Computer Security

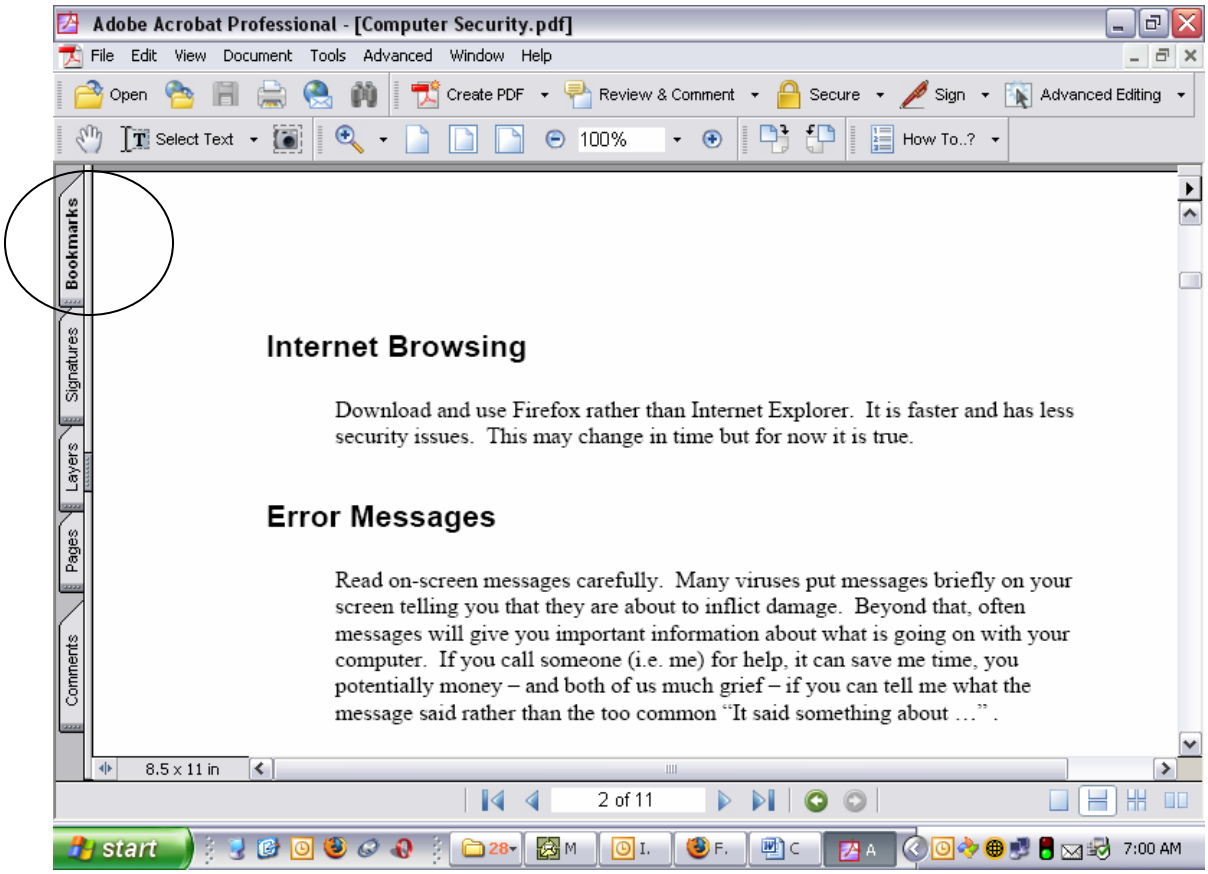
Please contact us by phone: 604-597-7970
email: barry@mycomputerprofessional.com
web: mycomputerprofessional.com

Table of Contents

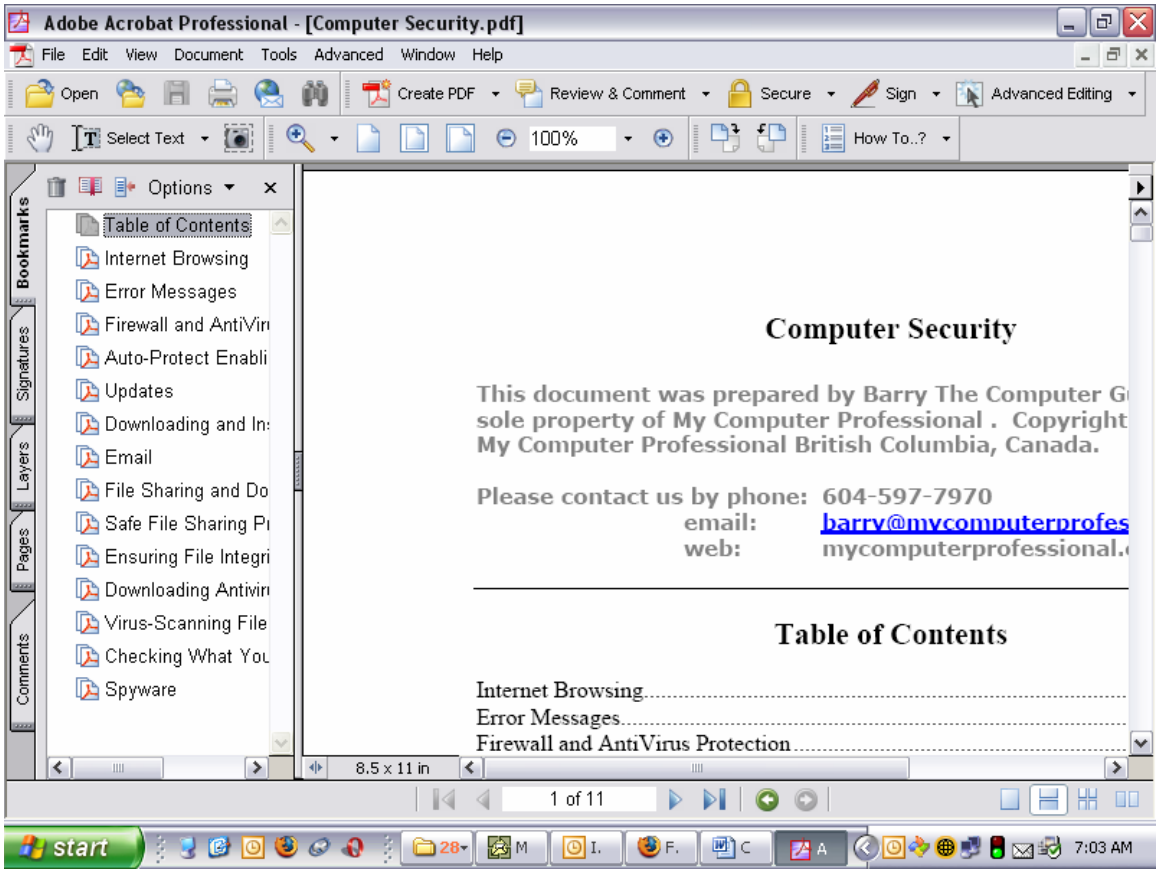
Navigating This Document

There are 3 ways that this document can be read:

1. Start at the top and read until the end!
2. (If Bookmarks are not showing), click the Bookmarks icon on the left side of the document …



… and you should see this:



You can then navigate by clicking the various Bookmarks.

3. Each of the items in the Table of Contents is a link. Clicking the item will take you to the page that item is on. Going back to the Table of Contents, when using this method, requires you to wither use the Bookmarks function or simply scroll back up to the top.

Internet Browsing

Download and use Firefox rather than Internet Explorer. It is faster and has less security issues. While Firefox has vulnerabilities – all software can be exploited and Firefox will become increasingly targeted as it grows), it is better-written than Internet Explorer. Additionally, the Firefox people have shown much quicker response to exploitation than Internet Explorer is capable of. This may change in time but for now it is certainly true.

You can download Firefox from http://www.mozilla.org/

Pop-ups and Threats / Warnings

If you see Pop-ups that say things like “Your computer is infected with viruses and/or Spyware. Click here to fix” or “Your computer is in need of maintenance.. Click here to fix” or anything similar, DO NOT RESPOND. CLOSE THE WINDOW.

This probably means you are already infected with Spyware and you need to take immediate action.

If you get messages (usually not pop-ups but small system message-like boxes) that TELL YOU your computer is infected, do not ignore this. TAKE IMMEDIATE action. Many viruses will do this. Some say “Your computer will shut down in 60 seconds” or something to that effect. And indeed, it will shut down and there is nothing you can do to stop it until you’ve rid yourself of the infection.

Other viruses will actually tell you what they are doing and will warn you that they are going to make your computer inoperable in one way or the other.

These are not jokes and ignoring the problem will only cause you more grief.

Infection Action Plan

There are many signals that indicate you have infection In addition to the information in paragraphs above, some of the common behaviors are:

1. Programs are installed or running on your computer which you DID NOT install.
2. You have search bars or toolbars which should not be there.
3. You are automatically being re-directed from your home page to other pages when you try to browse the Internet.
4. Your Antivirus and/or Firewall are disabled or not functioning properly.
5. You have dancing icons on your desktop.
6. You have links on your desktop to pornography, gambling, shopping, etc. websites which you DID NOT put there.

If you have these symptoms or others that cause you to suspect that you have virus or spyware infection, scan your computer for both viruses and spyware immediately. Keep scanning until you have a clean run.

If you are unable to scan, or you have completed scanning but still have symptoms, call Barry at 604-597-7970 or email me or visit our website.

DO NOT ignore the threats and **DO NOT** delay. Once the door is opened to threats, they will not go away and will only get worse, causing you more grief and ***probably costing you more money***. Deal with threats seriously and immediately.

Error Messages

Read on-screen messages carefully. Many viruses put messages briefly on your screen telling you that they are about to inflict damage. Beyond that, often messages will give you important information about what is going on with your computer. If you call someone (i.e. me) for help, it can save me time, you potentially money – and both of us much grief – if you can tell me what the message said rather than the too common "It said something about …" .

Read it and write it down.

Firewall and AntiVirus Protection

If you have an anti-virus and/or firewall running on your computer, DO NOT disable these functions. If you don't have antivirus and firewall protection, get it. You can call us for assistance in installing these products. They are your sole protection against malicious hackers, viruses, Trojan horses and other intrusions on your privacy.

Auto-Protect Enabling / Disabling

If you ever need to disable them in (order to install a program, for example), disconnect your internet by pulling the RJ-45 from the back of your computer BEFORE you disable the security and re-plugging it only AFTER you have re-enabled security.

Updates

Run the Norton Live Update manually every day or 2, just to be sure. Most of the time you'll find that you are up-to-date, but this is just another Best practice.

Downloading and Installing

When downloading from the internet, use common sense. Do NOT download programs from unknown sites. THINK about what you are going to download: Do you really need it? Be aware that every download is potentially inviting malicious code onto your computer. This is not to suggest that you should not download anything from the internet, but rather just that you should exercise caution and, again, use your judgment. Think of it in much the same context as you would your home security: Inviting anybody outside your immediate family into your hoe potentially invites theft, but since it is unrealistic to never have anyone in your home, you exercise caution in terms of who you invite into your home and how much latitude they have while there.

READ the EULA (End User Licensing Agreement) when you are installing software. It may sound like a pain – and it is – but often the EULA will inform you that you are agreeing to spyware on your computer. Furthermore, it is a legal agreement that you entering into and you should be aware of what you are agreeing to.

Finally, do not hit the NEXT key blindly and repeatedly while installing software. (You may see me doing that, but only with software that I have installed before, and I know the steps). Often there are sections allowing the user to customize the installation, including removing the spyware options … at least in theory.

If you need utility software (spyware/adware programs or other utility programs, get them from download.com. If they aren't available there, they probably are a problem more than a solution. If you aren't sure, call Barry at 604-597-7970.

Email

If you get emails with viruses, do not open the attachments even if the anti-virus has reported them as deleted, quarantined, etc. If the email is from someone you know, inform them that they have a virus. DO NOT REPLY TO THE INFECTED EMAIL. Rather, create a new email or, better yet, phone the sender. Don't necessarily be angry: They probably don't know they are infected.

Really, it is advisable not to open attachments at all, even unless you are explicitly expecting them. Some viruses effectively hijack the email client, emailing themselves out to the entire address book so that an email from someone you know may have been sent without his/her knowledge. Save attachments then scan them with an antivirus program before executing them.

Delete the infected email ASAP so that nobody else in your household can accidentally infect the computer.

File Sharing and Downloading

Safe File Sharing Programs

Use either Kaazalite or Limewire or both for file-sharing. These are preferred because Kaazalite has had the spyware stripped out that is normally part of Kaaza and Limewire is spyware-free. But they do not protect you from threats that may exist in files you download, so:

Ensuring File Integrity

When you download a file, your security software will check it for viruses, etc. (but not for spyware), but this is not a perfect solution. If the file is infected with a brand-new virus and you do not have the virus definition file for it, it will not be recognized and executing the file will activate the virus.

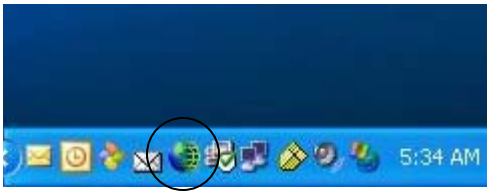
I recommend the following the procedure in the paragraph below. It is not difficult to follow, except, generally speaking, for kids (and some men!) in my experience because kids typically want to access whatever they've downloaded immediately. ***SO THIS QUESTION IS FOR THE KIDS: WHO PAYS TO FIX THE COMPUTER IF YOU INFECT IT WITH A VIRUS? IF THE ANSWER IS YOUR MOM AND/OR DAD, I WOULD RECOMMEND YOU EXERCISE SOME RESPONSIBILITY AND FOLLOW THE PROCEDURE. IT IS A BEST PRACTICE WHICH WILL, IN ALL LIKELIHOOD, KEEP YOUR COMPUTER SAFE.***

Once your file is downloaded, leave it alone for 24 hours. Then:

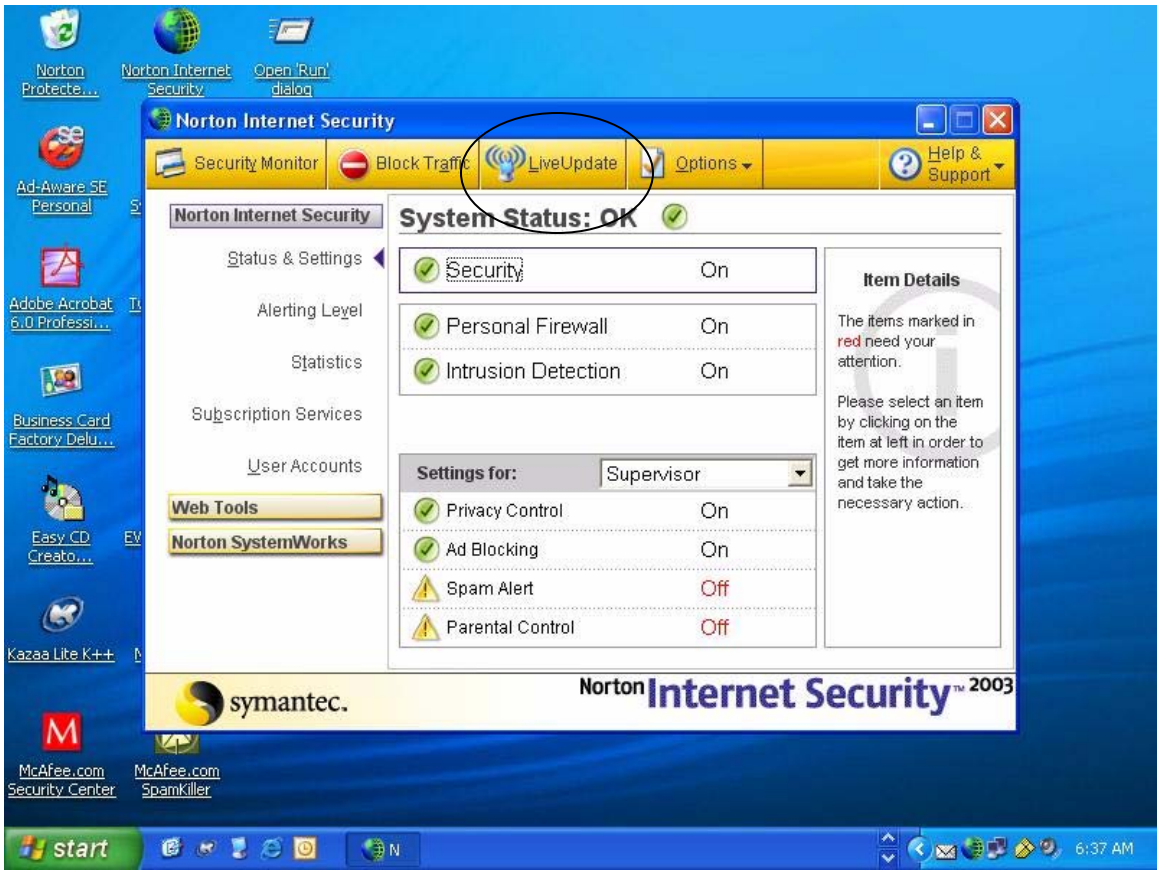
Downloading Antivirus Definitions Manually

Download the latest anti-virus definitions.

With Norton, you can do that by double-clicking any of the Norton icons in your system tray, like the Norton Internet Security icon circled below:



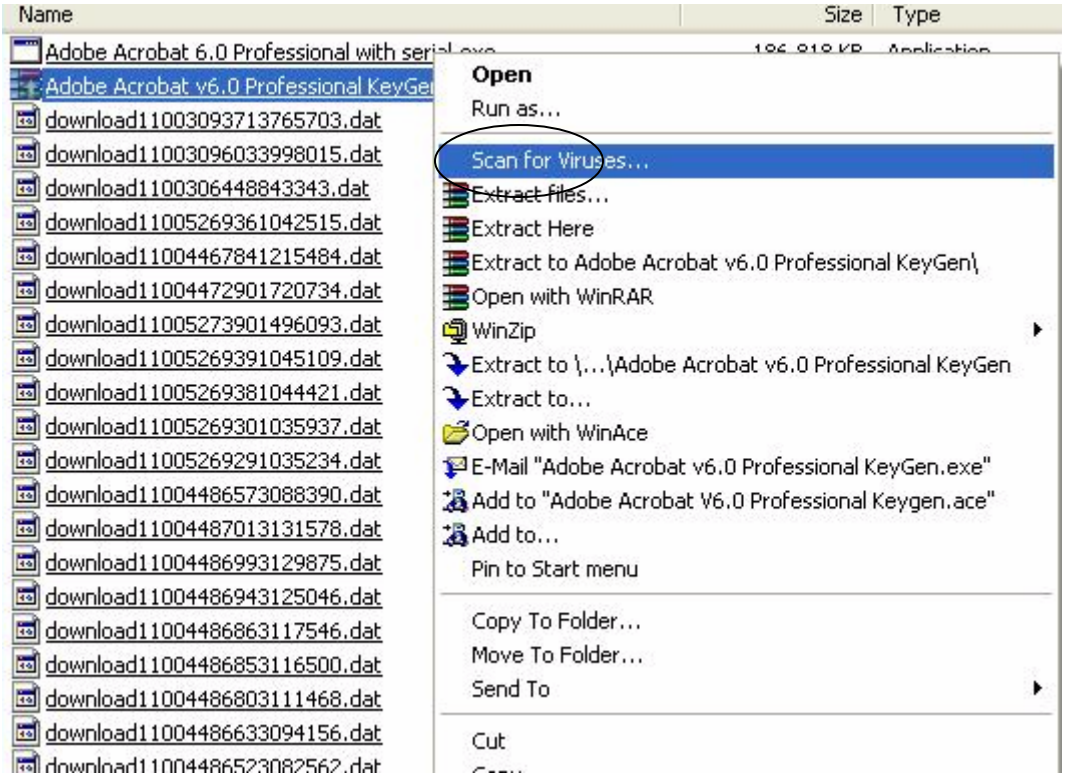
This will bring up Norton Internet Security:



Run Live Update by clicking the Live Update icon circled above and follow the instructions to download the latest updates which include any virus definitions.

Virus-Scanning Files Manually

Manually scan the file you downloaded. Locate the file and right-click it. This will bring up a context menu which will look something like (though not exactly like) this:



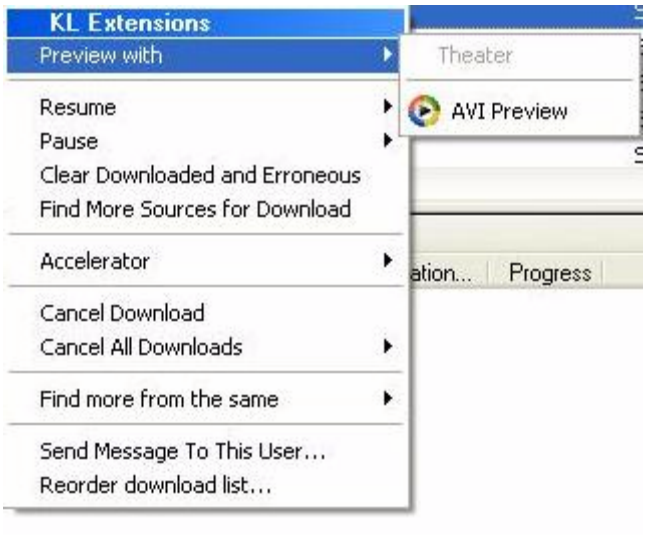
Use the Scan for Viruses option high-lighted above to scan the file and if it successfully scans it without finding any viruses, then you are probably safe. Bear in mind that there is no 100% guarantee, but you have now taken all reasonable precautions.

Checking What You Download

Downloading movie files can be particularly dangerous. This is because the name of a movie file can be anything. The name of a file is just a label and can easily be changed, so you may think you're getting Shrek or Fiddler on the Roof, but in fact it could be anything at all, including offensive or illegal material.

Not only do you risk downloading this onto your computer, but if the download completes and another user downloads it from your computer, you have also become a distributor of the material. So what can you do, besides not ever downloading movies?

Kaazalite has a preview option which works with most (but not all) movies. Once a movie has started downloading, right click it and you will see a context menu:



Use the AVI Preview option with .avi formatted movies and the theatre option with most other movie types. This will allow you to make sure that what you are downloading is what you expect.

If the file is a type which cannot or will not preview, your options are to continue to download but not to leave the computer unattended for long periods of time, so that you can check the file and make sure it is good before someone else can download it from you, cancel the download, or proceed knowing what the risks are. I recommend one of the first 2 options.

Spyware

Spyware in its various forms is becoming one of the worst threats on the internet. The most malicious forms can hijack your internet connection and bring your computer to its knees.

Spyware infection has become so rampant, and is spread so easily, that there is no longer any one program that will provide a complete solution. I use 3 programs and (at least so far) they have kept my computer clean:

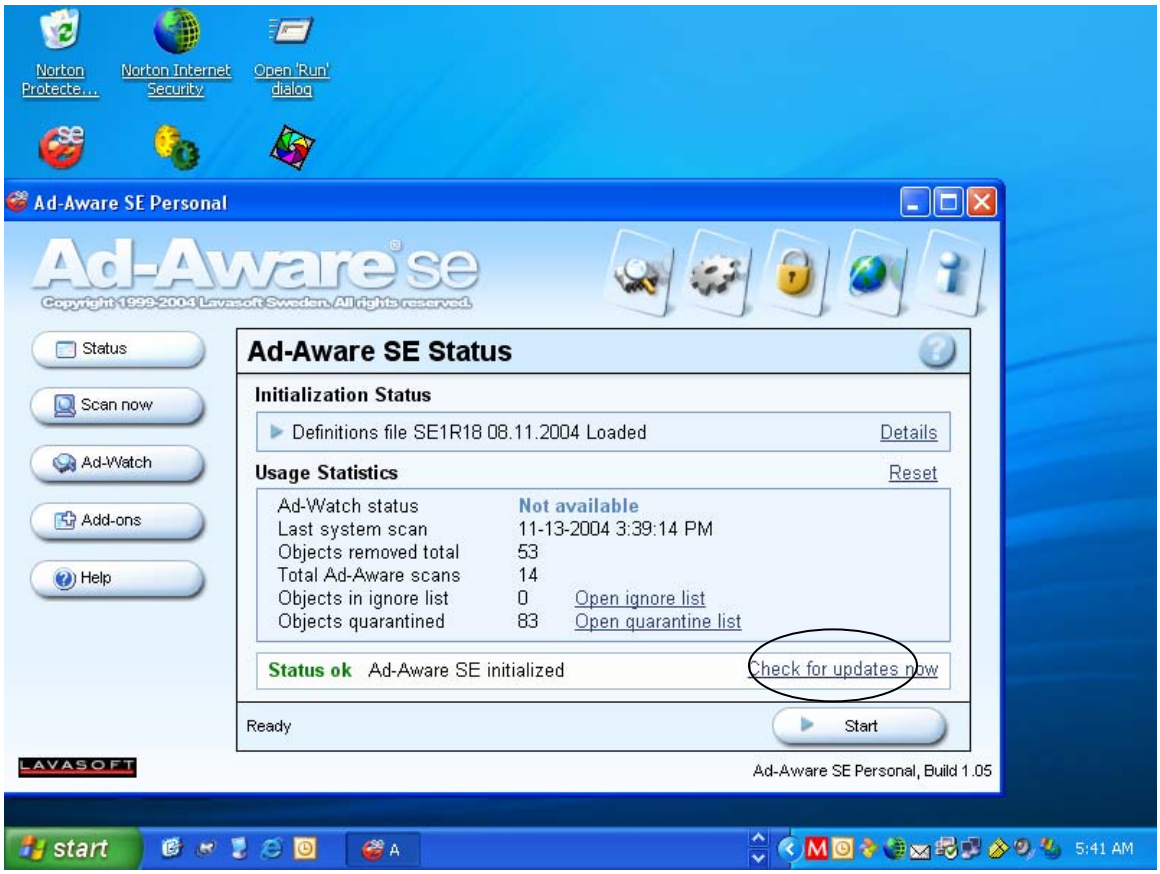
Norton AntiVirus 2005
Lavasoft Ad-Aware
Microsoft AntiSpyware (formerly Giant AntiSpyware, recently purchased)

The Microsoft product may not be usable much longer as Microsoft may have introduced incompatibility problems with the Norton products, either deliberately or accidentally – with Microsoft it is hard to tell!

1. Run each of these once every week or two. Ad-aware instructions as follows:

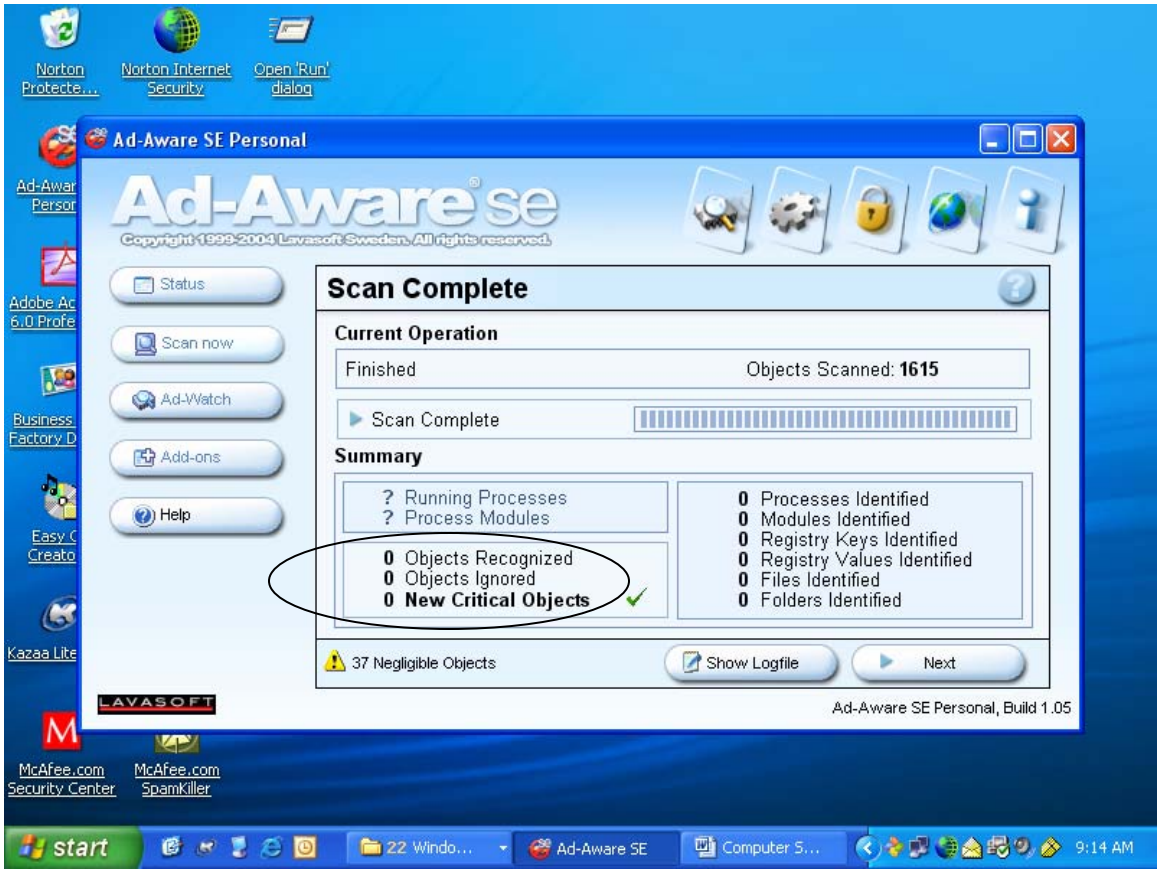
2. click the Ad-Aware icon

3. This will bring up the Ad-Aware main screen as below. Click where it says Check for updates now (circled below). On the next screen, ignore the "Configure" button and click "Connect" to get updates. If it finds any, click OK to install and the Finish when the install bar hits 100%.



4. Now click Start, just below the Check for updates now link. On the next screen, click Next. Now the program will scan for Ad-Aware/spyware.

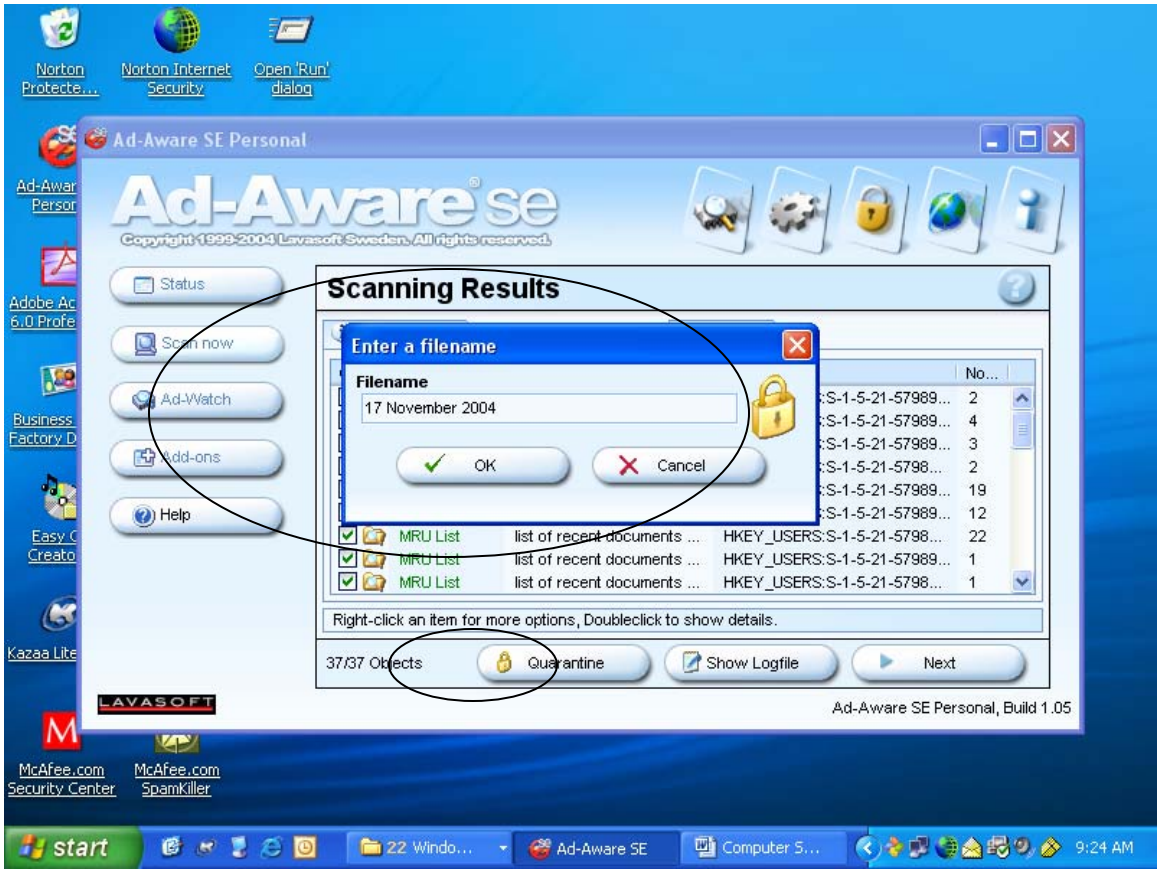
5. When it has completed the scan, it will show a screen indicating how many objects have been found:



6. As there were no objects found in this case, the numbers are all 0, but often – even with "normal" internet usage, there will be some. Click Next.

7. Select the files you wish to quarantine by right-clicking in the "Obj." field of any of the items and then clicking "Select all". Then click Quarantine. Give the quarantine file a name – I usually use the date – then click OK. You'll get an information screen telling you how many objects are being quarantined and then it will actually do the quarantine operation. Then click Next. It will tell you how many objects will be removed, click OK and it will remove the objects.


Norton Protecte...
Norton Internet Security
Open 'Run' dialog
Ad-Aware SE Personal
Ad-Aware se
Copyright 1999-2004 Lavasoft Sweden. All rights reserved.
Status
Scan now
Ad-Watch
Add-ons
Help
Scanning Results
Scan Log
Location
No...
HKEY_USERS:S-1-5-21-57989... 2
HKEY_USERS:S-1-5-21-57989... 4
HKEY_USERS:S-1-5-21-57989... 3
HKEY_USERS:S-1-5-21-5798... 2
HKEY_USERS:S-1-5-21-57989... 19
HKEY_USERS:S-1-5-21-57989... 12
HKEY_USERS:S-1-5-21-5798... 22
HKEY_USERS:S-1-5-21-57989... 1
HKEY_USERS:S-1-5-21-5798... 1
Item Details...
No Object Selected
Jump to Key...
Export Registry Bookmark File
Extensions
Select All
Unselect All
Inverse Selection
More Selection Options
Quarantine Selection
Add Selected to Ignore list
Export HTML Report
Export as Text File
Print Report
Show Scan Summary
Show Scan Log
Help...
Show Logfile
Next
LAVASOFT
Ad-Aware SE Personal, Build 1.05
McAfee.com Security Center
McAfee.com SpamKiller
start
Computer S...
9:19 AM



8. The safest thing is to run it again (and again) until no objects are found.

9. Unfortunately, the adware/spyware crisis has become such a nightmare that one product is no longer enough. I recommend running both Lavasoft Ad-Aware as well as Microsoft AntiSpyware. The only caveat to either one of these products is that you have to pay some attention. The Microsoft product, for example, will blindly identify Kaaza as being a problem, even though you may be running Kaazalite. If you delete it, then Kaazalite will no longer work. Use Ignore Always for Kaazalite and for other programs you ***KNOW*** are safe, but be sure you ***KNOW*** they are safe before using this.