TEMA

Un esempio di lezione sulla sicurezza informatica

Martino Sacchi

Liceo Scientifico Linguistico Giordano Bruno (Melzo)

martino.sacchi@libero.it

Nella mia scuola, il liceo Scientifico Linguistico Giordano Bruno di Melzo, è stata introdotta da alcuni anni una settimana di sospensione della normale attività di insegnamento nel mese di febbraio per consentire la realizzazione di percorsi di recupero per i ragazzi che hanno dimostrato difficoltà nel corso del primo quadrimestre. Per coloro che non devono seguire corsi di recupero vengono organizzate attività ulteriori, tra le quali un brevissimo corso sulle nozioni basi della sicurezza nell'uso dei computer. Pur non essendo certamente esaustivo della problematica della sicurezza in rete, esso può essere visto come una sorta di «kit di pronto intervento» per presentare alcuni aspetti fondamentali di questa tematica a studenti completamente digiuni di questo argomento.

Obiettivi e quadro di riferimento

Si tratta di un intervento spot indirizzato specificamente agli studenti del biennio, e in particolare a quelli delle classi prime, sia del Linguistico sia dello Scientifico. L'obiettivo, dato il basso numero di ore destinate a queste lezioni (di solito solo due per classe o per gruppi di classi), è necessariamente limitato. Ci si propone soprattutto di:

- sensibilizzare gli studenti alla problematica della sicurezza mostrando loro i possibili rischi di un uso ingenuo degli strumenti informatici (e in particolare dei social media)
- fornire alcuni strumenti pratici e operativi per affrontare le situazioni più comuni

Il quadro di riferimento ultimo non può che essere il documento europeo sulle competenze chiave con ovvio riferimento alla competenza digitale, la quale come noto «consiste nel saper utilizzare con dimestichezza e spirito critico le tecnologie della società dell'informazione (TSI) e richiede quindi abilità di base nelle tecnologie dell'informazione e della comunicazione (TIC)» come si legge nella sintesi di Eur-Lex.

La lezione è totalmente pratica e si svolge nel laboratorio di informatica del liceo. Gli studenti lavorano individualmente in postazioni singole (il laboratorio di informatica del liceo funge anche da laboratorio linguistico ed è organizzato secondo uno schema rigido di postazioni affiancate disposte in linee parallele alla cattedra, separate da un divisore) e sono invitati a:

- prendere appunti direttamente su Word o LibreOffice (sono disponibili entrambe le opzioni) per creare un testo da esportare su chiavetta o da inviare a se stessi via mail (per chi ha un account di posta elettronica e soprattutto… si ricorda a memoria la password!)
- operare direttamente su alcuni programmi particolari sotto la guida del docente.

Spesso i ragazzini di prima non sono mai entrati nel laboratorio informatico ed è necessario dedicare qualche minuto a spiegarne il funzionamento base, in particolare il sistema delle password di classe adottato dal liceo.

Il computer come strumento di lavoro

La prima parte della lezione viene dedicata ad alcune idee semplici ma fondamentali: il computer (nella maggior parte dei casi ormai si tratta di notebook o netbook) deve essere considerato come uno strumento di lavoro, non come una occasione di gioco o di svago. Di conseguenza deve essere trattato secondo certe procedure per poterlo usare al meglio delle sue potenzialità.

Normalmente vengono presentate due processi: la pulizia della cache, dei file temporanei e del file di registro e la deframmentazione del disco fisso.

Come si sa, durante l'uso sulla rete i nostri computer accumulano file che vengono tenuti sulla macchina locale per accelerarne il funzionamento; col tempo però si ottiene l'effetto opposto perché la macchina deve perdere troppo tempo per gestire queste informazioni, che per lo più sono inutili. Allo stesso modo, il file di registro finisce spesso per contenere istruzioni obsolete che però la macchina tenta inutilmente di eseguire rallentando il funzionamento generale.

Per risolvere questi problemi viene proposto Ccleaner, in quanto prodotto considerato universalmente affidabile e soprattutto gratuito (almeno nella versione base). Tutti i computer del laboratorio informatico del liceo sono dotati di questo programma. Gli studenti individuano sul desktop l'icona corrispondente e arrivano fino al pannello di controllo, senza tuttavia attivarlo; sono invitati a scaricare sui computer personali il programma ed effettuare periodicamente la pulizia della macchina.

Una seconda causa del rallentamento delle macchine è dato dal fatto che i nuovi file vengono copiati cercando di occupare tutti gli spazi disponibili (ricavati da precedenti cancellazioni), che però non sono mai delle stesse dimensioni dei nuovi file. Questi ultimi perciò devono essere divisi o «frammentati» in più parti. Il programma che si incarica di questa operazione si preoccupa anche di inserire gli opportuni collegamenti per permettere successivamente agli applicativi di ricostruire nella

corretta sequenza le informazioni necessarie. Questo processo però, per quanto eseguito rapidamente, porta via del tempo; più la percentuale di frammentazione dei file aumenta più la velocità operativa della macchina diminuisce. Per ovviare almeno in parte a questo inconveniente esistono degli appositi programmi che si occupano di «deframmentare» il disco, cioè di collocare nella corretta successione, per quanto possibile, le singole parti di un programma o di un file molto lungo (per esempio un video) così che possano essere eseguite in modo continuativo e quindi più veloce e fluido. È sufficiente per gli studenti usare l'utility di deframmentazione presente di default nei sistemi operativi Windows, oppure, in caso non fosse presente, utilizzare un programma gratuito come Defraggler. È opportuno sapere che se la macchina ha qualche anno di età l'operazione di deframmentazione, se non è mai stata compiuta prima, può essere molto lunga (anche mezza giornata o più) e rallenta sensibilmente il funzionamento: bisogna quindi scegliere il momento opportuno per effettuarla in modo da impattare il meno possibile sulle attività di lavoro proprie e della famiglia.

La conservazione e la protezione dei contenuti

Il secondo item della lezione riguarda la conservazione e la protezione dei contenuti. Per quanto incredibile possa sembrare, è normale sentirsi dire dagli studenti che non esistono copie di scorta dei lavori che producono (la cosa emerge di solito il giorno prima dell'interrogazione, quando un virus o un guasto rendono inutilizzabili i materiali che dovevano essere presentati). Un altro comportamento che si riscontra spesso da parte degli studenti è di limitarsi ad accumulare i materiali prodotti in una sola cartella generica (per esempio "Documenti" di Windows, o la root della chiavetta): è opportuno invece insistere perché almeno i materiali scolastici vengano conservati con ordine in cartelle ordinate gerarchicamente per poter essere rintracciati con facilità anche a distanza di mesi o di anni.

La regola ovvia, che però va ripetuta fino alla noia, è di realizzare copie di scorta di tutti i materiali importanti. Esistono diversi modi per assolvere questo compito, utilizzando tecnologie diverse che non si sovrappongono completamente. Essenzialmente si possono usare:

- chiavette flash
- hard disk esterni
- DVD
- siti di storage nel cloud

Per poter valutare vantaggi e svantaggi di questi sistemi è opportuna una veloce spiegazione sulle differenti tecnologie impiegate dai diversi tipi di strumenti. Le chiavette utilizzano memorie allo stato solido, sono molto veloci e costano relativamente poco: di fatto tutti gli studenti ne possiedono una. Per contro le chiavette possono essere facilmente smarrite, richiedono una connessione fisica con il computer che col tempo può rovinarsi e non funzionare più e infine possono essere danneggiate da campi magnetici intensi. La capienza delle chiavette in commercio cresce continuamente, ma in certi casi (per esempio se si tratta di immagazzinare video di grandi dimensioni oppure un gran numero di foto ad alta risoluzione) possono non essere sufficienti.

L'hard disk esterno è uno strumento molto più potente, soprattutto dal punto di vista della capacità. Nella maggior parte dei casi si tratta di modelli a piattelli (anche se si

stanno diffondendo i modelli a stato solido). L'estrema facilità di connessione con il computer permette di considerarli una vera espansione del disco fisso principale, consentendo di realizzare facilmente copie di back up di tutto il contenuto del disco fisso, o almeno di tutti i contenuti di interesse per la scuola. Per contro sono relativamente costosi e alquanto fragili (un hard disk che cada malamente da un tavolo può rompersi in modo irrimediabile).

Quando i dati da conservare sono ormai definitivi, ovvero non si prevede di doverli più modificare, si può pensare ad una archiviazione su DVD. È opportuno spiegare agli studenti che un DVD è realizzato con una tecnologia completamente diversa da quelle prese in considerazione fino a questo momento: i dati non sono registrati attraverso una qualche forma di magnetizzazione del supporto, ma mediante una trasformazione fisica del disco. Un sottilissimo raggio laser incide una lunga traccia a spirale sul supporto, che contiene al proprio interno uno strato capace di cambiare stato quando viene stimolato dalla luce polarizzata. Le informazioni sono immagazzinate sotto forma di piccolissimi linee e punti disposti lungo la traccia del DVD e non vengono alterate dalla presenza di campi magnetici. Se il DVD è conservato in modo corretto, senza esporlo a temperature troppo elevate (per esempio quelle che si raggiungono nel cruscotto di una macchina lasciata parcheggiata sotto il sole estivo) e senza sottoporlo a flessione o addirittura a tagli e incisioni, le informazioni possono essere conservate molto a lungo.

È importante spiegare bene che tutti questi supporti fisici andrebbero conservati lontano dal computer, per tenerli al sicuro da quegli eventi accidentali che potrebbero danneggiarli insieme alla macchina principale: il caso tipico, che viene suggerito come esempio durante la lezione, è la sorellina piccola che rovescia un'intera bottiglia di CocaCola sul computer. Se i DVD o gli hard disk vengono conservati nelle immediate vicinanze della macchina principale, è probabile che vengano danneggiati anch'essi, vanificando tutto il lavoro di backup.

Una soluzione elegante per prepararsi a questa evenienza consiste nel salvare copie del proprio lavoro nel cloud. Spesso i programmi e i siti specifici di storage sono a pagamento (e sono anche cari), e quindi poco adatti a un uso scolastico. Una soluzione accettabile potrebbe allora essere quella di far aprire agli studenti (se non l'hanno già) un account Dropbox, che ha il pregio della estrema facilità d'uso, o un account Google per poter accedere alle funzionalità di Google Drive.

Le password

Praticamente ogni registrazione a un sito implica una password. In teoria sarebbe opportuno avere password diverse per ciascun sito, perché se si usa la stessa password per più siti ed essa cade nelle mani di un malintenzionato, tutti i nostri siti saranno contemporaneamente esposti alla minaccia di essere visitati o danneggiati. Esistono programmi (disponibili anche in versione portable, cioè da utilizzare da chiavetta) capaci di generare password del tutto casuali (e perciò estremamente robuste) e di tenerne automaticamente memoria in modo da poterle utilizzare col sito giusto. Questo sistema, in sé molto efficace, ha però il suo lato debole nel fatto che crea un pericoloso «collo di bottiglia» rappresentato dal programma stesso: se per un qualche motivo ci si dimentica la password di accesso oppure ci viene rubata perdiamo in un colpo solo il controllo su TUTTI i siti ai quali siamo registrati.

Una soluzione meno drastica consiste nello scegliere una sorta di «algoritmo mentale» che ci permetta di inventare delle password che siano insieme robuste e facili da ricordare. Uno dei trucchi possibili consiste nello scegliere una canzone o una poesia che si conoscono a memoria e scegliere la prima lettera delle prime dieci parole (per esempio). Se prendiamo in esame una canzone famosa come «Azzurro» di Celentano, vediamo che il ritornello dice: «Azzurro, il pomeriggio è troppo azzurro e lungo per me». Le prime lettere delle parole che lo compongono sono: aipetaelpm. La «a» può essere sostituita dalla chiocciolina (basta ricordarsi che TUTTE le «a» devono essere sostituite dal simbolo della chiocciolina per non sbagliarsi): @ipet@elm. Se le condizioni previste dal sito prevedono una maiuscola, si può decidere (come regola personale) che SEMPRE la prima lettera sia maiuscola, e se, come in questo caso, ciò non è possibile che sia l'ultima a essere maiuscola: @ipet@elM. Secondo il servizio gratuito offerto da Kaspersky (la nota casa produttrice di antivirus) all'indirizzo https://password.kaspersky.com/it/, un normale computer avrebbe bisogno di 4 mesi di lavoro ininterrotto per violare questa password, che quindi possiamo già considerare sicura. Se 4 mesi ci paiono pochi, possiamo aggiungere la data in cui la canzone è nata (e perciò scriviamo i numeri DAVANTI alla password): 1979@ipet@elM. A questo punto ci vorranno 33 anni di lavoro per forzale la password. Per rendere le cose ancora più difficili possiamo aggiungere come regola nostra personale di chiudere SEMPRE (in modo da ricordarcelo facilmente) le nostre password con due punti esclamativi: 1979@ipet@elM!! Adesso ci vorrebbero 33 secoli per un normale computer per violare i nostri account, un periodo di tempo decisamente rassicurante! Evidentemente è molto difficile ricordarsi a memoria una password di questo tipo: ricordando però COME è stata costruita (abbiamo scelto la prima lettera delle prime dieci parole del ritornello di «Azzurro» di Celentano, una canzone che non possiamo dimenticare e che in ogni caso è facile rintracciare in rete; abbiamo aggiunto la data di composizione; abbiamo sostituito le «a» con la chiocciolina; abbiamo aggiunto due punti esclamativi alla fine), è possibile riscriverla senza difficoltà tutte le volte che ne abbiamo bisogno.

I social media

L'ultima parte della nostra lezione è dedicata ai social media, in particolare a Facebook, Youtube e Instagam, e alle attenzioni che bisogna usare per poterli usare con una ragionevole sicurezza. Il principio base è molto semplice: la Rete è un luogo pubblico, come se fosse una piazza. Noi tutti cadiamo facilmente preda dell'equivoco di pensare che, poiché siamo per lo più da soli davanti al computer quando scriviamo un post o scarichiamo un video, questi gesti siano privati. Invece non è così: quello che si dice e si scrive sulla Rete è letto e visto da un pubblico potenzialmente sconfinato e soprattutto a noi sconosciuto. Di conseguenza prima di scrivere un commento, caricare un testo o una foto, oppure scaricare un filmato dobbiamo sempre chiederci quali possono essere le conseguenze di questo gesto: bisogna in altre parole rinunciare alla spensieratezza di chi agisce o re-agisce per istinto a tutte le stimolazioni che la Rete ci offre.

Si dice spesso che «un contenuto caricato sulla Rete diventa eterno», intendendo dire che esso si sottrae di fatto al nostro controllo: può essere ripreso da altri, copiato e riprodotto, oppure distorto, senza che noi si possa più intervenire per fermarlo. È indispensabile perciò porre sempre la massima attenzione in questa operazione, tecnicamente così semplice da richiedere pochissimi secondi col rischio quindi che

venga effettuata senza nemmeno avere il tempo di riflettere sulle possibili conseguenze.

Oggi per esempio è prassi comune per le aziende che intendono assumere una persona andare a controllare sulla Rete la vita del candidato, cercando informazioni che potrebbero essere state volutamente nascoste durante il colloquio di assunzione. Secondo alcuni quotidiani ci sono aziende che pretendono perfino di farsi consegnare la password di accesso alla pagina Facebook del candidato, una ovvia violazione delle leggi sulla privacy. Tutto questo significa che una foto o un filmato per qualunque verso «compromettente» (tipicamente una foto scattata durante una festa in cui il soggetto, pur non facendo in realtà niente di male, essendo osservato fuori dal contesto in cui la foto è stata scattata offre di sé un'immagine negativa) potrebbero ricomparire tra cinque o dieci anni mettendoci in difficoltà.

L'unica strategia sensata appare quindi la prudenza preventiva. Ogni volta che carichiamo un contenuto (un qualsiasi contenuto) noi forniamo informazioni su noi stessi (è proprio su questo meccanismo che si regge l'offerta delle pubblicità che vediamo apparire sui nostri browser, o sulla nostra pagina Facebook, o nelle mail a noi indirizzate): è necessario essere consapevoli di questo e sapere che queste informazioni, ancora una volta, sfuggono al nostro controllo. Per esempio in Inghilterra pare che alcune compagnie di assicurazione si rifiutino di rimborsare i furti avvenuti nelle case di città durante le vacanze del proprietario se il derubato ha postato su Facebook foto da cui si potesse capire che era via di casa per godersi il meritato riposo.