

By Debra Littlejohn Shinder, MCSE, MVP

IE 7 includes new end-user features such as tabbed browsing, but its main claim to fame is added security. Both as a browser upgrade for XP and as the built-in browser for Windows Vista, IE7 provides a number of new mechanisms to make Web browsing more secure. Let's look at some of the most important new security features.

## Active X marks the (hot) spot

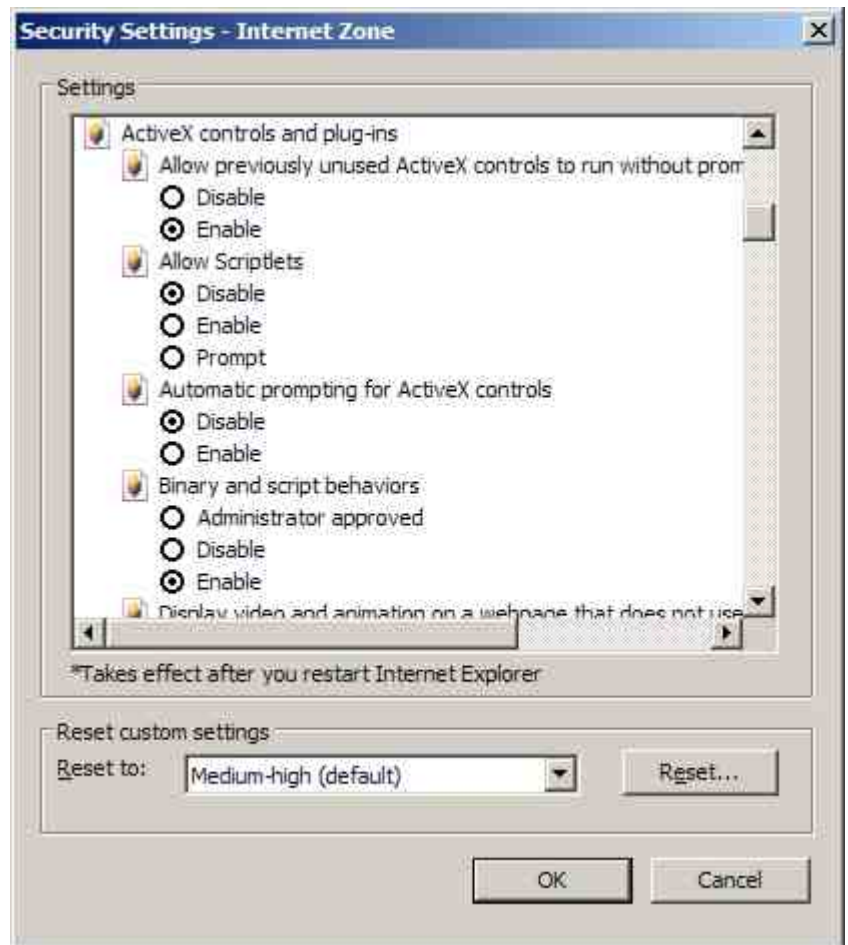
One of the biggest security complaints against Internet Explorer in the past, and the reason many people preferred Firefox and other browsers, was the risk that could be posed by Active X controls. Active X lets Web developers create more sophisticated Web pages than they can with regular HTML. However, because Active X controls are executable programs that can be automatically downloaded and executed by the Web browser, attackers can create malicious controls that manipulate the files on a user's computer, establish connections to other computers, and transfer data without the user's awareness.

Microsoft's response to security experts' concern over Active X led to some big changes in IE 7. A new feature called Active X opt-in disables by default the controls installed on your computer. If you go to a Web site that needs one of the disabled controls to work properly, you're prompted with a message in the information bar at the top of browser window that notifies you that the site wants to run the control (along with the name and publisher's name). You can choose whether to allow the control to run.

The problem with security mechanisms is balancing protection against user convenience. User complaints about Windows Vista's seemingly omnipresent UAC dialog box illustrate the frustrations that in-your-face security can present. In an attempt to enhance security without unduly inconveniencing users, Microsoft included a pre-approved list of controls that aren't automatically disabled by the Active X opt-in feature. These are commonly used controls that are known to be safe. Users won't be prompted before running those controls.

In addition, you can disable Active X opt-in on a per-zone basis. By default, it's enabled on the Internet and restricted sites zones and does not apply to intranet and trusted sites zones. The settings can be changed via the Internet Options | Security tab by selecting the zone and clicking the Custom Level button, then selecting the desired settings (**Figure A**).

Developers of Active X controls can make their controls more secure by using site-locking (restricting the control to a particular Web site domain) and zone-locking (restricting the control to operate only when IE is in a specific zone, such as the intranet) and by digitally signing their controls.



**Figure A:** You can customize the Active X opt-in behavior for each security zone.

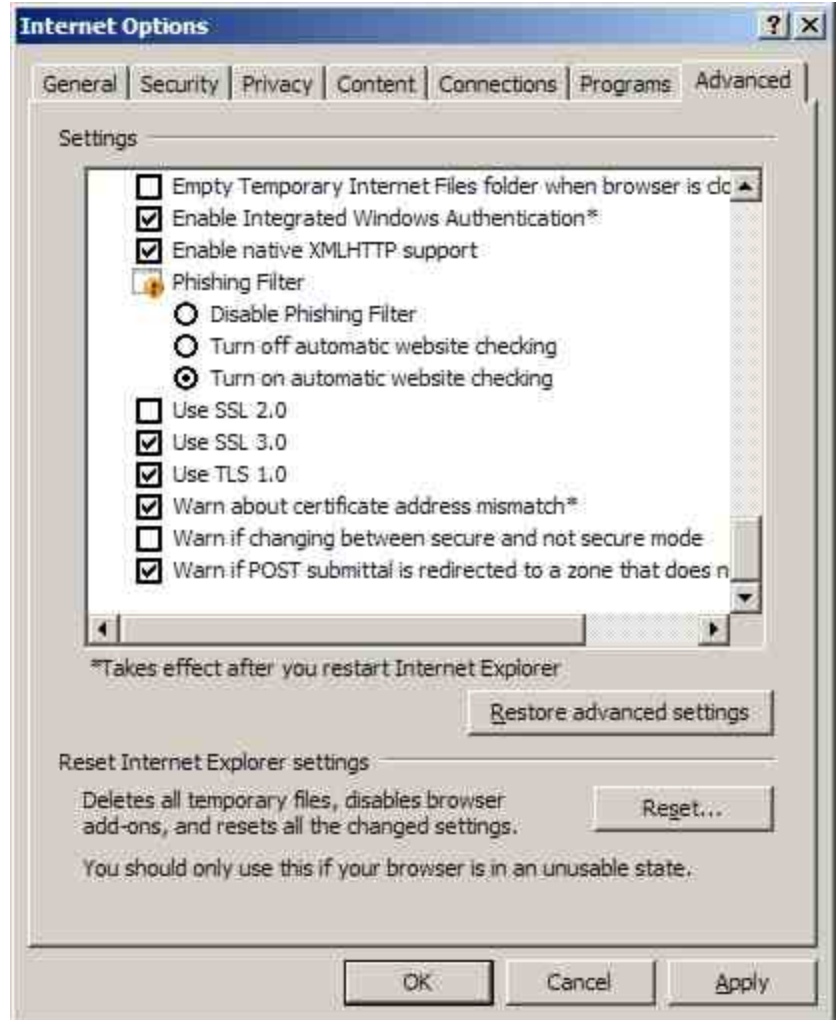
## No more going phishing

To cope with the escalating problem of phishing, IE 7 has added the Microsoft Phishing Filter. The Phishing Filter automatically checks the Web sites you visit against a list of known phishing sites and warns you if the site has been identified as a phishing site. If you prefer not to have sites checked automatically, you can check specific sites when you suspect they might be phishing sites. To do that, you just click Tools | Phishing Filter | Check This Web Site.

If you find a site that you believe is a phishing site and the phishing filter doesn't identify it as such, you can report it to Microsoft and it will be investigated and added to the database if appropriate. If the site you send is on a list of known good sites, it will not be checked. The Phishing Filter uses heuristics to determine whether a site displays common characteristics of phishing sites and if so, flags it as suspicious.

You can disable the Phishing Filter or turn automatic checking off and on through the Advanced Settings tab in Internet Options, shown in **Figure B**.

For more information about IE 7's Phishing Filter, see the [Phishing Filter FAQ](#) on the Microsoft Web site.



**Figure B:** You can configure the Phishing Filter through the Internet Options Advanced Settings tab.

## Cross-domain security

Cross-domain scripting is a tactic used by attackers to cause browser windows that are opened in one security domain to be redirected to a different security domain. IE 7 makes scripts and other Web objects keep the same security context even if they are redirected. By default, the configuration settings are set to deny cross-domain data access in all security zones. IE 7 blocks scripts URLs and blocks redirected navigation in DOM objects when there's a threat of a cross-domain exploit. This means that scripts on Web pages can't interact with the data contained in other domains.

## IE protected mode in Vista

In Windows Vista, IE 7 works with the User Account Control (UAC) feature to run the browser in protected mode by default. The browser has only the minimum permissions needed to surf the Web, and plug-ins and add-ons run with the lowest privileges possible.

Protected mode helps prevent Web sites from installing malicious code on the computer without the user's knowledge. It does this by prohibiting anything from being written to locations on the disk other than the Temporary Internet Files folder unless the user gives permission.

When it's necessary to write to files outside of the TIF folder, a "broker process" is used to provide a more secure means of elevating privileges. The broker process is designed so that it can't be scripted without user input. For a deeper technical understanding of IE 7 protected mode, see this [MSDN article](#).

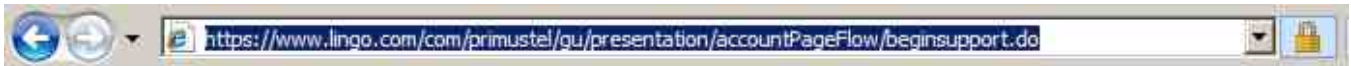
## Locked down security zones

The security zones in IE 7 are more locked down, with the intranet zone now being disabled by default on computers that don't belong to a Windows domain. This zone typically has less restrictive settings than the Internet zone, but most home and small business users whose networks operate on a peer-to-peer basis don't need the intranet zone because they don't have access to an intranet. In addition, the default settings for the Trusted Zones site provides higher security than before, and you can no longer slide the security setting down to Low or Medium Low--you must use custom settings to attain security settings lower than Medium.

## Better SSL/TLS notification

It's now easier for users to determine whether the transactions they engage in over a Web site (such as Internet banking or using a credit card to purchase goods from an online merchant) are secured by Secure Sockets Layer (SSL) or Transport Layer Security (TLS). These are protocols used by Web sites for authenticating the Web server and encrypting the information that's sent over the Internet.

IE 7 displays an icon to the right of the address bar when you access an HTTPS page, which you can click to view a report on the digital certificate used for encrypting the connection and information about it and the issuer, as shown in **Figure C**. In previous versions of the browser, the SSL icon appeared at the bottom of the browser window and was small and easy to overlook.



**Figure C:** The new, more prominent SSL/TLS icon makes it easier for users to determine whether a Web site is secure.

## Additional security enhancements

Along with the major security improvements discussed above, a number of smaller changes were made to help make the browsing experience more secure. These include:

- IE 7 uses a color coding scheme to identify Web sites that have gone through an identity verification process. These sites, which have obtained high assurance certificates, cause the address bar to change to green.
- Three new registry keys, called Feature Control keys, keep HTML (both Internet and intranet) from getting a user's personal information. By default, IE 7 is configured to opt in to this security feature. Access to cached objects is blocked when browsing within the same domain, as well as browsing across domains.
- You can more easily protect your privacy, especially on shared or public computers, by deleting your Web browsing history files, cached pages and objects (Temporary Internet Files), passwords IE has remembered, cookies, and data you've entered into forms, all from one simple interface (and all with a single button click if desired), as shown in **Figure D**.



**Figure D:** You can cover your tracks with just one click to protect the privacy of your browsing history.

- In the past, popups could open new windows that didn't contain an address bar. This made it easier to trick users into thinking a malicious site was legitimate if it was designed to emulate a Web site you'd normally trust. In IE 7, all windows contain address bars so you can see the URL of the site.
- Security threats often sneak in the back door via browser add-ons and plug-ins. If you're concerned about this, you have the option to run IE 7 in "no add-ons" mode. This also allows you to fix problems caused by malware that renders the browser unable to open. Previously, if a browser extension was causing IE to crash and you didn't have an alternative browser installed, you couldn't get to the Web to download information or programs to help you fix the problem.
- Some clever attackers have created URLs that use international characters to spoof legitimate Web sites. That is, the domain name might contain characters in another language that resemble the English characters making up a different domain. This type of domain spoofing is prevented in IE 7 because the browser lets you know that the characters are in a different language.

## Glossary

- **ActiveX:** A technology developed by Microsoft that is an outgrowth of Object Linking and Embedding (OLE) and Component Object Model (COM), which allows Web developers to make Web pages interactive and provide the same types of functions as Java applets.
- **User Account Control (UAC):** A security technology in Windows Vista that reduces exposure to attacks by running in nonadministrative mode, even when logged on with an administrative account, unless and until administrative privileges are required to perform a task. Users must give explicit permission to elevate to administrative mode and enter administrative credentials.
- **Phishing:** A type of technology-based social engineering ploy in which computers users are directed, usually via e-mail, to a Web site that purports to be that of a bank, loan company, credit card company, e-commerce merchant, governmental agency, or other site that requires users to enter confidential information, such as account passwords, account numbers, social security numbers, and other personal data that is collected and used for identity theft.
- **Scripting:** Use of a simplified programming language (calling scripting language) to create a set of instructions for a Web page.
- **Security zones:** A technique used in Internet Explorer to allow you to assign different levels of security to different sets of Web sites depending on where they're located or how much you trust them. For example, if you consider a site to be untrustworthy, you can place it in the Restricted zone; if you know it's safe, you can place it in the Trusted zone. Sites on the Internet will, by default, have tighter security imposed than those on an intranet.
- **SSL/TLS:** Transport Layer Security (TLS) is the successor to Secure Sockets Layer (SSL), which was originally developed by Netscape to make e-commerce transactions over the Internet safer. It uses public key (asymmetric) encryption and digital certificates to assure users that the Web servers with which they're doing business have had their identity verified (authentication) and symmetric encryption, such as DES/3DES or AES, to encrypt traffic.



Debra Littlejohn Shinder is a technology consultant, trainer and writer who has authored a number of books on computer operating systems, networking, and security. These include *Scene of the Cybercrime: Computer Forensics Handbook*, published by Syngress, and *Computer Networking Essentials*, published by Cisco Press. She is co-author, with her husband, Dr. Thomas Shinder, of *Troubleshooting Windows 2000 TCP/IP*, the best-selling *Configuring ISA Server 2000*, and *ISA Server and Beyond*.

## Additional resources

- TechRepublic's [Downloads RSS Feed](#) **XML**
- Sign up for TechRepublic's [Downloads Weekly Update](#) newsletter
- Sign up for our [Windows Vista Report](#) newsletter
- Check out all of TechRepublic's [free newsletters](#)
- ["Installing Windows Vista: The good, the bad, and the ugly"](#) (TechRepublic download)
- ["Get an in-depth look at Vista firewall's advanced configuration features"](#) (TechRepublic download)
- ["Vista's Windows Meeting Space offers enhanced functionality for real-time collaboration"](#) (TechRepublic download)

## Version history

**Version:** 1.0

**Published:** October 23, 2006

## Tell us what you think

TechRepublic downloads are designed to help you get your job done as painlessly and effectively as possible. Because we're continually looking for ways to improve the usefulness of these tools, we need your feedback. Please take a minute to [drop us a line](#) and tell us how well this download worked for you and offer your suggestions for improvement.

Thanks!

—The TechRepublic Downloads Team