IMAGE ANGST

"The latest Service Pack for Windows XP - Service Pack 2 (SP2) - is all about security." So began the blurb Microsoft sent out in 2004 urging users to install their latest security innovation.

Tired of ever-repeating mini-scandals in which hackers discovered security holes in Windows that could be exploited by viruses, the company developed a "super secure" package for Windows XP that would make it nigh impossible for pimply faced kids to remotely take over your machine for their nefarious slacker purposes.

And it worked, at least for a while. Microsoft has scrupulously updated SP2, issuing patches on a regular basis. If you use XP SP2 and have Automatic Updates turned on, you don't even notice the patches anymore - Microsoft installs them when you shut down your system.

But that doesn't mean that all is well for XP users these days. There are, of course, the run of the mill viruses that can take over Windows operations, often by installing rogue programs with the same names as legitimate Windows DLLs and applications.

This trash is supposed to be barred by your anti-virus software, which you of course need to update on a regular basis.

And if you don't install all the Microsoft patches as they are issued, exploits that were designed to take advantage of security holes could still compromise your system.

And once in a while, something comes up that Microsoft didn't anticipate - leaving you vulnerable until the company comes up with a patch.

It's possible that by the time you read this, Microsoft will have come up with a patch for the latest security scandal plaguing Windows users, but maybe it won't - which means that your computer will be vulnerable to the "WMF bug" - an exploit that could result in a hacker having total access to your computer, letting them do who-knows-what with it!

WMF stands for Windows Metafile Format, which is a "container" file type for graphics that lets the computer display images like bitmaps and jpegs more quickly.

WMF is a "legacy" format that has been with Windows since its '95 incarnation, and as such was never developed with the rigorous attention to on-line security that Windows 32 bit native code (i.e. Windows 2000 and XP) were.

In other words, all versions of Windows use WMFs - meaning they are all equally vulnerable to the exploit.

And some hacker somewhere has figured out a way to use a flaw in this code to install rogue software; the prize might be a keylogger that will record whatever you type, like a user name and password, a credit card number, or it might be a “spammer” program that will let them use your system as a drop zone for “Viagra” type messages , etc.

How do these rogue programs get installed? Easy - you, the victim get an e-mail with a sassy message, directing you to click on a Web link, or containing an in-line picture. No attachments or viruses here - just a link, or an image, like the ones in the dozens of messages in your inbox that you plan to check out “when you have time.”

However, clicking on this link lets the site download the rogue keylogger when your computer simply displays an infected image on the site! That's right - you don't have to click on anything if you're using Internet Explorer, Outlook or Outlook Express (not that Firefox, Thunderbird, Opera etc. are all completely immune either).

The IT (information technology) community is up in arms about this one - because if you do work on-line or get e-mail, there's almost no way you can avoid coming up against this problem. There are a couple of things you can do now - specifically, disabling Windows Fax and Picture Viewer.

Someone (more likely lots of people) at Microsoft Central has had some late nights this week, you can be sure of that. And if a patch hasn't been developed yet (I write these columns about a week in advance), sooner or later one will be.

This site will have details of when and where to download a patch, if you're not set up with automatic updates). But once again, MS is behind the 8 ball, giving Mac and Linux users more stuff to snigger at (believe me, sniggering at Microsoft is high on the agenda for both crowds).

Wouldn't it be great if you could anticipate these things in advance - or at least be on the cutting edge of security developments, so you can computer in peace without having to worry about what to click on or view? How would you like to have a seasoned staff of volunteers check out your system and keep it up to date with the latest fixes? For free? You'd like that, wouldn't you? Well, check out this column soon for details!

Dennis Turner

Update on WMF Patch:

On Thursday (1/12), Microsoft released a patch for the vulnerability 5 days ahead of schedule. All indications are that the patch works well, but Microsoft only released a patch for Windows 2000, Windows XP, and Windows Server 2003. Virtually all earlier versions of Windows remain vulnerable in one degree or another. See the Microsoft Security Advisory for links to specific patches or use Windows Update.

Microsoft states that earlier versions of Windows, including Windows ME and Windows 98, are not critically affected by this vulnerability because there is no attack vector that is easily available, as there is with Windows XP.

They might have said the same thing for Windows 2000, which also lacks a default component that could allow exploitation, but Windows 2000's place as a current, mainstream product likely made it more important to Microsoft.

While there are strong mitigating factors and effective workarounds for this vulnerability, Microsoft strongly recommends installing it as soon as possible.

Note on Microsoft Patch Advance Notification:

Microsoft went “out of cycle” for the WMF patch that they released this week, but they had other patches that they had scheduled for release this month.

Under the regular patch cycle, Microsoft releases security bulletins and patches for them midday on the second Tuesday of the month. On the Thursday before (actually, three business days before) they release a limited advance notice about the patches, and that notice is always at this address.

According to the current advance notice plan, on Tuesday, Microsoft will release two “Critical” security updates, one for Windows and one “affecting Microsoft Exchange and Microsoft Office.” Both updates may require a reboot of the computer. The patches will be available as explicit downloads for each platform they affect and through Windows Update and Microsoft Update.

In addition, it appears that Microsoft will release a number of non-security updates which are, nevertheless, labeled “High-Priority.”