Instructions for using the OCS Maintenance checklist

[Rev 1.0 August 2016]

I recommend checking the following items every month. Some of my client have me do it. Others handle it themselves. Some compromise and do it themselves but have me check quarterly in case I can see something they missed.

The Antivirus check

- RealTime Logs: Your antivirus program should offer a log of real time events. In Nod32 this is under Tools / Log Files / Detected threats. Examine the log and determine if it indicates a problem. For example, lots of detected e-mail viruses would indicate that you should have better spam protection. If you are getting more than one threat every few months you probably need to change something. Vipre has these options under Manage / History (you need to scroll down).
- Scan Logs: I setup computers to do a full computer scan once or twice a week usually around 2AM. You want to make sure this is happening and examine whether viruses are caught in it. Hundreds of new viruses come along every week, so the realtime scanner may have missed or not known about a particular virus. This is designed to find those. These logs are available with the same menu structure as the realtime logs. If it isn't happening figure out why. Even if you don't leave your computer on every night, I suggest you leave it on once a week for maintenance chores like this.
- Updates? You also want to check the the signature files and the program itself is being updated. This is usually found under an update menu.

Patches/Updates

- Microsoft: Be sure that the Microsoft updates are being done. I normally have a link in the maintenance folder to check. For Windows 10 do a Start / Settings/ Update and Security to see that you are up to date.
- Ninite: turns Red when updates are necessary. If it is red, then run Ninite and let it apply the updates. The Ninite Updater service scans almost 100 common applications for updates and quickly applies them without sneaking in unwanted applications. If you haven't got Ninite Updater, get it.

WinPatrol Check

I install WinPatrol on all my computers. It is a free program that monitors what starts up and runs on your computer. Using it, I check:

- Odd startups? I look at the startup programs and see if anything is odd. I do not know how to make this easy. Most people have a lot of stuff starting up and not very much experience sorting the good from the bad. A WinPatrol Plus account lets you check their database and you can do a Google search on that application. WinPatrol lets you save notes on each application, so you'll only need to look them up once. However, this is a good time to mention a basic rule. If you don't need it

running, tell the program to stop running. If you don't need it at all, uninstall it. Startups can also be disabled here.

- Temp Files: When I setup a new computer, I use the ancient open source TempFileCleaner from Mulder Software. I set it to run at startup every time the system is booted or rebooted. It is not very thorough, but it quickly cleans out most temp files that should be cleaned every time a system is started or rebooted. This gives us a reasonable cleaning so in depth cleaning is seldom needed. I use WinPatrol to check that is is running.
- Regular Defrag: If you have a spinning drive, NOT an SSD, then you should defragment it. I recommend a quick weekly defrag using the free Piriform Defraggler. As with the Antivirus scan, this can be done at night while we sleep for computers left on only once a week. This can be checked under scheduled tasks to make sure it was run this week.

Backup Logs

It is important to check that your backups are actually working. Many people have assumed that the backups were doing their job, only to find that important files weren't getting backed up or worse, no backup was happening at all. I recommend three backup systems for most of my clients.

- Local: A data backup to a USB drive attached to the workstation.
- Internet: An off-site data backup to somewhere in the cloud.
- Images: A monthly complete image of the entire hard drive.

Local:

I normally use Centered Systems Second Copy for the local backup. It will copy whatever files you want, whenever you want to a local drive and keep as many previous versions as you like. It is very configurable. For second copy I recommend looking at the log file to see if there were any problems. Just right click on the icon in the taskbar and examine the last few days of log files. From the full program, the icon on the right points to the log. There should be record of when files were backed up and whether the backups were successful. Second copy will show an "E" on the taskbar icon if there was an issue.

Occasionally, you should examine your external drive and see what is actually getting backed up and check for important files, especially new folders you have added.

Internet:

I recommend Spideroak for backup. But these programs all have some kind of logging function. In Spideroak, you can check Home/Completed to see all the files that have been backed up since the last reboot. I find it useful to check this frequently at the end of a workday when I can remember what was supposed to get backed up.

Image:

I recommend a full image of the entire C drive once a month and keeping a few

previous copies. This way, if Windows gets infected, or goes crazy, or the drive dies, you can restore the entire system to a new drive very quickly. This way all your programs, Windows, Windows updates, printers, video and network drivers and so forth will be back in just an hour or so along with your files up to that monthly image. Then you can restore the needed data files and be up and running.

I normally check to see that the monthly image was made, but you should occasionally open the image and check a couple of files to make sure you can get into the image and read the files.

My preferred imaging program is Macrium Reflect.

Other

- Heat and Fan: I use some software to check drive space, heat and sometimes fans to make sure the computer is not overheating. Fans can go out, computers get dirty inside and the dirt insulates the parts and they can overheat. In general computers heat up when working hard, and cool down when hardly working. If it isn't doing much and maintains a temperature over 150 degree Fahrenheit, then take action. Laptops tend to run hotter than towers because they have less ability to dissipate heat. I do not worry when temperatures remain below 130 at rest. Most of my newer computers tend to keep CPU temperatures and drive temperatures below 100 degrees Fahrenheit. I use one of the following programs:
  - Open hardware monitor : is my favorite program, but it is open source and the project is not active. The last release was almost two years ago and it does not work on all the latest computers.
  - My second choice is the excellent HWMonitor free version, which keeps up to date. I've used other programs in the past. As long as you can check the temperature you'll be ok.
- Empty the Recycle Bin
- Malware 2nd opinion: I recommend a monthly scan with Malwarebytes to see if there were any infections your antivirus missed. I prefer the free version.

Of course, keep you eyes open as you do your monthly maintenance for any issues that might come up.