ANOTHER FLAW FOUND IN INTERNET EXPLORER

Microsoft really can't catch a break. Not that it was ever a paragon of security. But this is getting ridiculous.

A new flaw in Internet Explorer was announced this week. So far, there isn't a patch for it. Hopefully one is on the way.

This flaw requires practically no user interaction. Visiting the wrong Web site is all it takes. Malware will be automatically downloaded and installed on your computer.

The flaw only affects Internet Explorer 6 and 7. IE 8 dodges this bullet. So, if you've been waiting to upgrade, now is the time.

Actually, I'd ditch IE altogether. Firefox and Chrome are two excellent alternatives. They'll import all your information from IE. So, you won't have to start over.

I have lots more about browsers and security on my site:

You're using Firefox; should you uninstall Internet Explorer?
There are good reasons to leave Internet Explorer on your computer. In fact, you cannot remove it. It is an integral part of Windows. You can remove the icon if you want but Internet Explorer will always be with you.

So, it's essential that you keep it updated. That's actually easy. Just set Windows for the most automatic updates possible. Then, let Microsoft take care of it.
Also, be sure you're using Internet Explorer 8. That is the safest version. There is no value in maintaining old versions of Internet Explorer. They simply make you more vulnerable to attacks.

Your computer will continue to use Internet Explorer. Some Windows utilities use it in the background. One of those is the aforementioned Windows Update.
Microsoft uses software objects called ActiveX Controls. These permit you to interact with Internet sites. They are also dangerous. Hackers and criminals can use them to attack your computer.

Windows Updates use ActiveX Controls. Other Windows utilities use them, too, behind the scenes. So, although you will not see it, Internet Explorer is still working. Other browsers cannot do these jobs.
Why is that? Everyone but Microsoft considers ActiveX Controls too dangerous. So, other browsers do not handle them. If you try to download Windows Updates with

Firefox, it won't work. You'll get the same result with Opera, Google Chrome and Apple Safari.

[You can subscribe on my site]().
I recommend that everyone switch to another browser. Firefox is my favorite. All four alternative browsers are available through my site:
• [Firefox]()
• [Opera]()
• [Safari]()
• [Chrome]()

• [Secure your computer against threats]()

Free antivirus software:
- [AVG AntiVirus]()
- [avast!]()
- [Avira AntiVir Personal]()
- [Microsoft Security Essentials]()
- [Panda Cloud Antivirus]()

Firewalls

A good firewall will also make your computer more secure. Firewall programs render your computer invisible to hackers' probes. Hackers run scanning programs over the Internet, looking for computers with electronic openings, called ports. Good firewalls make your computer invisible to the scanners. As with antivirus software, don't run multiple firewalls. They will conflict.

Free firewalls:
- [Zone Alarm]()
- [Outpost Firewall]()

You need programs to keep spyware and adware from taking root. And you need other programs to annihilate spyware and adware that collects on your computer. You should

use multiple anti-spyware programs on your computer. Unlike antivirus software and firewalls, they won't conflict.

Free anti-spyware programs:
- [Ad-Aware](#)
- [Spybot Search & Destroy](#)
- [Microsoft Windows Defender](#)
- [SpywareBlaster](#)

Safe Browsing

Microsoft's Internet Explorer is rife with security holes. Over the years, many of these security problems have been patched through Windows updates. But new ones continue to appear. I recommend that you switch to the Firefox browser. It's free. I think it is inherently safer.
- [Firefox Web Browser](#)

Get more help with computer security:
- [Test your computer security](#)
- [Secure your home wireless network](#)
- [Drive-by downloads and other online dangers](#)
- [Rootkits: a new security threat](#)
- [Secure data before PC repairs](#)
- [Secure your new Mac](#)
- [So your e-mail was hacked. Now what?](#)