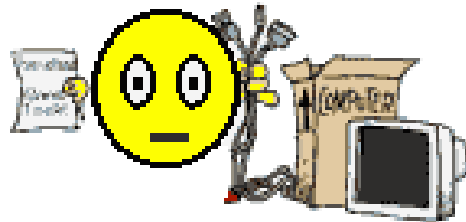




LE MISURE DI SICUREZZA IN PRATICA

RIOLO TERME
25 OTTOBRE 2008
CONVEGNO FIMMG
REGIONE EMILIA-ROMAGNA

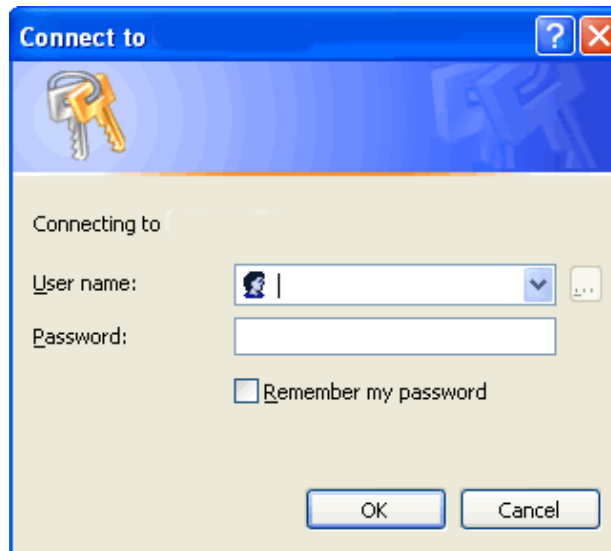
L'USO DEI SISTEMI INFORMATICI



PASSWORD



- ◆ LE CREDENZIALI E LE PASSWORD ASSEGNATE SONO PERSONALI E NON CEDIBILI
- ◆ DEVONO ESSERE CAMBIATE OGNI 3 MESI



Connect to

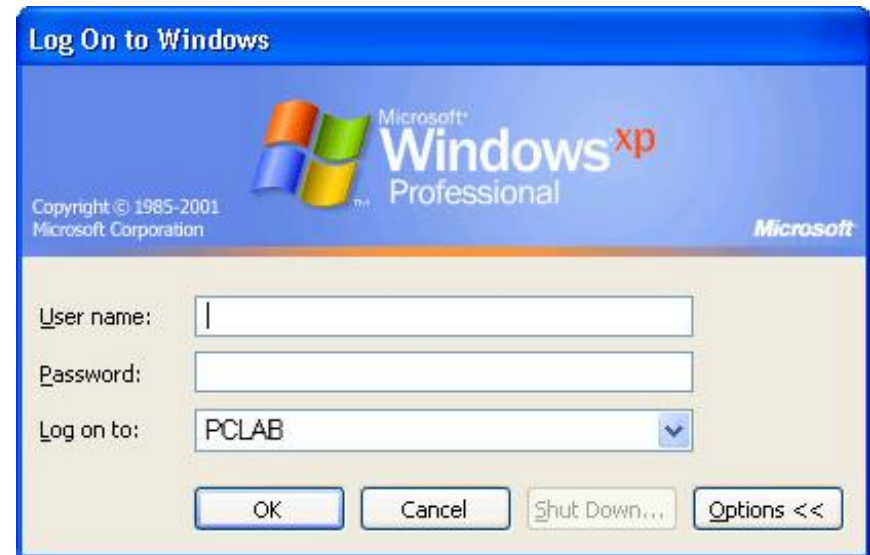
Connecting to

User name: []

Password: []

Remember my password

OK Cancel



Log On to Windows

Microsoft Windows XP Professional

Copyright © 1985-2001 Microsoft Corporation

User name: []

Password: []

Log on to: PCLAB []

OK Cancel Shut Down... Options <<

PASSWORD



COME FACCIAMO A CAMBIARLA?



PASSWORDS



LE PASSWORDS NON DEVONO MAI ESSERE TRASCRITE PER EVITARE CHE TERZI NON AUTORIZZATI VI POSSANO ACCEDERE



RISERVATEZZA



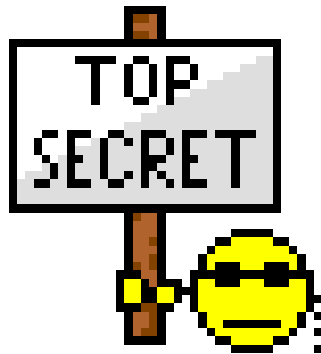
NON ATTACCARE BIGLIETTI CON LA
PASSWORD SUI MONITOR O IN
LUOGHI ACCESSIBILI A TERZI



RISERVATEZZA



NON RIVELARE AD ALCUNO LE
PROPRIE CREDENZIALI D'ACCESSO



RISERVATEZZA



NON UTILIZZARE LA POSTA
ELETTRONICA PER FINALITA'
PERSONALI O PER DIVULGARE
INFORMAZIONI D'UFFICIO



RISERVATEZZA



NON UTILIZZARE VIDEOFONINI E/O
SCATTARE FOTOGRAFIE ALL'INTERNO
DELLA STRUTTURA, SENZA
AUTORIZZAZIONE DEL RESPONSABILE



RISERVATEZZA



NON LASCIARE DOCUMENTAZIONE
SULLE SCRIVANIE ACCESSIBILI AL
PERSONALE DELLE PULIZIE





RISERVATEZZA



NON LASCIARE I COMPUTER ACCESI
DURANTE I SERVIZI DI PULIZIA

RISERVATEZZA



DISTRUGGERE EVENTUALI BRUTTE
COPIE E/O APPUNTI PER EVITARE CHE
TERZI POSSANO ENTRARE IN
POSSESSO DI DATI SENSIBILI

USO DI INTERNET



NON UTILIZZARE INTERNET PER:

- CONSULTARE SITI NON AUTORIZZATI O IMMORALI
- EFFETTUARE ACQUISTI PERSONALI
- CHAT O BLOG NON ATTINENTI ALLA PROPRIA MANSIONE
- SPEDIRE/RICEVERE MAIL PERSONALI



- FARE IL BACK-UP DEI DATI ALMENO UNA VOLTA ALLA SETTIMANA
- VERIFICARE SPESSO DI ESSERE IN GRADO DI RIPRISTINARE I DATI SALVATI

COME FARE IL BACKUP



- ◆ SU DISPOSITIVI ESTERNI:
 - HARD-DISK
 - CHIAVETTE USB
 - CD/DVD
 - SUPPORTI MAGNETICI
- ◆ TRAMITE SERVIZI DI RETE
 - SULLA RETE AZIENDALE
 - SERVIZI SU INTERNET



◆ MINACCE ESTERNE VOLTE A:

- COMPROMETTERE IL FUNZIONAMENTO DEL PC
- PERMETTERE L'ACCESSO A TERZI
- ENTRARE IN POSSESSO DI DATI
- ANALIZZARE (SPIARE) IL COMPORTAMENTO DELL'UTENTE

COME PROTEGGERSI



- ◆ UTILIZZARE UN ANTIVIRUS:
 - AGGIORNAMENTI AUTOMATICI
 - SCANSIONI PROGRAMMATE
 - PROTEZIONE FILE SYSTEM & E-MAIL

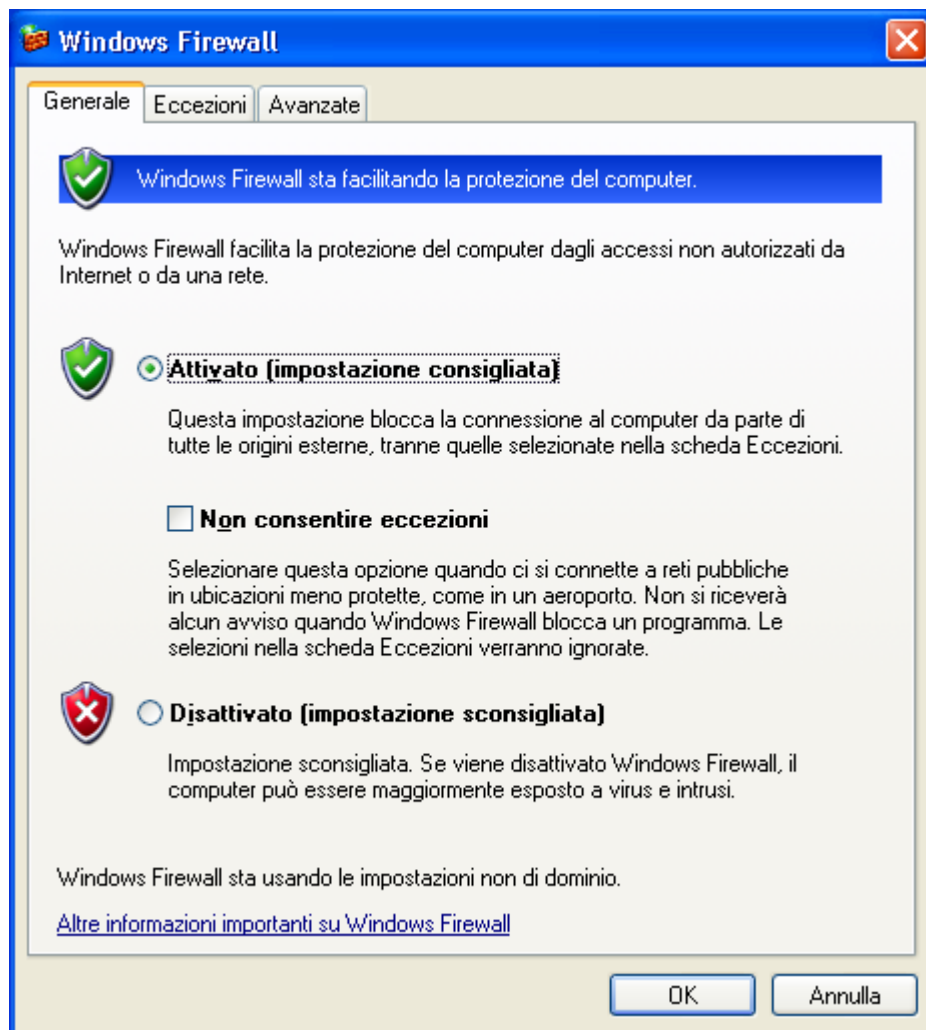
- ◆ UTILIZZARE UN ANTI-SPYWARE
 - AGGIORNAMENTI AUTOMATICI
 - SCANSIONI PROGRAMMATE



◆ UTILIZZARE UN FIREWALL:


- AZIENDALE (hw o sw)
- PERSONALE:
 - ◆ LIMITARE AL MASSIMO LE ECCEZIONI
 - ◆ CONTROLLARE PERIODICAMENTE LE IMPOSTAZIONI DEL FIREWALL
 - ◆ IN CASO DI DUBBIO CONSULTARE L'AMMINISTRATORE DI RETE

IMPOSTAZIONI FIREWALL




Windows Firewall

Generale | Eccezioni | Avanzate

 Windows Firewall sta facilitando la protezione del computer.


Windows Firewall facilita la protezione del computer dagli accessi non autorizzati da Internet o da una rete.

 **Attivato (impostazione consigliata)**

Questa impostazione blocca la connessione al computer da parte di tutte le origini esterne, tranne quelle selezionate nella scheda Eccezioni.

Non consentire eccezioni

Selezionare questa opzione quando ci si connette a reti pubbliche in ubicazioni meno protette, come in un aeroporto. Non si riceverà alcun avviso quando Windows Firewall blocca un programma. Le selezioni nella scheda Eccezioni verranno ignorate.

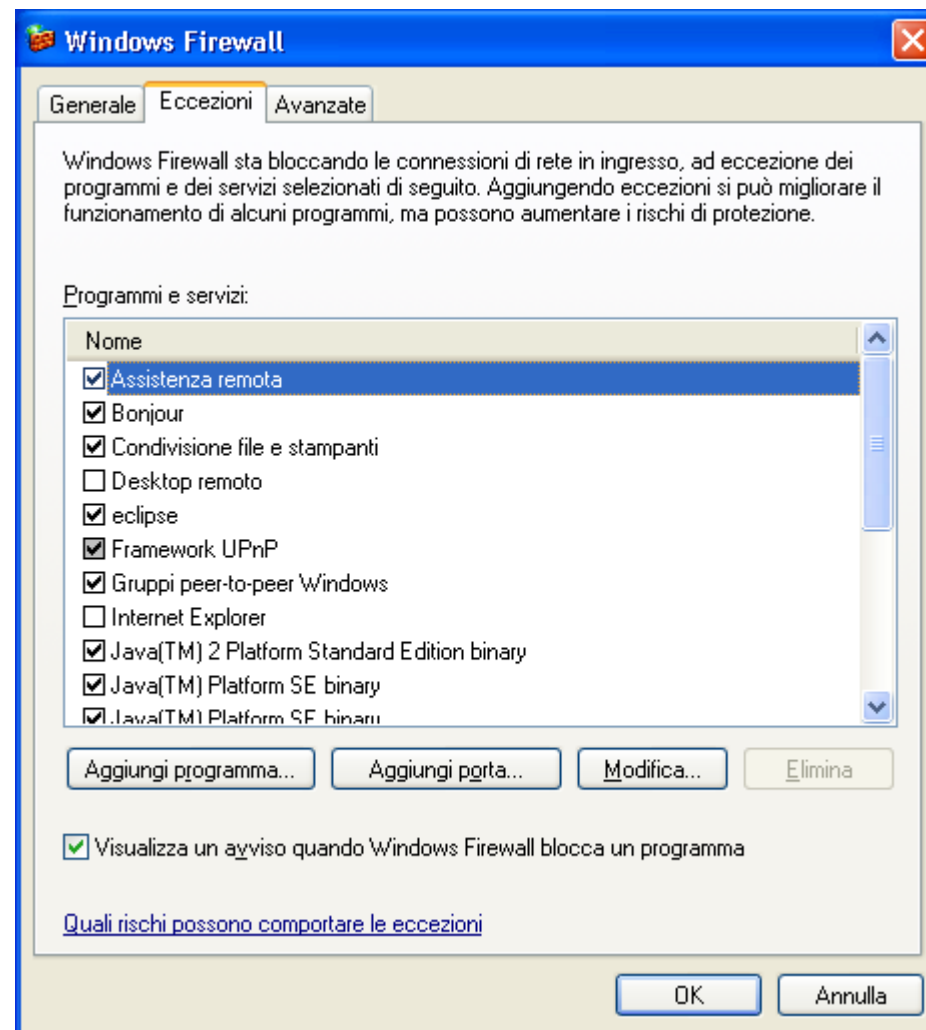
 **Disattivato (impostazione sconsigliata)**

Impostazione sconsigliata. Se viene disattivato Windows Firewall, il computer può essere maggiormente esposto a virus e intrusi.

Windows Firewall sta usando le impostazioni non di dominio.

[Altre informazioni importanti su Windows Firewall](#)

OK Annulla



Windows Firewall

Generale | **Eccezioni** | Avanzate

Windows Firewall sta bloccando le connessioni di rete in ingresso, ad eccezione dei programmi e dei servizi selezionati di seguito. Aggiungendo eccezioni si può migliorare il funzionamento di alcuni programmi, ma possono aumentare i rischi di protezione.

Programmi e servizi:

Nome
<input checked="" type="checkbox"/> Assistenza remota
<input checked="" type="checkbox"/> Bonjour
<input checked="" type="checkbox"/> Condivisione file e stampanti
<input type="checkbox"/> Desktop remoto
<input checked="" type="checkbox"/> eclipse
<input checked="" type="checkbox"/> Framework UPnP
<input checked="" type="checkbox"/> Gruppi peer-to-peer Windows
<input type="checkbox"/> Internet Explorer
<input checked="" type="checkbox"/> Java(TM) 2 Platform Standard Edition binary
<input checked="" type="checkbox"/> Java(TM) Platform SE binary
<input checked="" type="checkbox"/> Java(TM) Platform SE binary

Aggiungi programma... | Aggiungi pgrta... | Modifica... | Elimina

Visualizza un avviso quando Windows Firewall blocca un programma

[Quali rischi possono comportare le eccezioni](#)

OK Annulla

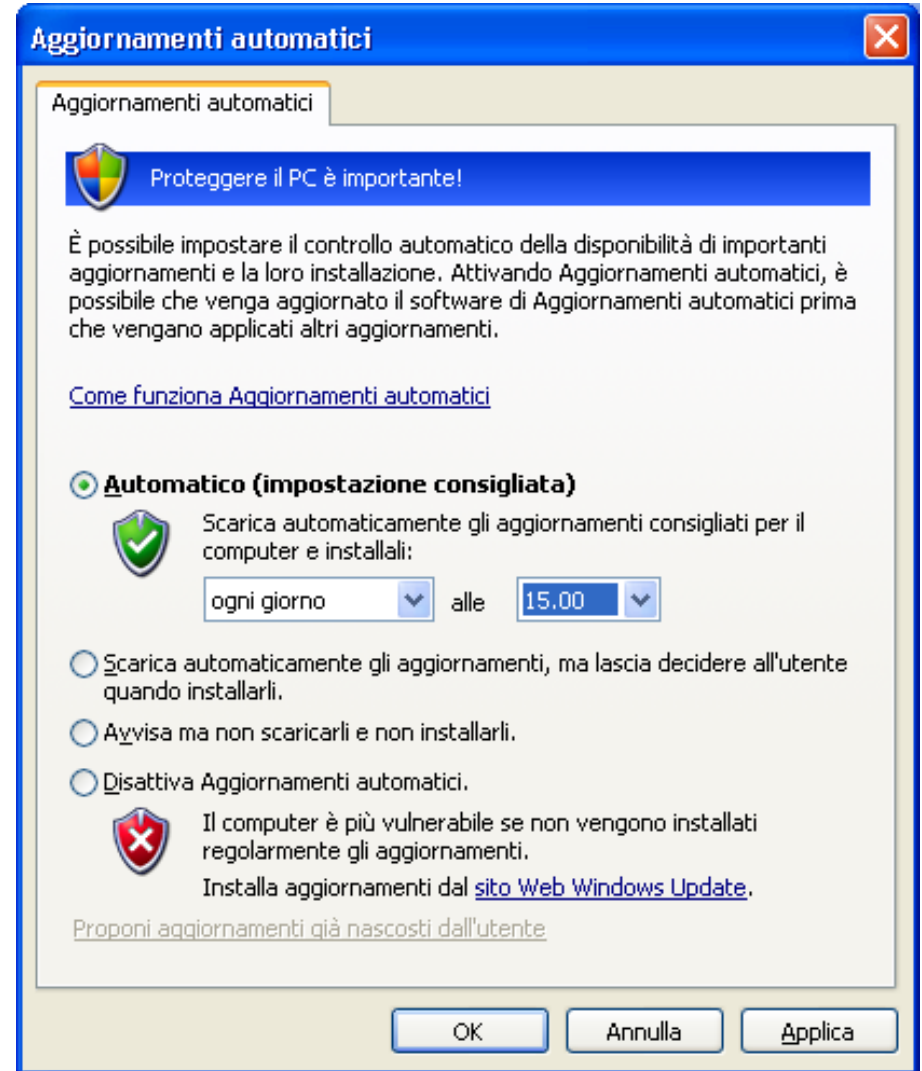
USO DEI PC PORTATILI



E' NECESSARIO PROTEGGERE LE
INFORMAZIONI AZIENDALI CON UN
PROGRAMMA O CON UNA CHIAVE USB
CHE PERMETTA LA CRITTOGRAFIA DEI
DATI



ABILITARE GLI AGGIORNAMENTI AUTOMATICI DEL SISTEMA OPERATIVO





ANTIVIRUS ATTENZIONE !



UTILIZZA UN ANTI-VIRUS E ANTI-
SPYWARE CON ATTIVAZIONE
AUTOMATICA



USO DEI PC PORTATILI



E' IMPORTANTE CONSERVARE I PC PORTATILI IN MODO CHE TERZI NON VI POSSANO ACCEDERE

USO DEI PC PORTATILI



CAMBIARE LA PASSWORD MOLTO SPESSO E COMUNQUE ALMENO OGNI 3 MESI ED UTILIZZARE UNA FORMULA COMPLESSA



USO DEI PC PORTATILI



NON LASCIARLO INCUSTODITO E NON DIMENTICARLO

