

## I know, you still love Windows XP, And you're still running the nearly four-year-old edition SP2.

What if, *SHUDDER*, you are using Vista and like it? (It could happen!) Support for Windows Vista Service Pack 1 (SP1) ends on July 12, 2011. Be sure you have the latest service pack for Vista, which is SP2.

Although July 13, 2010 marked the support retirement of the 2<sup>nd</sup> service pack for XP -- a date that some have called a "red alert" for people running SP2 -- that doesn't mean your copy of Windows will just one day refuse to run.

It does mean that, after that date, Microsoft stopped offering **any** security patches, no matter how severe the vulnerability, no matter what part of Windows or associated component is involved. No more Windows patches -- and no more patches for Internet Explorer (IE), no patches for Windows Media Player, no patches for Outlook Express. There are replacements for all of these components of course, but more on that below.

You can, of course, sidestep the whole problem by upgrading to Windows XP SP3, which will be supported until April 2014: Microsoft has posted a page that explains how to do that [here](#). (Note: Because there is no SP3 for the **64-bit version** of Windows XP, you'll continue to receive security updates if you're running SP2 of that edition.) Of course not many PCs were running 64 bit processors years ago.

Among your options: Download and install SP3 via Windows Update, download a disk image for upgrading multiple machines, or order a SP3 CD for \$3.99 from Microsoft.

But if you're committed to SP2, for whatever reason, and have no intention of upgrading anytime soon, there *are* steps you can take to make your PC more secure and your time on the Internet safer.

- **Dump Internet Explorer.** After Tuesday, Microsoft won't be providing IE patches of any kind, for any version -- IE6, IE7 or even 2009's IE8 -- to people running Windows XP SP2.

But other browser makers aren't halting updates for *their* wares. Mozilla, Google, Apple and Opera will be shipping fixes for Windows XP versions of their Firefox, Chrome, Safari and Opera browsers for the foreseeable future.

More than a year ago, Mozilla debated whether to drop support for older editions of Windows, including Windows 2000 and Windows XP SP2. But the company decided against the move.

According to the system requirements for the latest Firefox 4 Beta, the browser runs not only on Windows XP, but also Windows 2000. (Mozilla's systems requirement link for Firefox 4 currently takes you to the page for version 3.6.6, leading us to believe that the requirements will remain the same for Firefox 4, which is ready to release any day now.

And because Mozilla's policy is to continue supporting a browser with security updates for at least six months after the launch of its successor, moving to Firefox 4 down the road means that if the company ships Firefox 5, or whatever the next edition is called, a year later -- in early 2012 -- patches for it will be produced through May 2012 or later.

It's important to keep a browser up-to-date on patches because hackers continue to exploit browser vulnerabilities, particularly those in IE. They focus on IE bugs for a simple reason: Every Windows machine has it, and Microsoft's browser continues to be used by more people than any other.

Ironically, you may actual *improve* the security of your Windows XP SP2 machine if you dump IE . **Since you can't uninstall it, just stop using it**

- **Patch third-party programs, especially browser plug-ins.** According to most vulnerability experts, it's not your operating system that today's attackers target: It's non-Microsoft software, particularly browser plug-ins.

Antivirus vendors McAfee and Symantec have both reported huge surges in attacks exploiting bugs in Adobe's Reader, one of the most widely-installed plug-ins. McAfee, for example, said that exploits of Reader jumped 65% in the first quarter of 2010 compared to 2009's total.

Those kind of numbers, while dated, mean you should be spending more time patching third-party products, less time worrying about the inevitable vulnerabilities in Windows XP SP2 that Microsoft will no longer fix.

But that's tough: Most non-Microsoft software lacks automatic updating. Adobe, for instance, only instituted auto-updating for its regularly-exploited Reader and Acrobat in April -- and requires users to manually switch it on -- but it still hasn't offered the same functionality for its just-as-often-attacked Flash Player plug-in.

- **Stay safer.** Without patches for the operating system, it's even more important than ever to practice safe computing.
- ❖ Install antivirus software or a multi-component security suite if you don't have one on the PC already. If you do, keep it up to date by regularly downloading new signatures (aka definitions). Several AV programs, including Microsoft's own Security Essentials, are free.
- ❖ Also, keep the firewall turned on -- easily done since Windows XP SP2 was the first Microsoft OS that not only included a firewall, but enabled it by default.
- ❖ And remember the wisest advice: Don't steer to sites you're not sure can be trusted, don't open e-mails and attachments you didn't expect to receive, and don't download software from questionable sources.

the same advice you've heard a hundred times.

- **Keep reading Microsoft's security bulletins.** Just because your copy of Windows XP SP2 won't receive any more updates doesn't mean you should stop looking at the bulletins Microsoft publishes each Patch Tuesday.

Those bulletins may not strictly apply to XP SP2, but Microsoft often includes steps users can take to protect themselves if they're not able to deploy a patch. In the bulletins, that information is tucked under the subhead "Workarounds" beneath the information for each vulnerability.

The workarounds may include steps you can take with XP SP2 to deflect or hinder attacks. Obviously, your mileage may vary.

Microsoft's irregular security advisories -- generally issued as a prelude to an eventual patch -- also contain worthwhile information, including which Windows versions are affected, how attacks (if there are any at that point) are exploiting the bug and whether there are workarounds that can block or help block assaults. Get them at:

<http://www.microsoft.com/technet/security/advisory/default.mspx>

Once you get to the site then you need to search for Windows XP, and specifically for your version and your service pack. Then look through the various bulletins to be sure your system is up to date.