8 Ways to Protect Yourself From Microsoft's Dangerous Internet Explorer Bug

BY KIM LACHANCE SHANDROW | April 28, 2014

1. Don't use Internet Explorer at all.
Even the U.S. Department of Homeland Security says you should stop using it until Microsoft until untangles this big mess. Seriously. Instead, surf the web using a different browser, like Google Chrome or Mozilla Firefox, especially if you're running Windows XP, which you really shouldn't be anymore. You don't want to be the next victim of "Operation Clandestine Fox," do you?

2. Disable Adobe Flash.
FireEye said disabling the Adobe Flash plugin within Internet Explorer "will prevent the exploit from functioning." Basically, doing so will stop hackers in their tracks. Yeah, you'd better get on that right away.

3. Get behind a firewall.
Firewalls help safeguard your computer from hackers who could steal your identity, banking information, credit card numbers and more. Most computer operating systems already have a firewall built in. Double check that yours does and that it's turned on. If you're running a Windows operating system, check if it automatically comes with firewall protection here. You can also add additional firewall protection to your computer and network for free from ZoneAlarm or Sygate Personal Firewall Free.

4. Install antivirus and antispyware software.
Installing antivirus and antispyware software and regularly keeping it updated is critical, even when you're not reacting to the latest threats. Antivirus software detects and removes malware, including adware and spyware, and filters out potentially dangerous downloads and emails.

Brian Underdahl, author of *Cybersecurity for Dummies* (Wiley, 2011), suggests CheckPoint Software Technologies' ZoneAlarm Extreme Security, a comprehensive antivirus software security package. It costs $54.95 for one year and $84.95 for two years. Some other popular, equally effective antivirus tools include Bitdefender Small Business Security ($150 for one year) and Webroot SecureAnywhere Antivirus 2013 ($39.99 for one year).

5. Apply all software updates.
If you insist on still using Internet Explorer, install all of the latest software patches from Microsoft. It's a vital preventative step to add to your security hygiene routine. You can get all of the latest Microsoft software updates here.

6. Use Internet Explorer in "Enhanced Protected Mode."
This enhanced security feature, which was first rolled out with Windows 8, helps stave off cyber criminals looking to mess with your system settings, install harmful software and steal your personal data.

Enhanced Protected Mode is turned off by default in Internet Explorer and on the Windows 8.1 desktop. When it's enabled, it only loads add-ons, including browser toolbars and extensions, only if they're compatible with Enhanced Protected Mode. To turn it on, go to your Internet Explorer "Internet options," then select "advanced." Next, navigate to the security section. Choose "Enable Enhanced Protection Mode." Select "OK" and restart Internet Explorer.

7. Download this toolkit.
Microsoft advised in a blog post over the weekend that Internet Explorer users should install its Enhanced Mitigation Experience Toolkit (EMET) 4.1 to "help protect against this potential risk." Even Microsoft admits that the toolkit isn't completely hacker-proof, though. What is anyway these days?

8. Don't click on suspicious links.
By now, this should be old hat. Avoid sketchy looking URLs like the plague. Also, don't open emails from anyone you don't know or even suspicious seeming emails from someone you do know. If you accidentally open an email that contains suspect attachments or links, don't click on any of them.

Source: http://www.entrepreneur.com/article/233467