Rimestare nel torbido: allenare le capacità critiche ragionando su spam e phishing

Un'esperienza didattica per riflettere sull'attendibilità delle e-mail

Manuela Delfino, CNR - Istituto per le Tecnologie Didattiche
delfino@itd.cnr.it

INTRODUZIONE

Farmaci ed erbe senza prescrizione medica, materiale pornografico e software pirata, auto e orologi di lusso a prezzi competitivi, offerte di lavoro a distanza, il rapido conseguimento di un titolo di studio a fronte di un impegno minimo: è esperienza alquanto comune ricevere posta elettronica indesiderata e cestinarla, pensare che il filtro anti-spam sia stato nuovamente raggirato e sperare che venga nuovamente tarato in modo che intercetti e blocchi le e-mail spazzatura.

Lo *spam* viene normalmente visto dagli utenti della rete come una seccatura, inopportuna poiché lesiva del tempo delle persone e possibile veicolo di truffe (*scam*), volte a rubare i dati personali e l'identità, e a riutilizzare le informazioni private per fini di lucro (*phishing*). Eppure negli ultimi mesi, avendo l'obiettivo didattico di presentare il tema dello spam a studenti di una terza classe della scuola secondaria di I grado, ho trovato quasi dilettevole il razzolare nella spazzatura elettronica, alla ricerca di esempi variegati e interessanti da proporre agli allievi. Perché mai dedicare un'attività scolastica al tema dello spam? Innanzitutto perché se è sempre più frequente che i nostri giovani studenti abbiano un indirizzo di posta elettronica personale, è altrettanto diffuso che non siano informati sui pericoli in cui possono imbattersi. Malgrado i filtri anti-spam e malgrado i sistemi automatici che segnalano la scarsa attendibilità delle e-mail e dei siti visitati siano di volta in volta più sofisticati e affidabili, esiste sempre il rischio di imbattersi in posta elettronica non desiderata e siti non attendibili. L'utente della rete non può concedersi il lusso di sentirsi completamente protetto, affidandosi alla tecnologia antifrode, ma deve necessariamente stare all'erta, acquisire consapevolezza della necessità del sospetto.

E poi perché un'ipotetica *didattica dello spam* potrebbe essere un utile esempio di didattica dell'osservazione, dell'analisi critica dell'informazione, del sospetto e del dubbio. La caratteristica principale dello spam è che la fonte è totalmente assente e non facilmente individuabile, dunque la valutazione di affidabilità va fatta interamente sul testo e sull'intestazione del messaggio.

ANTI-SPAMMING E ANTI-PHISHING EDUCATION

L'*anti-phishing education* sta diventando un settore di studio a sé stante, associato con l'analisi delle dinamiche della credenza, volto tanto a indagare i modi per difendersi dal phishing, quanto a riflettere sui motivi per cui le persone cadono vittime di certi tranelli, in modo da creare le basi per predisporre strategie di difesa mirate [Dhamija et al., 2006].

Tra le esperienze più note e controverse si segnala un corso su "Spam e Spyware" tenuto dal 2005 presso il dipartimento di *Computer science* dell'Università di Calgary. Nel corso, basato in prevalenza su attività di laboratorio, non si insegna agli studenti (prossimi alla laurea o appena laureati, selezionati in base a criteri di merito e alle motivazioni espresse) soltanto come difendersi dagli attacchi della posta indesiderata, ma anche come generare spam e spyware [Aycock, 2006; Aycock et al., 2008].

Un approccio più tradizionale è quello di Robila e Ragucci (2006), che prevede la presentazione di esempi di phishing e la conseguente discussione. La loro attività, come accade in altre esperienze [Werner e Courte, 2008; Frank e Werner, 2007], è corredata dalla somministrazione del *SonicWall Phishing IQ Test* [1] ed è rivolta a studenti di informatica.

L'approccio di Kumaraguru et al. (2007; 2008; in stampa) si basa sull'invio di false e-mail di phishing: se la persona clicca sul link indicato, le viene fornito un feedback immediato contenente spiegazioni di quanto accaduto e alcuni consigli (nella forma di fumetti e vignette scherzose, volte a sdrammatizzare) su come evitare di cadere nelle trappole del phishing.

Malgrado questo tema abbia acquisito popolarità anche a livello nazionale[2], nel nostro Paese non ci sono molte testimonianze di esperienze didattiche che portino lo studente a fronteggiare direttamente i problemi.

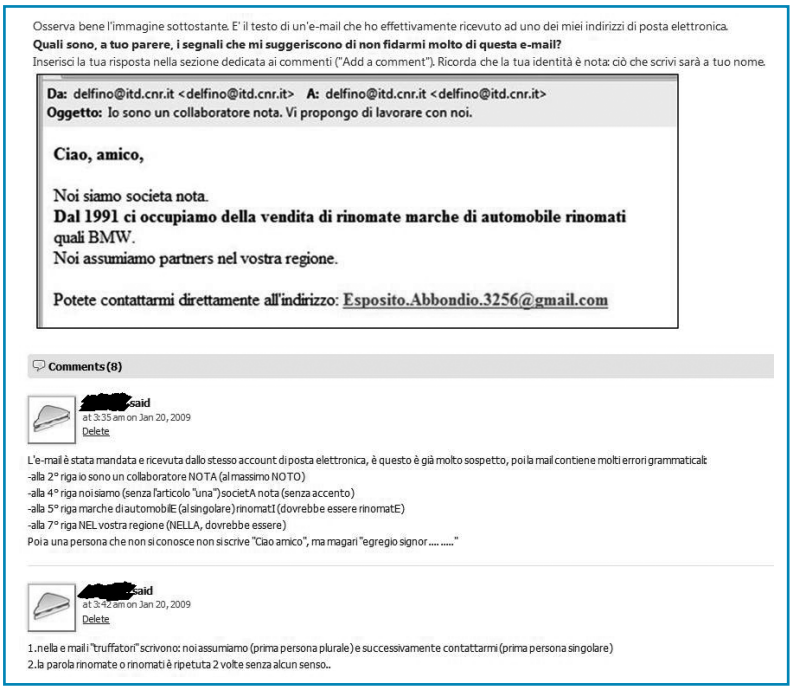
Quanto segue[3] riporta un'esperienza in cui lo spam è stato utilizzato come spunto per sensibilizzare gli studenti su un tema di attualità tecnologica e, al tempo stesso, per promuovere competenze di autodifesa.

L'ATTIVITÀ

L'esperienza, condotta con gli alunni di una terza della scuola secondaria di primo grado "D'Oria-Pascoli" di Genova, rientra nel percorso di informatica dedicato alla comunicazione asincrona, i cui obiettivi sono: (1) conoscere e saper utilizzare i principali strumenti di comunicazione asincrona (SMS, e-mail, forum, wiki, blog, etc.), (2) essere consapevoli degli effetti che tali strumenti possono avere sulle modalità comunicative (es., non rispetto delle convenzioni ortografiche), (3) saper decifrare i segni del pericolo che si possono accompagnare ad alcuni di questi strumenti (es., spam, phishing).

L'attività è stata organizzata in due lezioni, ciascuna della durata di un'ora.

La prima lezione è stata dedicata all'analisi di e-mail sospette. Inizialmente ciascun alunno è entrato in uno spazio personale di un wiki con accesso limitato per analizzare un'e-mail, il cui testo è stato presentato sotto forma di immagine per neutralizzare eventuali rischi contenuti nei link[4]. Il compito era di segnalare gli indizi sospetti e, successivamente, di entrare nelle pagine dei compagni per integrare quanto già scritto da loro o esprimere eventuale disaccordo


Osserva bene l'immagine sottostante. E' il testo di un'e-mail che ho effettivamente ricevuto ad uno dei miei indirizzi di posta elettronica.
Quali sono, a tuo parere, i segnali che mi suggeriscono di non fidarmi molto di questa e-mail?
Inserisci la tua risposta nella sezione dedicata ai commenti ("Add a comment"). Ricorda che la tua identità è nota: ciò che scrivi sarà a tuo nome.

Da: delfino@itd.cnr.it <delfino@itd.cnr.it> **A:** delfino@itd.cnr.it <delfino@itd.cnr.it>
Oggetto: Io sono un collaboratore nota. Vi propongo di lavorare con noi.

Ciao, amico,

Noi siamo societa nota.
Dal 1991 ci occupiamo della vendita di rinomate marche di automobile rinomati quali BMW.
Noi assumiamo partners nel vostra regione.

Potete contattarmi direttamente all'indirizzo: Esposito.Abbondio.3256@gmail.com

Comments (8)

[redacted] said
at 3:35 am on Jan 20, 2009
Delete

L'e-mail è stata mandata e ricevuta dallo stesso account di posta elettronica, è questo è già molto sospetto, poi la mail contiene molti errori grammaticali:
-alla 2° riga io sono un collaboratore NOTA (al massimo NOTO)
-alla 4° riga noi siamo (senza l'articolo "una") societA nota (senza accento)
-alla 5° riga marche di automobilE (al singolare) rinomatI (dovrebbe essere rinomatE)
-alla 7° riga NEL vostra regione (NELLA, dovrebbe essere)
Poi a una persona che non si conosce non si scrive "Ciao amico", ma magari "egregio signor ...."

[redacted] said
at 3:42 am on Jan 20, 2009
Delete

1. nella e mail i "truffatori" scrivono: noi assumiamo (prima persona plurale) e successivamente contattarmi (prima persona singolare)
2. la parola rinomate o rinomati è ripetuta 2 volte senza alcun senso..

(figura 1). Benché la consegna fosse la stessa ("Quali sono i segnali che suggeriscono di non fidarsi di questa e-mail?"), tutti i testi proposti erano diversi, per dar modo a ciascun alunno, indipendentemente dagli altri, di osservare, analizzare e proporre agli altri i risultati delle proprie indagini. Data l'età degli alunni, si è preferito escludere dal campione di spam usato a scuola messaggi dal contenuto pornografico o con allusioni esplicite ad attività sessuali. Questo non ha impedito tuttavia di affrontare il tema.

Alla fine della lezione è stato chiesto a tutti gli studenti di fare uno sforzo di astrazione, elencando, in base a quanto osservato, gli elementi cui si deve prestare attenzione quando si riceve un'e-mail.

La seconda lezione ha avuto l'obiettivo di riflettere collaborativamente su quanto emerso e di imparare a osservare l'intestazione di un'e-mail.

Per riprendere le fila del discorso della lezione precedente è stata video-proiettata e analizzata in gruppo un'e-mail sospetta. È stata quindi presentata una sintesi degli elementi segnalati dagli studenti come elementi di rischio quando si riceve un'e-mail. In questa fase, l'obiettivo del docente è duplice: (i) analizzare e discutere i commenti scritti dagli studenti; (ii) mostrare come alcuni degli elementi individuati fossero in realtà dei falsi positivi (nel senso che – come vedremo – sono stati indicati come segnali di rischio elementi che tali non erano) e, al contempo, come non tutti i segnali siano sempre stati identificati. A differenza dei ca-

figura 1
Consegna dell'attività ed esempio dei commenti scritti da due studenti.

1 http://www.sonicwall.com/phishing/

2 Cajani, 2008; Gaggioli, 2007; il "servizio antibufala" di Paolo Attivissimo; il progetto didattico "Missione Internet Sicuro!" dell'UNICEF Italia e di SicuramenteWeb, iniziativa ideata da Microsoft Italia sui temi della navigazione protetta dei minori sul Web e della sicurezza informatica.

3 Un'integrazione a quanto qui presentato è in Caviglia et al., (in stampa).

4 L'esperienza è ripetibile con altre tecnologie o anche su carta: in questo caso è stato utile introdurre il wiki, per consentire agli alunni di familiarizzare con l'ambiente in vista delle attività successive. È stato scelto PbWiki (http://pbwiki.com), un software gratuito e libero per gli educatori.

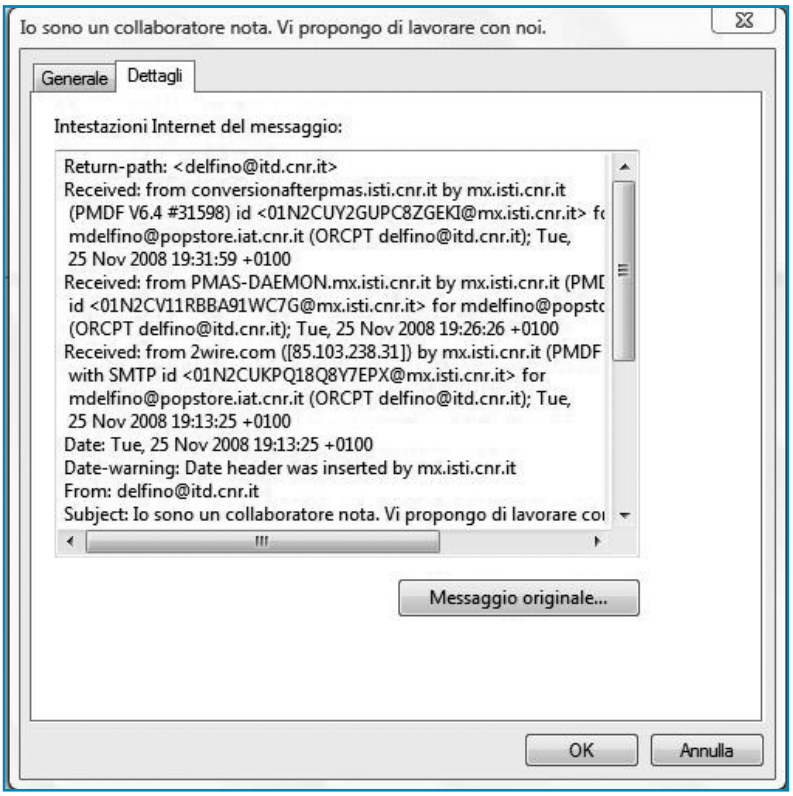


figura 2

Esempio di intestazione di una e-mail.

si visti nella prima lezione, infatti, esistono e-mail ben più subdole, ben scritte, che non presentano segni evidenti che possono generare sospetto. In questi casi è bene analizzare i dettagli dell'e-mail ricavabili dall'intestazione del messaggio, al fine di osservare i dati relativi all'indirizzo reale del mittente, al percorso compiuto dal messaggio, alla data di invio, etc. (figura 2).

Per familiarizzare gli alunni con il concetto di intestazione dell'e-mail, ognuno di loro è stato invitato ad analizzare alcune e-mail scambiate con i compagni, con la docente e con altri amici fin dall'inizio dell'anno, quando hanno aperto – previa autorizzazione dei genitori – una casella personale di posta elettronica.

CONSIDERAZIONI

Già dalla prima lezione sono emersi dati interessanti. I ragazzi - non giudicati con votazione, ma coinvolti in un'attività di ricerca e analisi dell'indizio - hanno partecipato molto attivamente. In particolare, è stato accolto positivamente il fatto di aver proposto un testo differenziato per ciascun alunno, che ha potuto vivere l'esperienza come un'attività di problem solving e non come un'esercitazione tradizionale con risposta predeterminata. Questo ha avuto ricadute positive sul lavoro incrociato di verifica e commento di quanto scritto dai compagni.

Benché i commenti siano stati in gran parte pertinenti, non tutte le osservazioni degli studenti si sono rivelate corrette o condivisibili, e sono stati gli stessi compagni a segnalare dubbi e perplessità. Per esempio, alcuni studenti hanno individuato errori di ortografia in parole scritte correttamente; uno studente, non avendo capito che quella che analizzava era un'immagine e non la vera e-mail di spam, ha inserito tra i segnali di sospetto il fatto che il link non fosse attivo[5]; un altro ha sostenuto che, non avendo mai sentito parlare della banca "UBI", quella non esiste. Tutti elementi preziosi, che possono essere oggetto di analisi e discussione in una classe, per capire insieme la natura dell'errore commesso: in alcuni casi si tratta infatti di applicazioni sbagliate su intuizioni corrette. Ad esempio, in generale è un'ottima idea non fidarsi di una banca che non si è mai sentita nominare, e il fatto che UBI rientri fra queste è un problema di (comprensibile) ignoranza dello studente, non di cattivo ragionamento.

Gli alunni hanno individuato diversi elementi formali di cui tenere conto per verificare l'attendibilità di un'e-mail, e con la guida dell'insegnante li hanno categorizzati come segue: (1) frequenti errori ortografici, semantici, sintattici (in particolare le concordanze tra maschile e femminile, singolare e plurale) e di pragmatica (es., alternare il dare del tu al dare del lei al proprio interlocutore); (2) simboli strani (es., caratteri cirillici mischiati con quelli latini); (3) stranezze nel nome del mittente o nel suo indirizzo di posta elettronica (es., la sua coincidenza con quello del destinatario); (4) stranezze nel nome del destinatario (es., diverso dal nome effettivo associato all'indirizzo e-mail); (5) incongruenze (es., tra l'indirizzo del mittente e un eventuale indirizzo di posta elettronica segnalato nel testo); (6) mancanza di informazioni sufficienti (es., sulla ditta o sul prodotto che si vuole pubblicizzare). Al di là della forma, hanno individuato altri elementi, più raffinati e di più difficile categorizzazione, riconducibili per lo più a conoscenze enciclopediche (es., se spesso è necessario presentare la ricetta medica per acquistare dei farmaci, com'è possibile prenotare gli stessi online, senza alcun parere medico?; com'è possibile ottenere una laurea senza studiare alcunché, come invece viene promesso?; è possibile che ci sia gente che regala soldi a sconosciuti?).

Tutti questi sono elementi la cui analisi non si esaurisce nell'arco dell'attività proposta, ma che in quelle due ore hanno avuto un

5

Qui l'errore non riguarda l'equivoco dello studente sulla natura grafica dell'e-mail, bensì il fatto che il funzionamento o meno dei link non è un buon indizio sull'attendibilità del messaggio. Intanto, può capitare di trovare link inattivi in messaggi del tutto innocui, ad esempio a causa di interruzioni di riga introdotte automaticamente dal programma di posta elettronica. Inoltre, cliccare sui link di un messaggio "pericoloso" è proprio una delle cose da evitare, e una delle ragioni per cui è utile diagnosticare la natura dei messaggi prima di avventurarsi in ulteriori esplorazioni.

ruolo importante. A partire dal tema dello spam, all'inizio della lezione neppure citato dal docente, si è cercato di creare le condizioni affinché gli studenti identificassero i problemi, ponessero domande e riconducessero i dati emersi dalla loro analisi a conoscenze già acquisite.
Una delle caratteristiche di questa attività è la relativa brevità e la potenziale ricchezza, testimoniata dai numerosi stimoli per ulteriori sviluppi. L'esperienza ha catturato l'interesse degli studenti e trasmesso, attraverso esempi concreti, l'idea che saper usare un computer richiede la comprensione di diversi aspetti formali e semantici della comunicazione, muovendo dal riconoscimento di indizi formali verso l'abilità di osservazione, analisi, ricerca, sintesi, revisione delle proprie credenze. In tal senso l'esperienza descritta si iscrive in un filone di uso didattico delle risorse informatiche centrato sui *processi* da mettere in gioco piuttosto che su una visione delle TIC come strumento per trasmettere *contenuti* [Caviglia e Ferraris, 2008].
Infine, l'attività presentata pone gli studenti in una situazione protetta, senza reale contatto con "veri" messaggi pericolosi. Se questa è parsa una scelta difendibile per *avviare* questo tipo di attività, un naturale prosieguo, previo beneplacito della dirigenza scolastica, consiste nell'inviare agli studenti, usando un account fittizio, messaggi genuini uniti a finte e-mail di spam, che conducano a pagine create ad hoc, in cui si ribadiscono gli elementi cui prestare attenzione prima di affidarsi ad un messaggio proveniente da estranei L'obiettivo sarebbe quello di valutare la capacità diagnostica degli studenti in termini di veri/falsi positivi e negativi. Questo potrebbe essere eticamente discutibile, ma usare contesti realistici per responsabilizzare gli alunni - potenziali vittime - e metterli in grado di difendersi da soli è probabilmente l'unico modo per aiutarli ad emanciparsi.

riferimenti bibliografici

Aycock J. (2006), Teaching spam and spyware at the University of C@1g4ry, in *Third Conference on Email and Anti-Spam (CEAS 2006)*, short paper, pp. 137-141.

Aycock J., Crawford H., de Graaf R. (2008), Spamulator: The Internet on a Laptop, *ACM ITiCSE 2008*, pp. 142-147.

Cajani F., Costabile G., Mazzaraco G. (2008), *Phishing e furto d'identità digitale. Indagini informatiche e sicurezza bancaria*, Giuffrè, Milano.

Caviglia F., Cerulli M., Davidzon I., Delfino M. (in stampa), Spam e phishing. Se le conosci, le eviti, in A. Andronico, L. Colazzo (a cura di), *Didamatica 2009*.

Caviglia F., Ferraris M. (2008), Il Web come ambiente di apprendimento: fuoco sul processo, in A. Andronico, T. Rosselli e V. Rossano (a cura di) *Didamatica 2008 - Informatica per la Didattica*, Laterza, Bari, Parte II; pp. 955-959.

Dhamija R., Tygar J.D., Hearst M. (2006), Why Phishing Works, in the *Proceedings of the Conference on Human Factors in Computing Systems (CHI2006), April 22–27, 2006*, Montréal, Québec, Canada.

Frank C.E., Werner L.A. (2007), Getting A Hook On Phishing, *Information Systems Education Journal, 5* (36).

Gaggioli A. (2007), *Spam*, Il filo, Roma.

Kumaraguru P., Rhee Y., Acquisti A., Cranor L.F., Hong J., Nunge E. (2007), Protecting people from phishing: the design and evaluation of an embedded training email system, in *CHI-07: Proceedings of the SIGCHI conference on Human factors in computing systems*, 905-914. ACM Press: New York.

Kumaraguru P., Sheng S., Acquisti A., Cranor L.F., Hong J.I. (2008), PhishGuru: Lessons From a Real World Evaluation of Anti-Phishing Training. e-Crime Researchers Summit, *Anti-Phishing Working Group*, October 15 - 16, 2008, Atlanta, USA.

Kumaraguru P., Sheng S., Acquisti A., Cranor L.F., Hong J.I. (in stampa), Anti-Phishing Education, in *Proceedings of The International Conference on E-Learning in the Workplace.*

Robila S.A., Ragucci J. (2006), Don't be a Phish: Steps in User Education, in *Proceedings ITiCSE*, pp. 237-241.

Werner L.A., Courte J. (2008), Analysis of an Anti-Phishing Lab Activity, in *Proceedings of ISECON 2008*, v. 25 Phoenix.