Microsoft® Word Macro Virus Protection Tool Readme

October 9, 1995

Please read this entire document for important information about the Macro Virus Protection tool, including problems you may encounter when you run it.

Contents

Installing the Macro Virus Protection Tool

The Macro Virus Protection tool includes two files:

Scanprot.dot	The template that sets up the protection macros on your computer
Readme.doc	This file, which provides information about the tool and its operation

To install the Macro Virus Protection tool, copy Scanprot.dot to your Templates folder (for example, Word:Templates). In Word, click Open on the File menu, locate and click Scanprot.dot, and click Open. The protection tool (which is also called “ScanProt”) will be automatically installed and will prompt you for any additional input required.

This installation procedure is the same whether you run Word as a single-user setup, as a workstation installation from the network, or directly from the network. Because the setup procedure requires that you change each user's Normal template on each local computer, there is no shortcut method of installing the protection macros on more than one computer at a time. The tool must be run on each computer that is to be protected against macro viruses.

If for any reason you need to reinstall the Macro Virus Protection tool, follow these steps:

1. In Word, open the list of macros by clicking Macro on the Tools menu. In the Macros Available In list, click Normal.dot (Global Template). If a macro called InstVer appears in the list, click it and then click Delete. Click Close. (If InstVer does not appear on the list, just click Close.)

2. On the File menu, click Open. Locate and click the Scanprot.dot template and click Open.

3. The Warning alert will be displayed. Click No so that the protection tool Setup will run.

The protection tool will be reinstalled completely.

Removing the Macro Virus Protection Tool Macros

To completely remove the Macro Virus Protection tool, click Macro on the Tools menu. In the Macros Available In list, click Normal.dot (Global Template). Click the AutoExit macro and click Delete. Also delete the following macros: FileOpen, ShellOpen, and InstVer. This will remove macro virus protection from your system.

Common Questions About the Macro Virus Protection Tool

***Q:** What is a macro virus?*

A: A macro virus is a new type of virus that uses a program's own macro programming language to distribute itself. Unlike previous viruses, macro viruses do not infect programs; they infect documents. For more information about macro viruses, see the “Common Questions About Macro Viruses” section below.

***Q:** What is the Macro Virus Protection tool?*

A: The Macro Virus Protection tool is a free tool that installs a set of protective macros that detect suspicious Word files and alerts you to the potential risk of opening files that contain macros. Upon being alerted, you are given the choice of opening the file without its macros, thereby ensuring that no viruses are transmitted. The tool also contains an updated version of the scanning code for the Concept Virus and can be used to scan your hard disk for Word files that contain the Concept Virus. For more information about the Concept Virus, see the “Common Questions About the Concept Virus” section below.

***Q:** How does this new tool work?*

A: The Macro Virus Protection tool installs a set of protective macros in your Normal template. If you open a document containing macros, the protective macros are activated, and you are alerted to the potential risk of opening files that contain macros. You are given the choice of opening the file without its macros, opening the file as is, or canceling the File Open operation. Opening the file without its macros ensures that macro viruses are not transmitted and does not affect the content of the document. Microsoft recommends that you open the file without its macros unless you can verify that the macros contained in the document will not cause damage.

***Q:** What does the Macro Virus Protection tool protect against?*

A: The Macro Virus Protection tool is a general alerting mechanism that alerts you to *any macros* found in a document. Although the tool scans for the Concept Virus, its primary purpose is not to detect or repair specific viruses, but to alert you to the fact that you are opening a document that contains macros and that these macros could contain viruses. You can then protect your computer against macro viruses by opening the file without its macros.

***Q:** Does the Macro Virus Protection tool change my files?*

A: Upon installation, the tool offers to scan for any files that contain the Concept Virus. If any infected files are found, the tool deletes the Concept Virus from the files and resaves the files. After you install the tool, if you try to open a document that contains macros, the protection alert is displayed. If you cancel the File Open operation, or choose No in the Warning alert dialog box, nothing in the file is changed, and the File Open operation continues as if the tool were not installed. If you choose Yes and open the file without its macros, Word creates a new document containing all of the original document’s content but none of its macros. You can choose to save this new document with the same name as the original (thus overwriting the original and permanently removing the macros), or you can close the new document without saving it, to preserve the macros in the original.

Q: What is the difference between the Macro Virus Protection tool and Scan831.doc?

A: Scan831.doc is a tool that Microsoft made available to customers to scan and remove the Concept Virus from Word files. Since the release of Scan831.doc, all of the major anti-virus vendors have either shipped or committed to shipping tools that detect the Concept Virus. Although the Macro Virus Protection tool includes an updated version of Scan831 scanning code, the protection tool's primary function is to alert you to the existence of macros in your documents so you can open documents without their macros.

Q: Are there any known limitations of the Macro Virus Protection tool?

A: The protection tool works by trapping File Open operations. There are some methods of opening files that the tool cannot trap. If you open an infected file using one of these methods, your computer is not protected. Microsoft recommends avoiding opening documents in the following manner unless you are certain that the document is virus free. The methods that bypass the protection tool include:

- Clicking an item on the Most Recently Used files list on the File menu in Word.
- Dragging a document and dropping it on the Word program window.
- In Word for the Macintosh®, double-clicking a Word file in the Finder.
- In Word for Windows® 95 or Windows NT™, double-clicking desktop scraps.
- In Word version 6.0 for Windows or Windows NT, opening files using Find File.
- In Word for the Macintosh, clicking a file on the Finder's Recent Files menu.

Q: Which versions of Microsoft Word does the tool run with?

A: The tool works with Word 6.0x running under Windows 3.1, Windows NT, Windows 95, or the Macintosh, and with Word for Windows 95 running under Windows 95 or Windows NT.

Q: Where can I get the Macro Virus Protection tool?

A: You can download the tool from the following online services:

- The Microsoft Worldwide Web site at http://www.microsoft.com/msoffice
- MSN™, The Microsoft Network, using go word: macrovirustool
- The Word forums on other online services such as CompuServe® and America Online®

You can also obtain the tool by calling Microsoft Product Support Services at (206) 462-9673 for Word for Windows, or (206) 635-7200 for Word for the Macintosh; or by sending an Internet e-mail message to wordinfo@microsoft.com.

Q: How will updates to the tool be distributed?

A: Any updates that become necessary will be distributed on the following online services:

- The Microsoft World Wide Web site at http://www.microsoft.com/msoffice
- MSN, The Microsoft Network
- The Word forums on other online services such as CompuServe and America Online

Updates can also be obtained by calling Microsoft Product Support Services at (206) 462-9673 for Word for Windows, or (206) 635-7200 for Word for the Macintosh; or by sending an Internet e-mail message to wordinfo@microsoft.com

Common Questions About Macro Viruses

Q: ***How many different macro viruses currently exist?***
A: To date, the anti-virus community is aware of three macro viruses: the Word Prank Macro, also know as the Concept Virus; the DMV Virus; and the Nuclear Virus. Specific information about each of these viruses is included in the three sections following.

Q: ***Does the boxed package of Word or Office that I buy in the store contain macro viruses?***
A: Macro viruses do not exist in any version of Word or Office that you would buy in a store. You can get macro viruses only by opening a Word document or template that already contains the macro virus.

Q: ***Can macro viruses be transferred with documents created with or being read by Internet Assistant?***
A: Internet Assistant and documents created or read by it cannot be affected. Internet Assistant blocks the mechanism that distributes this type of macro.

Q: ***Can macro viruses be transferred with documents created with or being read by WordMail?***
A: Word cannot send or receive this type of macro as a WordMail message. However, like many e-mail editors, WordMail supports file attachments. If an infected document or template is sent as a file attachment, your computer can become infected when you open the attachment.

Q: ***Can macro viruses be transferred by documents being read with the Word Viewer?***
A: Because the Microsoft Word Viewer cannot save documents, it is unable to transmit macro viruses.

Common Questions About the Concept Virus

Q: ***What is the Concept Virus (also known as the Prank Macro)?***
A: The Concept Virus is a macro virus that, once it installs itself, lets you save documents only as templates. The virus does not cause data loss or any other damage, but it will replicate and distribute itself through Word documents. If the Concept Virus has installed itself, the first time you open a document containing the virus, you will see a dialog box that contains only the number “1” and an “OK” button. You can also determine whether the virus is installed by clicking the Macro command on the Tools menu—if the list contains the following macros, the Concept Virus has been installed: AAAZAO and AAAZFS.

Q: ***Does the Macro Virus Protection tool protect against the Concept Virus?***
A: Yes. Upon installation, the tool scans for the Concept Virus. If it finds the Concept Virus, it deletes it and installs protective macros to prevent the Concept Virus from installing in the future. The tool does not, however, detect infected files that are embedded in other OLE files or your e-mail file. Contact your anti-virus vendor for an updated version of its scanning tools.

Common Questions About the Nuclear Virus

Q: ***What is the Nuclear Virus?***
A: The Nuclear Virus is the only macro virus currently known to cause damage to your printouts and MS-DOS® system files. It uses the following macro names:

AutoExec

AutoOpen

DropSuriv

FileExit

FilePrint

FilePrintDefault

FileSaveAs

InsertPayload

Payload

The Nuclear Virus may cause damage in the following situations:

- If you open an infected document and try to print it, the virus may append the text “STOP ALL FRENCH NUCLEAR TESTING IN THE PACIFIC!” to your print job. This problem occurs if you send the print job to the printer between the fifty-fifth second and sixtieth second of any minute (according to your computer clock—for example, at 9:15:57).
- If you open an infected document between 5 P.M. and 6 P.M. (according to your computer clock), the virus will attempt to infect your computer with the PH33R Virus. The PH33R Virus is not damaging, however, because it installs a terminate-and-stay-resident (TSR) program in an MS-DOS session that ceases to exist when the macro finishes.
- On April 5 of any year, the virus zeros out your Io.sys and Msdos.sys files and deletes the Command.com file from your root directory. MS-DOS can no longer start, but because the crucial files are zeroed out, your system won't notify you that MS-DOS is gone at startup.

Q: Does the Macro Virus Protection tool protect against the Nuclear Virus?
A: The Macro Virus Protection tool alerts you any time you open a document containing macros. Because the Nuclear Virus is spread through macros, you are alerted when you try to open a document containing the Nuclear Virus. You can protect yourself from the Nuclear Virus by choosing to open the file without its macros.

Common Questions About the DMV Virus

Q: What is the DMV Virus?
A: This virus is very similar to the Concept Virus. Instead of using AutoOpen to start replicating itself, the DMV Virus uses AutoClose to install itself in your Normal (Global) template. Other than replicating itself and changing the FileSaveAs command, it does not do any harm.

Q: Does the Macro Virus Protection tool protect against the DMV Virus?
A: The Macro Virus Protection tool alerts you any time you open a document containing macros. Because the DMV Virus is spread through macros, you are alerted when you try to open a document containing the DMV Virus. You can protect yourself from the DMV Virus by choosing to open the file without its macros.

Integrating the Protection Macros with Existing User Macros

To ensure strong anti-virus protection, the Macro Virus Protection tool disables certain macros when the tool is installed. Because of the wide variety of macros and the potential that your Word files could be infected with a virus, it is not possible for the tool to automatically detect “good” macros and merge them so that they coexist with the protection tool.

This section describes how you can integrate user macros with the macros that the Macro Virus Protection tool provides. This is a technical process that requires knowledge of the WordBasic programming language. If you do not have the technical skills required to complete this integration, you have three options:

- Keep the Macro Virus Protection tool installed, and do without the functionality that the conflicting user macros provide.
- Remove the Macro Virus Protection tool and reinstall your original user macros, and do without the anti-virus protection functionality.
- Seek technical assistance for the problem from your internal help desk, a knowledgeable WordBasic user, or the original author of the user macros.

General Information

Q: What macros are installed when I run the Macro Virus Protection tool, and what happens if macros with the same name already exist?
A: During setup, the Macro Virus Protection tool installs the following macros to your Normal template: AutoExit, FileOpen, InstVer, and ShellOpen. If an AutoExit or FileOpen macro already exists, Setup renames the original macros by appending “User” to the end of the macro name. For example, FileOpen becomes FileOpenUser.

Q: How can I tell if I need to do any macro integration work?
A: When ScanProt installs, it looks for FileOpen and AutoExit macros in your Normal template. If it finds FileOpen, it displays the message “Your FileOpen macro has been renamed to FileOpenUser.” You will see a similar message for AutoExit. If you want to know whether this will happen before you install ScanProt, click the Macro command on the Tools menu, click Normal.dot (Global Template) in the Macros Available In list, and look through the names of the macros in the Macro Name list. If FileOpen or AutoExit appears in the list, you will have some macro integration to do. If you have already installed ScanProt and are unsure whether it renamed FileOpen and AutoExit, look in the Macro Name list for FileOpenUser and AutoExitUser; if those macros exist, ScanProt renamed the original macros. In addition, if you have any custom templates that have their own AutoExit or FileOpen macros, you have some macro integration to do.

Q: Is it always possible for me to integrate my existing macros with the protection macros?
A: Not always. If any of your macros are *execute-only* macros, you will not be able to integrate the existing macros with the protection macros. To determine if your macros are execute-only macros, follow these steps:

1. On the Tools menu, click Macro. In the Macros Available In list, click Normal.dot (Global Template).
2. Click each of the *xxxx*User macros in turn.
3. As you click each macro, notice whether the Edit button becomes unavailable (dimmed). If the Edit button becomes unavailable when you click one of the *xxxx*User macros, it means that that macro is an execute-only macro, and it cannot be integrated with the protection macro in its present state.

You have three options for execute-only macros. You can (1) contact the author/vendor of the original macros and ask for editable versions of the macros or for a new version of the execute-only macros that are integrated with the protection tool; (2) install the protection tool macros and forgo the features of the original macros; or (3) not install (or remove) the Macro Virus Protection tool and do without the anti-virus protection functionality.

Specific Information

If you've determined that the Macro Virus Protection tool has renamed at least one of your user macros, and that none of the renamed user macros are execute-only macros. You will have to follow different steps to integrate your user macros with the protection macros, depending on which user macros have been renamed. The two sets of steps are described below.

Integrating Your User Macros with FileOpen

The FileOpen code that the Macro Virus Protection tool installs simply makes a call into the ShellOpen macro. Therefore, to integrate your code in the FileOpenUser macro, you must copy and paste the appropriate code into the ShellOpen macro (instead of the FileOpen macro). Examine the code in your FileOpenUser macro and determine which parts of the user macro code are to run *before* the actual FileOpen operation and which parts of the code should run *after* the FileOpen operation. Once you determine which code goes before and which code goes after, copy and paste the "before" code into the ShellOpen macro at the first point in the ShellOpen code where the comment reads "INSERT YOUR CODE HERE." Then copy and paste the "after" code at the second point in the ShellOpen code where the comment reads "INSERT YOUR CODE HERE." Note that copying your macro code into other points in the macro could cause the protection macros to lose their protection capabilities. In many cases, you will have to do additional coding or bug fixing to make the integration seamless, but these are the general guidelines to follow.

Important: The process above will let you integrate with any custom FileOpen macro you have in your Normal template. However, you also need to integrate the custom code into your custom templates that have FileOpen macros in them. Completing this procedure involves (1) copying the integrated ShellOpen macro from the Normal template to each of your custom templates that contains a FileOpen macro, (2) integrating the existing FileOpen macro in the custom template with the ShellOpen macro you just copied from the Normal template into the custom template, and (3) copying over the original FileOpen macro in your custom template with the integrated FileOpen macro from your Normal template. If you do not complete these steps on a template that contains a FileOpen macro, a macro virus could escape detection when you open a template that contains the FileOpen macro or when you open a document attached to such a template.

Integrating Your User Macros with AutoExit

To integrate with the AutoExit macro, you must examine the code in your AutoExitUser macro and determine which parts of the code should run *before* the actual FileExit operation and which parts of the code should run *after* the FileExit operation. Once you determine which user macro code goes before and which code goes after, copy the "before" code and paste it into the AutoExit macro at the first point in the AutoExit code where the comment reads "INSERT YOUR CODE HERE." Next, copy and paste the "after" code at the second point in the AutoExit code where the comment reads "INSERT YOUR CODE HERE." Note that copying your macro code into other points in the macro could cause the protection macros to lose their protection capabilities. In many cases you will have to do additional coding or bug fixing to make the integration seamless, but these are the general guidelines to follow.

Once you have completed all of your macro integration, you can delete all of the *xxxx*User macros in the Normal template, since they won't ever get called.