

Welcome to the Internet SIG

September 6, 2000

Protecting your computer from unsafe software

When you download or run programs from the Internet, you want to know that the program comes from a known, reliable source. That's why, when you choose to download a program from the Internet to your computer, Internet Explorer uses Microsoft Authenticode technology to verify the identity of the program. Authenticode technology verifies that the program has a valid certificate: that the identity of the software publisher matches the certificate, and that the certificate is still valid. Note that this does not prevent a poorly written program from being downloaded or run on your computer, but it does reduce the chance of someone misrepresenting a program that is intended to be malicious or intentionally harmful.

You can specify different settings for how Internet Explorer handles downloading programs and files, depending on the zone it is coming from.

For example, you might be confident that anything you download within your corporate intranet is safe. So, you might set your security settings for your Local intranet zone to a low level to allow downloading with little or no prompting. If the source is in the Internet zone or the Restricted sites zone, you may want your security levels set to Medium or High. Then, you'd be prompted with information about the program's certificate before it is downloaded, or you may not be able to download it all.

To set a security level for each zone

1. On the **Tools** menu in Internet Explorer, click **Internet Options**.
2. Click the **Security** tab.
3. Click the zone that you want to set the security level for.
4. Move the slider up for a higher level of security or down for a lower level of security.

Tip

- To specify custom security settings for the selected zone, click the **Customize Level** button. To set the options for a particular security level back to their original settings, click the **Default Level** button.

What you need to know about security zones

Internet Explorer divides your Internet world into zones, so that you can assign a Web site to a zone with a suitable security level.

You can tell which zone the current Web page is in by looking at the right side of the Internet Explorer status bar. Whenever you attempt to open or download content from the Web, Internet Explorer checks the security settings for that Web site's zone.

There are four different zones:

- **Internet** zone: By default, this zone contains anything that is not on your computer or an intranet, or assigned to any other zone. The default security level for the Internet zone is Medium.
- **Local intranet** zone: This zone typically contains any addresses that don't require a proxy server, as defined by the system administrator. These include sites specified on the **Connections** tab, network paths (such as \\server\share), and local intranet sites (typically addresses that don't contain periods, such as http://internal). You can also add sites to this zone. The default security level for the Local intranet zone is Medium.
- **Trusted sites** zone: This zone contains sites you trust - sites that you believe you can download or run files from without worrying about damage to your computer or data. You can assign sites to this zone. The default security level for the Trusted sites zone is Low.
- **Restricted sites** zone: This zone contains sites you don't trust - that is, sites that you're not sure whether you can download or run files from without damage to your computer or data. You can assign sites to this zone. The default security level for the Restricted sites zone is High.

In addition, any files already on your local computer are assumed to be very safe, so minimal security settings are assigned to them. You cannot assign a folder or drive on your computer to a security zone.

If you want, you can change the security level for a zone; for example, you might want to change the security setting for your Local intranet zone to Low. Or, you can customize the settings within a zone from the default settings in Low, Medium Low, Medium, and High.

To assign a Web site to a security zone

1. On the **Tools** menu in Internet Explorer, click **Internet Options**.
2. Click the **Security** tab.
3. Click a security zone: **Local intranet** zone, **Trusted sites** zone, or **Restricted sites** zone.
4. Click **Sites**, and then type the Internet address for the Web site that you want to add to this zone.

Note

- You cannot add Web sites to the Internet zone, which includes everything that does not belong to any other zone and is not on your local computer.

Protecting your identity over the Internet

You can use a personal certificate to protect your identity over the Internet. A certificate is a statement guaranteeing the identity of a person or the security of a Web site. You can control the use of your own identity by having the private key that only you know on your own system. When used with mail programs, security certificates with private keys are also known as "digital IDs."

Internet Explorer uses two different types of certificates:

- A "personal certificate" is a kind of guarantee that you are who you say you are. This information is used when you send personal information over the Internet to a Web site that requires a certificate verifying your identity.
- A "Web site certificate" states that a specific Web site is secure and genuine. It ensures that no other Web site can assume the identity of the original secure site.

How do security certificates work?

A security certificate, whether it is a personal certificate or a Web site certificate, associates an identity with a "public key." Only the owner knows the corresponding "private key" that allows the owner to "decrypt" or make a "digital signature." When you send your certificate to other people, you are actually giving them your public key, so they can send you encrypted information which only you can decrypt and read with your private key.

The digital signature component of a security certificate is your electronic identity card. The digital signature tells the recipient that the information actually came from you and has not been forged or tampered with.

Before you can start sending encrypted or digitally signed information, you must obtain a certificate and set up Internet Explorer to use it. When you visit a secure Web site (one that starts with "https"), the site automatically sends you their certificate.

Where do you get your own secure certificates?

Security certificates are issued by independent certification authorities. There are different classes of security certificates, each one providing a different level of credibility. You can obtain your personal security certificate from certification authorities.

Digital Signature Trust Co.
Global Sign
Verisign

To view security certificates

1. On the **Tools** menu in Internet Explorer, click **Internet Options**.
2. Click the **Content** tab.
3. In the **Certificates** area, click the **Certificates** or **Publishers** buttons to view the list of current certificates that you trust.

[Link to Symantec Antivirus Research Center Definitions](#)

<http://www.sarc.com/avcenter/reference/wormsvsvirus.pdf>

According to Symantec the difference between a virus and a worm is that a virus will infect files and programs on a single computer but will not intentionally try to infect another computer.

A worm, on the other hand, once activated on your system will execute with the intention of spreading itself to other computers on a network (e.g. via email).

Melissa and I Love You were very damaging from that perspective. I Love you even more so because if you were reading your email as HTML the scripting executed automatically as soon as you opened it. It used something known as Active X scripts written into the HTML code of the mail. This obviously caused a great deal of difficulty for many people including Microsoft, who by the way, has closed the security hole in Outlook, Outlook Express and Internet Explorer that allowed that to happen.

For a Glossary of Terms from Symantec see

<http://www.symantec.com/avcenter/refa.html>

Here are a few...

Bug

A programming error in a software program which can have unwanted side effects. Examples: Various web browser security problems, Y2K software problems.

Category: Hoax

Usually an email that gets mailed in chain letter fashion describing some devastating highly unlikely type of virus, you can usually spot a hoax because there's no file attachment, no reference to a third party who can validate the claim and the general 'tone' of the message.

Category: Joke

A harmless program that causes various benign activities to display on your computer (e.g., an unexpected screen-saver).

Category: Trojan horse

A program that neither replicates or copies itself, but does damage or compromises the security of the computer. Typically it relies on someone emailing it to you, it does not email itself, and it may arrive in the form of a joke program or software of some sort.

Category: Virus

A program or code that replicates, that is infects another program, boot sector, partition sector or document that supports macros by inserting itself or attaching itself to that medium. Most viruses just replicate, a lot also do damage.

Category: Worm

A program that makes copies of itself, for example from one disk drive to another, or by copying itself using email or some other transport mechanism. It may do damage and compromise the security of the computer. It may arrive in the form of a joke program or software of some sort.



Protection

Norton Internet Security 2000 Products consists of three programs:

Norton Personal Firewall 2000

Norton Internet Security 2000

Norton Internet Security 2000 Family Edition

			
Personal Firewall	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Privacy Control	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
AntiVirus		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Ad Blocking		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Parental Control			<input checked="" type="checkbox"/>
Configure Internet access for each user			<input checked="" type="checkbox"/>

View Details about these products at

<http://www.symantec.com/sabu/nis/>

Dr. Solomon and McAfee Products

[VirusScan](#)

[VirusScan Deluxe](#)

[Internet Guard Dog](#)

[Internet Guard Dog Pro](#)

[McAfee Firewall](#)

[McAfee Office 2000](#)

[McAfee Office 2000 Pro](#)

[Dr Solomon's Anti-Virus](#)

[Dr Solomon's Virex for Macintosh](#)

[McAfee Utilities](#)

[McAfee Utilities Deluxe](#)

[PGP Desktop Security](#)

[PGP Personal Privacy](#)