# Linux Lessons: Do I need an antivirus program in Linux?

“**Recent Linux converts may wonder just how secure their Linux box is.”**
by Pete Choppin

The question really is, "Do I need any antivirus software (at all)?" A question Windows users and recent Linux converts often ask, making a rather linear, one-for-one comparison between Windows and Linux—a classic mistake. There is much debate on this. Rather than take sides, let's examine this very crucial, if very simple, question and see if we can come up with an answer.

And the simple answer is: No, you do not need an antivirus program in Linux.

## First, a Secret

There is a dirty little secret, which, if you really think about it, is kind of obvious. You don't really need an antivirus program in Windows, either. Now, the simplicity of this statement is too much to bear for most Windows users, especially people indoctrinated to believe the only thing keeping their system safe is the one little program called antivirus.

In some specific cases, antivirus software might be useful in helping the user decide whether the execution of a certain program might be malicious, harmful or detrimental to the health, integrity and security of his/her operating system and/or data. But the emphasis is on the word might.

A much better, fool-proof security is achieved by the right kind of strategy and a reasonable, layered approach to identifying threats and mitigating them. Blind fear and sheep-headed reliance on brand names is never good practice, nor will it ever make your system secure.

ComputorEdge may focus an article on Windows security and safe Web practices in the future, but this article is mainly intended for Windows users mulling a move to Linux and new, less experienced users wondering how secure their Linux box is.

Suffice it to say that a combination of keeping your Windows system updated, as well as using good Web browsing and e-mailing practices, will keep you safe. Exploiting security holes in Windows is another matter entirely, but security vulnerabilities and virus risks are two different subjects. I will try to address some of this by comparing Linux and Windows with regards to their security approaches.

## User Accounts

While Windows has always struggled with providing the world with a multiuser working environment, where there's only one admin and lots of ordinary users with limited computing powers, Linux has always done this well. Based on Unix, the operating system created from these very foundations, Linux manages to have you enjoy utmost productivity with relatively low privileges. You need not be admin to perform 99 percent of tasks.

True, in Windows you have the same mechanisms, called Limited User Account and more recently, the combination of these limitations and User Account Control (UAC), which provide a rather decent security for the user. But it can still be flaky, because most programs for

Windows are created by people with the admin attitude, which makes it easier to code and deploy the software, but makes it more difficult to secure the box and prevent errors.

By running as user, by default, Linux makes both user-triggered errors and external attacks smaller in scope. While nothing can prevent deliberate self-destructiveness, the right permissions can prevent users from causing accidental damage.

This does not mean you can throw caution to the wind. Users still have full control of their own content. Nothing is easier than deleting your own files. But taking the self-inflicting metaphor further, you can still easily cut off your own arm in Linux too.

But the system remains intact. Most configurations cannot be read, let alone be changed by ordinary users. The only account in Linux that has full system access, called root, can do that. Or users that have been granted the right privileges, using the mechanism called sudo. But even then, it requires interaction and providing the right password.

Against a clueless user and automated attacks, the user account is quite sufficient. But it is not impregnable. And software does occasionally have vulnerabilities, which can be locally and remotely exploited to grant higher privileges or access to system files.

Which brings me to my second point.

**System Updates**

You have system updates in Windows, too, no big deal. The difference is, Windows updates are only available for Microsoft products. This means that programs downloaded manually will have to be periodically updated separately. Some programs make it very easy to keep them up to date, for example Firefox and Opera browsers, both of which check for patches and install them automatically, without any great hassle for the user. Others require that you uninstall the existing version, reboot, etc. All in all, almost every single Windows user is running at least a portion of his/her programs out-of-date.

This is not necessarily a bad thing. But it could be. Some programs may have vulnerabilities and they won't be solved until you proactively fix them. But when you have tens of programs waiting for updates, this can be a serious nag. The lack of desire to maintain your machine and just run it and enjoy, the fear of things breaking up, and plain simple forgetting to update them all add up into making your system less secure than it might be.

Up until Windows 7, Microsoft updates came only once a month. Even now, they are not that frequent. This means that you were running the risk of using an operating system with potential problems for up to a month without a known resolution.

Now, let's see what happens on Linux.

Linux distributions ship as a whole—from kernel, the heart of the operating system, to every single application installed. Your distribution includes not only the critical components, it includes fonts, programs, drivers and everything else. And when you update your Linux system, you update everything.

The built-in update-management utilities with daily checks are a common thing in pretty much every single Linux distribution. You merely need to confirm the installation of available packages. You do not need to think about what needs updating, when or why. The entire thing is done automatically. It's the perfect solution for the lazy and the forgetful, as well as less knowledgeable users who won't bother with computer maintenance.

Furthermore, the distribution updates are quite frequent—every day, minimizing the window of risk when your system is exposed. Then, there's also the question of reboot. Unlike Windows, which requires frequent reboots after updates, most Linux distributions will ask for a restart only when core components are replaced, far less frequently than you're used to in Windows, making the desktop experience more streamlined and pleasant. You can actually like the system updates and not treat them as a hassle.

So the beauty of Linux system updates is you get updates for everything, including the tiniest programs, themes, fonts, icons, kernel, drivers, security patches, bug fixes, everything. All in one mouse click. Your instant messenger, your e-mail client, your browser, your office suite, your microblogging software, your Web camera drivers, your graphic drivers—every single components gets updated, automatically, all the time.

**Availability of Software**

Many Windows users look for programs online, going from one site to another. There are many good programs available, some of which can be downloaded from official vendor sites, others waiting for you in megasoftware index sites like Softpedia, Download.com, MajorGeeks and others. Using these is quite safe and recommended. This is the best way to ensure you get the content you want, without any undesired surprises.

Unfortunately, too many Windows users do not know where to look for software, often visiting the wrong sites, downloading the wrong software or even malicious software. Then, there's the use of cracked and pirated software, which adds yet another element of uncertainty into the equation.

In comparison, Linux users manage all their software using a centralized utility called package manager, which is tightly integrated with the update manager. The utility is a window to the software repositories provided by the distribution you're using, where you can find tons of applications, tools, utilities and drivers for your system.

The repositories contain free and sometimes non-free (proprietary) software, including popular items like Nvidia drivers, Skype, Google Earth, Opera and many others. The content is digitally signed, so that when you download from the repositories, you know you're communicating with the real server and not a rogue, fake one. The use of digital signatures also makes software quality control easier and safer, reducing the chance of wrong or bad versions being either accidentally or maliciously pushed to the users.

The combination of frequent security updates for the entire system and digitally signed repositories that contain pretty much everything, both managed without even once using your browser and visiting this or that site searching for software, makes the chance of a Linux user stumbling upon a malicious piece of software rather slim.

Even in Windows, if you stick to reputable sources, download only from official Web sites and avoid pirated binaries, your chances of getting hit by a bad file are very, very low. In Linux, it's much lower, plus you have the enormous advantage of centralized software management. You simply don't need a reason to go about wandering and making mistakes.

**Distribution Diversity**

There are hundreds of Linux distributions around. Even though many are based on just a few big ones, cross-distribution compatibility is not that big. Sometimes you may run code built for another distribution on your own, but mostly, you will be forced to run packages specifically tailored for your own distribution.

RedHat code won't immediately run on Debian and Slackware code won't run on SUSE. Underneath, they're all the same, but different packaging and small nuances in the system conventions make the task of creating Linux malware more difficult. With hundreds of distributions and hundreds more different editions of said distributions available, writing malicious code that will target them all is near impossible. Windows is fairly easy, with just a few major versions, all rather compatible. For example, you can run DOS code on Windows 7 with a bit of sleight of hand. But try running a package meant for Ubuntu Heron on Jaunty. Just a year apart and yet you'll get into a lot of trouble.

The vast, almost infinite number of permutations containing kernel versions, patch levels, packaging, desktop environments, and software suites makes the Linux malware game a lottery.

It is possible to target specific versions, but it's a lot more work than doing the same thing in Windows. Low-hanging fruit is easier to pick. And let's face it. The virus writers simply do not want to put that much work into their efforts. It's not like they're getting paid to write their malicious software.

**Advanced Skills**

Using Linux is different than Windows. And it is not a given. While most computer users have been pretty much born with Windows in their mouth, Linux exists in a community of incredibly knowledgeable users less prone to accidentally ruining their system.

One of the main reasons for this is the fact Linux has to be installed manually, a procedure that is beyond the skill of most computer users worldwide. So is Windows installation, for that matter, but Windows comes preinstalled and prepackaged, whereas Linux is open-source software. Distributions build their own OS, including the kernel and the apps running on it. Furthermore, the very fact that someone wants to run an operating system that is not the default choice of the masses indicates a willingness to learn and explore—a huge advantage when it comes to running your machine safely and smartly.

**Other Reasons**

On top of these, we have a smaller Linux desktop market, which warrants smaller attention, the underdog attitude, as well as a range of various security mechanisms built into the system.

I have not really elaborated on these, as they vary from distro to distro, but there are all kinds of tools and utilities available in Linux distributions that make the system subversion more difficult. To name a few, there's SELinux, AppArmor and many others.

**Conclusion**

The combination of all these factors makes the Linux malware game a boring one. It's very boring on Windows, too, despite the best efforts by fear-mongers and doomsday preachers to keep the heat on. But seriously, if you don't download bad software, you won't end up with an unstable system. It's that simple.

Antivirus is just a tool, nothing more. Used properly, it can do something, but it is not necessary. However, when large companies have a keen and financial interest in selling their software, the question of security becomes one of politics. Luckily, you need not be a part of the game. You can enjoy safe, sane and pleasant computing without going overboard with worry or wasting your digital resources on inherently futile activities, like running antivirus software on your Linux box.

The only sensible application to this would be to spare your Windows friends from malware in transit, which you would be immune to, but they won't. However, this can be solved in many ways, without an antivirus tool, including not forwarding junk mail and not browsing unknown or questionable Web sites.