Computer Viruses, Malware and Spyware (Revisited 1/11/2021)

This write-up goes hand-in-hand with the Scams writeup from November 2020. The reason this is true is that very often unwanted programs and other nuisance items can appear on your machine as a result of improperly handling these scam attempts. Or they can be the result of what I referred to in that handout as "distractions". You may have the best of intentions about installing a program that you actually want, but due to the way the website appears, it is easy to click on the wrong thing and thereby install something unwanted.

An unfortunate part of modern personal computing is the need to deal with unwanted computer "invader" programs, often called viruses (e.g. Trojans, Rogues and Hijackers), Malware (sometimes called Scareware or Ransomware), Spyware, Potentially Unwanted Programs (PUPs) and cookies. These types of programs or files can infiltrate your machine simply by your being on the Internet and visiting "infected websites". In order to prevent, clean, block or eradicate these unwanted intruders you will need a several-pronged attack described below. Also, undesirable are tracking cookies - small pieces of information that eavesdrop on your internet habits. It seems cookies come from "everywhere", even popular websites. These, too, need to be dealt with.

*Note: As with other handouts, some of the ideas described here represent my opinion - often abbreviated IMO (In My Opinion). I have quite a lot of experience in this area but I'm sure some who read this may have counter examples. Also, if you ask a lot of different people for advice, you run the risk of getting differing opinions. It is usually a good idea to establish ONE source of information that **you** trust, and stick with that.*

The first question I am often asked when discussing this subject is, "What symptoms will my computer display that indicates that it has a virus or is burdened by some of the undesirables described above?" This is not meant to be a smart-aleck reply, but the answer is actually similar to what your doctor might say if you were to ask him, "How do I know if I'm sick?" Just as human illness may be accompanied by a fever, aches and pains, nausea, dizziness, a rash, weight loss, or fatigue, a computer infection can manifest itself in a number of ways. One or several of the following conditions may be observed:

- Your computer may simply slow down; functions that used to work suddenly don't work (e.g. webcam)
- Unusual messages may pop up offering to improve performance
- Internet surfing doesn't behave correctly - extra slow or strange pages appear
- Settings may change, home page may change or your background (Wallpaper) may change
- You may get (bogus) warnings of infections based on a "free scan" or the Internet may stop working altogether. Please know that legitimate programs don't install themselves, scan your computer, and then ask for money.
- In a worst case, your computer may lock up with a dire warning screen (FBI or Department of Justice for example) trying to extort money by saying you are guilty of a crime.

Viruses and AntiVirus (AV) Programs

Viruses can be grouped in several categories. Some are Trojans that get in by masquerading as good programs. They can corrupt files, cause unusual behavior or prevent certain things from working correctly. In extreme cases they can corrupt data which could inhibit your ability to boot up. Another category is the Worm virus that tends to mess with your email. Also, email is a possible source of a virus (typically through an embedded link), but by no means the only source. Simply visiting a website that is infected can expose you to the bad things. Just like human diseases, some are fatal, some are curable but leave scars, others are fixed and you're as good as new. With computer viruses - a rare few actually disable your machine, some can destroy data and others, when cured, will leave no trace. Many viruses today try to get you to voluntarily "buy" something. Buy is in quotes because it is really blackmail. Others will freeze your machine and state that you are guilty of some crime and owe a "fine" to release your machine. It's interesting that the "fine" needs to be paid in cash. Examples of this type include: FBI, Dept of Justice, Homeland Security and Wanna Cry Virus. They require special attention. (See my "Scams" handout from November).

There are a number of well-known AV Programs on the market that you can purchase. These include, but are not limited to, McAfee, Norton, Kaspersky, Trend Micro, ESET and WebRoot AntiVirus. (Many new computers today will have a trial version of one of these pre-installed - McAfee is the most common) These all cost in the neighborhood or $40 to $50 and must be renewed annually. There are a number of free AV Programs that are very good, so, in my opinion, there really is no need to incur this expense. These include Windows Defender, Avast, AVG Free and Avira. Probably the easiest approach is to make use of the Anti Virus program that is built

into Windows 10, 8 and 7 called Windows Defender (WD). WD is always there in those versions of windows, but to be safe you should uninstall others that may have been pre-loaded such as McAfee - see next paragraph.

If you are going to install a different virus checker in your computer from the one that is already there, it is necessary to remove the old one first. Example - you must uninstall Norton before installing Avast. If two virus checkers are loaded and active on the same computer, you sort of set up a civil war between them and neither functions properly. The proper way to uninstall a program is click the Start Button, (In Win 8 you need to use the charms) open the Control Panel and then use the Program and Features list. Highlight the item to be removed and then choose uninstall.

"How can anything that is free be any good?" you ask. The answer is, many free AntiVirus programs typically sell a more sophisticated version that is more suitable for companies. A free edition is usually enough for individuals. If you want greater protection more features, you can certainly upgrade.

Bottom Line: You should absolutely have an AntiVirus Program installed that runs a scan periodically. I recommend Windows Defender or, to a lesser extent, Avast or AVG. Once installed make sure you set it to update daily and scan at least once per week. I prefer Windows Defender over others for two reasons: 1) Well-known virus checkers such as McAfee and Norton can bog down your computer's performance - especially if the computer is older and 2) Avast can be downloaded, installed and updated for no charge; Windows Defender comes installed with Windows 10, 8 and 7. WD represents the easiest approach.

It is imperative that you are comfortable with your choice of a virus checker. Use the Internet to look up reviews and summary of features so you can make an intelligent decision of what works for you. If you have some corporate experience with a virus checker and you like what you experienced, go with that.

Malware

There is an entire category of unwanted programs called Malware that are frequently not detected by AV Programs. Malware, sometimes called Scareware, Hijackers or Blackmailers, often install themselves and then purport to give you a free scan. The scan will always tell you that your machine is badly infected and that for only $149.00 (or some higher fee) they will fix you. A characteristic of this type of program is that it gives you FAKE positive warnings in order to scare you into buying their (often) worthless product. This is like paying money to kidnappers or blackmailers - who knows where it will end? Instead, if you have Malwarebytes Anti-Malware installed, you can use it to scan, detect and remove many of these bad programs. Some of the BOGUS names that look very legitimate are: Cyber Security, Personal Anti Virus, AntiVirus 2021, Security Center, Think Point and Cyber Patrol… These ARE viruses! Remember no real program will install itself and run a free scan without asking you. If you see any of these names installed, you ARE infected. Another tell-tale sign is if it says "Microsoft has detected a virus". They don't do that. Some of these rogues are so insidious that they require that you boot your computer into "Safe Mode" before you can remove them. Sometimes even safe mode won't work and you need to boot from an external device such as a flash drive. There is an excellent program called Malwarebytes Anti-Malware that is available from the website www.filehippo.com that you should have available. (current version at this writing is 4.2.3).

Bottom Line: IMO, in addition to an AntiVirus Program you should install, at least, the free version of Malwarebytes - Anti Malware. There are other Malware detection programs, but I have had very good luck with Malwarebytes. The free version, which is very effective, lacks the feature that blocks or deflects the incoming "bad guys". If you invest in the "pay" version it actually sets up a shield.

Spyware

Spyware refers to programs, files or some cookies (small bits of information put on your computer by web-sites) that tend to eavesdrop on your activity on the Internet. These are often disguised as marketing tools or statistical tools. Cookies can be good (coming from a website where you want to be known, such as your bank) or bad (some come from third parties that want to track what Internet sites you visit). In general, spyware doesn't really harm your computer, but if you have too many of these items your performance may suffer. There are a number of free Spyware programs that can be installed. IMO the best of these is called SuperAnitSpyware, downloadable free from www.filehippo.com under 'Anti-Malware'. On these download pages, there are often "distracters" that try to get you to download a different program. If the program asks for money, you've got the wrong one. Another good one is Spybot Search & Destroy, but it takes longer to scan.

At this writing, the latest version of SuperAntiSpyware is 10.0.1208. This version has several very useful features. First it will look for "unwanted" programs when you perform a scan. If it finds any it will offer you an opportunity to remove them. Do it. Also, under System Tool, it will analyze your startup list and identify things that need attention.

Bottom Line: SuperAntiSpyware and/or Spybot S & D are good programs to have. The free versions will scan (at your request) for undesirable programs and cookies and remove them. AVG Free AntiVirus has a spyware seeking tool but it is not all-encompassing. Contrary to the way AntiVirus Program behave, AntiSpyware programs tend not to “resent” one another. You can have all you want. There is a program called Spyware Sweeper by Webroot that is a pay program that is often installed by Best Buy. There is a version of Spyware Sweeper that also includes an AntiVirus function. If you have this one, it will conflict with AVG. The Webroot programs are not bad programs, but remember they do cost. I have worked with a lot of these free ones and have found that, in most instances, the free application will perform just as well.

.

CCleaner & WinSysClean

Although not an AntiVirus Program, CCleaner is another free program that I have had success with. It can be downloaded from www.filehippo.com. CCleaner is a freeware system optimization, privacy and cleaning tool. As of this writing current version is 5.76. It removes unused files from your system, allowing Windows to run faster and freeing up valuable hard disk space. It also cleans (if you want it to) traces of your online activities such as your Internet history. Additionally, it contains a full-featured registry cleaner and an uninstall tool that can sometimes be accessed easier than the Windows tool. It has been one of the most popular downloads from filehippo for some time. BTW, CCleaner comes in a more comprehensive "pay" version that I have never purchased. Beware of unwanted programs that purport to do the same thing - example of one I consider bad is "Slim Cleaner".

Two other cleaner program that I have had some good luck with are WinSysCleanX9 and Glary Utilities. Like CCleaner, they come in a free and more full-featured, pay versions. They do much of what CCleaner does, but having them all available to isn’t really a bad thing. You certainly don't need all of them – that would be overkill. I have only used the free versions.

Bottom Line: Having a cleanup program that you run periodically will help keep your computer performing at its best. CCleaner has always worked for me. Download it, install it and run it once per week. It will remind you if a newer version is available. (Sometime back CCleaner was targeted by infiltrators and, for a while, was compromised. I believe that was version 5.33. Current version is 5.76)

Unwanted Programs (PUPs - Potentially Unwanted Programs)

Unwanted programs, that aren't really viruses, can install themselves on your machine and become a monumental nuisance. If programs continue to prompt you to things such as update drivers, you likely need to do a cleanup. These can be isolated and cleaned using Malwarebytes, or you can do them individually by opening the Control Panel, going to Programs and Features, sorting by Date Installed and then uninstalling things that happened lately that look suspicious. "Driver Updater" is the one I've seen most often.

Advertised Cleaners and Virus Checkers (as seen on TV)

There are a number of software products that are advertised on television or radio that claim to be "the fix" to whatever is wrong with your PC. Two of these are "pcmatic.com" and "mycleanpc.com". When you hear these ads in the media, my advice is to mentally tune them out. When you consider how much TV air time costs, you figure that these services must be expensive. Secondly, you wonder, if they are any good, why do they need TV or radio time? They should be featured in computer magazines or online. Remember the website www.filehippo.com, that features good, legitimate software, doesn't show these. I think there is a reason.

I personally did some investigation into the two mentioned above. An Internet search (avoiding the results marked as Ads) revealed very mixed reviews. When you install the programs they offer a free scan (I almost typed 'scam' instead of scan - must be Freudian). That scan will identify a high number of alleged problems. When you go to fix them the request for money kicks in. Many of them have tiers of service. If you call the 800 number, they will tell you that your list is serious and you require the package that costs several hundred dollars. It's amazing that people with brand new computers - out of the box - show ALL these issues. They will offer a 30-day money back guarantee to suck you in. Be careful. Once they get your money, getting it all back is

nearly impossible. I've known folks who have been victim to these items and only got a partial refund after much time on the phone.

Some of these programs also offer to speed up your PC. This is kind of a nebulous promise and tries to prey on a common complaint from computer owners - that your computer has slowed down. Speed can be measured in several ways and they never tell you how they are going to measure the speed-up. A benchmark must be taken first to verify that a change occurred. They don't do that. Speed problems can relate to boot time, opening an Internet Site, or calling up a program. They each should be addressed differently.

Bottom Line: IMO, be very leery of any software product mentioned on TV or radio (e.g. PC Matic) that seems too good to be true. Most of them are (too good to be true). I recommend that you get advice from someone you trust and/or use the programs described at the beginning of this handout to improve your PC's performance and keep it running virus free. There will be other things in other write-ups (later this year) to address ways to speed a machine up. It really irritates me to see people taken advantage of, and many of these products tend to do that.

Summary

Yes, you do need all four types of programs - AntiVirus, Malware Detector, AntiSpyware Program and a Cleaner Program. They all do slightly different things, as described above, and are therefore necessary. I like to describe it this way: Rate computer problems caused by "infiltrators" on a scale from 1 to 10. The AntiVirus programs concentrate on the high end (8s, 9s and 10s). Almost everyone has an AntiVirus program so these are covered. Malware falls in the next category down - numbers between 5 and 8. Spyware and tracking cookies would be rated 2 to 5. Cleaning more like 1 and 2. Based on this, the four programs cover the entire spectrum. I often jokingly refer to the group as your computer's "Health Plan" or medical Rolodex (we tend to be old enough to know what a Rolodex is… ha).

One More Thought

In this write up, I have tended to emphasize use of the free versions of most programs. This is taking into account that my audience is largely casual home users. Those of you with corporate experience or keeping more sensitive data, may disagree with this and want the “higher level” of protection that some of the other, well-known programs provide. If that gives you greater peace of mind, you should do that. There are so many products out there, that you will find a great variety of opinions too.

And finally, this Virus-Malware-Spyware topic is very complex and can only be superficially covered in a short discussion such as this. If you want to learn more about any topic you can always “Google It”. When you do perform an online search, take note of the source of the opinion you are reading. Websites (there are more) that I have come to trust regarding software reviews are “BleepingComputer”, “CNET” and “Major Geeks”. Be aware that there are bad programs that give THEMSELVES glowing reviews. See cartoon below.

Dan Phelka 535-7791