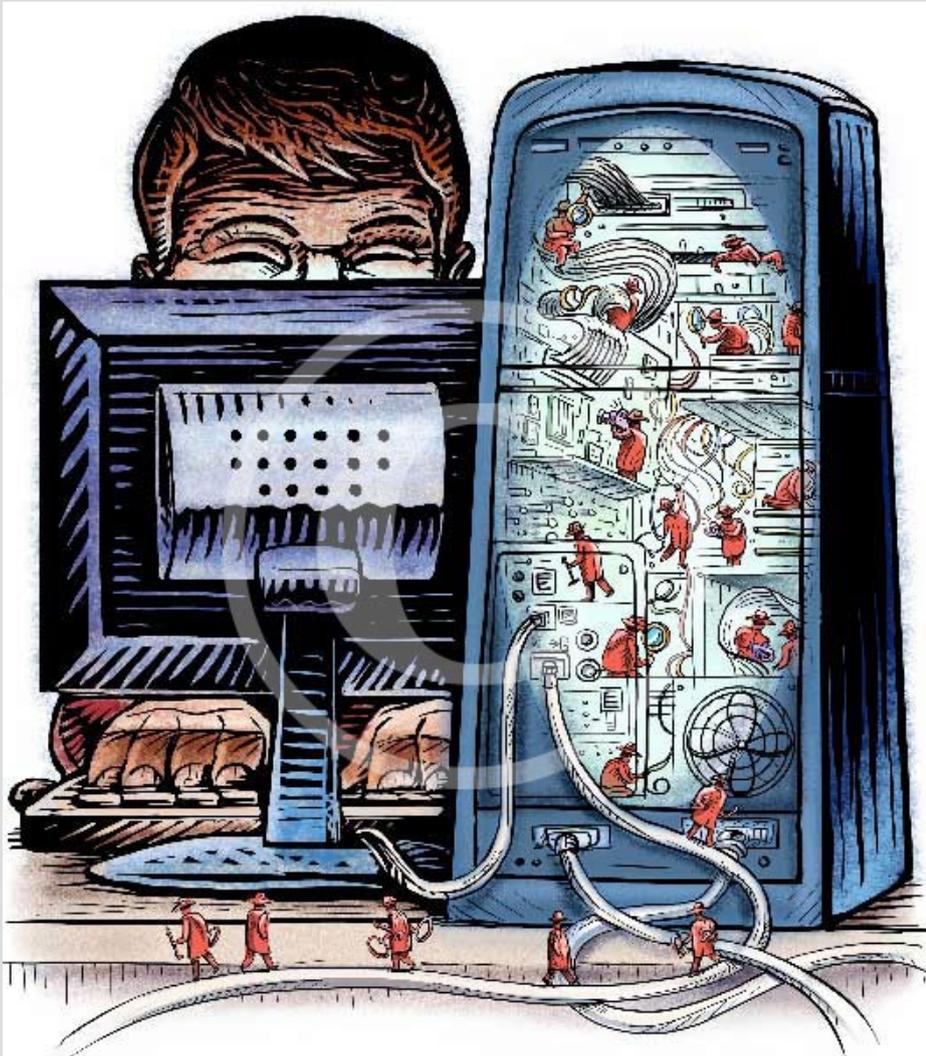


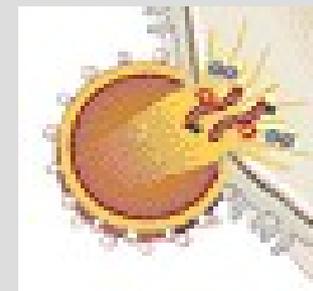
# Sicurezza in rete



**Virus-antivirus**  
**Attacchi dalla rete-firewall**  
**spyware-antispy**  
**spam-antispam**

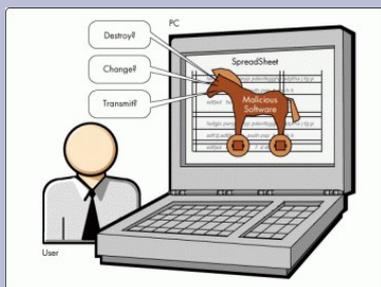
# Virus Informatici

Un **virus informatico** è simile ad un virus biologico: si tratta di un **piccolo programma**, che contiene una sequenza di istruzioni di cui alcune sono deputate alla **replicazione** dell'intero programma.



# Tipi di Virus Informatici

- **virus polimorfico**: è un virus che implementa una routine di **mutazione**, che gli permette di modificare il proprio codice (meno la routine di mutazione stessa) ad ogni nuova infezione, in modo da rendere più difficoltosa l'individuazione da parte dei software antivirus.
- **virus metamorfico**: simile al virus polimorfico, è però in grado di **mutare completamente** il proprio codice.
- **Macrovirus**: può essere contenuto generalmente in un documento di **Microsoft Word, Microsoft Excel o Microsoft PowerPoint** e consiste in una macro; può diffondersi a tutti i documenti che vengono aperti con quella particolare applicazione.



# Modalità di diffusione

## *Software Maligno*



- **worm:** (letteralmente "verme") è una particolare categoria di **malware (software maligno)** in grado di **autoreplicarsi**. È simile ad un virus, ma a differenza di questo non necessita di legarsi ad altri eseguibili per diffondersi.
- **trojan o trojan horse:** (dall'inglese per Cavallo di Troia), è un tipo di **malware (software maligno)**. Deve il suo nome al fatto che le sue funzionalità sono nascoste all'interno di un programma apparentemente utile; è dunque l'utente stesso che installando ed eseguendo un certo programma, inconsapevolmente, installa ed esegue anche il codice trojan nascosto.

# Falsi Positivi

*finti virus – bufale - scherzi*

- **Hoax:** (tradotto a volte in lingua italiana come bufala o burla) indica quei messaggi (in genere e-mail) contenenti comunicati, avvertimenti o richieste di aiuto di contenuto fasullo e ingannevole, che attraverso dei meccanismi di ingegneria sociale invitano ad essere rispediti al maggior numero di persone, in maniera tale da aumentare la diffusione in maniera esponenziale. Principalmente si tratta di leggende metropolitane, che magari prendono spunto da fatti realmente accaduti; **spesso riguardano virus inesistenti che eseguirebbero fantasiose operazioni distruttive (gran parte delle quali irrealizzabili da un punto di vista tecnico).**

# Antivirus

*come difendersi dal malware*

- Non è rilevante conoscere il nome di un virus: normalmente prima di essere spedito viene sempre rinominato e poi esistono **centinaia di migliaia di varianti!!!**.
- Non pensare mai di disinstallare un virus semplicemente cancellando un file, troppo semplice!!!.
- Affidarsi sempre e comunque ad un **antivirus** costantemente aggiornato e residente in memoria che controlli il web e la posta elettronica e che abbia implementato un dispositivo **heuristico** per la ricerca di virus sconosciuti



# Spioni della rete *spyware*

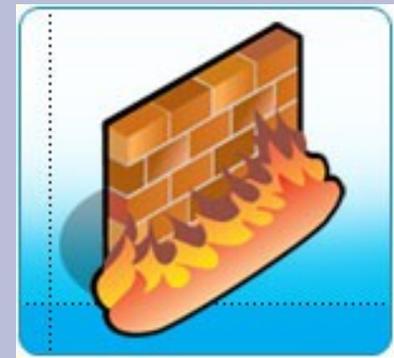


- **Spyware:** è un tipo di software che raccoglie informazioni riguardanti l'attività online di un utente (siti visitati, acquisti eseguiti in rete etc) senza il suo consenso, trasmettendole tramite Internet ad un'organizzazione che le utilizzerà per trarne profitto, tipicamente attraverso l'invio di pubblicità mirata o per scopi di lucro.
- L'arma migliore per difendersi dagli **spyware** è diffidare da qualsiasi software offerto gratuitamente su Internet: come detto l'inclusione in programmi molto scaricati è il mezzo più frequente di diffusione di questi malware.
- Evitare di scaricare ed installare software pirata e di navigare in siti porno o che offrono strumenti per piratare il software originale.

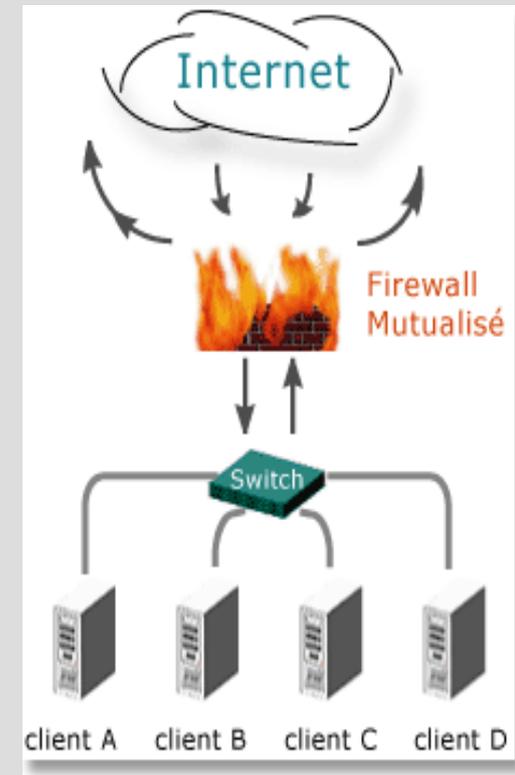


# Firewall

## *attenti alla rete*



- **Firewall:** (termine inglese dal significato originario di *paratia* o *muro antifuoco*) Software o apparato di rete hardware che filtra tutti i pacchetti entranti ed uscenti, da e verso una rete o un computer, applicando regole che contribuiscono alla sicurezza della stessa.
- La funzionalità principale in sostanza è quella di creare un filtro sulle connessioni entranti ed uscenti, in questo modo il dispositivo innalza il livello di sicurezza della rete e permette sia agli utenti interni che a quelli esterni di operare nel massimo della sicurezza.



# Cosa è lo SPAM ?

*Internet oggi*

La **SPAM** (Spiced Ham), era carne in scatola che veniva fornita ai soldati dell'esercito americano, per questo motivo si guadagnò una fama piuttosto negativa.

Nel gergo **Internet**, lo **spam** ha invece assunto un significato del tutto differente, ma mantiene la sua connotazione negativa. Lo **spamming** in Internet consiste nell'invio di messaggi pubblicitari di posta elettronica (SPAM) che non siano stati in alcun modo sollecitati.



# Phishing o Pishing

## *La nuova truffa informatica*

Il **Phishing** è un sistema illegale per raccogliere dati sensibili come le informazioni sulla propria carta di credito o accessi ad account bancari. **La modalità con cui si realizza questa truffa è molto semplice** e consiste nell'invio di false e-mail con grafica e loghi ufficiali di eBay, PayPal, ma anche di servizi di Bancari e di Carte di Credito, chiedendo di riempire un modulo su una pagina web con indirizzo internet presente nella stessa E-mail.

