Things People Do (or Don't Do) That Mess Up Their Computer

Home computers have been around for decades, and it seems just about every household has one. (I say "seems like", because I know not everybody has one but many homes have two or more). Many folks claim they only use them for email and Internet but actually, that's quite a lot. If computers are so common, why is it that they keep getting messed up and so often require outside help?

Viruses, Malware, Bad Cookies, Spyware, Adware, proliferate the computer world and, still, consumers struggle to understand what exactly makes things go wrong. I will try to address this subject here, because there are a number of items that can make things go awry.

To many people, computers are still a relatively new thing - and a little mysterious. Those who didn't grow up with them (especially those in our generation) may have acquired their first machine after age 50. They want one to keep in touch with their kids, grandkids and each other (or be on the PebbleCreek E-group). Most in this generation never took a computer course, so they are self taught. Many rely on their children or family members to learn how to use them. As a result many of the pitfalls that loom out there can easily happen (but not limited) to these folks. I even created a term I call "hand-me-ups" which are computers that kids give to their parents because they are too good to throw away, but the kids wanted a new one.

In reading this, you may experience some déjà vu. I have covered some of these items in other write-ups. I have addressed Scams in one handout and Viruses in another, yet they are listed here. That is testimony to their importance.

Here is a list of *common mistakes* that people make that can really foul up a machine. I mean to make no accusations here; I am just stating some facts. Keep these things in mind and you will likely have fewer problems. This is not meant to be the TOP 10 list or anything like that. It is meant to point out a few things that could lead to trouble. The below list is in no particular order.

Common Mistakes

- Visiting Unscrupulous Web Sites – First off… these don't have to be porn sites (Clearly porn sites, even free ones, should be avoided). There are many sites that "plant" things (like tracking cookies that follow you around or eavesdrop on your Internet activity) on your machine when you visit them. To minimize this, you should avoid visiting locations that try to lure you in with the promise of free gift cards, free laptops, shopping sprees or free scans. If you get a "pop-up" that congratulates you on being the 1,000,000th visitor to that site or something like that… run the other way! Remember things that appear too good to be true, usually are.

Also be careful about offers of gifts when you fill out a simple survey. Some information you must provide to these surveys should not be put out there for everyone to see.

A "little paranoia" is good, but don't become a nut case and pull into a shell. Anti Virus, anti Malware and anti Spyware programs can protect you from most of these things. Be a little careful and certainly don't be too gullible.

There is a setting in every version of Windows starting with Vista called User Account Control. It is found under User Accounts in the Control Panel. I recommend turning this off because it generates a very annoying message that continuously interrupts your computer work.

- Opening Email (especially attachments or links) from Unknown Sources - With a good virus checker, Email is no longer the main source of viruses, but be very mindful that attachments, especially if they are .exe (executable) files or clicking on website links within an email can infect you. You should utilize the delete key if an email looks at all suspicious. Also, I wouldn't answer an email to try and stop future messages from a given source. Answering can actually prove to the sender that you do, in fact, exist. They will likely keep sending things. Suspicious emails typically show all or several of the following four characteristics: 1) No subject; 2) No signature; 3) Very little message body; 4) Contains a link to click on promising something rewarding - e.g. funny, weight loss, etc. If you point the mouse at the link, the real destination link will show in the lower left. Clicking on an unscrupulous link will often "raise the ire of your virus checker" - so it will likely be blocked. When in doubt, don't even click on the link.

- Having Open Liquids too Close to Your Computer - It is amazing how many people have a cup of coffee, a glass of water, soft drink or wine (in an easily tipped stemmed glass) near their computer when they work on it. This is extra dangerous if you're working on a laptop. Accidentally spilling ANY liquid on a laptop can come close to destroying it. Keep your drinks at arm's length - literally. If you spill a drink on a regular keyboard it isn't such a tragedy since a new keyboard is only a few dollars.

- Failure to Back up your Vital Data - It's a fact that hard drives fail. Having an external drive (1000 GB or more can be purchased for under $100) to which you copy important information can save the day. You won't (can't) back up your Windows Operating System (e.g. Win7, 8 or 10) or Microsoft Office, but you SHOULD back up all your documents, Excel files, pictures, songs you've downloaded, your tax data and any other financial data (in Quicken or QuickBooks) you may be maintaining. Backing up can seem like a royal pain at the time, but if you have ever had a failure you know how valuable it can be. With apology to dentists, backing up is like flossing your teeth - you know you should do it, but most people don't.

There are legitimate websites or commercial services, such as Carbonite, that back your stuff up on the Internet. These sites require you to pay a subscription fee. Although they purport to be totally secure, some people worry about the safety of their backed up information. I believe they are OK, but it's still your call. A service like Carbonite will even save you if your computer is stolen.

The question often comes up, "Can you get data off of a hard drive after it fails?" The answer is usually yes, but it is quite time consuming (can be expensive) and requires special equipment and maybe outside help. Backing things up is still the best way. An old adage about an ounce of prevention certainly applies here.

One more thing (I sound like Lt. Columbo). Hard disks are in a hermetically sealed enclosure. Breaking this seal will cause a failure but so will overheating (without breaking the seal). Although the disk enclosure is impenetrable to dust, your computer fans are not, and they can get clogged with dust, pet hair or pet dander - which can lead to overheating. It is a good idea to vacuum your computer tower (not so important with laptops) to keep the fans clean and make sure there is no obstruction to air flow. If you open your computer tower to vacuum inside, be careful to not bump anything too hard. Also it can be helpful to occasionally blast a laptop's keyboard with canned air to flush out particles in between or under the keys. Another trick is take the sticky edge of a post-it not and run that between the keys. You may be surprised at what it attracts.

Disk maintenance, such as deleting temporary files can be helpful. This has less impact if your disk is not close to being full. CCleaner is a wonderful program to do this.

- **Failure to Have a Virus Detector (or not running it or not keeping it up to date) -** A good, up-to-date virus checker is a must. There are many for sale commercially, but free ones such as AVG, Avast or Windows Defender are more than adequate. With any virus checker it is imperative that it be kept up to date and run often - at last once per week. An AntiMalware Program (MalwareBytes) and AntiSpyware Program (SuperAntiSpyware) are good additions to your health plan so as to cover the complete spectrum of invasive programs.

- **Falling for Phishing (sic) Attempts.** Some cyber crooks send out very official-looking emails that look like they come from a bank or some financial institution. They will often have a company logo on it and say something to the effect, "Due to our error your account has been accidentally frozen. Please provide us with your account number and password and we will fix it." WRONG! No bank or broker would ever email you and ask for this information. First, don't answer it; second, if you want to, call the alleged source and tell them you got such an email. A dead give away, of course, is when you get an email from a bank, telling you that your account is locked, when you don't even have an account there.

There is a new approach involving a live person, which is quite prevalent, that you should be aware of. You may get a phone call (caller often has a heavy accent). Caller will say something about being a "Microsoft Partner" or "Microsoft Certified" (they will usually not say they are with Microsoft, because they are NOT) or they are with Windows Support and they have detected virus-related activity on your computer, or some other TOTALLY MADE-UP problem. They will then offer to take control of your machine and diagnose the problem. Remember this was a "cold call" and you likely have no problem. *Under no circumstance should you let a stranger, **no matter who they say they are**, take over your computer.* Their goal, if you give them access, is to run some bogus software to scare you (similar to scareware below) and then offer to fix you for some price that can range from$150 to $500. They may try to sweet talk you by saying this price includes a year of phone support. Don't do it! Hang up. If, perchance, you have given them a credit card number, call the card company and dispute the charge as soon as you can. If you make them angry they can introduce MAJOR PROBLEMS in your machine. If you gave them control and decide to hang up the phone, reboot you computer right away.

Sometimes these callers will ask if you are a senior citizen allegedly to offer you a discount. What they are doing is seeing if you are older in order to take advantage of you. They figure seniors may be more vulnerable because of their supposed lack of knowledge of computers.

One more warning. If you look up a phone number on the Internet to get help… be very careful. Let's say you have a printer problem and you want help from Hewlett Packard. You type "Hewlett Packard support" into Google. You will get a number from your search that may even be toll free. After you dial it and talk for a while they may try to charge you…RUN! Talking to a real manufacturer, especially about a newer machine that is under warranty, should not cost you. After you do your search for the number, have a look at the site that it references. It may way something like www.hp.support.techgurus.com. This is a site for **tech gurus**, not HP. There are so many scammers out there that looking carefully at the number source is certainly warranted.

- **Becoming a Victim of Scareware -** This is related to virus and Malware checking, but specifically, scareware installs itself, makes a fake scan of your computer and tells you about all the problems you have (also fake). Then they tell you for only $149.99 (or some fee) they will activate the program and fix you. Don't do it. Once you've agreed to that you have essentially paid a blackmailer. The program Malwarebytes Anti Malware (www.malwarebytes.org or www.filehippo.com) will get rid of most of these. No legitimate program will ever scan your machine without asking. Some of these may ask you to call an 800 number - DON'T!

- **Not Protecting your Computer from too Many Well-Meaning (human) Helpers** - There are an untold number of settings associated with operation systems, Internet Explorer, Anti virus programs and just about any application - even MS Word. The default values in all these programs may not be to your liking or for the best operating efficiency. Some messages that come up are hard to interpret. Well-intentioned people working in areas they don't fully understand can actually sometimes result in negative help. The old adage about too many cooks spoiling the dinner definitely applies here. Call someone you trust or if you are not sure what to do or how to do something on your machine, "Googling it" is always a good place to start to get useful information. Sites called "bleepingcomputer.com", "cnet.com" and "MajorGeeks.com" can be quite helpful.

- **Not Deleting Old Emails** - If you are using Windows Live Mail (Win 7, 8 or 10) or another email handler such as Mozilla Thunderbird, there are several folders that hold emails, e.g. Inbox, Outbox, Sent Items and Deleted Items. When you delete something from the Inbox it doesn't go to cyber heaven directly, but rather it goes into the Deleted Items Folder. It stays there until you either empty that folder or selectively delete items from it. If you forget about this, the Deleted Items folder can get filled to capacity - yes, there is a limit, but it's pretty big. When this happens, some strange behavior is observed - primarily not being able to delete items from the Inbox. It is, therefore, advisable to go through your emails now and then and get rid of ones you don't need. If you are on everyone's "joke" list or on the PC E-group, your boxes may fill up sooner than you realize. All the folders have limits. If Inbox gets full you won't be able to receive any email. If Sent folder gets full you may send out multiple copies of the same email.

Some Internet-based email addresses such as Gmail also have space limitations. Most of these give you several Giga-Bytes of space for free. When your free space is about exhausted, they will offer to sell you more. It is easier to just delete old, unneeded correspondence and stay within the original allotted space.

- Forwarding Nuisance Emails to the World - This is not so much a mistake as it is an annoyance. (This is kind of a pet peeve of mine) If you get an email from someone that warns you of a virus or some impending doom, Google it before sending to everyone you know. If you see an email describing a virus that says something like "Worst virus ever…" or "This comes directly from Microsoft…" or "Norton has no cure for this…" or "This will wipe out your entire hard drive…" you should definitely check this out before forwarding it. There is a high probability that something containing such a dire warning is a hoax, so don't go cluttering up other people's email boxes with stuff like this.

Also Microsoft, IBM or the government are not paying people to forward emails. If you get an email that says you are part of a test and that you will get a dollar for everyone you forward it to, check it out first. This is the cyber version of a chain letter. By the way, I'm sure you realize there is no money in Nigeria that is waiting to be shared with you if you front them a small investment!!!

- Downloading Unwanted Programs (PUPs) - Often when you download a program, one that you actually want, it may bring with it one or more unwanted programs. This may not be totally obvious until after the download has finished. It will manifest itself as programs that you may not recognize, that become obnoxious – asking you to back things up, or scanning for viruses, registry errors or driver updates - and then trying to sell you something. You may also notice new icons on your desktop that you don't remember putting there. Unwanted toolbars may appear in Internet Explorer and/or your home page may change. When you see these symptoms it is time for immediate action. There are three approaches: 1) you can do a System Restore to the date before these things appeared; 2) you can go to the Programs and Features in the Control Panel and manually remove these unwanted programs one by one; 3) You can run Malwarebytes AntiMalware and use it to remove most of these programs. The problem with approach #3 is that the symptom that the program created may not go away – e.g. changed home page. This means you may have some maintenance to do. Bottom line is that you should be very careful when you ask for a download. Check the name of the file being downloaded to make sure it looks like what you are asking for.

Note that in approach #2, above, it can be useful to sort the Programs List by "date installed". Then you can look for groups that have the same date. This usually means something significant happened on that date. It could be a good thing, such as the installation of a printer or it could signal a group of unwanted programs that came in on the coattails of another program.

- Having No Password Protection on your Wireless Network – Just about everyone who uses the Internet in their home has a router. The router provides for wireless Internet connection of your Computer(s), printers, tablets and smart phones. When you install a router, it comes pre-programmed with an SSID (broadcast name) and usually some hard-to-remember password, which is shown on the router's label.

During a router's installation it usually gives you a chance to alter the factory settings. A good practice is to change the SSID to something familiar, such as "SmithNetwork" and change the password to something easy to remember. I have found that a 10-digit phone number works very well as a password or WiFi key. Instead of using your current number, however, use a former number or a number of a family member. It should easy for you to remember but hard for someone else to guess.

All routers have a reset button. This sometimes requires a paper click to be inserted into the reset hole on the device. Be aware that resetting it clears the password and sets the SSID to the default - something like "Netgear1". This is a good thing to do if you forgot the password to the WiFi. However, if you leave it this way, you will have an open network that can be accessed by anyone within range - without a password. This is not a desirable situation. Even though those connected to your network really can't see into your computer, protecting your network is still a must. Who knows, those strangers could be "cyber criminals". Also with some older routers, too many devices connected can overburden it.

Also remember that if you do financial or other transactions that you want to be "secure", look for the https at the beginning of the address line. This stands for Hyper Text Transfer Protocol Secure. Make sure the "S" is there if you are going to do any banking or credit card purchase.

Dan Phelka (4/9/18)
623-535-7791

Final Thought: It has been a pleasure for me to be your facilitator again this year. Thank you for your attendance, interest and questions throughout the season. Having such a good turnout every week is very gratifying and motivating for me. I hope you enjoyed it as much as I enjoyed presenting the information to you. I think it's a tribute to you folks that you make learning about computers a high enough priority to spend a couple of hours out of your week at our meeting. Have a safe and pleasant summer and remember we start meeting again November 12, 2018.