Pericoli e insidie delle e-mail

La posta elettronica è uno degli strumenti di Internet più utilizzati. Consente alle persone che hanno dimestichezza con il computer e con Internet di comunicare velocemente ed efficacemente fra di loro.

Un messaggio e-mail, anche se provvisto di allegati più o meno pesanti (file di testo, immagini o video digitali, file musicali) raggiunge il destinatario in pochi minuti rimbalzando fra vari server prima di arrivare a destinazione nella casella di posta elettronica del destinatario.

Anche se qualche volta non tutto fila liscio e qualche messaggio può anche andare perduto, il "protocollo" è tutto sommato molto funzionale.

Il problema nell'uso della posta elettronica nasce dal fatto che è troppo facile usarla e, a volte, anche abusarne. Molti hanno scoperto che gli indirizzi e-mail possono essere collezionati, classificati e sfruttati per l'invio di pubblicità: si sono così creati **archivi abusivi di indirizzi** che vengono tenuti aggiornati e venduti alle aziende che hanno interesse a promuovere un loro prodotto.

Tale realtà nel corso degli anni ha portato al diffondersi del fenomeno dello **spamming**, cioè dell'invasione delle caselle postali da parte di messaggi indesiderati: pubblicità per medicinali, prodotti finanziari, lavori dai guadagni favolosi…

Ma, oltre allo spamming, si è diffuso anche il fenomeno del **phishing**, cioè della richiesta di dati personali con lo scopo di appropriarsene per mettere in atto truffe nei confronti degli utenti.

Un terzo pericolo che incombe nelle caselle e-mail è la diffusione di pericolosi **virus** e di fastidiosi **trojan**, cioè programmi che, pur non danneggiando il computer, ne compromettono il buon funzionamento.

Vediamo brevemente come arginare questi fastidiosi e pericolosi fenomeni.

Lo spamming

L'interesse degli *spammatori* è quello di raggiungere quanti più utenti possibile, che diano seguito ai messaggi pubblicitari.

- Un primo comportamento che scoraggi questi abusi consiste nell'**evitare** di servirsi di questi canali per procedere a **qualsiasi acquisto**.
- Un altro accorgimento per vanificare lo spam, è quello di **non rispondere mai a questo tipo di messaggi**, nemmeno per contrastarli. Ciò servirebbe infatti solo a confermare agli *spammatori* il raggiungimento del loro obiettivo.

In linea di principio, sarebbe addirittura una buona pratica quella di **non aprire i messaggi di posta elettronica provenienti da sconosciuti**. È comunque consigliabile cancellare del tutto messaggi contenenti allegati anche se provenienti da persone conosciute, che però non abbiano preannunciato tale invio. Questi messaggi, infatti, potrebbero non essere stati inviati dai nostri amici, ma da un *malware* che si è impadronito del loro indirizzo di posta elettronica, e che ci inoltra e-mail dannose.

È inoltre buona norma **evitare di dare seguito a messaggi a catena** che, in genere, contengono leggende metropolitane o bufale, cioè notizie non verificate o non più attuali. Tali messaggi sono stati in genere creati proprio per intasare le caselle di posta elettronica.

Quando si scrivono **e-mail a più destinatari**, evitare di aggiungere gli indirizzi nel campo "A", ma **usare il campo "Ccn"**. La differenza è subito intuibile: gli indirizzi nel campo "A" appaiono a tutti i destinatari e quindi possono finire in mano agli *spammatori*, mentre gli indirizzi nel campo "Ccn" (che vuol dire *Copia carbone nascosta*) sono invisibili.

Se si vuole **iscriversi a forum o a newsgroup**, è consigliabile usare un indirizzo e-mail non importante, eventualmente sacrificabile. Gli indirizzi presenti nei newsgroup, infatti, sono manna per gli *spammatori*, in quanto rivelano anche i gusti e gli interessi dei possessori degli indirizzi di posta elettronica. La pubblicità veicolabile verso tali indirizzi potrà così essere opportunamente mirata.

Nel combattere lo spamming non siamo soli: molti **client di posta elettronica** consentono di **impostare delle regole per eliminare lo spam**. Inoltre, è possibile installare programmi che filtrano messaggi evidentemente non richiesti. Alcuni sono gratuiti e possono essere configurati dedicando pochi minuti di attenzione. È possibile scegliere il programma a noi più congeniale inserendo i termini "mail spam software" in un motore di ricerca. Teniamo conto che a volte tali filtri possono essere "troppo prudenti" e cestinare messaggi che vengono riconosciuti come spam ma che tali non sono.

La prudenza non è mai troppa!

Il phishing

Mentre lo spamming colpisce tutti indiscriminatamente, il **phishing** in genere si rivolge agli utenti che hanno acceso un rapporto con una banca o con un servizio finanziario on line in genere. L'obiettivo del "pescatore" è quello di cogliere all'amo i dati personali (nome utente e password) con il quale l'utente accede a un servizio.

Il meccanismo per entrare in possesso di questi dati tramite e-mail funziona più o meno così. Il truffatore finge di essere la vostra banca e, allertandovi sul verificarsi di abusi di vario tipo, vi propone di "verificare la sicurezza dell'accesso" attraverso un link al quale vi invita a collegarvi per modificare o controllare i dati di accesso.

In realtà il link fornito non porta al sito della banca ma a un sito fasullo costruito ad arte dal truffatore: l'utente, cadendo nella trappola, inserirà i propri dati personali di accesso.

Posizionando il cursore del mouse sopra il link è possibile verificare la falsità del collegamento. Nella barra di stato del client di posta elettronica possiamo inoltre verificare la corrispondenza con l'indirizzo della nostra banca.

È essenziale **non seguire mai tali link**, anche se la truffa può apparire verosimile.

Una volta che il truffatore ha registrato i nostri dati, se ne può servire per accedere al nostro conto bancario e per tentare di portare a termine un furto di denaro, dopo che ha già avuto

successo con il furto dei nostri dati.

Alcuni consigli:

- **Non aderire mai alle richieste di dati personali**.
  I siti delle banche non usano tali procedure, quindi sospettate immediatamente di proposte simili e cestinate le e-mail fasulle. Tanto meno evitate di seguire i link, che sono pericolose trappole.
- **Verificare frequentemente il proprio conto in banca**.
- **Verificare** che i siti cui si fa riferimento nelle e-mail che ricevete, abbiano **connessioni protette** (prefisso *https* nell'indirizzo della pagina) e chiusura del lucchetto nella barra di stato del browser.

I virus

Le e-mail possono essere veicolo di **virus**. Il pericolo non è rappresentato soltanto dagli allegati. Spesso nelle immagini e nel corpo di una e-mail in html può nascondersi un software maligno. Per questo motivo è preferibile **inviare le e-mail in formato testo**.

Altro tipo di attacco è costituito dal **malware** che 'entra' nel computer, si impadronisce della nostra lista dei contatti e si autospedisce senza la nostra autorizzazione: in questo modo tutti i nostri amici e corrispondenti riceveranno messaggi insignificanti o quasi, con il solo scopo di replicare il danno in maniera esponenziale. Filtri presso i provider e procedure antivirus riescono a frenare la pazza corsa di questi applicativi virali, ma non sempre sono sufficienti.

Occorre fare molta attenzione anche nell'aprire tali e-mail: prudenza vorrebbe una **cancellazione "a priori"**, chiunque sia il mittente.

Per difenderci da questi attacchi possiamo ottenere aiuto dal **software antivirus**. Ricordiamoci di verificare un automatismo che in genere quasi tutti gli antivirus posseggono, cioè l'**abilitazione del controllo anche della posta elettronica in arrivo e in partenza**. Tale abilitazione dovrebbe rendere più tranquilli sia voi sia i vostri destinatari.

Le e-mail sono uno strumento potente e utile: attenzione, però, che, oltre a veicolare simpatici e utili messaggi, non portino sul nostro computer anche "bombe" non desiderate o, peggio, dannose!