Sicurezza in ufficio

Conoscere i pericoli in rete e comportarsi di conseguenza

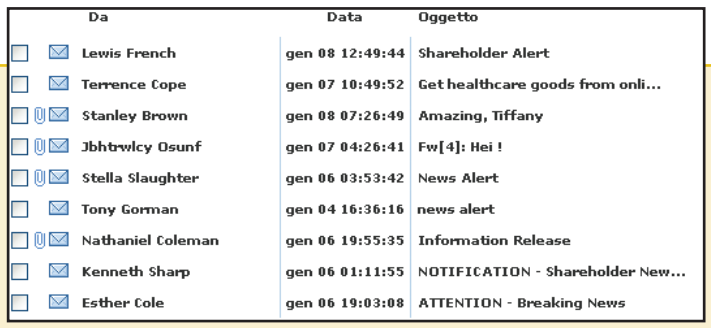
In una delle precedenti lezioni abbiano analizzato quali sono le differenze tra virus, worm e trojan horse. Vediamo quali soluzioni adottare per difenderci da questi e altri pericoli che possono nascondersi nel Web e causarci piccoli o grandi problemi. Conoscendo le minacce e le contromisure che abbiamo a disposizione e muovendoci con la dovuta cautela, possiamo garantirci una navigazione tranquilla nel… mare di Internet!

I **pericoli** che possiamo incontrare su **Internet** sono decisamente tanti: virus, worm, trojan, spamming, dialer, spyware, phishing e truffe varie. Cerchiamo di capire meglio di cosa si tratta e come difenderci in caso di "attacco".

Virus, **worm** e **trojan horse** sono software che, una volta entrati nel nostro sistema, sono in grado di replicarsi e di diffondersi all'interno del computer, provocando danni più o meno seri; attualmente una delle vie più comuni attraverso cui questi software si introducono nel nostro sistema è la **posta elettronica** (in passato invece sfruttavano i supporti esterni, come i floppy-disk).

Onde evitare spiacevoli contagi, dobbiamo quindi prestare molta attenzione agli **allegati** contenuti nelle email che riceviamo e ai **file** che vengono condivisi da fonti non sicure durante collegamenti a chat o a software P2P (peer-to-peer).

Dobbiamo poi anche installare sul nostro PC, e tenere periodicamente aggiornato, un **software antivirus**: ne esistono molti, anche gratuiti, che effettuano l'aggiornamento in automatico quando siamo connessi a Internet. Evitiamo sempre, comunque, di aprire allegati il cui mittente è sconosciuto, prestando molta attenzione agli allegati con **estensioni particolari**, come vbs, bat, exe, o in cui non compare l'**oggetto** del messaggio, anche se il mittente è conosciuto; eliminiamo subito gli allegati sospetti.



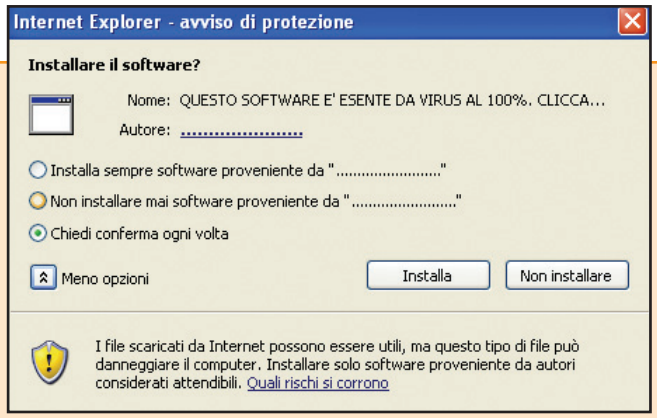
Da	Data	Oggetto
Lewis French	gen 08 12:49:44	Shareholder Alert
Terrence Cope	gen 07 10:49:52	Get healthcare goods from onli...
Stanley Brown	gen 08 07:26:49	Amazing, Tiffany
Jbhtrwlcy Osunf	gen 07 04:26:41	Fw[4]: Hei !
Stella Slaughter	gen 06 03:53:42	News Alert
Tony Gorman	gen 04 16:36:16	news alert
Nathaniel Coleman	gen 06 19:55:35	Information Release
Kenneth Sharp	gen 06 01:11:55	NOTIFICATION - Shareholder New...
Esther Cole	gen 06 19:03:08	ATTENTION - Breaking News

Un problema diverso è rappresentato dallo **spamming**, ossia l'invio generalizzato di email pubblicitarie senza il consenso dei destinatari.

Lo spamming è **perseguito legalmente**, perchè comporta una spesa per chi lo subisce in termini di perdita di tempo, intasamento della rete e misure di contrasto.

Per difenderci dallo spamming, dobbiamo innanzitutto evitare che il nostro indirizzo email vada a finire in mani "sbagliate": se frequentiamo chat, newsgroup, forum o utilizziamo software come ICQ, Messenger o simili, forniamo un **indirizzo alternativo** a quello che utilizziamo solitamente. È comunque fondamentale non rispondere mai a un messaggio di spam, neanche per "cancellarsi" dalla lista, per evitare di far capire al mittente che il

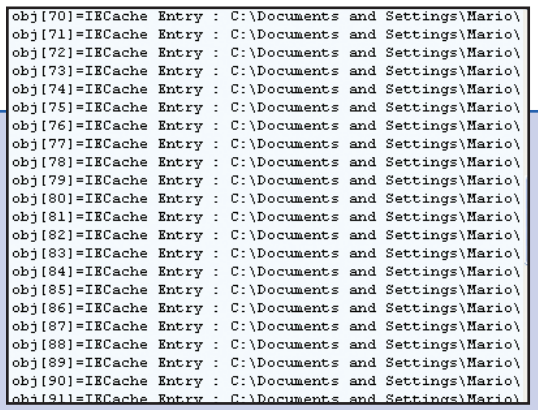
nostro account di posta è attivo e venire sommersi da altro spam. Possiamo poi attivare dei **filtri** antispam per evitare che questi messaggi intasino la nostra casella. Possiamo poi ancora ricorrere a programmi specifici (alcuni gratuiti sono anche reperibili in Internet) e segnalare ad apposite organizzazioni antispamming l'indirizzo del mittente.



I **dialer** sono invece programmi (con estensione .**exe**) che, una volta scaricati e lanciati, modificano la connessione predefinita per il collegamento a Internet utilizzando **numeri telefonici a pagamento** (con prefissi come 709, 899, 166, 144 ecc.) o **numeri internazionali** (tipo +00773).

Solitamente questi software sono "mascherati" da programmi che permettono di scaricare suonerie o loghi per i cellulari, sfondi per il PC, MP3 o materiale pornografico. Questi siti sono obbligati, per legge, a comunicare i costi della connessione, ma spesso tendono a mettere in secondo piano, o addirittura a nascondere, queste informazioni: in questo modo, potremmo continuare a navigare su Internet inconsapevoli dei costi reali della connessione.

Il problema non coinvolge le connessione **ADSL**; se invece abbiamo una connessione con modem tradizionale, possiamo richiedere al **gestore telefonico** di disattivare sulla nostra linea i numeri a pagamento. Esistono anche in questo caso software che possono proteggere il nostro PC, ma la protezione migliore è comunque evitare di scaricare file .**exe** da siti "sospetti".



Gli **spyware** sono software che, una volta installati nel sistema, riescono a registrare e a diffondere, a nostra insaputa, **informazioni riservate**, solitamente a scopi commerciali. Spesso gli spyware si trovano all'interno di software gratuiti che, quando vengono lanciati, visualizzano banner pubblicitari; possiamo rimanere vittime degli spyware anche navigando su siti "pericolosi" (pornografici e di gioco d'azzardo) o utilizzando applicazioni particolari come il peer to peer, che consente di condividere e scambiare file tra più utenti.

Gli spyware possono forzare la nostra navigazione verso siti prestabiliti, causare l'apertura incontrollata di finestre pop-up, oppure connetterci a dialer. Possono anche arrivare a rendere instabile il nostro PC, fino a causarne il blocco totale. Per risolvere questo problema utilizziamo il **firewall** e **software opportuni**, reperibili su Internet anche in versione gratuita.

NOTE

Il **phishing** è una truffa ormai molto diffusa: falsi messaggi di siti frequentati abitualmente ci possono richiedere di reinserire dei dati (solitamente i numeri delle carte di credito), dichiarando che questi sono andati persi per problemi tecnici; dirottati su siti simili all'originale, potremmo così rischiare di "consegnare" ai truffatori il nostro numero di conto corrente.

Al di là di questo pericolo, è sempre buona norma non utilizzare mai le nostre **carte di credito** per acquisti su Internet; utilizziamo, al loro posto, le carte di credito prepagate, che ci permettono di operare con tranquillità dato che la perdita, al massimo, sarà pari alla ricarica effettuata.