

INTERNET PRIVACY AND SECURITY: BEST PRACTICES

OVERVIEW:

Internet privacy and security are your responsibility. If you do not take sound privacy precautions, you may reveal more of your personal preferences, habits, etc than you wish, and you may find you are haunted by the ghosts of your internet usage in the offline world. If you do not take sound security precautions, you will expose your computer, and your files to being erased, locked out of, or taken over and used for illegal purposes, which you may be held responsible for depending on the laws of your country.

Presently, the threats to your internet privacy and security include the following in order of severity: various governments, organized criminals, marketers and websites who you do not want to collect your information and/or are careless with your information. Commercial tools, such as antivirus and firewalls, do not begin to protect you from all these threats.

You will be able to greatly increase your protection from all threats by following my recommendations. This paper makes the case for internet privacy, and internet security. It then lays out a procedure, in plain language, containing the practical methods that you, as a private citizen, can take to maintain maximum privacy and security online.

This paper is organized as follows:

- Overview – page 1
- The case for general privacy – page 2
- The case for internet privacy – page 4
- The case for internet security – page 5
- Case study - the present state of internet privacy: Google – page 6
- Procedure to help maintain internet privacy – page 7
- Procedure to help maintain internet security – page 22
- Hope for the future – page 64
- Appendix: other useful windows installation settings – page 65

THE CASE FOR PRIVACY

Privacy is the ability to keep things to oneself as one chooses. Privacy and privacy rights are a necessity in modern society, because of the intense and pervasive scrutiny under which everything is routinely placed.

Consider a world without privacy rights: Without privacy rights, there is nothing to stop someone else from placing a camera in your bedroom. Without privacy rights, there is nothing to stop someone else from stalking you, preparatory to a theft or assault. Without privacy rights, there is nothing to stop companies from putting you under surveillance for purposes of charging you a higher price than other people for your preferred services, brands and products. Without privacy, there is nothing to stop your government from deciding the choices of your life and conscience and enforcing your compliance against your will. In short, without privacy, there is nothing to prevent a stranger from knowing you as intimately as well as your most intimate confidant. Imagine a world where you can't prevent your worst enemy from accessing the most intimate details of your life and using it against you. Privacy is your most effective bulwark against many insidious harms that would otherwise occur to you and yours'. Furthermore, and perhaps, most importantly, privacy keeps other people and entities from being up in your face and business if you don't want that.

Privacy entails responsibility. It would be silly to walk naked through the streets, and then complain if someone else posts voyeur photos of you online. Common sense and reasonable precautions are also required before privacy rights can or should protect you.

Privacy is the presumption that individuals are not up to no good. In a court of law, innocence is presumed until guilt is proven, because of the many abuses and injustices that occurred in previous court systems where the opposite presumption was used. We should surely extend the same, or greater, rights to those who are not yet accused, as to those who are not yet convicted. Privacy is not the right to break the law or harm others; such things are already prevented by other laws (and the laws need not abridge privacy to prevent such crimes, as such crimes are already crimes by themselves).

Privacy is what Isaiah Berlin describes as a 'Negative Freedom.' That is, privacy is a freedom to be left alone by ___ from ___. Answer these honestly: May I please search your wallet? May I please search your bedroom? May I please search your body? May I touch you anywhere I please? Privacy allows you to answer 'No!' to all these questions. Privacy enables you to relax in your home. Internet privacy is to your information what personal space is to your body. It is your own and others should not invade it. You would not allow some creep to view into your bedroom. Why would you allow him view into your computer and internet use? Why should it make any difference if a creep is from a big company or the government? Why should he see into your private life?

Privacy is also an enabler of ‘Positive Freedoms.’ Negative freedoms, in general, and privacy, specifically, enable the enjoyment of all other freedoms, including, but not limited to: property ownership, freedoms of speech, assembly, religion, sexual choice, abortion (or the choice not to have one), traveling freely and voting. Privacy enables you to meet up with a lover for a sex act that the local religion would not approve of. Privacy enables you to research about some problem in your life, without embarrassment. Recall the American Declaration of Independence stated we fought for Life, Liberty and the Pursuit of Happiness. Privacy is a Liberty that enables you to pursue Happiness.

Privacy is also necessary to maintain mundane interests, such as keeping a job, or insurance coverage at a reasonable rate. If you doubt me, imagine, for example, how much property you would be able to successfully retain, if your bank account numbers, ownership deeds, and so on, were not private.

Privacy increases the benefit of other freedoms. Many people in this country happily pursue gun ownership or abortions. They enhance their enjoyment of these rights by enjoying them privately or anonymously. Pursuing these privately, that is, without registration and oversight from anyone else, increases the value of many freedoms popular with many people, regardless of their political ideology.

In its most potent form, privacy is the right to anonymity. The right to anonymity is necessary to protect oneself when expressing unpopular opinions. Anonymity protects whistleblowers who expose corruption and other illegal practices. Anonymity protects individuals when they disagree with their community in matters of conscience. Anonymity protects individuals from larger entities, such as communities, corporations or governments. Anonymity also includes the right to blend into the crowd, and remain unmolested in a public space, such as an observer at a public hearing or shareholder meeting, whether you attend in person, or virtually, via the internet. Anonymity is the right to be unknown, while making your case to your community, your company, your congregation or your government.

Privacy, in sum, is the right to not suffer any of a variety of potent harms. Privacy is a liberty that enables you to pursue happiness as you see fit. Privacy, including anonymity, is the right to challenge the conscience of the majority and the community without suffering their retaliation or condescension. Privacy, and privacy rights, enable the most basic, most cherished, experiences of modern life.

THE CASE FOR INTERNET PRIVACY

Why should I care about internet privacy? Privacy is an inalienable right – your business is no-one else's business. It is the law-abiding citizen's freedom to be un-molested. The courts in the USA have regularly found privacy to be both a necessary condition to achieving 4th amendment protection from arbitrary search and seizure, as well as a natural consequence of that amendment's protection. Individual states in the US, as well as many foreign countries, and the EU, have all recognized greater privacy rights than even the US 4th Amendment allows. Privacy is the subject of article 12 in the UN Declaration of Universal Human Rights.

How does internet privacy benefit me? Internet Privacy is practical. The internet allows you to connect to others as never before. Effective internet privacy allows you to choose who you disclose sensitive info to while doing legal things such as shopping, job hunting, sexual, political, religious or business activity. Common sense dictates: anything that you wish to keep private offline is something you wish to keep private on the internet.

In today's world privacy is most under attack from your government, and criminals and marketing companies. The foremost battleground of this fight is on the internet. Internet privacy is a special case of privacy in general. The internet makes this difficult, due to the prevalence of many different tracking devices, including cookies, deep packet inspection technologies, and tracking sites such as Doubleclick (owned by Google, and many other sites similar to Doubleclick), which follow you around the internet by maintaining a connection to your computer at all times.

Internet anonymity is the practical method of attaining internet privacy. Lately, many governments and companies, using the methods described above have begun attacking internet anonymity to the extent that it can no longer shield law-abiding citizens identities from casual drag-net surveillance by various governments, criminals and marketers.

It is frightening that various governments, criminals and marketers know everything you do online. If the government tracked you so thoroughly offline, they would need a warrant. If the criminals and marketers tracked you so thoroughly offline, you would be well within your rights to call the police and have them arrested for stalking you. You could likely get a restraining order against them from a court. Online, the privacy law is not developed. Lately, legislation has been introduced in the EU, and is under draft in the US. Please contact your congressmen and let them know you want your privacy protected online. Let's get a law in place that can put the stalkers in their proper place – which is in some jail far, far away from us

The Christian Science Monitor makes a strong case for internet privacy too:
<http://forums.mozillazine.org/viewtopic.php?f=7&t=1613775>

THE CASE FOR INTERNET SECURITY

There is a perception among many that Privacy and security are always incompatible. This is not so. What is true, is that there are many conflicts between individual and public that have spilled over into matters of computer and internet privacy and security due to advances of technology and incidents of terrorism in the last 2 decades. As far as individuals are concerned, anything that increases their personal online security also increases their personal online privacy.

Effective internet security is requisite for effective internet privacy. Privacy rights can not and should not protect you unless and until you practice reasonable privacy and security countermeasures. In addition, individuals may have further property interests that require security measures for protection from destruction as well.

Security vulnerabilities are a commonly used method of attacking the privacy and property of individuals. Security is an individual's best practical defense against such attacks and intrusions. That is, internet security is one of several critical means by which to achieve the end of internet privacy.

CASE STUDY - THE PRESENT STATE OF INTERNET PRIVACY: GOOGLE

Beginning in 2004, I noticed that Google began buying web-tracking companies. Google makes its money on advertising and related tracking. Google bought one such company, in 2005, Urchin Software Corporation, who authored a Javascript applet that allowed your computer to check in with their servers as you surf the internet. Astute users disabled that script, using browser settings, then browser plug-ins such as NoScript and Ghostery.

After purchasing this company, Google, adapted the script (urchin.js and renamed it ga.js) so that the webpage you visit would contact Google's servers, and Google's servers would then open a connection to your computer, and track you around the internet. (http://www.roirevolution.com/blog/2008/01/should_you_join_the_migration_urchinjs_migrates_to.html) See, also, my screen capture in 17.10.02 of this paper.

Google then bought the Ad.Doubleclick network, and began intensive behavioral targeting in spring of 2009 <https://www.eff.org/deeplinks/2009/03/google-begins-behavioral-targeting-ad-program>. This enables them to track you across a much broader swath of the internet than previously (all of the Google-owned websites + *now*, all of the Doubleclick affiliate websites). Because this tracking is so wide spread, your IP address becomes like an undeletable cookie to them.

Astute users then blocked the domain names that Google was using to track them. (<http://www.blogger.com/navbar.g?targetBlogID=7687465>) Google, then retaliated by reaching out to your IP address from their servers. Now even if you block it in your host file, it can still get through.

Now when I respond by blocking the affected IP addresses, I find I am unable to use any Google sites, such as Google (search engine), Youtube or Google News, because Google has set up its servers such that they all will instigate tracking.

It is worth pointing out the hypocrisy of Google: their corporate motto is 'do no evil' and they made big media splash in 2/2010 by condemning China's spying on political dissidents and refusing to censor search results beginning in 3/2010. Yet Google is willing to take all possible measures to force its own tracking onto users who do not wish to be tracked. <http://arstechnica.com/tech-policy/news/2010/03/google-keeps-your-data-to-learn-from-good-guys-fight-off-bad-guys.ars>)

It is also worth pointing out that Google is not alone in tracking your web use. Google is merely the highest-profile on-line stalker. Yahoo does the exact same thing and the list of other companies doing this is growing. <http://www.guardian.co.uk/technology/2008/jan/03/adobe.apple> Where Google is alone is that, so far, it is the only tracker that I have seen consistently get past the HOSTS File.

HOW TO MAINTAIN INTERNET PRIVACY

1.0 Maintaining Privacy Online.

1.1 Notice that Websites and, to a lesser extent, Internet Service Providers, make their money from advertising. Generally speaking, ad-serving companies such as Yahoo are paid per action taken such as clicks, sales, etc. Internet firms seek to maximize this revenue (and thereby their profit, because in the short term, in this industry, costs are essentially fixed) by targeting the advertisements to the users. They spy on their users to make ads more relevant so they can maximize revenue. In addition, many third party firms partner with websites to track you around the internet, regardless. Large firms such as Yahoo and Google have since bought some of these companies. They are relentless in their tracking. Finally, many governments and criminals are both interested in users' activity. The only difference is that the criminals are obviously out to screw you. The governments try to cloak their spying in the name of 'security,' 'safety,' and 'defending freedom'. Defeating the spying done by various marketers, governments and criminals requires your thorough and ongoing control of your computer and communications.

1.2 Surf only in the appropriate user account for a given interest. For example, I only do things related to my profession in my professional-interests account. I do not use the professional-interests account to view any political material. I use a separate account for that.

1.2.1 Until you tell a website otherwise, your username, for tracking purposes, is the username of the windows account you are using. (Open up a cookie on your computer and see -l in C:\Documents and Settings\YOUR WINDOWS USERNAME\Local Settings\Temporary Internet Files). If you do not allow cookies in any form (see more in 1.3.2 for other types of tracking cookies), then your ID for tracking purposes is the IP address of your machine.

1.2.2 Try to use any given website for only 1 interest – especially email and search engines. Any website that you allow to run code on your computer can use that code to determine your computer's hardware environment. This information can then be used to track your multiple interests across their website.

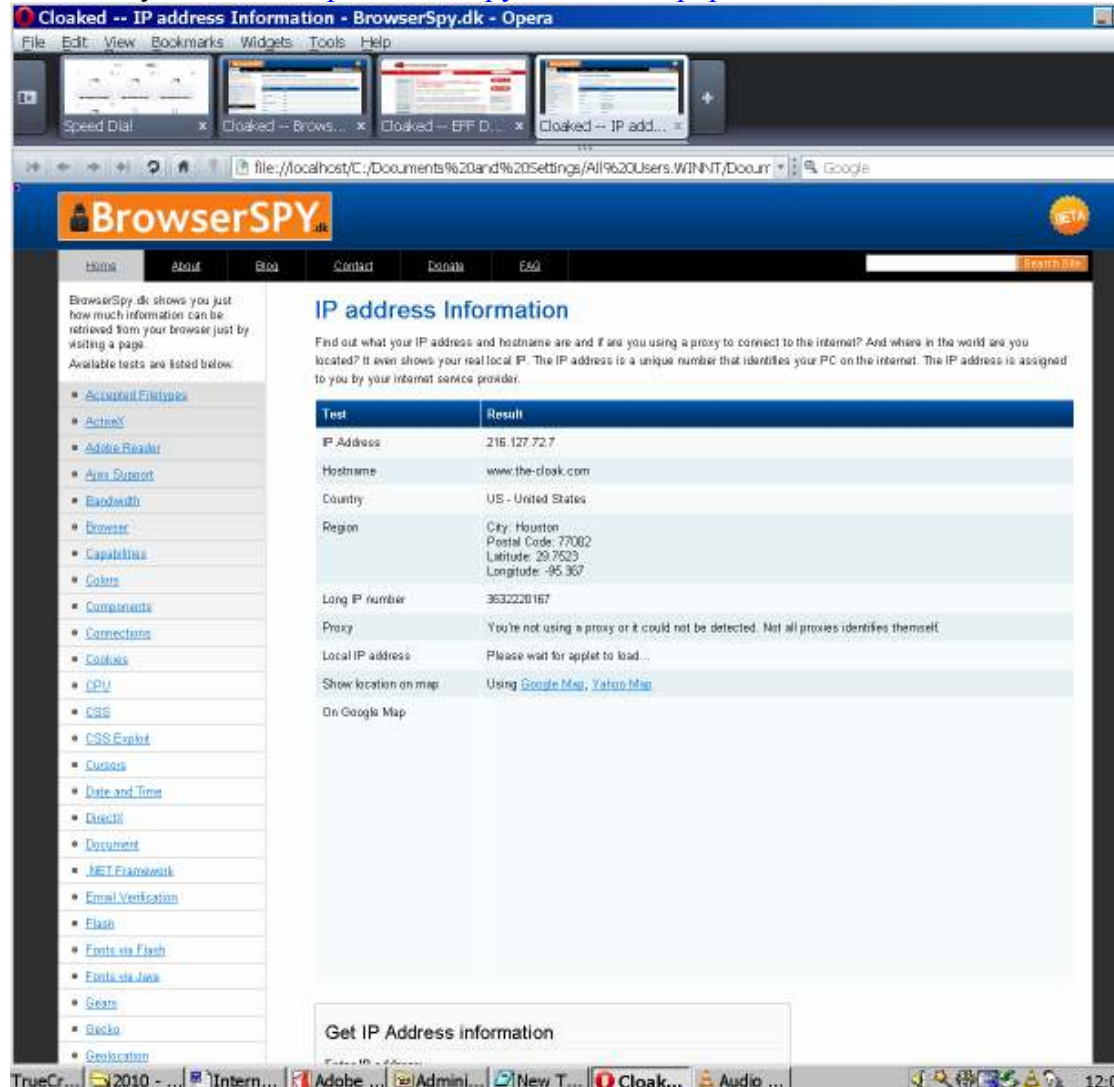
<http://www.quantcast.com/info/lookalike-modeling> This becomes an especial issue because search engines own some of the most popular email providers, and can quickly put the whole puzzle together. ISP's websites have the same privacy problem.

1.2.2.1 It can be difficult to find out who owns whom. Here is a start at identifying sites' owners.

<http://www.hology.com/media.html>

1.2.2.2 Try to use different browsers on your different accounts. Enforce this rule by using permissions. Right click your browser's executable, select 'properties' and then 'security'. Remove permissions for user(s) as desired.

Your Browser type, e.g. Internet Explorer 6 and OS, e.g. Windows 2000 are visible in packet data – i.e. they are visible no matter how much you lock down scripting, Java and ActiveX. See what info you are sharing about yourself as you surf at <http://browserspy.dk/browser.php>.



1.2.2.2.1 You also giving up a MAC address, which is an, absolutely, unique number. The MAC is a 48 bit number made by concatenating a 24 bit Network card vendor ID with a 24 bit unique number assigned by that vendor to your hardware. Present routing technology replaces data packets' MAC address each time the packet passes through a device such as a router or switch (aka a 'hop'). This does not mean in future that the MAC address of the original device, i.e. your computer can not be sent along

to advertisers and stalkers as an additional packet.

- 1.2.2.2.2 Many websites are now contracting their web-serving to third party Content Delivery Networks (CDNs) such as Cachefly, Akamai Technologies and Cloudfront to try to make their websites faster by being geographically closer to their users. These sites have ample opportunity to track you including across interests, depending on which websites contract with which third party web serving companies. Many ISPs are working with these same networks to speed up their services. Finally, some of these CDNs are beginning to dabble in the ad market. http://news.cnet.com/Akamai-to-help-Road-Runner-speed-up-in-hot-market/2100-1033_3-234711.html
- 1.2.3 People can be JERKS about anything. Don't leave yourself open to any problem arising from any possible association of your name and your particular interests. One woman got fired over comments she made on a social networking site. http://www.ohio.com/news/break_news/93945589.html
- 1.2.4 Do not allow Mobsync.exe to run (I show how in section 11.1). Mobsync is a well-intentioned Microsoft program that has the potential to undermine you privacy. Mobsync gets online when it wants and updates your homepage – and any other page it is set up to update. If you are logged in as your professional identity, and all of a sudden, it goes and starts downloading from sites linked to your other identity(s) then you probably will defeat your privacy.
- 1.2.5 There are certain anonymous browsing and proxy services and programs that can be used for a fee. They claim that they remove your identity from the communication by routing it through many other computers, before connecting to the site you intend. I don't use these because (1) you have to give your real name and info when you pay them (they want a credit card# to bill), (2) you may also have to host other communications for their service on your PC (which exposes you to potential privacy, security and legal issues), (3) this method of anonymizing is commonly broken, due to user ignorance and carelessness, leaky protocols, Javascripts designed to bypass them, and various other tracking technologies (4) these networks generally do not permit large volumes of data transfer per user. (Please see <https://ssd.eff.org/> for a more detailed discussion of these)
 - 1.2.5.1 If you use one of these services, be sure to thoroughly investigate its privacy practices and its effectiveness at maintaining your privacy

- 1.2.6 Many stalking companies practice a technique taken from Digital Rights Management technology, known as ‘device fingerprinting’, to uniquely identify computers. If your scripting is turned off, the IP address, MAC address and browser type are available to identify you. If your scripting is turned on, everything from your computer name and user account to your installed fonts, software and browser settings and plug-ins can be used to tag you uniquely out of all internet users globally, from day to day, session to session. http://en.wikipedia.org/wiki/Device_fingerprint and
- 1.2.6.1 There are at least 2 software projects working on spoofing the OS information (to make your windows version appear different periodically), by changing certain registry keys – but they may cause many side effects. They do not appear to be close to ready for our use, as they cause anything from connectivity issues to system instability – which might expose you to a security problem. <http://www.darknet.org.uk/2006/03/security-cloak-mask-against-tcpip-fingerprinting-for-windows/> and <http://www.irongeek.com/i.php?page=security/osfuscate-change-your-windows-os-tcp-ip-fingerprint-to-confuse-p0f-networkminer-ettercap-nmap-and-other-os-detection-tools> Linux is further ahead in developing these countermeasures. Check back for a version ported to Windows: <http://ippersonality.sourceforge.net/>
- 1.2.6.2 EFF presents 2 recommendations: use the tor button and NoScript plug-ins to reduce information leakage that can be useful for fingerprinting. It also presents 2 challenges that these plug-ins do not solve: browser http header info and user-agent strings <http://www.panopticklick.eff.org>.
- 1.2.7 In future, certain technologies, called darknets or I2P, may offer some hope for private person to person communication, but not for general surfing. <http://en.wikipedia.org/wiki/I2P> and <http://www.guardian.co.uk/technology/2009/nov/26/dark-side-internet-freenet>. I presently do not recommend Freenet, because, (1) it will only run in an account with administrator privileges (because it is creating an encrypted volume on your hard drive, maybe other reasons too), and (2) there is the possibility that if illegal materials are hosted on your computer, you may be legally liable for it – whether or not you have knowledge of their presence – which if Freenet or some similar application has encrypted it, and you don’t have the means to decrypt it, you won’t know there is a problem until the police show up at your front door with a warrant.
- 1.3 Do not enter personal information online unless you specifically want that site, and anyone else it affiliates, or contracts out its user-tracking to, with (or gets bought by) to have your identity AND associate any activity at that site, or at affiliated sites to your name and be affiliated with it in the real / offline

world. (<http://www.latimes.com/business/la-fi-cover-privacy16-2009aug16,0,5238484,print.story>). Affiliating your real name to your internet usage is the Holy Grail to many marketers – because they believe that will allow them to stalk you better and sell to you better. <http://www.quantcast.com/info/lookalikes> and <http://www.webtrends.com/AboutWebtrends/NewsRoom/NewsRoomArchive/2009/WebtrendsAndTeradataIntegrationHelpsMarketersMeasureOnlineAndOfflineData.aspx> Advertisers have been working on this since at least the early 1990s. <http://www.webtrends.com/aboutwebtrends>. Eloqua claims to have achieved it. <http://www.eloqua.com/> There are also commercial databases that can be used by these stalkers to identify you. <http://www.junkbusters.com/cookies.html>. See <http://www.quiettouch.com/> for one example. Lately content delivery and stalking are being carried out by the same company, such as Limelight <http://www.limelightnetworks.com/> or Google. Notice that Google's Ad.Doubleclick stalking subsidiary is now taking your name and personal information when you sign up for certain Paypal accounts <http://media.grc.com/sn/sn-219-lq.mp3> The purpose of getting your name is to tie you to offline income, demographic, political and other information about you. http://www.tvweek.com/news/2009/05/column_targeted_ads_the_holy_g.php and

1.3.1 Do not click ads - ever.

1.3.1.1 By clicking an ad, you are generating 1 more data point about yourself.

1.3.1.2 By clicking an ad, you are inviting any executable code hidden in the ad to run. This is a common way to install malicious software on your computer.

http://news.cnet.com/8301-27080_3-20000898-245.html

1.3.1.3 Do not respond to online solicitations ever. Anything that you will be in trouble for ignoring will wither come to your house or business in the snail-mail or be hand delivered by a process server. Do not believe any emails or other electronic communications that instruct you to pay money for anything.

<http://news.bbc.co.uk/2/hi/technology/8622665.stm>

1.3.2 Do not enter anything sensitive, such as your name, into any sites that you believe to be insensitive to your privacy. INTELLITXT is just one more way of accomplishing the association of your name and all of your interests.

1.3.3 I do not recommend purchasing anything online. There is no anonymous, safe way to do it.

1.3.3.1 I do not do any online shopping, banking, etc.. You should consult another source if you wish to learn about those topics.

1.3.3.2 Websites often do not follow applicable privacy law.

<http://news.bbc.co.uk/2/hi/business/8245799.stm>

- 1.3.3.3 Websites often try to bind you to unfavorable privacy and other policies in their terms of service, that you would not be subject to if you go to their physical store and pay cash. <http://www.eff.org/issues/terms-of-abuse>
- 1.3.3.4 Certain music sites will attempt to sneak DRM and other software onto your computer as unremoveable browser plug-ins.
- 1.3.3.5 Security is also a problem when shopping online. The Gumblar virus proved this by infecting many legitimate banks and retailers sites in 2009. (http://news.cnet.com/8301-1009_3-10244529-83.html) Criminals like these then drain your accounts, open new accounts in your name, run up debts, and leave you with the mess.
- 1.3.3.6 Even sites that are certified as complaint with Payment Card Industry (PCI), Site Key and hacker-proof security standards are not necessarily safe. ‘Many of the instances of massive credit card loss are from PCI-certified sites’ <http://media.grc.com/sn/sn-219-lq.mp3>
 - 1.3.3.6.1 Trust-e Privacy certification is also crap. All it means is that the site has a written privacy policy. It does not guarantee that the site will respect you privacy in any standard meaningful way.
- 1.3.4 Also, don’t Search for yourself online, or use real name online, or social security number or anything else like that.
- 1.4 Clear your usage tracks each time you start or finish using an account. I will briefly present here how to do it in Internet Explorer. Other browsers make this much easier to do. In Internet Explorer, select menu ‘Tools;’ then click ‘Internet Options.’ Delete cookies. Delete All Files (select ‘Delete all offline content’). Delete History. Select tab ‘Content’ Click ‘Autocomplete.’ Click ‘Clear forms,’ and ‘Clear passwords.’
 - 1.4.1 In ‘Privacy’ tab, select ‘Advanced’. Select ‘always accept session cookies,’ ‘block third party cookies,’ and ‘prompt before accepting cookies. This will block cookies that anywhere *other than* the sites you are surfing, allow cookies that exist only for the length of time you are visiting that site, and will ask you to specify a cookie policy (takes a couple clicks into a browser form) the first time you visit any given website.
 - 1.4.2 When you visit a website it always tracks you in 3 ways: cookies, a dual connection to an ad-tracking site such as ads.doubleclick <http://www.doubleclick.com/> , and server-side tracking. Windows checks against the Host file and prevents any connection to any site, such as ads.doubleclick listed in it by mapping the IP address of that site back to your computer. A website may also track you in additional ways beyond this.

- 1.4.2.1 A similar technique to cookies, often used in conjunction with both cookies and a dual connection, is a web beacon. A web beacon is usually (but not necessarily) a 1x1 pixel .gif file that is stored on your hard disk by a server and is read with cookies by the network contacted by a dual connection. These are used to further track you around the internet. Theoretically, clearing cache (see 1.3) combined with forbidding automated paste by script (see 13.4.2) allows you to restrict their activity to your current session on that user account.
- 1.4.2.2 Adobe Flash also places cookies that keep 100KB of data (by default) about you. They last forever - they don't expire like browser cookies and can track you across use accounts. Adobe went to great lengths to make them hard to find - they save them in folders with a # at the beginning of the folder name so that you can't directly search for them. You have to navigate to them - and they are stored in several places in each of your user accounts in documents and settings. Thus you should have an automated approach to removing them, such as a browser plug-in.
- 1.4.2.3 Document Object Model a.k.a. DOM Cookies are massive data repositories that sites can use to track you. DOM Cookies are not yet in widespread use. They
- Store over 5MB each about you by default
 - Are less private and secure than traditional site-specific cookies. DOM cookies can be read by anyone anywhere any time you are connected to the internet, and can track you across use accounts.
 - Are implemented in the latest versions of Opera, Internet Explorer and Firefox.
- 1.4.2.4 Your IP address may be used to track your usage even if you shut down all local tracking. This is the heart of server-side tracking, as independent from client side tracking (i.e. cookies and scripts on your computer). You can't use the internet without an IP address. An IP address is like the mailing address on an envelope. 1 IP address tells the postman who sent it, and the other IP address tells him where it needs to go. Your Internet Service Provider will assign you an IP address.
- 1.4.2.5 Any script running locally has the potential to effectively track you at any site you allow it to run. Forbid all possible active content including java and Javascript, to prevent this. <http://arstechnica.com/tech-policy/news/2010/01/even-without-cookies-a-browser-leaves-a-trail-of-crumbs.ars>
- 1.4.2.6 There are several states pushing reform to limit this tracking in various ways.

<http://www.nytimes.com/2008/03/20/business/media/20adc0.html> and

<http://forums.searchenginewatch.com/showthread.php?t=9700> and <http://arstechnica.com/tech-policy/news/2009/09/privacy-advocates-want-regulation-of-behavioral-advertising.ars> . Regular people, at a grass-

roots level are beginning to take privacy and security seriously too

<http://www.nytimes.com/2010/05/09/fashion/09privacy.html>

Other people and companies, such as the Network Advertising Initiative (NAI), are trying to push false-flag initiatives that will create an appearance of reform, without end to abuse. <http://arstechnica.com/tech-policy/news/2009/07/behavioral-advertisers-state-principles-for-self-regulation.ars>

- 1.4.3 Use a strengthened host file, such as the MVPS Host file (<http://mvps.org/winhelp2002/hosts.htm>).
 - 1.4.3.1 You can and should add items to your host file as you see them. Open Start Menu; Run; type 'CMD'; type 'Netstat - a'. Any connection that should not be there should be added to your HOSTS file. Your HOSTS file lives in C:\WINNT\System32\Drivers\etc. Be sure that you do not save it with any file extension (such as .txt or .doc) when you edit it.
 - 1.4.3.2 Companies have begun using direct connections at the server level, rather than at the domain level. This means that when you add the connection you see in Netstat to your hosts file, that it will not block anything. Now you must find the website associated with that server, using a who-is lookup, which is more time-consuming. I offer a great depth of information in Section 17 on defeating these methods.
 - 1.4.3.3 Companies have begun specifying tracking and advertising connections to connect to you from their server, thus bypassing the Hosts file completely. You should add the relevant IP addresses to your firewall's list of banned IP addresses.
- 1.4.4 Unplug your cable modem between sessions to get a new IP address, every time you shutdown.
 - 1.4.4.1 Verify this. Use Start Menu, 'Run' to launch cmd.exe. type IPconfig /all. Write down your IP address on paper – or make a screencap using the Printkey utility I recommend you install in 9.2. After rebooting, check it again.
 - 1.4.4.1.1 If it has not given you a new IP address, run IPConfig / release. Then run IPConfig /renew. Verify it has changed. You may need to reboot.

- 1.4.4.1.2 See <http://support.microsoft.com/kb/314850/?sd=R> MVP and [http://technet.microsoft.com/en-us/library/dd197434\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/dd197434(WS.10).aspx) for more IPconfig documentation.
- 1.4.4.1.3 In section 13, I will show you how to automate this task so it runs automatically for you.
- 1.4.4.2 You may not actually get a new IP address this way. There are various programs that automate switching your IP. I do not recommend any pay-for software or service, because you have to give them your real name and credit card – which defeats your privacy.
- 1.5 Email is both a necessity and a vulnerability.
 - 1.5.1 Your email is generally not private; see <http://www.YourHackerz.com>
 - 1.5.2 Do not use Google's Gmail, or Yahoo Mail. <http://www.informationweek.com/news/windows/security/showArticle.jhtml?articleID=224700847>
 - 1.5.3 Encrypted e mail services are available. They use sophisticated encryption and other technologies that can reduce the ability of third parties to intercept and read your emails. These are more effective, but still are not anonymous, because you generally have to provide real name and charge card billing info to the email provider. Furthermore, their privacy policies vary in strength.
 - 1.5.4 Many sites require registration using a valid email address, to which they send something to which you must reply before allowing you to browse. You should sign up at a couple email providers for a dummy account that such sites can have. You should have 1 such dummy account for each group of interests you wish to be separated.
 - 1.5.4.1 Use a temporary email account from <http://10minutemail.com/10MinuteMail/> for junk registrations.
 - 1.5.4.2 In 2008, I started noticing that certain asshole websites have begun requiring registration using a corporate, school or ISP email account so they can tie your use of their website to your name, etc. Google tried to tell you, in bold-face print, that this does not violate your privacy. Bullshit. http://mail.google.com/mail/help/about_privacy.html
 - 1.5.5 Emails and their attachments are the source of many problems ranging from annoying ads to phishing scams to malicious software being installed on your computer.
 - 1.5.5.1 Outbound attachments may have a privacy risk, if they contain so called metadata such as your name.
 - 1.5.6 Email is the source of many scams. Some warning signs to look out for are provided here:

<http://www.switched.com/2009/10/26/10-ways-to-spot-an-e-mail-scam/>

- 1.5.7 IMAP is preferred to POP for email retrieval, because it is less likely to lose messages. <http://www.emailaddresses.com/POP3EmailAccountReviews.mht> is a good place to start looking for an email account.
- 1.5.8 Attachments may occasionally need to be locked and encrypted. See <http://www.7-zip.org> and <http://www.truecrypt.org> for useful products. See section 2.6.3 for encryption best practice. Do not send the password via the same communications service you use to send the file.
- 1.6 Search is both a necessity and vulnerability. Companies such as Google make their money off of advertising. Because of this, you can be certain they will do everything in their power to track your internet use. Companies such as Google continually upgrade their snooping to counter your privacy-defenses.
 - 1.6.1 [Http://www.scroogle.org](http://www.scroogle.org) may be a useful option for some. They claim to act as an anonymizing intermediary between you and Google. They appear to be entirely funded by donations, and I have not yet seen anyone challenge their good reputation.
 - 1.6.2 <http://clusty.com/> is another search option maintained by the University of Pittsburgh.
 - 1.6.3 <http://www.ixquick.com> is another good search option.
 - 1.6.4 Be aware that since 2010, Yahoo Search and Microsoft's Bing engine are now one and the same. This has implications for anyone using any of their other properties such as Hotmail or Yahoo Sports...
- 1.7 Instant Messaging is a necessity for many people.
 - 1.7.1 Pidgin IM client and OTR (Off The Record plug in for Pidgin) can effectively secure instant messaging sessions. <http://pidgin.im/> and <http://www.cypherpunks.ca/otr/binaries/windows/>
 - 1.7.1.1 The Pidgin does not work with video, however. I know of no product that will do this at this time.
 - 1.7.1.2 Pidgin will work in a restricted user account.
- 1.8 Choose a good ISP. A good ISP will generally cost more – because they are not snooping on your usage and selling your usage info to advertisers.
 - 1.8.1 This is a must: if your ISP does not respect your privacy, it makes no difference how discreet you are.
 - 1.8.1.1 For over a decade, NETZERO has provided free dial-up internet service in exchange for tracking everything you do, and then serving you ads. At least they have the decency to tell you of this practice so that you can make an informed decision as to whether you want to use their service. <http://www.thefreelibrary.com/NetZero+Takes+In-Depth+User+Profiling+to+New+Level-a066357751>

- 1.8.1.2 Virgin's ISP business and Charter engage in such aggressive behavioral targeting. Others are considering it – and may have already begun.
- 1.8.2 You want one that does not engage in targeted or behavioral advertising, i.e. does not match up your name and other info to browsing habits. <http://seoserpent.com/isp-behavioral-targeting-2008>
 - 1.8.2.1 I am aware of no resource that will currently tell you if your ISP is doing this (<http://www.vancouver.cs.washington.edu> used to, but it is now defunct)
- 1.8.3 You want an ISP that gives a dynamic IP address. (recall 1.3.2.4)
- 1.8.4 You want an ISP that does not physically install Deep Packet Inspection hardware at its facilities to serve targeted advertising to you: such hardware generally associates your name to your browsing habits and is not able to be defeated by anything that you can *practically* do. <http://www.washingtonpost.com/wp-dyn/content/article/2008/04/03/AR2008040304052.html>
- 1.8.5 You want an ISP that does not save your DNS lookups and associate them with your name. DNS is the mechanism that allows your ISP to know where to route you when you try to open <http://www.somewhere.com>
 - 1.8.5.1 Various alternative DNS providers are available. Generally, these are fee-based services, that need your credit card (name) to bill which gains you no privacy, or they are ad-funded (evil) like Google.
- 1.8.6 You want an ISP that does not reduce your connection speed or block any traffic that you solicit. <http://arstechnica.com/tech-policy/news/2010/04/comcast-owes-users-16-for-p2p-blocking-should-they-take-it.ars>
- 1.8.7 You want an ISP that does not cap your usage at a level below what you expect to use (think 1GB/day is reasonable) and charge you for exceeding it. <http://massa.house.gov/?sectionid=24§iontree=23,24&itemid=205>
- 1.8.8 Read and print your ISP's Privacy and other policies. A good privacy policy will say something to the effect of "This ISP does not reveal any of your information, under any circumstance, unless we receive a subpoena from a court of law." Warning: proposed legislation, even in the most progressive countries, threatens to someday require your ISP to spy on you. <http://arstechnica.com/tech-policy/news/2009/05/eu-sues-sweden-demands-law-requiring-isps-to-retain-data.ars> and <http://www.eff.org/wp/anatomy-bogus-subpoena-indymedia>
- 1.9 Do not use social networking: The websites, such as Facebook do not respect your privacy (<http://www.itbusiness.ca/it/client/en/home/News.asp?id=56900>)

) and (<http://privacy.org/archives/003635.html>). Governments routinely trawl these networks looking for evidence that could be used against you. They also set traps for the stupid to get themselves into trouble.

(http://www.pcworld.com/article/191688/your_next_facebook_friend_could_be_a_federal_agent.html)

1.10 Do not store unencrypted passwords.

1.10.1 Note: the encrypted passwords in Firefox, Opera, Internet Explorer, are not truly locked down. They can be read, in unencrypted, by importing them into another browser. Users who are *not* using the NTFS file system, are even less secure in their encryption (see section 4.4) Use a Truecrypt (<http://www.truecrypt.org>) container to store passwords and any other sensitive material that you keep on your online computer. Generally, you should try to minimize the amount of sensitive material stored on that computer.

1.11 Your government is probably tracking you right now. The US and British governments began reading their citizens private emails several years ago. <http://cryptome.org/cryptome-01.jpg> provides several leaked documents that describe various companies policies for complying with government spying requests. Currently, there are calls for legislation to provide a single fair standard for this spying with judicial oversight (<http://news.bbc.co.uk/2/hi/technology/8595775.stm>)

1.11.1 The British Government is currently implementing a plan to store all emails for a period of 3 years.

1.11.2 Since the late 1990s, the US FBI has employed various software, popularly called ‘Carnivore’ and ‘Omnivore’ to scan the internet for various criminal activities. It deployed local software ‘Magic Lantern’ to log activity on citizens’ computers. More recently, a program, called CIPAV has been used to reveal IP and MAC address of computer users – and entered as evidence in criminal cases. (Please see http://epic.org/privacy/carnivore/foia_documents.html for a more detailed discussion of these). Lately, evidence obtained by government-spyware installations such as these were entered in court in at least 3 separate cases. More recently, rumors of varying credibility have circulated that the government was using commercial software in addition. For a look at one such commercially-available software, see (<http://www.eblaster.com>). IT is lately reported that the government is looking to require companies to provide a backdoor into all forms of communication and computing. http://news.cnet.com/FBI-adds-to-wiretap-wish-list/2100-1028_3-5172948.html

1.11.2.1 It is not known if these software and surveillances are ran only with a warrant from a court, which would probably a fair and a good thing for the government to do in the course of fighting actual crimes. It may instead be

instead that the government runs them every time it can get away with, which would be unconstitutional, and should be exposed and abolished.

<http://www.eff.org/press/archives/2009/06/23> and <http://www.aclu.org/safefree/general/41189prs20090929.html>

In at least some instances, these surveillance initiatives seem to be run in defiance of the law.

http://www.theregister.co.uk/2007/09/03/german_trojan_plan/

I am not aware of commercially available way to detect or disable these at present. Just pay attention to your computer security and usage logs and to your active connections (this will be discussed in depth in section 17).

1.11.2.2 For the sake of fairness, it should be noted that governments in several countries, including USA, are beginning to take action against certain malicious software and their creators.

1.11.3 The US government, since the passage of the 2001 USA Patriot Act has begun compiling vast databases of citizens' activities, including their online activities.

<http://www.aclu.org/safefree/general/24287res20060227.html>

There is essentially no limit to what information they collect.

<http://www.aclu.org/safefree/general/41144prs20090924.html>

In the 8 years since, the US government has compiled a data warehouse of over 900 million unique documents. For comparison, the US Library of Congress has collected less than 140 million unique documents in its 24 decades of operation.

Clearly the scope of this is much wider than the prevention of terrorism. What is more amazing is that the Obama administration is *expanding* the amount of surveillance both in this country and abroad. (<http://epic.org/events/Privacy%20Report%20Card.pdf>,

<http://www.eff.org/press/archives/2009/04/05> and

<http://www.mainjustice.com/2009/09/15/justice-department-supports-renewal-of-patriot-act-provisions/>) A 2009

congressional report states that random sampling is used to target individuals' communications for surveillance. (

<http://www.eff.org/issues/foia/investigative-data-warehouse-report>

) Finally, it should be noted that a Federal Judge has ruled that this program is ILLEGAL under American law (

http://www.salon.com/news/opinion/glenn_greenwald/2010/04/01/nsa/index.html)

The government has previously tried to create legal immunity for such practices and may try again. (

<http://news.bbc.co.uk/2/hi/americas/7269452.stm>)

The court system is not enforcing existing constitutional protections at this time.

<http://www.aclu.org/safefree/nsaspying/41223prs20091001.html>

- 1.11.4 In the USA, and most everywhere else, lack appropriate privacy safeguards in the law to protect citizens from their government. <http://arstechnica.com/tech-policy/news/2010/04/the-cloud-and-the-future-of-the-fourth-amendment.ars> . Many initiatives ranging from well-meaning to beside-the-point have been proposed to resolve this
<http://www.npr.org/templates/story/story.php?storyId=106479613>
- 1.11.5 Help yourself by not engaging in anything that is illegal in your country, such as online piracy.
- 1.11.6 Other foreign governments have been implicated in widespread online spying. In 2009, a Chinese government network of compromised computers in 103 countries was exposed. (<http://arstechnica.com/security/news/2009/03/potential-chinese-cyberspy-network-runs-across-103-nations.ars>).
- 1.11.7 Cyber warfare and spying is amazingly cheap, according to the military ... Rule of thumb: you should expect any government with any military capability and/or aspirations at all, is testing ways to attack and spy on computers and internet communications.
<http://www.npr.org/templates/story/story.php?storyId=105962021> and <http://news.bbc.co.uk/2/hi/americas/4655196.stm> The US government just transferred 30,000 air force personnel into cyber war duties
http://www.airforcetimes.com/news/2010/05/airforce_cyber_careers_051710/
- 1.12 Do not install any software on your machine that will violate your privacy.
 - 1.12.1 Note that certain games from Electronic Arts and Ubisoft, include Digital Rights Management technologies that require you to connect to their server in order to play. You should either avoid these studios' titles altogether, or you should obtain a crack for any game that you purchase that has such DRM in it. (http://news.cnet.com/8301-27076_3-20000506-248.html)
 - 1.12.2 Certain software connect to their company's server for purposes of updating. In most, but not all cases, this is harmless. Lock it down in the program, and set a rule in your firewall to prevent these programs connecting without your permission.
 - 1.12.3 Certain software have features that try to connect to the internet, for example, for uploading pictures or other information, or for downloading info, for example, about the CD you are playing on your machine. Again, you should lock it down in the program, and set a rule in your firewall to prevent these programs connecting.
- 1.13 Secure your computer!
 - 1.13.1 Understand that procedures for securing your computer are much stronger than those for protecting online privacy. Your online privacy depends first and foremost on you not giving out information online. It depends almost as much on securing your

computer. If you allow spyware, etc. to run on your computer, no amount of online caution will keep you private.

HOW TO MAINTAIN INTERNET SECURITY:

(Note: I find it takes 5 ½ hours to set up a computer. You should budget twice as long for the first time that you do this.)

2.0 Your Best Strategy:

2.1 Establish physical security. If you are reading this paper, you must have some reason you care about privacy and security; for example, you may be politically active in support of a controversial cause.

2.1.1 Use common sense and take simple precautions:

2.1.1.1 Close your windows before entering passwords or transacting sensitive business.

2.1.1.2 In case of fire, etc. keep an encrypted backup of anything important and all software installation CD images in a safe place, such as in the office of a lawyer whom you are friends with.

2.1.1.3 Do not invite police search and seizure by engaging in illegal activity, or by giving the appearance of engaging in illegal activity.

2.1.1.3.1 If you are critical of a certain government or business, try to operate outside of its jurisdiction or areas that will cooperate with it.

2.1.1.4 Know that any physical lock, safe or barrier can be broken quickly and easily.

2.1.1.5 Do not allow unnecessary people to have any access to your computers and associated things.

2.2 I recommend either Windows 2000 Pro or later for stability, privacy and security.

2.3 In Windows operating systems, most attacks involve the following items - and I recommend taking maximum precaution, especially in regards to these 3 notorious methods of attack:

- taking advantage of un-patched Microsoft vulnerabilities,
- people doing something dumb such as surfing in admin, and then clicking booby-trapped email attachments
- Finding some creative way to exceed the amount of memory allowed for storage of a particular data object – which then allows part of the object to ‘overflow’. The portion overflowing, if it is executable code, can then run and do whatever it wants to your system.

2.4 The procedures here are presented exactly as they appear in Windows 2000. Windows XP and 2000 are very similar operating systems; for purposes of configuring the security settings – they have essentially the same options – although they are presented slightly differently. (I have used Vista only a few times, and can not recommend settings for it. I am told that Linux and FreeBSD can be made just as secure as Windows, and I am looking into Red Hat Linux as a replacement for Windows 2000 when Microsoft ends its support.). For the record, Windows Vista and 7 introduce 4 legitimately

valuable security features who's improved security may be more important to you than the loss of privacy due to Microsoft Product Activation:

- Address Space Layer Randomization (usually abbreviated ASLR) load the system files to a different address in memory each time the computer is booted. This keeps malicious software from easily guessing their location and overwriting some of them with something to use against your system. For example root kits intercept and modify or eliminate certain procedure calls in memory to hide themselves and control the computer; certain Windows cracks prevent the Windows Product Activation and Windows Genuine Advantage check (for piracy) from functioning.
- Data Execution Prevention (usually abbreviated DEP) borrows an idea from UNIX and Linux: make a certain portion of memory un-executable so that no attacks can be launched from there. This is a neat solution to the Buffer Overflow method of attacks.
- Kernel Protection, theoretically, makes it impossible for a malicious program to edit or replace key operating system files
- User Access Control (usually abbreviated UAC) requires user confirmation before some (usually) admin level change is made. This is supposedly similar to but more thorough than the registry change protection provided by tea-timer from the maker of Spybot Search and Destroy.
- COUNTERPOINT: Different tests of these features have lately questioned their effectiveness at stopping malicious software.

2.4.1 The Case For Using Windows 2000: Microsoft products since Windows 2000 have not offered me any reason to upgrade. In fact they have offered many reasons not-to-upgrade, such as crippled versions, WGA / Product Activation, DRM/Trusted Computing, increased memory/processor consumption, high cost to upgrade, and many other lesser issues. I don't see any reason to upgrade MS Office either. For those of you who still need to run Windows apps (other than games), I suggest you get an old beater computer, and slap a copy of Windows 2000 on it. (I built an AMD Athlon XP system with win2k when I was in college – and it runs circles around my friend's brand-new laptop with Vista – almost a decade after I built it). Windpows 2000 run acceptably on as little as a 1GHz Pentium 3 with 64MB RAM. It can run very fast on a 2GHz Pentium4 with 384MB RAM.

2.4.1.1 COUNTERPOINT 1: Isn't there an unpatched vulnerability in Windows 2000? Yes... The vulnerability exposes servers running Windows 2000 to Denial of Service attacks – which should not be a privacy or security problem for home users. They note you can avoid such an attack by using a firewall.

(<http://www.microsoft.com/technet/security/bulletin/MS09-048.msp>)

2.4.1.2 COUNTERPOINT 2: Won't there be more problems with unpatched Windows 2000 vulnerabilities after Microsoft stops issuing patches in July 2010? Yes – you can expect that most vulnerabilities found in XP, Server 2003, etc. will also be found, in some form, in Windows 2000. There may also be other exploits specific only to Windows 2000. You can either make very certain of your other layers of defence or you can upgrade to another OS).

2.4.1.3 COUNTERPOINT 3: Aren't there many vulnerabilities in Windows 2000's default settings? Yes – but I will show you how to fix them quickly and effectively.

2.4.2 The Case Against Windows XP and higher:

- Product Activation – makes it difficult to reformat and reinstall on a schedule. System Restore does not provide effective substitute.
- Windows Genuine Advantage checks in with Microsoft periodically, including, to check if you are running any activation cracks.
- Volume Shadow Copy Service (enabled by default) makes backup copies of files, including, possibly, those you meant to erase
- Crippled versions (i.e. Home or Media editions) do not provide the security features you need.
- Require a faster computer with more memory.
- implement a variety of technologies in software, such as DRM that inhibit your use of your computer.
- Windows Vista and higher require hardware that enables a variety of DRM and “Trusted Computing” measures that can prevent you from using your computer and content as you see fit.
- Windows Vista and higher come with a Bit Locker feature that has backdoors built in that can be exploited, at least, by governments and police forces, and the domain administrator if you are a member of a network domain.
- Its not worth the high price.

2.5 Increasingly, it is reported that threats are being tailored to attack very specific systems – rather than all systems in general – partly to help avoid detection and being added to an antivirus program. The know-how and kits to do this are becoming increasingly common, so look for these attacks to become common among home users too.

2.5.1 Recently, some attackers have been using other peoples' computers for purposes of trafficking in child pornography, and the computer owner then is prosecuted instead of the pedophile(s) (<http://stevensponaule.wordpress.com/2009/11/09/computer-viruses-can-load-child-pornography-onto-computers/>) Never

- allow someone else to put you into a position where you can be charged with a crime of any sort: put your systems on lock-down.
- 2.6 You should use 2 computers: 1 computer for internet and 1 for everything else except internet. You can buy a computer to use for internet only for USD80 to 150. (Many people will not want to do this. This makes following the steps in the rest of the paper even more critical for them).
- 2.6.1 If you get a virus or other problem, from the internet, your loss is limited to your installation of Windows on the for-internet computer. All of your work, programs, etc. are still safe on your not-for-internet computer.
- 2.6.2 Never connect the not-for-internet computer to the network. Never plug any drives into the not-for-internet computer that have not first been scanned for viruses and other malware. Don't store personally identifying or sensitive files on your for-internet computer.
- 2.6.3 If your not-for-internet machine contains sensitive information, use an encryption program such as the Free Open Source Software at <http://www.truecrypt.org>.
- 2.6.3.1 Why bother with encryption? Sensitive files, such as political, financial, legal or government documents, lists of passwords to email or financial accounts, backed-up software-installation-images and systems-settings are all good things to encrypt. In addition, due to the mean and petty nature of our society, individuals, and companies, should have a policy of regular encryption and/or destruction of any data that is sensitive and/or could be used to harm them in any way, whether through blackmail, exposure of something one wants to keep private or through civil litigation, or a criminal complaint, etc...
http://www.csoonline.com/article/491786/Why_Information_Must_Be_Destroyed_Part_Two and
<http://www.bbb.org/us/secureid>
- 2.6.3.1.1 Question: Who cares what I have? Jealous ex spouses and lovers, corporate snoops looking to fire you, insurance companies, banks, criminals, marketers and your government would all like to know as much as they can about you.
- 2.6.3.1.2 Question: For a home user who can't afford a degaussing machine, as described in the previous link, how should I safely dispose of a dead unencrypted hard disk I have? Answer: unscrew the case, remove the platters (the round shiny things inside) and melt the platters in a hot fire.
- 2.6.3.1.3 Question: Why bother protecting my computer-info, when I have so many vulnerable account

statements, etc on paper? 1 option might be to scan key items onto an encrypted hard disk and destroy the originals. Pro this enhances privacy – as anyone with a pry-bar or a drill can break a filing cabinet lock. Con this takes much time.

2.6.3.1.4 Question: Isn't it hard to hack into a computer protected by everything in this paper? Answer yes – but – the communication coming out of the computer must also be protected. There are many tools that make it easy to break into your communications outside of your computer, see <http://www.wireshark.org/> .

2.6.3.2 Isn't encryption difficult and time consuming, and how does it work? Yes and no. Encryption involves an up-front effort to format a drive, and move files into it. There-after, encryption is not that much work. At a high level, encryption involves mathematically transforming the file system to some other representation that is understandable only to a machine that has the encryption/decryption software and the correct keys, etc. Then random data is written across the entire disk, to make it unclear where the data is stored. Finally one 'mounts' the partition (makes it appear as a hard disk to the system) and moves ones files into the encrypted partition.

2.6.3.2.1 When moving sensitive files into the partition, make sure to securely delete them. There are various utilities available to do this, such as the one that comes from <http://safer-networking.org>

2.6.3.3 Notice that encryption, properly done, is difficult to defeat. Notice that encryption is generally bypassed, not broken. Bypassing encryption involves either user error (leaving things decrypted, <http://cryptome.org/crypto-spy.pdf>), or various James Bond style gadgetry that picks up some leaked electronic signal that contains the password, or else some other forensic techniques such as capturing data from RAM or the windows swap file <http://www.irongeek.com/i.php?page=videos/anti-forensics-occult-computing> . There are certain software just for this <http://www.guidancesoftware.com/> There are many proposed attacks against encryption. Private citizens who are neither engaged in criminal activity, nor appear to be, should probably be OK to use a commercial product with a strong password, (see section 6 for good password practices) and a conscious policy of re-encrypting ones sensitive material as soon as one is through using it. Law-abiding citizens will probably not face James-Bond caliber

opponents. Notice that decryption is not permanent – powering off your machine should remove decryption of any files.

2.6.3.3.1 Various software such as Window Washer can help by cleaning up programs' caches after you edit an encrypted document (for example MS Word may cache your letter to your bank).

<http://www.ewasher.net/>

2.6.3.3.2 Do not count on such programs to protect you.

<http://cryptome.org/intelliforms-spy.pdf>

3.0 Prepare to install Windows: Reformat your hard drive. If you just reinstall Windows, it won't reformat the hard drive. Always reformat your hard drive before installing Windows to eliminate Root Kits.

3.1 Download all patches and save them to a flash drive. Before starting this procedure download the network (ENU) versions from

<http://www.microsoft.com/downloads/en/resultsForProduct.aspx?NextOrPrevClause=6%7c%2b12%2f11%2f2006%2014%3a59%3a25.750&DisplayLang=en&productID=A33A864D-A301-4DD8-830C-809D66BD6265&sortCriteria=date&sortOrder=descending&nr=20>

3.2 Prepare for installation. If your computer can not boot directly to the Windows 2000 installation CD, you should use 'Makeboot' (<http://support.microsoft.com/kb/197063>) to create the windows 2000 boot disks.

3.3 Using a Windows 9x/ME bootable disk, type 'FDISK' at the command prompt. Press Enter.

3.3.1 Navigate the menu to Display partition information. Make a note of all partitions.

3.3.2 Exit to the previous menu level and then use the menu option Delete Primary DOS partition (or Delete non-DOS partition, as the case may be).

3.3.3 Delete all existing partitions.

3.3.4 Reboot to save changes.

3.4 Run FDISK again and make any partitions you need.

3.4.1 Reboot to save changes.

3.5 Run FDISK again and verify the changes were successful.

3.6 Type 'Format C:' at the command prompt. Press Enter.

3.7 You can instead use G Parted. Just be sure to make your partition primary - that is - bootable (<http://www.gparted.sourceforge.net/downloads.php>).

3.8 You may automate subsequent installations, by using a disk backup software to make an encrypted image on a removable device before you ever get online. You can then Follow section 4, apply service pack 4, and then reload from the backup. This would save you much time that would be spent configuring your machine.

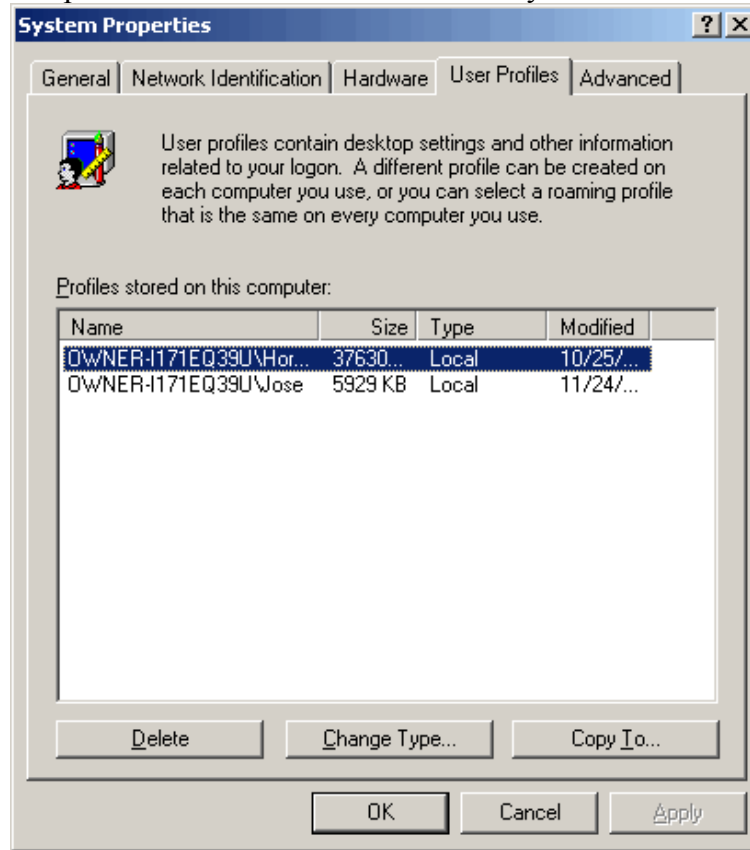
4.0 Install Windows:

- 4.1 Reboot.
- 4.2 Remove the Windows 9X/ME floppy.
- 4.3 If your computer can not boot directly to the Windows 2000 CD, then insert into the floppy drive, your Win2K boot Floppy 1.
 - 4.3.1 It will prompt you to put in disks 2 -4 and the install CD. Do as it asks.
- 4.4 Make sure the File system on all your drives is NTFS. NTFS implements several security and encryption features not found in FAT. Setup will ask you if you wish to convert to NTFS.
- 4.5 Install Windows with the standard features, using the registration key that came with the software. If you have mislaid the key since you purchased your copy of Windows, you may use any of the standard keys found online.
- 4.6 Do not make your computer part of a domain - unless you know what a domain is and that you need to be part of one.
- 4.7 Set Automatic Updates to Manual. Click 'Start,' 'Settings,' 'Control Panel,' 'Automatic Updates,' 'Turn off Automatic Updates'
 - 4.7.1 **BE CERTAIN OF THIS:** check Microsoft website yourself for updates. They are made available in the second Tuesday of every month. Skim the description of the update to make sure that you are really getting a security update and not something else (for example, Windows XP and higher users were given antipiracy updates that phone home to Microsoft). It is possible that Microsoft could put something unwanted into an update and say give it a false description... but at some point you have to trust something.
- 4.8 Do not *yet* specify a logon password.

5.0 Secure your PC with accounts:

- 5.1 Make an unprivileged user account for each of group of online interests you wish to keep separate by using 'User Accounts' in Control Panel.
- 5.2 Make 1 unprivileged account for each set of activities you wish to engage in. For example, I have 1 account each for professional, social, political and for any other interests you might have. You may wish to have more or different accounts.
- 5.3 Once you have got the first account set up you can clone it and rename it. Go to my computer. Right click properties. Click tab 'Users' and there should be

an option to clone accounts. This saves you a lot of time.



- 5.3.1 Never retain cookies and so on in any account after you are through surfing. Follow the instructions in section 1.3 before switching to any other account.
- 5.3.2 Never use an account to do things that you do in another account: for example, don't look at political material while logged in to your professional account under your real name...
- 5.3.3 **BE CERTAIN OF THIS:** write down your user name and password for each account and keep it in a safe place where you will remember it. **WRITE DOWN YOUR ADMINISTRATOR PASSWORD ON PAPER! KEEP IT IN A SECURE AND PRIVATE PLACE! AFTER YOU ARE POSITIVE YOU HAVE MEMORIZED IT, SHRED IT AND BURN THE SHREDDINGS!**
- 5.4 When setting up your passwords, try to use a combination of upper and lower case letter, numbers and several nasty characters like ? , ¥ □ û , ÷ , ½ , å , etc.
 - 5.4.1 Include a mix of
 - Letters a, b, c, etc.
 - Numbers 1, 2, 3, etc.
 - Symbols @, #, \$, etc.
 - punctuation !, ., , etc.

- non-standard characters ĩ, š, F etc. For example, make ñ by holding down the ALT key and, at the same time, pressing, in sequence, the 0, 2, 4 and 1 keys in your number pad on the left of your keyboard. You don't want to make this easy for someone else to guess.
- 5.4.2 Don't feel the need to restrict yourself to the latin alphabet. You can use greek, hebrew, cyrillic, arabic, and various eastern European characters. For example, one of my no-longer-used passwords was YmjB□226□t□@88ĩš%.
- 5.4.3 Make it at least 9 characters long. Passwords less than this length can be guessed very quickly by using the so-called LM Hash technique.
- 5.4.4 Make passwords easy for you to remember, by giving them some structure that makes sense to you, but would not to someone else. Several techniques are:
- 5.4.4.1 construct the password out of building blocks. The password š¼Pç111JzyP4583qVBMF%Jasmine is an easy password to remember. Really. The first block of 5 characters are all ALT characters. The second 3 characters are just a block of 1s. Then there is a block of letters, a block of numbers, another block of letters, then a symbol thrown in to make it a little more challenging, and then Jasmine.
- 5.4.4.2 Use easy blocks to remember. In the password example above, the first block of ALT characters are all made by pressing, ALT + 0 and then some other key 3 times, such as ¼ is made by ALT0444...The block QVBMF was a block from a software installation key I had to enter enough times, that it stuck in my head. Jasmine is a common name.
- 5.4.4.3 Lead yourself to build an easy password make it so that, each block should suggest the next block. Use odd combinations that make sense to only you.
- 5.4.5 One-time-use passwords don't have to be remembered. Make them using concepts from music. Lay down a bass line of junk by dragging your hand around the keyboard:
awzxdcftgvhbujnikop[:/olijuytreWSfdtyhujiklp;[opliuytrdfcguhiop
[o;ilu,jhmygtfds. Then add in treble to this. A few ALT characters and a few real words will do the trick:
ĩawzxdcftgvhbujnikop[:/olijuytreSonOfABitch!!!wsfdtyhujiklp;[
opliuytrdTfcguhiop[o;ilu,jhmPASCAGOULAYgtfds.
- 5.4.6 (5) Notice that things that are password protected are generally encrypted to shield them from access without the password. Encryption is generally effective at strengths of 256bit or higher. Done properly, 64bit can be difficult to break – but why take chances? Such strong encryption is generally not broken - it is

instead bypassed. There are many difficult, complicated and unlikely attacks that are known to be able to do this. For what we are doing, it is probably enough to use a commercial product, with good passwords, and take care that we don't expose the password unnecessarily.

- 5.4.7 This works too: <https://www.grc.com/passwords.htm> ... and it saves me the work of programming it myself.
- 5.4.8 Use 9 or more characters in your password. Shorter passwords can be attacked much faster using the 'LM hash' technique.
- 5.4.9 Never use combinations of personal information like your name or interests like 'football' that could easily be guessed by someone who knows *about* you.
- 5.5 Always make 1 temporary admin account not password protected, and write down your passwords, and test them thoroughly. (You can fix your mistakes using the unprotected admin acct.)
- 5.6 **BE CERTAIN OF THIS:** After you verify all passwords are functional, you should remove the temporary admin account before going online.
- 5.7 Rename your Administrator account.
- 5.8 **NOTE:** Especially for offline computers, certain programs may insist on installing to only 1 user account. In this case, you need to elevate privilege of that account using the same dialogue screen as you used to create accounts. Then log into that account, and install the program. Then re-open the accounts dialogue box and lower the account privilege to 'restricted user'. You will need to log out again for the lower privilege to take effect.

6.0 Install your Hardware Drivers: Install all the device drivers that you ever wish to use on the computer, such as your printer, camera, video card, and so on... If your motherboard or computer manufacturers have provided a driver CD, now is the time to use it. (You can always use your administrator account to install more devices later as you acquire them.)

- 6.1 Right Click 'My Computer'. Select 'Device Manager.' Write down, on paper, a list of any devices that are malfunctioning (indicated by a yellow exclamation point icon in 'Device Manager').

7.0 Set up Your Network:

- 7.1 In Control Panel, right-click each connection, and select 'properties'. De-select 'File and Printer Sharing for Microsoft Networks'. Click 'OK'.
- 7.2 In Control Panel, select 'Network and Dial-Up Connections'. Right-click each connection, and click Properties. De-select the box for 'Client for Microsoft Networks'.
- 7.3 In Control Panel, set the network tracking to display on the desktop when active (control Panel --> Networking --> LAN --> check the option to display network manager when online).
- 7.4 (OPTIONAL) While you are here, you may also set up TCP/IP filtering. TCP/IP filtering can provide an extra layer of security (it blocks connections over certain ports)

- 7.4.1 Highlight the line for 'Internet Protocol TCP/IP'. Click button 'Properties.' Click button 'Advanced.' Click tab 'Options.' Check the box for 'Enable TCP/IP Filtering'
- 7.4.2 At a minimum, you will need to allow these ports: 53 (DNS), 67-8 (DHCP) 80 (HTTP), 137-9 (NetBios). If you wish to allow updates by an antivirus or communication by other software, such as an email or instant messaging client, you will need to find out, from that company, what port it uses and open it.
 - 7.4.2.1 Another good source of info is <http://www.iana.org/assignments/port-numbers>
- 7.4.3 Caution. Certain applications will give you much trouble when you set up TCP/IP filtering: Back in the day, browsers and other applications used a small fixed set of ports. It was easy to block out most ports that should not be open. Presently, many applications, including web-browsers, instant message clients, etc. will assign a random port from within a large range – and may fail to function if their first-choice of port is blocked. Depending on your security needs, it may not be worth the hassle, especially if you have an excellent firewall (the firewall will create effective defensive rules for you).
- 7.4.4 A good reference is available at <http://i3.technet.microsoft.com/en-us/library/mtps-bn20100217.html>

8.0 Install Windows Patches: ALWAYS install patches from a local offline source, because your computer is not yet ready to get online (imagine a naked man walking to a store to buy clothes - he might have a problem).

- 8.1 For users of Windows XP and higher: NEVER allow WGA updates to install locally. Use the 'Alternative Validation method,' if you must validate. WGA violates your privacy by contacting Microsoft periodically to check your software for cracks.
- 8.2 (I present the patch process for Windows 2000. WinXP, etc., work similarly.)
- 8.3 Install Service packs 1 - 4, in order. Do not backup the files. It wastes time and disk space.
- 8.4 It is also a good idea to have a copy of Internet Explorer 6 Service Pack 1 – in case you ever want to let Windows Update check your machine for you. Download the installer from Microsoft's website (go to Microsoft.com and search for internet explorer 6) download the 481kb installer file and save it to C:\. This file does not install internet explorer what it does is fetch the files for you. Next click 'Start Menu' then 'Run'. Type this .

```
ie6setup.exe /c:"ie6wzd.exe /d /s:""#E"
```

that will download all the install files (over 50MB) for you.

- 8.5 Then install updates since then. As of 2-14-2010, my for-internet machine uses the patches shown below. Check the windows update site the first time

you do this to make sure you haven't missed anything you need. After that just pay attention to the monthly security bulletin
<http://www.microsoft.com/technet/security/bulletin>

Windows 2000 Professional Patches		
<ul style="list-style-type: none"> Q820608 000_USB Drivers 000_Windows Script5point6 001_BITS2point0 002_Windows Installer 3.1 Redistributable 003_KB329115_Reboot before 004_Dot Net Framework 1 and 2 005_KB901214 006_KB893756 007_KB899587 008_KB896423 009_KB905414 010_KB899589 011_KB901017 012_KB896422 013_KB896358 014_KB900725 015_KB905749 016_KB905495 017_MDAC2point8 018_KB911564 019_KB908531 020_KB913580 021_KB914388 022_KB917008 023_KB920670 024_KB920683 025_KB921398 026_KB905590 027_KB923191 028_KB923980 029_KB924270 030_KB928843 031_KB924667 032_KB918118 033_KB926436 034_KB925902 035_KB920213 036_KB927779_reboot before 037_KB927891 038_KB935839 039_KB925398 040_KB926122 041_KB938827 042_KB891861_Update Rollup 1 043_KB922582 044_KB923810 045_KB937894 046_KB943485 047_KB943055 048_KB944338 	<ul style="list-style-type: none"> 049_KB950749 050_KB950974 051_KB952954 052_KB958644 053_KB955069 054_KB957097 055_KB954600 056_KB956802 057_KB958687 058_KB960225 059_KB967715 060_KB960803 061_KB959426 062_KB923561 063_KB952004 064_KB961501 065_KB970238 066_KB971633 067_KB961371 068_KB971557 069_KB973869 070_KB958470 071_KB973507 072_KB933579 073_KB960859 074_KB973354 075_KB956844 076_KB973525 077_KB974112 078_KB958869 079_KB969059 080_KB971486 081_KB974571 082_KB969947 083_KB971961 084_KB976325 085_KB951748 086_KB974318 087_KB974392 088_KB976138 089_KB955759 090_KB973904 091_KB890830(MRT) 092_WMP9_Reboot before 093_KB828026 094_KB941569 095_KB938464 096_KB110806_DotNet FW 2SP1 097_KB952069 098_do net FW 1 sp1 099_KB973540 	<ul style="list-style-type: none"> 100_KB968816 101_KB954155 102_KB953297__DotNet FW 2SP1v2 103_KB971110 104_KB953300__DotNet FW 2SP2_Reboot before 105_KB971108 106_Silverlight 107_KB972270 108_KB955417 109_User Profile Hive Cleanup Service 110_KB978037 111_KB977165 112_KB978251 113_KB978262 114_KB977914 115_KB975560 116_KB978706 117_KB971468 118_KB917736 119_do net FW 1point1 sp3 and FW2SP2 120_Roots Certificates Update for windows 2000 121_Q886903 122_KB978207 123_MSXML6SP2 124_KB870669 125_KB955069 126_KB958215 127_KB954459 128_KB923694 129_KB951071 130_KB941202 additional patch set sp1network.exe W2KSP2.EXE W2Ksp3.exe W2KSP4_EN.EXE

9.0 Install Any Additional Software You May Desire: On my Internet-only computer, I have used, and recommend, Adobe Flash, Adobe Acrobat Reader, an instant messaging client such as Pidgin, 7Zip, VideoLan Video Player, Firefox, OpenOffice, etc.

9.1 Notice that most of these apps, have known (but manageable) security and privacy issues. Use additional apps at your own risk!

9.1.1 DO NOT use browser plug-ins, especially free toolbars. Many (but not all) plug-ins, especially toolbars, track your usage, and operate across Windows user accounts – which would make your privacy strategy ineffective.

- 9.1.2 IF you run Adobe Flash, beware of Flash Cookies. When viewing any Flash video, right click, select tab ‘settings’ find the setting ‘allow this website to store files on your hard drive’. Set the allowed space to 0KB. Alternatively, you can use a browser plug-in to remove the cookies.
 - 9.1.2.1 Note. Adobe Flash has a never-ending stream of security problems and patches. Pay attention and keep it patched.
 - 9.1.2.2 Microsoft Silverlight has the same problem.
- 9.1.3 Note If you install Adobe Acrobat Reader, it will also try to install Adobe Air. For privacy reasons, I do not recommend you allow Adobe AIR to install to your machine.
- 9.1.4 If you install .NET framework, I recommend using the .NET Configuration Wizard in Administrative Tools to set ‘Trust’ to ‘Low’ for all environments. Be sure to install the service packs and security updates for .NET.
- 9.1.5 Instant Messaging clients, especially when ran in privileged user accounts can introduce malicious software into your computer. http://news.cnet.com/8301-13554_3-10047186-33.html

10.0 Configure the Internet Explorer Security and Privacy Settings: It’s in menu ‘Tools;’ then click ‘Internet Options.’ NOTE for XP, Vista and 7 users: Internet Explorer 7 and 8 include additional settings for the things introduced since IE6. NOTE for all users, certain Neanderthal banks and software applications will only work with Internet Explorer – so be sure it is as secure as you can make it. The basic idea remains: lock it down.

- 10.1 Select ‘Use Blank’
- 10.2 Select Keep items in History for 0 days.
- 10.3 Select Button Settings. Select radio button ‘Every visit to the page.’
- 10.4 Select tab ‘Security’. Set Security to High. Click the ‘Custom Level’ Button. Do not allow activeX, VBscript, Java, JavaScript, or any other executables to run in IE or any other browsers you may use.
 - 10.4.1 JavaScript is a well-intentioned language first introduced in Netscape to automate webpages for appearance and functionality. Theoretically, it is secure because JavaScript can only run on the webpage that you downloaded them with, and they run in a ‘sandbox’ separate from the rest of the system so that they can not harm your machine. In actual practice, both of these safeguards are regularly breached. Java and Javascript are not related in any special way other than name.
 - 10.4.2 ActiveX is a well intentioned language first developed by Microsoft to compete with Javascript during the browser wars in the mid 1990s between Microsoft and Netscape. ActiveX is much more powerful than Javascript and does not attempt to include any ‘sandbox’ protection. If you allow Javascript or ActiveX, you are allowing whoever wrote that Javascript ActiveX ‘applet’ (little application-let) to do anything and everything to your computer.

And these days, you don't know who wrote that applet. You don't even know that a given website intended that applet to be there, or if it was inserted by some government or criminal. Microsoft tried to secure these ActiveX packages by having their creators sign them with expensive-to-buy electronic certificates ... but the certificates themselves are not a completely trustworthy solution (see 10.5). It then tried to positively identify all known malicious activeX controls using 'killbits' – which is hard to positively identify all variations and keep them up to date. Even if it the ActiveX control is something the website intended to put there, it could still be from some marketer who will not respect your privacy, or install, something you don't want, such as DRM.

- 10.4.3 VBScript was the predecessor to ActiveX, based on Microsoft's Visual Basic language, and can do a little bit less damage, practically speaking, than ActiveX, which is not a reason to allow it. Computer security experts like to joke that VBScript's .vbs extension really stands for 'Virus Building System'.
- 10.4.4 Java is a full-featured programming language that is structured in such a way that it runs quickly on anything. It is structured with security in mind: it includes the protection of a sandbox. More importantly, it requires the java runtime environment code from Sun) to run java code on your computer. The java run time environment inside a sandbox gives you a fighting chance that of preventing malicious code from damaging your system. Again that is not the same thing as good security, and I don't recommend allowing java to run.
- 10.4.5 The .Net is a suite of updated versions of many classic programming languages. Security was designed into the .Net framework, including a virtual machine runtime environment and rules for deciding whether to trust assemblies, but apparently is not well implemented.
- 10.4.6 Do not allow automated pasting by script.
- 10.5 Select tab 'Advanced'. Remove the check from both boxes that say 'Enable Install on Demand ...' and 'Enable SSL 2.0'. Check the box that says 'Use TLS1.0'
 - 10.5.1 Be aware that sophisticated entities such as governments can easily break into encrypted communications (<http://arstechnica.com/security/news/2010/03/govts-certificate-authorities-conspire-to-spy-on-ssl-users.ars>) and <http://media.grc.com/sn/sn-179-lq.mp3>
- 10.6 Select tab 'Content' Click 'Autocomplete.' Uncheck all boxes. Do not allow Autocomplete or stored passwords. Do NOT enter ANY profile information.
- 10.7 If a specific site such as your email requires JavaScript, etc, add the site to your 'Trusted Sites' and set 'Trusted sites'' security level to 'Medium' in tab 'Security' in 'Internet Options'.

10.7.1 If you wish to allow Windows Update, the necessary sites to trust are:

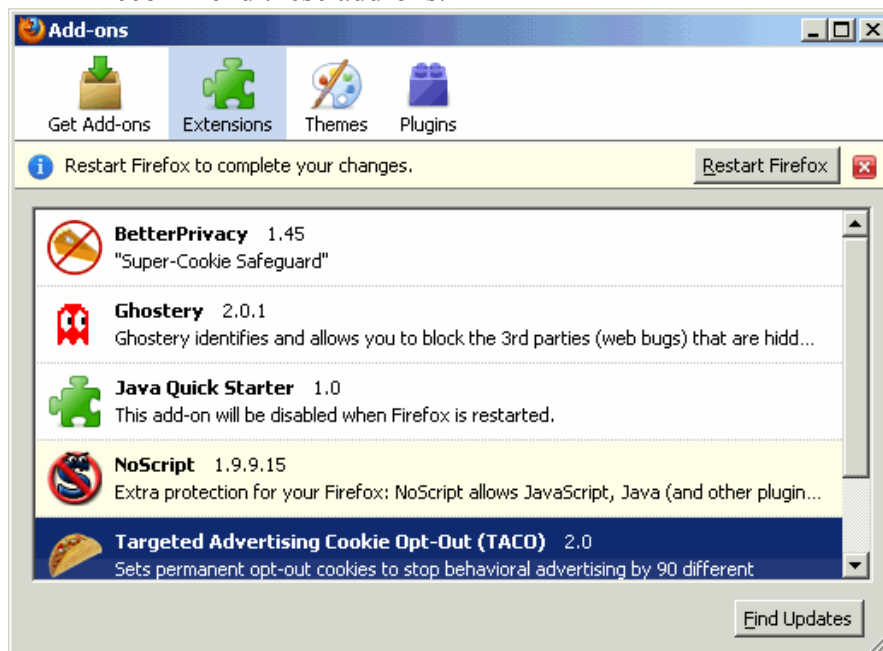
- <http://windowsupdate.microsoft.com/>
- <http://update.microsoft.com/>

10.8 Note that there are a number of programs available to purchase that do what we just did in 15 minutes in this section and section 1.3. Don't be a sucker for these programs.

10.9 If you use additional browsers, make sure they are locked down also. Repeat this configuration in each Windows account you created.

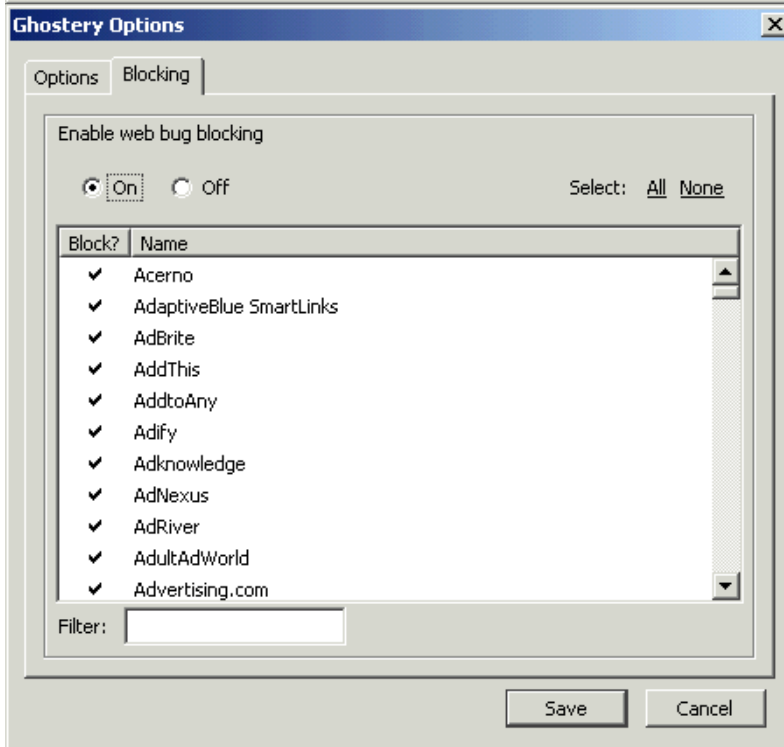
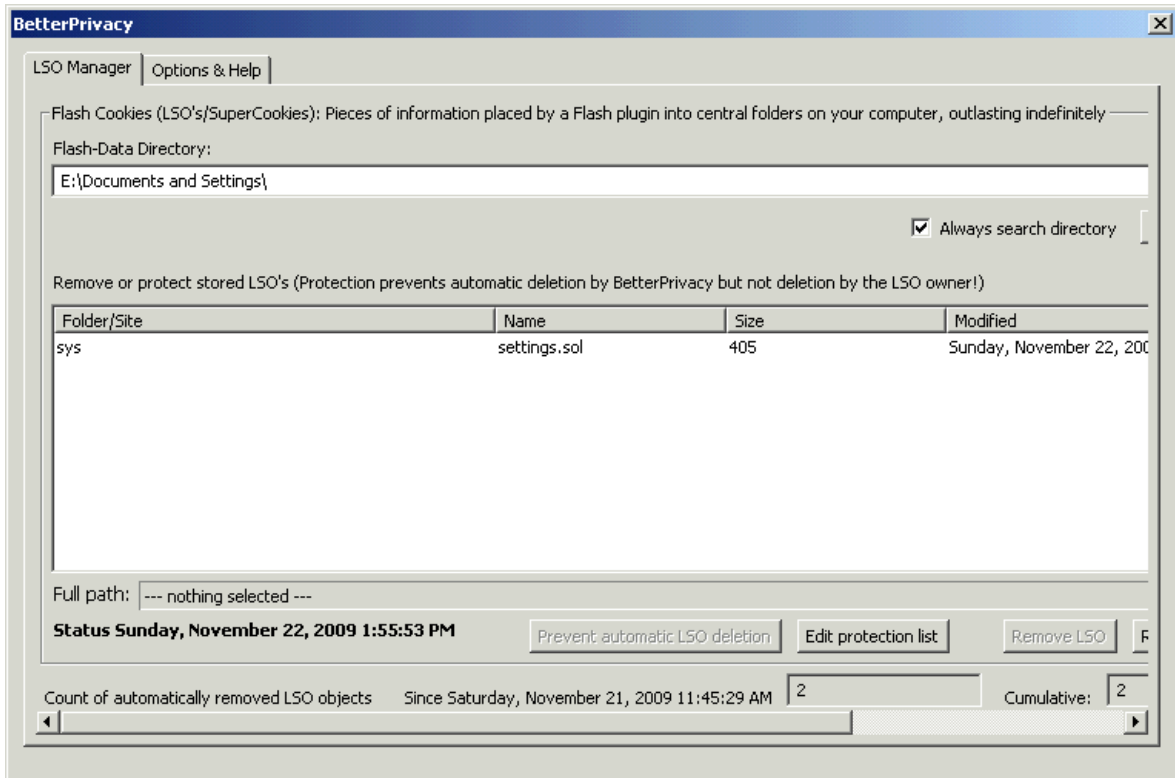
11.0 **Install Firefox:** Firefox is another useful browser. There are many browsers on the market: I do not recommend Chrome, because it is developed by Google, and there are currently plausible, but unsubstantiated, allegations of privacy issues (<http://hackers.org/blog/20090824/google-safe-browsing-and-chrome-privacy-leak/>). I do not recommend Internet Explorer, because it is developed by Microsoft. I do recommend Opera, because it is fast, and stable, and can be locked down to a level of privacy and security that is acceptable to most users (see the appendix for Opera configuration). For users with critical privacy and security needs, I recommend Firefox – even though the several privacy/security add-ons that I recommend will reduce its speed functionality and stability – but not to impractical levels. Firefox and Opera are also standards compliant – meaning that they will display things the way they were meant to be.

11.1.1 I do not recommend adding many browser widgets. They often reduce speed, stability, privacy and security of your browser. I do recommend these add-ons:

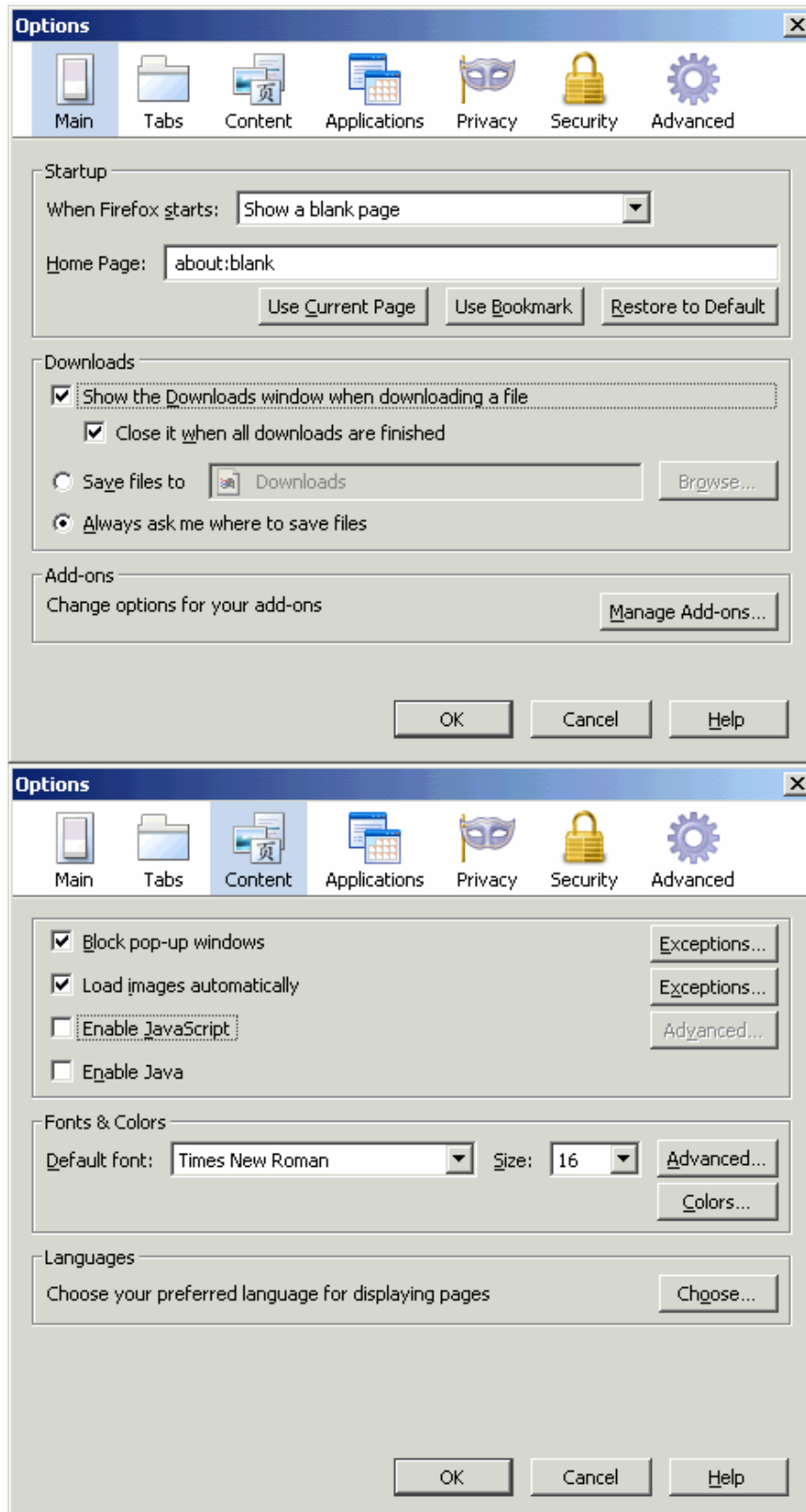


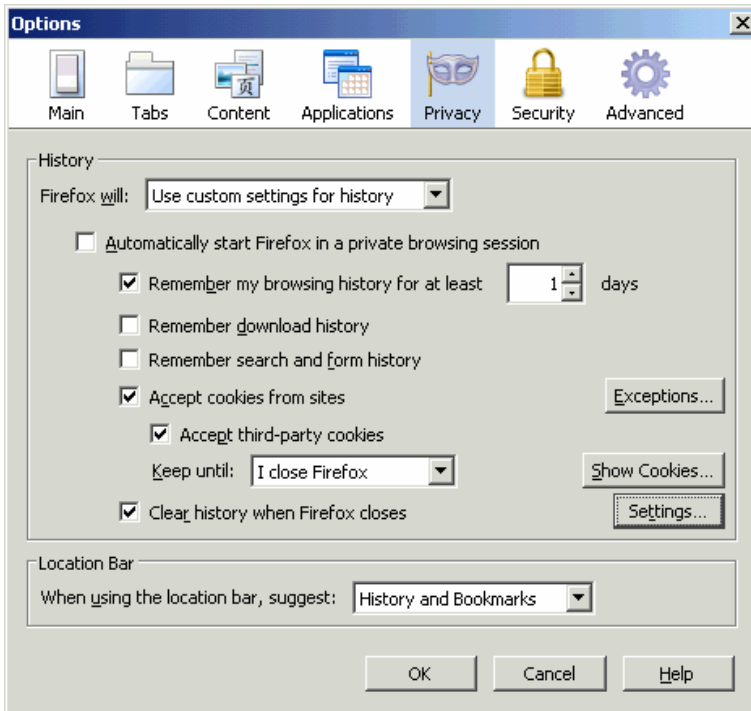
Note: using these add-ons will cause web pages to not save properly. There are several add-ons available (such as Un-MHT) to save pages' content properly after they have been stripped of their scripts.

11.1.2 These add-ons should be configured as shown:

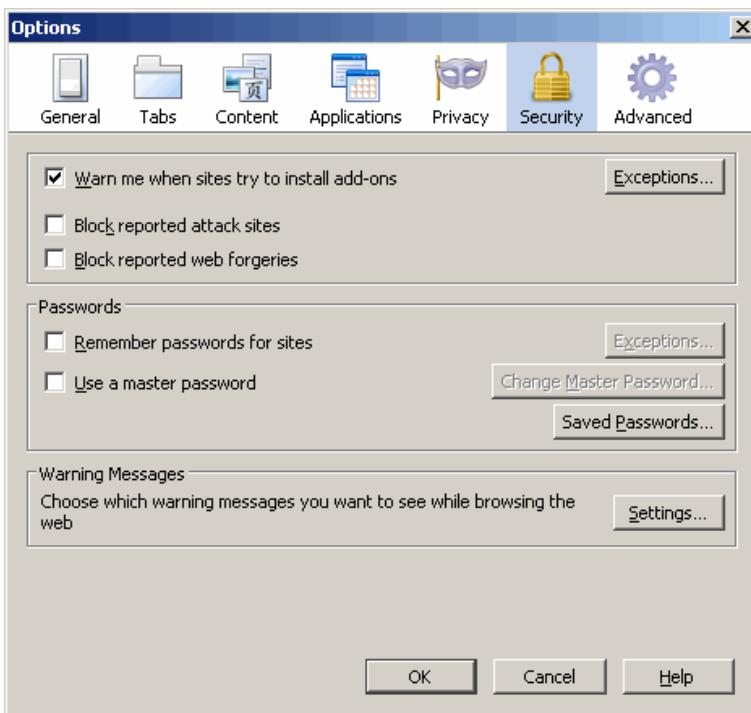


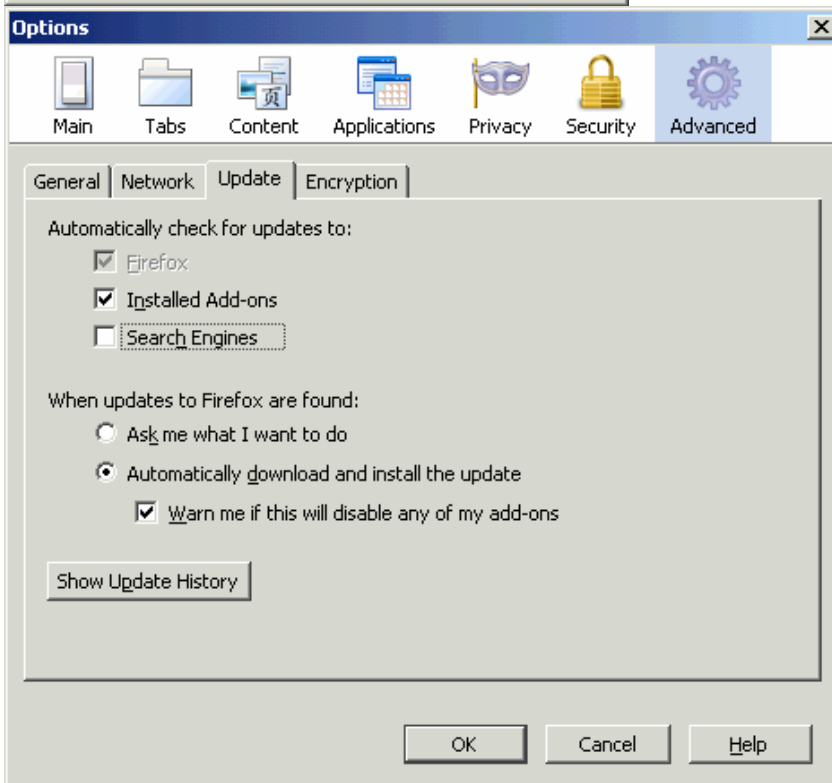
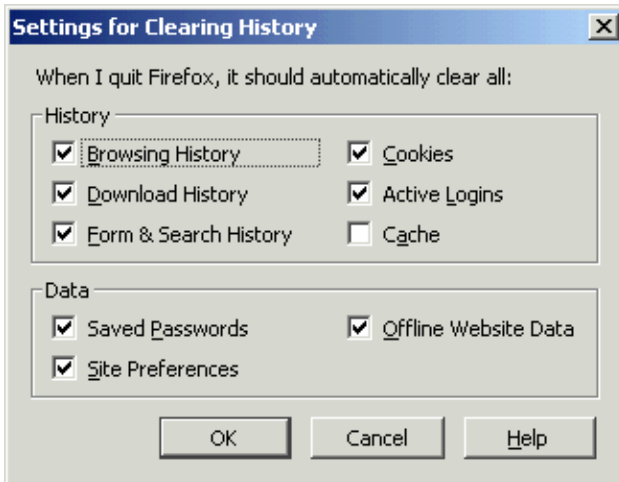
11.1.3 Configure Firefox's settings as shown Open 'Tools' Menu; 'Options'.



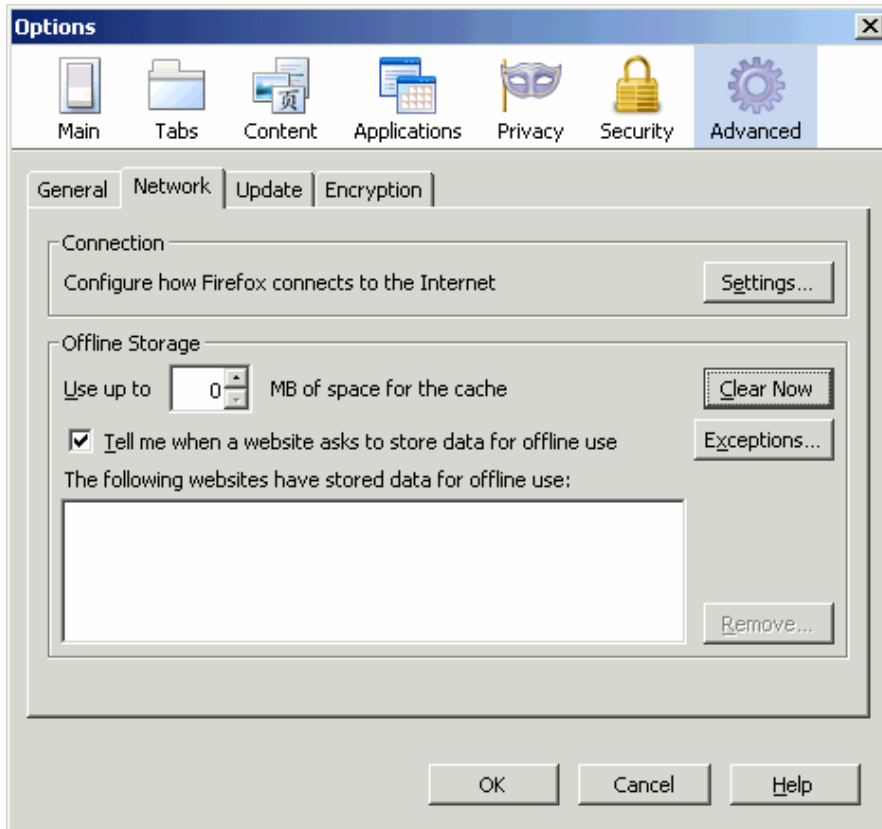


click 'Settings' to show the following menus. Note: in 'Security', I recommend you turn OFF the options to block attack sites and web forgeries. The list of sites is maintained, by Google, which mean that every time you go to a site, Google sees everywhere you go. <http://forums.mozillazine.org/viewtopic.php?f=7&t=1613775> Allowing this would render your *entire* privacy strategy ineffective. The loss in security that comes from this is zero, if you have locked down your system. Never allow sites to install add-ons. Sites may try to install everything from tracking software to Digital Rights Management software.





Warning: selecting 0MB will forbid your computer to use ROM cache. Users who wish to save content from their browser cache (such as Youtube videos) for offline use should allow 1GB or more, with the understanding that this incurs some small-but-manageable privacy risk (a risk of web beacons, a.k.a. web bugs (http://w2.eff.org/Privacy/Marketing/web_bug.html), which can be neutralized with the right plug-ins and policy).



When you are through, check through your settings, by entering 'about:configuration' into the address bar

12.0 Install additional security software:

- 12.1 Install Spybot Search and Destroy from (<http://www.safer-networking.org>).
- 12.2 Install print Key (http://www.webtree.ca/newlife/printkey_info.htm)
 - 12.2.1 Right Click Printkey. Select 'Properties,' then tab 'Security', then click button 'Add'. Add all the accounts you created.
 - 12.2.2 You will use this later to make a screen cap of the Processes running.
 - 12.2.2.1 Press ctrl alt delete
 - 12.2.2.2 Select tab 'Processes'
 - 12.2.2.3 After doing this, press CTRL-ALT-DEL. Select tab 'Process'. Select menu 'View'. Select ' option 'View Columns' check the boxes for columns 'Image Name', 'User Name', 'Session ID', 'CPU', 'CPU Time', 'Mem Usage', 'Mem Usage Delta,' 'Peak Mem Usage', 'VM Size', 'Base Priority', 'Handles', 'Threads', 'User Objects', "IO Writes", and 'IO reads'.

Image Name	PID	CPU	CPU Time	Mem Usage	Mem Delta	VM Size	Base Pri	Threads	I/O Read...	I/O Write...	I/O Othe...
avgam.exe	848	00	0:00:00	484 K	0 K	3,416 K	Normal	9	8,543,809	30,714	42,980
avgchsvx.exe	352	00	0:00:04	11,756 K	0 K	11,804 K	Normal	35	417,439	2,779,719	1,184,058
avgcsrvx.exe	1192	00	0:00:00	3,308 K	0 K	2,184 K	Normal	3	1,885,800	6,136	4,732
avgcsrvx.exe	1484	00	0:00:05	11,268 K	0 K	6,264 K	Normal	8	3,252,131	451,314	147,344
avgcsrvx.exe	1696	00	0:00:00	320 K	0 K	4,860 K	Normal	7	1,925,270	30,930	13,244
avgcsrvx.exe	2080	22	0:00:14	15,940 K	(12) K	3,736 K	Normal	5	16,322,671	3,803,655	3,390,360
avgemc.exe	824	00	0:00:00	1,164 K	0 K	4,572 K	Normal	19	4,893,595	15,202	38,761
avgnsx.exe	880	00	0:00:00	584 K	0 K	4,080 K	Normal	25	5,634,383	126,588	118,313
avgrsx.exe	1496	00	0:00:00	796 K	0 K	1,296 K	Normal	28	193,976	1,288,204	2,920,076
avgscanx.exe	980	49	0:00:48	40,464 K	1,016 K	73,772 K	Normal	8	121,400,...	202,785,...	105,088
avgscanx.exe	2056	13	0:00:04	6,280 K	0 K	2,852 K	Normal	13	5,293,661	537,018	33,012
avgtray.exe	1772	00	0:00:01	5,044 K	0 K	3,680 K	Normal	10	6,597,712	72,826	88,300
avgwdsvc.exe	572	00	0:00:07	2,132 K	0 K	3,772 K	Normal	27	79,420,549	2,733,976	411,144
CMD.EXE	1780	00	0:00:00	492 K	0 K	304 K	Normal	1	0	0	1,316
CSRSS.EXE	192	00	0:00:01	1,688 K	0 K	1,368 K	High	11	149,557	0	11,563
explorer.exe	1336	00	0:00:03	5,100 K	12 K	10,036 K	Normal	17	2,994,717	5,738	457,808
firefox.exe	912	02	0:00:01	19,448 K	68 K	20,280 K	Normal	16	11,347,918	375,799	279,709
js.exe	608	00	0:00:02	2,460 K	0 K	1,640 K	Low	6	123,304,...	252	497,642
LSASS.EXE	252	02	0:00:10	1,656 K	0 K	2,228 K	Above ...	14	1,179,528	321,778	105,988
nttask.exe	692	00	0:00:00	3,768 K	0 K	1,112 K	Normal	7	3,626	640	36,927
notepad.exe	2032	00	0:00:00	612 K	0 K	876 K	Normal	2	15,724	6,542	4,768
nsvsvc32.exe	656	00	0:00:00	2,380 K	0 K	672 K	Normal	3	1,796	12	3,766
Printkey2000.ex	1796	08	0:00:00	3,588 K	96 K	1,004 K	Normal	2	0	64,492	35,418
SERVICES.EXE	240	03	0:00:06	6,396 K	0 K	2,548 K	Above ...	25	1,973,422	1,319,570	190,636
SMSS.EXE	164	00	0:00:00	420 K	0 K	1,084 K	High	6	25,778,208	65,536	30,396
spoolsv.exe	548	00	0:00:00	5,244 K	0 K	2,792 K	Normal	14	3,177,880	244	260,585
stisvc.exe	712	00	0:00:08	2,040 K	0 K	524 K	Normal	4	119,134	12	325,356
svchost.exe	408	00	0:00:00	4,312 K	0 K	1,384 K	Normal	10	285,292	12	101,929
svchost.exe	588	00	0:00:00	8,604 K	0 K	3,980 K	Normal	29	1,210,738	323,696	194,670
svchost.exe	780	00	0:00:00	8,896 K	0 K	5,200 K	Normal	8	3,507,566	88,657	20,507
System	8	00	0:00:27	82,620 K	0 K	124 K	Normal	36	53,556,046	1,328,475	312,566
System Idle Process	0	00	0:09:36	16 K	0 K	0 K	N/A	1	0	0	0
TASKMGR.EXE	1168	00	0:00:00	1,484 K	0 K	696 K	High	3	0	0	78
vsmon.exe	440	02	0:00:09	22,032 K	0 K	23,744 K	Normal	23	115,608,...	13,041,948	2,375,955
WINLOGON.EXE	212	00	0:00:01	3,184 K	0 K	6,092 K	High	17	5,345,777	1,402	207,165
WinMgmt.exe	764	00	0:00:03	944 K	0 K	1,284 K	Normal	5	5,631,921	7,211,813	103,491
zclient.exe	1752	00	0:00:02	5,972 K	0 K	8,328 K	Normal	8	2,201,180	5,304	44,011

Processes: 37 | CPU Usage: 100% | Mem Usage: 454976K / 4571900K

12.3 Install your Antivirus software, using whatever instructions they give you.

12.3.1 DO NOT TRUST your security software(s) to detect all threats or protect you from them. Security software are only a few of the tools in your toolbox, and are limited tools at that!

12.3.1.1 Antivirus software relies, primarily, on detecting ‘signatures’ of viruses. Imagine a researcher wants to figure out what species a sample of cells came from: he would test the DNA – just as an antivirus package looks for a signature. There are many problems with this approach:

1. The bad-guys keep adding new features, rearranging existing code to look different, and finding new ways to code existing types of attacks – all of which make it difficult for an antivirus program to keep up. This is why your antivirus program receives updates so frequently.
2. Certain legitimate programs often show up as bad programs in a scan. This has led antivirus programs to include a ‘whitelist’ of known programs, such as Microsoft Word that are not detected and removed by the program. This whitelist can be, and has been, already exploited to deliver malicious software from companies and governments.

12.3.2 Set your Antivirus to maintain resident protection in memory on all accounts and Spybot to reside in memory for your administrator account.

12.3.2.1 I recommend AVG Antivirus + Firewall for Windows 2000, and AVG or Kaspersky Antivirus + Firewall for XP or higher. Others are available.

12.3.2.1.1 AVG is a Czech company. The Czech Republic has excellent personal freedoms and privacy, both in its own laws, and, to a lesser extent, as a European Union member. I have much more confidence that their antivirus software would detect malicious corporate or government software than an American company. Kaspersky is based in Russia, but, otherwise, has an excellent reputation.

12.3.2.1.2 Do not use McAfee. Last time I used it, its interface runs in Internet Explorer, and requires the general internet security to be set to medium – which opens a huge security hole in your computer.

12.3.2.1.3 Do not use Windows Defender. It violates your privacy.

12.3.2.1.4 I do not recommend buying any security software Microsoft. In addition to privacy concerns, there is a security concern: they made Windows, so you want a different company to provide security, and an independent audit of your security setup.

12.3.2.1.5 Do not install more than 1 antivirus program. They will fight with each other and may make your computer slow or inoperable.

12.3.2.1.6 Buy your security programs offline, paying cash, and do not give them your real information if you are required to register online to activate the product. Save your receipt, proof of purchase, serial #, fake name and information you gave them, etc., in a safe place.

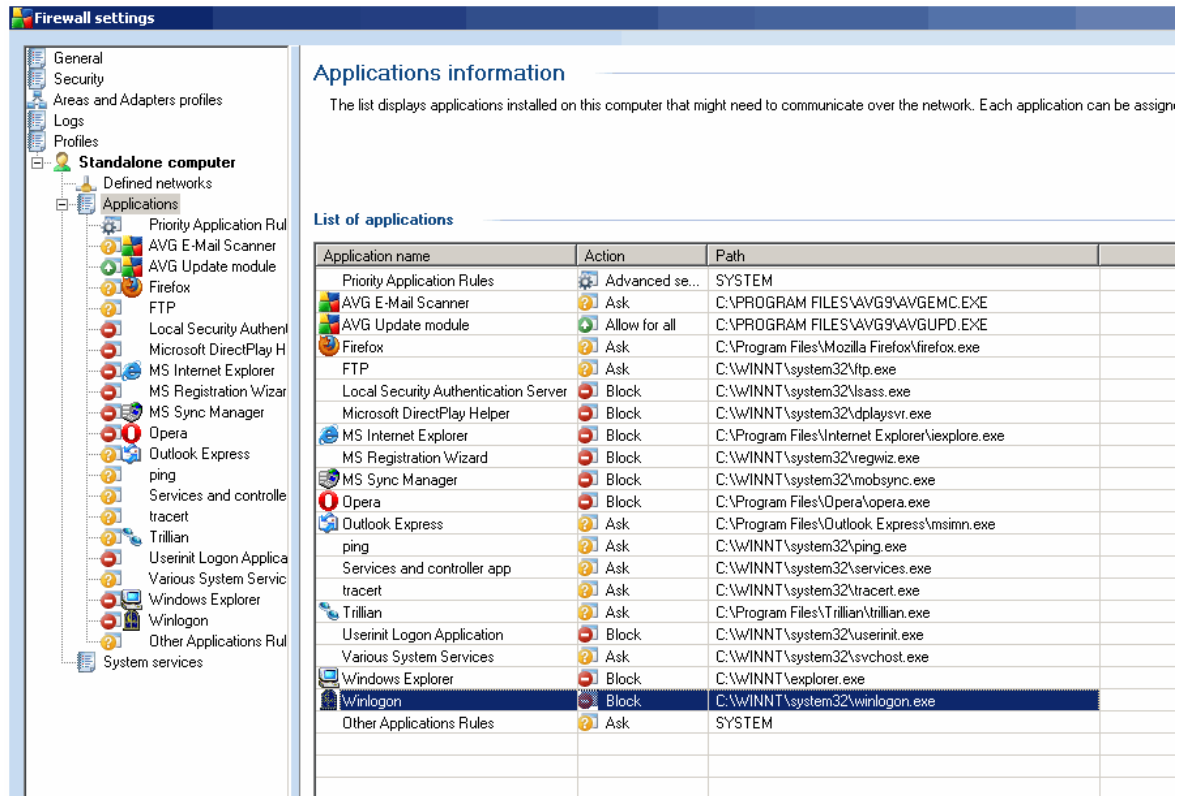
12.3.3 Set your antivirus to use heuristic scanning in addition to the default settings and to include system files and running system processes in its scan. These will be somewhere in the settings for your antivirus. To continue the analogy in 12.3.1.1, heuristic scanning for viruses is like detecting a shark by saying ‘I see it looks really scary and has sharp teeth’

12.3.3.1 Heuristic scanning is a must have: these days many malware attempt to hide by changing their file size, content, etc. This ability is called ‘polymorphism’ - the

same principle that HIV/AIDS uses to beat immune system defenses and medications inside the human body. Spyware and virus makers are constantly upgrading their wares to beat your defenses

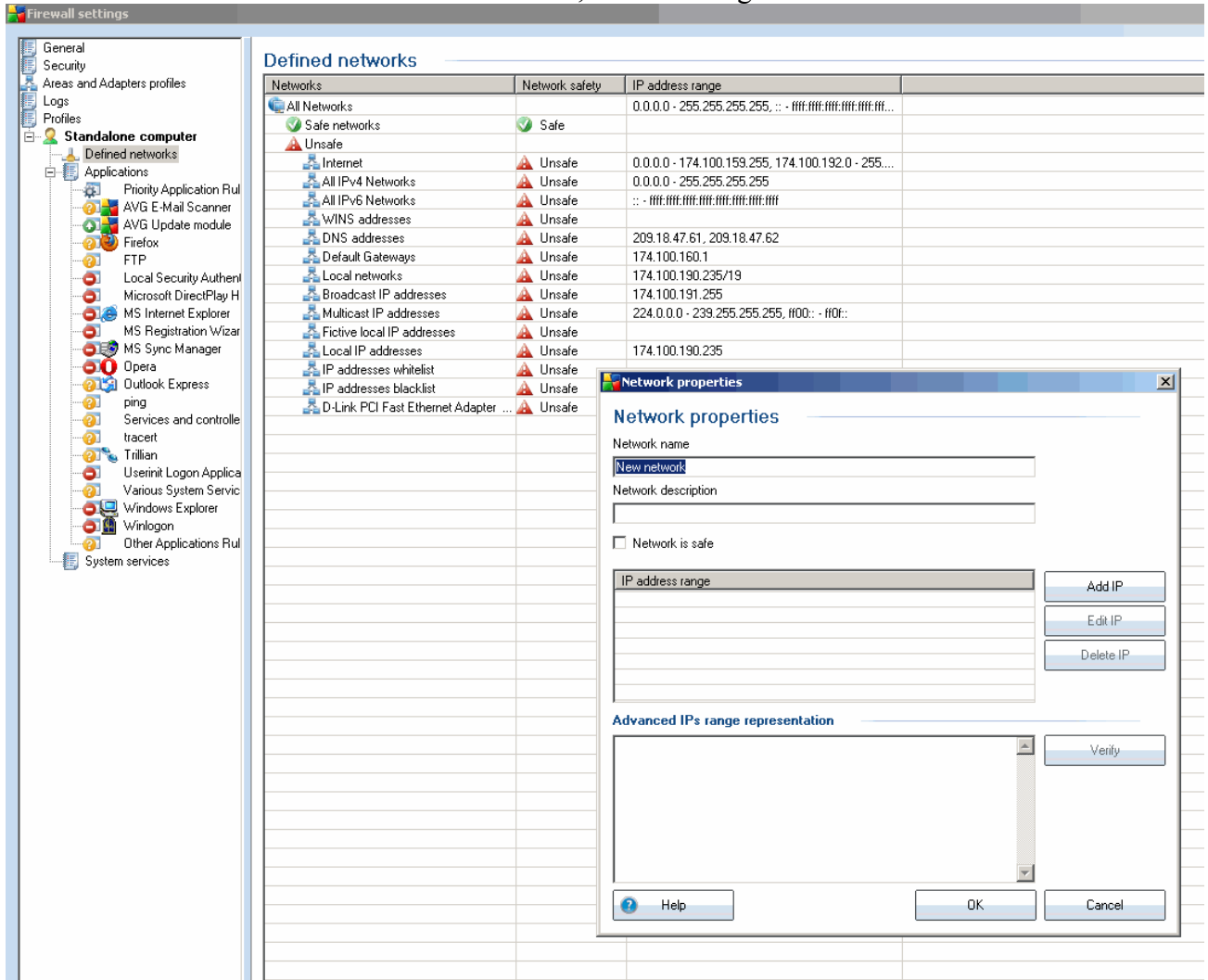
<http://www.crn.com/security/223101278>; .

- 12.3.3.2 Note: heuristic scanning will occasionally produce some false positives. You need to check these files out before whacking them.
- 12.3.4 Set your antivirus to scan regularly – at least every few days.
 - 12.3.4.1 Always scan everything with antivirus before you put it on your not-for-internet machine.
- 12.4 Install your firewall. The firewall is the most important security software.
 - 12.4.1 While setting up the firewall, make sure that only administrators have permission to change settings. Otherwise, it would be very easy to change these settings through code in your browser.
 - 12.4.2 Set your firewall to request your confirmation for *every time any program* attempts any remote connection.
 - 12.4.3 Set the access settings as shown below. Only 3 programs require *guaranteed unrestricted* access: services.exe, and the 2 programs that update Spybot and your antivirus package.
 - 12.4.4 For cable-internet users, it is OK for Services.exe to connect to the internet - you need to (through your Windows DHCP component) to get online. Spyware makers understand this and often setup their program to execute from within system processes such as services.exe or internet explorer to hide it.
<http://media.grc.com/sn/sn-105-lq.mp3> Pay attention to the logs and to the baseline screen captures you will take in section 16.
 - 12.4.4.1 If you see a request from any other Windows component, such as Winlogon.exe., LSASS.exe, Userinit.exe, Netlogon.exe, you should DENY it.



12.4.4.1.1 Exception, if for some reason, you decide to use the Windows Update site (a.k.a. WSUS, instead of manually downloading from the monthly Microsoft security bulletin) you may need to allow Automatic Updates, BITS, DLLhost, DTC, Windows Installer, MSCORSVW, etc. to be able to *ask* to connect to Microsoft.

12.4.4.2 Be sure to specify any IP addresses or ranges that should be blocked, such as Google.



12.4.4.3 Blocking Google Analytics: if you want to block Google Analytics, you have to entirely block Google, including Youtube, and everything else that it owns.

- 64.233.169.19 - 64.233.169.255
- 72.14.204.0 - 72.14.204.255
- 74.125.0.0 - 74.125.255.255
- 75.125.0.0 - 75.125.255.255
- 216.239.32.0 - 216.239.32.24
- 216.239.34.0 - 216.239.34.24
- 216.239.36.0 - 216.239.36.24
- 216.239.38.0 - 216.239.38.24

Be aware that the impending switch to IPv6 addressing may require a second session of blocking to get everything. <http://arstechnica.com/tech-policy/news/2010/03/as-much-as-one-percent-of-the-internet-is-now-using-ipv6.ars>

12.4.4.4 Many other companies have begun using Google Analytics tactics of connecting to your computer... You will need to block them all in your firewall.

12.4.4.5 Be sure to save a backup of your settings each time you update them. Then you can load from the file, rather than manually set them, going forward.

12.5 You may also wish to invest in an intrusion detection system (aka IDS) <http://www.acm.org/crossroads/xrds2-4/intrus.html> and <http://www.sans.org/security-resources/idfaq/>

The screenshot shows the Windows Firewall settings window. On the left is a tree view with categories like General, Security, Areas and Adapters profiles, Logs, Profiles, and Standalone computer. Under Standalone computer, there are defined networks and a list of applications with status icons. The main area is titled 'General information' and contains a paragraph: 'This dialog allows you to change Firewall advanced settings, in particular, edit Firewall profiles and assign these to the network a Firewall settings to the archive.' Below this is a 'Firewall status' section with three radio buttons: 'Firewall enabled' (selected), 'Firewall disabled', and 'Emergency mode (block all Internet traffic)'. A file explorer dialog is open in the foreground, titled 'Please select destination Directory and Filename', showing a 'PWE' folder containing a 'setup' subfolder and two files: 'AVG Firewall Configuration_2010-03-27\$1.cfe' and 'AVG Firewall Configuration_2010-03-27\$2.cfe'. The dialog's 'File name' field is set to 'AVG Firewall Configuration_2010-03-27\$3.cfe' and 'Save as type' is 'AVG Firewall Configuration Files (*.cfe)'. At the bottom of the settings window is a 'Settings management' section with 'Export' and 'Import' buttons and their descriptions. The taskbar at the bottom shows the Start button, taskbar icons for AVG Internet Security, Mozilla Firefox, and Spybot - Search & Destroy, and a system tray with a Help button.

13.0 Configure the Windows security settings:

13.1 In Control Panel, open 'Administrative Options', then 'Component Services'. Disable these services (not every computer will have all of these):

- Alerter
- Clip Book
- DNS Client
- FTP Publishing Service
- IIS Admin
- Internet Connection Sharing
- Messenger
- Net Logon
- Net Meeting
- Remote Registry Service
- Routing and Remote Access
- Run As
- SMTP Service
- Simple TCP/IP Services
- SNMP Service
- SNMP Trap Service
- TCP/IP Printer Service
- Telnet
- WMDM PMSP service
- WWW Publishing Service

Windows XP users who are using a 3rd party firewall should disable Windows Firewall Service so it does not fight with their 3rd party firewall. Close 'Component Services' and 'Computer Management.'

13.1.1 Alerter could be used as part of an attack on your computer.

13.1.2 Clipbook is a potential privacy hole.

13.1.3 DNS Client is un-necessary, and will fight with your Hosts file.

This would make your computer freeze up for many minutes.

13.1.4 FTP Publishing Service allows access to your computer.

13.1.5 IIS Admin could be abused to allow access to your computer.

13.1.6 Messenger is the source of many annoying ads. It could also be used to update an existing malware installation placed on your computer by other means,

13.1.7 Net Meeting allows a person not physically at your computer to view your desktop and any open files. Note: If you have frequent customer/client interaction from your computer, you may need this. If you have frequent customer/client interaction from your computer, you may want to have a second on-line computer just for that, to make sure nothing crosses over either way.

13.1.8 Remote Registry Service allows someone not physically at your computer to modify the system registry.

13.1.9 Run As allows a user to try to run some program under another user's logon (with a higher level of installation/configuration privilege).\

13.1.10SMTP Service is an insecure legacy email service

13.1.11SNMP Service is an insecure legacy remote management protocol

13.1.12SNMP Trap Service (see above)

13.1.13TCP/IP Printer Service could allow access to your computer.

13.1.14Telnet allows a remote user to run programs on your computer from the command prompt.

13.1.15WMDM PMSP service provides DRM for Media Player

13.1.16WWW Publishing Service could be used to move files from your computer to the internet.

13.1.17 Some other services, especially 'Remote Procedure Call' look scary. Don't disable them. Your computer needs them to run.

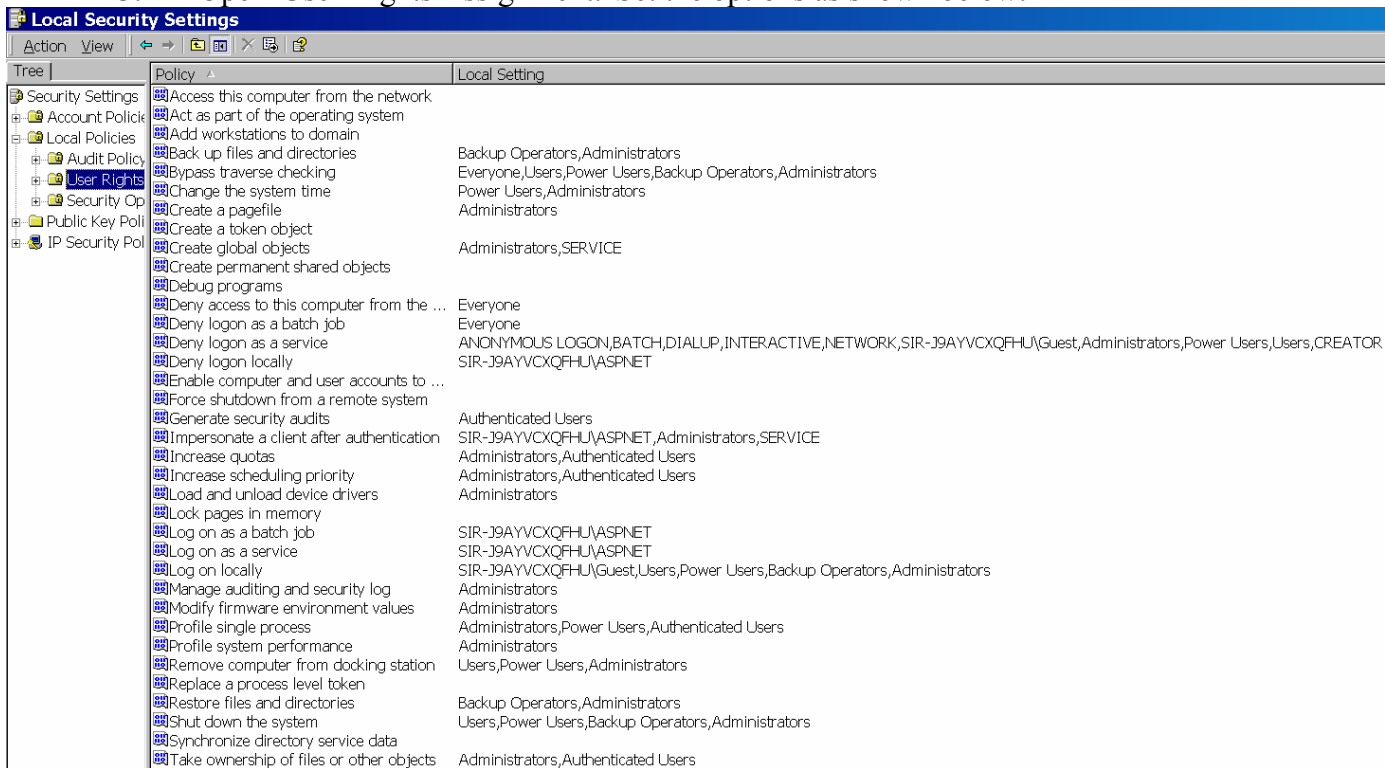
13.1.18 You can see what services depend on a given service by clicking 'dependencies' This is a useful clue to the possible effects of turning off a service.

13.1.19 If you accidentally disable something critical, you can often reboot to safe mode and fix it from there.

13.2 Open 'Local Security Policy.' Open 'Account Policies,' then 'Password Policies.' Set 'Maximum Password Age' to 999. Close 'Password Policies.'

13.3 Open 'Local Policies.' Open 'Audit Policy.' Set up logging of Success and Failure for all options. Close 'Audit Policy.'

13.4 Open 'User Rights Assignment.' Set the options as shown below:



The screenshot shows the 'Local Security Settings' console window. The 'Tree' pane on the left is expanded to 'User Rights'. The main pane displays a list of policies and their assigned permissions. The 'Local Setting' column is highlighted in blue.

Policy	Local Setting
Access this computer from the network	
Act as part of the operating system	
Add workstations to domain	
Backup files and directories	Backup Operators, Administrators
Bypass traverse checking	Everyone, Users, Power Users, Backup Operators, Administrators
Change the system time	Power Users, Administrators
Create a pagefile	Administrators
Create a token object	
Create global objects	Administrators, SERVICE
Create permanent shared objects	
Debug programs	
Deny access to this computer from the ...	Everyone
Deny logon as a batch job	Everyone
Deny logon as a service	ANONYMOUS LOGON, BATCH, DIALUP, INTERACTIVE, NETWORK, SIR-J9AYVCXQFHU\Guest, Administrators, Power Users, Users, CREATOR
Deny logon locally	SIR-J9AYVCXQFHU\ASPNET
Enable computer and user accounts to ...	
Force shutdown from a remote system	
Generate security audits	Authenticated Users
Impersonate a client after authentication	SIR-J9AYVCXQFHU\ASPNET, Administrators, SERVICE
Increase quotas	Administrators, Authenticated Users
Increase scheduling priority	Administrators, Authenticated Users
Load and unload device drivers	Administrators
Lock pages in memory	
Log on as a batch job	SIR-J9AYVCXQFHU\ASPNET
Log on as a service	SIR-J9AYVCXQFHU\ASPNET
Log on locally	SIR-J9AYVCXQFHU\Guest, Users, Power Users, Backup Operators, Administrators
Manage auditing and security log	Administrators
Modify firmware environment values	Administrators
Profile single process	Administrators, Power Users, Authenticated Users
Profile system performance	Administrators
Remove computer from docking station	Users, Power Users, Administrators
Replace a process level token	
Restore files and directories	Backup Operators, Administrators
Shut down the system	Users, Power Users, Backup Operators, Administrators
Synchronize directory service data	
Take ownership of files or other objects	Administrators, Authenticated Users

13.4.1 Notice that you want to allow all locally logged-on users to 'Profile a single process', 'Profile system performance' and 'view security audit', 'set quotas', and 'Change CPU scheduling priority'. These are necessary for diagnosing and resolving certain system issues as they occur. This is the one of the very few times you will ever wish to relax your security policy.

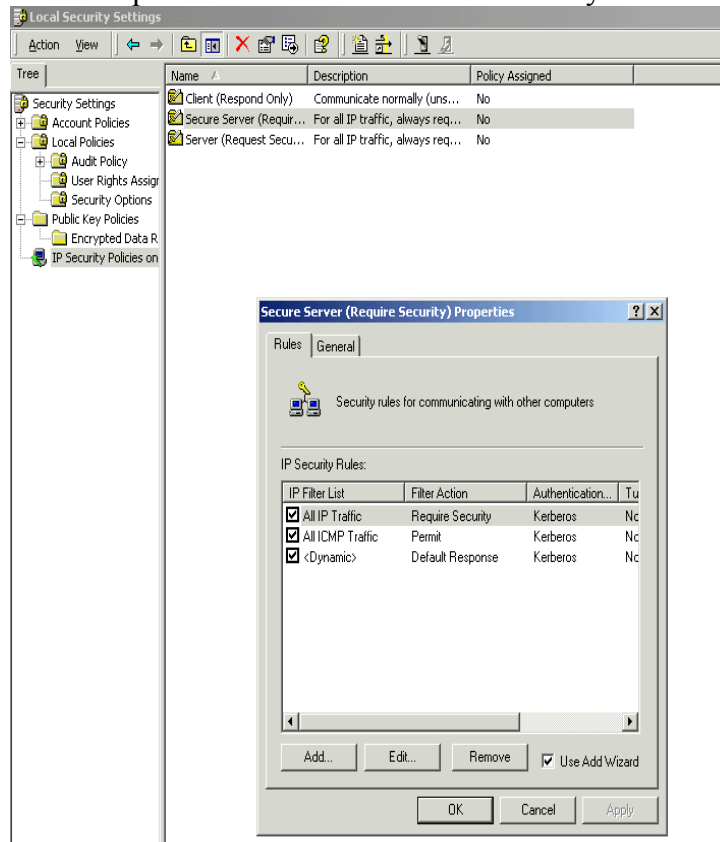
13.4.2 Do not become over-zealous in restricting logon options or you will lock yourself out of your computer permanently – and then you will have to reinstall Windows. (I accidentally did that once).

13.5 Open 'Security Options.' Set the options as shown below:

Tree	Policy	Local Setting
Security Settings	Additional restrictions for anonymous connections	No access without explicit anonymous permissions
Account Policies	Allow server operators to schedule tasks (domain controllers only)	Not defined
Local Policies	Allow system to be shut down without having to log on	Enabled
Audit Policy	Allowed to eject removable NTFS media	Administrators
User Rights Assignments	Amount of idle time required before disconnecting session	15 minutes
Security Options	Audit the access of global system objects	Enabled
Public Key Policies	Audit use of Backup and Restore privilege	Enabled
IP Security Policies on	Automatically log off users when logon time expires (local)	Enabled
	Clear virtual memory pagefile when system shuts down	Enabled
	Digitally sign client communication (always)	Disabled
	Digitally sign client communication (when possible)	Disabled
	Digitally sign server communication (always)	Disabled
	Digitally sign server communication (when possible)	Disabled
	Disable CTRL+ALT+DEL requirement for logon	Disabled
	Do not display last user name in logon screen	Enabled
	LAN Manager Authentication Level	Send NTLMv2 response only/refuse LM & NTLM
	Message text for users attempting to log on	
	Message title for users attempting to log on	
	Number of previous logons to cache (in case domain controller is not available)	10 logons
	Prevent system maintenance of computer account password	Disabled
	Prevent users from installing printer drivers	Enabled
	Prompt user to change password before expiration	14 days
	Recovery Console: Allow automatic administrative logon	Disabled
	Recovery Console: Allow floppy copy and access to all drives and all folders	Disabled
	Rename administrator account	Ralf Bart Burpenifart
	Rename guest account	Not defined
	Restrict CD-ROM access to locally logged-on user only	Enabled
	Restrict floppy access to locally logged-on user only	Enabled
	Secure channel: Digitally encrypt or sign secure channel data (always)	Enabled
	Secure channel: Digitally encrypt secure channel data (when possible)	Enabled
	Secure channel: Digitally sign secure channel data (when possible)	Enabled
	Secure channel: Require strong (Windows 2000 or later) session key	Enabled
	Send unencrypted password to connect to third-party SMB servers	Disabled
	Shut down system immediately if unable to log security audits	Disabled
	Smart card removal behavior	No Action
	Strengthen default permissions of global system objects (e.g. Symbolic Links)	Enabled
	Unsigned driver installation behavior	Warn but allow installation
	Unsigned non-driver installation behavior	Warn but allow installation

13.5.1 Notice that there are 2 columns next to each policy: Local Setting and Effective Setting. If you for some reason you needed to make you're computer part of a domain, then policy settings on the domain controller override your local settings. If you did not make your computer part of a domain, then you can ignore the Effective Setting Column. It will be updated after the next reboot. You can check it and see that it then says what you just specified.

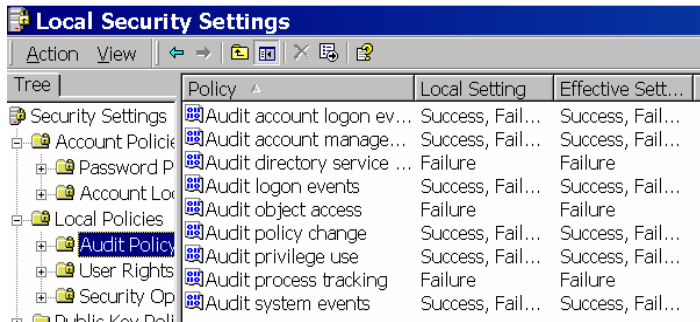
13.6 Open item 'IT Security Policies on...'. Select 'Kerberos' for all items in all three folders. Computers running Windows 2000/XP use various communications protocols to talk to each other. Only 'Kerberos' is still



secure.

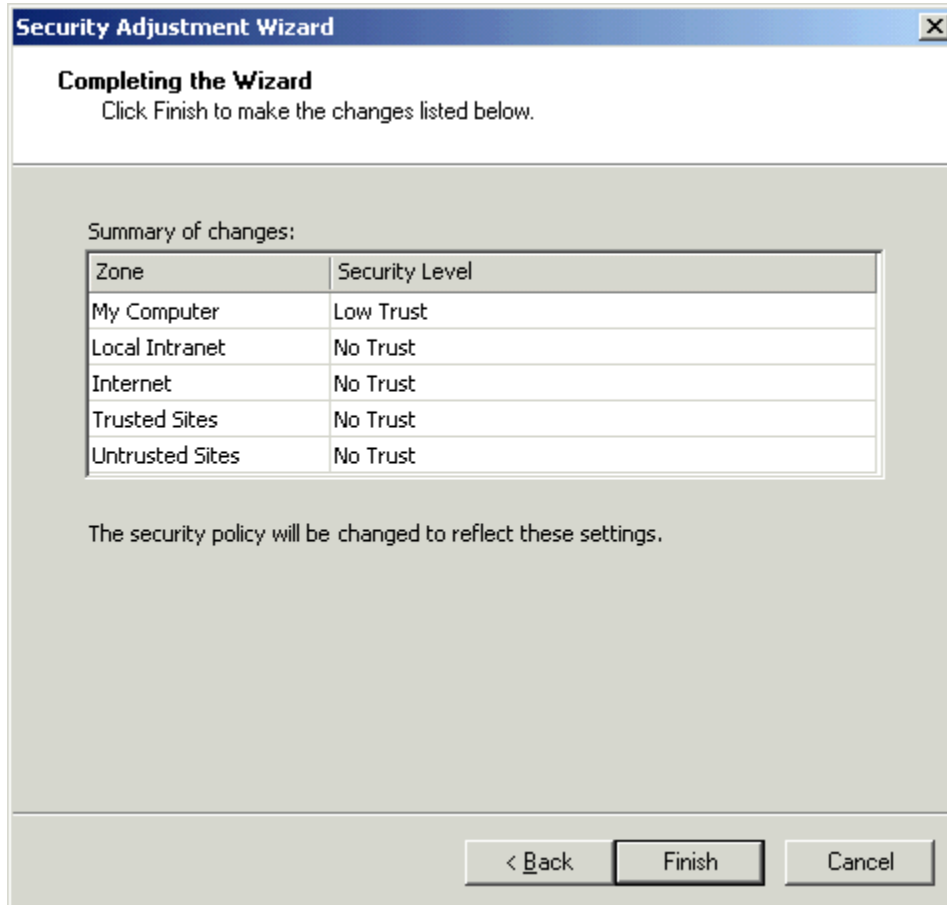
13.7 Windows XP Home, and other crippled Windows editions, do not have access to these screens. I am aware that Home Edition users may set these settings using Regedit – but have not attempted it myself. (The Center for Internet Security lists some of these registry keys <http://www.cisecurity.org/en-us/?route=downloads.show.single.windows2000.221>)

13.8 Set up event logging as shown below:



13.9 When you finish all of this, click menu 'Action', click 'Export Policy'. Save this policy in an encrypted drive that will be disconnected from this computer going forward.

- 13.10 Close the Local Security Settings Open the .Net settings. Open the .NET security configuration. Set My Computer's assemblies' trust level to 'low trust' and set all else to 'no trust'.



- 13.11 Automate Logoff IP release

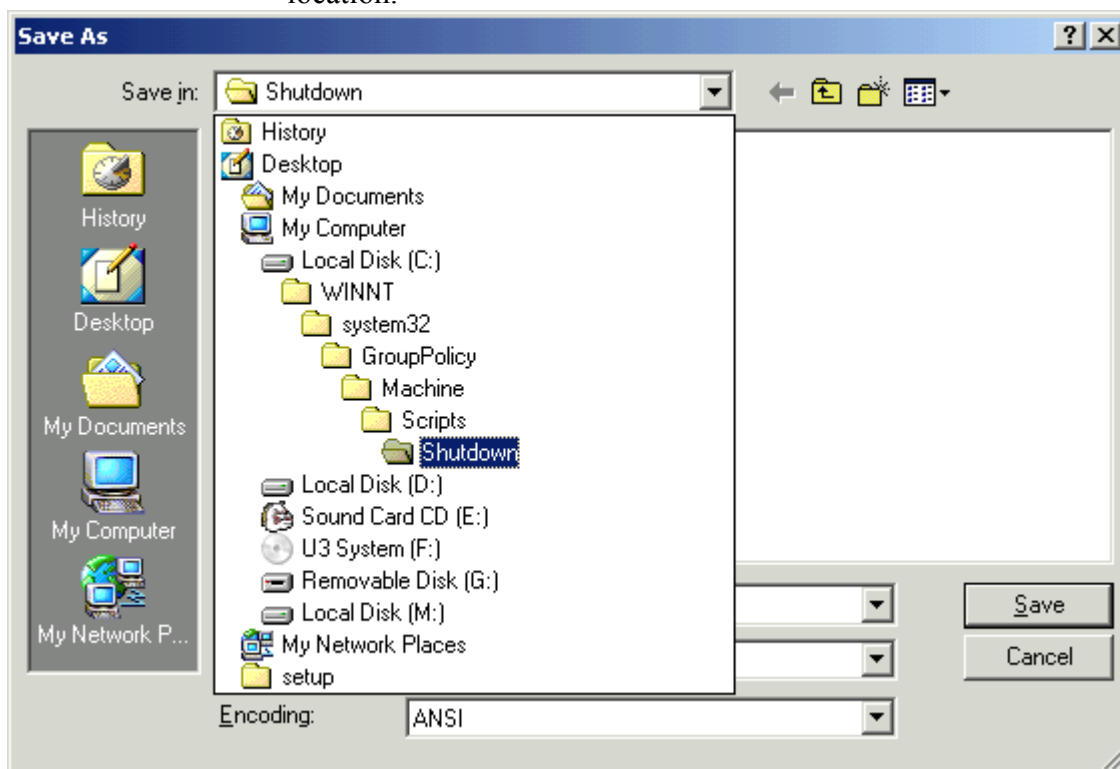
13.11.1 Create a .bat file containing the line 'IPCONFIG /RELEASE'.

13.11.1.1 You can set up other commands to delete cookies and other usage tracks. Your batch file can call the Spybot Search and destroy secure shredder to eliminate program cache files – that could come about, for example when typing a letter to your congressman or bank (that you only intend to keep encrypted copies of).

13.11.1.2 I notice I get an IP address much more frequently this way. It is not uncommon to have a new one several times a day.

13.11.2 Open 'Start', 'Run' and type 'CMD' to open the DOS Prompt. Type GPEDIT.MSC. Notice this is an expanded version of what we have already been working on. Open 'Windows Settings' then 'Scripts (Startup/Shutdown)' then item 'Shutdown', then tell it the name and location of your batch file. See these good references: http://en.wikipedia.org/wiki/List_of_DOS_commands and <http://www.computerhope.com/delhlp.htm>

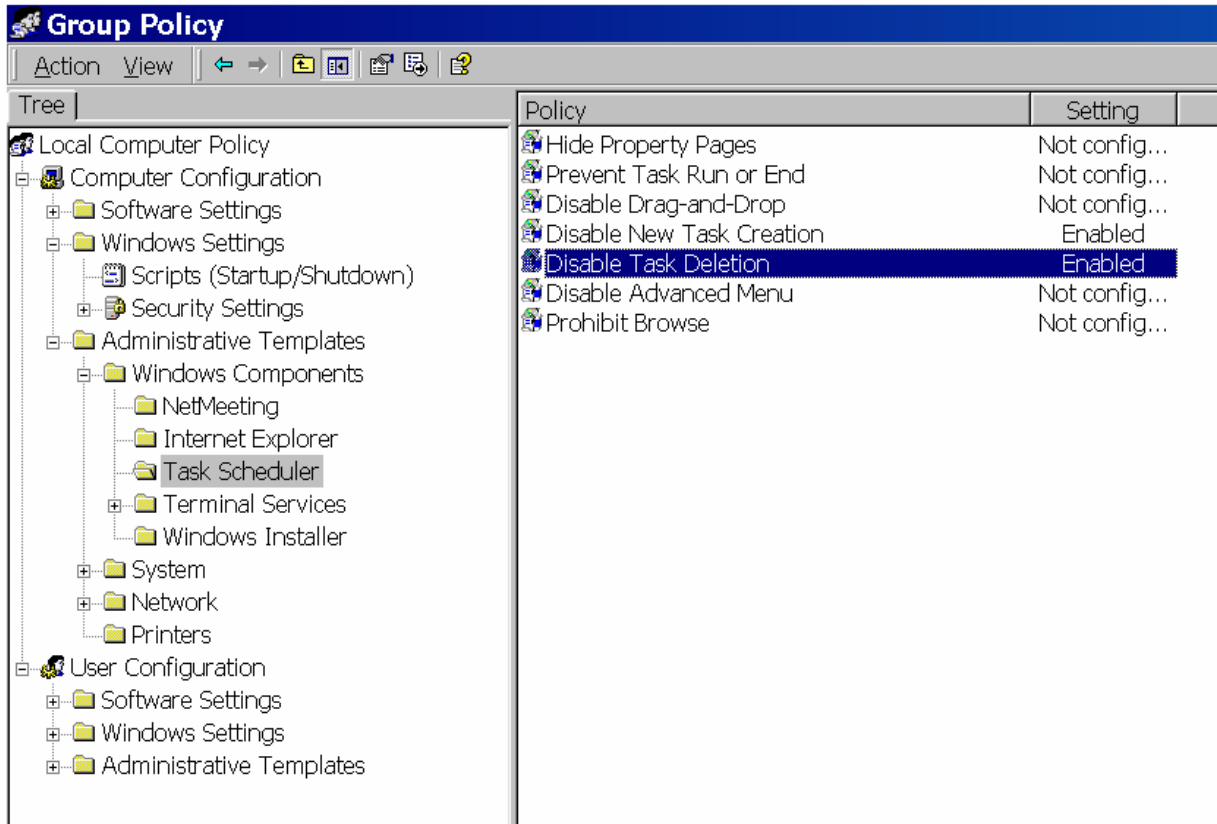
13.11.3 Your scripts live in here. Make a note of the filename and location.



13.12 Task Scheduler can be both a blessing and a curse.

<http://lifehacker.com/153089/hack-attack-using-windows-scheduled-tasks>

Schedule any tasks you may wish to run such as defrag, and then lock it down.



13.13 For more information, I recommend you consult Roberta Bragg [Hardening Windows Systems, 2004](#)

14.0 Secure certain registry settings:

14.1 For Privacy on machines with internet access... open 'Start Menu', select 'Run' type Regedit. Press enter. Select 'Edit' then 'Find'. Delete all entries containing the word 'Mobsync.' (Mobsync has the option of being turned off, by 'Start', 'Programs', 'Accessories', 'Synchronize' – but it does not obey the 'off' setting – this is why you must eliminate it from the system registry).

14.2 For Privacy on systems with encryption, change these keys to '0':

14.2.1 HKey_Local_Machine\Software\Microsoft\Dr.Watson\CreateCrashDump and

14.2.2 HKey_Local_Machine\Software\Microsoft\WindowsNT\CurrentVersion\AEDebug\Auto.

14.2.3 Disabling these helps prevent information which could be used to break your encryption from being saved to a crash dump or log file.

14.3 Make it more difficult for malware to install:

14.3.1 For Security, find all entries named 'NoDriveTypeAutoRun' and change their value to '255'. Find all other entries containing "autorun" that have the option of being set to 0 or 1. Change all these entries (depending on your Windows version and number of installed drives) to 0, except the entries for you local internal hard

drives (drive C, at least). This prevents CDs and other media from autoplaying when inserted into a drive on your PC. Autorun is a common method of distributing malware across computers. (<http://www.eff.org/cases/sony-bmg-litigation-info>) Keep yourself safe: disable autoplay.

- 14.3.2 Navigate to
HKey_Local_Machine\System\CurrentControlSet\Control\CrashControl\AutoReboot and set Reg_DWord to '0', to prevent the machine from automatically rebooting in case of blue screen of death, kernel stop, etc. Malware will still try to register at reboot, but this gives you a chance to notice and take action.
- 14.4 Strengthen logon procedures.
 - 14.4.1 Navigate to
HKey_Local_Machine\System\CurrentControlSet\Control\LSA and add the DWORD 'Restrict Anonymous'.
 - 14.4.2 Navigate to
HKey_Local_Machine\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon\AutoAdminLogon. To prevent automatic logon as admin, set the value of key 'AutoAdminLogon' and 'REG_SZ' to 0.
 - 14.4.3 Navigate to
HKey_Local_Machine\System\CurrentControlSet\Services\IPSec\Set to '0' the value in NoDefaultExempt, to prevent an end run around Kerberos.
 - 14.4.4 Microsoft provides a more in-depth look at their logon process. [http://technet.microsoft.com/en-us/library/cc780332\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc780332(WS.10).aspx)
- 14.5 Strengthen your connection's security:
 - 14.5.1 Navigate to
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\DisableIPSourceRouting and set REG_DWord to '2' to prevent outside sources from sending malicious data to your machine that appears to come from your machine, if you have 2 networking devices installed.
 - 14.5.2 Navigate to
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\EnableDeadGWDetect. Set REG_DWord to '0' to prevent your traffic from being redirected under certain circumstances.
 - 14.5.3 Navigate to
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\EnablePMTUDiscovery. Set REG_DWord to '0' to prevent exploitation of your system by inserting something malicious into the packets of info that make up your communication.
 - 14.5.4 Navigate to
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\

Netbt\Parameters\NoNameReleaseOnDemand. Set REG_DWord to '10' to prevent your computer from giving out its name. This is both a privacy and a security countermeasure.

14.5.5 Navigate to HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Lanmanserver\Parameters\Hidden. Set REG_DWord to '1' to prevent your computer from giving out its name. This is both a privacy and a security countermeasure.

14.5.6 Navigate to HKey_Local_Machine\System\CurrentControlSet\Services\LanmanServer\Parameters and then open the keys beginning with the word 'Null...' and clear all their values.

14.5.7 Remove Administrative shares. Navigate to HKey_Local_Machine\System\CurrentControlSet\Services\LanmanServer\Parameters. Set DWord 'AutoshareWks' to 0, to remove administrative share files.

14.6 It would be a good idea to export a backup of your registry – and store it in an encrypted drive.

14.7 <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/winntas/tips/winntmag/inreg.asp> is a good reference.

15.0 Install the MVPS host file described in Section 1.3.3. Follow the instructions that come from the MVPS website.

15.1 Open Spybot Search and Destroy.

15.1.1 Update and immunize. (Spybot will add additional sites to the host file).

15.1.2 Select 'Tools', 'Internet Tweaks'. Check the box 'Lock Host file as read only'.

15.1.3 You can personally edit your host file. It is best to save your additions in a separate file on your not-for-internet computer. Then you will be able to copy and paste from that file next time you reload windows.

15.1.3.1 At this time, you should add all your saved entries from your personal file.

16.0 Prepare to connect to the internet:

16.1 Take a preliminary screenshot of your system

16.1.1 Press both Alt and Printscrn together. (get a shot of tab 'performance' and tab 'processes'; for your convenience, sort the list by process name or ID)

16.1.2 Save the file and print a copy for your records. Label all your screen captures clearly so that you have a useful baseline, if you ever need to do any forensic analysis of a security incident in future.

16.1.3 Open Spybot Search and Destroy. Select menu 'Mode' then choose 'Advanced'. Click 'OK' on the 'Are you really sure' nag

screen. Select the menu 'Tools' from the list in the bottom left of the Spybot screen. In the center screen, check the boxes for 'System Startup', 'BHO', 'ActiveX', and 'Process List'.

- 16.1.4 Open BHO and save a screen cap. It helps to click on field 'name' to alphabetize the entries so you can search them easily.
- 16.1.5 Open ActiveX and save a screen cap.
- 16.1.6 Open 'Startup' Uncheck the entries for Icwconn.exe, and any communications clients such as Yahoo Messenger. You want to start these only when you're going to use them. Save a screen cap.
- 16.1.7 Open 'Process List'. Save a screen cap.
 - 16.1.7.1 Within Process List, open CRSS.exe. Click on the tab 'Loaded Modules' For processes that include many .dll files, drag the spacer bar up to the top so you can see as many as you can. Save a screen cap.
 - 16.1.7.2 Repeat 16.1.7.1 for these processes: LSASS, MSTASK, Services, SMSS, Svchost, system, Winlogon, Winmgmt. Take a screencap for each instance of these (for example you will likely have 3 instances of Svchost).
- 16.2 Reopen the registry editor (as described in section 14)
 - 16.2.1 Navigate to
\\HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa and take a screen capture of the allowed Authentication Packages.
 - 16.2.2 Search for all instances of entries 'Appint' 'Runonce' 'Rundll' 'Runservice' and take a screencap of them each.
- 16.3 Use the Truecrypt client to establish an encrypted volume of at least 200MB. Place these things into this volume:
 - A list of any administrative passwords you may need
 - A backup of your system registry
 - A backup of your Security Policy
 - A backup of your Services Policy
 - All screen captures you made in setting up the computer.
 - 16.3.1 Encrypting these settings protects them from accidental or malicious modification. It gives you an option to refresh your system at a later date. It gives you a useful forensic tool for analyzing any security incident that might occur in future.
- 16.4 For each user account you created, make an encrypted volume that contains a list of all the passwords specific to that account. Instead of trying to remember all of your email, etc passwords, you only have to know a logon password for each account + the password to the encrypted storage volume. This gives you a real chance of remembering them.
- 16.5 Save a copy of the encrypted volumes on your not-for-internet computer
 - 16.5.1
- 16.6 Plug your Ethernet/phone cable into your for-internet computer.
- 16.7 While logged into your Administrator account, go to the Windows update website that is linked to in your start menu.

- 16.7.1 Download all security updates, and any optional hardware updates at this time. Note: You may need to update Internet Explorer first.
- 16.7.2 Revisit the site until all remaining updates are installed.
- 16.7.3 Update your antivirus, firewall and Spybot.
- 16.7.4 Right Click 'My Computer'. Select 'Device Manager,' and the 'Update Driver,' or 'Reinstall Driver' for all malfunctioning devices. (Refer to your list from step 3.1.) Select source 'Windows Update Website.' Verify that each problem on your list is resolved and that no new problems appear.
- 16.7.5 Unplug your PC from the internet.

17.0 Maintaining Windows Systems:

- 17.1 NEVER get online when you are logged into administrator account, except, to update Windows, antivirus and Spybot. Immediately get offline and out of admin as soon as you have finished these tasks. Unplug from the network if you have lengthier tasks to perform.
- 17.2 Generally, you should surf in a modern, standards-compliant browser such as Firefox, not Netscape or Internet Explorer. Note some Neanderthal banking and corporate job-application pages will require Internet Explorer. There is not much you can do about this, except lock IE down to the minimum functionality required by the specific site(s) you wish to use. Add these sites to the trusted zone in IE (see 13.7).
- 17.3 Audit the security log using event viewer when you are logged into administrator account. (Start, Control Panel, Administrator Options, Event Viewer, Security Events) If you see anything suspicious, then start looking through the other events, starting with System Events. See <http://technet.microsoft.com/en-us/library/cc751219.aspx> for more info.
- 17.4 Reinstall Windows, every 6-12 months, or, immediately, if you have a virus or other security incident.
 - 17.4.1 Verify your security settings using an audit tool such as the Belarc tool available at http://www.belarc.com/free_download.html
- 17.5 Update your antivirus, firewall, Spybot and Windows daily, using the automatic settings in those programs.
- 17.6 Run an antivirus and Spybot scan at least every few days. You can set this up to run automatically (see Section 9.3).
- 17.7 Test your firewall at Shields Up! <https://www.grc.com/x/ne.dll?rh1dkyd2>
- 17.8 Be sure to keep all your applications patched on both your online and offline PCs. Attackers are beginning to exploit these – and not just with MS Office macros anymore. http://www.businessweek.com/magazine/content/09_48/b4157032795489.htm
- 17.9 Monitor system activity using the Windows Task Manager, and the Network Connection Manager. If it looks suspicious, it is.
- 17.10 Use Windows Task Manager if your computer is acting oddly or particularly slowly. Press CONTROL-ALT-DELETE, and select tab Task Manager. Look at the CPU Usage, the IO Reads, IO writes, Mem Usage and MEM Delta columns for excessive usage. Background programs such as

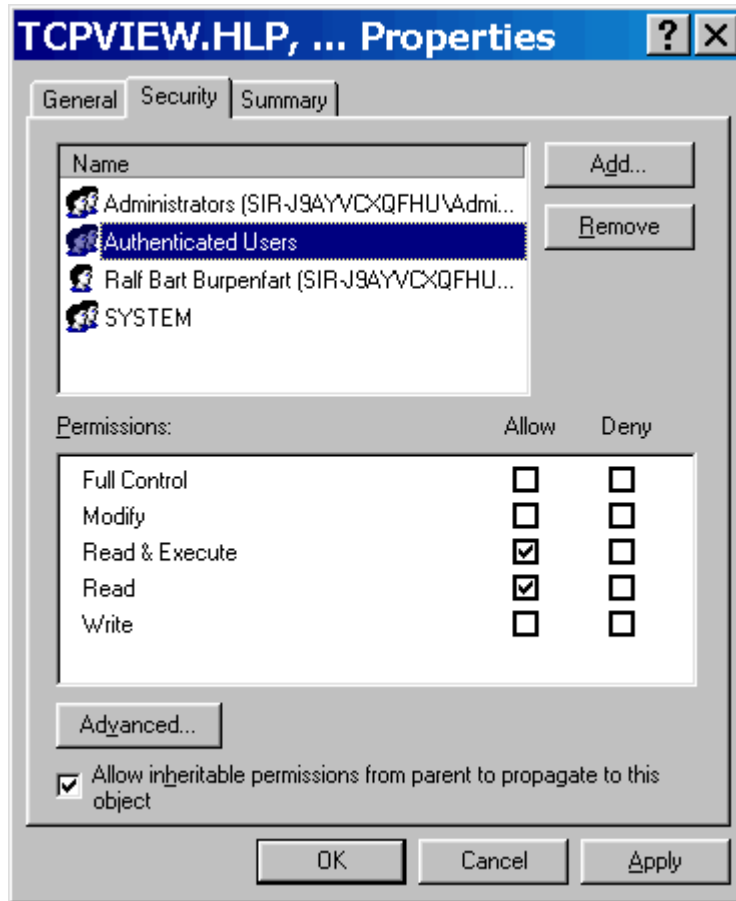
Services.exe, Svchost.exe, etc should not be using a lot of resources – recall the discussion of this in Section 9. The other columns are not of interest to most users.

17.10.1 If you see something acting funny, you should write down its process name and process ID, and Search for it. Take a screen capture too.

17.10.1.1 You can find the software components running within a given process, such as services.exe, by using Spybot Search and Destroy. (Make sure you are using ‘Advanced Mode’ – its in the ‘Mode’ menu). Select tab ‘Tools’ on the side bar, then item ‘Process List’. Select the process of interest, for example, Services.exe, and, at the menu along the bottom of the screen, select tab ‘Loaded Modules’. Make a screen cap of the modules, using the PrintKey utility, and Search for them. You may need several screen caps to get them all.

17.10.1.2 You may also reduce the offending process’s CPU scheduling priority by right clicking in the line containing that process and choosing ‘set priority.’ I do not recommend changing priorities on whim.

17.10.1.3 A more in depth look at running processes may be obtained by downloading Process Explorer (<http://technet.microsoft.com/en-us/sysinternals/bb896653.aspx> . Many other useful tools, mostly, beyond the scope of this paper are also included there.). Unzip the files to a directory. Change the file permissions as shown – you want to be able to call these from the command prompt in any account you are logged into. Do this by selecting all files in the directory. Right click. Select ‘Properties’. Click tab ‘Security’. Click Button ‘Add’. Select Entry ‘Authenticated Users’. Click Button ‘OK’. Then click the next Button ‘OK’. Then, open up ‘My Computer’ Open C:\WINNT\System32\. Cut and paste the files you just set permission for into the System32 folder. Allow it to overwrite the .dll file when it asks you.



17.10.1.4 Usually, if you are seeing extra activity, by services.exe, this is the result of (1) a hardware problem (no/wrong driver installed, loose power cable, dying power supply etc.), or (2) Windows is trying to start a service that is ran by either Services.exe, Svchost or rundll.exe (or dllhost in XP), or (3) DNS Client is fighting with your Host File, which you should resolve by setting DNS Client's startup type to 'manual' in Services.msc, as described in section 10. Your computer should not under any circumstances be trying to start one of the 5 services I recommend you to disable in 10.1.

17.10.1.5 You can 'Kill' certain offending processes from this interface, if you desire.

17.10.1.5.1 WARNING: Killing necessary processes, such as Services.exe, will force your system to shutdown. Make sure you have saved anything you care about before you play around with this.

17.11 Use the Network Connection Manager in the Quick Launch tray by the Start Menu to look at Network usage.

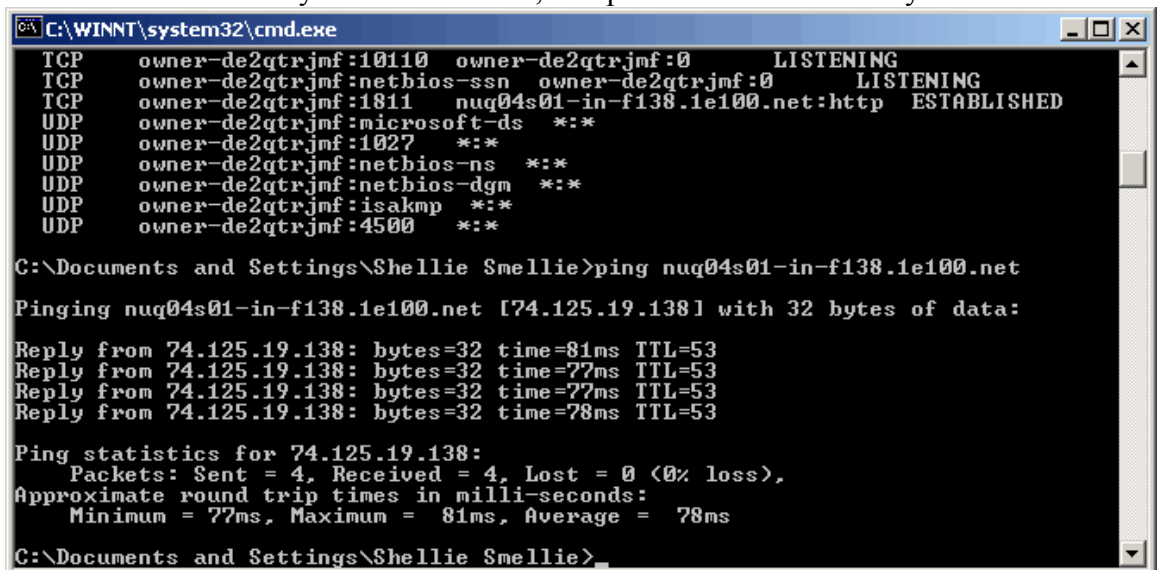
17.11.1 You can check your computer's connections: Open the Start Menu, click 'Run', type "CMD". Type "NETSTAT". Any active

connection will be displayed, along with other info, which may be of interest for very advanced users

17.11.2 To investigate a connection, you can search for the domain name. If that does not satisfy you, go back to the command prompt and type 'Ping' and then a space, and then the name of the connection of interest. The Ping command should return an IP address, as seen below. You can then look up that address on various websites, such as <http://www.robtext.com>.

17.11.3 TracerT is another useful command that complements Netstat and Ping, by tracing the route your communication takes from your computer to the server.

17.11.4 Note that the System Internals website <http://technet.microsoft.com/en-us/sysinternals/bb896653.aspx> also includes a utility called TCPView, that provides a similar utility.



```
C:\WINNT\system32\cmd.exe
TCP    owner-de2qtrjmf:10110  owner-de2qtrjmf:0      LISTENING
TCP    owner-de2qtrjmf:netbios-ssn  owner-de2qtrjmf:0      LISTENING
TCP    owner-de2qtrjmf:1811  nuq04s01-in-f138.1e100.net:80  ESTABLISHED
UDP    owner-de2qtrjmf:microsoft-ds  *: *
UDP    owner-de2qtrjmf:1027  *: *
UDP    owner-de2qtrjmf:netbios-ns  *: *
UDP    owner-de2qtrjmf:netbios-dgm  *: *
UDP    owner-de2qtrjmf:isakmp  *: *
UDP    owner-de2qtrjmf:4500  *: *

C:\Documents and Settings\Shellie Smellie>ping nuq04s01-in-f138.1e100.net

Pinging nuq04s01-in-f138.1e100.net [74.125.19.138] with 32 bytes of data:

Reply from 74.125.19.138: bytes=32 time=81ms TTL=53
Reply from 74.125.19.138: bytes=32 time=77ms TTL=53
Reply from 74.125.19.138: bytes=32 time=77ms TTL=53
Reply from 74.125.19.138: bytes=32 time=78ms TTL=53

Ping statistics for 74.125.19.138:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 77ms, Maximum = 81ms, Average = 78ms

C:\Documents and Settings\Shellie Smellie>
```

17.11.5 Question: Doesn't this take a lot of time? Answer: Yes. Most connections are benign from a standpoint of both privacy and security if you have properly locked down your computer.

17.11.6 Question: why are there at least 4 connections from my machine to itself? Answer: Windows NT, 2K, XP, Vista and 7 are designed for a networked corporate environment. The machine connects to itself, because there is no domain controller to connect to, or because I have blocked its connection to some outside service that MS did intend. More than 4 connections from your machine to itself may indicate that something nasty is being blocked by your HOSTS file. Note the connection on port 10110, in the screenshot above; it is a standard part of Windows. Microsoft intended it to connect to a geographic mapping service that I have blocked by forcing it to connect back to my own PC.

https://www.grc.com/port_1027.htm

17.12 On a monthly basis, take an afternoon, when you expect to be working on only things not requiring internet, and boot your computer to Safe Mode

(press F8 after the BIOS screen disappears, and Windows is just beginning to load). Run a full system scan with your antivirus program, Spybot, and Windows Malicious Software removal tool. When you download the monthly Microsoft Updates, the Malicious Software Removal Tool will install here in C:\WINNT\System32\mrt.exe.

- 17.13 If you should ever get a virus or spyware on your for-internet machine, save any files you may care about to a flash drive or CD-R(W), and set them aside. IMMEDIATELY erase the hard disk on that computer and follow the Windows installation procedure beginning in section 2.0.
 - 17.13.1 Sophos, the joint venture of all antivirus companies to identify and describe all viruses for the purpose of making members' antivirus programs able to remove them, publishes a good overview paper: 'The challenge of detecting and removing installed threats' at <http://www.sophos.com>. Key takeaway: you can't be sure you did it right, so don't waste your time trying.
 - 17.13.2 If you are interested in diagnosing the attack for purposes of strengthening your system, you may wish to use the Rootkit revealer tool from <http://technet.microsoft.com/en-us/sysinternals/bb896653.aspx>. Notice that this functions, at one level, similarly to Spybot Search and Destroy by searching for places in the registry where malware can hide itself at boot-up. At a deeper level, it installs itself, using its own version of Rootkit technology to scan your disk natively and see if there are any files on the disk that Windows is not aware of. It then looks to see if any possibly bad registry entries are pointing to those files.
 - 17.13.3 Fence the disk of saved files for a month or two before loading them onto any machine. Then scan them thoroughly, in safe mode, or from a LINUX machine, and don't let any of them execute.
 - 17.13.4 Prepare to Reload and Reinstall Windows
 - 17.13.4.1 Take a final screencap of running processes.
 - 17.13.4.2 Review the security logs.
 - 17.13.4.3 Backup any bookmarks, etc. that you wish to save to files using the functionality in your browser(s). I do not recommend taking configuration settings, as they may be compromised. Fence the backed up materials on a thumb drive for a month. Then, in safe mode, scan them with updated Spybot and antivirus programs. Be sure to delete any executable files from the backup device regardless.

HOPE FOR THE FUTURE ?

Long term, a better solution is needed. These procedures are difficult and not guaranteed to be effective against all threats – particularly your government and your ISP. Technologies to pierce our privacy are constantly being deployed and upgraded.

Upcoming specific threats to your privacy will include:

- Deep Packet Inspection, where your ISP will scan inside the packets of information sent between you and a website to see what your doing, such as Phorm, or NebuAd
- Government Spyware such as CIPAV, Carnivore, Magic Lantern. The CIPAV, is reported to obtain MAC address – this is especially dangerous, because the MAC Address identifies, uniquely, the modem or router that is connected to the internet. This makes privacy and anonymity impossible.
- Commercial Spyware, such as EBlaster
- Commercial Interest Profiling, whether by your ISP, or big advertisement services, such as DoubleClick (owned by Google)

Call your ISP and tell them you are concerned for your privacy and do not want any form of Deep Packet Inspection, whether for advertising or network management purposes, and that you don't want your usage profile or interests profile to be compiled or sold to anyone. Furthermore, if you see a practice that is illegal under current law, start or join a class action lawsuit – such as those that have since forced NebuAd out of business.

Write to your elected politicians and make the case for privacy. This is what I said:

Dear President Obama,

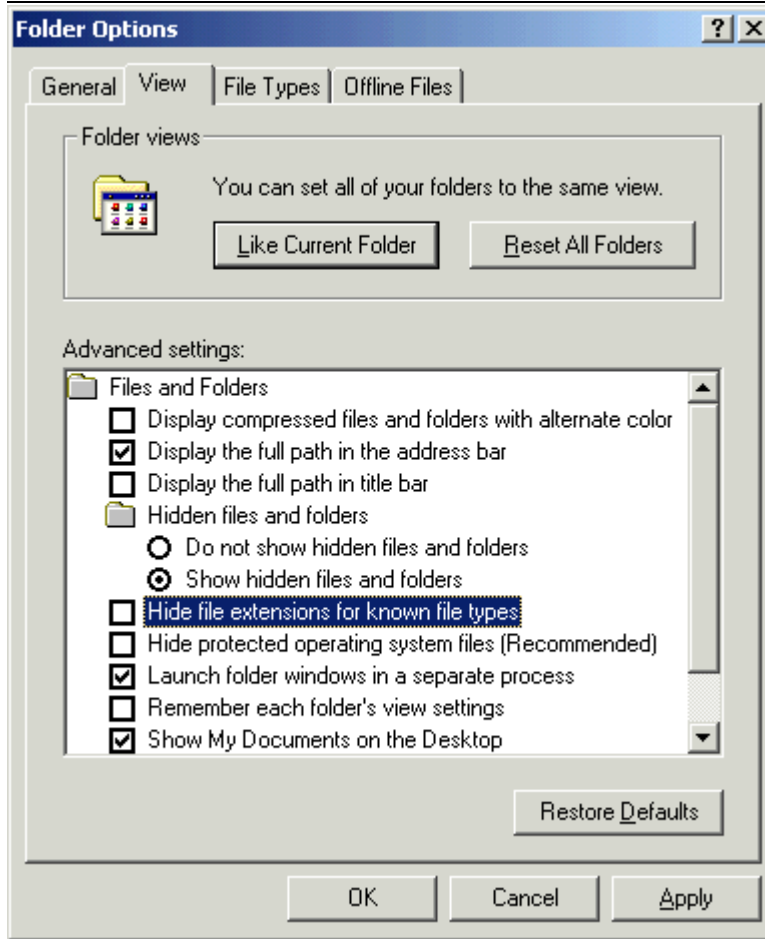
I write you to request your support for Senator Leahy's effort to establish a Truth Commission to examine the many and heinous crimes against privacy and liberty that were perpetrated during the previous 8 years, including, most especially, the unconstitutional surveillance all citizens electronic communications (internet monitoring, cell phone location tracking and so on). I deeply desire the passage of strong reforms that would prevent a repeat of the abuses of the last 8 years.

The last 8 years have seen the erosion of fundamental freedoms both through acts of law, and actions in defiance of the law. If we are to remain a free country with functioning individual liberties, we must both expose and stop these practices now.

Thanks,

At some point, given the present trajectory of law and technology, the costs of internet may come to outweigh the benefits. At some point, it may be best to just cancel your internet service.

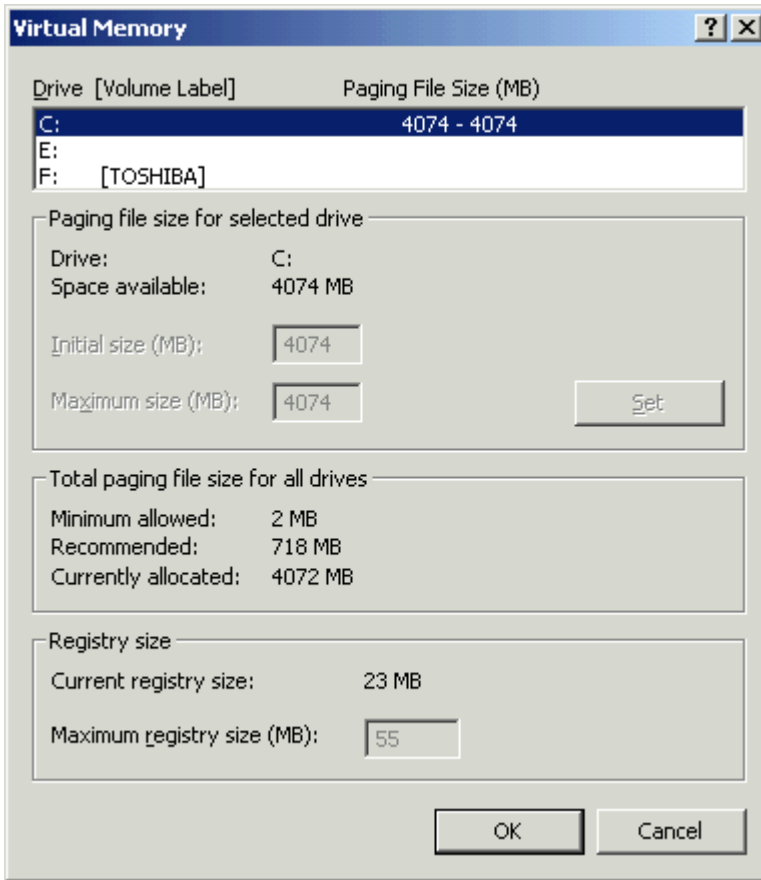
APPENDIX: OTHER USEFUL WINDOWS INSTALLATION SETTINGS



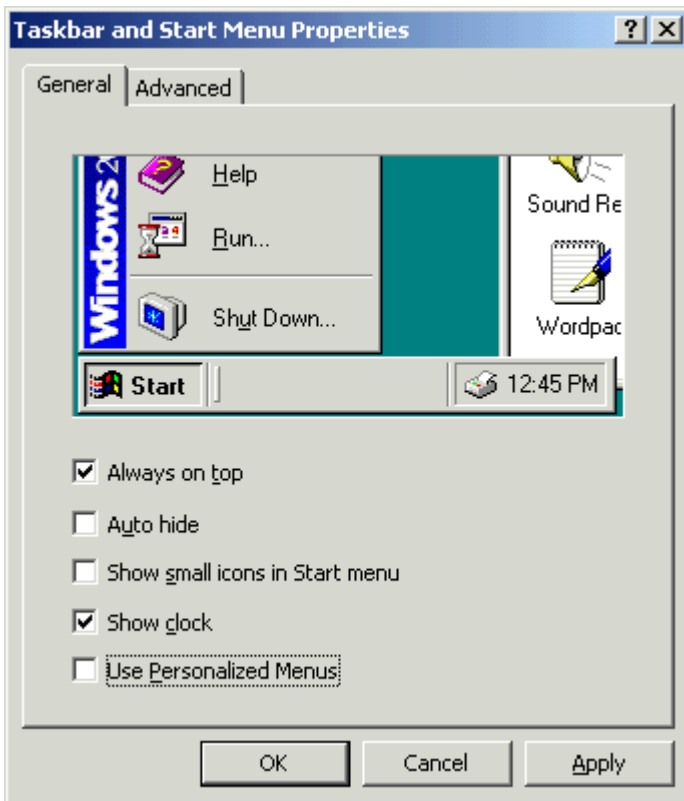
Make it easy to see what you need in Windows.



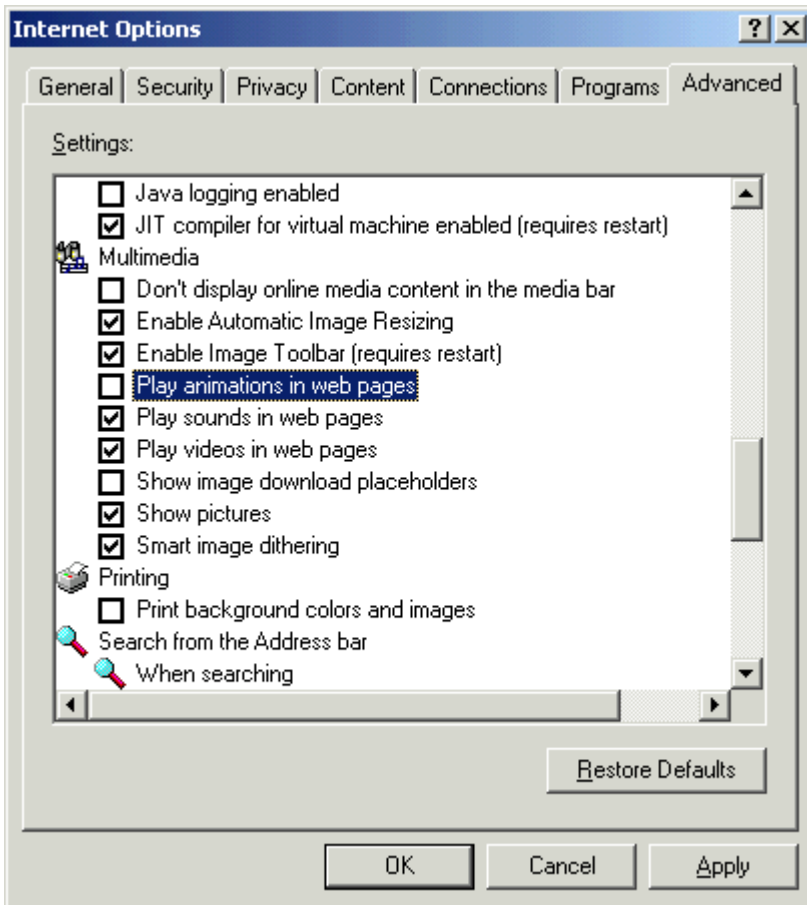
Eliminate this nag screen.



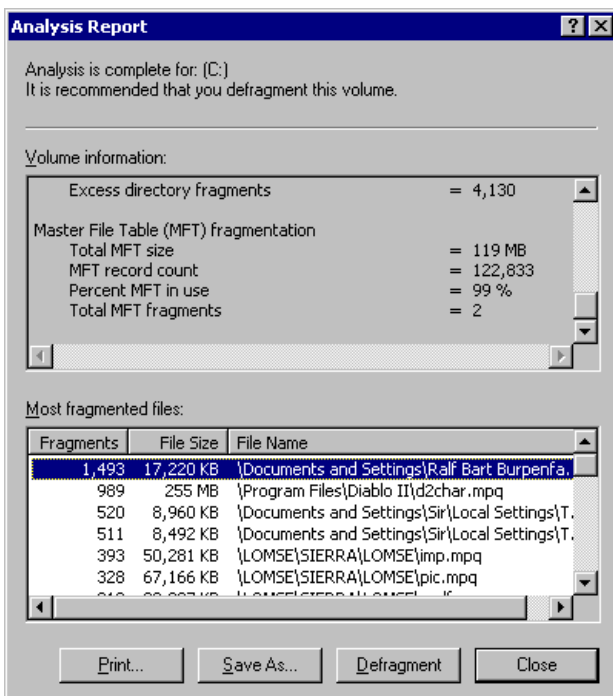
Increase system speed by putting your swap file on a different *physical* hard disk than your OS and Apps (or on a USB2 flash drive).



Turn off Personalized Menus so you can always find your apps.



Turn off animations in websites (the obnoxious moving distractions, including most flashing ads).



You will gain some system responsiveness by defragmenting your hard disk after you have finished all these installations. For example, a not-for-internet computer had severe fragmentation after set-up.

Defragmentation comes in two forms: (1) consolidating free space and making files hole (instead of spread out in multiple pieces on a hard drive – which is slower to use). The built in Windows defrag utility will do this. (2) optimizing file arrangement. The disk spins at constant speed, which means that a point on the outside can be read faster than one on the inside (more circumference passes your hard drive's read head in the same amount of time). 3rd party utilities are available to rearrange files to place them to take maximum advantage (hard disk read/write speed) of this.

Offline computers need fewer services to run.

Tree	Name	Description	Status	Startup T...	Log On As
Services (Local)	COM+ Event System	Provides a...	Started	Automatic	LocalSystem
	Event Log	Logs event...	Started	Automatic	LocalSystem
	IPSEC Policy Agent	Manages I...	Started	Automatic	LocalSystem
	Logical Disk Manager	Logical Dis...	Started	Automatic	LocalSystem
	Machine Debug Manager	Manages l...	Started	Automatic	LocalSystem
	NVIDIA Display Driver Service	Provides s...	Started	Automatic	LocalSystem
	Plug and Play	Manages d...	Started	Automatic	LocalSystem
	Print Spooler	Loads files...	Started	Automatic	LocalSystem
	Protected Storage	Provides p...	Started	Automatic	LocalSystem
	Remote Procedure Call (RPC)	Provides t...	Started	Automatic	LocalSystem
	Removable Storage	Manages r...	Started	Automatic	LocalSystem
	Security Accounts Manager	Stores sec...	Started	Automatic	LocalSystem
	System Event Notification	Tracks sys...	Started	Automatic	LocalSystem
	Task Scheduler	Enables a ...	Started	Automatic	LocalSystem
	User Profile Hive Cleanup	Cleans up ...	Started	Automatic	LocalSystem
	Windows Management Instrumentation	Provides s...	Started	Automatic	LocalSystem
	Windows Management Instrumentation Driver Extensions	Provides s...	Started	Automatic	LocalSystem
	Alerter	Notifies sel...	Disabled	LocalSystem	LocalSystem
	Automatic Updates	Enables th...	Disabled	LocalSystem	LocalSystem
	Background Intelligent Transfer Service	Transfers f...	Disabled	LocalSystem	LocalSystem
	ClipBook	Supports ...	Disabled	LocalSystem	LocalSystem
	Computer Browser	Maintains ...	Disabled	LocalSystem	LocalSystem
	DHCP Client	Manages n...	Disabled	LocalSystem	LocalSystem
	Distributed Link Tracking Client	Sends noti...	Disabled	LocalSystem	LocalSystem
	DNS Client	Resolves a...	Disabled	LocalSystem	LocalSystem
	Fax Service	Helps you ...	Disabled	LocalSystem	LocalSystem
	MATLAB Server		Disabled	LocalSystem	LocalSystem
	Messenger	Sends and...	Disabled	LocalSystem	LocalSystem
	Net Logon	Supports p...	Disabled	LocalSystem	LocalSystem
	NetMeeting Remote Desktop Sharing	Allows aut...	Disabled	LocalSystem	LocalSystem
	Network Connections	Manages o...	Disabled	LocalSystem	LocalSystem
	Network DDE	Provides n...	Disabled	LocalSystem	LocalSystem
	Remote Access Connection Manager	Creates a ...	Disabled	LocalSystem	LocalSystem
	Remote Registry Service	Allows re...	Disabled	LocalSystem	LocalSystem
	Routing and Remote Access	Offers rout...	Disabled	LocalSystem	LocalSystem
	RunAs Service	Enables st...	Disabled	LocalSystem	LocalSystem
	Server	Provides R...	Disabled	LocalSystem	LocalSystem
	Sygate Personal Firewall		Disabled	LocalSystem	LocalSystem
	TCP/IP NetBIOS Helper Service	Enables su...	Disabled	LocalSystem	LocalSystem
	Telephony	Provides T...	Disabled	LocalSystem	LocalSystem
	Telnet	Allows a r...	Disabled	LocalSystem	LocalSystem
	Workstation	Provides n...	Disabled	LocalSystem	LocalSystem
	.NET Runtime Optimization Service v2.0.50727_X86	Microsoft ...	Manual	LocalSystem	LocalSystem
	Application Management	Provides s...	Manual	LocalSystem	LocalSystem
	ASP.NET State Service	Provides s...	Manual	LocalSystem	LocalSystem
	Distributed Transaction Coordinator	Coordinate...	Manual	LocalSystem	LocalSystem
	Indexing Service		Manual	LocalSystem	LocalSystem
	Internet Connection Sharing	Provides n...	Manual	LocalSystem	LocalSystem
	Logical Disk Manager Administrative Service	Administra...	Manual	LocalSystem	LocalSystem
	Network DDE DSDM	Manages s...	Manual	LocalSystem	LocalSystem
	NT LM Security Support Provider	Provides s...	Manual	LocalSystem	LocalSystem
	Performance Logs and Alerts	Configures...	Manual	LocalSystem	LocalSystem
	Portable Media Serial Number Service	Retrieves t...	Manual	LocalSystem	LocalSystem
	QoS RSVP	Provides n...	Manual	LocalSystem	LocalSystem
	Remote Access Auto Connection Manager	Creates a ...	Manual	LocalSystem	LocalSystem

Installing Opera Browser: Opera 9 is another useful browser. It is a lot more user-friendly, faster and up-to-date than Internet Explorer. It is proven to be more secure than Internet Explorer and is also standards compliant – meaning that it will display things the way they were meant to be.

- 1.1 I do not recommend adding browser widgets or plugins. Certain of these have been shown to reduce browser stability, speed, privacy and security.
- 1.2 Be sure to select ‘Tools’, ‘Delete Private Data’ when beginning and ending your Opera session.
- 1.3 Before operating Opera for the first time, in each account, you should select ‘Tools’, ‘Preferences’
- 1.4 ‘General’
 - 1.4.1 ‘Startup’
 - 1.4.1.1 ‘Start from blank page’
 - 1.4.2 ‘Popups’
 - 1.4.2.1 ‘Block unwanted popups’, or ‘block all popups’
- 1.5 ‘Wand’
 - 1.5.1 uncheck ‘Let the want remember passwords’; do not enter any info into the form
- 1.6 ‘Advanced’
 - 1.6.1 ‘Content’
 - 1.6.1.1 Uncheck ‘enable JavaScript’
 - 1.6.1.2 Uncheck ‘enable Java’
 - 1.6.1.3 Uncheck ‘enable Plug-ins’
 - 1.6.2 Click ‘Manage Site Preferences’. This is the same thing as ‘Trusted Sites’ in Internet Explorer.
 - 1.6.3 ‘History’
 - 1.6.3.1 Set ‘Addresses’ to 0
 - 1.6.3.2 Check ‘Remember content on visited pages’.
 - 1.6.3.2.1 This is useful: a lot of sites, particularly news, make their content difficult to save. You can often grab it out of the disk cache, and remain it whatever.html to save the text of it.
 - 1.6.3.3 Check ‘Empty on Exit’
 - 1.6.3.4 Set ‘Check Documents’ to ‘Never’
 - 1.6.3.5 Set ‘Check Images’ to ‘Never’
 - 1.6.4 ‘Cookies’
 - 1.6.4.1 Check ‘Accept cookies only from the site I visit.’
 - 1.6.4.2 Check ‘Delete New Cookies When Exiting Opera’
 - 1.6.5 ‘Security’. Notice that these settings are all acceptably configured by default. You should review them the first time you install Opera for your education.
 - 1.6.6 ‘Network’
 - 1.6.6.1 Uncheck ‘Send Referrer Information’

1.6.7 After you have got your Opera preferences set up the way you want, copy your 'operaprefs.ini' files (for each account) to your offline computer. Next time you install, you can just copy and paste. Likewise your favorites/bookmarks live in a file named 'opera6.adr'.