10 things you should know about Internet Explorer 7.0 enhancements

Version 1.0
November 10, 2005

By Debra Littlejohn Shinder, MCSE, MVP

Microsoft has made many changes to Internet Explorer that will improve both the user browsing experience and security. The next generation of IE will be included in Windows Vista, but you don't have to upgrade the operating system to enjoy its benefits. Although some IE features will be available only with the Vista version, a version of IE 7.0 will also be available to run on Windows XP with Service Pack 2. This article discusses some of the new features that will make IE 7.0 better and more secure.

1 Tabbed browsing

Users asked for it and now they're going to get it—tabbed browsing, that is. It's a feature made popular by Mozilla Firefox, Opera, MyIE2, and other third-party browsers, and it allows you to view multiple pages with "tabs" in the same browser window so you can switch back and forth between them quickly and easily instead of having numerous browser windows open. You simply click on a tab to view a different open Web page.

Because IE was originally designed as a single-window browser and because IE shares code with Windows Explorer, the addition of tabbing to IE was a challenge. However, Microsoft has done it in such a way as to overcome these problems and also retain compatibility with most third-party add-ons. Because the tabbing implementation is multithreaded and each tab uses a separate thread, users will experience faster performance.

2 No phishing allowed

Phishing often involves directing users, via e-mailed links, to fraudulent Web sites (for example, a site that purports to be that of the user's bank but is really the site of a con artist who uses it to collect bank logon credentials). It has become a major threat to Web users.

IE 7.0 contains a phishing filter that can automatically check the sites you visit against a list of known phishing sites, warn you if it is a reported phishing site, and automatically take you away from the site. The browser can also detect that a site uses common phishing tactics even though it hasn't been reported and will display a different alert. A mechanism is included that allows users to easily report phishing sites they discover, to be checked out by Microsoft and added to the list if they're found to be conducting phishing activities.

If you wish, you can configure the browser not to check sites automatically. You can still manually check a specific site that you suspect may be a phishing site.

3 Clear your tracks

Privacy is a big concern, with identity theft on the rise. Many users share computers with others at work or at home, and/or use public computers such as those at libraries and Internet cafés. They want to be able to quickly clear any personal information they've entered in browser forms and get rid of the records of what sites they've visited. In previous browser versions, this requires multiple steps to clear history, temp files, cookies, and so forth.

IE 7.0 simplifies the process with its Clear Tracks option, which is implemented as a top-level menu item. This feature deletes the index.dat files that contain browsing records. Users will no longer need to buy third-party privacy protection software to easily clean up browsing history and other "evidence."

4 Protected mode (low rights IE)

IE 7.0 runs in protected mode, which in early implementations was referred to as *low rights IE*. This is one of the most important new security features, but unfortunately, you have to run IE 7.0 on Windows Vista to take advantage of it. The feature works in conjunction with Vista's User Account Protection (UAP), which is a philosophy as much as a technology. Simply stated, it runs everything with least privilege by default.

IE protected mode gives the browser only the permissions that are absolutely necessary and also runs add-ons

and plug-ins with the lowest possible permissions. Processes run at one of three integrity levels: high, medium, or low. There's no way for a process running at a low level to send data to a higher level process, thus preventing unauthorized elevation of privileges (a favorite trick of hackers).

5 Add-on free mode

Another new mode makes it much easier to troubleshoot problems with IE. Originally called *safe mode* but renamed *add-on free mode*, it allows you to boot IE without any plug-ins or extensions. In previous versions, you often ran into problems if, for example, spyware or other malware rendered IE unusable. You needed to download and run an anti-spyware program to fix it, but the catch-22 was that you couldn't download anything because you couldn't open IE.

Add-on free mode will fix this, allowing you to bypass the extension that's causing the problem and run IE without add-ons in much the same way that you can boot Windows into safe mode and run it without loading drivers that may be keeping you from booting the operating system normally.

6 Opt-in for ActiveX

ActiveX controls allow Web developers to make Web pages much more sophisticated by running miniature applications (similarly to Java applets) that can add high-level interactivity for Web site visitors. However, ActiveX can be exploited to download viruses or Trojans to users' machines and perform other harmful actions, so it can create a security risk.

IE 7.0 attempts to ensure that controls can run only if they're safe to run in the browser. It maintains a database of controls that are intended to run in the browser and checks this list before running an ActiveX control. If the control isn't on the list, the browser will display a prompt to allow the user to opt in (or not) for that control to run in IE.

7 Cross-domain protection and consolidated URL class

A common type of browser attack uses something called cross-domain scripting to redirect browser frames opened in one security domain to a different security domain. IE 7.0 protects against this by making scripts and other objects retain their security context regardless of whether they're redirected. This means, for example, a would-be attacker from the Internet won't be able to run a script in the local machine zone where he would have the permissions of the currently logged on user. Another method of attack exploits the browser's handling of special characters in the URL.

8 Zones lockdown

Internet Explorer has long used the concept of security zones to allow you to implement different security settings depending on whether the site you're accessing is on your local computer, an intranet on the LAN, or the Internet. Zones also make it easy to build a list of sites you trust and other sites that should be restricted.

Security templates in previous versions of IE (Low, Medium-Low, Medium, and High) can be used or you can customize the individual security settings for each zone. IE 7.0 adds a new template, Medium High, for more granular control without having to customize. This template is available when you run IE 7.0 on Vista with protected mode turned on. Other changes include:

- The Intranet zone is disabled by default for most home and small business computers (those that aren't members of a Windows domain).
- The default settings for the Trusted Sites zone provide higher security.
- The slider bars will no longer allow you to select Low or Medium Low security; they only go down to Medium. You can set a zone to lower security by using the custom settings.

9 SSL and TLS

Secure Sockets Layer (SSL) is a standard for encrypting data exchanged between a Web browser and Web server. It's based on public key cryptography and digital certificates to validate the identities of the machines involved in the transaction (server only or client and server).

If there's a problem with a secure site in IE 6.0, the user has to decide what to do. IE 7.0 defaults to the most secure choice. If there's a problem with a certificate, you get a page that explains the problem. Sites are blocked if the certificate has expired or been revoked, if it was issued by an untrusted root certification authority, or if it was issued to a different hostname from the one in the site's URL. Users can still click through the warnings and visit the site anyway unless the certificate was revoked, but they'll get constant warnings.

One warning you won't see anymore (to the relief of many users) is the one that says "this page contains both secure and non-secure items." Instead, only the secure content will be displayed and if you want to see the non-secure content, you can use the Information Bar to unblock it.

Transport Layer Security (TLS) is the successor to SSL and is more secure. IE 6.0 supports SSL versions 2.0 and 3.0, which are enabled by default, and TLS, which has to be explicitly enabled. In IE 7.0, SSL 2.0 (the least secure version) is disabled by default and TLS is enabled.

10 Secure authentication

IE supports various authentication schemes used by Web servers, including basic, digest, integrated Windows authentication, and client certificate mapping. Some of these are more secure than others. For example, basic authentication sends the password as plain text, making it nonsecure unless it's used in combination with SSL/TLS.

Previously, the browser would use the first authentication scheme offered by the server. IE 7.0 corrects this by defaulting to the strongest authentication scheme that's supported by the Web server. It also displays a warning for basic authentication over HTTP, telling the user that the password will be sent in clear text.

Additional resources

- TechRepublic's **Downloads RSS Feed** XML
- Sign up for our Downloads Weekly Update newsletter
- Sign up for our Network Security NetNote, delivered on Mondays, Tuesdays, and Thursdays.
- Check out all of TechRepublic's free newsletters
- "Photo gallery: Internet Explorer 7.0 Beta 1" (TechRepublic)
- "Internet Explorer 7 could extinguish the re-ignited browser war" (TechRepublic article)
- "Make Internet Explorer as secure as possible with this step-by-step guide" (TechRepublic download)

Version history

Version: 1.0
Published: November 10, 2005

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