

# **A Naive User's Guide to Running Windows More Securely**

Written by special contributor Alcibiades on 2006-01-04 18:04:04

Like a lot of people who have worked in the business, I find myself in conversations about computer security with people who are having problems or know people who have problems. I wrote this to save me from explaining the same thing over and over again to different people, and to save them the trouble of having to make notes as we talked. It was meant to be something you could give to a 'naive user' and have them be able to read and follow it more or less unaided, and while not being a complete guide, at least be something that made them more secure than before they got it.

## **What is the danger?**

That a machine will have 'malware' loaded onto it. This will then allow criminals to use it to send spam (often promoting pornography), hack other computers, make it dial up premium rate numbers, or steal information from it, including bank account numbers and passwords. In bad cases bank accounts can be stolen, in extreme cases identity theft is possible. The risks are mainly financial, but if a machine is captured by pornographers, they may also be legal. In the UK, for example, the existence of some kinds of material on a computer is going to be a strict liability offence. The onus is going to be on the holder to prove he/she was not the agent/owner, and it may not be easy.

## **How bad is it?**

Bad and worsening. Here is one example. USA Today, in November 2004, set up 6 machines on the net and observed the results. In two weeks they attracted 306,000 attacks, and an XP SP1 machine was broken into in four minutes. The Denver Post did the same thing in February 2005, and attracted 45,000 attacks in a week. This is the risk from simply being connected. To it, you have to add user actions - unwittingly visiting fraudulent and malicious sites, receiving malicious emails or attachments. There have been 100,000+ Windows viruses, 2,500 Windows spyware releases, and some studies show 80% of home PCs may be infected with spyware broadly defined. The latest thing is Windows rootkits - essentially undetectable infections.

## **Who is at risk, and from who?**

Anyone connecting to the net with Windows 95, 98, ME, or XP with Service Pack 1 or lower. Broadband makes the risk much greater. Fully up to date versions of XP SP2 are much less at risk. People running Unix based systems (including MacOS and Linux flavours) are much less at risk. People running firewalls are also much less at risk.

Basically, connect Windows XP SP1, 98 or 95 to the net without a firewall, and the evidence is, you'll likely be hacked within an hour. You are almost certain to get infected if you (or your children) use music sharing software, or if you agree to download and install software as a condition for free access to some kinds of services. Downloading

ring tones for mobiles is a common source of infection. Downloading bootleg software (so called warez) is another.

You can find out how secure your machine is to some kinds of attacks by going to Steve Gibson's Shields Up site: <https://www.grc.com> (go to the Shields Up section) to test the vulnerability of your firewall and system. Recommended. This tells you about liability to incoming attacks. Leak Test, from the same site, will tell you whether your firewall protects from outbound leakage.

The perpetrators are mostly criminals in it for profit. The days of the amateur teenage hacker in a suburban bedroom are over.

### **If I follow these recommendations am I safe?**

No. You are safer. You are still running an Operating System with a proven record of security faults in a network environment. And this guide is not a complete account of the subject.

### **Are there alternatives to these recommendations?**

Yes. Plan B is: go to a Unix based Operating System, like Linux or MacOS or one of the BSDs. Here are some thoughts on this one.

It helps because there's been far less malware. Probably under 50 real viruses for both MacOS and Linux, even less for Commercial Unix. Spyware is so far unknown (according to Webroot).

Linux or BSD will run on your existing machine side by side with Windows. It is also free, so this is the cheapest of the Plans B. However, don't try moving to Linux or a BSD without help. Your helper should agree to be available for support for six months after the installation. MacOS, which is similarly or maybe more secure, and also Unix based, one probably can do unaided. But you need a whole new computer for it, and new versions of your applications, so it gets expensive. The Mac Mini is worth considering if you are tempted.

The best bet in Linux/Unix for the end user is probably PCLinux, available free for download over the net as a single CD iso. Mepis is also very good. Either will come, free, with all the applications you are likely to need, including Office packages. Maybe fewer games than you would like. In BSDs, PCBSD and DesktopBSD are end-user oriented distributions. They are so far a lot less popular than the Linuxes.

### **How to safeguard Windows? Four rules go a long way.**

**Rule 1. Use a limited user account for normal work, and for connection to the net. Never connect from an account with administration privileges.**

How to do this. Use the Users and Passwords control panel to create a new Administrator account. Reset your current account to limited user. Then only use the Administrator account to manage the system, install software etc, and then sign off. Never connect to the net when signed on as Administrator, except to do Windows Update. Enable privacy between user accounts, and have separate user accounts for everyone who uses the computer. Make a separate dedicated limited user account for shopping & banking.

Why this helps. Any attacks made on you while on the net will have the same privileges as the account you signed on with. (There have been some exceptions, but this is mostly true for up to date systems). Administrator accounts can do anything at all to the system. Limited user accounts can do relatively little. Signing on as a limited user restricts the attacker's options. Microsoft's default on this is for you to sign on as administrator. It is as if, in an hotel, every guest key opened all guest rooms and the main safe, kitchen and boiler room as well. Change it.

**Note1:** Windows 9x has only one account, so this won't work with 95 or 98 or ME. Either upgrade to XP, but its not simple, or consider buying Anti-Executable from [www.faronics.com](http://www.faronics.com). Learn to use it to lock down your machine. Note that I have not used this package - the recommendation comes from the product specification, user guide, and testimonials. Also use ZoneAlarm (below) to disconnect from Broadband when not actively using it.

Note2: Some older software, and all CD burning software, will have problems running as a limited user. Use the 'run as' function (right click on the program icon) to run them as Administrator.

## **Rule 2. Connect to Broadband via an ADSL Router, never just an ADSL modem.**

How to do this. Either ask your provider to supply Broadband with an ADSL Router, or buy a combined modem/router yourself (cheapest by mail order). Make sure you have the right PC ports to connect it up and that you get cables. If you have a choice, use an Ethernet connection, in preference to USB. Find out how to address the hardware firewall it will have in it, and set it to high protection if it isn't already.

Why this helps. If you just connect via a modem, your machine will be visible to hackers worldwide. If you use a Router, it will use a private address for your machine, and the only thing visible on the net will be the Router (a much harder target). If you set the hardware firewall to high, the router also will be invisible.

## **Rule 3: Only use secure software.**

This falls into three parts.

First, don't use the chronically insecure Microsoft Explorer and Outlook; get (free) Mozilla Firefox (Web) and Mozilla Thunderbird (Email). Also get the Firefox Spoofstick plugin and Adblock to guard against phishing. One or two UK banks require Explorer,

and firewalls off. Avoid them. Use Mailwasher to screen and delete unwanted mail on the server.

Second, get the following:

ZoneAlarm is a free software firewall. You do need this as well as the router hardware firewall. Replace the weak XP built in firewall with it. Use it to disconnect from the net when inactive, and to control outbound traffic from applications.

AVG is a free anti virus package (Kapersky and McAfee are also very good, paid packages). Update at every connection.

AdAware & Spybot Search and Destroy are free anti-spyware packages. Get both, and update at least weekly. Microsoft's own anti-spyware package is free and highly rated. Webroot's Spysweeper is a paid, well regarded package, as is Pestpatrol. One anti spyware package is definitely not enough. Find all these by using Google, or on Tucows. Also, install SpywareBlaster for real time protection, but still sweep with the others weekly.

If using Anti-Executable, I wouldn't rely solely on these scans, to clean up the system first, but would do a clean Windows reinstall as explained later.

WinPatrol is also highly rated, and protects against some system parameter changes.

**Third, keep Windows up to date using the Windows Update control.** You'll have to sign on with an account with admin privileges. Check out Sans Institute Internet Storm Center, 'Windows XP, Surviving the First Day', for instructions on doing this safely - find it using Google. This helps because security updates for Windows come out often - as more holes are discovered and exploited. The quicker you get them in, the shorter the time you are at risk.

One should also disable insecure Windows services, as Greene's book (below) explains. And never install anything when prompted to do so by a web site or email.

**Rule 4: Keep as much personal information as possible off the machine, on paper.**

Never have your browser remember passwords or logon information. Never keep NIS numbers, passport numbers, drivers license numbers, bank account numbers or branch addresses on disk. Never use Quicken or MS Money to connect to your bank to download data. Never dispose of a PC with a hard drive in it: take out the drive first, and destroy hard drives before disposal.

If you have children, have a dedicated machine for gaming, music downloads, chat etc, keep no personal data whatever on it, and if you allow it to share the Broadband connection, firewall it off totally from the other machines. Consider using Anti-

Executable or even DeepFreeze (also Faronics) on it. All this will be fairly technical, and will probably require professional help. It will be worth it.

Microsoft has just published the 'Shared Computer Toolkit' for making a machine safe for multiple users in a walkup environment. Professional help will probably be needed to install and use this, and it may be overkill for home users.

### **Reading.**

Thomas Greene's book 'Internet Security for the Home and Small Office', is essential reading if you ever use Windows on the net, dialup or broadband, to bank or shop. Get it (from Amazon). Clear, detailed (lots of screen shots) how-to on hardening Windows. It explains how to disable insecure Windows services, which is a must, but which is too big a topic for these pages. Steve Gibson's site, see previous page, is worth a visit. Secunia and SecurityFocus are very good but technical. Wilders.org has lots of good links and clear explanations.

### **How to know if your machine is infected, and what to do.**

You'll know because of slowdowns, crashes or unpredictable behaviour, especially of Explorer or Outlook, or because scans with anti-virus or anti spyware software tell you of infections. You may find lots of popups appearing, you may find yourself on sites which you have not clicked on. Your internet connection may be very active when you are not doing anything. Your ISP or other people may tell you your machine is sending spam. Trying to find out what is going on by Ctrl-Alt-Delete may not permit you to examine running processes.

Take this very seriously and do not bank or shop online until fixed.

What to do? It used to be a very simple matter, get and run anti-virus software and keep it up to date. No more. In the last year, it has become decreasingly possible to be sure of having cleaned a badly infected Windows OS that one has booted from. The only method reasonably certain to succeed nowadays is, back up your work files to removable storage, then format and partition the affected hard drives and reinstall Windows, harden it, and then copy back the work files and reinstall software. I would personally do this by buying a new hard drive (Seagate Barracuda) with an OEM copy of XP, and starting from scratch. I would do the data backup by booting from Knoppix or similar Linux live CD.

Advice. Find a professional and say this is what you want done. If he tells you it is not necessary, and that simply running AdAware etc is enough, well, it may be. But there again, it may not be. The question is, how much do you want to bet?

I would demand (and pay for) a clean install...

### **Appendix: where does this problem come from?**

If you are just trying to keep systems secure, this may seem a bit academic. But people do ask, so here is a very short account. First, to avoid being forced by anti-trust actions to give equal treatment to all browsers, Microsoft, during the 'browser wars', made Explorer part of the Operating System, and also linked Outlook to Explorer. This means it really cannot be removed. But it also means any vulnerability of Explorer or Outlook is a vulnerability of Windows. Second, it's the social culture of Windows use - in particular, the universal practice of signing on with Administrator privileges. This means any infection is automatically a system wide infection. Third, its to do with myriad vulnerabilities in the way Windows handles services. As an example, the recent wmf flaw enables graphics, regardless of browser, to carry malicious code. This is because of flaws in the way thumbnails and graphics rendering is done in Windows. RPC (Remote Procedure Calls) is another example.

Bottom line: it is not going to go away any time soon.

#### Caveat

I've taken care over this, but its a very brief guide to a very complicated and rapidly changing subject. I can't be responsible for any inaccuracies or any consequences of following these recommendations. Do not follow them blindly. Verify first, and then use them only as the basis for formulating your own security policy, and arriving at your own list of dos and don'ts.