saper comunicare e saper parlare in pubblico: due distinte competenze. In C. Tino & D. Frison (a cura di), *Employability skills. Riflessioni e strategie per la scuola secondaria* (pp. 46-58). Milano-Torino: Pearson Italia.

Cheong, C., Cheong, F., & Filippou, J. (2013). Quick Quiz: A Gamified Approach for Enhancing Learning. *Pacific Asia Conference on Information Systems (PACIS) 2013 Proceedings*. Consultabile all'indirizzo http://aisel.aisnet.org/pacis2013/206

Comoglio, M. (1996). *Insegnare e apprendere in gruppo. Second Cooperative learning*. Roma: LAS.

Conti, M. et al. (2015). Can't you hear me knocking: Identification of user actions on Android apps via traffic analysis. *Proceedings of the 5th ACM Conference on Data and Application Security and Privacy 2*, 297-304.

Cornetti, M. (2016). *Gamification Design: A Starting Point*. Consultabile all'indirizzo http://www.aedu.tech/category/international/monica-cornetti/

Coryell, J. E. (2016). Active learning and interactive lectures. In M. Fedeli, V. Grion, & D. Frison (Eds.), *Coinvolgere per apprendere. Metodi e tecniche partecipative per la formazione* (pp. 143-166). Lecce: Pensa MultiMedia.

De Conti, M., & Giangrande, M. (2017). *Debate. Pratica, teoria e pedagogia.* Milano-Torino: Pearson Italia.

Detering, S., Dixon, D., Khaled, R., & Nacke, L. (2011). From game design elements to gamefulness: defining "gamification". *Proceedings of the 2011 MindTrek Conference*. Consultabile all'indirizzo http://85.214.46.140/niklas/bach/MindTrek_Gamification_PrinterReady_110806_SE_accepted_LEN_changes_1.pdf

Dewey, J. (1949). *Scuola e società*. Firenze: La Nuova Italia. Ed. Or. (1900). *The school and society*. Chicago: The University of Chicago Press.

Di Nubila, R. D. & Fedeli, M. (2010). *L'esperienza: quando diventa fattore di formazione e di sviluppo: dall'opera di David A. Kolb alle attuali metodologie di Experiential Learning Testimonianze e case study*. Lecce: Pensa MultiMedia.

Eurostat (2018). Digital economy and society statistics - households and individuals. Consultabile all'indirizzo http://ec.europa.eu/eurostat/statistics-explained/index.php/Digital_economy_and_society_statistics_-_households_and_individuals#Internet_usage

Fabbri, L. (2007). *Comunità di pratiche e apprendimento riflessivo: per una formazione situata*. Roma: Carocci.

Faria, A. J. (2001). The changing nature of business simulation/gaming research: A brief history. *Simulation & Gaming, 3*(1), 97-110.

Fantacone, F.(2016). *Gamification: adesso giochiamo sul serio!* Consultabile all'indirizzo http://www.aedu.tech/intervista-1-federico-2/

Fedeli, M. (2011). Dalla metodologia alle metodologie esperienziali. Nuove sfide per i formatori. *FOR Rivista per la formazione*, 86(2011), 32-37. doi: 10.3280/FOR2011-086005

Fedeli, M. (2012). Il valore dell'esperienza nelle pratiche formative. *Quaderni di Economia del Lavoro*, 14, 95-108. doi: 10.3280/QUA2012-097007

Fedeli, M., Grion, V., & Frison, D. (Eds.). (2016). *Coinvolgere per apprendere. Metodi e tecniche partecipative per la formazione*. Lecce: Pensa Multimedia.

Fedeli, M., Frontani, L., & Mengato, L. (Eds.). (2015). *Experiential learning. Metodi, tecniche e strumenti per il debriefing*. Milano: FrancoAngeli.

Frison, D. & Surian, A. (2018). Come incoraggiare Data Security Awareness. Il caso del progetto Edu4Sec. *Qwerty, 13*(2), 83-107. DOI : 10.30557/QW-000006

Frison, D., Tino, C., & Fedeli, M. (2018). L'adozione di un additional collaborative tool nell'insegnamento in lingua veicolare: un'esperienza con Padlet. *Exellence and Innovation in Learning & Teaching*, 2, 73-87. 10.3280/EXI2018-002005

Glatthorn, A. A. (1999). *Performance standards and authentic learning*. Larchmont, NY: Eye on Education.

Hoover, J. D., Whitehead, C. J. (1975). An experiential-cognitive methodology in the first course in management: some preliminary results. *Simulation Games and Experiential Learning in Action, 2*, 25-30.

Il Sole 24 Ore. (2018). *Fake news: quando le bugie hanno le gambe lunghe*. Online https://www.infodata.ilsole24ore.com/2018/05/04/fake-news-le-bugie-le-gambe-lunghe/?refresh_ce=1

ISTAT (2017). Cittadini, imprese e ICT. Retrived from https://www.istat-.it/it/files//2017/12/ICT_Anno2017.pdf

Johnson, D. W., & Johnson, R. T. (1987). *Learning together and alone: Cooperative, competitive, and individualistic learning*. Prentice-Hall, Inc.

Kapp, K. M. (2006). *Bridging the boomer/gamer knowledge gap*. Consultabile all'indirizzo http://www.karlkapp.com.

Kapp, K. M. (2012). *The Gamification of Learning and Instruction: Game-Based Methods and Strategies For Training And Education*. San Francisco: Pfeiffer.

Kolb, D. A. (1984). *Experiential Learning: Experience as the source of learning and development*. Englewood Cliffs, NJ: Prentice Hill.

Kolb, D. A., Boyatzis, R. E., & Mainemelis, C. (1999). Learning Theory: Previous Research and New Directions. Consultabile all'indirizzo http://learningfromexperience.com/media/2010/08/experiential-learning-theory.pdf

Korpela, K. (2015). Improving cyber security awareness and training programs with data analytics. *Information Security Journal: A Global Perspective, 24*(1-3), 72-77.

Lave, J., & Wenger, E. (1991). *Situated learning: Legitimate peripheral participation*. Cambridge, UK: Cambridge University Press. (Trad. it., *L'apprendimento situato. Dall'osservazione alla partecipazione attiva nei contesti sociali,* Trento, Erickson, 2006).

Ligorio, M. B. (2003). *Come si insegna, come si apprende.* Roma: Carocci.

Longo, A., & Natale, R. (2018). GDPR, tutto ciò che c'è da sapere per essere in regola. Online https://www.agendadigitale.eu/cittadinanza-digitale/gdpr-tutto-cio-che-ce-da-sapere-per-essere-preparati/

Mathieson, K. (1991). Predicting user intentions: comparing the technology acceptance model with the theory of planned behavior. *Information systems research, 2*(3), 173-191.

Merriam, S. B., Caffarella, R. S., & Baumgartner, L. M. (2007). *Learning in adulthood: A comprehensive guide*. San Francisco: Jossy-Bass.

Mortari, L. (2003). *Apprendere dall'esperienza: il pensare riflessivo nella formazione*. Roma: Carocci.

Novak, J. D. (1990). Concept mapping: A useful tool for science education. *Journal of research in science teaching, 27*(10), 937-949.

Novak, J. D. (2001). *L'apprendimento significativo: le mappe concettuali per creare e usare la conoscenza*. Trento: Erickson.

Novak, J. D., Bob Gowin, D., & Johansen, G. T. (1983). The use of concept mapping and knowledge vee mapping with junior high school science students. *Science education, 67*(5), 625-645.

Poirier, C. R., & Feldman, R. S. (2007). Promoting active learning using individual response technology in large introductory psychology classes. *Teaching of psychology, 34*(3), 194-196.

Ranieri, M., Bruni, I., & Raffaghelli, J. E. (2018). Gli Student Response System nelle aule universitarie: esperienze d'uso e valore formativo. *Lifelong Lifewide Learning, 14*(31), 96-109.

Rotondi, M. (2004a). *Facilitare l'apprendere: modi e percorsi per una formazione di qualità*. Milano: FrancoAngeli.

Rotondi, M. (2004b). *Formazione outdoor: apprendere dall'esperienza. Teorie, modelli, tecniche, best practices*. Milano: FrancoAngeli.

Ruighaver, A. B., Maynard, S. B., & Chang, S. (2007). Organisational security culture: Extending the end-user perspective. *Computers & Security, 26*(1), 56-62.

Schön, D. A. (1983). *The reflective practitioner*. New York: Basic Books (Trad. it., *Il Professionista riflessivo: per una nuova epistemologia della pratica professionale*, Bari, Dedalo, 1993).

Slavin, R. E. (1991). *Student team learning: A practical guide to cooperative learning*. West Haven, CT: National Education Association Professional Library.

Sobiesk, E., Blair, J., Conti, G., Lanham, M., & Taylor, H. (2015). Cyber education: a multi-level, multi-discipline approach. In *Proceedings of the 16th Annual Conference on Information Technology Education* (pp. 43-47). Consultabile all'indirizzo http://www.gregconti.com/publications/p43-sobiesk.pdf

Stokes, B. (2005). Videogames have changed: time to consider Serious Games? *The Development Education Journal, 11*(2).

Swain, A., & Guttman, H. (1983). *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications*. Washington, DC: Nuclear Regulatory Commission.

Tessaro, F. (2015). Compiti autentici o prove di realtà? *Formazione & Insegnamento, 12*(3), 77-88.

Tosoni, L. (2018). *Direttiva NIS, così è l'attuazione italiana (dopo il recepimento): i punti principali del decreto*. Online https://www.agendadigitale.-eu/sicurezza/attuazione-della-direttiva-nis-lo-lo-schema-decreto-legislativo/

Troiano, G. (2018). *Privacy, cosa sono le direttive 680 e 681 e quali rischi ci sono*. Online https://www.agendadigitale.eu/sicurezza/guglielmo-troiano-direttiva-680-e-681/

U.S. Department of Commerce, Economics and Statistics Administration, U.S. CENSUS BUREAU, The Older Population: 2010. Retrieved online http://www.census.gov/prod/cen2010/briefs/c2010br-09.pdf

Waly, N., Tassabehji, R., & Kamala, M. A. (2012). Measures for improving information security management in organisations: the impact of training and awareness programmes. Consultabile all'indirizzo:

https://pdfs.semanticscholar.org/207e/648e5c42721817b0d10b4dc5e600-acc2c1ad.pdf

Wang, A. I. (2015). The wear out effect of a game-based student response system. *Computers & Education, 82*, 217-227.

Warman, A. R. (1992). Organizational computer security policy: the reality. *European Journal of Information Systems, 1*(5), 305-10.

Wenger, E. (1998). *Communities of practice: Learning, meaning, and identity*. Cambridge, UK: Cambridge University Press.

Wilson, M., & Hash, J. (2003). Building an information technology security awareness and training program. *NIST Special publication, 800*(50), 1-39. Consultabile all'indirizzo http://citadel-information.com/wp-content/uploads/2012/08/nist-sp800-50-building-information-security-awareness-program-2003.pdf

Ringraziamenti

Il progetto Edu4Sec si è strutturato intorno alla collaborazione fertile e generativa con dirigenti scolastici e animatori e animatrici digitali e con le nostre colleghe e i nostri colleghi di Dyaloghi, Spin-off dell'Università di Padova.

Al prof. Mauro Conti, professore ordinario presso il Dipartimento di Matematica dell'Università di Padova e al dott. Giuseppe Cascavilla, Dottorando del Dipartimento di Matematica dell'Università di Padova, va il nostro ringraziamento per lo scambio fruttuoso sollecitato dall'incontro tra i nostri rispettivi ambiti disciplinari.

Il nostro grazie va anche al dott. Angelo Canal, che ha dedicato al Progetto Edu4Sec la propria tesi di laurea magistrale in Management dei Servizi Educativi e Formazione Continua e ha contribuito attivamente alla conduzione dei focus-group e degli interventi formativi a scuola.

Infine, il nostro ringraziamento si rivolge agli studenti e alle studentesse che hanno attivamente partecipato alla realizzazione di Edu4Sec, mettendosi in gioco e condividendo esperienze e comportamenti personali e delle proprie famiglie sul tema della *data security.* A tutti loro va il nostro sentito grazie per averci fatto entrare nelle loro "abitudini online"!

Alessio Surian e *Daniela Frison*

Cresce la consapevolezza dell'importanza di un utilizzo più informato di Internet e delle tecnologie digitali. Si tratta, da un lato, di adeguare e aggiornare le normative e la loro attuazione, per esempio in relazione al Regolamento Generale sulla Protezione dei Dati Personali (GDPR), dall'altro, del promuovere un atteggiamento attento e critico da parte di chi naviga e maneggia le tecnologie digitali. Il volume intende sostenere chi si propone di introdurre, nei percorsi di chi studia e di chi lavora, momenti formativi che possano fornire un lessico di base ed occasioni di aggiornamento in merito ai fattori di rischio e ai comportamenti da monitorare e adottare per prevenire ed intervenire su questioni di *data security*. Più in generale, offre dati, riflessioni e proposte formative per fare i conti con la nostra *intelligenza digitale* e con la nostra consapevolezza in materia di privacy e sicurezza informatica intrecciando questi temi con quello della formazione in chiave esperienziale e trasformativa.

9 788867 606290

pensamultimedia.it