Microsoft to stop updates for XP SP2

July 12 2010, By Byron Acohido

Microsoft this week will stop issuing security fixes for computers running the Windows XP operating system updated with Service Pack 2.

The switch-off will result in hundreds of millions of PCs worldwide, including tens of millions in the U.S., instantly becoming riper targets for hackers.

So-called XP SP2 desktops and laptops are still widely used in corporate networks. A service pack is a collection of feature upgrades and security fixes delivered in a single download.

Microsoft released SP2 in August 2004 mainly to beef up security. Then in April 2008, the company released SP3 with less fanfare, recommending that all XP computers be updated with the latest service pack. Yet more than two years later, thousands of companies worldwide have not done so.

Tech services firm Softchoice recently surveyed 117 financial, health care, manufacturing and educational organizations in the U.S. and Canada. It found eight of 10 organizations continue to use XP SP2 computers widely.

Now security experts worry that companies won't pay much attention to Microsoft dropping all tech support for SP2. "It's a virtual guarantee laggards will miss this deadline," says Dean Williams, services development manager at Softchoice. XP SP2 computers will "become fair game," he says. "There will just simply be more ways to hack in."

Companies can continue to get security updates for XP computers through April 2014 by upgrading to SP3. It's free. Testing and deployment is not trivial but can be automated, noted research firm Gartner. Or they can replace old XP units with new Windows 7 PCs, which Microsoft fully supports.

Microsoft typically issues security fixes, called patches, for freshly discovered flaws on the second Tuesday of the month.

Hackers continually flush out fresh Windows security holes, particularly in the Internet Explorer Web browser. And they are adept at taking control of Windows PCs with unpatched security holes.

Cybercriminals typically activate a malicious program inside the Web browser. They harvest the PC owner's sensitive data, then use the compromised PC to spread spam, sell worthless anti-virus protection, hijack online banking accounts and probe deeper into corporate networks.

Cyberattacks have escalated in recent years.

"As soon as the next suitable vulnerability appears, I am expecting that attackers will seize the opportunity created by the large pool of unpatched SP2 machines," says Wolfgang Kandek, chief technical officer at tech security management firm Qualys.

Microsoft remains optimistic that "as customers understand the value of staying on a supported version of Windows, they will upgrade their PC to the version that's right for them," spokesman Frank Fellows says.