Open and Interdisciplinary
Journal of Technology,
Culture and Education

Publisher
Progedit, via De Cesare, 15
70122, Bari (Italy)
tel. 080.5230627
fax 080.5237648
info@progedit.com
www.progedit.com

qwerty.ckbg@gmail.com
http://www.ckbg.org/qwerty

Registrazione del Tribunale di Bari
n. 29 del 18/7/2005

ISSN 2240-2950

Indice

Come incoraggiare Data Security Awareness? Il caso del progetto Edu4Sec

Daniela Frison, Alessio Surian**
DOI: 10.30557/QW000006

Abstract

This paper presents a set of data generated and analyzed by the *Edu4Sec Project – Effective Education for Improving Data Security Awareness*. The project commenced in 2016 and is being implemented by a multidisciplinary team based at the University of Padova. The aim is to improve secondary school students' data security awareness and develop behaviors and strategies to reduce cyber risks arising from data security issues. Three secondary schools have been involved in a quasi-experimental research design. A training intervention was provided to 116 students engaged in experiential and interactive learning activities related to key concepts of data security. The same intervention was provided to the experimental group of 140 students, supplemented by *gamification* elements. The paper focuses on the pre- and post-intervention questionnaire results.

* Università di Padova.
Corresponding author: daniela.frison@unipd.it

Keywords: Data Security Awareness; Learning by Doing; Secondary School; Quasi-Experimental Design

1. Introduzione

L'uso di dispositivi quali smartphone, computer e tablet e l'accesso, tramite essi, alla rete, per frequentare i social network o realizzare online il nostro shopping, è attività quotidiana per una percentuale sempre più ampia di popolazione. In questa nostra cyber-quotidianità, quanto sappiamo dei rischi che possiamo correre in rete? Quanto siamo in grado di adottare comportamenti che proteggano i nostri dispositivi da virus e malware e i nostri dati personali da saccheggi e frodi? L'Eurobarometro 431 (Directorate-General for Justice and Consumers, 2015) rileva che, nell'UE, oltre la metà degli intervistati (57%) non ritiene questione secondaria il "fornire informazioni personali" e che la maggioranza delle persone si sentono a disagio sapendo che gestori di servizi Internet utilizzano informazioni fornite durante le attività online per inviare informazioni pubblicitarie mirate. L'Eurobarometro rileva, anche, che vengono fornite informazioni personali soprattutto per effettuare pagamenti e per farsi recapitare acquisti.

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 genesi di questi sforzi, in termini di ricerca, analisi e sperimentazioni, sia stata soprattutto informatica e abbia osservato la *data security* 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 cospicua letteratura internazionale che guarda alla *data security* da un punto di vista informatico e le più limitate, ma in aumento, risorse che guardano ad essa da una prospettiva olistica che attribuisca 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 ai comportamenti dei molteplici utenti della rete, riconosciuti come attori protagonisti delle performance di sicurezza (Albrechtsen & Hovden, 2010). In particolare, in ambito organizzativo, questo approccio sta generando riflessioni e sperimentazioni volte a identificare adeguati moduli formativi: ne è un esempio Cybersecurity, modulo online di otto settimane offerto da HarvardX[1]. Di particolare importanza è identificare i fattori che possono influenzare gli attacchi informatici a scapito di singoli e di imprese, osservando i comportamenti personali e le opportunità di formazione a riguardo, per arrivare a tracciare gli elementi centrali di una formazione efficace per incoraggiare *data security awareness* (Albrechtsen & Hovden, 2010; Kruger & Kearney, 2006; Rezgui & Marks, 2008; Shaw, Chen, Harris, & Huang, 2009; Waly et al., 2012). Come evidenziano Waly e colleghi (2012), riprendendo Tassabehji e Kamala (2012) "il problema della sicurezza riguarda le persone, non solo le tecnologie" ("security is a people problem, not just a technology problem", p. 1270) e, come sappiamo, pensando alle nostre pratiche quotidiane, non si tratta di un problema circoscritto all'ambito professionale e organizzativo. La sicurezza dei cyber-comportamenti riguarda infatti, a livello nazionale, quel 63,2% di persone, dai 6 anni in su, che si sono connesse alla rete negli ultimi 12 mesi, rappresentato per ben il 91% da 15-24enni, come evidenzia il report ISTAT 2016 *Cittadini, imprese e nuove tecnologie*, riferito a un campione di circa 24mila famiglie residenti in Italia e realizzato nel primo trimestre del 2016. Secondo Eurostat, l'82% dei cittadini dell'UE ha utilizzato Internet almeno una volta nei tre mesi precedenti all'indagine 2016 e il 79% lo utilizza regolarmente (almeno una volta a settimana) a casa, al lavoro o altrove[2]. Volendo, dunque, puntare il riflettore sugli adolescenti e giovani che utilizzano la rete quotidianamente, come possiamo promuovere *data security awareness*?

[1] Si veda https://harvardx.harvard.edu.

[2] http://ec.europa.eu/eurostat/statistics-explained/index.php/Internet access and use statistics - households and individuals#More than four fifths of Europeans used the internet in 2016.

È stato questo l'obiettivo principale del Progetto *Edu4Sec – Effective Education for Improving Data Security Awareness*, attivato nel 2016 dall'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). Più precisamente, con riferimento agli studenti della scuola secondaria di secondo grado, il progetto si è proposto di promuovere la conoscenza dei rischi che si possono correre in rete a partire dalla valorizzazione e condivisione delle loro cyber-esperienze. Oltre al coinvolgimento degli studenti, gruppo di riferimento dell'esperienza qui descritta e analizzata, *Edu-4Sec* si è basato sulla collaborazione attiva con gli animatori digitali[3] degli istituti coinvolti, gettando le basi per una più ampia sperimentazione che veda i docenti in grado di replicare e sviluppare in autonomia i moduli proposti a partire dalla proposta formativa testata.

2. Il disegno di ricerca

Nell'ambito di *Edu4Sec* sono stati, dunque, progettati e realizzati moduli formativi rivolti a studenti della scuola secondaria di secondo grado. In fase esplorativa, sono stati condotti tre focus-group con 36 studenti afferenti a tre istituti superiori di secondo grado del territorio di Padova e provincia e interviste semi-strutturate con due animatori digitali al fine di orientare la progettazione degli interventi formativi presso gli stessi istituti durante l'a.s. 2016/2017.

Gli stessi tre istituti sono stati coinvolti, tra novembre 2016 e gennaio 2017, in una sperimentazione a cui hanno preso parte 12 classi, 4 per ogni istituto, per un totale di 256 partecipanti, come evidenziato in Tabella 1.

[3] Ricordiamo che si tratta della figura inserita per la prima volta nel *Piano Nazionale Scuola Digitale* (PNSD), un documento pensato per accompagnare le scuole in un percorso di innovazione e digitalizzazione secondo quanto previsto nella riforma *La Buona Scuola* approvata nel 2015 (legge 107/2015). Come evidenzia il Ministero dell'Istruzione, dell'Università e della Ricerca, l'animatore digitale è incaricato di coordinare la diffusione dell'innovazione a scuola sviluppando i contenuti del PNSD e le attività ad esso ispirate previste nell'offerta formativa del proprio istituto. Nel caso del progetto *Edu4Sec*, i referenti dei moduli formativi sono stati proprio gli animatori digitali, d'intesa con il proprio dirigente scolastico.

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 piano quasi-sperimentale a due gruppi (Campbell & Stanley, 2015; Trinchero, 2002) con identificazione di un gruppo sperimentale (GS) (6 classi, 2 per ogni istituto, per un totale di 116 studenti coinvolti) e di un gruppo di controllo (GC) (6 classi, 2 per ogni istituto, per un totale di 140 studenti coinvolti) definiti secondo un campionamento di comodo basato sull'identificazione di classi simili per anno e tipologia (tradizionale o digitale[4]). L'adozione di un campione di comodo ha consentito la realizzazione degli interventi nel rispetto delle tempistiche riconosciute come più opportune dagli animatori digitali.

I due gruppi, sperimentale e di controllo, hanno beneficiato ciascuno di un intervento formativo della durata di 2 ore scolastiche ossia una durata media di 105 minuti.

Tabella 1. Sintesi degli interventi realizzati

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 ripartiti: - 140 GS - 116 GC

[4] Con l'accezione "classe digitale"si fa riferimento al PNSD e alla strategia di innovazione digitale per le scuole italiane. Come riporta il Piano, le iniziative a favore dell'innovazione digitale nella scuola sono precedenti all'emanazione del Piano stesso e già nel 2008 l'*Azione LIM* aveva previsto la diffusione capillare della Lavagna Interattiva Multimediale nella didattica in classe. A seguire, nel 2009 l'*Azione Cl@ssi 2.0* si era proposta di modificare gli ambienti di apprendimento attraverso un utilizzo costante delle tecnologie a supporto della didattica, per proseguire poi, nel 2011, con l'*Azione Scuola 2.0* orientata a coniugare l'innovazione nella programmazione didattica con nuovi modelli di organizzazione delle risorse umane e infrastrutturali dell'istituzione scolastica, come riporta il PNSD (2015).

I moduli formativi proposti hanno sviluppato le aree tematiche di seguito illustrate, centrali in tema di *data security* e al contempo rilevanti nell'esperienza quotidiana degli studenti, a partire da quanto emerge dai focus-group svolti negli istituti coinvolti:

1. Internet: rischi e pericoli
2. e-Commerce: shopping in sicurezza
3. Password: la nostra difesa
4. Smartphone: sono veramente smart?
5. Social network: privacy & security.

A partire da queste aree tematiche, il modulo è stato progettato con l'obiettivo di allestire per gli studenti uno spazio dialogico e riflessivo in cui poter riconoscere e scambiare esperienze personali, informazioni, curiosità, dubbi, in materia di *data security.* Come Albrechtsen e Hovden (2010) evidenziano, infatti, di norma, gli interventi di in-formazione sulla *data security* tendono a basarsi sulla trasmissione frontale di conoscenze tecniche proposte da un esperto del settore a grandi numeri di utenti. In ambito organizzativo, inoltre, la letteratura evidenzia come molti percorsi formativi sul tema risultino inefficaci a causa di un limitato coinvolgimento dei destinatari e dell'impossibilità di questi ultimi di sperimentare e sperimentarsi attivamente nelle problematiche di *data security* proposte. Tale limitato coinvolgimento fa sì che i partecipanti ascoltino, acquisiscano informazioni, ma poi, nel momento in cui tornano alle loro pratiche quotidiane, riprendono le loro abitudini precedenti senza apportare cambiamenti significativi (Waly et al., 2012). Come favorire, dunque, un cambiamento effettivo nelle pratiche degli studenti coinvolti nel progetto *Edu4Sec*? Come sollecitare una riflessione significativa sulle esperienze che quotidianamente vivono in rete al fine di sensibilizzarli alla percezione e prevenzione dei possibili rischi?

Per ogni modulo è stata prevista una presentazione frontale[5], per quanto possibile contenuta, intercalata da attività e tecniche di "manipolazione" di concetti chiave a partire da una rielaborazione delle loro

[5] A tale proposito, si ringraziano il prof. Mauro Conti, partner del progetto *Edu4Sec*, e il dott. Giuseppe Cascavilla, dell'Università di Padova, per aver messo a punto i contenuti chiave di ciascuna area tematica. Si ringrazia inoltre il dott. Angelo Canal che ha dedicato al progetto *Edu4Sec* la propria tesi di laurea magistrale in Management dei Servizi Educativi e Formazione Continua, affiancando tutti gli interventi nelle scuole.

esperienze in materia di gestione delle password, scelta e download di applicazioni, uso delle reti sociali, ecc. Secondo un approccio esperienziale, 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*, ovvero l'applicazione di elementi e meccaniche proprie del gioco, a situazioni non di gioco (Detering, Dixon, Khaled, & Nacke, 2011; Cheong C., Cheong F., & Filippou, 2013; Kapp, 2012). Più precisamente, entrambi i gruppi hanno beneficiato di interventi che hanno previsto l'ausilio di slides 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 e un quiz Kahoot sulla gestione delle password.

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.

2.1 Lo strumento di 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 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. 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.

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).

Tabella 2. Ripartizione rispondenti per classe di appartenenza e gruppo

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

La Tabella 2 mostra una 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). Tale variazione è da imputarsi a due cause principali. Talvolta, si è trattato di 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, 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 e 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. Si consideri che, a riguardo, il report ISTAT (2016) riferisce che l'uso del web è più frequente tra i 15-24enni (più del 91%), ma è in aumento anche l'uso da parte degli individui di 60-64 anni (dal 45,9% del 2015 al 52,2% del 2016). Il report evidenzia inoltre come i cellulari e gli smartphone siano sempre di più il traino dell'accesso a Internet. Tra gli utenti che dichiarano di andare in rete, il 42,1% lo fa con il cellulare/smartphone (contro il 38,6% del 2015), mentre l'uso del computer portatile è passato dal 21,5% al 19,3%. Si consideri inoltre che la quasi totalità degli utenti della rete che naviga fuori casa o del posto di lavoro utilizzando un computer portatile fa anche ricorso allo smartphone, mentre ben un 22,5%, si connette esclusivamente utilizzando lo smartphone (ISTAT, 2016).

Tornando al nostro campione di studenti, coerentemente con quanto evidenziato dal report ISTAT, 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. Si segnala, a tale proposito, che da un punto di vista metodologico, a partire dai singoli dispositivi in possesso dichiarati dai rispondenti, sono state costruite delle categorie via via inclusive che integrano il binomio smartphone-PC con gli altri dispositivi, dal tablet alla smart TV, alla console.

3. Risultati

3.1 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.

Tabella 3. Strategie di gestione delle password, gruppo complessivo

	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%

Relativamente all'impostazione delle password, la Figura 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 slide con un quiz Kahoot, che il GC, che ha invece beneficiato della sola presentazione frontale.

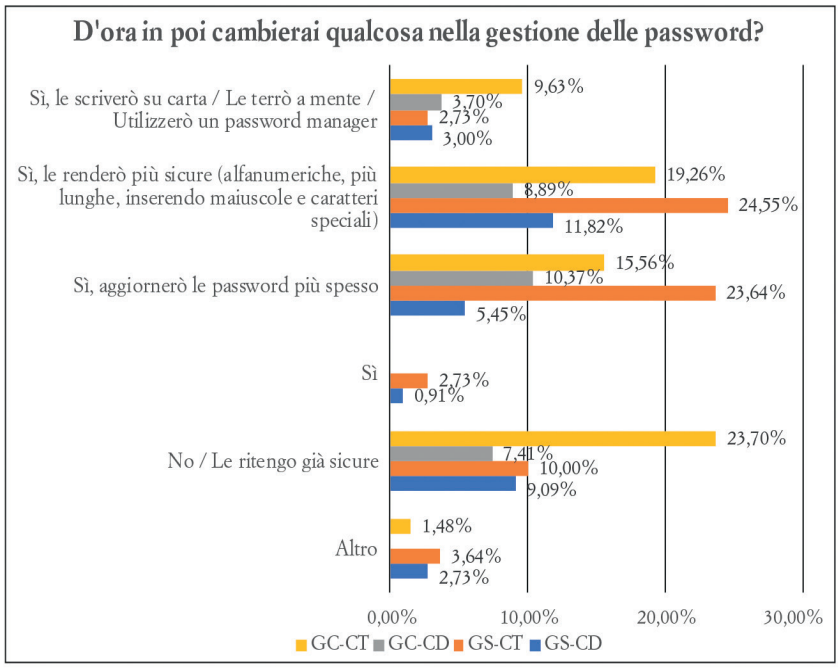

Figura 1. Cambiamenti nella gestione delle password, post-intervento. Confronto tra gruppo di controllo (GC)/sperimentale (GS) e classe digitale (CD)/tradizionale (CT)

Come evidenzia la Figura 2, inoltre, 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.

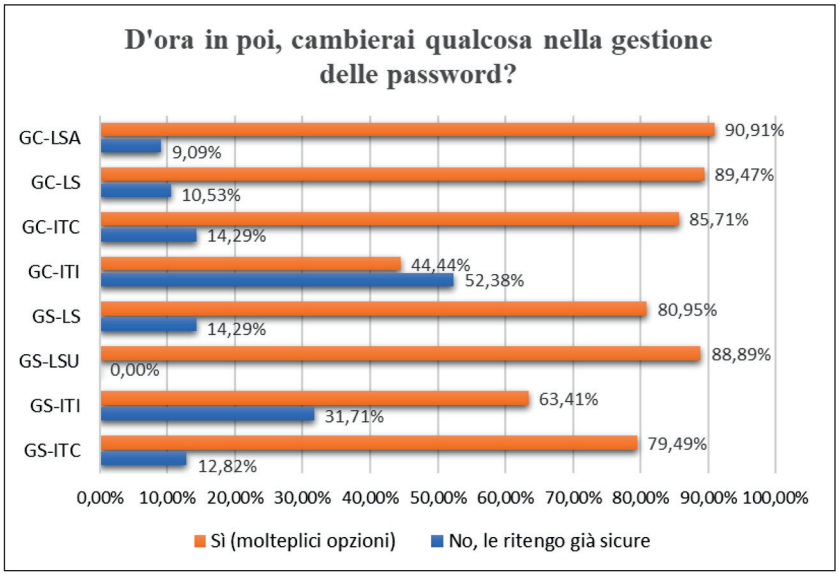

Figura 2. Cambiamenti nella gestione delle password, post-intervento, per istituto

3.2 Sezioni "Io e Facebook" e "Io e i social"

La batteria successiva ha indagato la presenza e l'attività dei rispondenti nei social network. A riguardo, il Report ISTAT 2016 riporta che "fra le persone che hanno usato Internet negli ultimi 3 mesi, l'85,8% ha fruito di contenuti culturali" (interessante evidenziare che i maggiori fruitori di contenuti culturali online, fatta eccezione per la lettura di giornali e riviste, sono i 15-24enni), "il 57,8% ha utilizzato un social network e quasi un terzo ha pubblicato sul web contenuti di propria creazione" (p. 1). Con particolare riferimento al gruppo dei 15-24enni presi in considerazione dall'indagine ISTAT, oltre l'80% utilizza un social network.

In particolare, nel nostro caso, 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?") a 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 a 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.

Tabella 4. Tipologia di informazioni postate, gruppo complessivo

	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%

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 Figura 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.

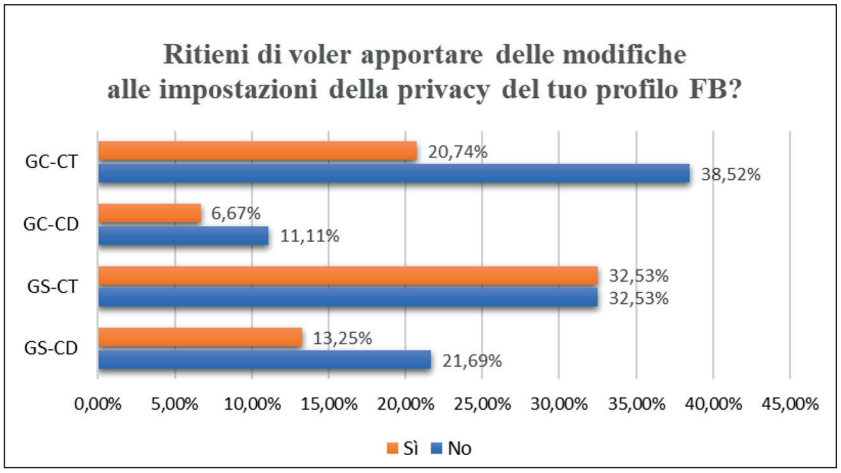

Figura 3. Modifiche al proprio profilo Facebook, post-intervento. Confronto tra gruppo di controllo (GC)/sperimentale (GS) e classe digitale (CD)/tradizionale (CT)

Anche per Facebook, così come per le password, la Figura 3 evidenzia come siano soprattutto gli studenti delle classi tradizionali a 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", come evidenziato dalla Figura 4.

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" a 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 Figura 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.

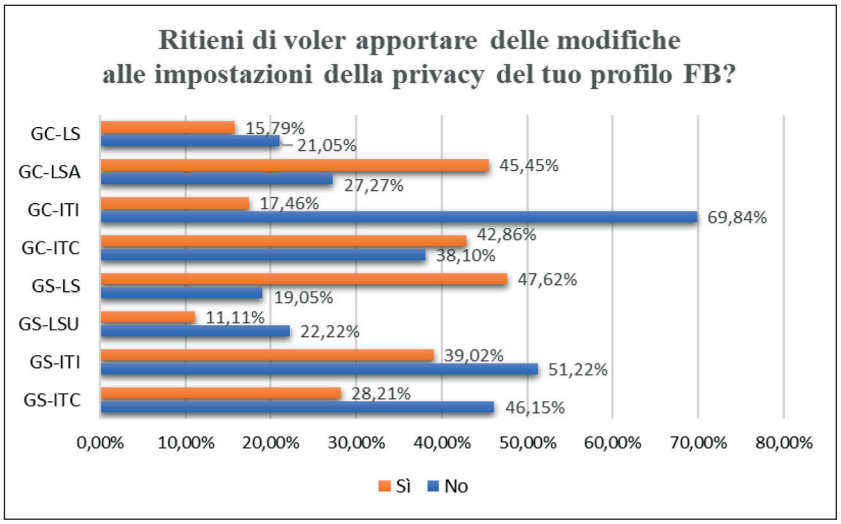

Figura 4. Modifiche al proprio profilo Facebook, post-intervento, per istituto

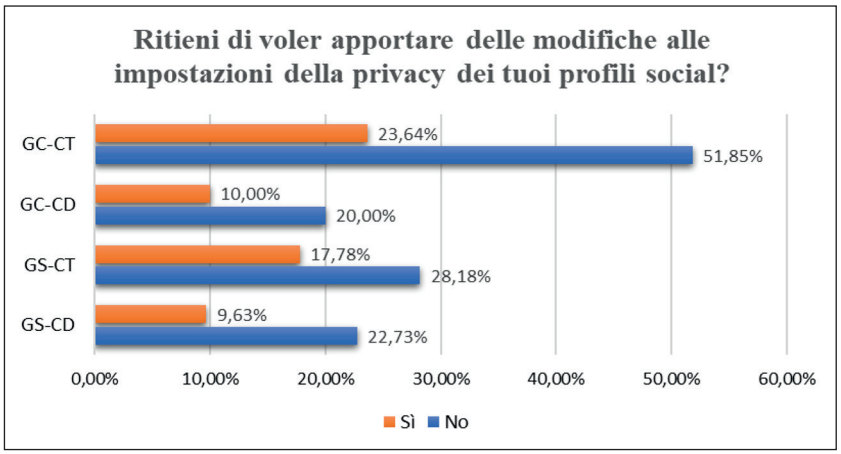

Figura 5. Modifiche ad altri profili *social*, post-intervento. Confronto tra gruppo di controllo (GC)/sperimentale (GS) e classe digitale (CD)/tradizionale (CT)

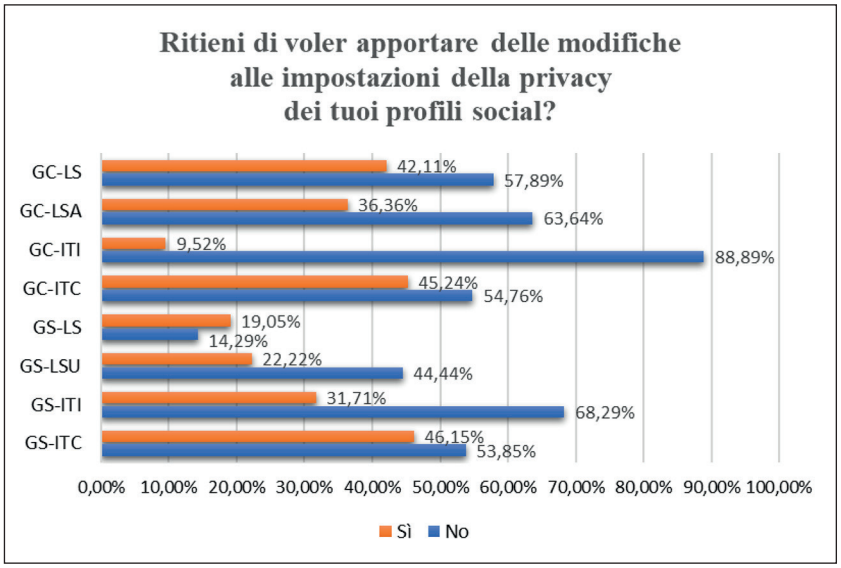

Figura 6. Modifiche ad altri profili social, post-intervento, per istituto

Viene replicata nuovamente la distribuzione percentuale relativa ai profili Facebook, con un maggior orientamento al modificare 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 a 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 e inconsapevole, senza adottare alcuna precauzione contro i rischi che potrebbero incontrare. La *data security* e i rischi a essa connessi potrebbero così riguardare soprattutto gli utenti 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.

3.3 Sezione "Io e Internet"

Proseguendo con il questionario, la terza batteria di domande ha indagato il fenomeno del *phishing*, tematica che si è rivelata in

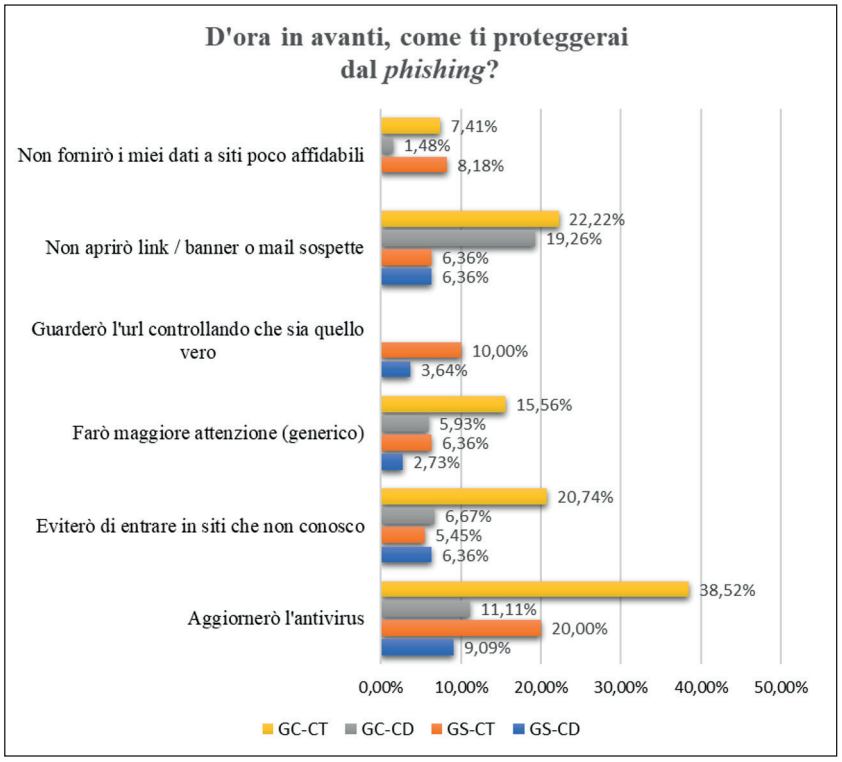

Figura 7. Esempi di strategie di protezione dal *phishing*, post-intervento. Confronto tra gruppo di controllo (GC)/sperimentale (GS) e classe digitale (CD)/tradizionale (CT)

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.

A fronte dell'intervento formativo, emerge dalla Figura 7 come gli studenti, invitati a riflettere sulle modalità di protezione dal *phishing*, abbiano ripreso quanto evidenziato nel corso del modulo. La figura evidenzia inoltre come, ancora una volta, siano soprattutto gli studenti delle classi tradizionali a 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.

3.4 Sezione "Io e le app"

La quarta batteria proposta ha riguardato le applicazioni (app) 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, nel pre-intervento il 28,13% le ritiene una minaccia per i propri dispositivi a un livello 3 o 4 (dove 1 = per nulla sicuro e 4 = moltissimo). Ciò significa che per oltre un 70% non costituiscono una minaccia. Nel 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 (Figura 8), in particolare, ancora una volta, gli studenti delle classi tradizionali.

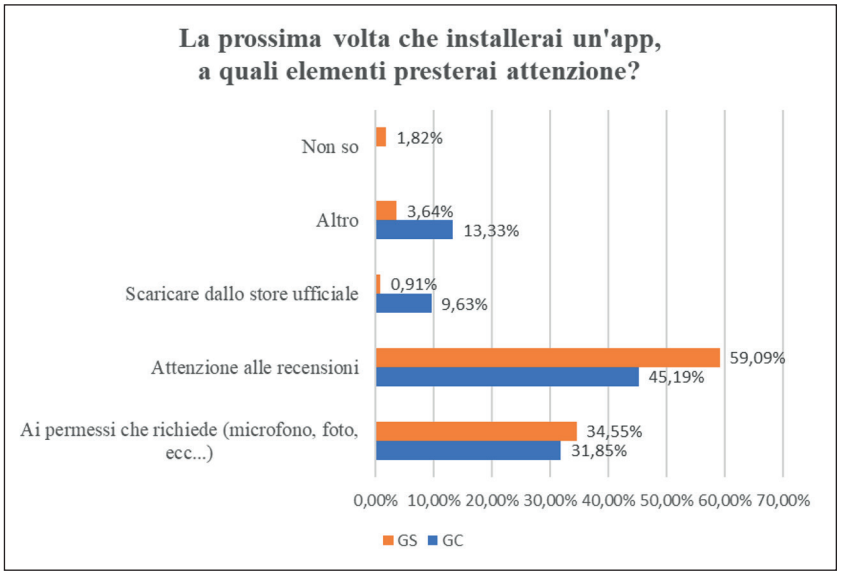

Figura 8. Elementi concreti a cui prestare attenzione al download di nuove applicazioni, post-intervento. Confronto tra gruppo di controllo (GC) e gruppo sperimentale (GS)

3.5 Sezione "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 questionario pre-intervento ha esplorato le abitudini di acquisto e in particolare le modalità di pagamento maggiormente utilizzate dal gruppo. Il sopra citato Report ISTAT 2016 ha evidenziato a tale proposito che il 50,5% degli intervistati d'età pari o superiore a 15 anni, ha navigato in Internet ed effettuato acquisti online nei tre mesi precedenti l'indagine (il 48,7% nel 2015); precisamente, il 28,7% ha ordinato o comprato merci o servizi negli ultimi 3 mesi, il 12,0% nel corso dell'anno e il 9,7% oltre un anno prima.

La Figura 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 a un conto proprio o dei propri genitori. Il 7,03% adotta entrambe le strategie (PayPal o prepagata, carta di credito).

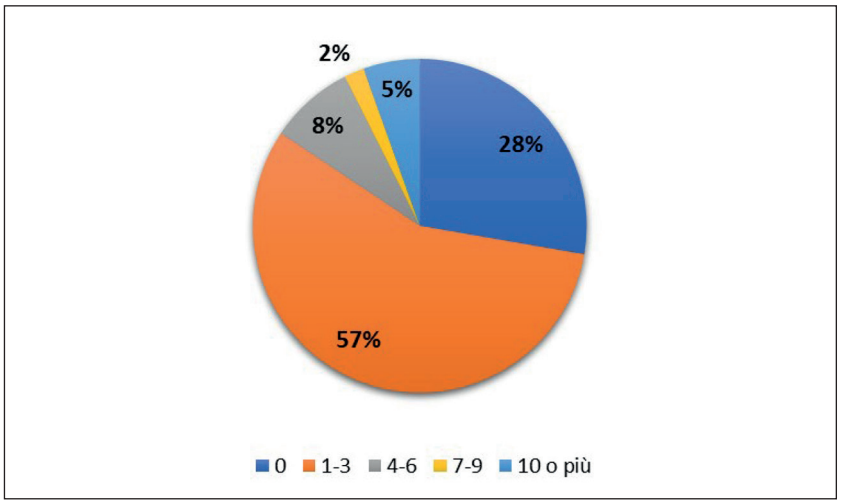

Figura 9. Frequenza mensile degli acquisti online. Campione complessivo

La Figura 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.

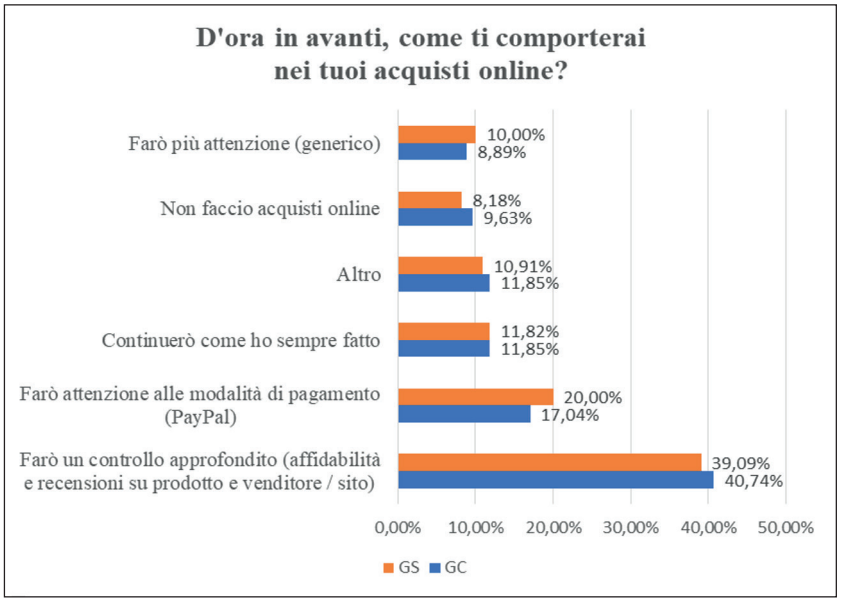

Figura 10. Intenzioni di comportamento negli acquisti online, post-intervento. Confronto tra gruppo di controllo (GC) e gruppo sperimentale (GS)

3.6 Sezione "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 a indagare attività/momenti ritenuti maggiormente coinvolgenti e nuove conoscenze. Osservando la Figura 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).

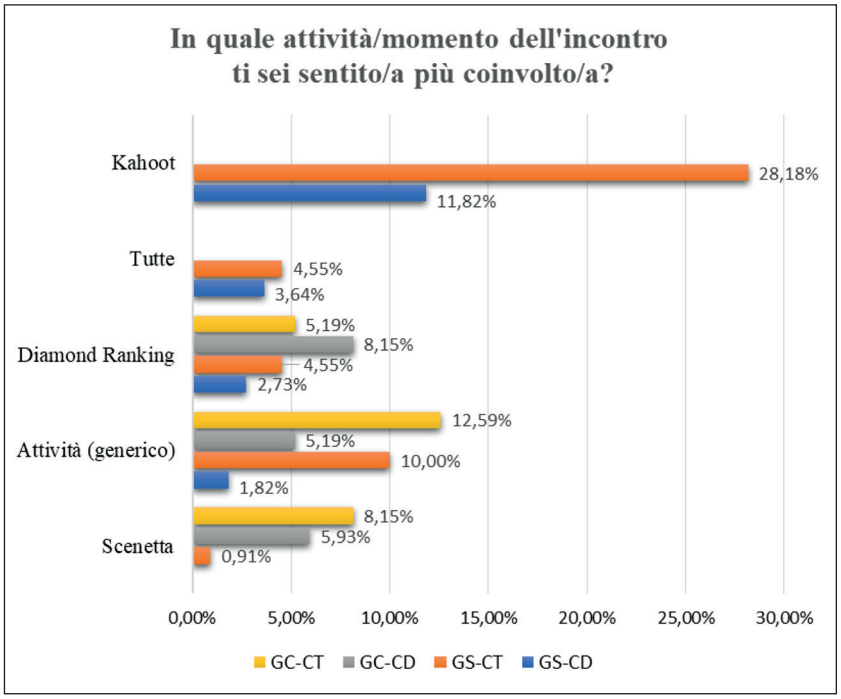

Figura 11. Attività/momento di maggior coinvolgimento, post-intervento. Confronto tra gruppo di controllo (GC)/sperimentale (GS) e classe digitale (CD)/tradizionale (CT)

4. Conclusioni

I dati qui presentati si propongono di sollecitare una riflessione in merito alle strategie da adottare per promuovere, in particolare attraverso proposte formative, la consapevolezza tra gli adolescenti riguardo ai rischi che il cyberspazio può riservare loro e al ruolo che la scuola può rivestire a riguardo. Un limite del modulo offerto dal progetto *Edu4Sec* e dei dati da esso 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. Consapevoli di questo limite, gli interventi proposti avevano come principale obiettivo quello di avviare un dialogo con gli istituti coinvolti e con gli animatori digitali per motivare ulteriori opportunità formative e di approfondimento sulla *data security*. In tal senso, materiali e strumenti messi a punto nell'ambito del progetto *Edu4Sec* vengono messi a disposizione di istituti e insegnanti interessati a lavorare sul tema e ad ampliare quello spazio dialogico, di riflessione e di confronto che il progetto ha inteso avviare. Inoltre, l'utilizzo da parte di *Edu4Sec* di metodologie esperienziali sollecita l'emersione delle esperienze e opinioni personali degli studenti in merito a Internet e alle connessioni digitali. Queste attività offrono, quindi, a insegnanti e animatori digitali occasioni per riconoscere vissuti, punti di vista e priorità degli studenti. La loro osservazione e valorizzazione costituisce un terreno di partenza per offrire attività di approfondimento e di riflessione sulle loro abitudini e atteggiamenti legati a Internet. Tali attività non riguardano solo i comportamenti degli studenti, ma anche l'approccio alle connessioni digitali in ambito educativo e, quindi, i comportamenti di insegnanti e istituti scolastici. L'invito che rivolgono ricercatori come Porterfield (2016) è che questa prospettiva e riflessione condivisa possa produrre e mettere a disposizione strumenti free software cui possiamo consapevolmente rivolgerci a partire dai dispositivi che usiamo quotidianamente per testare le condizioni di sicurezza dei programmi e delle procedure che utilizziamo in rete.

References

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.

Campbell, D. T., & Stanley, J. C. (2015). *Experimental and Quasi-Experimental Designs for Research*. San Francisco, CA: Ravenio Books.

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. doi: 10.14605/MED821709

Cheong, C., Cheong, F., & Filippou, J. (2013). Quick Quiz: A Gamified Approach for Enhancing Learning. *Pacific Asia Conference on Information Systems (PACIS) 2013 Proceedings*. Retrieved February, 20th, 2018 from http://aisel.aisnet.org/pacis2013/206

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.

Detering, S., Dixon, D., Khaled, R., & Nacke, L. (2011). From game design elements to gamefulness: defining "gamification". *Proceedings of the 2011 MindTrek Conference*. Retrieved February, 20th, 2018 from http://85.214.46.140/niklas/bach/MindTrek Gamification Printer-Ready 110806 S E accepted LEN changes 1.pdf

Directorate-General for Justice and Consumers (2015). *Special Eurobarometer 43. Data Protection*. Retrieved February, 20th, 2018 from http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs 431 sum en.pdf [consultato in data 20.02.2018].

ISTAT (2016). *Cittadini, imprese e ICT*. Retrieved February, 20th, 2018 from https://www.istat.it/it/files/2016/12/Cittadini-Imprese-e-nuove-tecnologie.pdf

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

Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers & security*, *25*(4), 289-296.

Porterfield, T. (2016). Patterns of Security Flaws in Ed-Tech Applications, and the Risks They Pose to Student Privacy. *Federal Trade Commission First Privacy Conference*, Washington.

Rezgui, Y., & Marks, A. (2008). Information security awareness in higher education: An exploratory study. *Computers & Security*, *27*(7), 241-253.

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

Shaw, R. S., Chen, C. C., Harris, A. L., & Huang, H. J. (2009). The impact of information richness on information security awareness training effectiveness. *Computers & Education*, *52*(1), 92-100.

Tassabehji, R., Kamala, M. (2012). Evaluating biometrics for online banking: the case for usability. *International Journal of Information Management 32*(5): 489-494.

Trinchero, R. (2002). *Manuale di ricerca educativa*. Milano: FrancoAngeli.

Waly, N., Tassabehji, R., & Kamala, M. (2012). *Improving Organisational Information Security Management: The impact of Training and Awareness. Proceedings of the 2012 IEEE 14th International Conference Proceedings*, 1270-1275.