Computers and Stuff.

Sam Houliston.

Is there a last reprieve for the enduring Windows XP?

By now, every Windows XP user and his third cousin should know that on April 8, the clock runs out on the venerable OS.

There are people who say provided you "do this and/or do that" you *should* be ok. My advice, don't believe it, after the 8th April you are completely on your own and very vulnerable to those "sick" people who get their jollies from writing all sorts of viruses, Trojans, malware stuff and/or who want to get into your computer and pinch all your files or all your money.

As the Walrus says, "The time has come" – UPGRADE now!!

The Internet.

If you're interested in how the internet works, and would like to know in language that you can understand, see HERE

JavaScript.

You hear a lot about JavaScript. Some people say having JavaScript on your computer is no different from having a great big open door with a sign saying "Viruses this way". Is this a fair description of the software or is it all wild hysterics.

JavaScript makes the type of web pages we have and enjoy today possible and while it is easy to disable JavaScript, it would be a lot of annoyance for little benefit. In reality, the security benefits of disabling JavaScript are dubious, it's a case of cutting off your nose to spite your face.

What is JavaScript?
JavaScript isn't the same thing as Java. JavaScript and Java aren't really related at all, aside from the name. JavaScript is a programming language used on web pages. JavaScript was

initially pretty basic and was used for things like alert boxes and menus that appeared when you hovered your mouse over elements on the page. However, JavaScript isn't just used for such minor things anymore. It's the language that powers modern web apps, allowing web pages to dynamically load and send content in the background without page loads and do other dynamic, interactive things. Most websites use JavaScript to provide various features.

JavaScript is built into your web browser – Chrome, Firefox, Internet Explorer, Safari, and Opera all have their own JavaScript engines. Unlike Java (with its yet-to-be-discovered security holes) Javascript is not a plug-in produced by a single company. It makes more sense to disable or remove Java than to disable Javascript.

Java is the one that should be disabled or even better, should be removed from your computer – not JavaScript.

If you disable JavaScript, many websites, like Gmail, won't work properly. When you perform a search on Google, JavaScript allows you view these images seamlessly.

So, why do people disable JavaScript?
Many people who disable JavaScript do it because of a perceived security benefit. There have been a few browser vulnerabilities that were exploited via JavaScript, however, this is extremely uncommon and the rare security holes in JavaScript engines have been patched very quickly. Most websites use JavaScript – it's what makes the web we have today possible. In contrast, Java has had a never-ending series of security holes. They're often not patched very quickly – in fact, the Java plugin is still vulnerable today. Java seems to spend most of its time with unpatched security holes, waiting to be exploited.

Very few public-use internet sites use Java. Creating properly signed and trusted Java items is a lot of trouble for small players and is reportedly something cybercriminals can do, which makes it difficult to know how safe running a bit of Java from a public we site might be. Probably you'll get by OK without it.

However Java applications running on a corporate intranet are an entirely different matter. Security issues are completely different when the organisation writing the code is the same as the organisation running it, and in that environment Java offers the advantage of platform independence, ie you can run the same code on Windows Mac or Linux.

How You Can Be Infected via Your Browser, and How to Protect Yourself.

In a perfect world, there would be no way for your computer to be infected via your browser. Browsers are supposed to run web pages in an untrusted Sandbox, isolating them from the rest of your computer. Unfortunately, this doesn't always happen.

Websites can use security holes in browsers or browser plugins to escape these sandboxes. Malicious websites will also try using social-engineering tactics to trick you.

Insecure Browser Plugins
Most people that are compromised through browsers are compromised through their browsers' plugins. Oracle's Java is the worst, most dangerous culprit. Other browser plugins, particularly Adobe's Flash player and PDF reader plugins, also regularly have to patch security vulnerabilities. Adobe has become better than Oracle at responding to these issues and patching their plugins, but it's still common to hear about a new Flash vulnerability being exploited.

Plugins are juicy targets. Vulnerabilities in plugins can be exploited across all different browsers with the plugin across all different operating systems. A Flash plugin vulnerability could be used to exploit Chrome, Firefox, or Internet Explorer running on Windows, Linux, or Mac.

To protect yourself from plugin vulnerabilities, follow these steps:

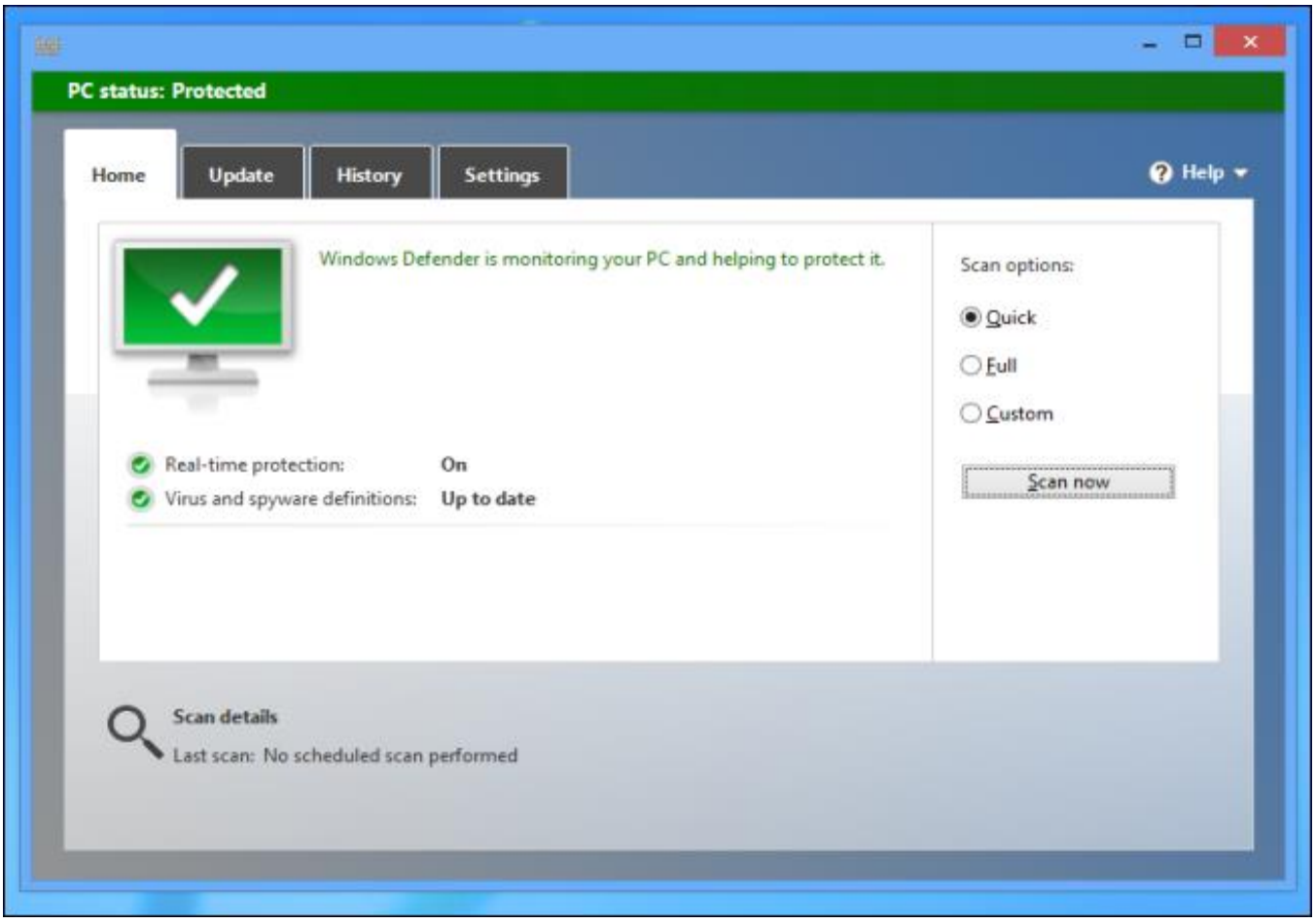
- Use a website like Firefox's plugin check to see if you have any out-of-date plugins. (This website was created by Mozilla, but it also works with Chrome and other browsers.)
- Update any out-of-date plugins immediately. Keep them updated by ensuring automatic updates are enabled for each plugin you have installed.
- Uninstall plugins you don't use. If you don't use the Java plugin, you shouldn't have it installed. This helps reduce your "attack surface" – the amount of software your computer has available to be exploited.
- Consider using the click-to-play plugins feature in Chrome or Firefox, which prevents plugins from running except when you specifically request them.
- Ensure you're using an antivirus on your computer. This is the last line of defence against a "zero-day" vulnerability (a new, unpatched vulnerability) in a plugin that allows an attacker to install malicious software on your machine.

Browser Security Holes.
Security vulnerabilities in web browsers themselves can also allow malicious websites to compromise your computer. Web browsers have largely cleaned up their act and security vulnerabilities in plugins are currently the main source of compromises.

However, you should keep your browser up-to-date anyway. If you're using an old, unpatched version of Internet Explorer 6 and you visit a less-reputable website, the website could exploit security vulnerabilities in your browser to install malicious software without your permission.

Protecting yourself from browser security vulnerabilities is simple:

- Keep your web browser updated. All major browsers now check for updates automatically. Leave the auto-update feature enabled to stay protected. (Internet Explorer updates itself through Windows Update. If you use Internet Explorer, staying up-to-date on updates for Windows is extra important.)
- Ensure you're running an antivirus on your computer. As with plugins, this is the last line of defence against a zero-day vulnerability in a browser that allows malware to get onto your computer. If you're using a PC, Microsoft's Security Essentials, which is free to download, is very good.

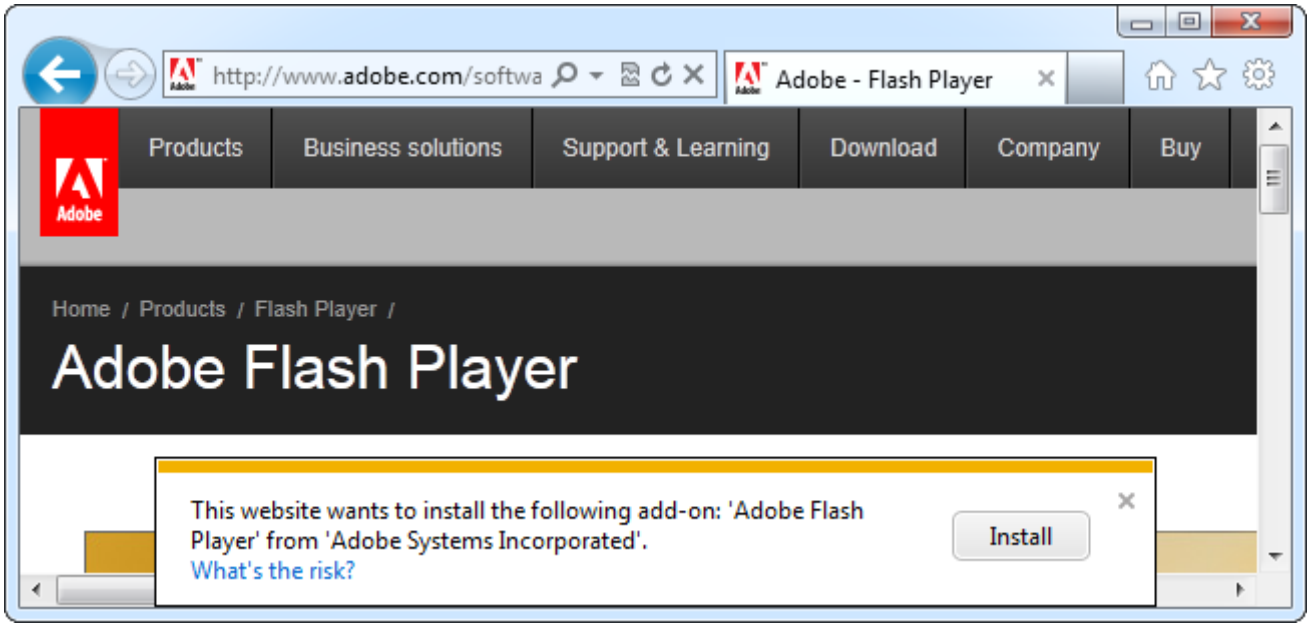


A clean house is a sure sign of a broken computer.

Social-Engineering Tricks.
Malicious web pages try to trick you into downloading and running malware. They often do this using "social engineering" – in other words, they try to compromise your system by convincing you to let them in under false pretenses, not by compromising your browser or plugins themselves.

This type of compromise isn't just limited to your web browser – malicious email messages may also try to trick you into opening unsafe attachments or downloading unsafe files. However, many people are infected with everything from adware and obnoxious browser toolbars to viruses and Trojans via social-engineering tricks that take place in their browsers.

ActiveX Controls.
Internet Explorer uses ActiveX controls for its browser plugins. Any website can prompt you to download an ActiveX control. This can be legitimate – for example, you might need to download the Flash player ActiveX control the first time you play a Flash video online. However, ActiveX controls are just like any other software on your system and have permission to leave the web browser and access the rest of your system. A malicious website pushing a dangerous ActiveX control may say the control is necessary to access some content, but it may actually exist to infect your computer. When in doubt, don't agree to run an ActiveX control.



Auto-Downloading Files.
A malicious website may attempt to automatically download an EXE file or another type of dangerous file onto your computer in the hopes that you will run it. If you didn't specifically request a download and don't know what it is, don't download a file that automatically pops up and asks you where to save it.

Fake Download Links.
On websites with bad ad networks – or websites where pirated content is found – you'll often see advertisements imitating download buttons. These advertisements try to trick people into

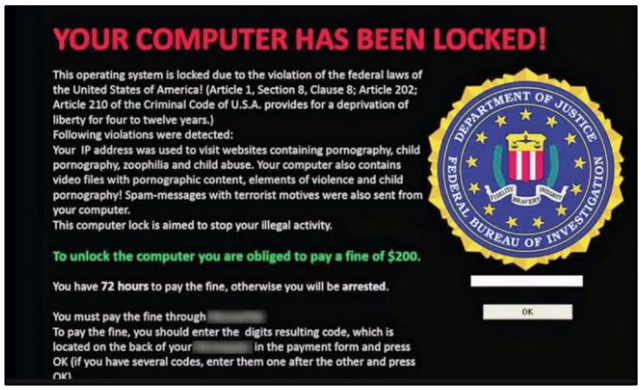
downloading something they're not looking for by masquerading as a real download link. There's a good chance links such as this one contain malware.

You Need a Plugin to Watch This Video.
If you stumble across a website that says you need to install a new browser plug-in or codec to play a video, beware. You may need a new browser plugin for some things – for example, you need Microsoft's Silverlight plugin to play videos on Netflix – but if you're on a less-reputable website that wants you to download and run an EXE file so you can play their videos, there's a good chance they're trying to infect your computer with malicious software.

Your Computer is Infected.
You may see advertisements saying your computer is infected and insisting you need to download an EXE file to clean things up. If you do download this EXE file and run it, your computer probably will be infected.

This isn't an exhaustive list. Malicious people are constantly on the look-out for new ways to trick people. As always, running an antivirus can help protect you if you do accidentally download a malicious program.

Ransomware!!



Security experts warn of growing threat of ransomware. Imagine turning on your computer and finding all your files have been taken hostage. You have just three days to pay a ransom or you lose the data forever. Computer security companies say it is a scenario more Australians are likely to face over the next six to 12 months.

CryptoLocker, a piece of malicious software which runs on Windows operating systems, is a major concern, says Sean Kopelke, director of technology at computer security company Symantec. "It encrypts your files and then demands a modest ransom in return for a unique key to unlock the files". It may have the name of a B-Grade Hollywood thriller, but CryptoLocker has already caused enormous headaches throughout the United States and the United Kingdom.

In Australia, at the moment, we're seeing about a 2 per cent infection rate, which is sort of low but growing quite rapidly. In the US and Europe the rates are much higher and it is said they're quite good early indicators for us. The Australian Communications and Media Authority says the malware is most often spread by email. It's sent out by cyber criminals ... a user clicks on

the email and then the program runs quietly in the background. It's not until CryptoLocker is finished locking up the files that a ransom message appears.

Real estate agents, a Sydney council, a medical centre and the Queensland University of Technology have already been attacked.

The virus encrypts not only all of your local drives but it encrypted all of your shared drives it can see. Ransomware is not new, it is just getting more sophisticated. CryptoLocker's code is currently unbreakable and the ransoms are generally quite modest, often less than the cost of getting help. If they penetrate someone's machine and lock up mum and dad's family photos of the kids, that's something we're emotionally attached to and we want.

"There's no doubt Ransomware is here to stay and we will see more of it in years to come - the criminals will already be working on the next new program – so be careful. Don't download anything with an .EXE extension unless you are 100% sure of the program.

Is your free AV tool a 'resource pig?'

Windows Secrets put six popular, free antivirus tools through their paces and measured their impact on startup and shutdown times, disk space, and RAM use.

Windows Secrets
Everything Microsoft forgot to mention.

It has been suggested that Microsoft's Security Essentials (MSE) adds time to your computer's boot time – but does it?? It was time to compare MSE with other free AV programs.

These AV programs were not checked for their ability to detect and remove viruses and malware as most are considered acceptable and some even excellent.

The following programs were selected for comparison:

- **Microsoft Security Essentials.** (site)
- **Avast Free Antivirus** (site)
- **Avira Free Antivirus** (site)
- **AVG Technologies' AVG Anti-Virus Free** (site)
- **Comodo Antivirus** (site)
- **ClamWin Free Antivirus** (site)

To produce this comparison, a fresh, clean, fully up-to-date Windows 7 SP1 installation in a virtual PC (VPC) was used. This was then cloned (copied) 5 times which meant there were six identical virtual PCs. Piriforms CCleaner was then added to each VPC.

	Startup seconds
MSE	36
AVG	53
Comodo	43
Avast	40
Avira	83
ClamWin	35

One of the six AV tools was installed on each VPC, accepting whatever default settings the apps set at installation. When

prompted, they were allowed to update themselves and run an initial, post-installation scan. Next, each VPC was rebooted to make sure the setup was 100 percent complete and running normally. Any and all installation file(s) were then removed using CCleaner to make sure nothing was left over from the setup that would affect the tests.

Each VPC was then powered off and on again 3 times and the times were recorded and averaged. The times given at left are the averages of the three runs. (The green is the best, the red the worst).

Windows' startup happens in two parts, the initial system bootup before the sign-in prompt, then the time Windows takes to load user settings (from sign-in to the full appearance of the desktop). All 6 VPC were started and timed the same way and the times recorded.

As you can see, the open-source ClamWin offered the fastest average startup time (about the same as starting up the PC without AV software), closely followed by MSE. Avira had a significant impact on startup — more than double the fastest three products.

In this test setup, MSE doesn't have any real impact on startup time. In a real-life situation, very few PC users will notice the one-second difference between ClamWin's 35-second boot and MSE's 36-second boot.

On the other hand, Avira's 83-second average boot is quite noticeable. In fact, Avira's boot was so slow, it was thought something was wrong with the setup and so it was done again from scratch but the results were consistent — consistently awful.

Measuring the effects on shutdown times was simple, the stopwatch was started at the same time as the Shutdown button was clicked then stopped when the VPC session stopped. The results are at left.

	Shutdown seconds
MSE	11
AVG	12
Comodo	14
Avast	11
Avira	13
ClamWin	8

Although there were differences in shutdown times, they were much smaller than with the startup times — too small to worry about. ClamWin again was the fastest, its eight-second time stood out among the six apps. At 14 seconds, Comodo was the slowest — but it was only three seconds slower than MSE and Avast, the two second-place finishers.

To measure the amount of disk space each of these apps occupies, Windows Explorer was used to view the properties of the C: drive on each VPC - the amount of disk space available before and after installing each anti-malware app was recorded.

	Disk footprint (GB)
MSE	-
AVG	+0.2
Comodo	-0.6
Avast	0
Avira	0
ClamWin	-0.3

MSE use of disk space was set as the yard-stick and the other programs disk usage was shown as more or less than that of MSE. The table at left shows the results, ie: AVG uses 0.2GB more than MSE but Comodo use 0.6GB less than MSE.

Disk-space use varied only negligibly. Unless your hard drive is near capacity (in which case you have more pressing

problems than the AV software footprint), there are really no significant differences among the six products. In today's era of 750GB and larger drives, disk space use should not be a factor in picking one of these AV products over another.

For RAM use, after waiting 5 minutes after installation, Task Manager was checked in each system to see how much RAM was in use before and after the apps were installed. To make the RAM-utilization numbers easy to understand, once again MSE's results were used as the yard stick.

	RAM footprint (MB)
MSE	–
AVG	+2
Comodo	+76
Avast	-13
Avira	+139
ClamWin	-1

The table at left shows the results.

RAM use varied significantly. Avast consumed the least amount of RAM — 13MB less than MSE, AVG and ClamWin were on par with MSE, but Avira used a whopping 139MB more.

Summing up antivirus-software resource use.

The table below shows all the results, for easy side-by-side comparison. The best results are shown in green, the worst in red. The immediate conclusion, at least in these controlled-environment tests, is that MSE is not the "resource pig" some PC users think it is. In fact, it offers respectable, near-best numbers in every category.

If there's one app that consumes more PC resources than its competitors, it's Avira, with the heaviest RAM use and significantly slower startup time.

ClamWin is a pleasant surprise; it performed well in every category and earned two "best of breeds," however, because it's a relatively new product and is used by a relatively small number of people, we wouldn’t recommend it.

For our money and for personal use, Microsoft Security Essentials is hard to beat. It's free, it's in widespread use and it has proven itself in the real world. And on most systems, it has little effect on system resources.

Bear in mind that this is a snapshot taken at a particular point in time. Run the same comparison six months later using Windows 8 rather than 7 and the numbers are likely to be completely different. But this does serve to show that there is a difference between these products that the normal user is likely to notice.

It’s your choice though.

A Yawn is an honest opinion openly expressed.

Test-driving 'free scan' tune-up suites.

Everyone has seen them, you download something then a little while later, up pops a program that offers to scan your computer “completely free” and tell you if there are any problems – and if it finds any, will offer to fix them for you. So! With nothing to lose, you say yes and off it goes, impressively scanning the whole box and dice - then bingo!!

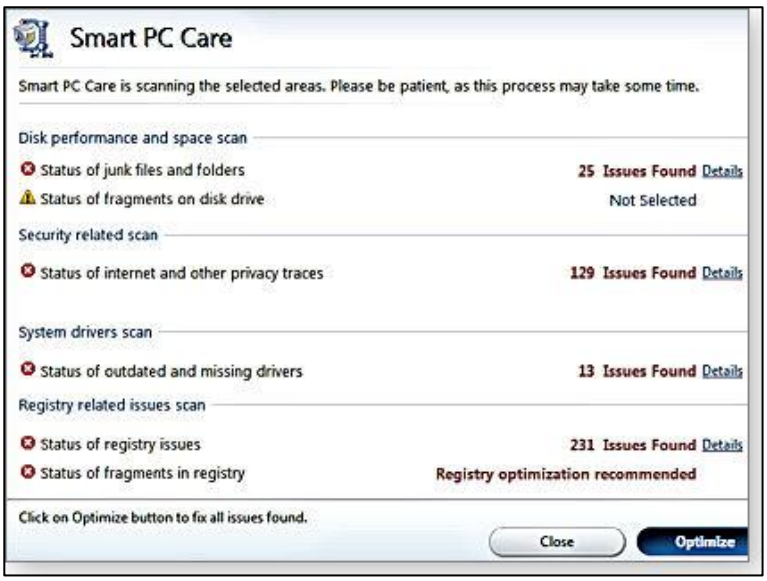
Even on the best maintained systems, these free system scanners always find hundreds of "problems," but when you click the “Fix Problems” button you get a surprise. This is where you discover that to fix the problems you need to download the full program, and surprise, surprise, there is a charge, usually $29.95 or $39.95.

We thought it would be a good idea to check and see if these problems were really problems or just a way to sell “fixit” programs. No PC is perfectly clean after even minimal use but we know ours is free of ‘baddies’ as we keep a close eye on it, so we decided to use it to check the system scanners.

It was decided to test three “Free” system scanners,

1. Corel's WinZip System Utilities Suite.
2. Norton PC Checkup.
3. AVG PC Tuneup.

Corel’s program is free to scan but requires you parting with $40 to fix things. The scan was run and returned the result shown below right. (“Smart PC Care” is part of the suite.) That’s a total of 398 problems – it’s a wonder the machine ran at all. This definitely called for a closer look.



Clicking the *details* link for each problem resulted in some surprising results.

The 25 problems found in the junk files section were normal and harmless, files that have been temporarily cached by the browser, any cleanup tool could remove them.

The 129 issues in the ominous-sounding "Internet and privacy traces" category turned out to be ordinary browser cookies – completely normal and harmless. Calling ordinary cookies "privacy traces" could inflate their perceived threat in the minds of unwary users, inaccurately suggesting serious security problems that do not exist. Next to be checked were the 13 out-of-date or missing drivers WinZip reported and funnily enough, when the PC manufacturer's official driver update tool was run it reported that all the drivers were fully current. None of the computer’s drivers needed updating. This is bad form as needless driver updating can destabilize a PC or even cause

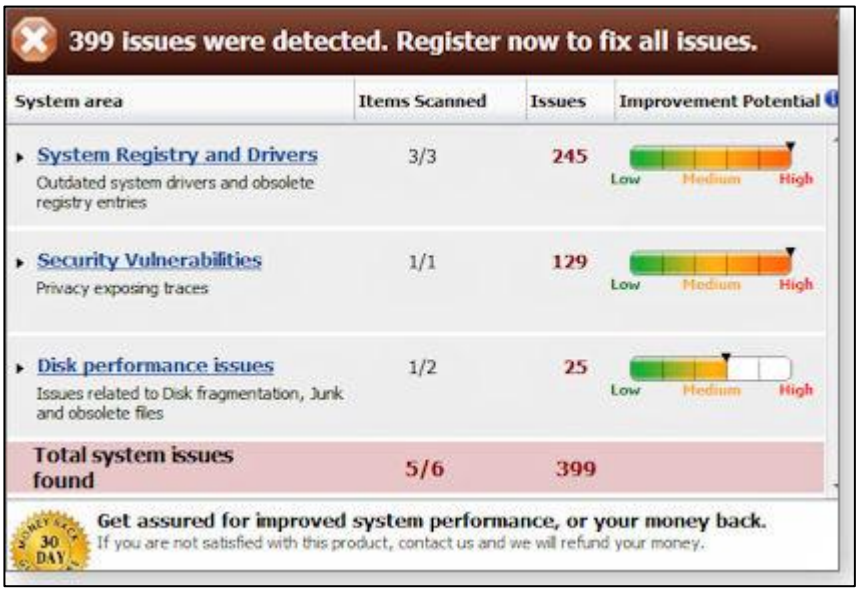
working hardware to fail, so this portion of the WinZip report was completely wrong — and *potentially dangerous* to the health of the PC.

Next to check was the report that found 231 registry issues on a freshly cleaned system. This turned out to be a mixed bag as although some of the items were real they were mainly trivial. Most were files associated with uninstalled programs and the wasted space used by the entries is minuscule. Other issues were too vague to call. For example, it's hard to tell what was going on with most of the 138 "orphaned" ActiveX and COM objects. Would removing all 138 references save a lot of space? Answer – No!!

All of this seems designed to make your PC appear to be in dire need of paid-for repairs, when in fact there appear to be no real operational problems.

Similar results with Free Norton PC Checkup
Its report was less detailed than WinZip System Utilities Suite's, but it produced almost identical results, claiming to find 399 "problems" on my system. See Figure below.

There's no point in going into detail because, on examination, almost all of the Norton-reported issues closely paralleled those reported by WinZip: harmless cookies (some created by the Norton site itself) reported as security "vulnerabilities," fully up-to-date drivers being reported as obsolete, and so on.

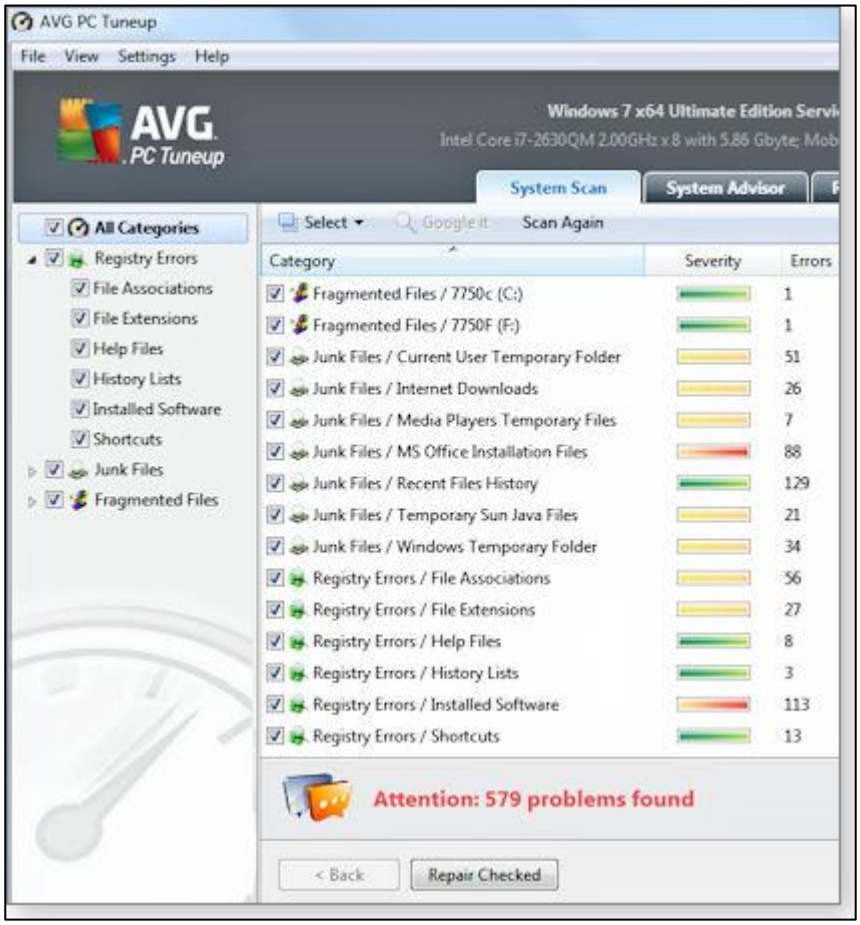


But Norton had some major faults all its own.

It reported that the Windows firewall was disabled (it was not), and it reported that the PC had startup "speed issues." This was curious because the Norton software did not actually time the system startup. If it had, it would have seen the system boot to the Windows desktop in about 12 seconds, which most would agree isn't slow at all.

Once again, you can download and run Norton PC Checkup for free, but it makes no repairs until you pay $70. The repairs are then effected by a live tech using Remote Assistance to take over your PC and make adjustments for you. Don't bother!!

AVG's PC Tuneup
This set the record for the day, reporting almost 600 problems (see right) on a clean and stable PC. Same as the others, it's free to download and run but when you want it to do something it cost $35. Once again, don't bother!!



Like the other products in this article, AVG's PC Tuneup can find some legitimate problems on your system, but like its competitors it has inflammatory language, exaggerated problem counts, and in some cases, offer potentially dangerous fixes.

With only three products in this test-drive, nothing here should be taken as a blanket condemnation of this class of software however, they clearly seem to be aimed at inexperienced users who are more likely to purchase "repairs" when confronted with frightening reports of critical and numerous system problems.

My recommendation – don't bother with any of them!!!