

Copies FYI, Inc. presents:

Security Policies and Procedures

Security Training



Course contents

- Overview: Fundamentals of security
- Lesson 1: Password protection
- Lesson 2: About viruses and macros
- Lesson 3: Trust, certificates, and security settings

One lesson includes a list of suggested tasks, and all have a set of test questions.

Overview: Fundamentals of security



Worried about computer viruses? Does the mention of malicious macros scare you? Is there a way to protect yourself from these things?

Learn about security fundamentals in Microsoft Office programs and what you can do to help protect your computer and documents.

Course goals

- Create robust passwords and password-protect all of Copies FYI documents and information.
- Understand the importance of using antivirus software.
- Define what a macro is and set macro security levels to protect against viruses.
- Check a digital signature to see if a macro was created by someone you can trust.

Lesson 1

Password protection

Password protection

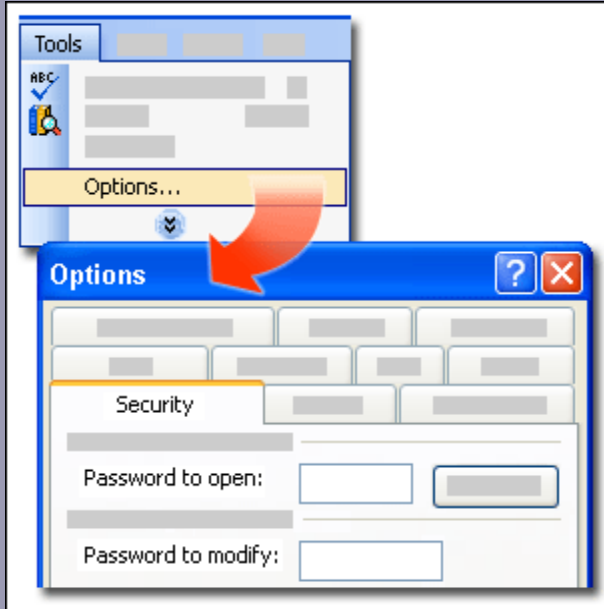


Strong passwords help protect your documents.

Passwords are your first line of defense in protecting your computer and your documents from malicious attacks:

- Strong passwords make it more difficult for someone to gain access to your files.
- You can password-protect individual Office documents to prevent others from seeing or editing them.

Password-protect a document

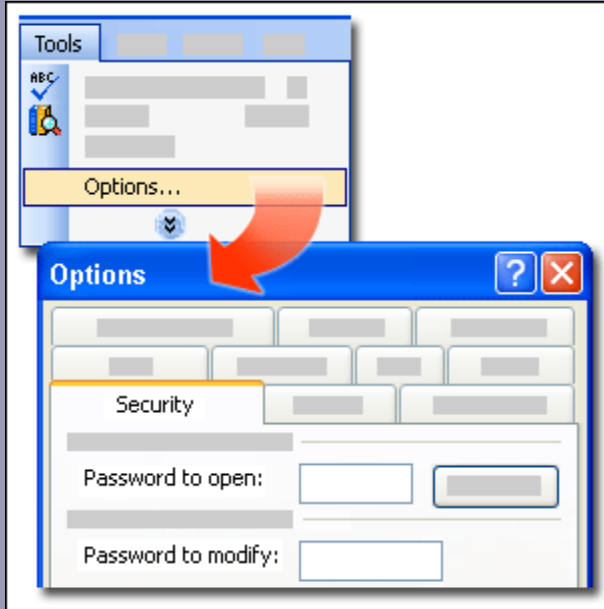


Create a password when you save a workbook.

Just as you can lock people out of your computer by using a password, you can "lock" a document. You can password-protect your document if you don't want other people to see it or if you don't want others to edit it.

Password protection for documents is available in various Office programs.

Password-protect a document



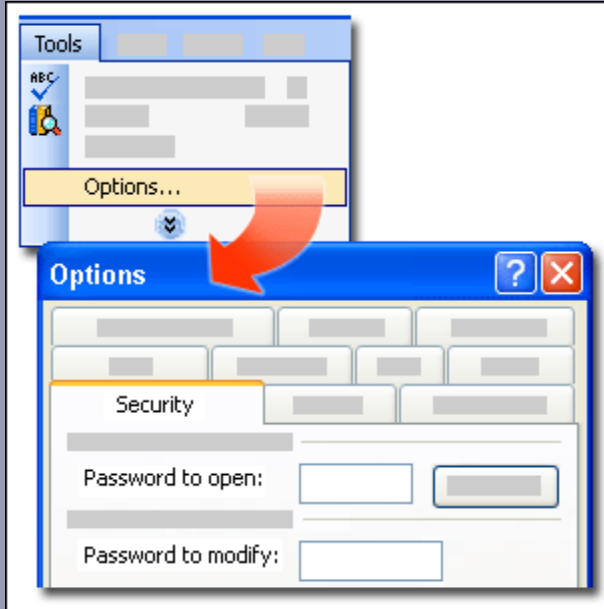
Create a password when you save a workbook.

In Word, Excel, and PowerPoint, the method is exactly the same:

- On the **Tools** menu, click the **Options** command.
- Click the **Security** tab.

From here you can select several options, including file encryption and file sharing, to help protect your document.

Password-protect a document



Create a password when you save a workbook.

The **Password to open** option is designed to help safeguard your documents.

The **Password to modify** option is not a security feature. It is intended to help you against making accidental changes to your documents.

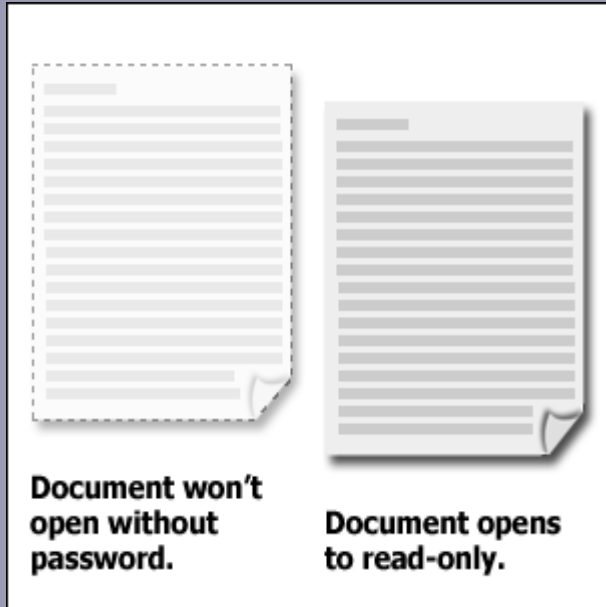
Password options



You have two basic options for password protection:

- **Password to open**
- **Password to modify**

Password options



To help prevent unauthorized users from seeing your document, you can require a **password to open** the file.

When you set a password to open a document, **encryption** is used to protect the contents of the file.

Password options



You can also choose to let other people read your document (known as a read-only document) but require a **password to modify** it.

Requiring a password to modify a file does not encrypt the file contents.

What's not secure



Others may have access to your documents.

Some of the settings that appear on the **Security** tab, including some that *sound* like security features, do not actually secure documents.

For example, **Read-only recommended** (available in Word and Excel) does not secure a document. It is only a guideline for readers; someone could still edit the document.

What's not secure



Others may have access to your documents.

The **Document Protection** task pane and **Protect Document** features (available in Word) do not secure your documents against malicious interference either.

They protect the format and content of your document when you collaborate with coworkers.

Create a strong password



A strong password is like a padlock.

No password is 100 percent secure. It can always be guessed or worked out. However, you can swing the odds in your favor by using a strong password.

A **strong password** cannot be easily worked out by anyone else.

Create a strong password



A strong password is like a padlock.

Strong passwords:

- Are *at least* seven characters long.
- Include both uppercase and lowercase letters, numbers, and a symbol character between the second and sixth characters.

Create a strong password



A strong password is like a padlock.

- Look like a random collection of characters.
- Have no repeated characters, nor do they have characters that are consecutive, as in 1234, abcd, or qwerty.
- Do not contain patterns, themes, or complete words (in any language).

Create a strong password



A strong password is like a padlock.

- Do not use numbers or symbols in place of similar letters. For example, \$ for S or 1 for l, as this makes the password easier to guess.
- Do not use any part of your user name for logging on to the Internet or a network.

Create a strong password



A strong password is like a padlock.

Change passwords frequently — at least every one to three months. When you replace a password, make sure it's totally different from the previous one and do not reuse any portion of the old password.

Do not write passwords down — Memorize them!

But I've forgotten my password...



A forgotten password can lock you out.

If you forget a password, there's nothing you can do. You're locked out.

The situation might not be too drastic, depending on which password you've forgotten.

But I've forgotten my password...



A forgotten password can lock you out.

- If it's a network password, the administrator can reset it.
- If it's the password for a Web account, most service providers will send you an e-mail message with the password or a reminder.
- If you forget the password to a document, you're locked out until you remember it.

Suggestions for practice

1. Create a strong password.
2. Set a password to open a document.
3. Recommend read-only.
4. Set a password to modify a document.

[Online practice](#) (requires Excel 2003)

Test 1, question 1

Which of these passwords is the strongest?
(Pick one answer.)

1. andy1234
2. 678AsDf!
3. STRONG
4. 9T&m2G7

Test 1, question 1: Answer

9T&m2G7

This is a strong password. It has numbers, letters (in upper- and lowercase) and symbols.

Test 1, question 2

You want to password-protect a document so that anyone can read it, but those who want to modify it must supply a password. What settings should you use on the Security tab in the Options dialog box? (Pick one answer.)

1. Enter a password in the **Password to modify** text box.
2. Select the **Read-only recommended** check box.
3. Enter a password in the **Password to open** text box.
4. Print a hard copy of the document for people who need to read it, and send a soft copy only to people who may need to modify it.

Test 1, question 2: Answer

Enter a password in the **Password to modify** text box.

With this setting, only people who know the password can modify the document, but anyone can open and read it.

Test 1, question 3

You've forgotten the password to open a password-protected file. What can you do? (Pick one answer.)

1. Call the Microsoft Office Support Center; they'll tell you how to crack the password.
2. Nothing.
3. Open the file through Windows Explorer rather than using the program's Open command.
4. Create a copy of the file, and open that one instead.

Test 1, question 3: Answer

Nothing.

Until you remember the password, there's nothing you can do to open that file.

Lesson 2

About viruses and macros

About viruses and macros



Viruses can attack your computer.

To take steps that make your computer more secure, you need some basic information about sources of infection. Know your enemy:

- A computer virus is a program hidden inside another file that may damage your documents or computer.
- A macro is an automated sequence of commands.

About viruses



Many potential sources of viruses exist.

A virus is a program that can be hidden inside another file — it replicates itself and spreads to other files and computers.

Different viruses cause different types of damage: One could scan your Microsoft Outlook® Address Book and send junk mail to all the addresses; another may actually destroy information on your hard drive.

About viruses

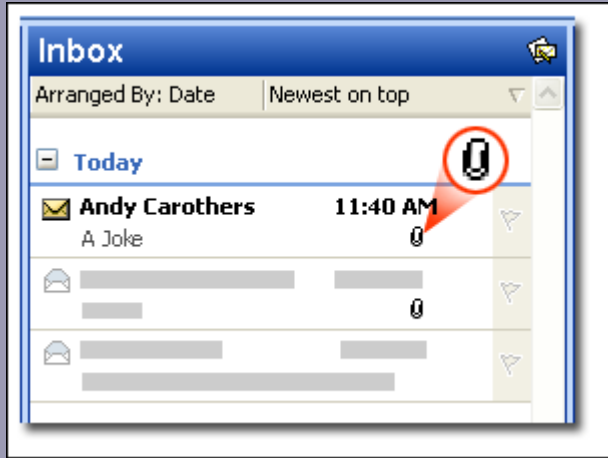


Many potential sources of viruses exist.

Your computer is always at risk from viruses. Some potential dangers that you might have to navigate include:

- Shared files, networks, floppy disks
- E-mail attachments
- Web-based e-mail
- Downloads
- Malicious Web sites

E-mail attachments

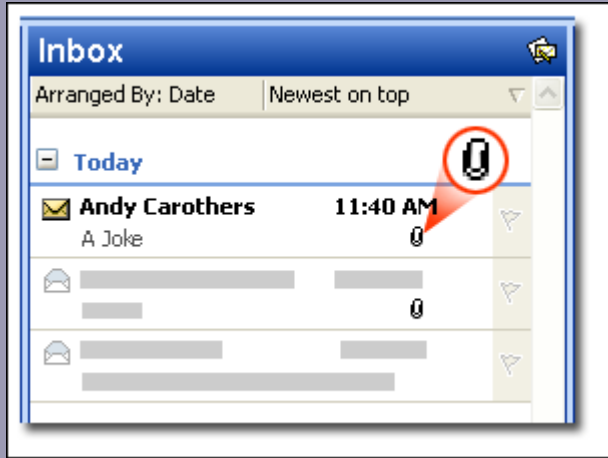


The paper clip icon indicates a message attachment.

Attachments in e-mail messages are one of the most common ways that your computer can "catch" a virus. Sometimes just opening the message can trigger the virus.

As you can see in the picture at left, it's easy to tell if a message has an attachment — it comes with a paper clip icon.

E-mail attachments

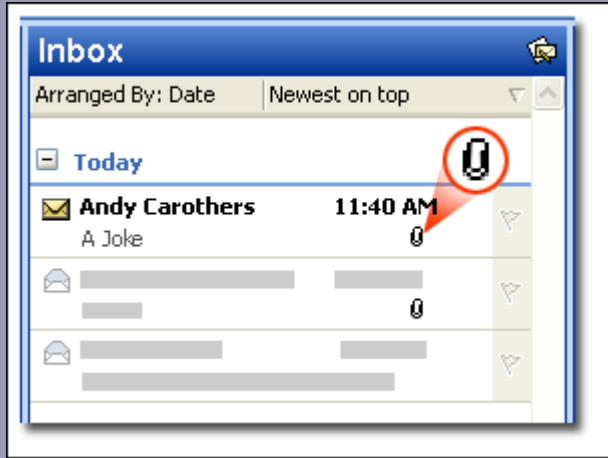


The paper clip icon indicates a message attachment.

Be especially suspicious if:

- The message is from someone you don't know or aren't expecting to hear from.
- The subject line is strange.

E-mail attachments



The paper clip icon indicates a message attachment.

If you are concerned that a message is infected, you can always e-mail the sender and ask for confirmation before opening it.

If the message does turn out to be viral, delete it *without* opening it, and then delete it from your **Deleted Items** folder.

Antivirus software



Protect your computer
against known viruses.

Your most important defense
against viruses is **antivirus
software**:

- Install it, use it, and keep it up to date.
- This software is essential as a defense against viruses.

Antivirus software



Protect your computer against known viruses.

Antivirus software is designed to detect *known* viruses. Because new viruses are always being written, it's essential to keep your antivirus software up to date.

When a new virus hits the world, the antivirus software manufacturers normally have an update available for download on their Web sites within hours.

Antivirus software

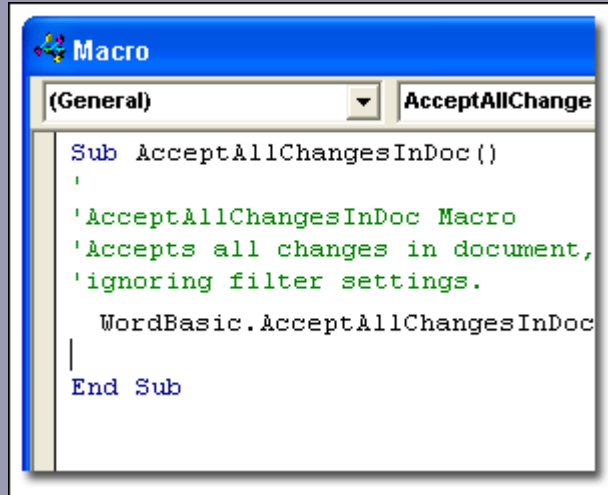


Protect your computer
against known viruses.

Antivirus software uses two basic screening methods:

- It scans for viruses when you download a file.
- It scans when you open a file.

About macros



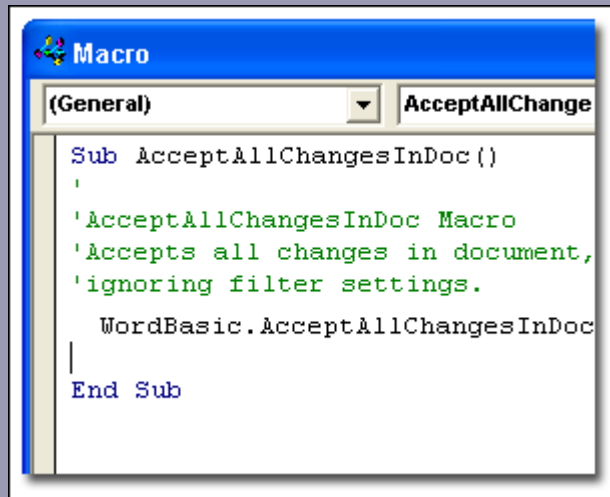
```
Macro
(General) AcceptAllChange
Sub AcceptAllChangesInDoc ()
'
'AcceptAllChangesInDoc Macro
'Accepts all changes in document,
'ignoring filter settings.
WordBasic.AcceptAllChangesInDoc
End Sub
```

A macro can quickly run a sequence of steps and commands.

You've heard about macros, but what are they?

A **macro** is a sequence of commands that can be run automatically. For example, it is useful for running a repetitive set of steps.

About macros



```
Sub AcceptAllChangesInDoc ()
|
'AcceptAllChangesInDoc Macro
'Accepts all changes in document,
'ignoring filter settings.
WordBasic.AcceptAllChangesInDoc
|
End Sub
```

A macro can quickly run a sequence of steps and commands.

Why do you need to worry about macros?

- Unfortunately, anyone can write a macro that includes a harmful sequence of commands.
- Harmful commands can do something simple, like add or remove text in a document, or they can remove data from your computer.

Test 2, question 1

If you get an e-mail message with an attachment from a source that looks legitimate but who you don't know, what should you do? (Pick one answer.)

1. Open the attachment and let your antivirus software check it.
2. Send e-mail to the sender and ask if the attachment is safe.
3. Delete the message; if it's important it will be sent again.
4. Wait for a colleague to open it and see if he or she has any problems.

Test 2, question 1: Answer

Delete the message; if it's important it will be sent again.

Test 2, question 2

What is your most important defense against computer viruses? (Pick one answer.)

1. Use antivirus software.
2. Never use macros.
3. Never let other people use your computer.
4. Check all e-mail attachments.
5. The computer user's knowledge and their diligence.

Test 2, question 2: Answer

The computer user's knowledge and their diligence.

Test 2, question 3

**Which of these statements best describes a macro?
(Pick one answer.)**

1. A sequence of commands written with malicious intent to damage your data.
2. The method by which all computer viruses are delivered.
3. A sequence of commands that can be run automatically.
4. A security device built into Office programs.

Test 2, question 3: Answer

A sequence of commands that can be run automatically.

Many macros are useful time-saving devices.

Lesson 3

Trust, certificates, and security settings

Trust, certificates, and security settings



Only download files that you trust.

To work efficiently, you may have to run some macros on your computer, which means at some point you'll have to decide whether you can trust their authors.

Trust is a big issue with security. Who do you trust? How do you know? Fortunately, there are features in your Office programs to help you make these decisions.

Office security

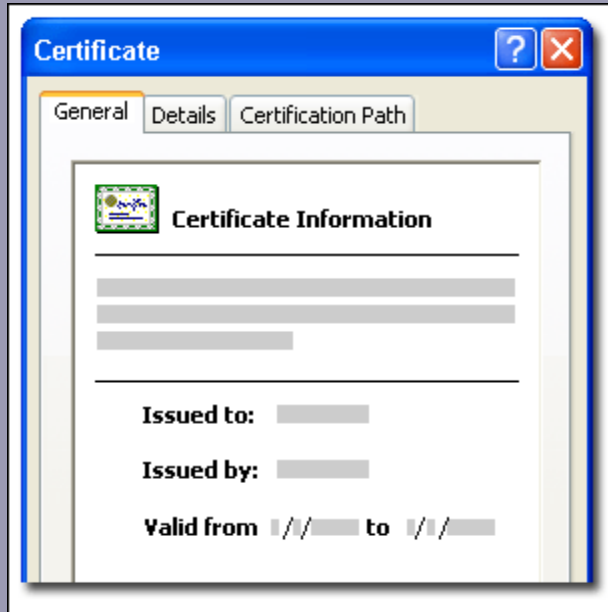


Download macros from trusted sources.

Two security features in Word, Excel, and PowerPoint are essential in helping protect you against macro viruses:

- Macro detection using macro security levels
- The **Trust all installed add-ins and templates** feature

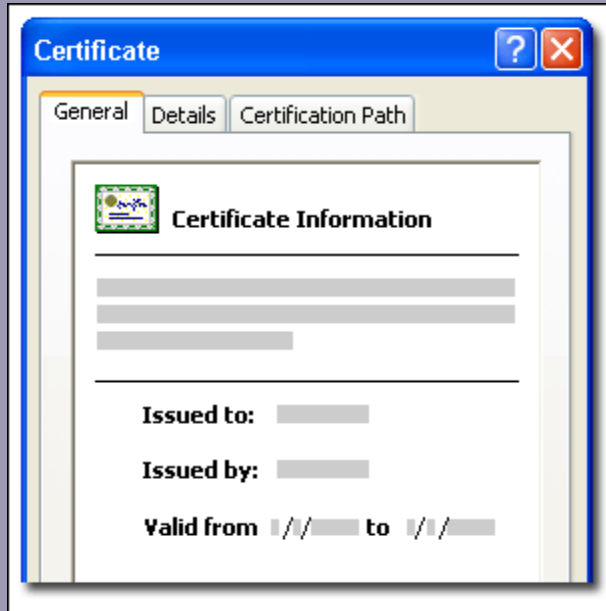
Digital certificates and signatures



Digital certificates are issued by commercial certification authorities who do background checks to verify that the writers or producers of macros (known as *publishers*) are reputable.

A digital certificate

Digital certificates and signatures



A digital certificate is used to *sign* macros, creating a **digital signature** on the macro.

A digital certificate can be used many times to create many digital signatures.

A digital certificate

What's trustworthy?



By definition, there are no trusted sources — you have to agree to trust them before they can get added to your **Trusted Publishers** list.

Security Warning dialog box

What's trustworthy?

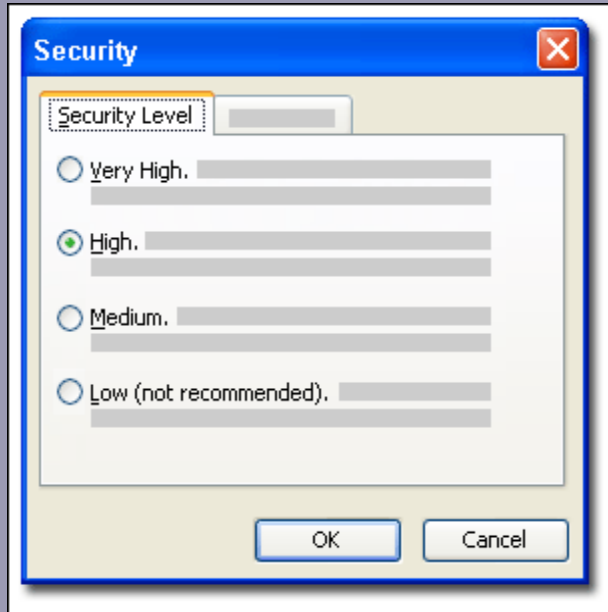


Security Warning dialog box

When you select the **Always trust macros from this publisher** check box, that publisher is added to your trusted sources list for both macros and other files.

But if you click **Enable Macros**, the macro will run just that particular time.

Macro security levels

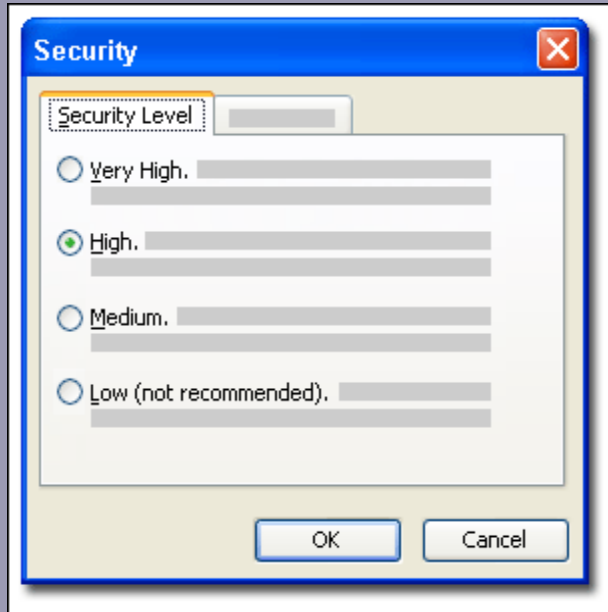


You can set up Word, Excel, and PowerPoint to detect macros.

These programs have a variety of security levels for macros so you can choose the level that is most comfortable for you.

Macro security levels dialog box

Macro security levels

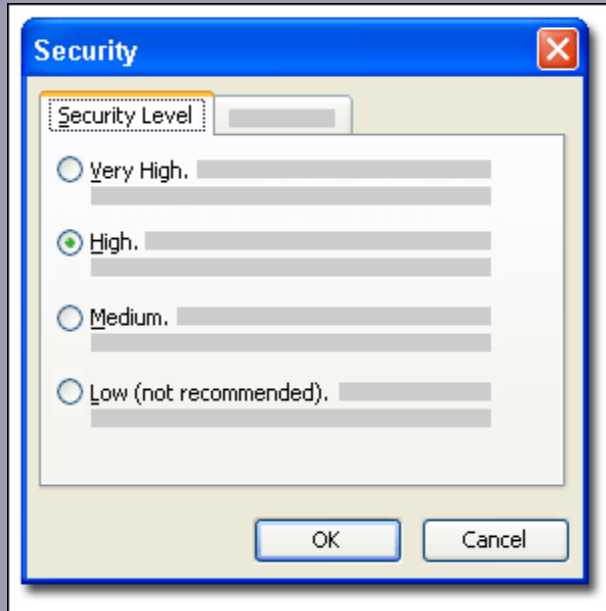


Very High: All macros will be disabled even if they have valid digital certificates.

This setting also disables all Com add-ins and Smart Tag .dlls, which you might need for Office programs to work as you expect.

Macro security levels dialog box

Macro security levels

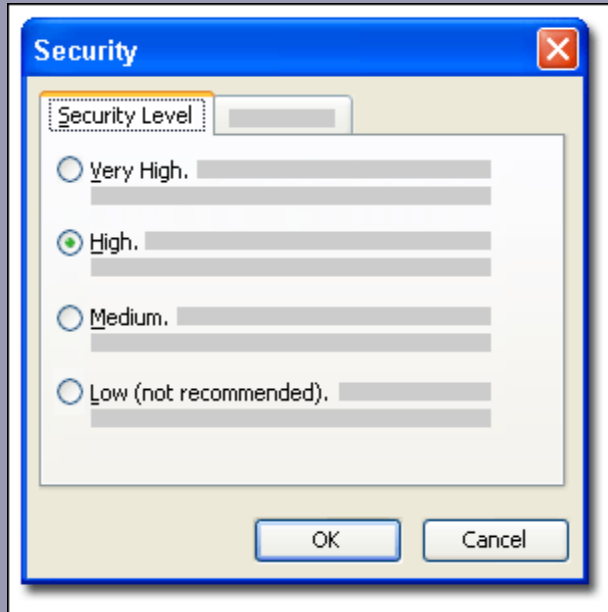


Macro security levels dialog box

High: Unless you have a specific reason to do otherwise, **High** is probably the setting you should use. This is the default setting.

Although macros from your trusted sources will run, you'll be prompted about unknown but signed macros and unsigned macros will be disabled.

Macro security levels

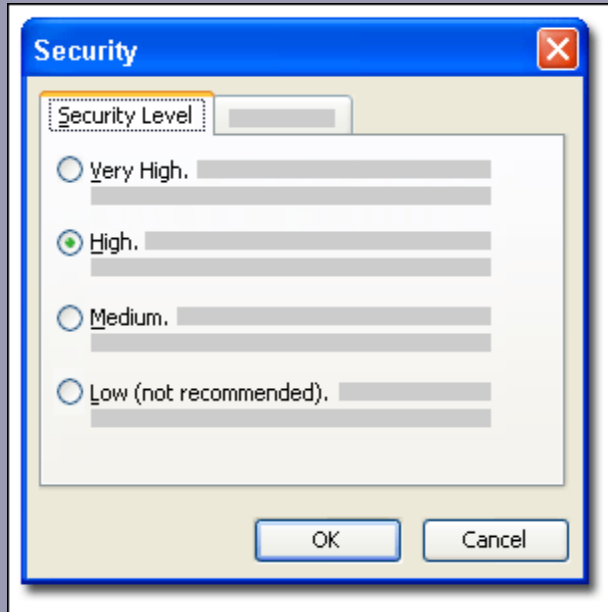


Macro security levels dialog box

Medium: Macros from trusted sources will run but you'll be prompted about all unknown macros, including unsigned ones.

Low: You should be very sure when using this setting. You will not receive any prompts or warnings. **All** macros will run.

Macro security levels

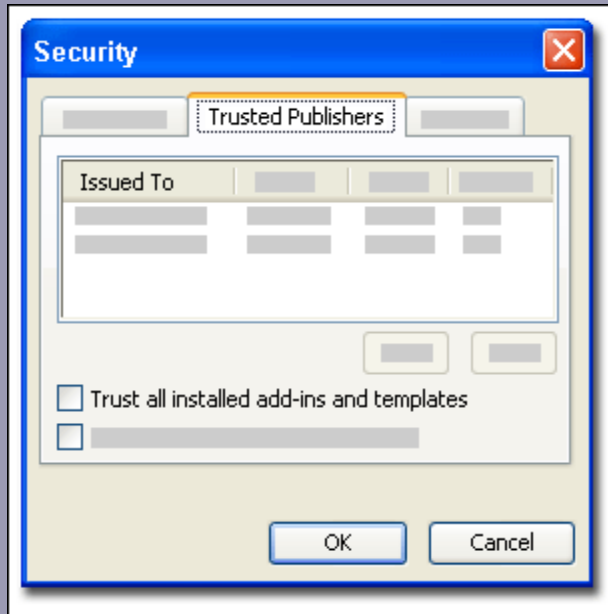


Macro security levels dialog box

To set macro security levels in Word, Excel, and PowerPoint:

1. Click the **Macro Security** button on the **Security** tab of the **Options** dialog box.
2. Click the security level you want.

Reduce your computer's vulnerability

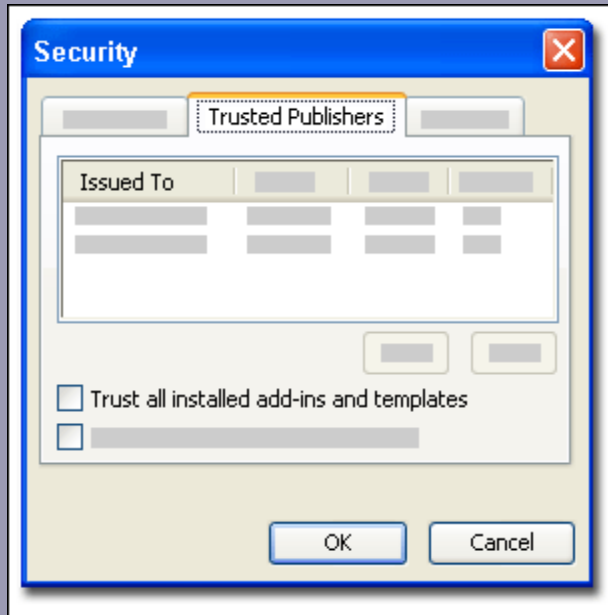


Clear the check box for **Trust all installed add-ins and templates**.

At the beginning of this lesson, we mentioned the feature called **Trust all installed add-ins and templates**.

There is a check box for this feature that is selected *by default* in the **Trusted Publishers** list in the **Security** dialog box.

Reduce your computer's vulnerability

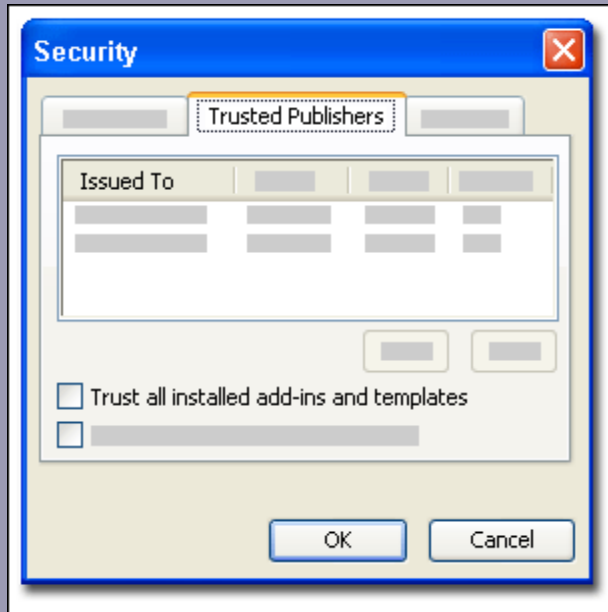


Clear the check box for **Trust all installed add-ins and templates**.

The macro security levels described in the previous slides interact with this feature.

For example, even if your macro security level is set to Very High, when the **Trust all installed add-ins and templates** check box is selected, all installed add-ins will be trusted.

Reduce your computer's vulnerability



Clear the check box for **Trust all installed add-ins and templates**.

What does this mean to you? To reduce your computer's vulnerability to malicious macros, you should *clear* the **Trust all installed add-ins and templates** check box.

Otherwise, macros and add-ins in the folders mentioned previously will run without prompting you to confirm this action.

Suggestions for practice

1. Review a digital certificate.
2. Check macro security levels.
3. Clear the Trust all installed add-ins and templates check box.

[Online practice](#) (requires Word 2003)

Test 3, question 1

Which of these macro security levels should you use as your default setting? (Pick one answer.)

1. Low.
2. Medium.
3. High.
4. What's a macro security level?

Test 3, question 1: Answer

High.

This setting allows only signed macros from trusted sources to run. It prevents any unsigned macros from running.

Test 3, question 2

What is a trusted publisher? (Pick one answer.)

1. Someone who Microsoft trusts to write macros.
2. Someone whom you decide is trustworthy after examining his or her digital certificate credentials.
3. Someone who has a digital certificate.
4. Microsoft.

Test 3, question 2: Answer

Someone whom you decide is trustworthy after examining his or her digital certificate credentials.

You can choose whom to trust after examining the available facts.

Test 3, question 3

For optimum security, you should clear the Trust all add-ins and templates check box. (Pick one answer.)

1. True.
2. False.

Test 3, question 3: Answer

True.

You should clear the check box and set your macro security level to **High** to help protect your computer.

Quick Reference Card

For a summary of the tasks covered in this course, view the [Quick Reference Card](#).