Istituto di Terapia Cognitivo Interpersonale
Presidente: Prof. Tonino Cantelmi
www.itci.it

SICUREZZA

di

Massimiliano Marzocca

Arrivati sin qui, i ragazzi saranno sufficientemente pronti a riconoscere eventuali minacce ed individuare potenziali rischi che potrebbero incontrare navigando nel *Web*. Quest'ultimo paragrafo tirerà le fila di quanto affrontato precedentemente, aggiungendo diversi elementi e importanti spunti di riflessione per certi versi maggiormente tecnici, ma di necessaria trattazione. Teniamo a sottolineare però, che per una esaustiva argomentazione su di essi è bene fare riferimento a specifiche pubblicazioni sulla sicurezza informatica.

Prevenire è meglio che curare!

Il motto del presente capitolo, come recitava un vecchio slogan pubblicitario, potrebbe essere: *"inutile installare una porta blindata e rinforzare la finestra dopo che gli intrusi sono già entrati, bisogna prevenire!"*
I rischi sono molteplici, i principali li abbiamo già visti: violazione della *privacy*, furto di identità, cyberbullismo, adescamento *online*. Essi possono divenire ancora più temibili e meno controllabili poiché talvolta sono veicolati da "mezzi tecnici" complessi, sviluppati appositamente con finalità malevoli, come esempio i *virus* informatici.
Gli accorgimenti che potremmo adottare sono davvero tantissimi, in questa sede ci limiteremo a menzionarne due, che sono di larga diffusione e di facile comprensione, anche per i più piccoli.

Lezione 1

Password

La funzione della *password* è quella di assicurare che gli utenti non abbiano accesso ad un terminale, a meno che non dispongano delle autorizzazioni necessarie per farlo.
La *password* rappresenta quindi la chiave di accesso a molte delle informazioni riservate che custodiamo sui nostri computer.

Pochi semplici consigli ci tuteleranno da spiacevoli problemi:

1) La *password* deve essere "forte", ovvero NON composta da parole di senso compiuto, bensì da un insieme di numeri,lettere e simboli, superiore alle 8 unità.
2) La *password* deve essere diversa per ogni sito
3) La *password* è privata, e quindi non deve mai essere comunicata a nessuno.

Antivirus

Un *antivirus* è un *software* atto a prevenire, rilevare ed eventualmente eliminare programmi malevoli, in grado di danneggiare, spiare o rubare credenziali presenti sul computer "vittima". *L'antivirus* per poter funzionare al meglio, deve essere attivo, aggiornato e devono essere effettuate regolari scansioni per evitare che si propaghino eventuali infezioni.

Phishing

Il phishing è una truffa informatica che permette di carpire, attraverso un'e-mail, i dati di accesso personali ad un sito, ad un social network, ad un portale al quale si è registrati.

Avviene in questo modo: arriva nella nostra casella di posta elettronica un'e-mail che sembra provenire da un sito presso il quale siamo "registrati e che frequentiamo abitualmente, segnalandoci un imprecisato problema al sistema di verifica password.

La mail ci invita pertanto a cliccare su un link presente al suo interno, chiedendoci di "verificare" le nostre credenziali su di una pagina fasulla, che è però uguale in tutto e per tutto a quella originale. Una volta inserite, il truffatore avrà a disposizione i nostri dati di accesso e potrà così appropriarsi di dati, foto, informazioni che credevamo al sicuro. Pensate a cosa potrebbe succedere se con la stessa tecnica un malintenzionato accedesse ai dati della nostra banca!!! Il phishing è, senza mezzi termini, una truffa on-line, e coloro che la attuano, chiamati "phisher", non sono altro che ladri di informazioni personali con competenze tecniche. Il termine "phishing" è una variante di "fishing" che, in lingua inglese significa letteralmente "pescare", metafora del pescatore che "fa abboccare all'amo" le proprie prede.

"Bufale" ed attendibilità delle fonti

Internet permette di accedere ad una quantità di informazioni impensabile fino a pochi anni orsono, è tuttavia necessario ricordare che non sempre tali informazioni sono documentate, attendibili e scritte da autori competenti. Sostanzialmente quindi, non tutto ciò che rinveniamo tra le pieghe del web rappresenta una fonte affidabile di conoscenza.

Ciò accade perché:

1) Chiunque, per qualsiasi scopo, può creare un sito e metterlo online rendendolo credibile agli occhi di chi legge.

2) Non esistono controlli su ciò che viene pubblicato nel Web e le informazioni non veritiere non sono rimosse neppure quando vengono scoperte.

3) Quasi nessuno controlla le informazioni che legge e tende a diffondere ciò che lo colpisce senza alcun controllo.

4) Le informazioni fantasiose e sensazionalistiche attirano molto più facilmente rispetto a quelle veritiere.

5) Internet è il luogo ideale dove attirare persone con la finalità di acquisre notorietà e guadagnare denaro.

6) La maggior parte degli utenti del Web non ha le capacità per riconoscere le bufale perché è profondamente impreparato in materie scientifiche e storiche.

La semplicistica convinzione che ogni notizia rinvenuta sul Web sia attendibile, fa sì che molte persone incappino ricorrentemente in bufale e truffe di ogni tipo, anche perché chi "confeziona" simili raggiri ben conosce i trucchi sia psicologici sia di forma che rendono credibile ciò che scrive.

Riuscire ad individuare falsi su internet non è una operazione semplice poiché, come già detto, i falsi vengono presentati in modo elaborato o comunque con un aspetto apparentemente professionale ed accattivante, in modo da indurre ad abbassare le difese e farsi sopraffare dalla bufala.

La diffusione di truffe e bufale è così capillare che sovente miete vittime anche tra i giornalisti, cioè tra chi ha una preparazione certificata in materia. Spesso le bufale dal web hanno migrato sui media tradizionali, con conseguenze letteralmente disastrose. Risulta dunque fondamentale vincere la pessima e consolidata abitudine, di non verificare "alla fonte" e su siti attendibili, l'informazione che si è letta.

Le pubblicazioni attendibili sono quelle caratterizzate da una struttura definita, che consente il controllo delle informazioni e le revisioni editoriali. Un sito attendibile è un sito che fa capo ad una università, o ad un centro di ricerca, o ad una struttura governativa. E' bene dunque, prima di diffondere una informazione "sensazionale" appena appresa dal Web, verificarne la sua esattezza.