

This Free E-Book is brought to you by Natural-Aging.com.

100% Effective Natural Hormone Treatment
Menopause, Andropause And Other Hormone Imbalances
Impair Healthy Healing In People Over The Age Of 30!

Windows XP Safe and Secure?

By Richard Lowe

Windows XP Safe and Secure? by Richard Lowe

Microsoft has come under fire lately because of their habit of releasing software which has serious flaws, most especially problems with security. Unfortunately the criticism is justified and verges on the criminal: flaws (implementation bugs as well as just plain silly design decisions) have resulted in literally tens of billions of dollars in damage and losses worldwide.

Don't believe me? Think of all of the viruses that have devastated not hundreds, not thousands, not even millions, but tens of millions of systems. All of these viruses are allowed to "breed" (spread) because of one of the silliest, misguided, downright stupidest decisions ever made by a major corporation. This was the addition of email scripting – without that incredibly powerful and almost totally unused (and many would argue not necessary) feature viruses could not spread in a matter of days or even hours. Since when does anyone need to script their email program anyway? I've never heard of a single person or corporation using this feature legitimately.

On top of this kind of issue (and there are several others), Microsoft's products tend to have blatant bugs – problems in programs which should have been caught by adequate design, testing and quality assurance. The most famous of these is probably the series of bugs that led to Nimda and Code Red. Again, millions of systems were damaged and countless millions of man hours were wasted in efforts to eradicate these issues.

The firestorm that landed on Microsoft as a direct result of these and other problems and issues was fantastic to behold.

Naturally Microsoft responded, trying desperately to reduce the impact on their business. They claimed the problems were with administrators who did not apply patches, with people reporting problems too early (thus giving hackers information before fixes were complete) and any number of other problems. It seemed that everyone except for Microsoft was doing the wrong thing – of course, the mighty Microsoft could do no wrong.

In spite of what the left side of their face was saying, Microsoft did introduce some changes. They announced a new security service to help keep systems locked down and system administrators happy. Automatic security patch downloads were

added to Windows XP and, I'm sure, dozens of other changes happened.

With the release of Windows XP, Microsoft was adamant that they had tested it from top to bottom. The software giant even claimed it had written a special program to check for the nastiest kind of software problem – buffer overflows. You see, a buffer overflow is one of the most common ways for a hacker to break the security of a system. It does this by writing some code beyond the end of where it is supposed to write it. The code is then executed in privileged mode to give the hacker entrance to the system.

Well, a short time ago Microsoft released a patch to Windows XP to fix exactly this problem. It seems there is a buffer overflow problem in the UPnP service. What the heck is UPnP, you ask? That's a good question.

UPnP is a special plug-and-play service. What is plug-and-play? Well, when you install a new device on Windows XP it automatically detects it and configures it for you. Plug-and-play is a very nice feature, and it works very well in Windows XP.

On the other hand, UPnP is a special kind of plug-and-play. This looks for printers and other devices added on the network (wired and wireless). It's actually a pretty cool idea. Now, when someone adds a printer to the network you must configure it on each and every workstation. With UPnP the configuration is totally automatic.

However, UPnP is very, very new and there is almost no real support for it with any devices. So UPnP is more or less not

used, and it is certainly not needed by home computer users. By shipping Windows XP with the product Microsoft was solving the classic "which came first, the chicken or the egg" problem. They had to send out support for these devices in order to convince vendors to start providing them.

But Microsoft made one big mistake – when you install Windows XP, this unused service is turned on! What that means is everyone who has ever installed Windows XP is running this service.

And the service has a bug – a huge bug, the kind of bug that if it hit your windshield would smash the car and cause it to explode in flames, killing all of the passengers and the driver.

The problem is very bad, and Microsoft has released a patch to fix it. But the story gets even more interesting.

The National Infrastructure Protection Center released an advisory stating that everyone who is not using this service should disable it. This is an incredible statement from this agency. What they are implying is the UPnP service problem directly puts the United States computer infrastructure at risk (that's what this agency protects)! That's a big thing for them to be saying.

What are they afraid of? That hackers and perhaps hostile governments can use the bug to their advantage. You see, special programs called Zombies can be installed on Windows XP machines with this problem, and Zombies can be used to launch distributed denial of service attacks on computers throughout the world.

In fact, I'll bet you heard about the denial of service attack performed by the Code Red worm recently against the Whitehouse (the attack failed, if you remember). That's exactly what this agency is afraid of and what they are trying to prevent.

So the next time you are thinking about giving all of your credit card data to a site which uses Microsoft Passport, think about this article. Do you want to trust all of your confidential data to a company which cannot keep it secure? Just think about it, read some more, and make the rational decision.

For more information, check out the following articles.

Microsoft Security Bulletin MS01–059

<http://www.microsoft.com/technet/review/default.asp?url=/technet/security/bulletin/MS01-059.asp>

eEye Digital Security

<http://www.eeye.com/html/Research/Advisories/AD20011220.html>

NIPC ADVISORY 01-030.2 Universal Plug and Play Vulnerabilities

<http://www.nipc.gov/warnings/advisories/2001/01-030-2.htm>

Richard Lowe Jr. is the webmaster of Internet Tips And Secrets at <http://www.internet-tips.net> – Visit our website any time to read over 1,000 complete FREE articles about how to improve your internet profits, enjoyment and knowledge.

The only sure way to shop safe on the Internet

By William Milham

The only sure way to shop safe on the Internet by William Milham

After all my years as an Internet Professional, I can't begin to count the number of phone calls and emails I've gotten regarding safe shopping on the Internet. When you really think about it, there's about the same amount of risk shopping in a regular walk-in store (remember those?) as there is shopping on the Internet. Actually, there's less risk on the Internet. If you're robbed in a regular store, your life could be in danger. If you pay attention to what you're buying on the Internet and what type of site you're on, the worst that will happen is the occasional impulse buy.

Of course, if you're really concerned about your credit information: Your best defense when it comes to keeping your credit card information safe on the Internet is not to use your credit card on the Internet. However, shopping on the Internet – on secure sites – is perfectly safe and a great way to shop (Granted, the "great" part is only my opinion, but the ease of point and click shopping beats the great googly-moogly out of a crowded mall....).

When you shop on the Internet, remember, your common sense is your best weapon. If a site looks a little goofy in the security department & your gut tells you not to enter in your personal information... DON'T!

You can pretty much always trust established businesses such as amazon.com, macys.com, and the like, to have secure servers for credit card and check transactions. If you're unsure about the site, you can see if they're secure or not by looking for the little "secure" icon in your browser. When on a secure page in Internet Explorer, there will be a little padlock icon on the lower right-hand corner of the browser window. Netscape has a similar icon. Secure pages also have the "https://www.domainnamehere.com/secure.htm" distinction in their address as opposed to a non-secure site, which would read "http://www.domainnamehere.com".

If you're fairly new to the Internet shopping scene, Windows (WIN'95, '98 and ME) has an excellent

Windows XP Safe and Secure?

little feature that will tell you exactly what pages are secure and/or not secure on any site.

To access this feature open your browser to any site and on the top toolbar, select "Tools" then "Internet Options", then "Advanced". In the "Advanced" section, scroll down until you see the "Security" options.

Once there, go ahead and check the following boxes:

Warn about invalid site certificates

Warn if changing between secure and not secure mode

Warn if forms submittal is being redirected

Once that's finished, click "Apply" then "OK"

You're finished. Your computer will now tell you when you're on a secure page and warn you when you're on a not secure page.

Still not sure about being secure? Want a step-by-step ILLUSTRATED version of this tutorial? Want lots more FREE computer and Internet tips and tricks? Visit <http://www.sunsetinn.net/guardian.htm>

William Milham is an Internet Professional with more than a decade of experience on the WWW. For more articles and eBooks written by Mr. Milham, please visit www.sunsetinn.net and click on the "Publications" link.



This Free E-Book has been brought to you by Natural-Aging.com.

100% Effective Natural Hormone Treatment
Menopause, Andropause And Other Hormone Imbalances
Impair Healthy Healing In People Over The Age Of 30!