

As our student body - and by extension, the school - grows, we encounter more and more situations where reliance on our technical infrastructure becomes critical. The IT Dept works very diligently to maintain a clean & safe networking environment, so that personal and educational information relating to our faculty, staff, and students remain secure and protected. This predominately involves security enveloping our servers, the staff systems permanently resident on site, and the systems located in the labs. Those systems that physically leave this protected environment - aka student and instructor laptops - become more of a hazard as they are exposed to access points to the internet that are not filtered through the various layers of our on site security. We continue to take steps - Cisco Clean Access for instance - which are intended to make it more difficult for the integrity of these satellite systems to become compromised. But a very large part of protecting these individual systems falls upon the end user.

There are many resources available on line which are extremely effective at describing the damage malicious software can cause, and at detailing methods for avoiding the problem. Many of these same sites are, in fact, purveyors of the very problem that they pretend to be addressing. In other words, pop up warnings that you are infected, or that you need to run this or that update in order to fix a critical problem can often be false, and may be intended as the foothold that the malicious program needs in order to get installed. The only real preventative that works for avoiding this type of ruse is to educate yourself regarding the problem, and become comfortably aware of the ways in which you can work to avoid becoming a victim.

For the past several years I have been compiling a resource library of effective tools for cleaning infected systems, and preventing future problems from occurring. Unfortunately, there is not a "once and done" solution, nor is there a "perfect solution" that prevents all manner of problems. Those of you who have had your PC's for several years will recognize many of the programs that I currently use, you may recall that some have been around longer than others, and you may notice that some of the programs I advocated in the past are no longer on my list of effective tools. The parasites and their methods of infection continually change, and our approach to solving the problem must change at times as well.

In the past I have tried to pass this information along to any and all interested parties, whether student, faculty, staff, relatives, friends, people wandering in off of the street, etc. - basically anyone who would listen. Unfortunately, this type of informal distribution proved somewhat ineffective.

Therefore, I am providing links to some of the more informative and trustworthy sites, and hope that you will take it upon yourselves to follow up with these resources so that you may more effectively use your laptops, as well as being

able to use this information to protect the computers that you use at home.

The following list details some of the more common symptoms that could indicate the system has fallen victim to malware. (malicious software)

1. It appears to be operating substantially slower than it used to. (computers do not in fact "slow down" as they get older - they slow down because there is a greater drain upon their resources, most commonly associated with hidden software running in the background, preventing processing and memory from being effectively utilized by legitimate programs.)
2. Advertising interruptions - This could be in the form of popups, redirects to different websites than you intended to go to, additional browser windows opening behind the one you are viewing, or slower download speeds to legitimate sites.
3. The system "locks up" or "blue screens" - Because parasites are often poorly coded, and are trying to hijack resources devoted to more mainstream processes, they can lead to system conflicts which cause legitimate processes to halt, or act erratically.
4. There is software installed that you don't recognize or remember downloading. Very often parasites take advantage of security loopholes and open the system up to further intrusion, often resulting in programs being installed without direct user intervention. This can occur as sort of a "piggyback" to an intentional installation where the enduser was not aware of everything that the installation would entail. Many of the "Peer to Peer" music sharing schemes are notorious for installing secondary advertising programs in the background during their initial installation, and in some cases these "sharing" programs actively turn off security components of Windows which are intended to prevent further infection. This actually opens up the system to further problems, as there are now fewer safeguards in place to protect the user.

I have found the following resources to be invaluable in combatting this continuing problem:

<http://www.doxdesk.com/parasite/>

This website contains a very informative database of known offenders, with links to effective tools for use in cleaning up current issues and preventing future problems.

<http://aumha.org/a/parasite.htm>

A very informative site intended to educate the user on what the problem is, as well as how to avoid it.

<http://www.bleepingcomputer.com/tutorials/index.php?act=print&tut=41&client=printer>

This printable document explains the basics of the various parasite threats, and provides links very effective tools.

<http://aumha.org/a/health.php>

This website has a comprehensive list of things you can do to keep your system "healthy." This addresses more than just parasite and malware issues, and may be of more use in relation to maintaining your home computers than it does in relation to your school issued laptops, but it is a great resource.

<http://www.bleepingcomputer.com/tutorials/>

Here are 91 tutorials covering everything from formatting a floppy disk to setting up your own home network. Very useful in many situations, provided you are willing to take the time to search for issues relevant to you.

There are many more I could list, and if you should desire more, I will provide them, but all of the above are in and of themselves excellent resources for fighting the good fight. Each has links to further resources and tools, as well as discussion forums where current problems are discussed and resolved. On many occasions when I have encountered a students system with a particularly invasive infection, I have turned to the discussion boards and found solutions there. It can get exceptionally geeky, but on most of the forums the moderators do their best to keep things on an "everyman" level, and attempt to avoid making the solutions sound more complicated than the problem.

The direct tools that I install and use most often are the following:

SpyBot Search & Destroy -

http://www.download.com/Spybot-Search-Destroy/3000-8022_4-10401314.html?tag=lst-0-1

arguably one of the best all around tools for keeping your computer functioning cleanly.

LavaSoft Ad Aware -

<http://www.download.com/3405-8022-5153545.html?part=dl-ad-aware&subj=dl&tag=top5>

Another very effective tool that I often use in tandem with SpyBot S&D.

SpywareBlaster -

http://www.download.com/SpywareBlaster/3000-8022_4-10486084.html?tag=lst-0-1

This one is more of a preventative medicine than a cure. It does very little in the

way of finding and removing problems that you may already have, but it is very effective at preventing the malware from getting onto your system in the first place.

Now, these are by no means the best and only tools to use. There is no perfect solution to this problem. But these 3 programs together, providing they are kept up to date, and are run occasionally (say every other week or so) are very effective at maintaining a cleanly running system. And, on the plus side, each is free for personal /educational use. If you happen to stumble across some wonder program that promises to do everything, and only cost such and such, avoid it like the plague. In all likelihood it is part of the problem. This is especially true if this program is trying to convince you that you already have a problem, and that the only way to fix it is to pay their fee and use their software.

<http://www.benedelman.org/news/121905-1.html> - this link discusses the whole conundrum surrounding who is trustworthy, and who isn't. Interesting reading.

<http://www.benedelman.org/> This is the same individual as above, he has quite a compilation of very well documented research into the whole industry of invasive advertising, and it serves to underscore the level of threat that all this entails, and strives to shed light on the whole sordid mess.

Additional requirements to maintaining a cleanly functioning system are that your operating system be up to date, and that you have current antivirus definitions. All of the school systems should now be set to run windows updates automatically, and so should not require much in the way of input from the end user, but in reference to your home systems, you will want to check with Microsoft updates on a regular basis.

<http://windowsupdate.microsoft.com>

Many forms of malware and viruses rely on exploiting windows security holes in order to obtain access to your system. Merely maintaining a current update of windows can prevent these problems.

All of the school owned systems have the corporate edition of Norton (Symantec) Anti-virus installed, and they are set to refer to one of the school servers for current updates, so you should not encounter problems with this issue. On your home systems, I highly advise getting a solid, reputable antivirus solution, and keeping it up to date. I advocate Norton's by personal preference, but anything up to date is better than something out of date. And similar to parasite prevention software, it is only effective if you actually run it occasionally, and keep it updated.

So, you may be wondering why I have brought all of this to your attention. In part it is in response to requests from various individuals who sought information

relative to cleaning up their home systems. In part it is my way of trying to shift part of the responsibility for keeping the laptops clean over to the people most capable of doing so - aka, those who are using them. It can take over 8 hours (sometimes considerably longer) to completely clean up an infested system. In many cases, it would often be a simpler solution to just format the drive, and start over. But that approach runs the risk of losing the users data if not properly backed up, and performing a full install can be a time sponge as well. With the roll out of Cisco Clean Access, faculty and students systems which do not meet the criteria of cleanliness that Cisco is checking for, will not be able to connect to our network at all. No internet, no blackboard, no mail, no printing - no network activity of any kind until the system meets the required standards. This kind of consequence requires that we provide you with the tools and the knowledge such that you will be able to maintain the systems integrity so that your ability to work does not become compromised by an infected system.

It is my intent to continue to be available to assist students and faculty with these types of problems. But, since there is no formal class where the PC students have this sort of information provided to them in a "study it, learn it, live it" format, I wanted to provide a reference for instructors. Should you encounter students with questions, you will be able to refer them to the types of tools which can benefit them. I have encountered numerous situations where a student will have a virus infested system - and have Norton's installed - but when I launch their antivirus program, it shows that this is the first time it has ever been run, and indicates that the virus definitions are way out of date. If we can prevent that sort of thing by being there to remind them, and encouraging them to learn how to most effectively use this tool that we forced them to buy, it can only benefit all of us.

Viruses, parasites, and malicious advertising software are here to stay. We can't press a button and make them all go away, but with forethought and preparation, we can regulate them to a minor nuisance level, instead of allowing them to cripple our systems performance.

Common sense and current updates are the key.