DATA SECURITY AWARENESS: METODI E STRUMENTI PER PROMUOVERLA NELLA SCUOLA SECONDARIA. IL CASO DEL PROGETTO EDU4SEC

DATA SECURITY AWARENESS: METHODS AND TOOLS TO PROMOTE IT IN SECONDARY SCHOOL. THE CASE OF THE EDU4SEC PROJECT

Giuseppe Cascavilla, Sapienza Università di Roma, cascavilla@di.uniroma1.it
Mauro Conti, Università di Padova, conti@math.unipd.it
Daniela Frison, Università di Padova, daniela.frison@unipd.it
Alessio Surian, Università di Padova, alessio.surian@unipd.it

SOMMARIO

Il contributo presenta la cornice teorica e metodologica e l'articolazione del progetto *Edu4Sec – Effective Education for Improving Data Security Awareness* attivato nel 2016 presso l'Università di Padova con l'obiettivo di promuovere, negli studenti delle scuole secondarie di secondo grado, consapevolezza circa i rischi che si possono correre in rete ed i comportamenti più efficaci per prevenire e far fronte a tali rischi.

PAROLE CHIAVE

Data Security, Data Security Awareness, Experiential Learning, Cooperative Learning, Scuola Secondaria di Secondo Grado

MEDIA EDUCATION – Studi, ricerche, buone pratiche
http://riviste.erickson.it/med

ISSN 2038-3002 – Vol. 8, n. 2, anno 2017, pp. 276-284

ABSTRACT

The paper presents the theoretical and methodological framework and the activities proposed by the *Edu4Sec Project – Effective Education for Improving Data Security Awareness*. Since 2016 the project is being implemented by a multidisciplinary team based at the University of Padova. The training project aims at improving data security awareness in secondary school students in order to encourage effective behaviours to prevent cyber risks and to deal with data security issues.

KEYWORDS

Data Security, Data Security Awareness, Experiential Learning, Cooperative Learning, Secondary Education

Autore per corrispondenza

Giuseppe Cascavilla, Dipartimento di Informatica, Sapienza Università di Roma, Via Salaria 113 - 00198 Roma, cascavilla@di.uniroma1.it

LUOGO: Padova e provincia, 3 Istituti Secondari di Secondo Grado
UTENTI: 12 classi, 4 per ogni istituto, un totale di 256 partecipanti
DURATA PROGETTO: a.s. 2016-17, novembre 2016-gennaio 2017
MATERIALI E TECNOLOGIE: PC, videoproiettore, scanner, schede e colori per le attività previste
PRODOTTO IN CORSO DI REALIZZAZIONE: manuale open source del Progetto *Edu4Sec*

1 Introduzione

Nei comportamenti sociali e lavorativi, attraversiamo frequentemente, oltre allo spazio fisico, anche il «cyber» spazio, quello che ci vede variamente connessi a persone e programmi software tramite collegamenti Internet. La rete è entrata a fare parte dei contesti e dei comportamenti quotidiani e sollecita consapevolezza e abilità specifiche. In almeno cinque ambiti siamo sollecitati a sviluppare e aggiornare competenze relative ai contesti digitali in rete: la navigazione, la creazione di contenuti, la dimensione mobile, le reti sociali, le funzioni operative (Helsper & Eynon, 2013).

Trasversale a queste cinque aree di competenza è la dimensione della *data security*. I collegamenti in rete possono essere sia potenziali fonti di condivisione e collaborazione, ma anche minacce e intrusioni nella nostra vita. L'ambito della *data security* si traduce in una costellazione di temi e rimandi: l'accesso ai dati, l'identità digitale, la privacy, l'Agenda Digitale, ecc. Se, da un lato, sono sempre più necessarie competenze specifiche, e quindi specialisti, per creare sistemi informatici che funzionino in modo da proteggere chi agisce nel cyber-spazio, dall'altro è importante che i concetti chiave alla base di tali competenze possano essere condivisi in modo generativo con chiunque navighi in Internet, in modo da migliorare rapidamente il grado di consapevolezza e il tipo di atteggiamenti utili a prevenire inconvenienti e minacce in rete. In tale direzione, è importante la capacità di affinare progressivamente i comportamenti quotidiani da parte degli utenti e la messa a fuoco di 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.

Cosa intendiamo, dunque, quando parliamo di *data security* e di *data security awareness*, con riferimento alla consapevolezza rispetto ai comportamenti che generano rischi?

Possiamo definire la *Data Security e* la *Data Security Awareness* come due facce della stessa medaglia. Se da una parte la comunità scientifica informatica continua il processo di sviluppo di nuove tecniche e di nuovi strumenti per garantire la *Data Security* (sicurezza dei nostri dati), dall'altra parte è oggigiorno fondamentale sensibilizzare gli utenti alle problematiche derivanti da una divul-

ISSN 2038-3002 – Vol. 8, n. 2, anno 2017, pp. 276-284

gazione involontaria di dati sensibili, e informarli circa la disponibilità di alcuni strumenti e buone pratiche per proteggere la privacy e la sicurezza dei sistemi.

Più nel dettaglio, la *Data Security* è quel ramo dell'informatica che si occupa della protezione dei dati sensibili, personali o aziendali, attraverso lo sviluppo di nuovi strumenti e strategie per la rilevazione di minacce informatiche o accessi non autorizzati (https://www.its.bldrdoc.gov/fs-1037/dir-010/_1443.htm). Un esempio di tecnologie di *Data Security* sono la cifratura dei dati sensibili e l'autenticazione degli utenti, che può avvenire attraverso l'uso di passphrase per l'autenticazione, più semplicemente note come passwords.

Diversamente, la *Data Security Awareness* si occupa della divulgazione delle problematiche legate alla *Data Security* e alle strategie di prevenzione. Lo scopo principale della *Data Security Awareness* è quello di creare consapevolezza nelle persone di qualsiasi grado e estrazione sociale sulle varie criticità dovute a una scarsa attenzione della gestione dei propri dati e di quelli di terzi (https://securityintelligence.com/cybersecurity-awareness-is-about-both-knowing-and-doing/). La *Data Security Awareness* ha dunque il compito di educare e sensibilizzare gli utenti all'uso corretto delle tecnologie informatiche fornendo strumenti per prevenire e ridurre un'eventuale divulgazione involontaria di dati sensibili.

2 Obiettivi del progetto Edu4Sec – Effective Education for Improving Data Security Awareness

Formare alla *Data Security* e incoraggiare la *Data Security Awareness*: sono questi gli obiettivi del 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. Più precisamente, con riferimento agli studenti della scuola secondaria di secondo grado, target di riferimento dell'esperienza qui descritta, il progetto si è proposto i seguenti obiettivi:

- incoraggiare la collaborazione scuola-università;
- favorire negli studenti la conoscenza dei rischi che si possono correre nel cyber-spazio;
- favorire e valorizzare la condivisione delle «cyber-esperienze» vissute dagli studenti;
- incoraggiare il peer learning;
- incoraggiare una cultura della *data security*;
- fornire ai docenti informazioni, materiali e una proposta formativa da sviluppare e replicare in autonomia.

Come perseguire tali obiettivi? Come educare ragazzi, studenti, ma anche adulti, professionisti alla percezione dei rischi che possono correre in rete? A

riconoscerli? Ciò è particolarmente rilevante in merito agli strumenti che quotidianamente maneggiano per comunicare, giocare, relazionarsi con i pari, fare acquisti, per compiere dunque azioni comuni della quotidianità.

3 La cornice teorica

La progettazione didattica di interventi rivolti specificamente alla scuola secondaria di secondo grado si è ispirata ad alcune teorie e modelli di apprendimento.

Un primo riferimento riguarda il modello dell'apprendimento esperienziale (experiential learning) (Kolb, 1984; Kolb, Boyatzis & Mainemelis, 1999), che vede il processo di apprendimento realizzarsi attraverso l'azione e la sperimentazione di situazioni che vedono il soggetto quale attivo protagonista di fasi diverse. Noto è il cosiddetto learning circle tracciato da Kolb (1984), che ha attribuito all'apprendimento esperienziale una forma ciclica che parte dall'esperienza concreta passando per l'osservazione riflessiva e la concettualizzazione astratta, per giungere infine alla sperimentazione attiva. Da un punto di vista metodologico, questo approccio offre stimoli interessanti per la progettazione formativa di metodi e tecniche ad esso ispirati: dalla proposta di learning game o di attività ludico-metaforiche che favoriscano l'immersione nel problema, tema o concetto oggetto di lavoro e formazione e la sua sperimentazione e manipolazione attiva, all'osservazione e riflessione sull'esperienza vissuta mediante domande chiave per riflettere sulla tematica, discussioni in piccoli gruppi, storytelling (Coryell, 2016).

Un secondo riferimento a sostegno di una progettazione formativa che incoraggi la presa di consapevolezza in merito ai comportamenti rischiosi è l'approccio dell'apprendimento situato (situated learning) (Lave & Wenger, 1991; Wenger, 1998), che evidenzia la dimensione contestuale dell'apprendimento. Sul tema della data security appare pertinente stabilire connessioni tra apprendimento ed esperienza che gli studenti sviluppano nella loro vita quotidiana. Guardare all'apprendimento da questa prospettiva invita a favorire in aula situazioni il più possibile vicine ai contesti quotidiani degli studenti: situazioni «autentiche». Si ispirano a questo approccio role play, casi studio, simulazioni, scenari che provengano dal mondo reale e che vengono riproposti in aula.

Il terzo approccio preso qui in considerazione è quello del cooperative e peer-to-peer learning (Comoglio, 1996; Johnson & Johnson, 1987): una metodologia didattica che favorisce lo sviluppo delle competenze sociali e il lavoro in piccoli gruppi. 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, materia o curricolo, con obiettivi che intersechino l'imparare a relazionarsi e a lavorare in contesti complessi ed eterogenei, come spesso richiesto dalla società e dalle modalità lavorative contemporanee (Comoglio, 1996; Slavin, 1991).

ISSN 2038-3002 – Vol. 8, n. 2, anno 2017, pp. 276-284

4 L'articolazione del progetto

Nell'ambito del progetto *Edu4Sec* sono stati progettati e realizzati moduli formativi rivolti a studenti della scuola secondaria di secondo grado. In fase esplorativa, sono stati condotti 3 focus-group con 36 studenti afferenti a 3 Istituti Superiori di Secondo Grado del territorio di Padova e provincia e interviste semi-strutturate con 2 Animatori Digitali, al fine di orientare la progettazione degli interventi formativi presso gli stessi istituti durante l'anno scolastico 2016/2017.

Gli stessi 3 Istituti sono stati coinvolti, tra novembre 2016 e gennaio 2017, in una sperimentazione a cui hanno preso parte 12 classi, 4 per ogni istituto, così ripartite: 1 classe seconda, 7 classi terze e 4 classi quarte, per un totale di 256 partecipanti. Ciascuna classe ha beneficiato di un intervento formativo della durata di 2 ore scolastiche (corrispondenti a una durata media di 105 minuti).

A un primo gruppo (6 classi, 2 per ogni istituto, per un totale di 140 studenti coinvolti) è stato proposto un intervento che ha previsto attività e tecniche ispirate alle teorie e modelli di apprendimento precedentemente illustrati.

A un secondo gruppo (sempre 6 classi, 2 per ogni istituto, per un totale di 116 studenti coinvolti) è stato proposto un intervento che ha previsto le medesime attività e tecniche e, oltre ad esse, l'inserimento di elementi di gamification (Detering et al., 2011; Kapp, 2012) con l'obiettivo di rilevare eventuali differenze significative nei gruppi coinvolti in termini di conoscenze e previsioni/intenzioni di comportamento dopo l'intervento.

5 I contenuti dei moduli formativi

I moduli formativi proposti hanno sviluppato le aree tematiche di seguito illustrate, centrali in materia di *Data Security* e al contempo vicine all'esperienza quotidiana degli studenti secondo quanto rilevato mediante i focus group:

1. «Internet: rischi e pericoli». Quest'area tematica ha evidenziato 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.
2. «e-Commerce: shopping in sicurezza», con riferimento ai rischi derivanti dallo shopping online: come evitare acquisti indesiderati o truffe online. Ha offerto, inoltre, 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.
3. «Password: la nostra difesa», con riferimento alle problematiche derivanti dalla scelta di una password inappropriata e poco sicura e i rischi che potrebbero insorgere. Essa si è posta l'obiettivo di mostrare quali sono i criteri alla base della scelta di una password che può essere definita sicura.
4. «Smartphone: sono veramente smart?». Quest'area tematica ha evidenziato 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 manie-

ISSN 2038-3002 – Vol. 8, n. 2, anno 2017, pp. 276-284

ra chiara e attraverso esempi pratici le minacce derivanti da una app malevola o da un utilizzo improprio dello smartphone evidenziando poi possibili rimedi per evitare eventuali fuoriuscite di informazioni private.
5. «Social Network: privacy & security» ed esempi concreti sulle varie problematiche relative alla privacy e alla sicurezza dei propri dati derivanti da un uso incauto dei social networks. Dopo aver affrontato le varie problematiche, in quest'area sono stati presentati i comportamenti da seguire nei social network per evitare problemi relativi alla privacy.

6 Le attività e le tecniche proposte

Coerentemente con le aree tematiche sopra descritte e con l'approccio esperienziale che il progetto ha inteso promuovere in aula, sono state progettate e proposte attività ad hoc.

1. La prima area tematica dedicata a «Internet: rischi e pericoli» è stata introdotta da un'attività di discussione di gruppo. Agli studenti è stato chiesto di classificare, in gruppi di 4/5 secondo la composizione della classe, i rischi più diffusi relativamente alle 5 aree tematiche proposte.
2. La seconda area tematica dedicata «e-Commerce: shopping in sicurezza» è stata introdotta da un Learning Game a cui gli studenti hanno potuto accedere dalla piattaforma Moodle dell'ateneo di Padova. Tale attività è stata proposta al solo gruppo che ha beneficiato del modulo integrato con elementi di gamification.
3. La terza area tematica «Password: la nostra difesa» è stata introdotta da un quiz elaborato mediante la piattaforma di game-based learning, Kahoot.it. Il quiz è stato proposto al solo gruppo che ha beneficiato del modulo integrato con elementi di gamification.
4. La quarta e quinta area tematica dedicate a Smartphone e Social Network sono state introdotte da un role-play volto alla drammatizzazione di eventi vissuti direttamente dal gruppo di studenti coinvolti o a loro noti perché vissuti da compagni di scuola, amici, conoscenti, sui temi della sicurezza nell'uso degli smartphone e nei social network.

Secondo un approccio esperienziale, ciascuna delle attività proposte ha preceduto una mini-lecture sull'area tematica di riferimento.

7 Strumenti di valutazione pre- e post- intervento formativo

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

ISSN 2038-3002 – Vol. 8, n. 2, anno 2017, pp. 276-284

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 dopo la partecipazione al modulo formativo. I questionari, somministrati mediante Google Moduli, hanno proposto sia domande aperte sia domande chiuse a scelta multipla a una sola risposta o a più risposte, proponendo batterie di domande collegate alle aree tematiche proposte: «Io e le Password», «Io e Facebook», «Io e i Social», «Io e Internet», «Io e le App», «Io e gli acquisti online». I dati raccolti sono attualmente in fase di analisi e orienteranno futuri interventi formativi sulla promozione della *Data Security Awareness.*

8 Conclusioni

Edu4Sec è oggi in grado di offrire moduli di 60' o 120' che sollecitano l'attenzione degli studenti delle scuole secondarie di secondo grado riguardo ai temi della *data security*. Tali strumenti sono a disposizione di insegnanti e animatori digitali. Le attività e gli strumenti proposti agli studenti sono stati condivisi con gli animatori digitali, ex-ante, mediante un momento formativo ad essi destinato e gli stessi sono stati coinvolti, ove possibile, nella gestione e conduzione delle attività. In alcuni casi, sono stati anche discussi insieme a insegnanti e animatori digitali in incontri di verifica degli interventi condotti nell'ambito del progetto.

La verifica ha riguardato le modalità del percorso formativo svolto in classe e gli effetti dell'azione formativa in relazione alle conoscenze palesate dagli studenti tramite il questionario auto-percettivo compilato prima e dopo l'intervento. Insegnanti e animatori digitali dispongono anche di un *Manuale Edu4Sec* che è stato redatto per incoraggiarli a farsi promotori, in collaborazione con i colleghi, di iniziative volte a sensibilizzare gli studenti sulla importanza della *Data Security* e a trarre spunto dalle proposte formative elaborate per valorizzare eventi, esperienze, riflessioni dei loro studenti su tematiche che sono parte integrante della loro quotidianità.

L'analisi dei dati raccolti mediante focus group e questionari sarà oggetto di ulteriori comunicazioni scientifiche. Ciò consentirà una più ampia valutazione degli interventi formativi realizzati e orienterà la progettazione di nuovi interventi negli Istituti già coinvolti e in altri interessati durante l'anno scolastico 2017-2018.

Bibliografia

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

Conti, M., Mancini, L. V., Spolaor, R., & Verde, N. V. (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.

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* (143-166). Lecce: Pensa MultiMedia.

Detering, S., Dixon, D., Khaled, R., & Nacke, L. (2011). From game design elements to gamefulness: defining «gamification». *Proceedings of the 2011 MindTrek Conference*, http://85.214.46.140/niklas/bach/MindTrek_Gamification_PrinterReady_110806_S E_accepted_LEN_changes_1.pdf [Accesso 03/10/2017].

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

Helsper, E., & Eynon, R. (2013). Distinct skill pathways to digital engagement. *European Journal of Communication*, *28*(6), 696-671.

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

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*, http://learningfromexperience.com/media/2010/08/experiential-learning-theory.pdf [Accesso 03/10/2017].

Lave, J., & Wenger, E. (1991). *Situated learning: Legitimate peripheral participation*. Cambridge, UK: Cambridge University Press.

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

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

Sitografia

ITS – Institute for Telecommunication Sciences – https://www.its.bldrdoc.gov/fs-1037/dir-010/_1443.htm [Accesso 03/10/2017].

Security Intelligence – Analysis and Insight for Information Security Professionals – https://securityintelligence.com/cybersecurity-awareness-is-about-both-knowing-and-doing [Accesso 03/10/2017].

ISSN 2038-3002 – Vol. 8, n. 2, anno 2017, pp. 276-284