

Choosing Anti-Virus Software

Keywords: Anti-virus; Install; Virus; Error; XP; Vista; Download; Firewall; Problem; Software; Protection

Introduction (Please Read):

This article will provide a perspective on some of the features and issues with security and anti-virus software when working with Windows Vistas. Now that Windows Vista has been available for a while, the comparative performance benchmarks are in.

- [Windows XP vs. Vista: The Benchmark Rundown](#) (Tom's Hardware)
- [Windows Vista Performance Guide](#) (Anandtech)

It's about what I expected; rough parity with the performance of Windows XP. Vista's a bit slower in some areas, and a bit faster in others. **But shouldn't new operating systems perform *better* than old ones? There are plenty of low-level improvements under the hood. Why does Vista only *break even* in performance?**

To be fair, Vista does a lot more than XP. I don't want to get into the whole XP vs. Vista argument here, but suffice it to say that [the list of new features in Vista is quite extensive](#)-- although perhaps not as extensive as some would like. [Vista's integrated search](#) alone is enough for me to banish XP from my life forever.

Microsoft has gotten a giant security shiner from Windows XP over the last five years. That's why Windows Vista goes out of its way to radically improve security, with new features like User Account Control (UAC) and Windows Defender. The existing security features in XP, such as Windows Firewall and System Protection (aka restore points) were significantly overhauled and improved for Vista, too. Enhanced security is a good thing, but it's never free. **In fact, Vista's new security features will slow your PC down more than almost any other kind of software you can install.**

For best performance, the first thing I do on any new Vista install is this:

1. Turn off Windows Defender
2. Turn off Windows Firewall
3. Disable System Protection
4. Disable UAC

I've had friends remark how "slow" Vista feels compared to XP, but when I ask them whether they've disabled Defender or UAC, the answer is typically no. Of course your system is going to be slower with all these added security checks. Security is expensive, and [there ain't no such thing as a free lunch](#).

You might argue that three out of these four security features wouldn't even be necessary in the first place if **Windows had originally followed the well-worn UNIX convention of separating standard users from privileged administrators**. I won't disagree with you. But Windows' long historical precedent of setting user accounts up by default as privileged administrators is Microsoft's cross to bear. I can't rewrite history, and neither can Microsoft. That's why they came up with these painful, performance-sapping workarounds.

But this doesn't mean you have to give up on security entirely in the name of performance. If you're really serious about security, then **create a new user account with non-Administrator privileges, and log in as that user**. This isn't the default behavior in Vista, sadly. Post install, you get an Administrator-But-Not-Really-Just-Kidding account which triggers UAC on any action that requires administrator privileges. I'm sure this torturous hack was conceived in the name of backwards compatibility, but that doesn't mean we need to perpetuate it. The good news is that Vista is probably the first Microsoft operating system ever where you can actually work effectively as a standard, non-privileged user. As a standard user, you get all the benefits of UAC, Defender, and System Protection.. without all the performance drain.

Let me be clear here. I'm not against security. I'm against retrograde, band-aid, *destroy all my computer's performance* security.

Speaking of retrograde, band-aid, *destroy all my computer's performance* security, the one security feature Vista doesn't bundle is anti-virus software. **And nothing cripples your PC's performance quite like anti-virus software**. This isn't terribly surprising if you consider what anti-virus software has to do: examine every single byte of data that passes through your computer for evidence of malicious activity. But who needs theory when we have Oli at The PC Spy. Oli conducted [a remarkably thorough investigation of the real world performance impact of security software on the PC](#). The results are truly eye-opening:

	Percent slower		
	Boot	CPU	Disk
Norton Internet Security 2006	46%	20%	2369%
McAfee VirusScan Enterprise 8	7%	20%	2246%
Norton Internet Security 2007	45%	8%	1515%
Trend Micro PC-cillin AV 2006	2%	0%	1288%
ZoneAlarm ISS	16%	0%	992%
Norton Antivirus 2002	11%	8%	658%

Windows Live OneCare	11%	8%	512%
Webroot Spy Sweeper	6%	8%	369%
Nod32 v2.5	7%	8%	177%
avast! 4.7 Home	4%	8%	115%
Windows Defender	5%	8%	54%
Panda Antivirus 2007	20%	4%	15%
AVG 7.1 Free	15%	0%	19%

The worst offenders are the anti-virus suites with real-time protection. According to these results, **the latest Norton Internet Security degrades boot time by nearly 50 percent. And no, that isn't a typo in the disk column. It also makes all disk access sixteen times slower!** Even the better performers in this table would have a profoundly negative impact on your PC's performance. Windows Defender, for example, "only" makes hard drive access 54 percent slower.

And yet, despite the crushing performance penalty, anti-virus software is *de rigeur* in the PC world. Most PC vendors would no sooner ship a PC without preinstalled anti-virus software than they would ship a PC without an operating system (yeah, [you wish](#)). The very thought of running a PC naked, vulnerable, unprotected from viruses sends system administrators screaming from the room in a panic. When you tell a sysadmin you dislike running anti-virus software, they'll look at you mouth agape, as if you've just told them that you hate puppies and flowers.

I don't see why they're so shocked. anti-virus software itself, while not self-propagating like a virus, certainly fits the definition of a Trojan Horse. Once installed on your system, it has a hidden, unadvertised payload: it decimates your computer's performance and your productivity. In my opinion, **what we really need is Anti-Anti-Virus software to keep us safe from the ongoing Anti-Virus software pandemic.**

I've never run any anti-virus software. And Mac or Linux (aka UNIX) users almost never run anti-virus software, either. Am I irresponsible to run all my computers without anti-virus software? Are Mac and Linux users irresponsible for not participating in the culture of fear that Windows anti-virus software vendors propagate? I think it's braver and more responsible to recognize that anti-virus software vendors are not only telling us to be afraid, they are selling us fear. The entire anti-virus software industry is predicated on a bad architectural decision made by Microsoft fifteen years ago. And why, exactly, would any of these vendors want to solve the virus problem and put themselves out of business?

I'll certainly agree that [you can't stop users from clicking on dancing bunnies](#) if they have their mind set on it. You should have a few different security layers in any modern operating system. But we should also be treating the disease first -- *too many damn users running as administrators*-- instead of the symptoms.

As for remediation strategies, I'm a fan of [the virtual machine future](#). We should treat our operating system like a roll of paper towels. If you get something on it you don't like, you ball it up and throw it away, and rip off a new, fresh one. But if that's too radical for you, I think Jan Goyvaerts is on to something with [good old plain common sense backups](#):

In fact, with a proper backup system in place, you don't have to be afraid of messing up your system. **I don't use any anti-virus or anti-spyware software.** If my system starts acting up, I'll restore the backup, and have a guaranteed clean system. No spyware remover can beat that. If I want to play with beta software, I don't have to inconvenience myself by running it in a virtual machine. I do use VMware for testing my applications on clean installs of Windows. But when beta testing new versions of tools I use for development, I want to test them in my actual development environment rather. When the beta expires, I wipe it off by restoring the OS backup.

It's not terribly different from my virtual machine solution. Either way, you go back to a known good checkpoint. And I'll take a backup strategy over a computer with hobbled performance any day.

This also begs the question of what safety really means. No matter how much security software you install, nagging users with dozens of security dialogs [clearly doesn't make users any safer](#). We should give users a basic level of protection as standard non-administrator users. But beyond that, let users make mistakes, and **provide automatic, unlimited undo**. That's the ultimate safety blanket.

Posted by Jeff Atwood [57 blog reactions](#)

Comments

And since i'm already being pedantic, the definition of Trojan Horse software is not that it destroys your performance or productivity, the definition is that it's hidden inside something else.

This is from the legend of the Trojan Horse, where soldiers hid inside a big wooden horse so they could get into the city of Troy.

And furthermore, "begs the question" means to presuppose that which one is trying to prove. You mean "raises the question".

I hope that helps, have a nice day.

[Kreiger](#) on March 1, 2007 04:20 AM

> definition [of a Trojan Horse] is that it's hidden inside something else.

Right, the complete destruction of your computer's performance is hidden inside the illusory, incomplete promise of security offered by anti-virus software vendors.

It is hidden. If Symantec told people how much slower their computers would be after installing Norton Internet Security, they'd never let it inside the gates.

(the percentages were definitely wrong, though, so thanks for that correction)

[Jeff Atwood](#) on March 1, 2007 04:30 AM

Granted that unlimited undo is available, how can you protect yourself against the mechanism itself being compromised? The idea to throw the compromised state cleanly away is good, but I don't think using that state to undo to a previous, presumably uninfected state will be effective.

[Daniel](#) on March 1, 2007 04:50 AM

I honestly didn't think that ZoneAlarm slowed down my pc that much, at least not to noticeable levels. However, I'm not using version 7 of the engine - which version were you using as apparently they aren't using the same anti virus engine at all? I don't think the latest version supports Vista yet.

Paul Tew on March 1, 2007 04:58 AM

Two things made the difference for me:

- 1) Router firewall: block ports 135 and 445.
- 2) Disable ALL JavaScript (NoScript extension for Firefox).

I still run AVG and Spybot but it has been a long time since they have detected anything.

[Frank Wilhoit](#) on March 1, 2007 05:10 AM

I never run any anti-virus software either, and the only time ever I got a virus was when a roommate got a little insecure and had to read one of THOSE emails, and run the attachment.

However, I'm not sure using virtual machines or backups or anything like that really solves the problem. Viruses by nature attempt to corrupt the system, so even in a VM it will try to do that. If your VM has access to your data drive, the virus will end up on that drive waiting for the chance to break everything. If you backup before you notice the virus, the virus can go with it and destroy your backups.

Mac/Linux users don't worry about antivirus because they don't have to, for the most part. They'll probably have to some day, but right now most virus writers just don't care to write viruses for those systems. You can talk all you want about how secure those OS's are, but users are the weak point in any system.

Telos on March 1, 2007 05:15 AM

Hi Jeff:

You mention in "The Power of Defaults":

"For most users, the default value is the only value. Your choice of default values will have a profound impact on how your application is used."

That's why your friends don't turn off all the new security features in Vista.

Vista IS slower than XP "BY DEFAULT"...

Evidently XP doesn't include ANY security software. That's "the reason" for the lack of performance in Vista.

Well, that AND all the D.R.M. crap (it IS).

Why there is no Kaspersky on the benchmark? Its by far the best anti virus I had used (I'd use ALL of the mentioned above).

Great article as usual.

Saludos...

[Rodrigo](#) on March 1, 2007 05:25 AM

I agree. I've been saying for a long time to many of my associates - if you're a sensible enough person, if you can recognise some of the (not very subtle) signs of a potential virus, etc, and if you run on a standard user account, and not as an administrator, you're fine.

At least, you're fine enough.

I'm happy to sacrifice my largely imagined protection from viruses that I get with virus software and subscriptions for speed. You know, speed. The thing that lets you use your computer and get work done.

X on March 1, 2007 05:26 AM

The day will come when someone produces the necessary analytics software for the masses. It will be Task Manager on steroids. It will be the sunlight we need.

It will tell you what activities -- services, apps, etc -- are consuming disk, CPU, bandwidth

It will combine strong knowledge of what the governing process is. Right now if I want to know what AluSchedulerSvc.exe is, I have to Google it. But this app will know, and it will know that these 5 other services and this running process actually all run for the benefit of this app (Norton LiveUpdate, the pig), and it will be able to tell the user that.

Maybe it's already written; if so I'd love to know about it.

But when it goes mass-market, the cost of anti-virus, and the cost of too many other poorly written memory-resident apps, will hit everyone's radar screen.

John Pirie on March 1, 2007 05:40 AM

I'm have about 6 Windows installations as Parallels images. If I install something, I create a copy before and after the installation. If something goes wrong, I just go back to whenever stuff was still working.

[LKM](#) on March 1, 2007 05:50 AM

I think it totally depends on what you do with your computer, when I was back in University and had no money I had to download certain "tools" from untrusted sources (or do without). I recently switched to AVG because I was sick of all the extra crap that Norton tries to do and it found some viruses in those old archived files that Norton has missed for years.

Now that I've been out in the work force for a few years if I need something I buy it from a trusted source so I don't have as high a risk anymore but working as a software developer I regularly need access to areas and files on my system that would be restricted to a "Power User".

Kevin Taylor on March 1, 2007 05:50 AM

Hey, dunno if you've probbably already all seen this, but i find it holarious

uniquepeek.com/viewpage.php?page_id=534

'How to install Vista'

Fish on March 1, 2007 05:50 AM

On a slightly unrelated note, I wanted to try out Vista on my main desktop machine but it turns out that my Motherboard manufacturer is behind on getting those drivers out. I would think that DFI would be a little faster since it caters to the DIY market of PC Geeks (DFI LanParty NF4 SLI-DR).

I'm also running RAID 0 (and I know the risks which is why I have a rigorous back up routine between internal hard drives, my two other computers and two external hard drives) and I couldn't find drivers for Vista for that either (it didn't like the ones on the floppy that came with the drives and of course no help from DFI either).

Kevin Taylor on March 1, 2007 06:01 AM

I couldn't agree more. I have been running as a Limited User on XP for years without any antivirus software and I couldn't be happier. I simply scan my computer with an online virus scanner every couple of weeks. The one thing I will say is that you really should have antivirus software that simply scans emails. My biggest fear is that I will get a virus in an email and pass it along to someone else (even though it doesn't harm my computer). I can't afford to have that happen when I have clients counting on me. So you don't need full blown antivirus protection all the time. Just email protection.

I also couldn't agree more on the idea that Microsoft has really blown it with Vista. They needed to FORCE people to run as standard users. The time has come to educate the masses. Instead, even so-called "computer experts" aren't getting the message. How many times have you read articles by "experts" claiming that UAC is worthless because users will just learn to click "ok" and ignore it? Well this tells you that they are obviously still running as administrators because if you are running as a standard user you have to enter your username AND password. Not just click OK. So it just shows that Microsoft is obviously not doing enough.

Here are some thoughts on what could have been done.

- 1) Force the user to create an admin AND a standard user account during install. Give ample information as to what each account is for.

2) Do NOT show admin accounts on the login screen. Instead, have a link that takes you to a separate page called "Admin Accounts". On that page put a big warning about what those accounts are used for. Only standard accounts show on the login page by default.

3) When you log in with an admin account, pop up a big warning message that must be cleared EACH time (no checkbox saying "don't show this message again"). Inform the user that the account is only for administering the computer.

4) Allow all of these settings to be overridden using group policy so that people installing servers/appliances or who REALLY know what they are doing can use the computer the way they want too.

Until Microsoft FORCES its users to run in a safe manner we simply won't be able to get rid of things like UAC for administrators.

As a side note, UAC is great for standard users. It is the feature that makes running as a standard user so painless. I just wish that you could turn off UAC on a per user basis. I would turn it off for the Admin account (which I rarely have to log in to) and turn it on for the standard user accounts.

Finally... "But shouldn't new operating systems perform better than old ones? " implies that Vista should be faster than DOS. Hmmm....

Matt on March 1, 2007 06:08 AM

John Pirie said: "The day will come when someone produces the necessary analytics software for the masses. It will be Task Manager on steroids. It will be the sunlight we need... Maybe it's already written; if so I'd love to know about it."

What you want is Sysinternals' free utility, Process Explorer:

<http://www.microsoft.com/technet/sysinternals/ProcessesAndThreads/ProcessExplorerer.msp>

It's not for completely non-technical users, but it definitely fits the description of "Task Manager on steroids"; you even get a one-click way to do web searches for process names so you can figure out what mysterious processes are doing. (Unfortunately, when Microsoft bought out Sysinternals they switched the search engine in Process Explorer to Live Search from Google. At least the tool is still free, though.)

And to Jeff's comment about "too many administrators": What I want is a user account `_between_` administrator and standard. One that will let me install programs, but only into a location that's specific to me (say a "My Programs" alongside "My Documents"), and that'd be limited to programs that don't attempt to modify resources that are shared among all users. Windows' notion of a "standard" user is too limiting and its notion of an "admin" is too expansive, IMHO.

[Jason Lefkowitz](#) on March 1, 2007 06:21 AM

Real-time antivirus software on client machines is for the birds.

Antivirus software on mail servers is essential. Even if you read your mail on Linux, you can be overwhelmed with the bulk of computer viruses during a virus crisis. The world hasn't had a serious virus outbreak for the last few years, but back in the age of MYDOOM and NETSKY, I had addresses that would get upwards of 50,000 messages a day.

I do like Windows Defender. I've found that most Windows machines in real life do have several kinds of malware on them, and Windows Defender does do a good job of removing them.

Windows XP made a good deal of progress towards making it possible to work as a non-admin user. It's sad that Microsoft didn't bite the bullet and move closer to the Unix model.

Alas: Microsoft copied the idea of symbolic links from Unix, which could have been a great boon to Windows administrators everywhere. Unfortunately, the user-space in Windows can't cope with them -- deleting a symbolic link from Windows Explorer or with the DEL command deletes the original file.

Microsoft seems to be as bad as copying ideas from the Unix world as the Unix world is at copying ideas from Microsoft.

[Sailor Moon](#) on March 1, 2007 06:37 AM

I seem to have gotten a lot better performance using Symantec Antivirus (the SMB version). It provides significant control over the real-time scanning and lets me push out common settings to all machines. I turn scanning off for my development and VM partitions to improve performance and limit all real-time scanning to "scan on create" so every file read is not scanned. Email is scanned in and out so I feel pretty good that I've got the borders protected. It does do a memory scan on boot which definitely extends boot time, but that can be turned off. I let it run a full scan weekly, but even when I do use the computer then its not really that bad. (This

may be hardware to - dual core, 10k drive.) So far the price and renewal of a 5 machine license has seemed reasonable.

[Jamie da Silva](#) on March 1, 2007 06:41 AM

Egads! No anti-virus software? No anti-spyware software? And you rationalize that by saying you'll just tear off a new sheet of paper towel and start fresh? Well, great. Without that software, how are you going to know your hands are dirty and you need a new piece of paper towel? You'll have to observe some change in system behavior. What happens if that "change" is your bank accounts are empty because somehow you got a keystroke logger on your system yesterday just before visiting your bank? What if the "change" is that your customers start calling up asking why THEIR bank accounts are empty after installing your freshly compiled and shipped software which contains the same keystroke logger?

You've got to have some kind of software to notify you of bad behavior caused by malware as soon as it manifests. My personal preference is for software that notifies me of malware as it enters the system. Right now, I'm using OneCare on Vista. Unlike most of those other pieces of software you mentioned, OneCare doesn't scan stuff as it enters the system. It either waits for the malware to activate, or it waits for its system-wide tune-up. Then it catches the bad stuff. I don't quite like that method, but it's acceptable. And, it sure beats eye-balling your system behavior as a metric of infection.

David A. Lessnau on March 1, 2007 06:48 AM

Dave A.: I think you are jumping the gun a bit.

#1: Use of a good firewall (I use Tiny Firewall) will tell you when a program runs that doesn't have a hash it recognizes, and will ask you if you want to run it and if you want to trust it.

#2: If you get infected with a program that steals account information like that, chances are its cutting edge and won't be detected by antispy/mal/virus anyways.

The important bit is that you don't let programs freely access the internet. The most secure way IMO is deny all/allow some, not the other way around.

My setup uses tiny firewall (which i think got bought out, lame.), sysinternals process explorer and tcpview, firefox w/ adblockplus, and gmail. I just don't get viruses or malware.

Dan on March 1, 2007 07:08 AM

>But shouldn't new operating systems perform better than old ones?

Has that ever been the case? At best, any performance improvements offset slowness added by new features.

>I've never run any anti-virus software.

I've only just started running AV at home - and only to protect myself from my company's virus infected network when I VPN in. ;)

[Kevin Dente](#) on March 1, 2007 07:21 AM

I've been saying this very thing about anti-virus software for years and am in total agreeance with Dan's post. I also use an older version of Tiny Firewall (before it got bought out and spammed up), block all access and set exceptions where needed. I run a basic anti-virus check online at McAfee once every six-months, use Ad-Aware once a month and in all my years in front of a Windows computer have not ever caught a single virus.

The worst thing is, convincing people that Norton and the like is not a good idea and it actually massively degrades your machines performance and is an absolute nightmare to configure and uninstall (like AOL in fact).

[Chris](#) on March 1, 2007 07:22 AM

Here's my two cents. I'm sick and tired of everyone trying to tell Micro\$oft what to do. People need to realize that these products are not designed and released specifically for "you". Microsoft has to cater to billions of people around the world, and that means that they have to find a common ground for every feature of their OS. If you don't like what their doing, or specific features they've included, find another operating system (there are plenty to choose from). Security vulnerabilities exist in every OS and they always will. Microsoft controls the majority of the user market; which is the reason they are targeted more often.

It's not up to Microsoft to force a user to do anything. Just like it's not up to anyone else to tell me not to smoke, or to tell the fat guy over there to not have that second doughnut. Don't get me wrong, I am in now way condoning what they've done with their new OS; in fact, the thing that irritates me the most is Microsoft telling me what my computer can, and cannot, do. You want a safer computer, then setup a non-admin account yourself, but don't force me to use a user account that is useless to me. Let me decide how I want to run my computer. And if anyone want to argue that the average user doesn't know anything about security, well then

it's time they become proactive and do some research. What are they gonna do if they get a flat tire out in the middle of nowhere and can't get a signal on their cell phone. They better learn how to change a flat real quick. Quit being lazy and expecting people to do things for you. Google isn't that hard to use, so use it. You don't want a virus or spyware, then don't open that email that claims to have nudey pictures of Britney Spears, and don't click on that porn ad.

As far as anti-virus software goes, of course you're going to take a performance hit. If you think you're safe just because you can use system restore to recover those corrupt system files. Think again. Some viruses are capable of corrupting file contained in the system restore folders. It may not have happened the last time, or today, or tomorrow, but it will one day. Think one AV software is better than the other, well then your wrong again. Different AV software may detect viruses that other won't, and vice versa. No one AV software will ALWAYS detect everything, no matter what they may claim. Sure one may run faster than the other, and detect more viruses more often than another, but there will always be that one time when one virus is left dangling in your system32 folder. If you don't want to run AV software well then that's fine too, but don't think that you're not vulnerable to losing everything on your computer because you run an online virus scan once every couple of weeks. Who are you to tell Joe Blow over there that he doesn't need to run AV software, because you don't know what his surfing habits are. And if you're using a separate backup, well then kudos to you because you're in the small percentage that do.

To the System Administrators out there, if you don't have some sort of virus protection on your network because "it slows thing down", then I must tell you that you're a fool. People can flame me all they want, but it only takes one idiot to open that email from the hacker in Thailand and you may never see daylight again because your too busy trying to remove the viruses from every computer in the office. Don't want to run AV on the computers themselves, then put it on the router separating your LAN from the rest of the world, but have something or you're just asking for it.

Well my venting is over, let the flaming begin!!!

Robert on March 1, 2007 07:24 AM

(I like the name. Sometimes quote-success-unquote is truly Worse Than Failure - with failure you have to do it over again better. With "success" you have to live with all the problems, because why would the company spend time fixing something that works?)

Very informative discussion - I think I need to tweak some settings when I get home...

Allen on March 1, 2007 07:38 AM

looks at post

looks at Firefox tabs

reaches for more coffee

Apologies to all.

Allen on March 1, 2007 07:41 AM

And why, after reading the investigation results, did you only comment on the Norton Internet Security 2006 row?

From your table, my conclusion is:

Perfect! I'll just use AVG Free, which does a good job with minimum performance issues.

Why risk a system restore, when a decent antivirus can scan my mail and system files without hogging the system?

[Filini](#) on March 1, 2007 07:42 AM

Bro, you forgot about Kaspersky. Its by far the best right now. Runs only 1 process and the detection % is quite high. Ask CNET they reviewed it and its "By Far"

Mike on March 1, 2007 07:52 AM

I used to think the VM solution was an answer. Before that I was even looking at write-protected flash memory that boots then creates, loads, and transfers control to a RAM drive (a stripped Win95 as a guinea pig). Usable for browsing and as a terminal client but that's about it.

The problem is neither of these work unless you never pesist ANYTHING. Sooner or later your "data" partition (even a NAS share) will get infected. Rolling back to a "clean VM" is no help unless you trash all of your data outside (as well as inside) the VM.

So far the safest technique seems to be to locate machines behind a simple NAT device that doesn't have known exploits, run something lightweight like AVG, delete all spam unread, browse with the highest security settings available, explictly request a scan of anything downloaded before using it, and run with a normal user account

whenever possible. Running Defender as well probably makes sense... though pretty soon we're right back where we were performance-wise.

Bob on March 1, 2007 07:56 AM

Good post, but I still run W2K as I couldn't stomach XP.

You didn't list AntiVir, which I like a lot. Before I bought a router I would get the Code Red (?) virus regularly because I have IIS 5 installed.

When I moved and my cable company came over to hook me up, I asked if I should install my router first and they said "no, we have anti-virus software". Well, after they left I found I had a nasty one, caught by AntiVir.

A router, Spybot (which catches stuff each time I run it), AntiVir, PestPatrol, Firefox and I have a very snappy machine with no re-installs in almost 2 years and hardly ever an issue.

[Steve](#) on March 1, 2007 08:07 AM

John Pirie: There is a pretty good process-based performance monitor built in to Vista. Open up task manager, click the Performance tab, and click the "Resource Monitor" button.

However, do NOT follow these steps if you're a non-admin user with UAC disabled. Task manager will go into a loop of restarting itself over and over as fast as possible and you won't be able to stop it without rebooting.

[c](#) on March 1, 2007 08:20 AM

Silly rabbit, dual core processors and gigs of ram is not for gaming, it is for that antivirus suite.

Dave on March 1, 2007 09:08 AM

Here's the thing, and I speak as a man that has used Mac (7,8,9,X.1,X.4), Linux (too many distros to list) and Windows (98SE, 2000,XP)... Anti-Virus software is only necessary if you're a dumb-ass. Those same SysAdmins that look at you mouth agape also secretly harbor the opinion that you're a knuckle-dragging moron that will click on every banner, download from every prompt and install every open-ended malicious piece of software you can get your mitts upon.

And if they're a typical user who doesn't understand safety, well, they're probably correct. Not that they mean to be that way, it just happens through lack of education. But if you've got a good knowledge of your system, understand what you're downloading and from whence it comes, you're pretty safe. If you're unsure, run a virus scan pre-install and post-install. No need to have constant vigilance if you're not installing some crappy new thing or another every single day.

I keep a copy of AVG Free 7.1, which I almost never allow to run its automatic scan. I know what I've installed on my system, I know what's malicious and what isn't. If it's malicious, I avoid it. I use a closed browser, FireFox, with additional security measures added into the mix. I avoid file-sharing, gray-area downloads and the like. I don't have virii on my computer simply because I don't let them into my system. GMail protects my email (and it being web-based means I have access to it anywhere, any time, and as long as I'm using FireFox, I'm basically secure).

Most users, however, aren't educated. I educated my parents: time and again I told them "If you aren't sure, ask me. If you are sure, ask me. If you're 100% positive, just ask me." Then I explained. After awhile, they stopped needing to ask me. As far as I know, they never get viruses anymore. Of course, I pounded the basics into their head early. AVG, SpyBot, Ad-Aware, HijackThis. I make them install HijackThis, but they still have me look the list over before they disable anything.

Frankly, an informed user is a safe user. The only thing you really need is a simple firewall, because DoS attacks are just /so/ 1993.

[Jae](#) on March 1, 2007 09:08 AM

I'd love to run without anti-virus and anti-spyware, but children (especially teenagers) are incredibly adept at filling any PC with trojans and viruses in a matter of minutes. They even know how to bypass most internet filter software. I sometimes think children are viruses!

Jimbo on March 1, 2007 09:15 AM

Jimbo, set up their computer as a non-admin and your troubles will simply disappear. That is the main message in this blog post. But it seems to be lost on so many users and so-called "experts".

Quit running as admins. Quit making excuses. After that, if you feel more comfortable using antivirus software as well, then do so.

Matt on March 1, 2007 09:24 AM

I agree with Jimbo, sometimes you have to protect your PC from your own family!

You put a wolf in bunny suit and everytime most users click on it until the word comes out that the bunny is bad.

How about real punishment for virus, malware, spyware creators? No viruses, no anti-virus programs needed.

Conspiracy Theory - 50% of Norton Anti-Virus Employees write Anti-Virus software. 50% of thier employees write viruses...

Jon Raynor on March 1, 2007 09:42 AM

Matt - you're assuming the children have their own computer! Back in the real world, there's one family PC and it's needs are too varied to have a single non-admin user. I tried the multiple XP users approach, and that was an appauling experience - I was forever trying to find lost homework for the kids!

I'm a developer, not a net admin, so the easiest of several approaches has been to protect the PC to the hilt (minus on-access scan), then turn it all off when I get a chance to play with it! :D

Jimbo on March 1, 2007 09:54 AM

Jeff, are you running normally from an admin account, yourself? It sounds like you are. Because you suggest to turn off UAC, and if you run as a standard user, isn't UAC effectively just a convenience allowing you to do admin-ish things without having to explicitly switch users over to the admin account? (That's how I think it works, anyway, on my system. Otherwise, if a standard account could do admin-ish things without UAC and entering the password, it would essentially be an admin account.)

If you don't run from a standard account, why do you expect everyone else to?

LintMan on March 1, 2007 09:57 AM

> sometimes you have to protect your PC from your own family!

Wouldn't it be easier/better to have virtual machines for each family member? And inside the VM they are running as standard, non-privileged users?

The only risk in a VM is that any local data/content you've created would be lost or compromised in some way.

[Jeff Atwood](#) on March 1, 2007 10:00 AM