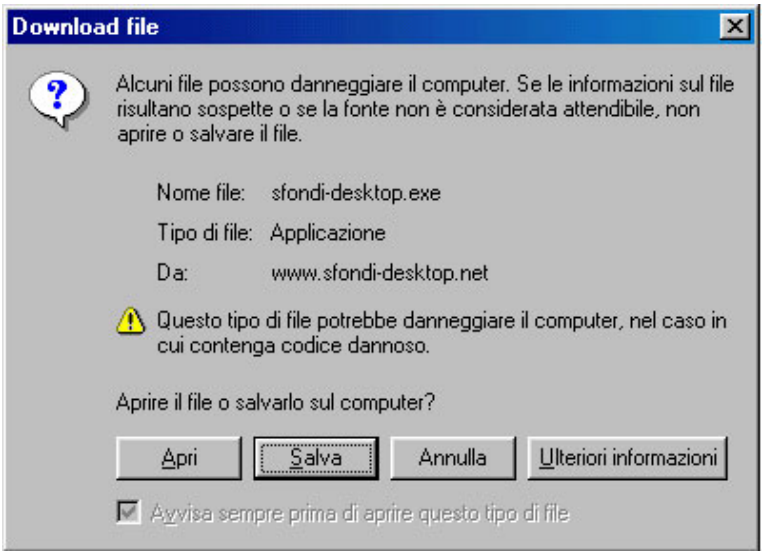
PER PROTEGGERSI DAI DIALER

Dialer, che cosa sono. Su alcuni siti internet, sopratutto quelli che offrono gratis, loghi e suonerie, tesi di laurea, musica MP3 e filmati, o materiale pornografico, per effettuare il download del materiale desiderato, viene richiesto di scaricare un file eseguibile (.exe), camuffato da innocuo programma. In realtà questo programmino è un Dialer e una volta scaricato sul PC provvede a interrompere a insaputa dell'utente la connessione con il proprio provider, dirottando il collegamento su un numero telefonico a pagamento (709, 899, 166, 144, 002, 0088,…). Chi utilizza la banda larga (ADSL) non rischia di incappare nei dialer, dal momento che esiste una connessione diretta continua tra il proprio PC e il provider e quindi, non viene eseguito alcun numero telefonico.

Tipi di Dialer. I Dialer vengono classificati in base alla tipologia d'installazione eseguita. La prima generazione di Dialer sono dei **file eseguibili (.exe)** che vengono proposti per il download. Ecco la proposta fatta da un sito di sfondi per desktop gratis dello scarico di uno di questi file.

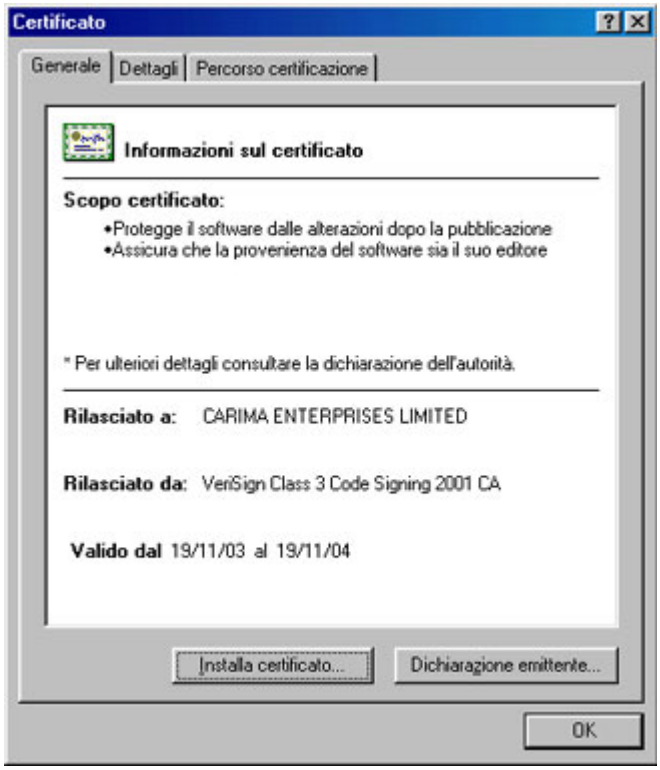


Quelli più avanzati vengono incorporati nelle pagine Web come se fossero un applet o un controllo **ActiveX (.ocx)**, cioè come una sorta di componente interno alla pagina. Quando Internet Explorer visita una pagina con ActiveX incorporato, propone l'installazione del file mostrando una finestra di "**Avviso di protezione**" che invita a installare un certificato di protezione, come mostra la figura seguente.

Basta un clic che si viene automaticamente collegati ai numeri a pagamento. Pertanto, **All'apertura di questa finestra scegliere sempre l'opzione Annulla o No!**
I Dialer più avanzati si installano automaticamente (**Silent-Install**) perché sfruttano particolari bug o exploid (buchi di sicurezza) del browser Internet Explorer per autoeseguire o copiare nel PC determinati file eseguibili. E' pertanto fondamentale tener sempre aggiornato il sistema operativo.

Come difendersi. Purtroppo contro i Dialer non esiste un prodotto valido in grado di riconoscerli ed eliminarli dal sistema. pertanto è necessario ricorrere ad espedienti per riconoscerli ed eliminarli dal sistema.

Eliminarli alla fonte. Quando si incontra un controllo ActiveX su un sito, se il controllo ha una firma elettronica la configurazione di sicurezza di Internet Explorer ne permette l'installazione dopo il nostro consenso. I Dialer, pur non essendo sicuri, portano al loro interno una firma elettronica valida. Per avere informazioni sull'autenticità di un programma e su chi lo propone basta visualizzare il suo certificato facendo clic sul nome del programma sottolineato nella finestra di dialogo dell'"avviso di protezione" come mostrato nell'immagine sottostante.



Per impedire che i Dialer che si nascono in un controllo ActiveX entrino nel PC cliccare il tasto destro del mouse sull'icona di Internet Explorer (Win 98) andare *Proprietà/Protezione*, cliccare su *livello personalizzato* e alla voce *scarica controlli ActiveX con firma elettronica* spuntare *disattiva*. Si tenga presente che i controlli ActiveX utili installati in precedenza, come Flash e QuickTime, continueranno a funzionare normalmente.

Se il Dialer è già nel nostro PC. Per verificare se è stato installato un Dialer sul nostro PC si devono controllare tutte le connessione create digitando il comando **netstat** nel **Prompt di MS DOS** la cui icona, se non è presente su Start/Programmi, è attivabile nel seguente modo: cliccare il tasto destro del mouse su uno spazio libero del Desktop, selezionare *Nuovo/collegamento* e alla voce *Riga di comando* digitare ***command,*** poi cliccare su avanti e fine; sul Desktop comparirà la relativa icona. Per intercettare e inibire le chiamate ai numeri speciali una soluzione semplice è costituita dai software gratuiti **StopDialer** oppure **DialGuard**.
Se è stata individuata una connessione non autorizzata si deve procedere alla operazione non semplice di rimuovere i file installati dai Dialer. La prima operazione da fare è quello di controllare la lista dei processi attivi, premendo *Ctrl+Alt+Canc* ed entrando nella maschera dei processi attivi (per Win XP). Guidati dall'intuito si deve individuare in questo elenco, il file.exe associato al Dialer. Nella ricerca si tenga presente che Windows XP ha la seguente lista di processi che non devono essere terminati: SVCHOST.EXE, LSASS.EXE, INETINFO.EXE, MDM.EXE, SPOOLSV.EXE, WINLOGON.EXE, SMSS.EXE, SERVICES.EXE.
Solitamente i Dialer si installano all'avvio di Windows. Per scoprire quali sono i programmi che vengono lanciati automaticamente all'avvio, si può usare l'utility **msconfig** da START/ESEGUI e andare sull'etichetta *Avvio* (Win XP) o *Esecuzione automatica* (Win 98). Spuntando il Checbox dei programmi sospetti, è possibile disattivare la loro esecuzione all'avvio. E' necessario anche rimuovere dal comando ***Regedit*** la chiave di registro presente in HKEY_LOCAL_MACHINE\Software\Microsoft\CurrentVersion\Run che carica il Dialer ad ogni avvio.

Se aveste già subito la truffa. E' possibile scorporare dalla bolletta la cifra relativa ai numeri 709 e 899 facendo immediatamente denuncia alla polizia postale. Un sito dove trovare indicazioni pratiche su come ottenere indietro i soldi da Telecom è: www.internet-marketing.it/nodialers.html. Chiamando la Telecom (al 187) è possibile richiedere la disattivazione dei numeri telefonici a pagamento. In questo modo, ogni tentativo di connessione da parte del Dialer verrà ignorato.