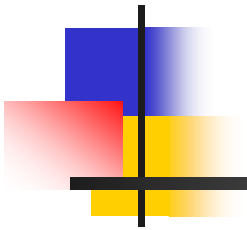


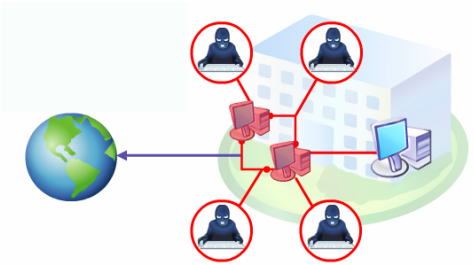
Informatica
Corso AVANZATO

Internet Protection: Firewall, Virus e Spam

Dott. Paolo PAVAN

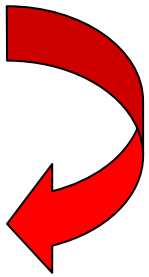
Collegarsi ad Internet: un'opportunità un rischio

- Al giorno d'oggi collegare semplicemente un computer ad Internet significa esporlo ad ogni sorta di rischi, un po' come uscire di casa e dimenticarsi di chiudere la porta a chiave.
- Occorre dotarsi di una serie di strumenti di difesa minimi, potremmo definirli una "sorta di antifurti"



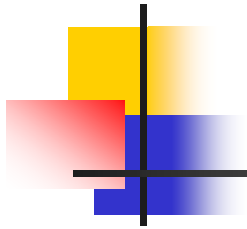
Cos'è la Sicurezza Informatica?

- E' la capacità di proteggere la:
  - Riservatezza
  - Integrità
  - Disponibilità



delle informazioni:

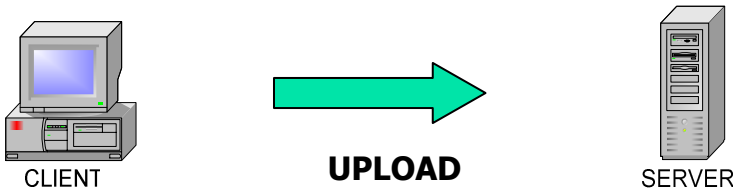
- Elaborate dai computer
- Memorizzate su supporti (archivi e/o database)
- Trasmesse attraverso linee e reti di comunicazione (dati o fonia)



Rischi informatici

- Umani
  - Voluti
    - Hacker
    - Violazioni di sistema
    - **Virus informatici**
  - Accidentali
    - Danno per negligenza e imperizia
- Disastri naturali
  - Inondazioni
  - Incendi

Scambio Dati: fonti del Contagio

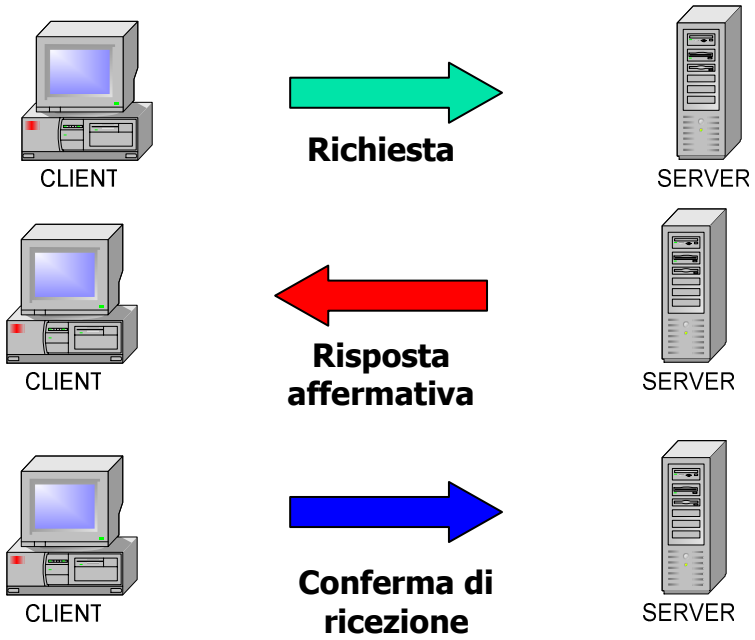


Carico i dati (file) su un server internet remoto in modo da poterli condividere e distribuire con gli utenti di tutto il mondo.

Scarico i dati (scarico email, file, musica, video) da un server sul mio computer locale

Sessione TCP: 3 way handshake
Cosa deve far passare un Firewall

- Richiesta e risposta: connessione SYN/ACK:



4 Livelli di Pericolo

- **Virus**
  - → Antivirus
- **Accessi Indesiderati**
  - → Firewall
- **Spyware/Malware/Trojan**
  - → Antispyware
- **Spam**
  - → Antispam

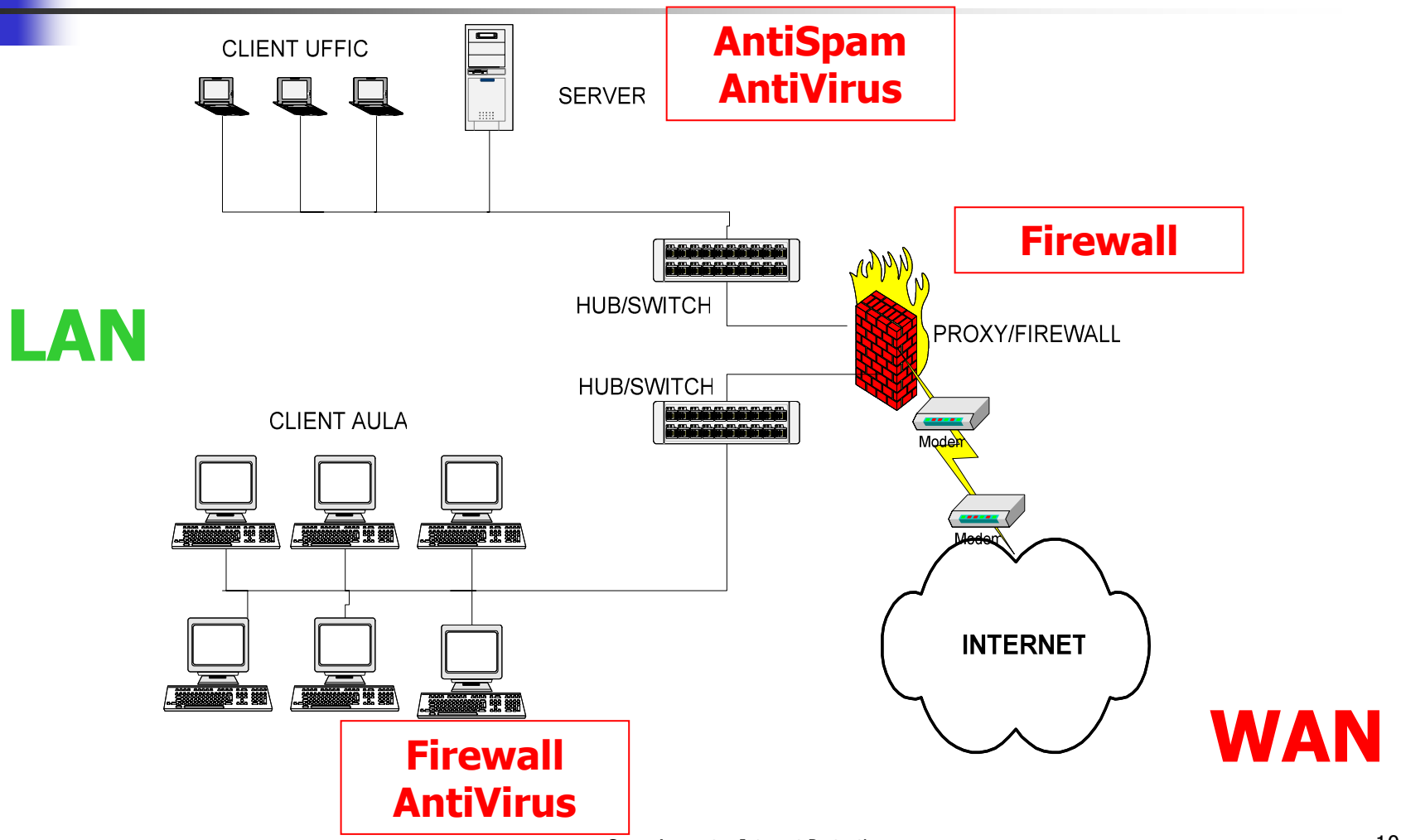
Come funzionano questi strumenti

- **Antivirus**
  - Controlla i file presenti nel computer sulla base di un database di firme costantemente aggiornato via Internet
  - Presenta uno strumento attivo in memoria (RAM) del computer e intercetta qualsiasi virus che vada in esecuzione
- **Firewall**
  - Filtra le connessioni (pacchetti) che entrano, escono ed attraversano il computer. Permette di stabilire quale connessione sia abilitata a transitare da e per il nostro computer
- **Antispyware**
  - Controlla il nostro computer (file temporanei, cookies, barre e popup) alla ricerca di programmi sospetti ed eventualmente li rimuove. E' una estensione dell'antivirus, ma in genere è un programma separato
- **Antispam**
  - Controlla la posta in ingresso sulla base di una serie di regole o criteri e permette di intercettare e bloccare messaggi non desiderati. Ad esempio blocca sulla base del mittente, dell'oggetto o del corpo del messaggio, della dimensione o dell'allegato.

Strumenti di Protezione per Windows gratuiti

- Antivirus
  - http://www.free-av.com/
- ZoneAlarm
  - http://www.zonelabs.com/store/content/home.jsp
- SpyBot Search & Destroy
  - http://www.safer-networking.org/en/download/
- Antispam
  - http://www.spampal.org/download.html
  - http://www.spamihilator.com/download/
  - http://www.spamterminator.it/download.asp

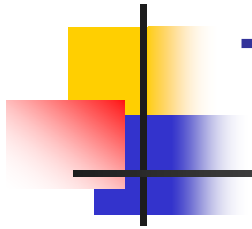
LAN to WAN
Rischi per Client e Server



Virus Informatici

Un virus informatico è un programma, cioè una serie di istruzioni scritte da un programmatore ed eseguibili da un computer, che ha le seguenti caratteristiche:

- è stato scritto per **inglobarsi** e cioè confondersi alle istruzioni di altri programmi modificandoli;
- chi l'ha scritto ha previsto la possibilità che il virus sia in grado di **replicarsi**, ovvero di copiare le istruzioni che lo compongono in altri programmi;
- dopo un tempo prestabilito, necessario per effettuare la replicazione, il virus comincia a **compiere l'azione** per cui è stato scritto, che può consistere, per esempio, nel **distruggere dati** e/o programmi presenti su di un supporto magnetico o, semplicemente, nel far comparire a video un messaggio oppure **spedire a ripetizione messaggi di posta elettronica** (spam).

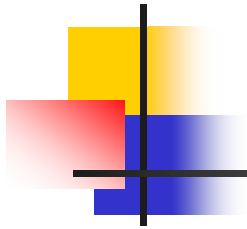


Tipi di Virus

- La nomenclatura tradizionale prevede diverse tipologie di Virus, le principali sono:
  - virus polimorfico
  - exe e com virus
  - companion (replicanti) virus
  - virus di boot
  - macrovirus
  - virus multipiattaforma
  - Worm e Trojan Virus (Cavalli di Troia)
- Ciò che distingue i virus propriamente detti dai worm è la modalità di replicazione e di diffusione: un **virus è un frammento di codice che non può essere eseguito separatamente** da un programma ospite, mentre un **worm è un applicativo a se stante.** Inoltre, alcuni worm sfruttano per diffondersi delle vulnerabilità di sicurezza, e non dipendono quindi dal fatto di ingannare l'utente per farsi eseguire.

La diffusione dei Virus: Internet e la posta elettronica

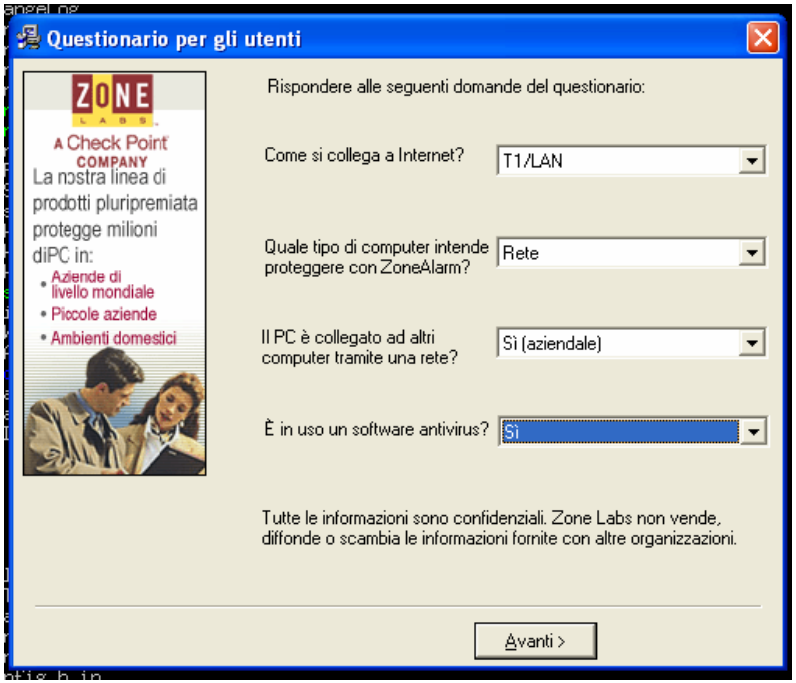
- Oggi il metodo principale di infezione **avviene per email,** una volta erano floppy e poi i CD.
  - La mail può contenere un **allegato potenzialmente pericoloso**. E' l'esecuzione del file allegato (un file eseguibile) sul nostro computer a causare l'infezione. Quindi il messaggio non è pericoloso solo perché lo si è ricevuto ma quando viene letto (aperto) e l'allegato eseguito.
  - Il solo messaggio di posta (un semplice file di testo) non può propagare un virus, anche se le mail info formato HTML possono contenere codice javascript potenzialmente dannoso, in grado di autoeseguire dei programmi
  - I file di Office (Word ed Anche Excel in particolare) possono contenere set di istruzioni (macro) in grado di eseguire operazioni dannose sul nostro PC



Politica semplificata di un Firewall

- Effettua un filtraggio dei "pacchetti" che lo attraversano
  - INPUT
  - OUTPUT
  - FORWARD
- Nego tutto in partenza
  - Abilito solo determinati protocolli
  - Abilito solo determinati servizi/applicativi
  - Filtro per indirizzo IP sorgente e destinazione

Come funziona ZoneAlarm



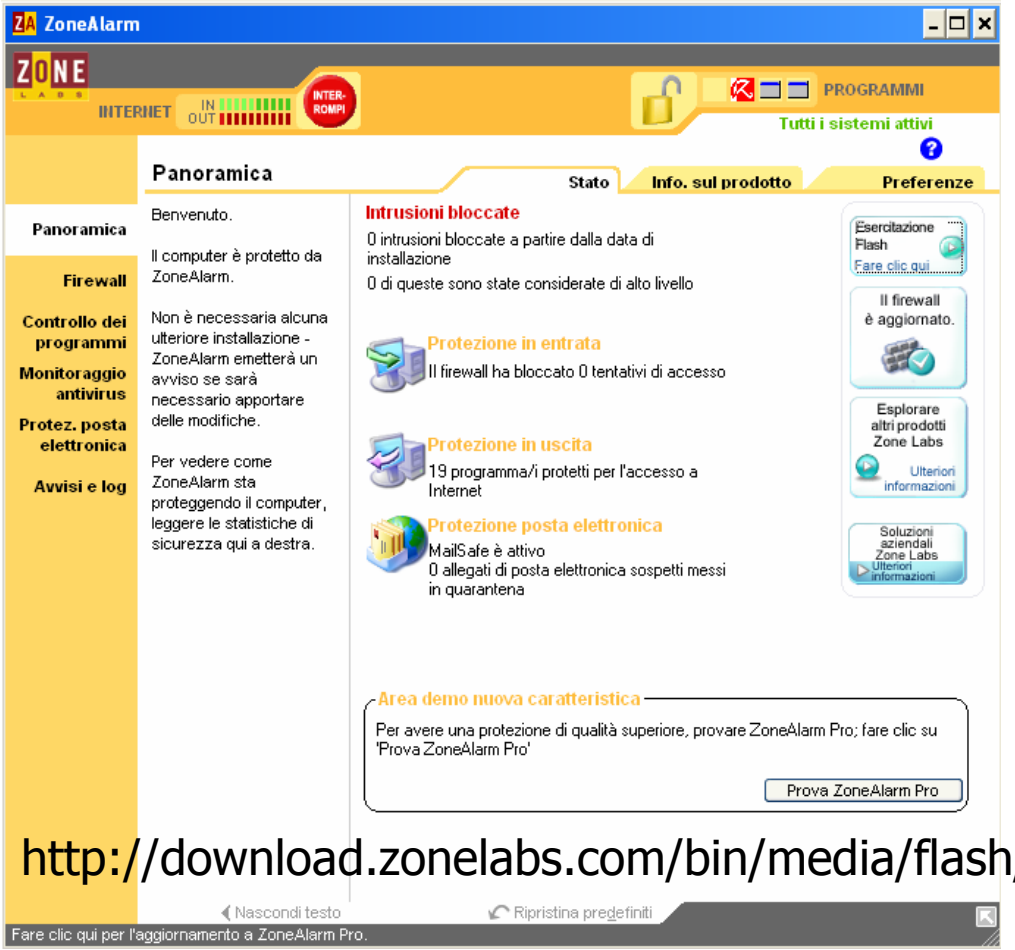
Installazione

- Specificare come ci si collega ad internet
- Se si condivide l'accesso con altri computer in rete locale oppure se lo si usa come singolo computer da casa

Pregi/Difetti

- Facile da Installare
- Semplice da configurare
- Subito operativo

L’interfaccia di ZoneAlarm



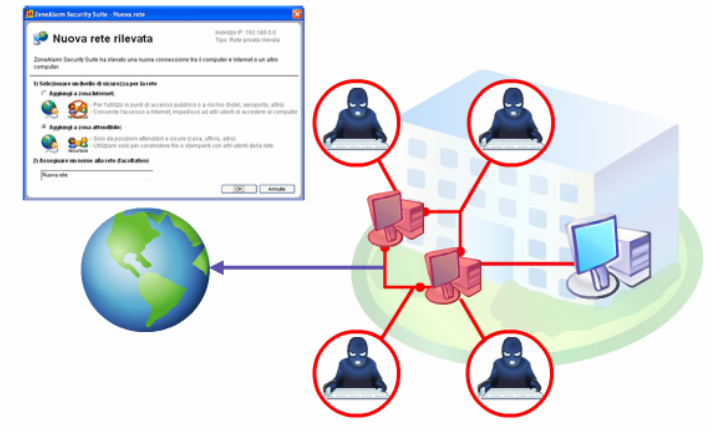
- Panoramica
- Firewall
- Controllo Programmi
- Monitoraggio Antivirus
- Protezione Posta elettronica
- Avvisi e Log

http://download.zonelabs.com/bin/media/flash/clientTutorial/it/overview.html

La logica di ZoneAlarm

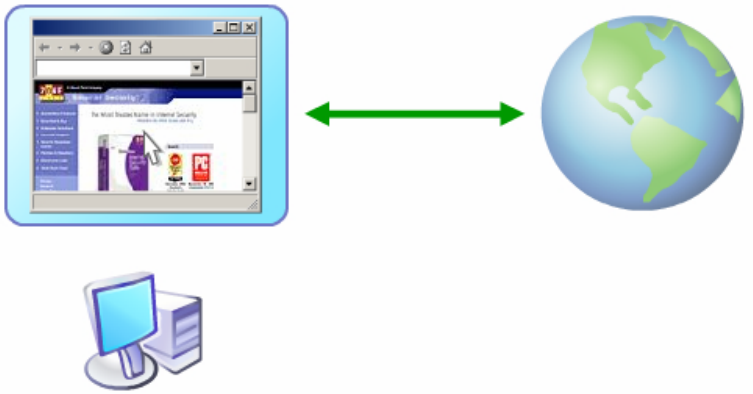
- Le zone:
  - Zona Internet (Protezione Alta)
    - È la zona relativa alla connessione ad internet, in pratica coincide con la nostra scheda di rete.
    - In questa zona il computer è invisibile e protetto dagli attacchi
  - Zona Attendibile (Protezione Media)
    - Zona in cui il computer condivide informazioni con altri computer della rete.
    - Gli host o le reti della zona attendibile vanno specificati per consentire l'accesso al sistema

Le zone e l'abilitazione dei Programmi

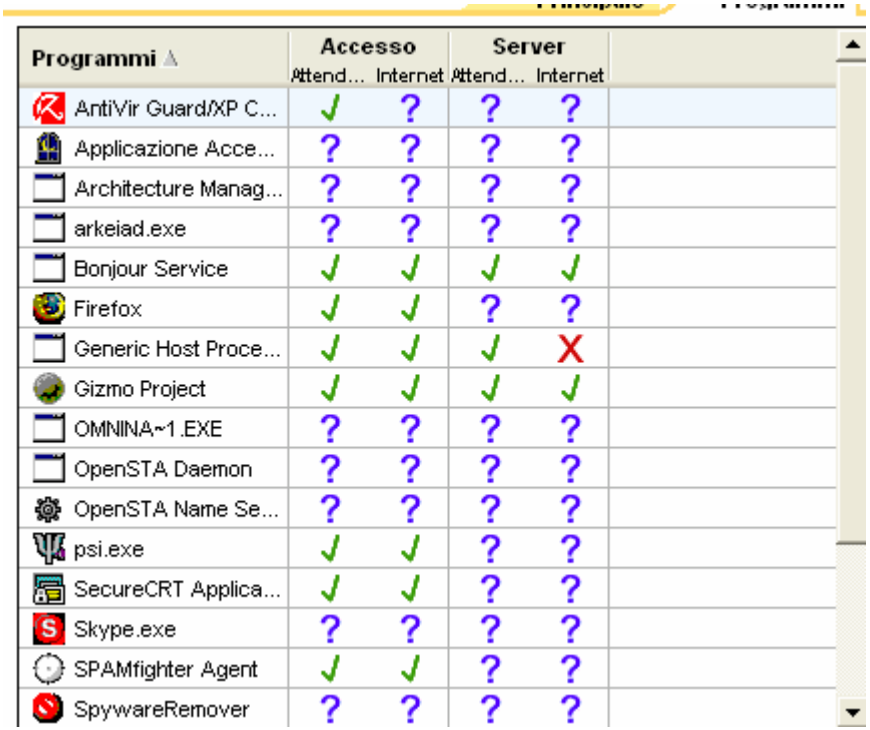


- Le zone attendibili permettono al condivisione dei dati a sistemi certi, ma permette comunque la connessione ad Internet protetta dal Firewall

- Il firewall è in grado di mappare i programmi leciti e permettere il loro accesso ad internet, confrontandoli con un database contenente i programmi considerati accettabili (Smart Defense)



Il controllo dei programmi

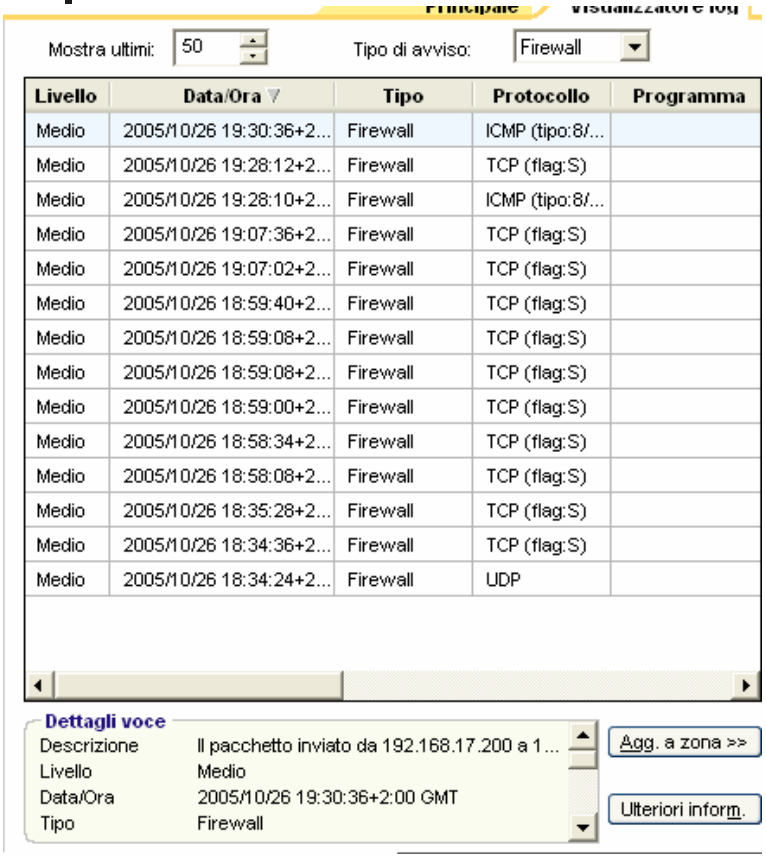


- Il controllo dei programmi permette a ZoneAlarm di imparare a proteggere i programmi
- La protezione media obbligai programmi che dal nostro computer vogliono accedere ad internet a richiedere l'accesso, che deve essere esplicitamente fornito dall'utente

Gli Avvisi del Firewall

- Avvisi di controllo dei programmi
  - Occorre abilitare il loro accesso ad Internet, basta un click su Ok
- Avvisi di tentativi di accesso al firewall
  - Avvisano e vengono loggati i tentativi di apertura di connessioni non autorizzate dall'esterno verso il nostro sistema

Log del Firewall



- Il Firewall registra tutti i tentativi di connessione non autorizzati in un file di testo
- Ogni entry del file di log può essere analizzata per ottenere informazioni circa l'IP del sistema che ha cercato di accedere oppure il tipo di servizio che è stato contattato

Configuriamo gli strumenti Internet Explorer

- Sotto il menu strumenti abbiamo le voci:
  - **Generale**: per rendere la nostra navigazione invisibile eliminare i cookies ed i file temporanei e cancellare la cronologia. Impostare la cache a pochi Mega e la cronologia a pochi giorni.
  - **Protezione**: permette di definire delle impostazioni per l'accesso ad internet, inibendo per gruppi di siti determinate funzionalità come i controlli ActiveX, i download, la visualizzazione di immagini ecc ecc
  - **Privacy:** permette di bloccare parzialmente o del tutto i cookies
  - **Contenuto**:
    - Per attivare il controllo sui siti visitati (Contenuto Verificato)
    - per rimuovere le password e la cache dei moduli (Completamento automatico)

Configuriamo gli strumenti Outlook Express

- Disabilitare il formato HTML potenzialmente pericoloso, piccoli programmi (java o javascript) si possono auto eseguire ed usare al suo posto il formato TESTO.
- Richiedere mail in formato Testo, senza allegati o con allegati pdf eventualmente compressi (file zip)
- Non inviare o ricevere mail di grosse dimensioni, 1 MB è già molto
- Seguire la Netiquette
- Non inviare spam, richiedere il consenso all'invio di mail pubblicitarie (secondo quanto prescrive la legge sulla privacy)
- In pratica eseguire queste operazioni:
  - Menu Strumenti-Opzioni-Formato Invio Posta- Testo Normale
  - Menu Strumenti – Protezione- Non consentire salvataggio allegati con virus
  - Menu Visualizza – Layout – Disattivare Visualizza riquadro anteprima
  - Attenzione agli allegati dei programmi MS (doc) e a file con estensione .bat o .pif. Usare se possibile i pdf (Portable Document Format).

Outlook Express: Come Difendersi dai Virus

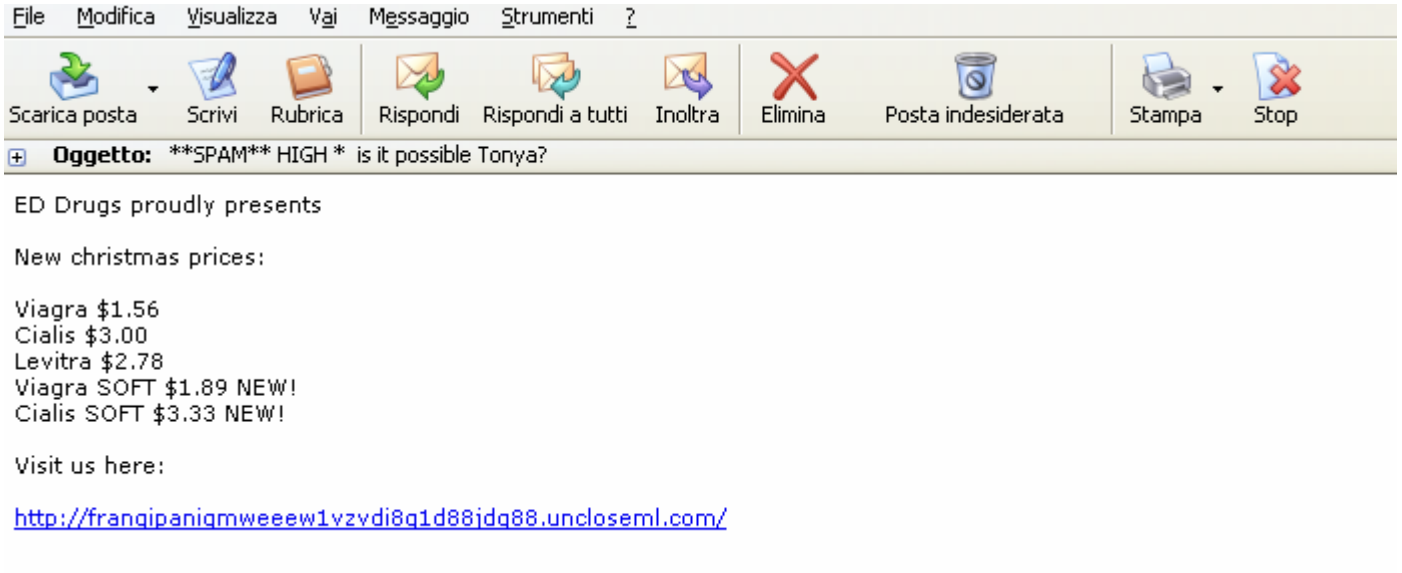
- Esistono una serie di contromisure da mettere in atto.
  - La prima consiste nell'installazione di un antivirus possibilmente licenziato, in modo da avere gli aggiornamenti in tempo reale
  - La seconda prevede la configurazione dei propri strumenti di accesso ad internet in modo da ridurre i rischi
    - Il browser: Internet Explorer
    - Il client di posta: Outlook
  - La terza prevede una politica di comportamento:
    - Non aprire gli allegati di mail il cui mittente ci è sconosciuto, per questo eliminarle del tutto in modo definitivo
    - Impostare un filtro antispam
  - Ulteriore protezione può venire data dall'installazione di ulteriori strumenti di protezione:
    - Firewall: permette di proteggere il sistema da attacchi esterni filtrando le connessioni in ingresso ed in uscita
    - Worm Searcher: ricerca spyware, bot e worm installati sul nostro sistema, com Adware o SpySearch

Spam come difendersi

- Richiedere un filtraggio al livello server
- Impostare un filtro a livello client (Spamhilator o SpamPal)
- Dirottare le email in ricezione verso cartelle preimpostate
- Due ottimi programmi gratuiti e facili da utilizzare sono Spampal e Spamhilator
  - Recensione software antispam gratuiti
  - http://sicurezza.html.it/articoli.asp?IdCatArticoli=9&idarticoli=41

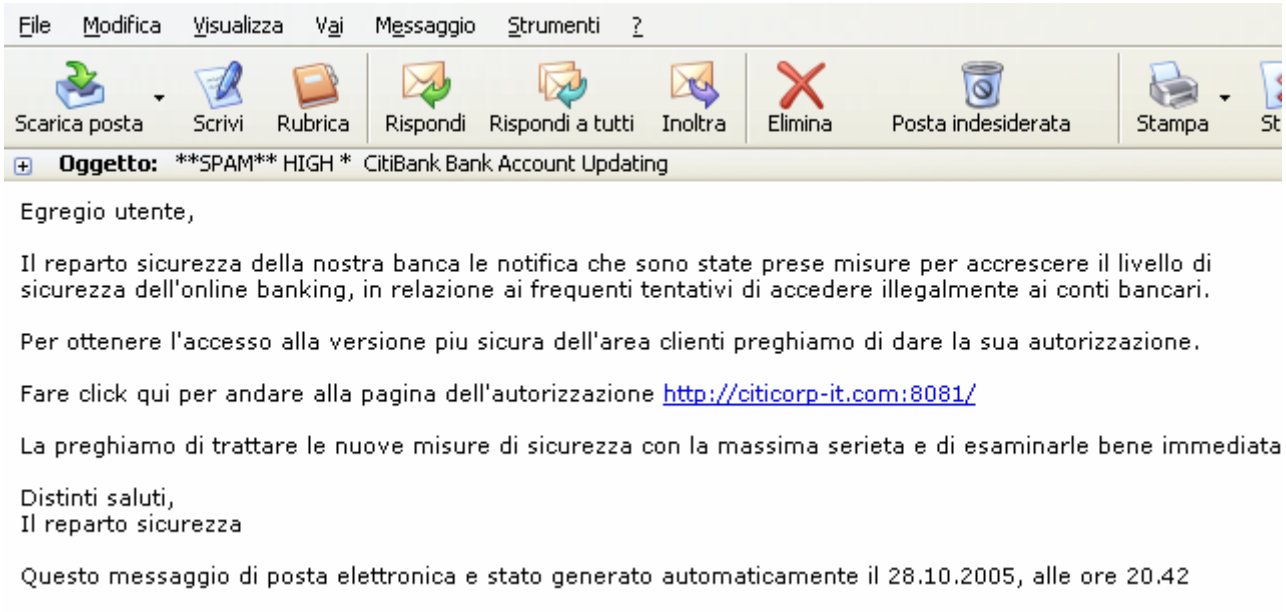
Esempi di Spam

Pharmacy Spam



Esempi di Spam

Banking Phisyng



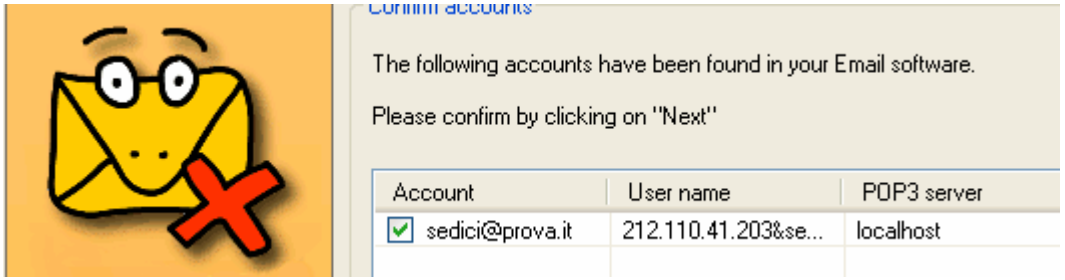
Decalogo Antispam

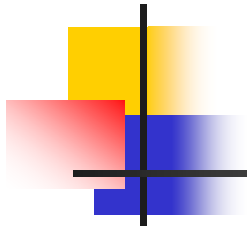
- Non diffondere il proprio indirizzo con leggerezza.
- Utilizzare il CCN. Quando si invia una mail a molti destinatari è bene mascherare gli altri indirizzi alla vista di ogni singolo ricevente.
- Non diffondere i cosiddetti "virus alerts" o messaggi riguardanti presenti pericoli o virus
- Mascherare sempre il proprio indirizzo quando si partecipa a un gruppo di discussione (Newsgroup).
- Non rispondere mai a un messaggio di spam con toni offensivi, il rischio sono le flame war o i mailbombing

Installare Spamhilator

- Si installa facilmente occorre solo selezionare:
  - Il client di posta (Outlook, Thunderbird, ecc)
  - L'account o gli account identificati da proteggere
    - Modifica automaticamente i parametri dell'account per cui la posta passa prima dal suo servizio (localhost) e poi viene inoltrata al client

Installare Spamhilator

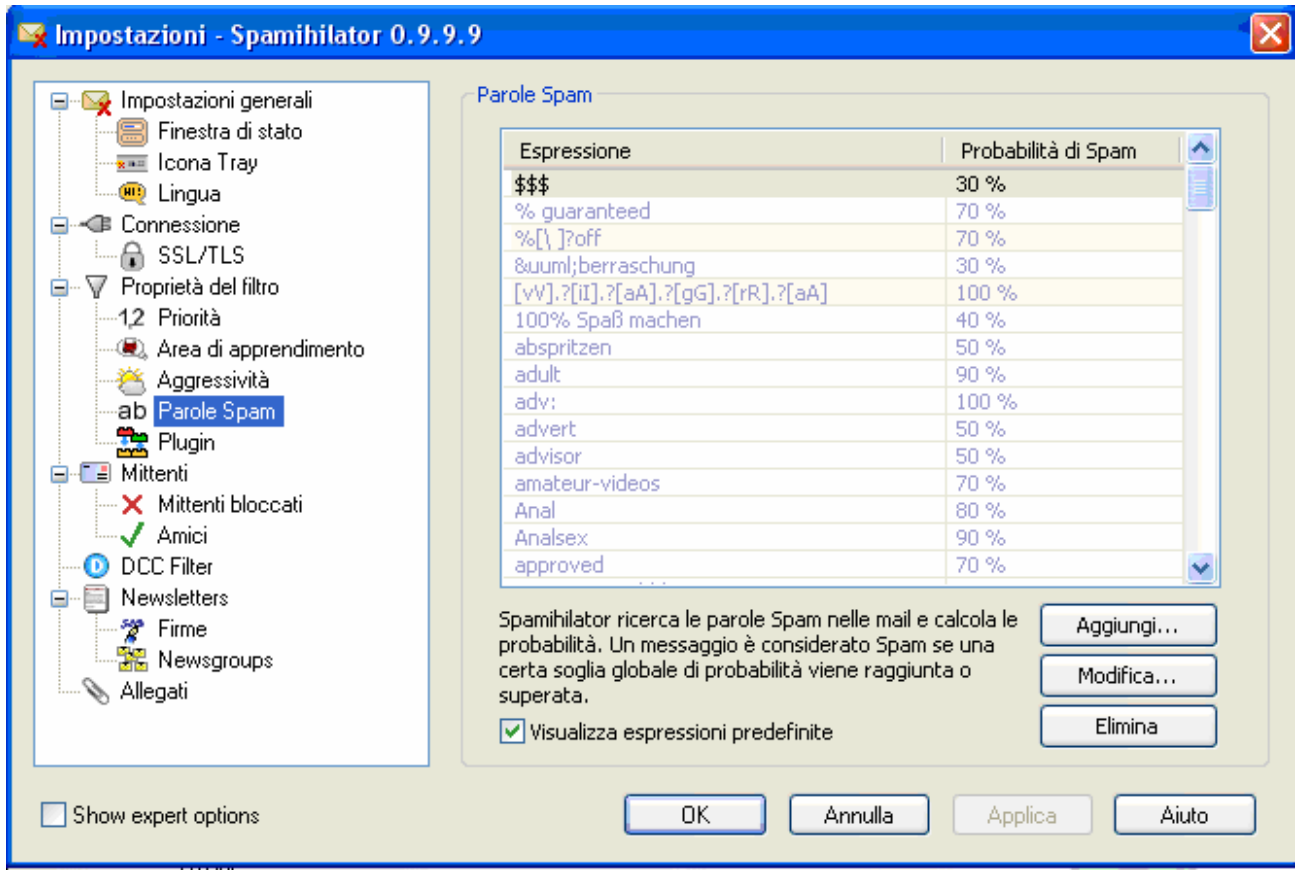




Proprietà di Spamhilator

- Funzioni base
  - Recycle Bin
  - Training Area
  - Funziona anche con i protocolli criptati
- Problemi comuni
  - Uso del DCC filter
  - I falsi positivi
  - Rallenta lo scarico di email

Configurare Spamhilator

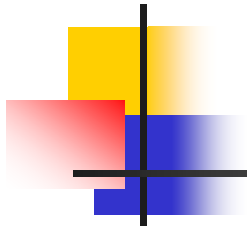


Configurare le **Proprietà del Filtro:**

- **Priorità**
- **Apprendimento**
- **Aggressività**
- **Parole Spam**
- **Plugin**

Allegati da rifiutare: almeno

cmd,com,cpt,exe,lnk,pif,reg,scr,vb*,wsh



Un esempio pratico

This is the GTUBE, the
Generic
Test for
Unsolicited
Bulk
Email

If your spam filter supports it, the GTUBE provides a test by which you can verify that the filter is installed correctly and is detecting incoming spam. You can send yourself a test mail containing the following string of characters (in upper case and with no white spaces and line breaks):

XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL*C.34X

You should send this test mail from an account outside of your network.

Un esempio pratico