Microsoft Office 2000 and Security Against Macro Viruses

A White Paper

by Darren Chi
Symantec AntiVirus Research Center
Symantec Corporation

Contents

INTRODUCTION **4**

AN INTRODUCTION TO MACROS AND MACRO VIRUSES **4**

MACROS 4
Visual Basic for Applications *4*
Macros are stored in document files *4*
MACRO VIRUSES 5

MACRO SECURITY SETTINGS IN OFFICE 2000 ..... **5**

SETTING THE MACRO SECURITY LEVEL 5
Low security level *6*
Medium security level *6*
High security level *8*
MODIFYING THE LIST OF TRUSTED SOURCES 9
Adding a digital signature to the trusted sources list *9*
Managing the list of trusted sources *10*
TRUSTING ADD-INS AND TEMPLATES 11

MICROSOFT OFFICE ANTI-VIRUS API **11**

DIFFERENCES BETWEEN OFFICE 97 AND OFFICE 2000 ..... **14**

SECURITY 14
Opening an Office 2000 document with digitally signed macros in Office 97 ..... *14*
Opening an Office 97 document with macros in Office 2000 ..... *14*
FILE FORMATS 14
Web page format *14*
VBA macro storage format *14*
Word, Excel, and PowerPoint *14*
Access *14*

QUESTIONS CONCERNING SECURITY AGAINST MACRO VIRUSES IN OFFICE 2000 ..... **15**

EXCEL 4.0 MACROS 15
Can Excel 4.0 macros be signed? *15*
Can a document containing both Excel 4.0 macros and VBA macros be signed? *15*
If I have a document with signed VBA macros and then add Excel 4.0 macros to the document, will the VBA macros retain their digital signature when I save the modified document with the new Excel 4.0 macros? *15*
Does Excel 2000 provide a way to disable Excel 4.0 macros when opening a document? *15*
Do I get a warning when opening a document containing Excel 4.0 macros? *15*
DIGITAL SIGNATURES 16
Can a digital signature be forged? *16*
Does a digital signature guarantee the safety of a document's macros? *17*
What indications can I look for that the digital signature on the macros in a document has been tampered with or that the macros themselves have been modified since being signed? *17*
When I install Office 2000, will the trusted sources list contain any entries? *18*
Are the add-ins and templates that ship with Office 2000 signed? *18*
I have a document whose macros are originally virus-free and signed. What can I expect to see happen when it is subsequently infected with a macro virus? *18*
SECURITY LEVEL SETTINGS 18

I don't use macros at all. If I set my security level to high, am I guaranteed to be protected against macro viruses? *18*
I know that all my installed add-ins and templates are safe and so I have enabled the "Trust all installed add-ins and templates" setting. Am I really safe with respect to the already installed add-ins and templates? *18*
If I disable the "Trust all installed add-ins and templates" setting, will I also get a warning when using an add-in or template installed by Office 2000? *19*
EMBEDDED DOCUMENTS 19
Am I protected against macro viruses residing in embedded documents? *19*
Can web page documents contain embedded documents? *19*
WEB PAGE DOCUMENTS 19
When I save a document in web page format, the document can be round-tripped. Does this mean that the file format is the same for both web page format documents and for native format documents? *19*
Can a web page document contain macros? *19*
Can a web page document containing a virus infect my system if I am only using a web browser to view the document? *19*
Through what means would a web page document containing a virus be able to infect my system? *19*
Does the ability to round-trip a document also imply that my current anti-virus program will be able to detect and repair viruses in web page documents? *20*
ANTI-VIRUS API 20
Am I guaranteed protection against macro viruses if I install a third party anti-virus program that supports the new Anti-Virus API in Office 2000? *20*
PREVIOUS VERSIONS OF OFFICE 20
What happens when I use Office 97 and open an Office 2000 document with digitally signed macros? *20*
What happens when I use Office 2000 to open an Office 97 document with macros? *20*
ANTI-VIRUS PROGRAMS 20
Will my current anti-virus program provide me the same level of protection for Office 2000 documents as it does for Office 97 documents? *20*
What are some of the key criteria I should use in determining whether my anti-virus program will protect me against macro viruses in Office 2000 documents? *20*
NORTON ANTIVIRUS 21
Is Norton AntiVirus able to detect and repair macro viruses present in documents created using Office 2000? *21*
Is Norton AntiVirus able to detect and repair macro viruses present in the new web page format available for documents created using Office 2000? *21*
What happens to the digital signature of the macros in a document when the document is repaired of a virus by Norton AntiVirus? *21*
SECURITY MEASURES AGAINST MACRO VIRUSES 21
What are some recommendations for administrators? *21*
What are some recommendations for the everyday user? *22*

REFERENCE 22

Introduction

This white paper discusses the new macro security features in Microsoft Office 2000. The first half of the paper provides information about the new features. The second half answers questions about the issues that people are likely to have about what all this means in the context of macro viruses.

If you are unfamiliar with what macros and macro viruses are, then the immediate next section gives a brief introduction. Those who are already familiar may want to skip the macro virus introduction.

An Introduction to Macros and Macro Viruses

Before discussing macro viruses, it is important to understand what a macro is, so this section starts off with a discussion about macros.

Macros

In the "old" days before applications got as complex and multi-featured as they are today, a macro meant a convenient way of storing a sequence of keystrokes that performed some *macro* operation. The macro operation could then be invoked with only one or two keystrokes instead of the many that would otherwise be necessary, hence the term *macro*. For example, let us say that you are in charge of public relations at a company named ACMESoft and that you often write letters where you need to type in the company's name. Then in your word processing application, you might assign the sequence of keystrokes needed to type the name ACMESoft to a macro such that you could invoke it with, for example, the F3 key. Instead of having to type ACMESoft each time you needed to type it, you would just hit one key, the F3 key.

Those were the old days. Today, macros are much more than just a way of recording a sequence of keystrokes. In Microsoft Word, you can still record a macro in that way. But instead of the macro being represented as just a sequence of keystrokes, it is actually represented using a fully functional and powerful programming language. The term *macro* still applies, however, it is not in the same sense as it used to be. Now, when you record a macro you are actually indirectly writing a program.

Visual Basic for Applications

The programming language used to represent macros in Microsoft Office is called Visual Basic for Applications, or VBA for short. In addition to being used for recording user macros, the VBA programming language can be used to write fully functional programs. In fact, there are many third party independent software vendors who use VBA to develop add-on functionality for Microsoft Office applications. If someone wanted to, they could write an entire word processor using VBA. Any takers?

A simple example of how a macro looks in VBA is shown here:

```
Sub Macro1()
    Selection.TypeText Text:="ACMESoft"
End Sub
```

The above VBA program is in fact the representation of the macro that was discussed above, namely, the one that types out ACMESoft.

As mentioned, VBA can be used to write an entire application. Applications written using VBA have the ability to provide just as much functionality as the everyday applications that you use. They have access to system resources, such as reading and writing files and sending output to the printer.

Macros are stored in document files

In Microsoft Word, when you record a macro, you can choose to have it either stored in the current document you are working on and thus only available for use when working with that document or you can make it available globally so that it will be available for use no matter which document you are working on.

In the first case, you can transfer the document to another user who will also be able to use the macro because it was stored with the document. In the second case, if the macro is only stored globally, it is only stored on the computer where it was recorded and thus only usable there. However, you can still give another user the ability to use the macro if you first copy it to a document. That other user could then use this document to install the macro globally on his computer for use.

Microsoft Excel, PowerPoint, and Access documents can hold VBA macros as well.

Macro viruses

The term *macro virus* is used to refer to a computer virus that has been written using a macro programming language. VBA is an example of a macro programming language. A computer virus is designed to spread itself among as many computers as possible. In most cases, the virus will also have a *payload*. The payload may be as harmless as displaying an annoying dialog every so often or as harmful as formatting the hard drive. In order to be a potent threat, a virus needs the ability to distribute itself and to do so without being detected easily. The VBA environment in Microsoft Office provides such niceties for viruses.

The factors that make VBA macro viruses a real threat are the following:

1. VBA is a general purpose programming language. This means that a macro virus can be programmed to do anything.
2. A program written using VBA has access to system resources. This means that a macro virus can write to the hard drive among many other things.
3. In Microsoft Office documents, VBA programs are stored within documents. This means that a macro virus can be easily transported to another computer simply by copying the document.
4. VBA macros can be set to automatically run when a document is opened. This means that a macro virus in a document can be the first to get control when the document is opened.
5. People share document files (i.e., spreadsheets, drafts of letters, etc.). This means that macro viruses can be inadvertently transported to another computer.

A document might thus harbor a macro virus that can easily spread to other computers when the document is shared with other users. The ability to easily access system resources gives these macro viruses the potential to carry very harmful payloads.

Macro Security Settings in Office 2000

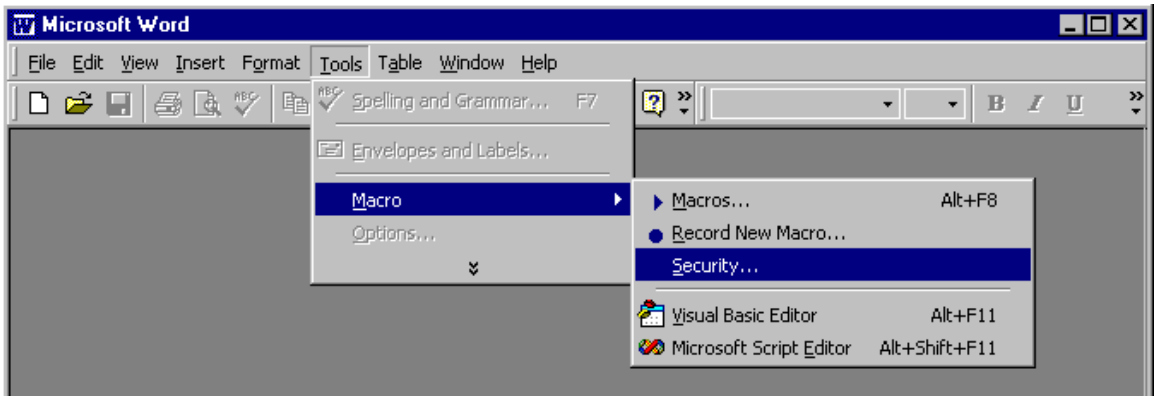
Word, Excel, PowerPoint, and Outlook each allow customizable macro security settings. Macro security settings are not available in Access.

These macro security settings affect the types of warnings the user gets when opening a document containing macros. The settings also allow the user to specify that documents digitally signed by specified individuals can automatically be trusted.

Setting the macro security level

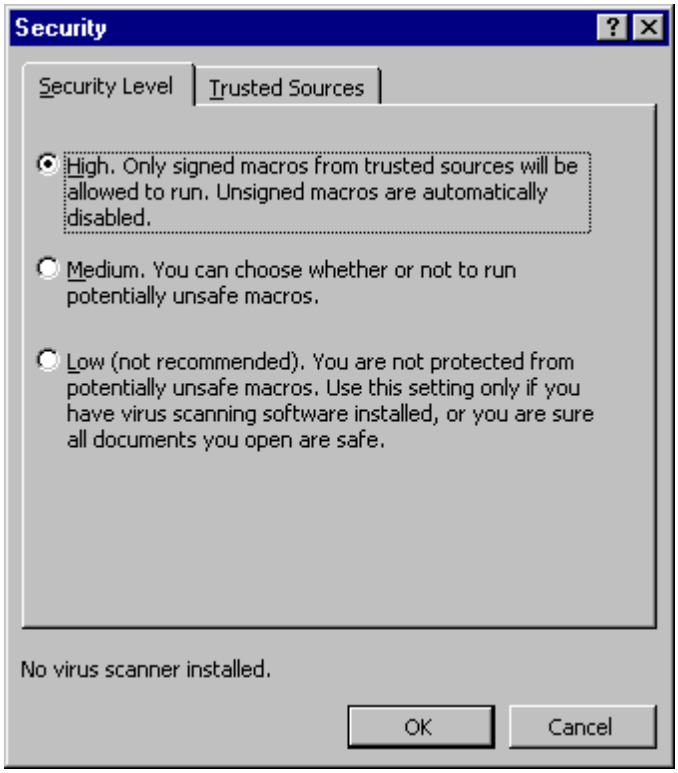
To modify the macro security level settings, invoke the Security dialog by selecting the **Security...** command under the **Macro** submenu of the **Tools** menu as shown Figure 1.

Figure 1. Invoking the Security dialog.



This displays the Security dialog shown in Figure 2. The Security dialog has two panels, one for setting the security level to one of three settings and one for specifying a list of trusted sources. Select the Security Level panel.

Figure 2. The Security dialog.

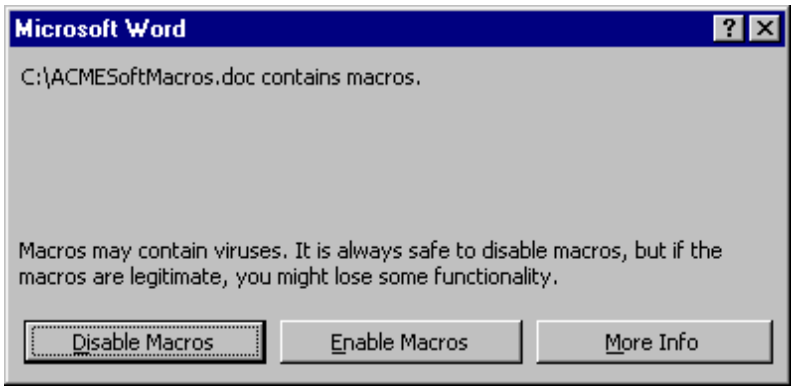


Low security level
The low security level setting is essentially no security. When opening a document containing macros, the application does not present a dialog warning of their presence. This is not the recommended setting.

Medium security level
When opening a document containing macros using the medium security level setting, the application presents a dialog warning of the presence of macros. The dialog gives the user the option of either disabling or enabling the macros in the document. The user can also choose to not open the document.

If the document's macros have not been digitally signed, then the security warning dialog looks like the one shown in Figure 3.

Figure 3. Medium security warning dialog presented when opening a document containing unsigned macros.



Opening a document whose macros have been digitally signed will present a dialog that looks like the one in either Figure 4 or Figure 5. The difference between the two is in whether or not the digital signature has been authenticated or not. Notice that the dialog in Figure 4 contains the additional wording of "This publisher has not been authenticated...". An authenticated digital signature is one whose chain of authentication leads to a trusted root certification authority. This includes digital signatures that are in the list of trusted root certification authorities that the user may have placed there.

Figure 4. Medium security warning dialog presented when opening a document containing macros signed using an unauthenticated digital signature.

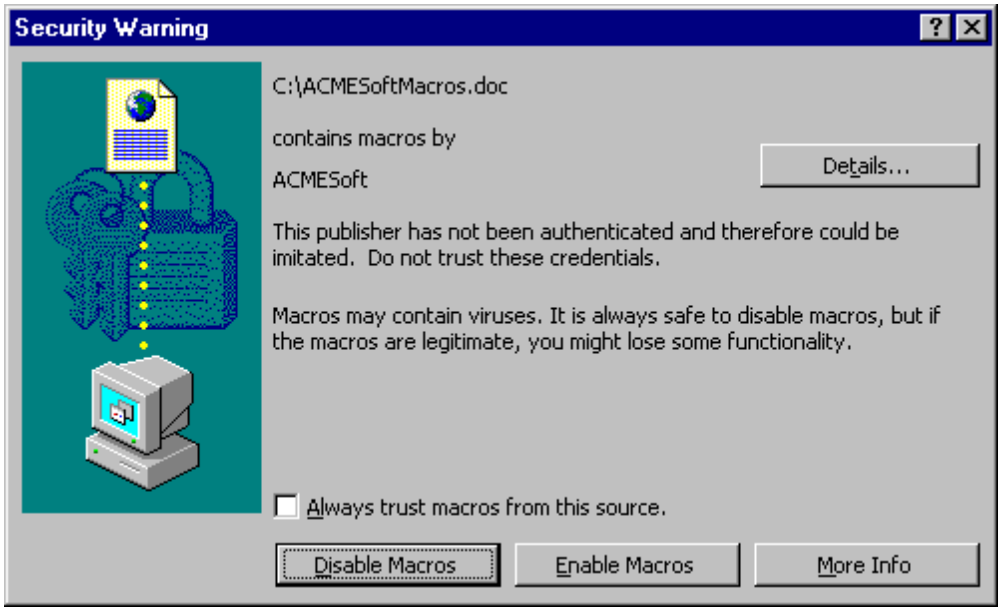
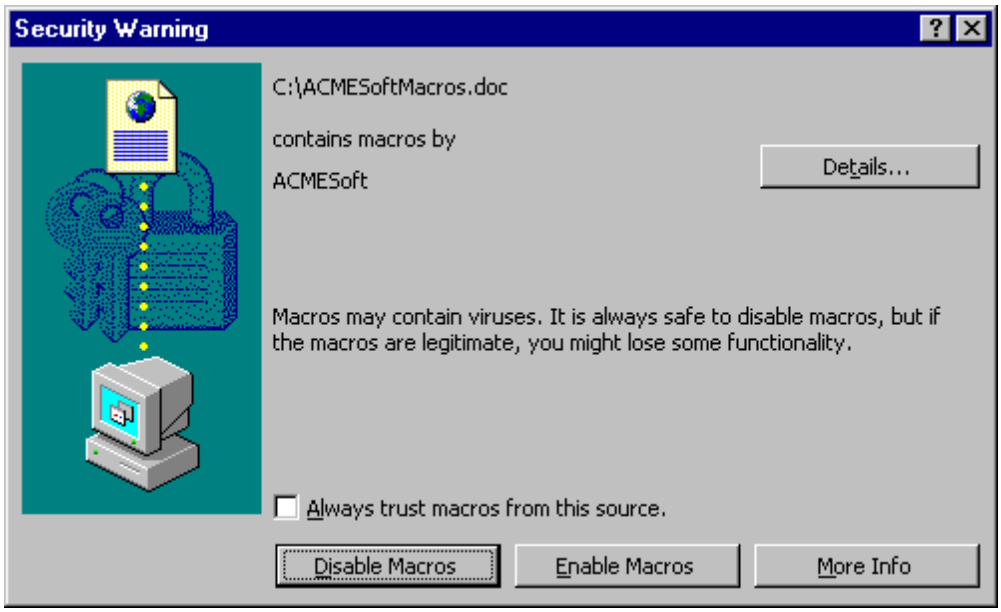


Figure 5. Medium security warning dialog presented when opening a document containing macros signed using an authenticated digital signature.

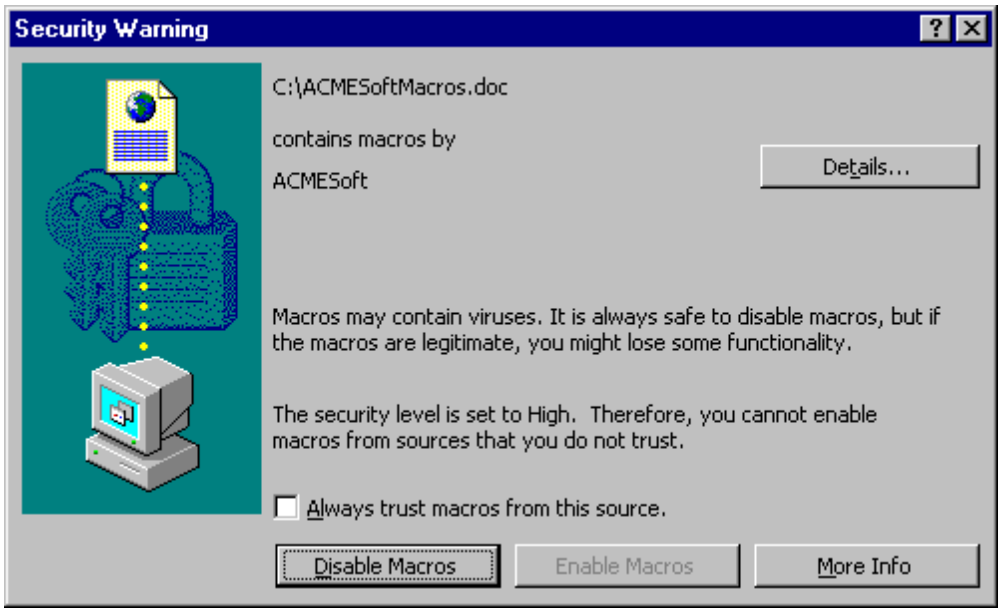


High security level

The high security level setting is the strictest. Opening a document containing macros that have not been signed with a digital signature that is in the user's list of trusted signatures presents the user with a Security Warning dialog with only the **Disable Macros** button enabled, as shown in Figure 6. High security warning dialog presented when opening a document containing an authenticated digital signature. When opening a document containing macros that have been signed with a digital signature that *is* in the user's list of trusted signatures, the macros are automatically enabled without the presentation of a Security Warning dialog.

Thus macros in documents that do not contain a digital signature are surely prevented from executing. Even macros in a document signed with an authenticated digital signature are prevented from executing, unless the signature is in the user's list of trusted signatures. Note that just because a digital signature has been authenticated does not mean that the content signed by that digital signature can be trusted. The authentication is only a measure of guarantee that the content came from the entity identified by the digital signature.

Figure 6. High security warning dialog presented when opening a document containing an authenticated digital signature.



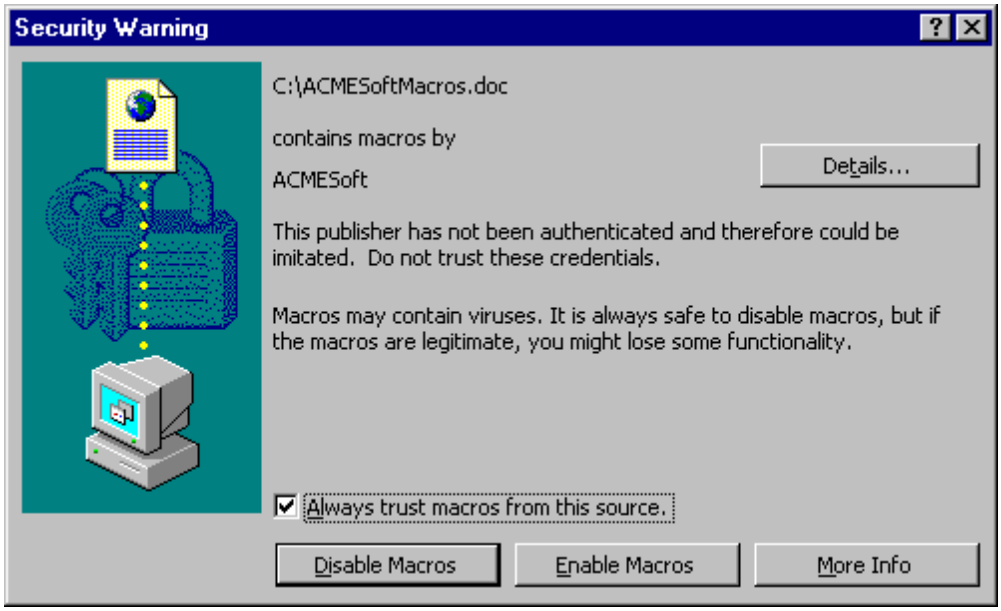
Modifying the list of trusted sources

If a digital signature is in a user's list of trusted sources, when the user opens a document containing macros signed by that digital signature, the macros are automatically enabled. *Note: This means that the Office application does **not** present the Security Warning dialog **regardless** of the security level setting.*

Adding a digital signature to the trusted sources list

As shown in Figures Figure 4, Figure 5, and Figure 6, the Security Warning dialog has a checkbox labeled "Always trust macros from this source." Checking the checkbox, as shown in Figure 7, and then selecting the **Enable Macros** button adds the digital signature of the document's macros to the list of trusted sources. Under the high security level, the **Enable Macros** button becomes enabled once the checkbox is checked.

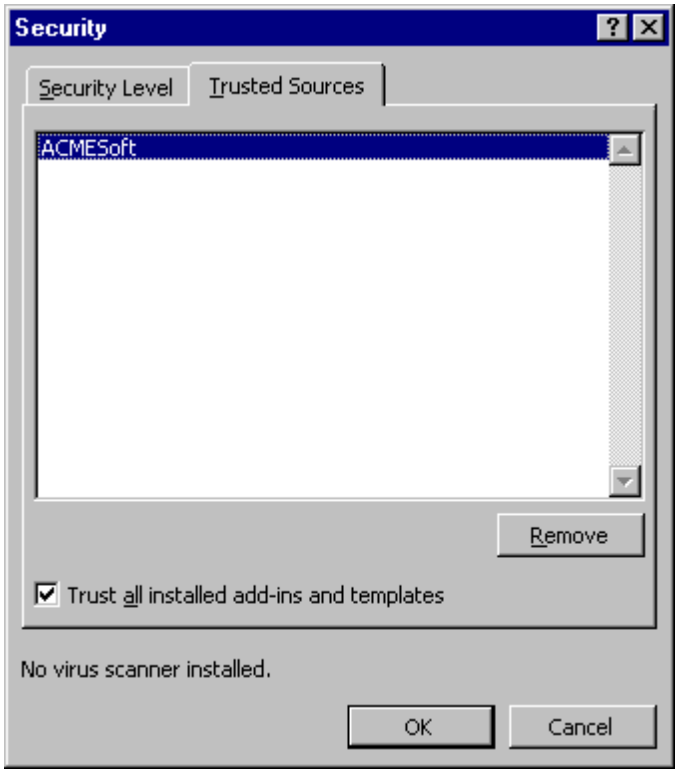
Figure 7. Adding the digital signature to the trusted sources list.



Managing the list of trusted sources

To view or modify the trusted sources list, invoke the Security dialog by selecting the **Security...** command under the **Macro** submenu of the **Tools** menu as shown Figure 1. In the Security dialog, select the Trusted Sources panel as shown in Figure 8.

Figure 8. The Trusted Sources panel in the Security dialog.



Contained within this panel is a list of trusted sources. A trusted source can be removed from the list by selecting it in the list and then using the **Remove** button.

Trusting add-ins and templates

In a default installation, add-ins and templates are automatically trusted. This includes add-ins and templates that come with the installation of Office 2000 and well as add-ins and templates the user subsequently installs or modifies. A well-known template is the "NORMAL.DOT" template that contains the global settings for Word documents. More examples of add-ins and templates are those that may be placed in Excel's "XLSTART" folder, such as "PERSONAL.XLS", to automatically load when Excel starts.

The trusting of add-ins and templates can be enabled or disabled through the Security dialog in the Trusted Sources panel. To disable the automatic trusting of add-ins and templates, the checkbox labeled "Trust all installed add-ins and templates" must be unchecked as shown in Figure 9. Do not trust installed add-ins and templates..

Figure 9. Do not trust installed add-ins and templates.

When automatic trusting of add-ins and templates is disabled, anytime an add-in or template is loaded by the application, the Security Warning dialog appears if the add-in or template contains macros.

Microsoft Office Anti-virus API

The Office 2000 applications Word, Excel, and PowerPoint allow the user to install third-party anti-virus modules for detection and repair of viruses in documents automatically when a document is opened within the Office application.

The anti-virus module must have been specifically written to understand the API. If any such modules are installed, then the status line near the bottom of the Security Level panel in the Security dialog will say "Virus scanner(s) installed", as shown in Figure 10. If not, then the status line will say "No virus scanner installed", as shown in Figure 11.

Figure 10. Virus scanner(s) installed status.

Upon opening a document, the Office application will call upon each installed virus scanner to perform a scan. Office itself does not provide any form of user interface nor feedback to the user in support of results from such scans. However, the status line of the Office application will have the text "Requesting virus scan..." while the scan is occurring. Thus the third party anti-virus module is responsible for essentially all aspects of performing the scan except for the notification that it receives from the Office application that a document is being opened.

Figure 11. No virus scanner installed status.

Differences Between Office 97 and Office 2000

Security

Opening an Office 2000 document with digitally signed macros in Office 97
Office 97 does not have the ability to verify digital signatures on macros. When an Office 2000 document containing macros is opened from within Office 97, the user will get a warning that the document contains macros if the Macro Virus Protection option is enabled. The user will have the choice of enabling or disabling macros in this case. Even if the macros in the document have been signed, the user will get no indication that this is so. However, if the user tries to view the source code of the macros, the user will not be able to do so. The Office 2000 application that saved the document has set this state for the macros so that if the document is opened under Office 97, the macros will not be modifiable. If this were not the case, the macros would loose their digital signature upon resaving from within the Office 97 application. The state preserves the digital signature on the macros.

Opening an Office 97 document with macros in Office 2000
Since a document with macros created in Office 97 cannot possibly have a digital signature on the macros, opening the document in Office 2000 will result in the Security Warning dialog being presented under the medium and high security level settings. The dialog will have the standard appearance for the case where the document's macros have not been signed.

File formats

Web page format
Word, Excel, and PowerPoint in Office 2000 allow documents to be saved in the new "Web Page" format or HTML format. This web page format has two implications. The more obvious one is that the document's contents are viewable with a web browser. The second implication is that the document can be *round-tripped*. This means that a document saved in web page format retains all the formatting capabilities that would normally be expected when the document is saved in its native format. This is accomplished by the use of XML (Extensible Markup Language) tags. These additional tags embedded in the HTML content of the document store the formatting information needed by the Office 2000 application. Additionally, the main HTML file will usually contain references or links to companion files that store yet more information needed by the Office 2000 application. These companion files will of course make transportation of such files slightly less convenient, but still manageable.

VBA macro storage format
The representation of VBA code has changed slightly, enough to the point where anti-virus programs will need to be updated to be able to detect viruses reliably in Office 2000 documents.

Word, Excel, and PowerPoint
Word, Excel, and PowerPoint documents created with Office 97 can be opened with the applications in Office 2000, and vice versa. But this does not mean that all aspects of a document created in an Office 2000 application will be available when the same document is opened with the corresponding Office 97 application. Furthermore, documents saved in web page format from within Office 2000 do not appear as native documents to Office 97. Office 97 does not understand the round-tripping information embedded in the XML tags.

Access
Access 2000 databases can not be opened with Access 97 because the format has changed. An Access 97 database can however be opened in Access 2000 with the option of converting the database to Access 2000 format.

Questions Concerning Security Against Macro Viruses in Office 2000

Excel 4.0 macros

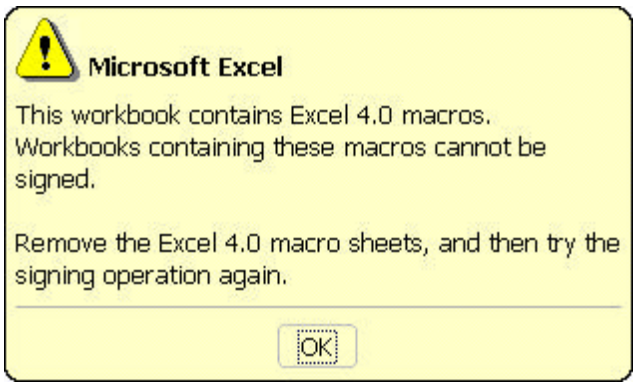
This section addresses issues about Excel 4.0 macros in Office 2000. Excel 4.0 macros are macros that reside on Excel 4.0 macro sheets in the main workbook of the Excel document and can be created with any version of Excel since version 4.0. Thus these types of macros are not specific to documents created using Excel 4.0.

Can Excel 4.0 macros be signed?
Unfortunately, only VBA macros can be signed. Microsoft Excel 2000 does not provide any method for signing Excel 4.0 macros.

Can a document containing both Excel 4.0 macros and VBA macros be signed?
A document containing both Excel 4.0 macros and VBA macros cannot be signed. This means that it is also not possible to sign just the VBA macros alone.

If I have a document with signed VBA macros and then add Excel 4.0 macros to the document, will the VBA macros retain their digital signature when I save the modified document with the new Excel 4.0 macros?
No. When you save the document, Excel will present the dialog shown in Figure 12. Although the dialog does not say it very clearly, what Excel will do is save the document, but the signature on the VBA macros will be removed as well. In order to resign the VBA macros, the Excel 4.0 macros must first be removed.

Figure 12. Adding Excel 4.0 macros to a signed document and then saving.

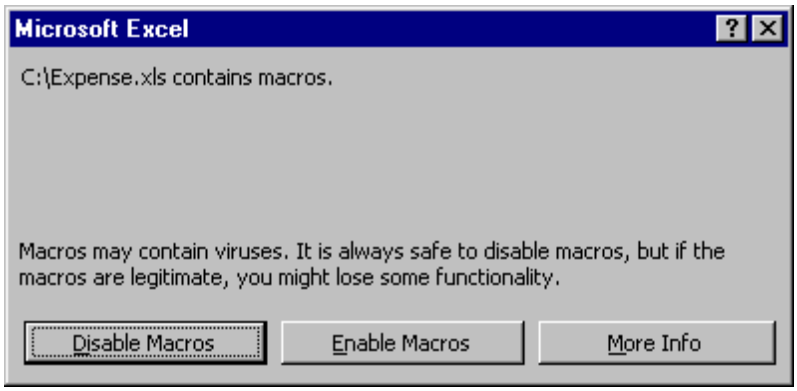


Does Excel 2000 provide a way to disable Excel 4.0 macros when opening a document?
Short of not opening the document, the answer is no. See the answer to the next question for details.

Do I get a warning when opening a document containing Excel 4.0 macros?
Fortunately, when the macro security level setting is either medium or high, Microsoft Excel 2000 will warn of the presence of Excel 4.0 macros in a document. As with VBA macros, when using a macro security level of low, a dialog warning of the presence of Excel 4.0 macros will not appear when opening a document containing them.

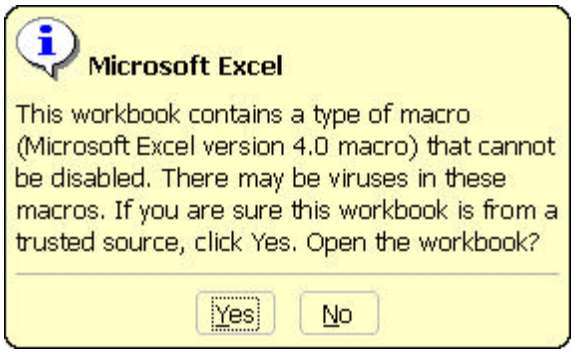
As expected, when the security level is medium, Excel 2000 will present a dialog warning of the presence of macros for a document containing Excel 4.0 macros, as shown in Figure 13. The dialog has a button for disabling the macros. However, Excel 4.0 macros can *not* be disabled. Selecting the **Disable Macros** button results in Excel 2000 presenting the dialog shown in Figure 14.

Figure 13. Excel 2000 macro warning dialog for a document with unsigned macros.



The dialog in Figure 14 is the actual dialog that informs of the presence of Excel 4.0 macros in the document. The dialog in Figure 13 is the standard dialog presented when opening a document containing unsigned macros. Because document containing Excel 4.0 macros cannot be signed, that dialog is presented first under the medium security level setting.

Figure 14. Excel 4.0 macros warning dialog.



The dialog in Figure 14 basically warns the user that Excel 4.0 macros cannot be disabled. With this warning, the user can then choose whether or not to open the document.

Digital signatures

This section addresses issues about the security of digital signatures. The term *macros* will refer to VBA macros only.

Can a digital signature be forged?
It is theoretically possible, but is extremely difficult to do. However, the owner of a digital signature also has a part in the security of a digital signature. In order to digitally sign a set of data with a particular signature, the signer must have possession of the digital certificate for the signature. This means that if a third party obtains possession of the digital certificate for a signature, that third party will be able to digitally sign data with the signature corresponding to that digital certificate. Thus the owner of a digital signature must maintain the security of the associated digital certificate.

Does a digital signature guarantee the safety of a document's macros?
The simple answer is no. However, if the following three conditions are met, it may be enough of a guarantee for yourself:

1. You trust the authenticity of the signature
2. The entity that signed the macros guarantees to you that the macros are safe
3. You trust the entity that signed the macros

The signature is a measure of guarantee that the macros have not been altered since they were signed. However, this does not preclude the possibility of the macros having been infected with a macro virus and thus signed along with the virus.

What indications can I look for that the digital signature on the macros in a document has been tampered with or that the macros themselves have been modified since being signed?
There are three main possible indications.

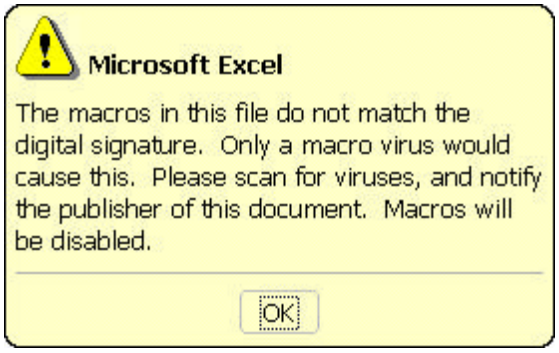
If the macros are modified on a system that does not contain the original digital certificate used to sign the macros and the document is then saved, the original digital signature will be removed. The person who performs this operation will see the dialog shown in Figure 15.

Figure 15. Modifying signed macros without the proper digital certificate.

Thus opening the modified document under the medium or high security settings will result in the macro warnings dialog that indicates that the document contains macros. There will be no indication that the document contains a signature since it has been removed. Neither will there be an indication that the document once contained a signature. Examples of how this dialog appears for the medium security setting are shown in Figure 3 and Figure 13.

If the digital signature does not correlate with the macros in a document, then upon opening the document under the medium and high security settings, a dialog will appear that warns that the digital signature does not match the macros as shown in Figure 16. This dialog indicates tampering has occurred on either the macros or the digital signature of the document.

Figure 16. Mismatched digital signature and macros warning dialog.



The last main indication of tampering requires careful attention to the Security Warning dialog. If the identification information presented does not correspond with what you expect, then there is cause for suspicion. For example, the information may indicate that the document's macros have been self-signed. If the normal scenario is that the information indicates that the macros in the document have been signed with a signature that is certifiable through a chain to a root certificate authority, then the digital signature on the macros has surely been altered.

When I install Office 2000, will the trusted sources list contain any entries?
It will be empty. You must explicitly add trusted sources. Only you can decide who to trust.

Are the add-ins and templates that ship with Office 2000 signed?
No, they are not.

I have a document whose macros are originally virus-free and signed. What can I expect to see happen when it is subsequently infected with a macro virus?
In general, macro viruses use the facilities of the Office application to perform the infection. Specifically, this means that when a macro virus infects a document, it will be as though a user modified the macros in the document. If the system on which the infection occurs does not have the digital certificate needed to resign the macros, the digital signature certifying the original macros in the document will be removed.

Security level settings

This section addresses issues about the various security level settings.

I don't use macros at all. If I set my security level to high, am I guaranteed to be protected against macro viruses?
You are protected against most macro viruses. For example, a high security level setting does not prevent Excel 4.0 macros from running, since they cannot be disabled as discussed in the section titled Excel 4.0 macros. Also, as discussed below, a virus could get into trusted add-ins and templates.

I know that all my installed add-ins and templates are safe and so I have enabled the "Trust all installed add-ins and templates" setting. Am I really safe with respect to the already installed add-ins and templates?

Enabling the setting to trust all installed add-ins and templates is essentially an option that provides a convenience to the user. The convenience is that under the medium and high security level settings, you will not get a macro warning dialog when an installed add-in or template containing macros is accessed. When the setting to trust all installed add-ins and templates is off, the frequency with which the macro warning dialog appears may become an annoyance.

Getting more to the point, the setting does not prevent modification of the installed add-ins and templates by a malicious program. For example, a malicious program or person may very well replace your

NORMAL.DOT template used by Word with a viral one. Another example is that an Excel document with malicious macros may be placed in your XLSTART directory without your knowledge and it would be trusted automatically. Thus the next time you start Excel, this new Excel document will automatically load and the malicious macros within it would be able to do their duty at will.

If I disable the "Trust all installed add-ins and templates" setting, will I also get a warning when using an add-in or template installed by Office 2000?
Yes. The Office applications do not distinguish between add-ins and templates created by Microsoft and those from third parties.

Embedded documents

Am I protected against macro viruses residing in embedded documents?
When viewing the contents of embedded documents, Office 2000 uses the same security protocol when opening the embedded documents. For example, if you are using the medium security level setting in Word 2000 and you open an embedded Word document, you will be presented with a dialog warning of the presence of macros in the document.

Can web page documents contain embedded documents?
Yes.

Web page documents

One of Office 2000's new features is the ability to save a document in web page format in a way that allows the document to be *round-tripped*, that is, retain all the information that a document saved in the normal format would have, such as formatting information.

When I save a document in web page format, the document can be round-tripped. Does this mean that the file format is the same for both web page format documents and for native format documents?
No. The web page format allows the document to be viewed using a web browser, thus Office will save it in HTML format so that web browsers are able to display the content. However, Office will write additional information to the file so that the document can be round-tripped. Some of this information will be in files separate from the main file but referenced from the main file either directly or indirectly through another file.

Can a web page document contain macros?
Yes. The VBA macros are stored in a file named "EDITDATA.MSO" that is stored in a folder under the folder containing the main HTML file of the document. This main HTML file contains a reference to the "EDITDATA.MSO" file.

Can a web page document containing a virus infect my system if I am only using a web browser to view the document?
If you are simply only viewing the web page document using a web browser, a virus that resides in the web page document cannot infect your system.

Note that this question specifically addresses the issue of viewing a document saved by Office 2000 into the web page format and does not address issues related to the security of using a browser.

Through what means would a web page document containing a virus be able to infect my system?
When the web page document was saved, the Office 2000 application that saved the document also included information about which Office 2000 application created the document. Internet Explorer 5.0 understands this additional information and can automatically start the appropriate Office application if you select Internet Explorer's Edit command available under the File menu. Doing so will thus launch the

appropriate Office application, at which point the behavior will be the same as opening a normal document with the possibility that if the web page document has macros that are viral, your system may become infected.

Does the ability to round-trip a document also imply that my current anti-virus program will be able to detect and repair viruses in web page documents?

The macros in a web page document are packaged in a new format. Anti-virus programs which have not been specifically designed to understand this new format will not be able to see the macros in the web page document. Consequently, they will not be able to detect nor repair viruses in web page documents.

Anti-Virus API

Am I guaranteed protection against macro viruses if I install a third party anti-virus program that supports the new Anti-Virus API in Office 2000?
You will need to ask the publisher of the anti-virus program for answers to this question. In general though, the protection offered is equivalent to installing an on-access anti-virus program. Such an anti-virus program will scan a file for viruses when the file is accessed, such as when a document is opened within an Office application, including add-ins and templates.

Note that the Anti-Virus API is not supported by Access 2000.

Previous versions of Office

What happens when I use Office 97 and open an Office 2000 document with digitally signed macros?
Since Office 97 does not support digital signatures, when you open the document, you will not get any information with regard to the fact that the macros in the document have been digitally signed. The Office 97 application will only have knowledge of the fact that the document contains macros. Thus, assuming that the Macro Virus Protection setting is enabled, the Office 97 application will present the usual dialog warning of the presence of macros along with the option to disable the macros.

What happens when I use Office 2000 to open an Office 97 document with macros?
Since Office 97 does not support digital signatures, when you open the document, the behavior will be identical to the behavior when opening an Office 2000 document with unsigned macros.

Anti-virus software

Will my current anti-virus software provide me the same level of protection for Office 2000 documents as it does for Office 97 documents?
If the anti-virus software has not been specifically updated to address the changes in the format of Office 2000 documents, then the answer is no.

What are some of the key criteria I should use in determining whether my anti-virus software will protect me against macro viruses in Office 2000 documents?
There are three main areas you should be concerned with:

1. Has the anti-virus software been updated to reliably detect and repair Office 2000 documents in light of the changes that have been made to the format? Note that the interchangeability of documents between Office 97 and Office 2000 does not mean that there are no differences in format.
2. Does the anti-virus software remove the digital signature when repairing an infected document? If it does not, then you may be subject to unnecessary warning dialogs presented by Office 2000 when opening a document with signed macros after it has been repaired by the anti-virus software.

3. Is the anti-virus software able to detect and remove viruses from infected web page documents? Specifically, has the anti-virus software been updated with the ability to detect viruses residing in the EDITDATA.MSO file that accompanies a web page document? Web page documents can harbor viruses just as well as documents in the normal format.

What will I need to do to update my anti-virus software so that it can properly provide me protection against macro viruses residing in Office 2000 documents?
The core technology in your anti-virus software needs to be updated. This core technology is a software engine that provides the capability to handle Office 2000 documents. Most anti-virus software requires that you re-install a new version of the software that has the new technology in it. However, if you are using Norton AntiVirus, making sure that you have the newest engine technology only requires that you perform a normal virus definitions update. Further details about Norton AntiVirus are given in the next section.

Norton AntiVirus

Norton AntiVirus is Office 2000 ready.

Is Norton AntiVirus able to detect and repair macro viruses present in documents created using Office 2000?
Yes.

Is Norton AntiVirus able to detect and repair macro viruses present in the new web page format available for documents created using Office 2000?
Yes.

What happens to the digital signature of the macros in a document when the document is repaired of a virus by Norton AntiVirus?
Since Norton AntiVirus does not possess the digital certificate used to originally sign the macros of a document, it cannot re-sign the macros after removing the virus. Thus Norton AntiVirus removes the digital signature during repair of a document. If Norton AntiVirus did not do so, then when the document is next opened, the Office 2000 application would present a warning that the document's macros do not match the digital signature and could possibly be a virus, as demonstrated in the dialog shown in Figure 16.

In the medium and high security level settings, removal of the digital signature results in the standard macro warning dialog being presented when the document is next opened.

How do I ensure that my installation of Norton AntiVirus has the updated technology required to completely protect me against viruses in infected Office 2000 documents?
Simply perform a virus definitions update with the LiveUpdate feature of Norton AntiVirus. This simple procedure is made possible by a modular engine technology called NAVEX. Through a virus definitions update, NAVEX allows the Symantec AntiVirus Research Center to provide the user with the latest state-of-the-art technology for protection against the latest new virus threats. In contrast, other anti-virus software will more often than not require that you obtain and re-install a new version of the entire product rather than just performing a virus definitions update to obtain the new technology.

Security Measures Against Macro Viruses

What are some recommendations for administrators?
In order to minimize the number of malicious macro incidents, the administrator may want to take the following measures to maximize security:
1. Set all security level setting to high for all workstations. This ensures that if a document has VBA macros, only VBA macros signed by a trusted source will be able to execute.

2. Populate the list of trusted sources with the digital certificates from sources that you trust. If your organization also authors VBA macros, then your organization may want to obtain a digital certificate for signing VBA macros created by the organization.
3. Lock the security settings and disable the user interface commands that allow them to be changed. The Office Resource Kit provides a policy editor tool for doing so. Note, however, that if the user has access to the registry and knows where these settings are stored, the user can still change them. This also means that a virus could also tamper with the settings, for example, setting the security level to low.
4. Use a proven and trusted anti-virus program with an on-access scanner, such as Norton AntiVirus.

What are some recommendations for the everyday user?

1. Set the security level to at least medium. This ensures that if a document has VBA macros you will be alerted of their presence and have the option of disabling them.
2. Populate the list of trusted sources with the digital certificates from sources that you trust. If you create VBA macros for your own use, you may want to create a self-signed digital certificate for signing the macros you create by using the SELFCERT.EXE tool provided with Office 2000.
3. Use a proven and trusted anti-virus program with an on-access scanner, such as Norton AntiVirus.

Reference

Sources for additional information on topics discussed in this white paper:

- Symantec AntiVirus Research Center: http://www.symantec.com/avcenter
- NAVEX white paper
- Office 2000 Resource Kit
- Microsoft Security Advisor: http://www.microsoft.com/security/default.asp
- Verisign: http://www.verisign.com
- Thawte: http://www.thawte.com