I pericoli della rete

Corso di formazione per incaricati del trattamento dei dati personali

Parte III

- Analisi dei criteri logici, fisici e organizzativi per la protezione dei sistemi informativi
  - I pericoli della rete
  - Misure elementari di sicurezza
  - Organizzazione dei dati

Introduzione

- Cosa si intende per **sicurezza**?
  - Riservatezza
  - Integrità
  - Disponibilità
- Quali scenari?
  - normale gestione
  - intrusioni
  - eventi calamitosi

Pericoli informatici

A chi fa gola il vostro computer?

- *hacker*
- *cracker*
- *spammer*
- virus / worm

… e a cosa può servire?

- untore
- spam
- attacchi DoS (denial of Service)
- testa di ponte per altri attacchi
- deposito di materiale illegale
- cava di password

Hacker & Cracker

- Un estraneo può facilmente impadronirsi dall'esterno del vostro PC, se non è opportunamente protetto e senza le ultime versioni del software installato.

Virus

- Un **virus** è un codice in grado di riprodursi attaccandosi ad un altro programma (o documento), in modo che venga eseguito ogni volta che lo sia il programma infettato.
  - Si propaga trasportato dal programma infetto
    - internet, cd rom, floppy…
  - Di solito, ha bisogno di una qualche azione da parte dell'utente.

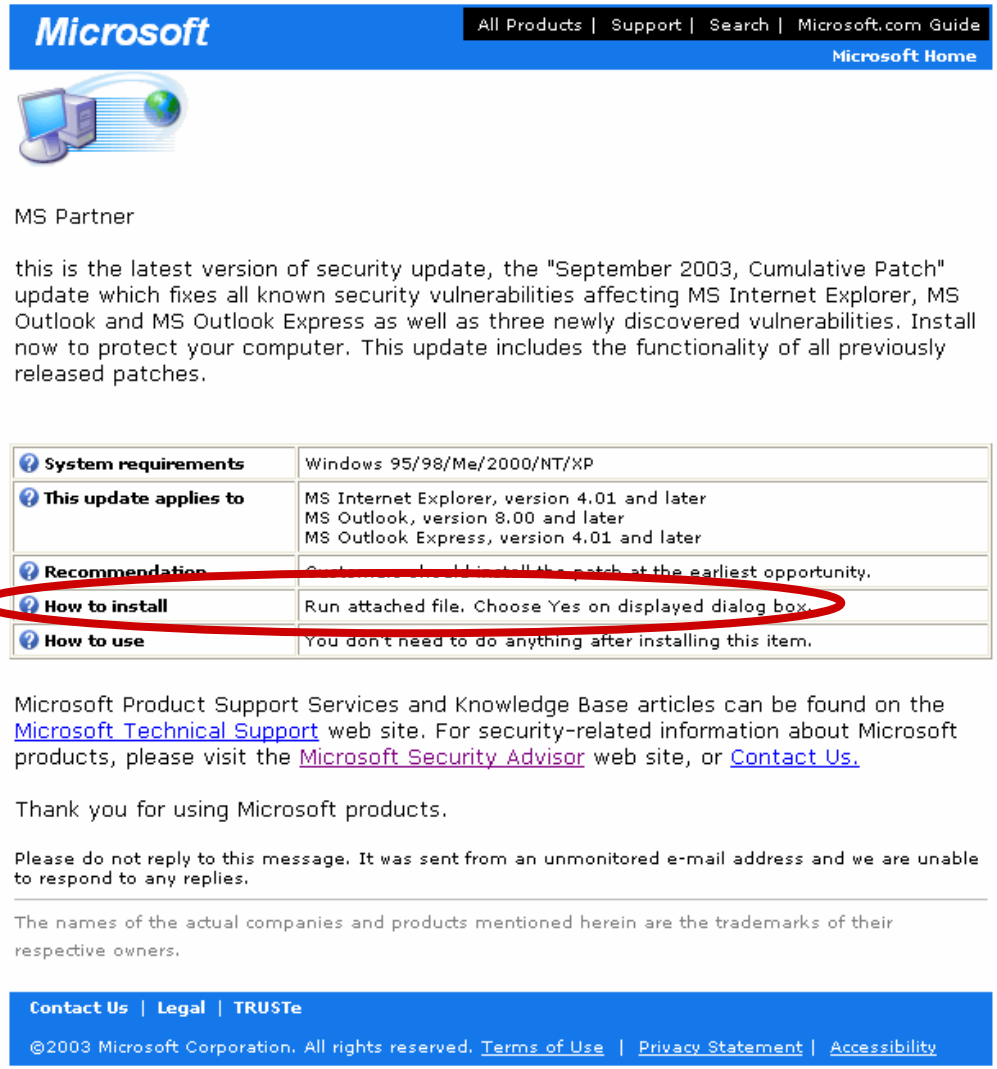
Worm

- Un **worm** è un eseguibile in grado di creare copie di sé stesso, senza infettare altri programmi (come fanno i virus).
  - Si propaga via posta elettronica o sfruttando difetti dei programmi installati.
  - Non necessita di azioni da parte dell'utente (a parte la trascuratezza …).

Virus & worm

- Virus e worm, oltre a propagarsi, possono compiere un'infinità di altre azioni nocive:
  - cancellare file;
  - diffondere informazioni riservate (compresi i vostri mail privati …);
  - permettere ad intrusi di accedere alla vostra macchina;
  - spedire mail di spam
  - …

Virus via e-mail: un esempio



Microsoft

All Products | Support | Search | Microsoft.com Guide

Microsoft Home

MS Partner

this is the latest version of security update, the "September 2003, Cumulative Patch" update which fixes all known security vulnerabilities affecting MS Internet Explorer, MS Outlook and MS Outlook Express as well as three newly discovered vulnerabilities. Install now to protect your computer. This update includes the functionality of all previously released patches.

System requirements	Windows 95/98/Me/2000/NT/XP
This update applies to	MS Internet Explorer, version 4.01 and later MS Outlook, version 8.00 and later MS Outlook Express, version 4.01 and later
Recommendation	[illegible] patch at the earliest opportunity.
How to install	Run attached file. Choose Yes on displayed dialog box.
How to use	You don't need to do anything after installing this item.

Microsoft Product Support Services and Knowledge Base articles can be found on the Microsoft Technical Support web site. For security-related information about Microsoft products, please visit the Microsoft Security Advisor web site, or Contact Us.

Thank you for using Microsoft products.

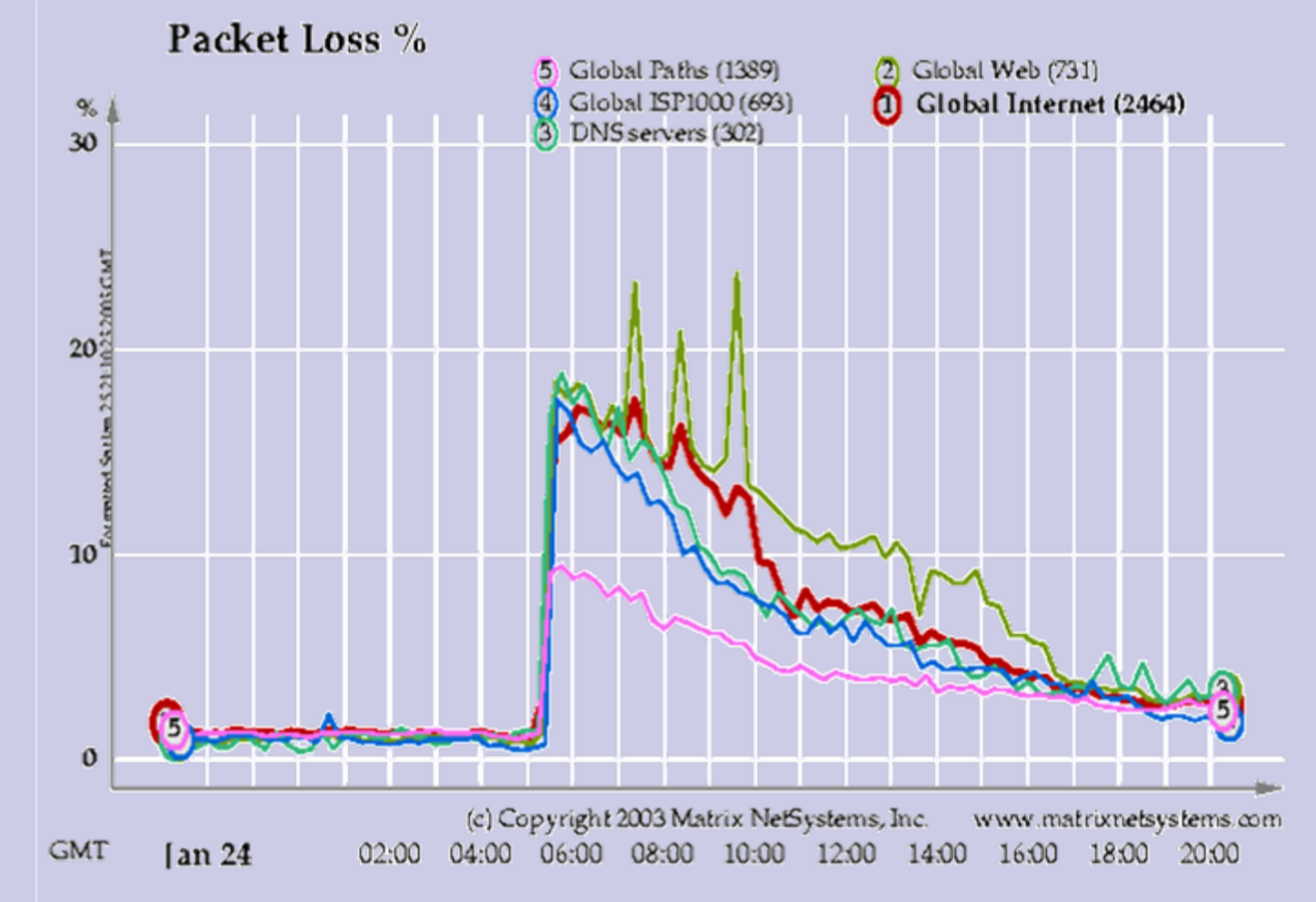
Please do not reply to this message. It was sent from an unmonitored e-mail address and we are unable to respond to any replies.

The names of the actual companies and products mentioned herein are the trademarks of their respective owners.

Contact Us | Legal | TRUSTe

©2003 Microsoft Corporation. All rights reserved. Terms of Use | Privacy Statement | Accessibility

Worm: propagazione



spam

- Un messaggio non richiesto, spesso a carattere pubblicitario:
  - Oltre il 40% degli e-mail inviati!
- Truffe:
  - Cartoline elettroniche con *dialer*;
  - Catene di S. Antonio.
- http://sicurezza.html.it/articoli/articoli.asp?IdCatArticoli=17&idarticoli=31

Adware, spyware & co.

- **Adware**: programmi “gratuiti” con annunci pubblicitari
- **Spyware**: inseriti in altri programmi, inviano informazioni sulle attività dell’utente
  - malware, hijacker, dialer, trojan horse, collectware
- Informazioni e software per la rimozione
  - http://simplythebest.net/info/spyware.html
  - http://www.safer-networking.org/

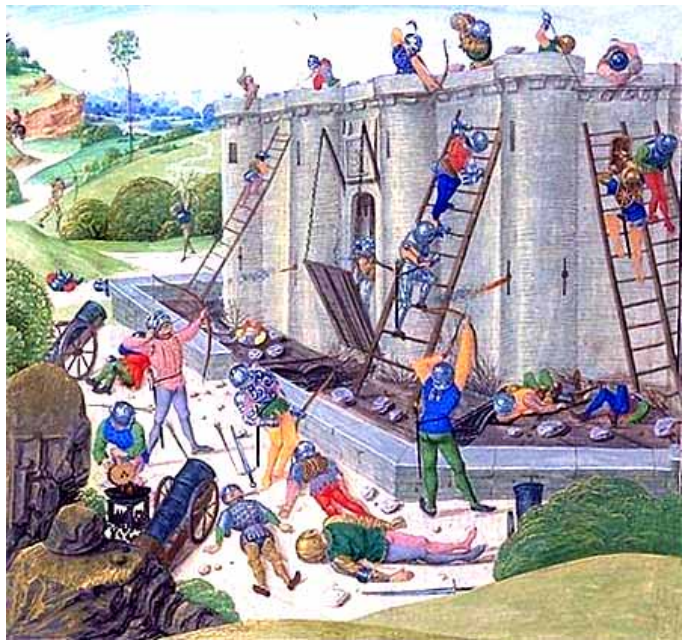
Le “bufale” (Hoax)

- Notizie false:
  - aumentano le e-mail inutili in circolazione;
  - diffondono indirizzi di e-mail;
  - effetti simili a quelli di un virus.
- Frasi tipiche:
  - “Nuovo virus pericolosissimo”;
  - “Notizia proveniente da Microsoft/IBM”;
  - “Bambina/o in fin di vita”;
  - “Diffondete la notizia quanto più possibile”.

Le “bufale” (Hoax) segue

- Prima di ridiffondere la notizia, controllatene l’autenticità:
  - http://dep.eco.uniroma1.it/econometria/hoax1.htm
  - http://www.symantec.com/avcenter/hoax.html
- Anche se la notizia è vera (anche se per una nobile causa) valutate attentamente l’opportunità della sua diffusione via la rete INFN.
- **In ogni caso, mettete i destinatari in BCC:**

Misure elementari di sicurezza

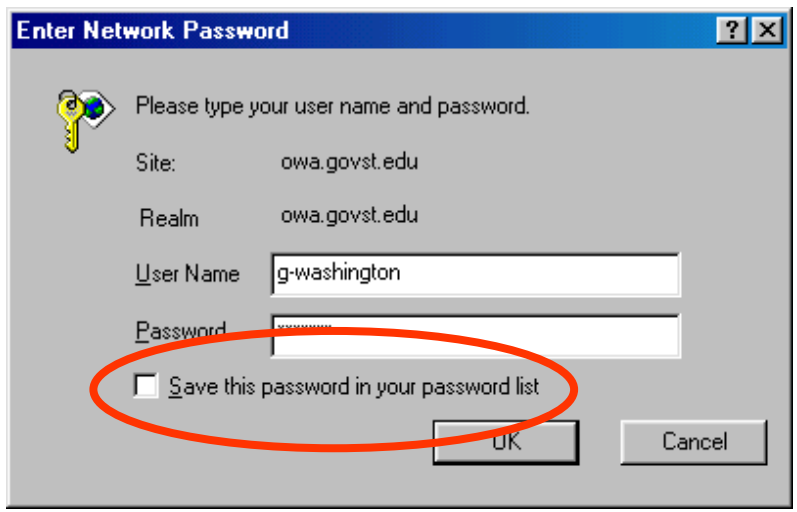


Autenticazione: password

- La madre di tutti i meccanismi di autenticazione.
- Un segreto condiviso tra l'utente e il sistema da proteggere.
- Personale e non cedibile.
- Da proteggere con cura:
  - sniffing, social engineering, forza bruta.

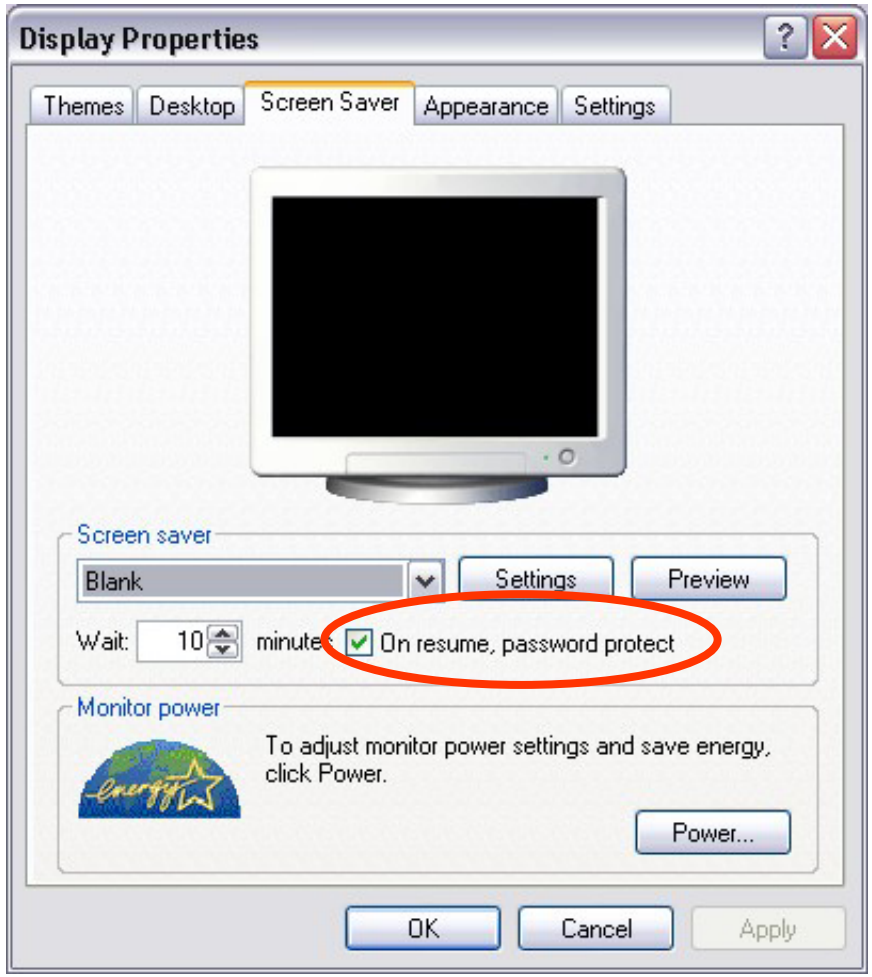
Autenticazione: password segue

- Non memorizzatele sulla vostra macchina.
  - Rendereste la vita troppo facile ad eventuali intrusi (remoti o locali).



Autenticazione: password segue

- Attivate la password del salvaschermo:
  - per evitare che altri possano usare il vostro computer, che avete lasciato incustodito

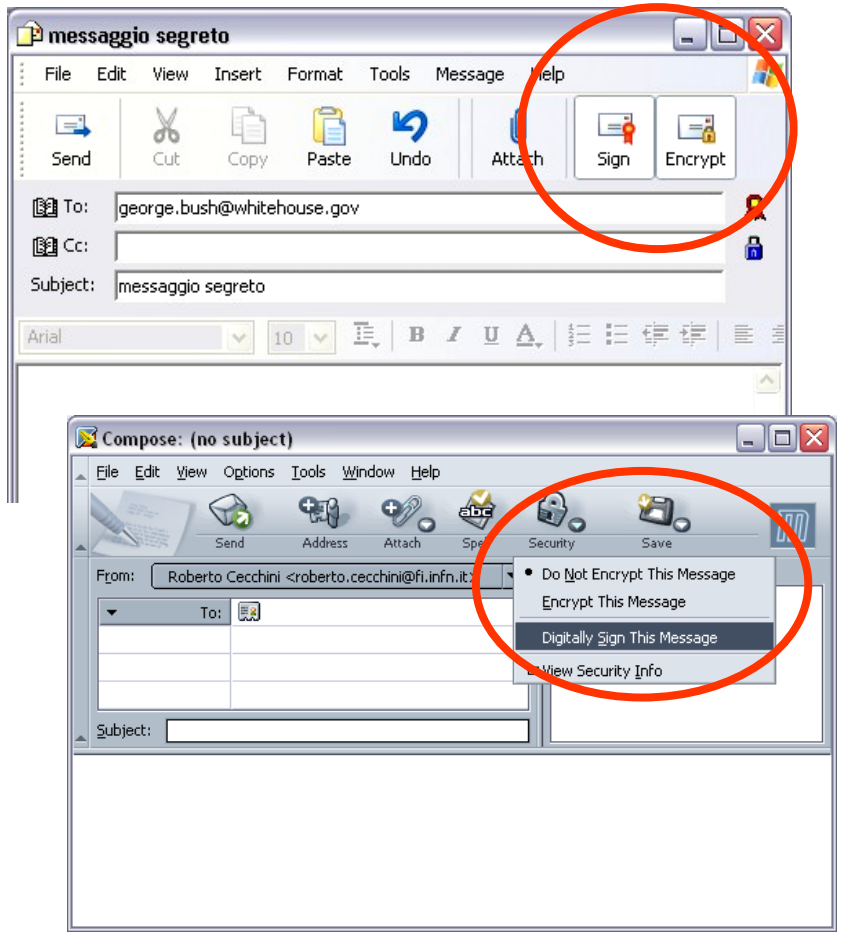


Crittografia

- I dati (mail, file, database, cartelle) possono venire cifrati:
  - “impossibili” da capire tranne che per i possessori della chiave di cifratura;
  - la chiave può essere di tipo hardware (ad es. smart card) o software (password);
  - se la chiave viene persa, i dati sono “irrecuperabili”.

Crittografia segue

- Alcuni programmi di e-mail permettono di spedire mail cifrati e/o “firmati”
  - serve un certificato digitale
    - http://security.fi.infn.it/CA/



Crittografia segue

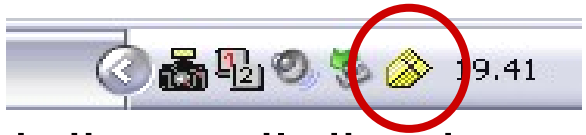
- Può essere usata per proteggere i documenti più sensibili:
  - EFS: Windows2000/XP;
  - Word.
- Ma attenzione: non è facile da configurare!
  - Seguite le indicazioni del Servizio Calcolo.

Condivisione di cartelle

- Se non necessario, evitate di condividere le cartelle del sistema.
- Proteggete con password le cartelle condivise.
  - Se non è possibile, limitate la condivisione all'intervallo di tempo strettamente necessario.

Antivirus

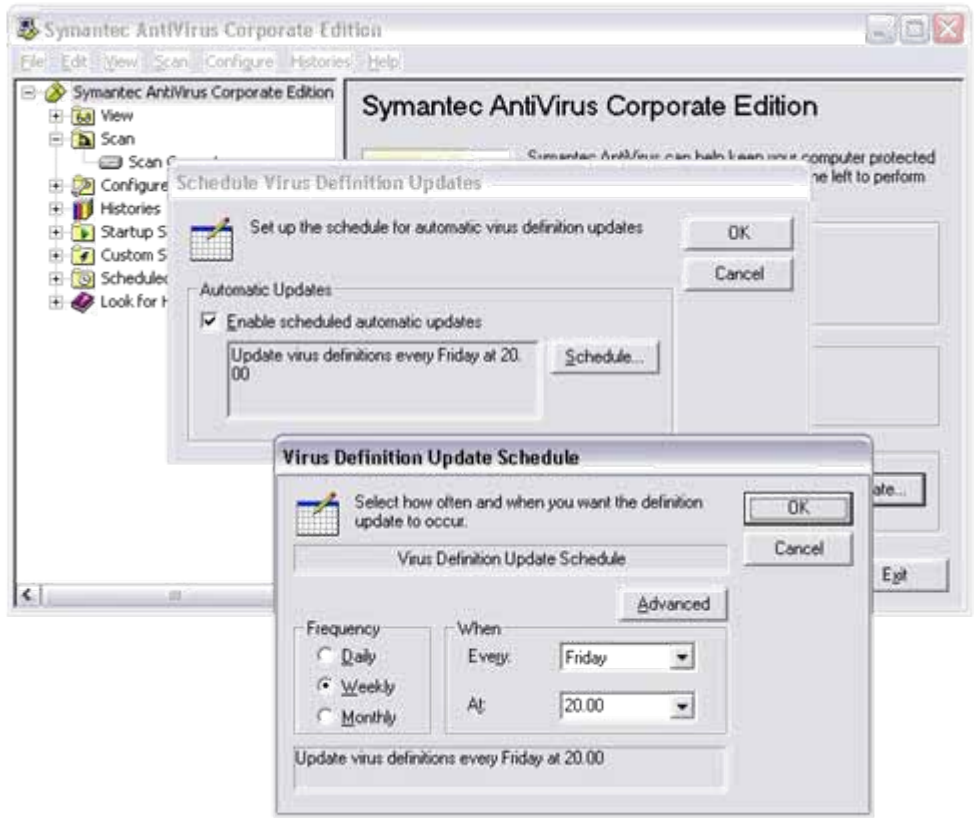
- È **indispensabile** installare un antivirus
  - Il Servizio di Calcolo dispone di software e licenze e può prestare consulenza al riguardo
- In ogni caso:



  - non aprite allegati di e-mail di cui non siete sicuri, **anche se il mittente è una persona di cui vi fidate**;
    - ricordate che il campo **From:** può essere molto facilmente falsificato;
  - usate solo programmi provenienti da fonti fidate

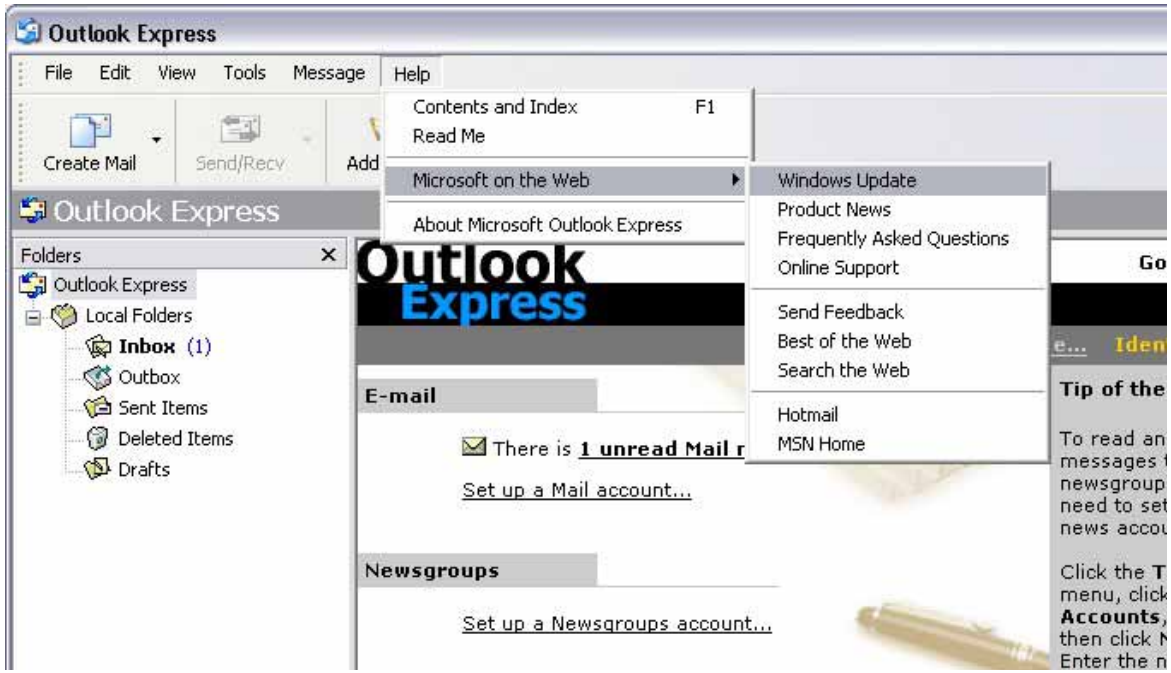
Antivirus segue

- Abilitate l'aggiornamento automatico e la protezione in tempo reale.
  - un antivirus non aggiornato serve solo a dare un falso senso di sicurezza!



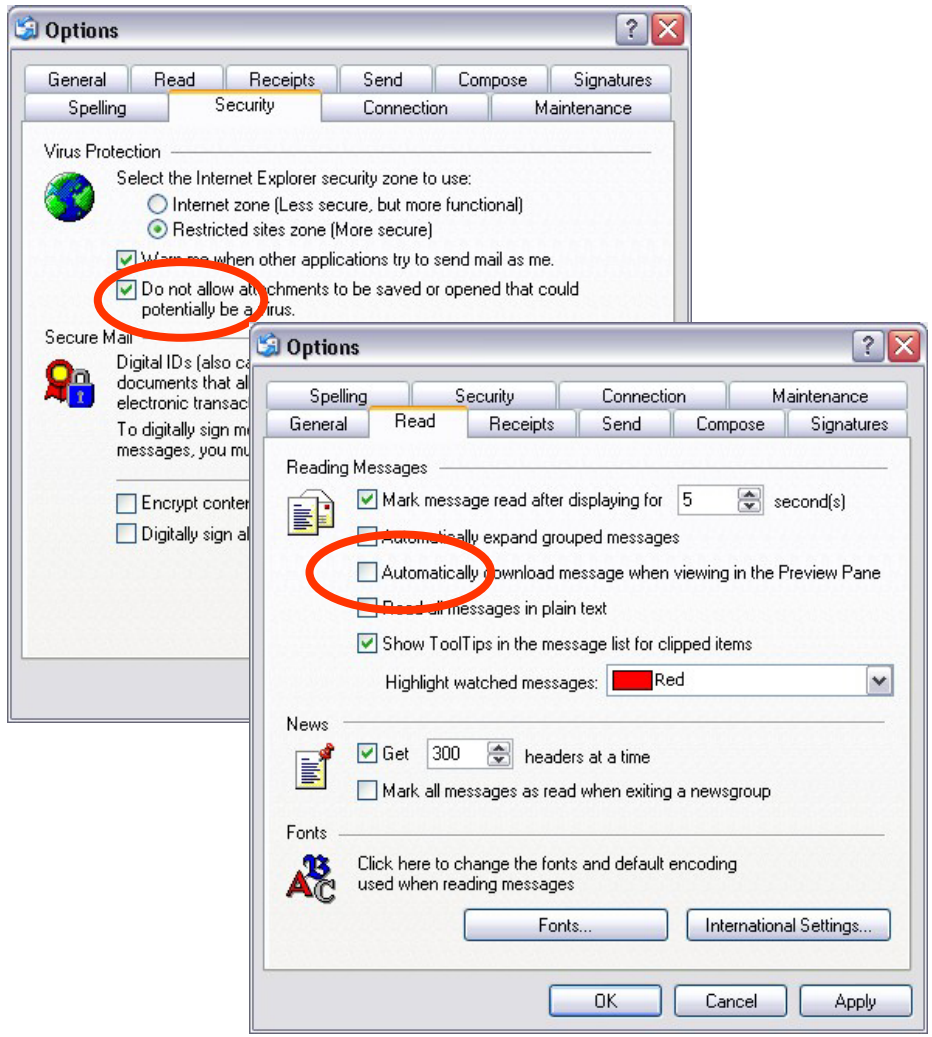
Clienti di e-mail

- Teneteli aggiornati all'ultima versione



Clienti di e-mail segue

- Con alcune vecchie versioni di Outlook è possibile rimanere infettati anche **senza aver aperto l'attachment!**



Le patch di sicurezza

- Mantenete il software del vostro sistema sempre aggiornato (“applicate le patch”)
  - **seguite le indicazioni del Servizio Calcolo sull’attivazione del servizio di Update Atomatico**
- Ricordate che i worm si propagano grazie ai sistemi con software non aggiornato

Personal Firewall

- Attivate (o meno…) un Personal Firewall, **secondo le modalità indicate dal Servizio Calcolo.**
- Ma attenzione:
  - non sono facili da usare;
  - possono rendere impossibile l'uso di programmi o la condivisione di risorse;
  - vanno tenuti aggiornati.

I dati

Protezione

- Analisi dei rischi
- Sicurezza del sistema
  - errori
  - intrusioni
  - eventi eccezionali
- Integrità dei dati
  - copie di salvataggio (*backup*)
    - periodicità, custodia, eliminazione
  - protezione aree e locali

Protezione segue

- Compiti e responsabilità
  - autenticazione e autorizzazione
- Gestione emergenze
  - piano di ripristino
  - verifiche periodiche
  - aggiornamento

Accesso ai dati

- L’autenticazione degli incaricati del trattamento deve avvenire attraverso account (username / password) individuali;
- L’autorizzazione deve essere la minima indispensabile per svolgere il lavoro.
- I dati sensibili devono essere conservati su di un server.

Organizzazione dei dati

- L'organizzazione dei dati **deve** rispecchiare questa necessità di separazione:
  - ogni cartella contiene dati omogenei;
  - la cartella è condivisa tra gli incaricati del trattamento (e solamente tra loro);
  - tutti devono conoscere come i dati sono strutturati.

E comunque, ricordate che…

- Il Servizio Calcolo, anche se spesso non ha risorse sufficienti, va comunque sempre interpellato.
- Il System Manager è il vostro miglior amico!

Domande?