Welcome to InVircible for Windows95/NT version 7.01!

Please select one of the following:

Options dialog box.

In this dialog box you can change the way InVircible operates. Please select one of the topics below to get more detailed help.

{button , JumpId(IDH_OPT_ACTION)} Action

{button ,JI(`',`IDH_OPT_REPORT')} Report file

{button ,JI(`',`IDH_OPT_ACCELERATE')} Accelerated processing

{button ,JI(`',`IDH_OPT_FILES')} Files to check

{button ,JI(`',`IDH_OPT_SUBDIRS')} Check subdirectories

{button ,JI(`',`IDH_OPT_EXIT')} Exit when done

{button ,JI(`',`IDH_EXC_EXCLUDE')} Exclude dialog box

Action

Choose action to be taken when active word document or suspicious template are found:

- *Warn & Continue* - Do nothing, only place the note into the log.
- *Ask on Each* - Ask the user on each suspicious file.
- *Clean All* - Disable or rename macros in all suspicious files found.

Report file

Choose whether you want printed report or not, and how it should be created.

- *Append* - If file with the specified name already exists, then append to it, else create one.
- *Overwrite* - Delete the file with specified name, and then create a new one.
- *None* - Do not create report file at all.
- *Location* - Press this button to choose drive, directory and filename of report file.

Accelerated processing

When you select *Check created/modified* option, the program will check only the files which were modified or created during the last *n* days, where *n* is the number you enter in *within last...* edit box.

Files to check

- *Default only* - Check only files with *.DO? extension (Microsoft Word documents).

- *All files* - Check all files.

When this box is checked, the program will work recursively on subdirectories, starting with the one selected on the main screen.

When this box is checked, the program will terminate as soon as it completes the scan.

When clicked this button will lead you to the Exclude dialog box.

Exclude dialog box.

In this dialog box you can select which directories or files with specific names or extensions will be skipped during the scan. This is useful when you are sure about integrity of specific files, or if you have "fancy" documents or templates which include document automation, multimedia, etc. and may trigger InVircible's alarm.

Select one of three tabs: *Directory*, *File name* or *Extension* and use *Add* and *Delete* buttons to add or remove entries to/from corresponding list.

Directories in this list will **NOT** be scanned.

Files in this list will **NOT** be scanned.

Files with extensions in this list will **NOT** be scanned.

Use this button to add an entry to the currently visible list.

Use this button to remove an entry from the currently visible list

Cleaning the file.

Active Word Document or suspicious template was found. You could do the following:

- Disable or rename macros (depending whether document or template was found).

- Do nothing, continue scan.

- Cancel scanning.

What's new in InVircible for Windows95/NT version 7.01

This is a major update version. Many new features were added and the overall speed of processing was greatly increased. Among the most significant inclusions in this release are:

- Full support for Long File names.

- New enhanced user interface.
- Full Network support.

Primer on Macro Viruses

A macro virus is code written in an application's macro language that is capable of replicating. Macro viruses will reproduce only if the automatic execution of macros is enabled in the targeted application. By definition, macro viruses are **application specific**, to distinguish them from DOS viruses.

Unlike DOS viruses, that can use DOS and BIOS services (documented as well as undocumented), application specific viruses can only use commands that are available in the specific application's macro language. Not every application that uses macros is exposed to macro malware abuse, to this date only Word for Windows were successfully targeted by macro viruses although there were attempts made to target Microsoft's Excel by macro malware.

Applications' macro language is rather limited compared to the set of instructions available to the operating system as it should only provide for the application to perform its tasks. Winword is not expected to configure a hard drive or to manipulate the boot or partition sector. Although not absolutely impossible, the formatting of your hard drive by a Winword macro virus is unlikely.

Another distinction of the Winword macro viruses from the DOS ones is that macro viruses affect **data** rather than the application itself. To read how to protect from Word macro viruses click here.

Protecting from Macro Viruses

There is more hype than substance in the Word macro virus issue, yet justified or not, they are a serious concern to many, especially in the corporate and network environment.

InVircible uses generic methods for detecting and cleaning macro viruses from Word files. It will screen Word files for the presence of active macros and check if templates contain automatic macros. It will then issue action depending on what action mode was selected in the options dialog.

"Active word documents" or "Suspicious template" alarm may be issued when customized documents or templates are found, like the ones containing document automation, multimedia, etc. For that purpose there is an exceptions list option in InVircible.