Xmetalfanx Computer Security Guide

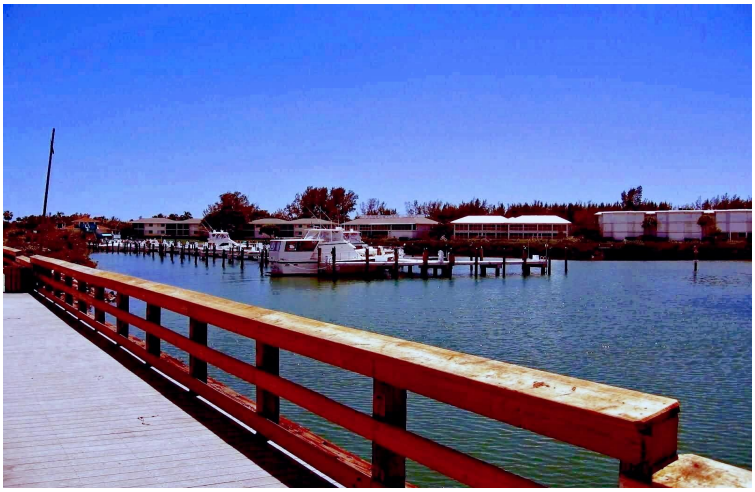

Table of Contents

Thanks

Before I begin I want to give thanks to sites, programmers, and friends, along with people I never met, but give great advice .. I know I may forget some (there are so many I want to thank, but hopefully I will include everyone I want

- **Ghack.net** – News, "new" (to me) programs, tech advice and news
  - Of course I mean the contributors to Ghack, not just the webmasters themselves
- Programmers and developers (along with all beta testers, ...etc) of the mentioned programs...
  - I am constantly updating this "Guide", so I am not sure if listing all programs here would really be "smart" though if you see your program listed, I thank you for making a great product

My Goals with these guides

I have a lot of different guide on my site and for some users it may be confusing to go all over the site for computer optimization tips in various areas. My hope is to summaries and put a lot of info all into one document that people can look over and then go to detailed parts of my site for areas of optimization that "Interest them".

I am not claiming any one task I list here is a "FIX ALL" to optimize your PC (Though I will list programs which can preform a number of tasks that I list)

The example I use is coupons … Like Coupons, maybe each task can do a little-fix here (or a little bit of money saved here") … a medium-optimization there … and together they all add up to a "happier computer"

Bottom line: I just want to help people .. .THAT Is my only goal .. I do not recommend a program for any other reason that it has helped me, or has helped a few people I know who used the same programs

Optimization Sites (many advertised on TV)

These are those "as seen on TV" sites that I personally hate.

There are legit sites for this sort of thing (I haven't been there in years, however, "PCPitStop" comes to mind as a legit option)

The problem I have with these sites

1. The fact they they "find errors" (that are not errors, but simple "Most Recent Used Files" (aka MRU) in various programs …
2. Then flag this as a "PRIVACY INTRUCTION" or something like that … "Critical System Error" … you get the idea
3. "IF YOU WANT TO REMOVE/FIX THESE ERRORS, BUY OUR PRODUCT OR SERVICE"

THAT IS JUST WRONG, if you ask me. That is preying on people who just don't know any better.

Optimizations

Not all of these have to be done, by all users. Just do the ones you are comfortable (and if it's a family computer, … one's you have PERMISSION to do).

Some people go on their computer only a few times a week and they never really install anything, so some of the more “in depth” tasks .. are really not needed at all

Updating AV's and/or Malware Scanners

I may include a few screen-shots for my recommended programs; though I (in early releases of this guide) do not plan on adding guides with screen-shots on how to update “every” anti-virus on the market.

Types of Programs needed for common maintenance

- **Anti-virus**
- **Anti-malware/ Anti-spyware**
    - These are great programs to have, but do not confuse them with anti-viruses. Anti-viruses, CAN detect malware and these scanners COULD detect some viruses, but my advice would be to have both types of scanners on your system.
    - Typical Anti
- **Firewall**
- **Host File**
    - These assign addresses of common “bad” locations on the web to your home computer's own address, so instead of trying to go to the actual location of the “bad data” (viruses, malware, ..etc), your “computer will connect to itself”. No harm done
    - **“Sub Categories”**
        - Cleaner (Temp File/Folder Cleaner) – These are good to include here, if you ask me, though now as “Important” security-wise as the first main groups of categories

Common "Everyday" Security Measures

Computers need to be maintained, though it doesn't have to be a long, complicated process... nor does it have to be an expensive process. These are tasks you can do to make sure your computer runs efficiently.

Temp File Cleaning such as Bleachbit or CCleaner

Here are some temp file/Temp Internet Folder Options. I have used all of them and though some seem slightly better than others, they all are pretty good

- **CCleaner** - (http://www.ccleaner.com/)
  - One of the best and most well known programs for this purpose ... it also has the options to remove custom (which ones you select) restore points and to clean the registry but the most powerful part of the program is the temp file removal .. .If you only use one program, I suggest CCleaner. It has support for the latest IE, Opera, Firefox, and Chrome Browsers among other programs and temp file locations

- **CCEnhancer** - (http://majorgeeks.com/CCEnhancer_d6547.html)
  - This little app is for CCleaner and adding many more programs to it's "Database" ... It doesn't remove anything (CCleaner) unless you TELL IT to. ... you run this from time to time updating like a malware or antivirus scanner

- **Cleanup** (http://cleanup.stevengould.org/)
  - Mainly for Internet Explorer users and the one I used before finding CCleaner ... I still like this one

- **Bleachbit** (http://bleachbit.sourceforge.net/)
  - A program that gets some of the LSO persistent cookies in various locations that some other programs (at the time I am typing this) can not

Anti-virus Sections

Install an Anti-virus

Both of these top two scanners have similar (Good) detection rates and are “neck and neck” as the best Free anti-virus if you ask me, though I must say … Avast has been consistently getting better with each release, though whether choosing Avast or Avira, either one, would be great additions to your computer's security

Free Options

1 ***Avast***

- http://www.avast.com/free-antivirus-download

2 **Avira**

- http://www.avira.com/en/avira-free-antiviru

Paid Options

- **Eset's NOD32 Anti-virus** (http://www.eset.com/)
  - which provides great protection and no system lag, though its not free.
  - Eset NOD32 Anti-virus has been consistently rated high since back to about 2001, that I know of and despite the fact that

- **Kaspersky** (http://www.kaspersky.com/)
  - My current #4 pick
  - I do not think it is as good as it use to be, though, saying “It's no longer the best” is not saying much, other than the fact that it's the “King of the Mountain” anymore
  - my #1 AV recommendation from about 2000-2009.
  - I feel loyal to, since it kept me safe for so many years (FYI, I switched for free products getting reviews just as good from security sites... not due to infections getting by Kaspersky)

- *Online Scanners*

  - http://www.eset.com/us/online-scanner is **Eset's Online Scanner** that is free to use (though other AV companies offer free online scanners too)

- Anti-virus and Malware Scanner Update

  Anti-viruses and Malware scanners while providing protection, should be updated regularly … though I do not think this means “Every single day”, still depending on how much the computer is used, it should be done “weekly” or “monthly”

  Updating your Malware Detection and your Virus detection insures that you are protected against the latest batch of infections on the internet

Monitor Start-up Items

The fact of the matter is there are way too many programs for me to list, so instead I have opted to suggested general guidelines. Instead of blindly removing as many things as possible, do a search on the internet, and 99 percent of the time one of the first results of any good search engine will completely explain what that item is.

- **What to POSSIBLY keep**
    - a overall start-up monitoring program like WinPatrol (Freeware) [THIS CAN REALLY HELP DISABLING ITEMS LISTED FURTHER DOWN THE PAGE]
    - Firewalls
        - Firewall "accent" programs
            - Peerblock IP Blocker, for instance.
    - Anti-viruses
    - anything specifically related to drivers (although not "always" needed). I for instance leave ATITray Icon on, although i probably "COULD" remove it
    - (if applicable) Malware/Spyware scanner's real time scanners

- **What to remove**

  This just means it's not starting when Windows starts up, and does not prevent the program from working when you click the icon on the desktop or start menu

    - Internet Messenger
        - *(Yahoo Messenger, Pidgin, MSN Messenger, ...etc)*
    - Anything that you may want to run from time to time but do not always have to have running,...
        - ESPECIALLY every-time you startup the computer ... uncheck/disable/...etc
    - *As a side-note to the last point ... basically any type of program not listed above in the "what to keep" sections.... can probably be removed ...*
    - Always research things before you just start removing entries)...

- **Programs that may help**
    - Both of these programs are FREE

      

    - **Win Patrol** - (http://www.winpatrol.com/) - Scans AND Monitors

    - **Autoruns** - (http://www.sysinternals.com/)
        - Not for new users, but power users who have never heard of this before can get a lot of use out of it.
        - DOESN'T monitor; however, it DOES allow you to get to any start-up item you can think of which is more than almost all other “start-up managing” programs out there

Installing a Firewall

Without doing a description of a firewall that will bore you to tears, I hope to give a general description that anyone will understand

- A software (program) firewall is a program that monitors connects between you and other machines (example ones used to host, websites), and the internet,
- Control over LAN (Local Network), or Wi-Fi (Wireless Connection), are also included in any decent firewall, as well as the ability to give the user control over what is allowed to connect any what isn't to their computer.
- **A key that I know of, and want to mention is that if you see something trying to connect to the internet .. DONT WORRY .. many programs have auto-update features that just want to check if there is a new versions. In some cases, a program (say an antivirus for instance) will check for updates "every x hours" so out of no where, you may see an alert that a certain program is checking for an update again.**
    - **This feature is usually in "Options" or "Preferences" somewhere (in the program that is trying to connect); and, simply "unchecking" this option will stop further connection attempts on the part of the program, in question.**
- What Firewall to use?

  Firewalls (some of these are security suites)

    - My old firewall (Outpost) is one I still like, and it only rates slightly below (protection wise) than Comodo. I still highly recommend Outpost (Free or Pro)

      

        - **Comodo Internet Security**
            - (http://personalfirewall.comodo.com/)
            - Note: Comodo Internet Security is the same as Comodo Firewall but with Comodo Anti-virus too ... I never use the Comodo AV, so I just opted for Comodo Firewall.
            - *** BOTH ("Comodo Firewall" and "Comodo Internet Security") have Defense+, which is the program "defense" (I am sorry, but I do not know how else to put it) feature that many firewalls have now-a-days and it controls what a particular program IS ALLOWED (not related to the internet, necessarily) to do or not do on your system, adding an additional layer of protect to your system.
            - Please see some tips I have for Comodo, further down the guide, to get the most out of this firewall.
            - *Feb 2013 Update*: After Trying it on a few computer, I have found that Comodo is starting to remind me of Roxio and Nero (Burning software)
                - What I mean by this is that once I used Roxio, then switched to Nero after Roxio got too bloated (in my opinion), and THEN, years later stopped using Nero for the exact same reason. I once used Zone Alarm (Roxio in this metaphor) years ago, before it got way too bloated for my tastes, then I find myself now with Comodo on only one of my computers (I am staying with version 5.x on this one), and the idea that I may switch that to one of the other firewalls, I list below

- I want to take a second, to explain what I mean by “bloated”. Programs always get bigger as more features are added and bugs are corrected.
  - I AM NOT counting the installer size as I found that instead of a 30MB installer for each 32bit or 64bit version of the program, now they seem to have one @80MB version that has both 32bit or 64bit versions in one (so you can use the same installer on either Windows 32bit or 64bit).
  - It is perhaps a matter of opinion, though I have to say that, “bloat” includes adding a ton of “useless” features, taking up a lot more resources (“power”... not necessarily meaning electricity) from your computer. Having a few “Bloated” programs on your system can end up slowing even somewhat faster computers down, significantly
    - Just as a quick example, I found that with either Privatewall OR Online Armor (Free Edition), INSTEAD OF Comodo 5, my older (1.79GHz, XP 32bit, 768MB of RAM, and Avast 7 … to give you a reference point), resulted in MUCH better system performance.
    - I actually thought it was Avast slowing my system down (and while it could have been the Avast + Comodo Combo), I almost by mistake found that when I disabled everything Comodo (when it was installed) related and kept Avast running, my system performed like it use to, with no lag or slowdown.
  - I hate to say it, but I feel that Comodo version 6 has taken a step back. I think users who love the new Windows 8 interface, my like the new interface of Comodo 6, though after awhile it turns out to be a pain to get to any basic setting.
  - Endlessly clicking to menus to get to another menu to get to an option that shouldn't be that difficult to adjust in the first place is just going to confuse users and in my opinion that may “turn people off” from using any firewall in the first place.

- **Outpost Pro**
  - (http://www.agnitum.com/products/outpost/)

- **Outpost (Freeware)**
  - (http://www.agnitum.com/products/outpost/)
  - Rates high on many review sites [(security review sites that test firewalls), NOT just user reviews]; although not as high as Comodo rates.
  - I use the pro version, but I still love the free version of Outpost

(Feb 2013 Additions)
Both of these two listed below seem to be decent on resources and they get reasonably high reviews, from security sites and users. (Granted NO SOFTWARE FIREWALL, is “unhackable”). Right now I have each of them on my older computers (Online Armor on one computer, PrivateWall on the other), and I must say I am impressed.

- **Online Armor** (Free Ed) - (http://majorgeeks.com/Online_Armor_Free_d4872.html)

AND

- **PrivateWall** (http://www.privacyware.com/personal_firewall.html)
- (a FORMER Shareware, now freeware)
- This one is NOT for “new” users and I personally could see newer users getting confused by the interface. If you are a new user, and you want to give this one a chance, “go for it”, though note my comment, please.

- **Peerblock**
  - (**http://www.peerblock.com/**)
  - ** This is an IP blocker and NOT SUPPOSE TO BE USED AS A FIREWALL REPLACEMENT... BUT RATHER A FIREWALL COMPLEMENT **
  - This is a nice IP Blocker that can block access from/to certain IP address on your computer. You can Google (Search) “IP Blocklists” that you can import into Peerblock; although, I have found sometimes there are too many IP's blocked and sites like www.google.com can be blocked ... It IS *VERY EASY* to remove those "extra" entries., so its not really a big deal

GENERAL FIREWALL RULES

- **Local Connections**

  I find its usually O.K. to allow (I use as strict rules as possible) anything where the DESTINATION ADDRESS IS 127.0.0.1. For those of you who do not know, this is basically telling the computer to connect to itself ... 127.0.0.1 is your OWN computer... no matter what computer your on ... the address of ITSELF is 127.0.0.1.

- **General Predefined rules**

  The predefined rules are only found in Comodo, from what I can see, though you can use some tips below to set up whatever firewall you choose.

  Here (Despite the firewall you choose to use), I will list a few rules, that you can use as guides, if you'd like. As with most ,,, you can look at your firewall log if you can not make a connection and adjust the rules for your need. I am just listing "guidelines"

  - *(ALLOW) Local connections only*
    - I have set to allow All connections (TCP or UDP) to LAN addresses (your LAN addresses may vary)
    - Block and Log Everything else
  - *Outgoing Only*
    - Allow All outgoing (TCP or UDP) connections to any port and any address
    - Block/Log Anything else

- **Firewall Rules - Per process**

  Below are some are rules I found to be good. I am NOT claiming to be a security expert, but after some research I found found that these will not effect my system in a negative way. (I have tested these on a few of my computers, with NO ill effects)

1. *SVCHOST.EXE*

   This one is tricky,.... I am talking about the original version located in C:\Windows\System32. IF YOU HAVE AN INFECTED COPY OF SVCHOST.EXE, I can not speak for the safety of that

   - I set this Outgoing Only on this laptop;
   - I believe I HAD it set to Local Connections only on my old laptop due to my new laptop was unable to connect to the LAN on it.

Extra's

This branch is really “extra” and not counting wiping your data off a computer when you sell it (of passwords, and personal data) … I would say most users can skip this section (doing the tasks in it .. .though some of these tasks , listed below, may seem useful to even some novice users.

- **Wiping Files, Folders and Free Space**
  - There are many reasons you may want to wipe a something on your computer …. mainly security would be the reason
    - To use a brief summary, Wiping an item over-writes the existing data based on the program's settings and what the user selects with other data, making data recovery harder *(I am NOT SAYING a true professional can not recover the data with the proper training and recovery tools/programs)*
    - I am not going into details about the wipes, or the technology behind it, here, though I do plan on adding links to great resources for those that do want to look this information up
      - There are many tools that work, however, I find the best option to be the freeware, Eraser


      - (Granted, that I am no security “expert”, but I did check the wipes with Dir(ectory) Snoop and they seem to work)
      - The 6.x series seems to be buggy if you ask me
        - I am NOT ATTACKING the developers (which are not the same as every version up to 5.89 I believe)
      - Doing random tasks like setting up tasks to be wiped (say Temp files), or even running created tasks, seem to cause the program to crash (close automatically) and crash repeatedly on both computers I have tried ANY version of 6.x Eraser on
      - I am sure this issue is being worked on for future releases

Comodo Maintenance

Clearing Comodo Logs

- This is one of those "judgment call" steps
  - *Personal Experiences*
    - I reached this idea, after checking COMODO logs on a few machines, and finding entries for over three weeks before. This is completely un-needed to me.
      - **If you are using is not solely yours, CONSULT the other users/admins before doing this.**
    - **This is not** a "your computer will run 100% faster" step, but rather a "why keep items for that long, if you don't have too?... Like Coupons … every little bit (optimization) helps … put them all together and your computer will run better (baring any hardware issues)

- **How to Clear Log (in Comodo 5.x)**

  1. When Comodo interface is open, click `Firewall` (or `Defense+`) tab
  2. Click (based on which one you clicked in step 1) `View` (Firewall/Defense+) `Events`
  3. Click `More`
  4. Go to `File` and `then Clear`
  5. Your Logs are now clear

- ***Purging Trusted Entries in Comodo***
  - First off, even if you have Comodo, this is NOT a step you need to do often, though if you never have done this one, it may remove a lot of entries. In theory, this is like the clearing the log step, listed above
  - Going to Defense+ and "Trusted Files" and Purging this from time to time to prevent un-needed clutter
  - **How to Purge "Trusted" software of un-needed entries**
    1. Open the Comodo Main Window
    2. Go to the `Defense+ Tab`
    3. Click Trusted files
    4. When that next screen appears, click Purge
    5. Look over the list of "removal entries" to make sure there are no entries you DO NOT want to remove (though it is easy to "Re-add" them)

Closing

My Website:

For more tips. programs suggestions, and security information, please visit my sites at http://xmetalfanx.awardspace.us or http://xmetalfanx.x10.mx/ .. When I have fully uploaded my files, both sites will be exactly the same (think of them as mirrors). I have had bad luck with web-hosts, and did not originally intended to "have a mirror setup" for my site, though once the idea came to me, it seems to make sense.

When fully uploaded, both sites will be considered my "homepage" and I do not have any preference as one host as a "homepage" and the other as a "Mirror of my homepage".

Different web-hosts I have had in the past, have canceled service without notifying me and when signing up for another host, I have had to wait, so my site was offline (off the internet) for in some cases a week or more at a time. I figure even if one of these hosts, stop service, then I still have the other host to refer people to.

This guide was typed in:

- **Libre Office** (Free Office Client for a variety of Operating Systems)
  - (http://www.libreoffice.org/)

Thanks

I want to give thanks to sites, programmers, and friends, along with people I never met, but give great advice .. I know I may forget some (there are so many I want to thank, but hopefully I will include everyone I want

- **Ghacks.net** – News, "new" (to me) programs, tech advice and news
  - Of course I mean the contributors to Ghack, not just the webmasters themselves
- Programmers and developers (along with all beta testers, ...etc) of the mentioned programs...
  - I am constantly updating this "Guide", so I am not sure if listing all programs here would really be "smart" though if you see your program listed, I thank you for making a great product

