Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at http://www.giac.org/registration/gsec

Microsoft Internet Explorer 6.0 Security: Step-by-Step

Chris Christianson
February 11, 2002
Version 1.3

Introduction

Are you concerned about your security while you surf the Internet? If not, you should be. Every time you connect to the Internet, your computer is constantly sending and receiving information with other computers. How secure is the communication between all these computers? Well, it all depends on the sites you visit; and your Web browser's security features.
Microsoft Internet Explorer version 6.0 is a state of the art Web browser that contains the latest technology available on the market. Internet Explorer has numerous configurable security settings that can be used to help protect yourself from malicious code, offensive content, and possible invasions of your privacy while you surf. However, to make the product easier to use, by default, many of these security settings are disabled or set to very low settings. Unfortunately, most people don't take enough time to figure out what these security settings do or how to set them. Thus they leave themselves exposed to a number of vulnerabilities while they surf.
The purpose of this paper is explain the various security features of Internet Explorer 6, where to locate them and how to set them to make surfing the web safer and more secure. It is assumed that the reader has a basic understanding of the Internet and the common terminology used when discussing surfing the web. If you are unfamiliar with any of the terms is this document go to the NetLingo Dictionary of Internet Words at www.netlingo.com.

Overview of Internet Explorer Security Features

As was mentioned before, Internet Explorer has a number of security features, that if set correctly can make surfing the web much safer and more secure. Some of the more prominent security features include: Security Zones that allow you to customize the different levels of security for the different areas you surf, Content Advisor which allow you to block web sites that contain inappropriate material, and Privacy Settings which allow you to control the way Cookies are handled. There are also many other features such as Authenticode, support for Digital Certificates, 128-bit encryption, and more. Combined together these various technologies provide a good measure of protection from many of the common threats facing you while on the Internet.

Before You Begin

Accessing Your Security Needs

Before you begin to configure Internet Explorer you need to know what your security needs are. What web sites do you regularly surf, what features do they require? Do they require Active X controls, Cookies, or use Java Applets? You need to know what features web sites require so you can configure your browser. And, not just so you can configure your browser, but so you can protect yourself. You *need* to know what they are doing and why they are doing it. Would you allow just anybody to have the keys to your car? No, because eventually somebody is going to drive off with it; and the same applies here. If you allow just any Web site to execute whatever applet they want, sooner or later you're going to get taken advantage of.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Most of the sites you probably surf on a day to day basis may not require that you have all of these features enabled. On the other hand, some sites such as your financial institution and shopping sites will. Make a list of the web sites you surf that require any of the following: Active X controls, Java, Scripting, or Cookies. Then you can add these sites to the proper location and set them up correctly when configuring your Security Zones and Privacy Settings.

Patches

The first and most important thing you can do to protect yourself from security vulnerabilities is to update your browser with all the current patches and updates. Usually as soon as an exploit has become known, a patch is immediately released to fix the problem. It's a never-ending process, and there are always new patches and updates that will need to be applied. These patches can be obtained a variety of ways. Windows Update works well for most people; but sometimes it may take a while for security patches to appear. If you'd like to be kept abreast of all the latest and be notified immediately of any Security Flaws and vulnerabilities, go to Microsoft's Security Web Site at www.microsoft.com/security, and register to automatically receive bulletins. You'll be sent e-mails as soon as security vulnerabilities become known and patches become available. These bulletins are very informative and explain problems in detail, as well as provide links to patches that you can download to correct them.

Step 1-Configuring Security Settings

Internet Explorer includes four configurable zones: Internet, Local Intranet, Trusted Sites, and Restricted Sites. You can set the security settings that you want for each zone, and then add or remove Web sites from these zones, depending on your level of trust in a Web site. The following is a brief description of each of the zones.

- **Internet**—this zone contains all Web sites you haven't placed in other zones. The default level for this zone is set to Medium.
- **Local Intranet—**this zone contains all Web sites that are on your organization's intranet. The default level for this zone is Medium-low.
- **Trusted Sites—**this zone contains Web sites that you trust not to damage your computer or data. By default this zone is set to Low.
- **Restricted Sites**—this zone contains Web sites that could potentially damage your computer or data and contains Web sites that you do not trust. When you add a Web site to the Restricted Sites zone, you believe that files you download or run from the Web site may damage your computer or data. By default, there are no Web sites assigned to the Restricted Sites zone, and the security level is set to High.

But, as was mentioned before these default settings don't provide an adequate level of protection. Let's take a look at each of these security settings, briefly explain their purpose, and then make some recommendations so that you can set them appropriately.

All settings in this section may be accessed by opening Internet Explorer, clicking the Tools menu, selecting Internet Options, and then clicking the Security tab. Once at the Security Zones, select the appropriate security zone, and then click Custom Level.

To add a site to a zone from the Security tab, select the zone to which you would like to add the Web site to, click the Sites button, then type the Web address of the site you would to add in the box, and then click the Add button.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

To add a site to the Intranet Zone, you must click the Advanced button before you type the Web address in the box.

Note: To add a non-secure (HTTP) site to the Trusted sites zone uncheck Require server verification (https:) for all sites in this zone.

Note: Instead of typing the full Web site address for each site, try using the following shortcut https://*.domainname.com. The '*' is a wildcard character. Now you do not have to enter all the different host names, if there is more than one, for that site.

Note: These are only recommendations and may not be suitable for all systems. Always follow your company's security policy and be sure that the changes you make are appropriate for your environment.

ACTIVEX CONTROLS AND PLUG-INS

Download signed ActiveX controls

The first Security Zone setting allows the downloading of signed ActiveX controls to be handled in one of three ways. They can either be disabled all together, happen automatically, or prompt you for action. As with all settings, this affects all web pages on sites within the zone. Signed controls are programs that contain a valid digital signatures, this means that Internet Explorer can identify who wrote the program and if it's been tampered with. If ActiveX controls are downloaded there is always the potential that a malicious program may be downloaded and installed on your computer.

To stop this from happening 'Disable' the downloading of Signed ActiveX controls in the Internet zone, Intranet, and 'Prompt' for the Intranet zone and Trusted sites zone only if required in your environment. Never 'Enable' the downloading of ActiveX controls to happen automatically.

Download unsigned ActiveX controls

This setting is the same as the previous setting except that it allows the downloading of unsigned ActiveX controls. These are programs that don't have a valid digital signature, and that Internet Explorer can't identify who wrote the program or check to see if it's been tampered with, making them even more dangerous than signed ActiveX controls.

'Disable' the downloading of Unsigned ActiveX controls in the Internet zone and the Restricted sites zone, and 'Prompt' for the Intranet zone and Trusted sites zone only if required in your environment. Again, never 'Enable' the downloading of ActiveX controls to happen automatically.

Initialize and script ActiveX controls not marked as safe

This setting allows scripts embedded in web pages on sites within zone to interact with ActiveX controls not marked as safe. Unsafe controls are controls that have not been specifically designed

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

to interact with scripts. If allowed there is the potential that a malicious script that interacts with an ActiveX control could be run on your computer.

'Disable' the initializing and scripting of ActiveX controls not marked as safe in the Internet zone and the Restricted sites zone, and 'Prompt' for the Intranet zone and Trusted sites zone only if required in your environment. Never 'Enable' this setting.

Run ActiveX controls and plug-ins

This setting allows Internet Explorer to automatically run ActiveX programs on web pages on sites within the zone. If ActiveX controls are allowed to run on your computer, it is possible that a malicious program could be instructed to be run.

'Prompt' for the running of ActiveX programs in the Internet zone, and the Intranet zone. 'Enable' only the Trusted sites zone if required, and 'Disable' in the Restricted sites zone.

Note: If you don't need to run ActiveX programs in your environment, "Disable" it.

Script ActiveX controls marked safe for scripting

This setting allows scripts embedded in web pages on sites within the zone to interact with ActiveX controls marked as safe. Safe controls are ActiveX programs that are specifically designed to interact with scripts. This does not mean that the program is safe; only that the program can safely interact with script. If allowed, a malicious script that interacts with an ActiveX control could be run on your computer.

'Prompt' for the Internet zone, and the Intranet zone. 'Enable' only the Trusted sites zone if required, and 'Disable' in the Restricted sites zone.

DOWNLOADS

File download

This is a self-explanatory setting that allows you to download files. It is possible that these files could contain malicious code. Make sure that you have Anti-Virus software installed and that your virus definitions are up to date.

'Disable' for Internet zone and Restricted sites zone, and 'Enable' for the Intranet zone and Trusted sites zone.

Font download

Another self-explanatory setting, it allows fonts to download. It is sometimes needed for a web page to display correctly, if you don't have the font installed on you computer that a particular page uses.

'Prompt' for Internet zone and the Intranet zone, 'Enable' for the Trusted sites zone, and 'Disable' for Restricted sites zone.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

MICROSOFT VM

Java permissions

This setting allows Java Applets to run outside of the protected area called a sandbox. This allows them to perform high level functions such as accessing the file system and other system resources. They are HTML-based programs built with Java and usually integrated into web pages and run by a browser whenever that page is opened. As with ActiveX controls, if Java Applets are allowed to run on your computer there is possibility that a malicious program could instructed to be run.

If you need to run Java Applets, set Java permissions to 'High safety' for the Internet zone and Intranet zone. Set the Trusted sites zone to 'Medium' safety, and 'Disable' Java for the Restricted sites zone.

Note: If you don't need to run Java Applets in your environment 'Disable' it.

MISCELLANEOUS

Access data sources across domains

This setting allows Internet Explorer to access pages that receive data from multiple sources in different domains. If allowed you may get data from sites that you do not necessarily trust.

Set this to 'Disable' for the Internet zone and the Restricted sites zone. 'Prompt' to be asked before it occurs for the Intranet zone. 'Enable' this setting for the Trusted sites zone.

Allow META REFRESH

The Meta Refresh setting allows you to be redirected from one web page to another after a certain amount of time. If allowed you may get redirected to a web page that you don't want to go to, possibly one that has a malicious program.

The problem with this setting is it is often used legitimately on many web pages to redirect to you to the newest version of that page. If 'Disabled', you may not be able to get to the new web page. Set Allow META REFRESH to 'Disable' for the Internet zone, Intranet zone, and the Restricted sites zone. 'Enable' for the Trusted sites zone. If you constantly need to be redirected and it's becoming a nuisance, you may need to 'Enable' this setting, but be aware of the risk.

Display mixed content

This setting allows you to view a web page that contains both secure (HTTPS) and non-secure (HTTP) content. If allowed it is possible that you could send confidential data over a connection that you believe to be secure, but in reality is not.

This setting may be confusing. If set to 'Prompt' then a warning message is displayed asking if you want to display both secure and non-secure items. If you 'Enable' it then you don't receive any warning message and non-secure content *can* be received, and when you 'Disable' it then you don't receive any warning message and non-secure content *cannot* be received.

© SANS Institute 2000 - 2002 Author retains full rights.

Many web sites do display mixed content, so you probably need the ability to display it, but don't 'Enable' it. Instead, 'Prompt' for the Internet zone and the Intranet zone, 'Enable' for the Trusted sites zone, and 'Disable' for the Restricted sites zone. You'll receive that annoying message a little more often than you'd probably like, but that's better than sending confidential information, like a credit card number, over a non-secure connection.

Don't prompt for client certificate selection when no certificates or only one certificate exits

This setting determines whether or not you are prompted to select a certificate when you don't have a trusted certificate or only one trusted certificate has been installed on the computer.

'Disable' this setting to be prompted for a certificate for the Internet zone and the Restricted sites zone, and 'Enable' this for the Intranet and Trusted sites zone, so that you are not prompted for a certificate for sites within those zones.

Drag and drop or copy and paste files

This setting controls whether you can drag and drop or copy and paste files from a web site to your computer. If you are dragging and dropping or copying and pasting files to your computer, there is the possibility that the file could contain malicious code. Again, make sure that you have Anti-Virus software installed and that your virus definitions are up to date.

For maximum protection only 'Enable' this option for the Intranet zone and the Trusted sites zone, 'Disable' it for the Internet zone and Restricted sites zone.

Installation of desktop items

This setting controls whether or not users are allowed to install desktop objects from a Web page. These desktop items could be an ActiveX control, which means that they could contain malicious code.

'Enable' this option for the Trusted sites zone and 'Prompt' for Intranet sites zone. But, if you work in a corporate environment and you don't want users to make changes to their desktops you'll probably want to 'Disable'. 'Disable' it for the Internet zone and the Restricted sites zone. If you don't ever need to install desktop items, then 'Disable' this setting for all zones.

Launching programs and files in an IFRAME

This setting controls whether or not you can download files or run applications from an IFRAME element on a web page if that IFRAME element contains directory or folder references. This setting was in response to a security vulnerability that allowed a malicious web page to read files on your computer, which has since been corrected. If you'd like to read more about this vulnerability read the Microsoft IE5 IFRAME Vulnerability from SecurityFocus at http://online.securityfocus.com/bid/696.

'Enable' this setting for the Trusted sites zone, 'Prompt' for the Intranet sites zone, and 'Disable' it for the Internet zone and the Restricted sites zone.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Navigate sub-frames across different domains

Navigating sub-frames across different domains allows Internet Explorer to display sub-frames that originated from different domains. There is a vulnerability that allows a malicious web page to open another browser, another site's main frame, and then set any sub-frames to any web site they want. To learn more read the SecurityFocus document on Internet Explorer Subframe Spoofing Vulnerability at http://online.securityfocus.com/bid/855.

'Enable' this setting for the Trusted sites zone, 'Prompt' for the Intranet zone, and 'Disable' for the Internet zone and the Restricted sites zone. If you require this feature for the Internet sites zone then you should probably set it to 'Prompt' you rather than 'Enable.'

Software channel permissions

This setting allows the automatic installation of software updates from web channels within the zone. A software channel is a subscription based service that allows web sites to automatically notify users of software updates and also deliver and install the updates on their computers. If allowed there is the potential that a malicious program may be downloaded and installed on your computer.

'High' safety on the Internet zone and the Restricted sites zone. 'Medium' safety on the Intranet zone and the Trusted sites zone, if required.

Submit nonencrypted form data

This setting allows Internet Explorer to submit non-encrypted form data on sites within the zone. Confidential information may be intercepted by packet sniffing.

Set Submit non-encrypted form data to 'Prompt' for the Internet zone and the Intranet zone, and 'Enable' it for the Trusted sites zone. Of course, 'Disable' this setting for the Restricted sites zone.

Userdata persistence

This setting allows web sites to save a small file to your computer that helps the site remember personal information about you. If you value your privacy, you'll probably want to 'Disable' this setting.

'Disable' this setting for the Internet zone and the restricted sites zone, and 'Enable' it for the Intranet zone the Trusted sites zone.

SCRIPTING

Active scripting

This setting allows the execution of Active scripts, programs written in ActiveX, JavaScript, or VBScript. Allowing these scripts, by default, to automatically execute is one of biggest vulnerabilities in Internet Explorer. There is the potential that a malicious program may be executed on your computer. Nimda used Active scripts, to infect people while they were surfing the web.

© SANS Institute 2000 - 2002, Author retains full rights.

'Disable' active scripting for the Internet zone and Restricted sites zone, 'Prompt' for the Intranet zone, and 'Enable' it for the Trusted sites zone.

Note: Even though you can 'Disable' this setting, there is still a flaw in the Internet Explorer that will still allow a script to execute. You can read the SecurityFocus article about it at Microsoft Internet Explorer Forced Script Execution Vulnerability at http://online.securityfocus.com/bid/4082.

Allow paste operations via script

This setting controls whether or not scripts are allowed to copy (or cut) and paste information using the clipboard. A malicious script on a web site could access your clipboard's contents and then forward it to another site. If you'd like to learn more read Microsoft Internet Explorer Clipboard Reading Vulnerability from SecurityFocus at http://online.securityfocus.com/bid/3862.

'Disable' this setting for the Internet zone and Restricted sites zone. 'Prompt' for the Intranet zone, and 'Enable' for the Trusted sites zone.

Scripting of Java applets

This setting allows scripts to be embedded in web pages on sites in the zone to access Java Applets. Java Applets are HTML based programs built with the Java programming language that can be integrated into a web page and run by the browser when the page is opened. If scripting of Java applets is allowed, it is possible that a malicious program could be instructed to be run.

Set this to 'Prompt' for the Internet zone and Intranet zone only if required to do so in your environment, otherwise 'Disable' it. 'Enable' this setting for the Trusted sites zone, and 'Disable' it for the Restricted sites zone.

USER AUTHENTICATION

Logon

This setting controls how you authenticate to Web sites. The following are the four possible choices for this setting:
Anonymous Logon—Internet Explorer will disable authentication and use the Guest account of the Web server you are visiting for access to the site's resources.
Automatic Logon Only In Intranet Zone—This option allows you to automatically logon to Web sites that are in the Intranet zone that you have setup. You will be prompted for a username and password for all other sites.
Automatic Logon With Current Username And Password—This option automatically logs you on with your current username and password, however, it only works if the Web server you are connecting to supports NT Challenge/Response. If not, you'll be prompted for your username and password.
Prompt For Username and Password—This option, of course, prompts you for your username and password.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Select 'Prompt For Username and Password' for the Internet Zone, 'Automatic Logon Only In Intranet Zone' for the Intranet zone, 'Automatic Login With Current Username And Password' for the Trusted Sites zone, and 'Anonymous Logon' for the Restricted sites zone.

Step 2-Configuring Privacy Settings

One of the new and most exciting features of Internet Explorer 6.0 is the ability to configure the way it handles cookies. Today, cookies are a concern for those worried about their privacy. What are cookies? They are files that are stored on your computer by a web site, which contain all sorts of information about you including your identity and preferences. There are also a couple of different of types of cookies:

First-party Cookies—First-part cookies are cookies that originate on or are sent to the Web site you are currently viewing.

Third-party Cookies—Are cookies that either originate on or are sent to a different Web site other than the one you are currently viewing. These are often used to track where you surf for advertising purposes. Web sites may be able to collect personally identifiable information about you, which could be used for ulterior purposes without your consent.

Note: It is important that you understand the difference between first-party and third party cookies, so that you can configure your browser correctly.

Privacy Settings can be configured by opening Internet Explorer, click the Tools menu, then the Privacy tab, and sliding the Settings slider bar to the appropriate setting.

Set your Privacy settings to 'Medium High', or higher if possible.

Overriding cookie handling for individual Web sites

Disabling cookies may prevent you from being able to access certain Web sites or affect their functionality, because they require that you have cookies enabled. If this is the case, you can make exceptions to your default privacy settings by adding those sites to this section.

To override your cookie handling settings click the Edit button, type the URL of the Web site in the Address of Web Site box, and then click either the Allow button or the Disallow button to allow or disallow cookies to that particular web site.

To edit the settings of an existing Web site you must remove that site from the list. To remove a site from the list, select the site to remove and then click the Remove button.

Note: As you're surfing, if Internet Explorer blocks a cookie from the web site you're currently visiting it will display an icon with an eye and minus sign on the status bar. Click the icon to display a Privacy Report for the site to see what cookies are currently being blocked or to override the settings.

To learn more about privacy settings read Microsoft's article on Configuring Privacy Options at http://www.microsoft.com/windows/ie/using/howto/privacy/config.asp.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Step 3-Content Settings

Content Advisor

Content Advisor can be used to control access to Web sites, and the type of content that can be viewed. This can be done by using content rating systems, or by specifying the Web sites yourself. Administration of content-rating systems is done by independent organizations. Internet Explorer defaults to the ratings from the Internet Content Ratings Association.

To enable the Content Advisor, open Internet Explorer, click the Tools menu, then Internet Options. In Internet Options click the Content tab, and then in the Content Advisor section click the Enable button.

Note: For the content rating to work, the Web page must be rated by the author. Web pages with no rating, by default, will be blocked. You can change this setting so that pages with no rating are allowed, and also create a password that allows you to view restricted content. The Approved Sites feature can also be helpful in this situation.

To enable Ratings from the Content Advisor section of the Content tab, click the Settings button, then the Ratings tab, select the category, and adjust the slider bar to the level you desire. Repeat for each category.

To specify access to certain Web sites from the Content Advisor section of the Content tab, click the Approved Sites tab, type the URL of the site, and then the Always button to allow the site or the Never button to block it.

To edit the settings of an existing Web site you must remove that site from the list. To remove a site from the list, select the site to remove and then click the Remove button.

To learn more about Content Advisor read Microsoft's How To: Use the Internet Explorer 6 Content Adviser to Control Access to Web Sites in Internet Explorer (Q310401) at http://support.microsoft.com/search/preview.aspx?scid=/search/viewDoc.aspx?docID=KC.Q310401%26url=kb;en-us;Q310401%26dialogID=10712972%26iterationID=1%26sessionID=anonymous|9681218.

PERSONAL INFORMATION

Autocomplete

The only other setting in this section that may be a security concern is that of AutoComplete. AutoComplete stores pervious entries that you've made for Web addresses, Forms, Usernames and Passwords; and then automatically enters them for you the next time you are asked for them. As time saving as this feature is, having this type of information automatically entered for you is never a good idea. If someone else were to gain access to your computer, then they too could automatically logon as you. This should be a serious concern to you, if you share a computer and don't have different profiles.

© SANS Institute 2000 - 2002, Author retains full rights.

To disable Autocomplete open Internet Explorer, click the Tools menu, then Internet Options. In Internet Options click the Content tab, and then in the Personal Information section click the AutoComplete button. Uncheck the boxes for Web addresses, Forms, Usernames and Passwords, and Prompt me to Save Passwords.

If you would like to clear all the existing information that has been stored by Autocomplete click the Clear Forms button and Clear Passwords button.

Step 4-Advanced Settings

All settings in the Advanced Settings section may be accessed by opening Internet Explorer, clicking the Tools menu, selecting Internet Options, clicking the Advanced tab, and scrolling down to the Security section.

Note: These settings are usually enabled by checking the box next to the appropriate setting, and disabled by un-checking it. Be sure to read carefully.

Check for publisher's certificate revocation

This option enables Internet Explorer to check to see if the Software Publisher's Certificate has been revoked. Certificates are revoked when they have been compromised or are no longer valid. It is important that you enable this option, so that you don't submit confidential data to a site that may be fraudulent and/or not secure.

Enable the 'Check for publisher's certificate revocation'

Check for server certificate revocation (requires restart)

Similar to the previous setting, except that, this option will enable Internet Explorer to check if the server's certificate has been revoked.

Enable the 'Check for server certificate revocation (requires restart)' option.

Check for signatures on downloaded programs

Internet Explorer does not check for digital signatures before downloading executable programs. A digital signature identifies the publisher of signed software and verifies that it hasn't been modified or tampered with. Otherwise, potentially malicious or virus-infected programs may be downloaded onto the computer.

Enable the 'Check for signatures on downloaded programs' option.

Do not save encrypted pages to disk

This option will prevent Internet Explorer from saving encrypted pages that contain secure (HTTPS) information such as such as passwords and credit card numbers to disk, which may be insecure.

Enable the 'Do not save encrypted pages to disk' option.

© SANS Institute 2000 - 2002, Author retains full rights.

Empty Temporary Internet Files folder when browser is closed

Enable this setting to have Internet Explorer delete the contents of your Temporary Internet Files folder, when you close all Internet Explorer windows. This is especially important if you share your computer with someone else, and as an added bonus it also saves space.

Enable the 'Empty Temporary Internet Files folder when browser is closed' option.

Note: Even though this option does empty your Temporary Internet Files folder, that information is still recoverable by a determined individual. If you need a higher level of security than this you can use any number of other third-party programs to securely delete these files.

Enable Integrated Windows Authentication (requires restart)

Enable Integrated Windows Authentication allows you to Negotiate/Kerberos authentication, when enabled.

Enable the 'Enable Integrated Windows Authentication (requires restart)' option.

Enable Profile Assistant

Profile Assistant stores your registration and demographic information, and then Internet Explorer automatically sends this information to Web sites that require it. This saves you from having to type the same information over again. Even though you will be prompted before sharing this information, it could be of a concern if you're worried about your privacy. You must have a profile in order for this option to work.

Disable the 'Enable Profile Assistant' option.

If you'd like more information about Profile Assistant read Microsoft's article Description of Profile Assistant (Q220017) at
http://support.microsoft.com/search/preview.aspx?scid=/search/viewDoc.aspx?docID=KC.Q220017%26url=kb;en-us;Q220017%26dialogID=10715978%26iterationID=1%26sessionID=anonymous|9688344

Use SSL 2.0

SSL is a protocol that authenticates, encrypts, and ensures the integrity of your communications over the Internet. SSL 2.0 is an older version of the protocol that has some known vulnerabilities, and should not be used if at all possible.

Disable the 'Use SSL 2.0' option.

Note: If you have trouble communicating with some secure sites, you may have to enable this option.

Use SSL 3.0

This option enables the most current version, of the SSL protocol to secure your communications.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Enable the 'Use SSL 3.0' option.

Use TLS 1.0

Transport Layer Security (TLS) 1.0 is another protocol that provides authentication, encryption, and integrity of your communications over the Internet.

Enable the 'Use TLS 1.0' option.

Warn about invalid site certificates

Internet Explorer will issue a warning when viewing data from a web site whose security certificate does not match its Internet address. Certificates help verify if a Web site is safe, so if a certificate does not match the site's address, or it has expired, then the site should not be trusted.

Enable the 'Warn about invalid site certificates' option.

Warn if changing between secure and non-secure mode

This option displays a warning when switching between secure (HTTPS) and non-secure sites (HTTP). It is important to enable this option, to help prevent you from mistakenly sending confidential information like your password or credit card number information over a non-secure connection.

Enable the 'Warn if changing between secure and not secure mode' option.

Warn if forms submittal is being redirected

Warn if forms submittal is being redirected will issue a warning when information submitted from a form is sent to an address different from the one hosting the form. This option helps ensure that you don't send confidential information in a non-secure connection.

Enable the 'Warn if forms submittal is being redirected' option.

Internet Explorer In The Enterprise

If you're using Internet Explorer in the Enterprise, when configuring these settings you need to keep your entire company's security needs in mind. After going through and configuring Internet Explorer to the appropriate settings according to your company's Security Policy (If your company doesn't have a Security Policy, get one) you can use the Microsoft Internet Explorer Administration Kit to deploy your customized Internet Explorer throughout your enterprise.

For more information on go to Microsoft's Internet Explorer Administrator Kit Home Page at http://www.microsoft.com/windows/ieak/default.asp.

Other

While going through these various settings of Internet Explorer and setting them to more secure settings greatly increases security, it isn't enough. There are many other things you should do to protect yourself online. The following programs, many which are free, can help in this regard and will provide a well rounded secure environment.

© SANS Institute 2000 - 2002, Author retains full rights.

If you haven't purchased and installed the latest version of an anti-virus program such as McAfee Anti-Virus or Norton Anti-Virus, do so. If you don't want to spend the money you can even download AVG AntiVirus from GRISOFT for free at www.grisoft.com. Again, make sure that you keep your virus definitions up to date. It makes no sense to have, if you don't.
Another way to increase your safety while on the web is to use one of the many Personal Firewall programs available such as BlackIce Defender, Norton's Personal Firewall, or ZoneAlarm. They allow you to control what computers and services are accessing your computer from the Internet.
If after configuring Internet Explorer you're still concerned about your privacy there are some additional products such as Annonymizer from anonymizer.com and Freedom Security & Privacy Suite from Zero Knowledge Systems that allow you to surf the web anonymously. These programs prevent Web sites from tracking you, hide your IP Address from the Internet, and even remove possible threats to your privacy from the Web pages you visit.
Programs such as SurfSecret by SurfSecret, Windows Washer by Webroot, and ZDelete by Lsoft cover your tracks by cleaning (and I mean cleaning) your browser history, cache, cookies, image files, you name it.
A couple of other little free utilities that don't have a lot to do with security, but that are still very useful, are programs such as Ad-Aware and Pop-Up Stopper. Ad-Aware and programs like it will scan your computer for spyware programs, alert you to their presence, and delete them for you. Pop-Up Stopper is a handy utility that prevents Web pages from opening another browser window, which can sometimes be very annoying.

Conclusion

Internet Explorer 6.0 has security features, that if set correctly can make surfing the web much safer and more secure. There are Security Zones, Content Advisor, Privacy Settings, and many other features that when combined together provide a good measure of protection from many common threats facing you while on the Internet. These when used in conjunction with other security products such as an anti-virus program and a personal firewall can provide a good well rounded secure environment.
After configuring these settings you can use the Internet Explorer Administration Kit to distribute your customized settings throughout your enterprise.
Again, these settings are only recommendations and may not be suitable for all systems. Always follow your company's security policy and be sure that the changes you make are appropriate for your environment.

References

Drakar Pty Ltd—Internet Guardian Lite (v3.0)
http://www.drakar.com.au/

Microsoft—Internet Explorer Administrator Kit Home Page
http://www.microsoft.com/windows/ieak/default.asp

Microsoft—Microsoft's Security Web Site
http://www.microsoft.com/security

Microsoft—Internet Explorer 6 Technical Overview

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

http://www.microsoft.com/windows/ie/techinfo/overview/default.asp

Microsoft—Configuring Privacy Options
http://www.microsoft.com/windows/ie/using/howto/privacy/config.asp

Microsoft—Setting Up Security Zones
http://www.microsoft.com/windows/ie/using/howto/security/setup.asp

Microsoft—HOW TO: Use the Internet Explorer 6 Content Adviser to Control Access to Web Sites in Internet Explorer (Q310401)
http://support.microsoft.com/search/preview.aspx?scid=/search/viewDoc.aspx?docID=KC.Q310401%26url=kb;en-us;Q310401%26dialogID=10712972%26iterationID=1%26sessionID=anonymous|9681218

Microsoft—Description of Profile Assistant (Q220017)
http://support.microsoft.com/search/preview.aspx?scid=/search/viewDoc.aspx?docID=KC.Q220017%26url=kb;en-us;Q220017%26dialogID=10715978%26iterationID=1%26sessionID=anonymous|9688344

Microsoft—Configuring Content Advisor Settings
http://www.microsoft.com/windows/ie/using/howto/contentadv/config.asp

Microsoft—Use Security and Privacy Features in Internet Explorer 6
http://www.microsoft.com/windowsxp/pro/using/howto/security/ie6.asp

NetLingo
http://www.netlingo.com

SecurityFocus—Microsoft Internet Explorer Clipboard Reading Vulnerability
http://online.securityfocus.com/bid/3862

SecurityFocus—Microsoft Internet Explorer Forced Script Execution Vulnerability
http://online.securityfocus.com/bid/4082

SecurityFocus—Internet Explorer Subframe Spoofing Vulnerability
http://online.securityfocus.com/bid/855

SecurityFocus—Microsoft IE5 IFRAME Vulnerability
http://online.securityfocus.com/bid/696

© SANS Institute 2000 - 2002 Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.