The Rochester Computer Society, Inc.
a computer club open to everyone

MONITOR

Vol. 34, No. 1 January 2017

Next Meeting – Tuesday, January 10
Movie/Video Night
Learning to Use Facebook, by Hank Drayton
What is Patreon, by Leo Notenboom
Comparing Windows 10 to Windows 7

In This Issue

Founded 1982
www.rcsi.org
Rochester, NY

Member of apcug
An International Association of Technology & Computer User Groups

"Your Computer User Group of the Air", Saturdays from 12:00 pm to 2:00 pm with Nick Francesco, Dave Enright, and Steve Rae. Broadcasting on JAZZ 90.1 FM from Rochester, NY.
Call 966-JAZZ (585-966-5299) or 800-790-0415

The RCSI '**Monitor' newsletter** can be found in most public libraries in Monroe County. *Free* copies can also be found in the following computer stores: Microworx, Just Solutions, TSC Electronics, and Pod Computers. Digital copies may be obtained from **www.rcsi.org** or my cloud storage at **http://tinyurl.com/tonydel-rcsi-newsletters/**.

Some Past Presentations:
Protecting Your Identity
Keeping Mobile Devices Secure
Mobile Payments
Flash Drives-Not Just for Storage
Features, Mac OS X & Windows
Tablets, the Programs and Uses
Preview of Windows 10
Personal Finance Software
Amazing Browser Tips
Linux is Like Cars
Close up Photography

Special Interest Group

Linux Sig

The workshop is the **third Saturday of each month**, at Interlock Rochester, 1115 East Main St. www.interlockroc.org
Enter through door #7 on the end of building, near *Comics Etc* and Goodman St. Find 'Interlock' on the intercom directory to get buzzed in and go upstairs to suite #200. We have experts on hand to fix problems and answer questions about Linux and FOSS (free and open source software). Bring your system in so we can help you get the most out of it. Hope to see you there.

Free, online
Virtual Technology Conferences,
presented by APCUG
Saturdays from 1-5 pm, on
February 11, 2017
May 6, 2017
August 19, 2017
November 4, 2017

Ransomware - Protecting your ability to recover from an attack

By John Langill, Newsletter Editor
STPCC (Southern Tier Personal Computing Club)

A recent posting to Yahoo.com reminded me that the key element to recovering from a ransomware attack is to have a reliable system image backup. Most computer users — you among them, I'm sure — are aware of this and have diligently performed regular backups. Some may have chosen to back up their systems to a Cloud-based service for which, if their backup files are sufficiently large, they pay a monthly fee based on the storage capacity required. Others have preferred to keep things "close to the vest" and store their backup files on a local external hard-drive (never, ever store backup files on an internal hard drive) for which one with a three-terabyte capacity, for example, presently costs about $100.

I fall into the latter group.

Cost aside, both methods provide protection but also have their own particular drawbacks that are too often overlooked. What will happen, for instance, if some enterprising ransomware purveyor one day successfully manages to hijack (encrypt) all the client files that have been stored with the cloud-based service. Not possible, such services say. Well, that may be but just how sure of that are you really — or are they, for that matter? And, as sure as God made little green apples, you can bet that there is at least one someone somewhere trying to do just that.

The uncertainty of cloud-based services is what led me to rely on a USB-connected external hard-drive for storing my backup files; and I have been doing so for years with a blissful — and perhaps a false — sense of confidence that they would be secure and uncorrupted should they be needed. Ok, so what's the drawback in this method? The fact is that a ransomware attack will — along with all files stored on the internal hard-drives — also hijack the backup files stored on an external hard-drive unless the drive is either powered off or physically disconnected from the computer at the time of the attack. Not a problem, said I — my USB 3.0 external hard-drive is equipped with an On-Off switch and I power it ON only for the time it takes to create a backup.

There's one other precaution I take and that's to set my cable modem to "Stand by" mode to disrupt Internet traffic during the time that a backup is created; thereby assuring that my system and external hard drives will not be vulnerable to attack while a backup is in progress.

Accordingly, I considered the risk of the backup files becoming corrupted was minimal. And all was fine and dandy until I decided to swap a relatively low-capacity external hard-drive over to my laptop PC and to install two larger capacity USB 3.0 hard-drives on the desktop PC. The problem with doing this was that the newer drives did not have On-Off switches; and rummaging around behind my desktop PC (which, despite what it's called, is actually located under a desk) to connect and disconnect the USB cables from either the drives themselves or the PC was a real pain — it's a rats-nest back there, as many will probably know.

My solution: I purchased a powered 4-port USB 3.0 hub (under $20) specifically for use with the two newly installed external hard-drives. Now, all I have to do is connect/disconnect the one cable between the hub and the PC. Fortunately, a USB 3.0 port on the front of my PC makes this convenient and easy. The only thing I need to be careful of is making sure that the external hard-drives have both completed their respective operations before disconnecting the hub from the PC which, by the way, also removes power to the drives (i.e., acts as a defacto power On-Off switch).

Of course, if you use just one external hard-drive to store your backup files, and it has an accessible On-Off switch, you've no problem. Even if the drive doesn't have an ON-Off switch it's likely that restricting Internet access to it will be simply a matter of disconnecting the USB cable from the back of the device and that should not be much of a problem either.

Why do I have two external hard-drives? One is used to directly store backup files — which by the way, are always full system image backups — as they are created. The other serves to archive copies of previously created backups; that is, to back up my backups.

OK, so I'm paranoid when it comes to protecting my system image backups — it's not the worst of my faults. Admittedly, over the past 25 years or so, I can recall only once having to restore a system from a backup. I consider myself lucky on that score. But, with the chance of suffering a malicious attack rapidly increasing at the rate at which it is in today's world — and the risk will only get worse with time — I'd rather be overly cautious than suffer the consequences that could result from a lack of vigilance.

From the June 2016 issue, Rare Bits,
http://www.pageorama.com/?=stpcc1979jlangil1@stny.rr.com

File Encryption

By Dick Maybach, Member
Brookdale Computer Users' Group, NJ

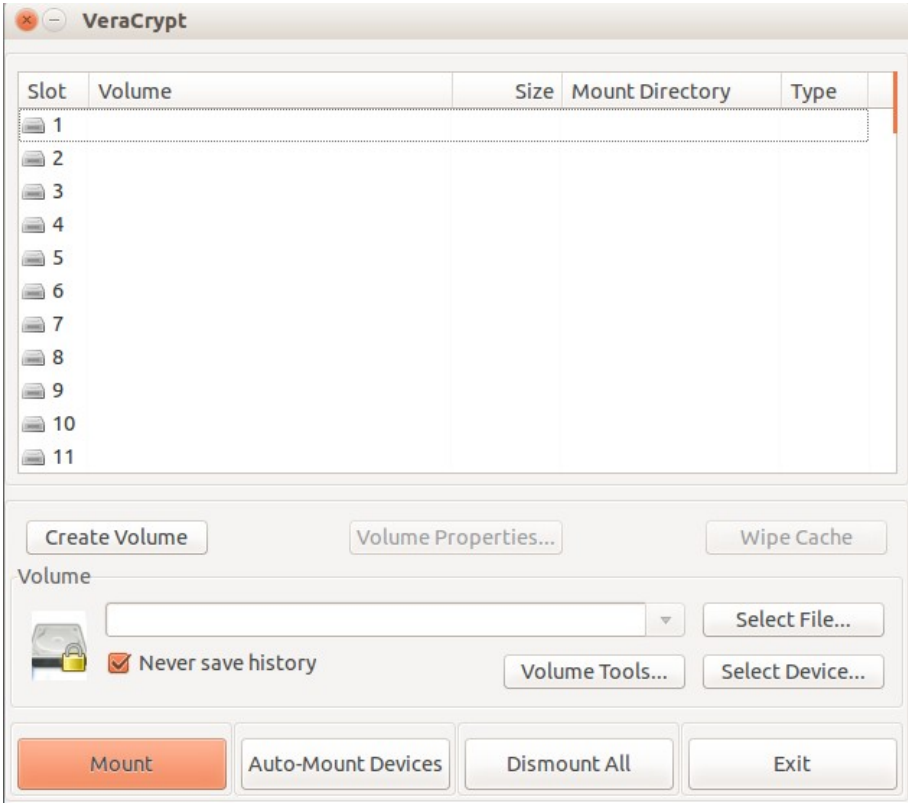
I wrote an article on file encryption that appeared in the August 2014 Bytes, available at http://www.bcug.com. While I was writing, TrueCrypt, a popular tool for this task, was discontinued by its anonymous developers amid speculation that it had been compromised. As a result, I recommended using GnuPG for file encryption. This is still valid advice, but two successors to TrueCrypt have since appeared, CipherShed, http://ciphershed.org/, and VeraCrypt, http://veracrypt.codeplex.com/. Both can read files encrypted with TrueCrypt, but only CipherShed can write in this format. If compatibility with TrueCrypt files is important, you should use CipherShed, otherwise use VeraCrypt, which has somewhat improved security and appears to be the more active project. The remainder of this article will discuss only VeraCrypt, which is available at the CodePlex site given above. You can also get from SourceForge, but this site has been known to include malware with its downloads. SourceForge now has new owners and may again be reliable, but why take a chance?

You may be using GnuPG with its public/private key method to encrypt your e-mail, and as I discussed in my previous article, you can also use it for file encryption. The advantages of doing this are fewer keys to manage and having only one encryption program. However, you may find some features of VeraCrypt useful, and its single-key encryption can be more secure than the GnuPG's public/private type, provided you use a strong password. You should view encryption as a means of reducing, not eliminating risk. If the NSA really wants to decrypt your file, it most likely can.

VeraCrypt creates and maintains on-the-fly-encrypted volumes, and data is automatically encrypted before it is saved. No data stored in an encrypted volume can be read without using the correct password. VeraCrypt stores decrypted data only in RAM; it stores only encrypted data on a disk. Even when the volume is mounted, data on the disk remains encrypted. When you restart or turn off your computer, the volume will be dismounted and files stored in it will be encrypted. To read them, you have to mount the volume with VeraCrypt and provide the correct password.

You can download a 162-page manual from VeraCrypt's Website, but I won't try to cover that here. Instead, I'll walk through establishing and

using an encrypted volume to show how easy this is. The screen-shots are from a Linux machine, but the differences for other operating systems are quite minor. Screen 1 shows VeraCrypt's opening screen. (On Windows the slots column would be labeled “Drive” and the rows would be labeled D:, E:, etc.) Your first step will be to create an encrypted volume, which you do by selecting a slot and clicking the *Create Volume* button.

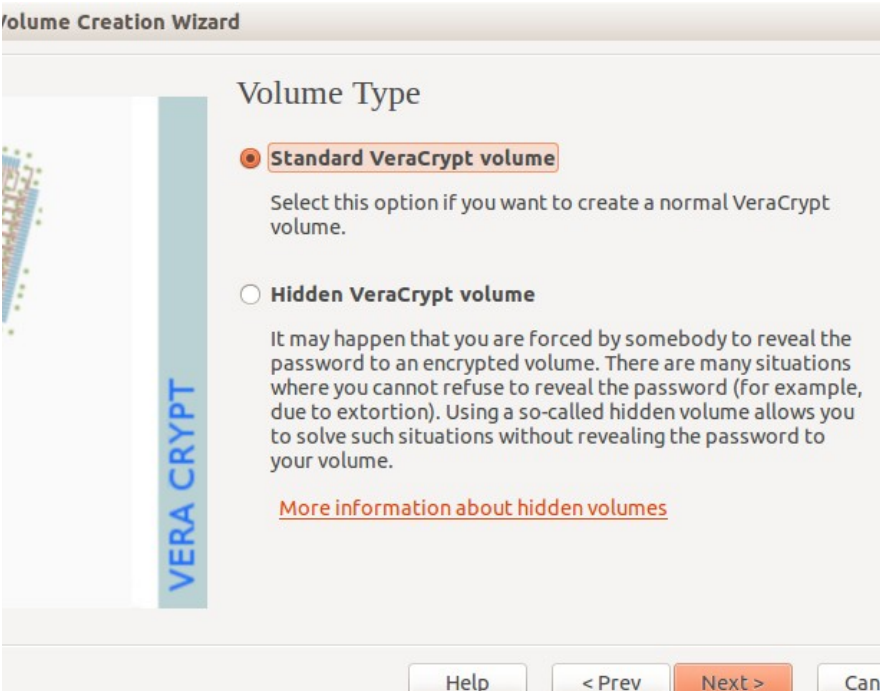


Screen 1. VeraCrypt Main Window

You will then see Screen 2. Select the upper option to create an encrypted volume as a file and the lower to encrypt an entire external device, such as a memory stick. Then click *Next* to continue.

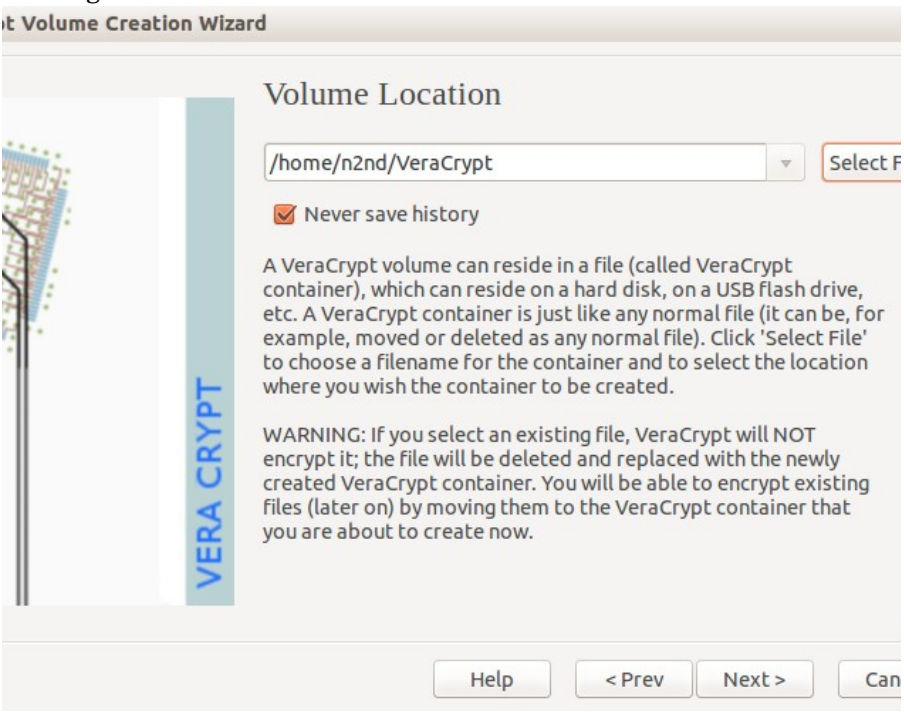
Screen 2. Volume Creation

On Screen, 3 you choose whether the encrypted volume will be visible or hidden. The first choice is by far more common.



Screen 3. Volume Type

You next specify where to store the volume, Screen 4. Initially the location window will be empty. Just click on *Select File...*, choose its directory, and enter a filename. Important – be sure to choose a filename different from that of an existing file in the chosen directory, or the existing file will be deleted!

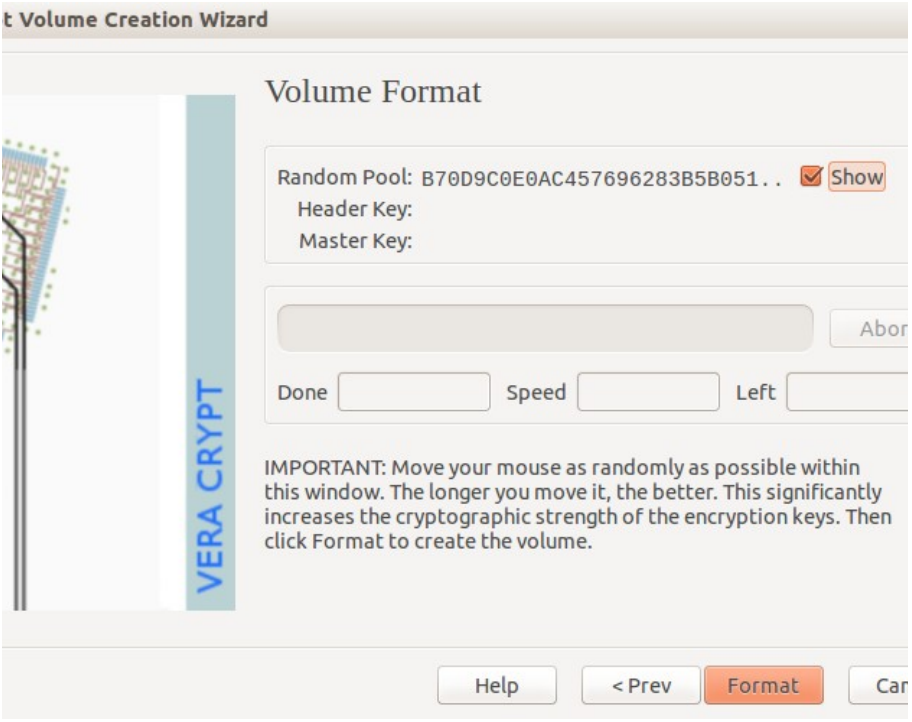


Screen 4. Volume Location

You will then go through screens where you select an encryption method (the default, AES, is fine), a volume size, and a password. Give some thought to the size. If you choose 100 Mbytes, the volume will occupy that much room on your disk, even though it contains only a 1-kbyte file. But if you choose 1 Mbyte and have 10 Mbytes of data, you will have to create another volume with enough capacity for your data. Password choice is also important. For example, if the volume will be stored in the cloud and contains sensitive data, such as passwords to your on-line banking account, you should use a long and obscure password, which you safeguard, perhaps in a password manager such as KeePassX. The password screen also offers additional safeguards, such as key files; see the VeraCrypt manual for more information. You then select a file-system, probably FAT or NTFS for Windows users.

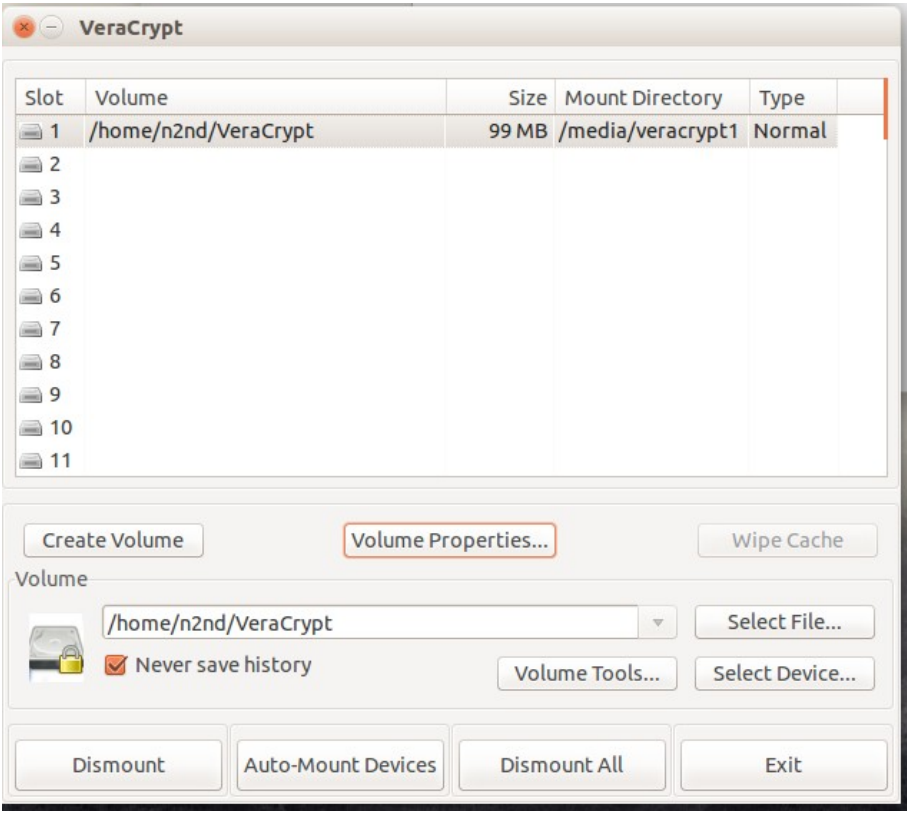
Finally, you'll see Screen 5. Before you click the *Format* button, move

the cursor randomly around the screen, which will increase the strength of the encryption. When you click *Format* VeraCrypt will create an empty volume with the name and location you specified previously.



Screen 5. Format Volume

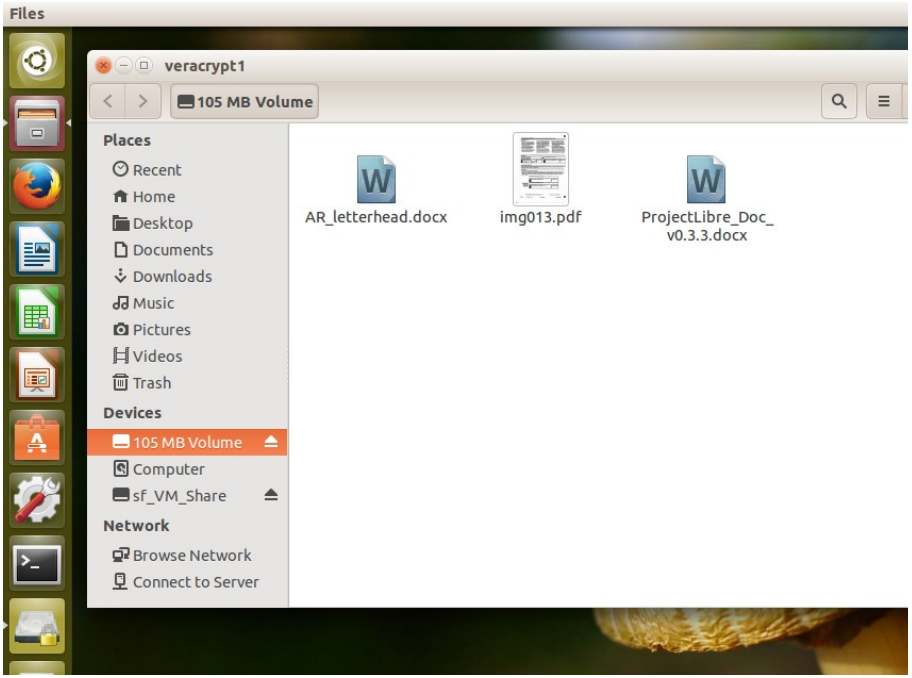
Before you can use the volume, you must mount it. In the VeraCrypt opening screen (Screen 1) click *Select File*, choose the volume you created, click the *Mount* button, and enter its password. (Depending on your operating system and permissions, you may also be asked for the administrator password.) Screen 6 shows the result, in this case, the volume is located at home/n2nd/VeraCrypt and is assigned to Slot 1. (On a Windows PC, the column would be labeled “Drive” and you would see the usual drive letters.) I find it convenient to minimize the VeraCrypt window rather than exit the program, so I can recall it quickly to dismount the volume. This isn't really necessary, as it would be dismounted when you log off or power down.



Screen 6. Volume Mounted.

This discussion has been on using a file as a secure volume, but the procedure for using an entire device, such as a USB memory stick or hard drive is the same.

Screen 7 shows the Linux desktop with the file manager open. The encrypted volume is accessed the same as a normal directory. You can copy and paste files to and from it as usual. Linux users should note the mount directory in Screen 6, which shows where to access files from the command line.



Screen 7. Linux File Manager Accessing a VeraCrypt Volume.

You might be wondering what could possible require a 162-page manual. Although its basic use is quite straight-forward, VeraCrypt has many features, which can make it more convenient and more secure. If your information is sensitive and if the encrypted volume could be accessed by others, for example if it will be stored in the cloud, on a publicly-accessible PC, or a laptop with which you travel, you will want to at least scan the entire manual.

Although both VeraCrypt and GnuPG protect your data using encryption, they do it in quite different ways, GnuPG by encrypting single files and VeraCrypt by creating encrypted volumes. If you want to e-mail a friend some private information, GnuPG will be simpler. and it avoids the issue of securely sending a password. If you have several files containing sensitive data that will stay on your computer or on a memory stick, then creating a secure container with VeraCrypt is preferred. If you will keep the secure container in the cloud or sync it among several computers, its size is important. This is because file sharing is usually done with entire files. If you change one small file in a large encrypted volume, the entire volume must be exchanged, and this probably won't happen until you dismount it. Thus, you must take care to dismount the volume, but stay logged on until the syncing is complete. This isn't an

issue with memory sticks, since these are updated incrementally as you change the volume's contents.

Finally, VeraCrypt stresses using hidden encrypted volumes to establish “plausible deniability,” which lets you deny that your computer contains any encrypted data. You shouldn't try to use this casually, for example to bring pirate music or movies into the country, as it could place you in serious conflict with our or another country's authorities.

From the July 2016 issue, BUG Bytes, www.bcug.com, n2nd@att.net.

Ask Leo !

By Leo Notenboom, https://askleo.com/
Making Technology Work For Everyone

Should I Accept My Security Software's Recommendation of What to Remove?

Should you trust your security software to make the right recommendations? Typically, yes, as long as you're using reputable software.

//

I downloaded the Malwarebytes you suggested and did a scan. It showed more than 330 things which it asked whether to remove. Do I just accept that these are things that should be removed? The things recommended for removal are listed below. Some of the sentences include microsoft explorer, lenovo browser guard, etc, which when I look at them I am uncertain about deleting because I do not know if I am deleting something that’s important.

Do I just delete whatever Malwarebytes asks to delete every time it makes such suggestions?

<~300 entries, mostly registry-related, snipped>

//

This is one of those questions we never think about until someone asks. What we’re really asking is, “Do I trust my security software to make the right recommendations?”

And the answer, as it is so many times, is: it depends.

Protecting yourself

The concern, of course, is that your security software might mistakenly

recommend that something important be deleted. It's not an unfounded fear. While it doesn't happen often, it has happened.

The good news is, it's really easy to protect yourself. You can probably already guess what action might be involved.

If there's ever even the slightest doubt, *back up first*. And by "back up", I mean a full system image backup of your entire system drive (typically C:), and ideally the entire hard disk on which it resides. If you're doing daily image backups, as I so often recommend, you're already ready.

The issue is, we don't know ahead of time what might be removed, or what might be important. That's why we're asking the question in the first place. A system image makes no assumptions. It saves *everything*.

If, after allowing the anti-malware software to do its job, you find something is broken, you simply restore the image and get on with your life — nothing lost except the time to perform the operations.

Trustworthy software is worthy of trust

I realize this is a kind of chicken-and-egg statement, but there's a reason computer folks such as myself have recommendations: we've come to trust the software we recommend. In the case of anti-malware and security tools, that trust encompasses at least two distinct considerations:

1. The security software will prevent as much malicious software as possible from doing harm.
2. The security software will itself do no harm.

It's the second one we're concerned about today. Security software might cause performance impacts or do things like prevent some email or files from being downloaded by intrusive scanning, but at worst, they can break *the system* if they delete or quarantine the wrong thing in the name of "security".

I try not to recommend software that has a history of doing that.

And yes, Malwarebytes remains a recommendation.

"Yes" is easy when you trust

Given that I trust Malwarebytes, my default answer is easy.

Yes: when it recommends something be deleted, it's probably safe to delete it.

In this case, the list of around 300 registry entries our questioner shared

were all flagged as relating to PUPS, or "potentially unwanted programs". There's rarely any "potential" about it; you don't want them, and Malwarebytes Anti-malware is a tool I often recommend for its ability to ferret out and remove exactly those types of programs.
In your shoes, I'd say "Yes", and I'd say "Yes" to whatever Malwarebytes identifies in the future.

Why do you have so many PUPs to begin with?
First, let's be clear about at least one thing, lest you really panic: 300 discoveries by a tool like Malwarebytes does not mean you have 300 separate PUPs, or pieces of malware. My guess is you have maybe half a dozen or so. Each PUP can be responsible for any number of traces that tools like Malwarebytes identify individually and remove.
But we're still left with the question: why do you have even those six? And if Malwarebytes is repeatedly identifying things after having run, why are things returning?
In my opinion, once security software cleans your system, the real lesson to be learned here is to stop installing software that causes PUPs to be installed, or perhaps visiting sites that cause questionable software to be downloaded and installed.
I have no way to know what those might be in any specific case, but things like accepting the default installations of downloaded software is by far the leading cause of PUPs and other malicious software. The solution? Always choose "custom install" instead, and be careful to decline any software you didn't ask for.
In general, be more vigilant and discerning. PUPs in particular usually install with your consent, and your consent can often be implied when you take shortcuts like a default installation, or fail to read all the installation options presented.

When IBM introduced magnetic hard drives in the 1950s, the price was so astronomical that companies rented them by the month; the rental price of their first hard drive was $3,200 a month (equivalent to about $180,000 today). The first IBM drive was approximately the size of two medium-sized refrigerators and stored five million six-bit characters (3.75 megabytes), on a stack of 50 disks.

Virtual Reality & Augmented Reality Explained

By Sandy Berger, Compu-KISS

If you want to be up-to-date in the high tech world you need to understand the terms VR and AR. They are both amazing technologies that are quickly moving into our everyday world.

Preface

It has always been a joy to be transported to a different time and place. The Greeks, Romans, and American Indians did this for their listeners by telling wonderful stories. These story tellers transported their listeners to alternative realities. With radio we were immersed in tales like Fibber McGee and Molly where we could listen and vividly imagine being right in the McGee's home. Then came movies, television, and gaming devices. These devices totally immersed us in their stories.

Now we have moved on even farther into other realities and amplified realities with two newer technologies: Virtual Reality (VR) and Augmented Reality (AR).

Virtual Reality Explained

Virtual Reality replicates an environment that lets you see and feel like you are in another world. This is generally done by wearing goggles which put a screen in front of your eyes to show you that new world. Some of these VR devices have built-in audio and vibrations and other haptic feedback that help to make the new world feel quite real.

Many have immersive 360 degree visual capabilities so you are completely surrounded by the new world. Often you can interact with that new world as when you might play a VR game. This new storytelling technique is totally immersive since you are completely pulled into the world inside the headset.

Dedicated VR devices started reaching the market in 2016. Samsung and Oculus have recently released their first everyday consumer product, the Samsung Gear VR headset. At $99 it is well-priced, but must be paired with a newer Samsung Galaxy smartphone to make it work. Other VR devices like the Oculus Rift and the HTC Vive start at $599 and require a powerful PC to work. Sony will soon release their PlayStation VR at $399.

Augmented Reality

Augmented Reality is another way to look at a different world. Instead of replacing the current reality with an alternate reality as VR does, AR

adds to our current reality. So with AR, you can still see the real world around you, but certain things in your world are augmented. With AR, information about the real environment and its objects is overlaid on the real world. For instance, a nurse wearing a pair of AR glasses would be able to see everything in the room exactly as it really is. However, when he or she is ready to insert an IV into your arm, the veins in your arms would be totally visible.

AR technology is sometimes accomplished with goggles, like VR, but there are also AR applications that use lightweight glasses or partial glasses. There are also small handheld AR displays, digital AR projectors, and even contact lenses that project AR information. Several companies, including Google, are working on lasers that send information directly to the eyes.

Microsoft is working on a HoloLens AR headset that will work with Windows 10. Google is still working on their Google Glass project which will now focus on the workplace.

With AR you can interact with it through gaze, voice, and/or hand motions. If you saw the movie Minority Report and remember Tom Cruise moving information around in the air you have seen an accurate depiction of an augmented reality device.
When Minority Report came out in 2002, it was very futuristic. Now that future is already here.

From the newsletter of Compu-KISS, www.compukiss.com, Sandy@compukiss.com

Data Privacy Day (known in Europe as Data Protection Day), is an international holiday that occurs every **January 28**th. The purpose of Data Privacy Day (DPD) is to raise awareness and promote privacy and data protection best practices. It is currently observed in the United States, Canada, and 47 European countries. DPD began in the United States and Canada in January 2008 as an extension of the Data Protection Day celebration in Europe. DPD commemorates the January 28, 1981, signing of Convention 108, the first legally binding international treaty dealing with privacy and data protection. DPD is now a celebration for everyone, observed annually on January 28. The Internet is a powerful and useful tool, but in the same way that you shouldn't drive without buckling your seat belt or ride a bike without a helmet, you shouldn't venture online without taking some basic precautions. Check out https://staysafeonline.org/.

* * * SOFTWARE & COMPUTER TIPS * * *

Synchronize mail, contacts, calendar, notes on all your devices

By John King, SIG Leader/Instructor, Intro to Computing Class
Golden Gate Computer Society

Many people have more than one computer these days: a desktop computer at home, a notebook or tablet for when you are away, and a smartphone. You can use each of these devices to:

- Send and receive e-mail.
- Check and record information about your contacts, the people you interact with.
- Add or check appointments on your calendar.
- Make or consult to-do lists or notes.

However, for them all to be fully useful, you have to be able to access the same e-mails, contact information, calendar appointments, and notes on every device so they are always available wherever you are.

The Windows 10 Mail, People, Calendar, and OneNote apps make synchronizing this information on your computers and phone easy, free,

and automatic. All you have to do is use the same Microsoft account (a Microsoft e-mail address and password) to log onto all your Windows 10 devices and be connected to the Internet. You can receive an e-mail on your desktop computer and reply on your notebook or phone. If you delete the message on your tablet, it will be deleted on all your devices. You also can add an appointment to your calendar on your phone, and it will appear on your calendar on your desktop and notebook computer. Add a new contact in People on your desktop computer, and it will be with you on your notebook, tablet, and phone.

In addition, apps for Microsoft Mail, People, Calendar and OneNote are available for Android phones, iPhones, and iPads, so you can stay in sync on those devices also. Windows 10 phones have all these apps, but few Windows 10 phones are in service.

You can even make the Microsoft Office version of Outlook 2016 synchronize your mail, contacts, and calendar on all the Windows 10 computers, notebooks, and tablets where you install it. To accomplish this, you must log onto each device with the same Microsoft account and make your Microsoft e-mail account the first e-mail account you add to Outlook. This makes Microsoft Office 365 Home for five computers a good deal if you prefer the Outlook 2016 interface for mail, contacts, and calendar.

An important requirement makes this syncing work. The first email account in the Mail app must be the Microsoft e-mail account that you will use to log onto all the devices you want to keep in sync. This first e-mail account controls syncing and cannot be changed or deleted. No Delete option exists for it. Here's the key point: The e-mail address and password that you use when you initially set up Windows 10 becomes the first e-mail address in Mail. Therefore, you must use the same Microsoft e-mail address and password (the same Microsoft account) when you initially set up Windows 10 on each computer and phone on which you want to sync your Mail, People Calendar, and OneNote apps.
For these reasons and more, you should have a Microsoft e-mail address and password (a Microsoft account) before you set up a new Windows 10 computer or upgrade to Windows 10.

To create your Microsoft account, go to www.outlook.com and sign up for an e-mail account. If you already have a Hotmail, MSN, or outlook.com e-mail account, you can use that. Use this e-mail address and password, your Microsoft account, when you set up and first logon to all your Windows 10 devices. You have nothing to lose and a lot to gain by doing this. If you change your mind and do not want to use your Microsoft account to log onto your computer, you can change to a local

account at any time.

From the June 2016 issue, GGCS newsletter, www.ggcs.org, john.king@ggcs.org.

DO YOU HAVE AN IDEA THAT YOU WOULD LIKE TO SHARE?

Monthly club 'planning meetings', are held on the **first Tuesday** of each month, beginning at 7:00 pm, and are currently held at St John's Meadows, in the Briarwood building foyer. Any member is welcome to attend and help develop ideas for running the club, as well as help decide on future presentations for our general meetings.

SPEAKING OF PRESENTATIONS, it is becoming more difficult to find presenters for our monthly general meetings. During the past year, we have had presentations given by five members, one guest speaker, and five remote programs, from various APCUG speakers from around the country, using Skype. Anyone, that would like to share something with the club, is welcome to do so. This can be any topic from a piece of software that you like, or possibly a tech device that you recently bought, or simply something that you find interesting and might like to share it with other club members. A topic of interest can be presented anywhere from five minutes to an hour or so. I am downloading some short videos that can be used as fillers for our meetings. Requests to do a presentation, may be sent to the newsletter editor.

* * * * * * REVIEWS * * * * * *

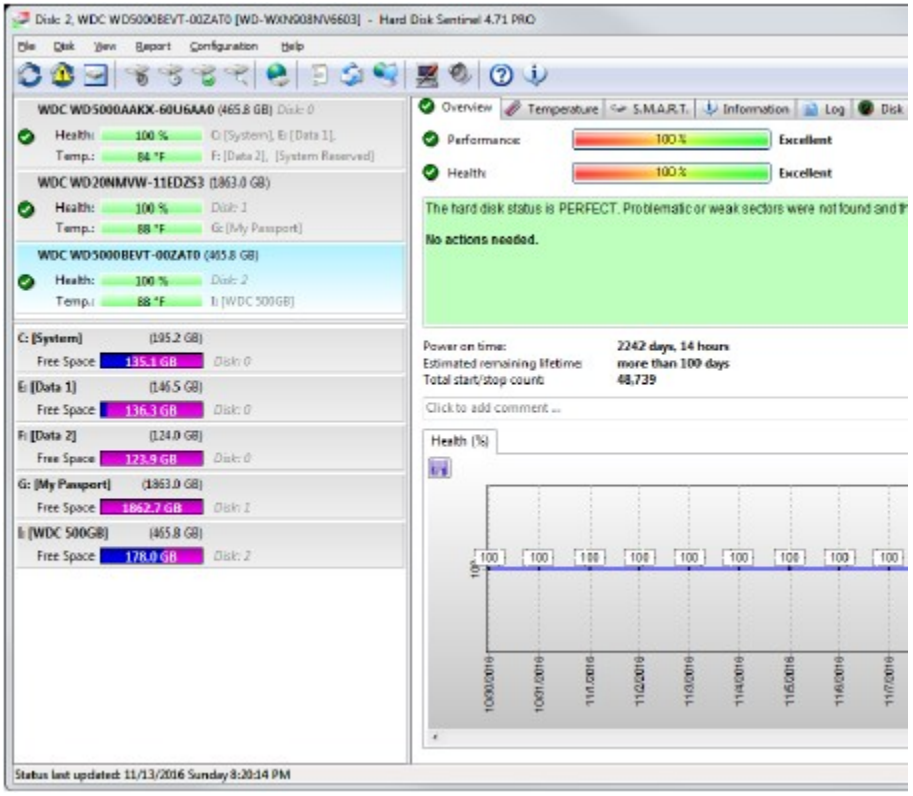
Monitor and Protect Your Precious Data With Hard Drive Sentinel

Review by Gabe Goldberg, APCUG Representative
Potomac Area Technology and Computer Society
APCUG Advisor, Region 2
ggoldberg@apcug.org

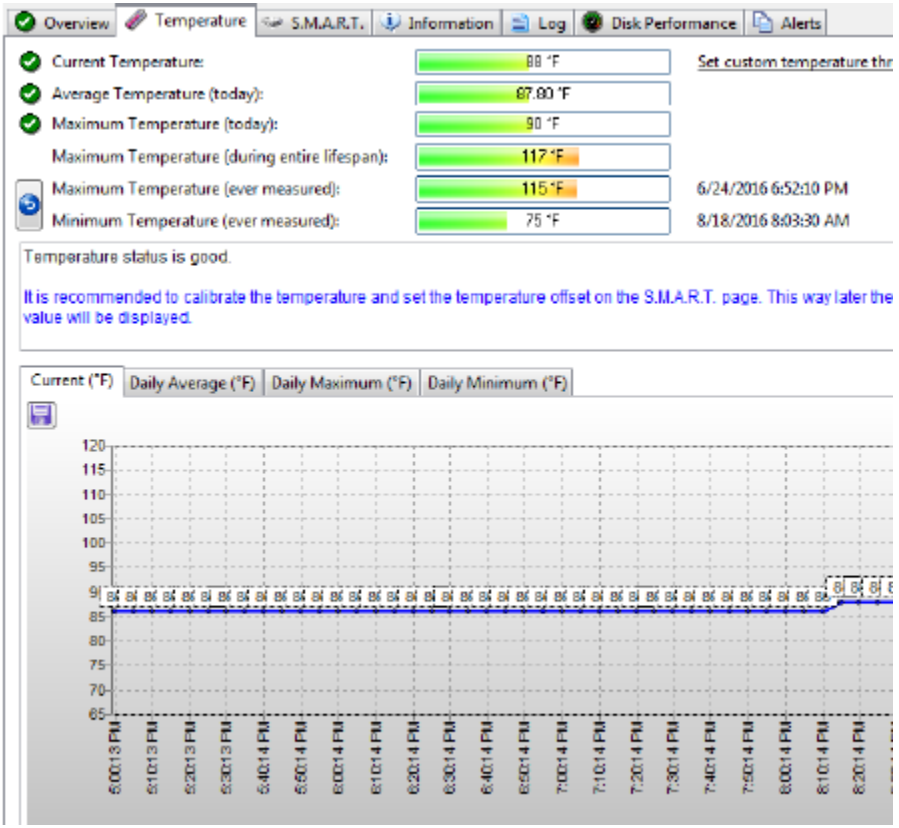
Storage devices are unappreciated workhorses: spinning hard drives and immobile memory chips reliably and rapidly save and fetch your data, year after year. Until – uh oh, something's wrong and where's my data?!

I've been running HD Sentinel (HDS – http://www.harddisksentinel.com/) for about five months on two computers -- my desktop system and my wife's laptop. It's a powerful tool for monitoring storage device health, and for learning more about how they work than you likely imagined possible. While the tool's website focuses on simple hard drives, HD Sentinel also supports other storage devices: SSDs, SSHD (hybrid drives), memory cards and thumb drives (where available), tape drives, and RAID controllers. On both my systems, I've configured it to show icons for each connected hard drive: one on the laptop and three (one internal, two external) on my system. By default, the icon shows current disk temperature (with green/orange/red visually indicating status); mousing over icons displays a summary of disk health and clicking opens the comprehensive display.

Overview Display



Temperature Display

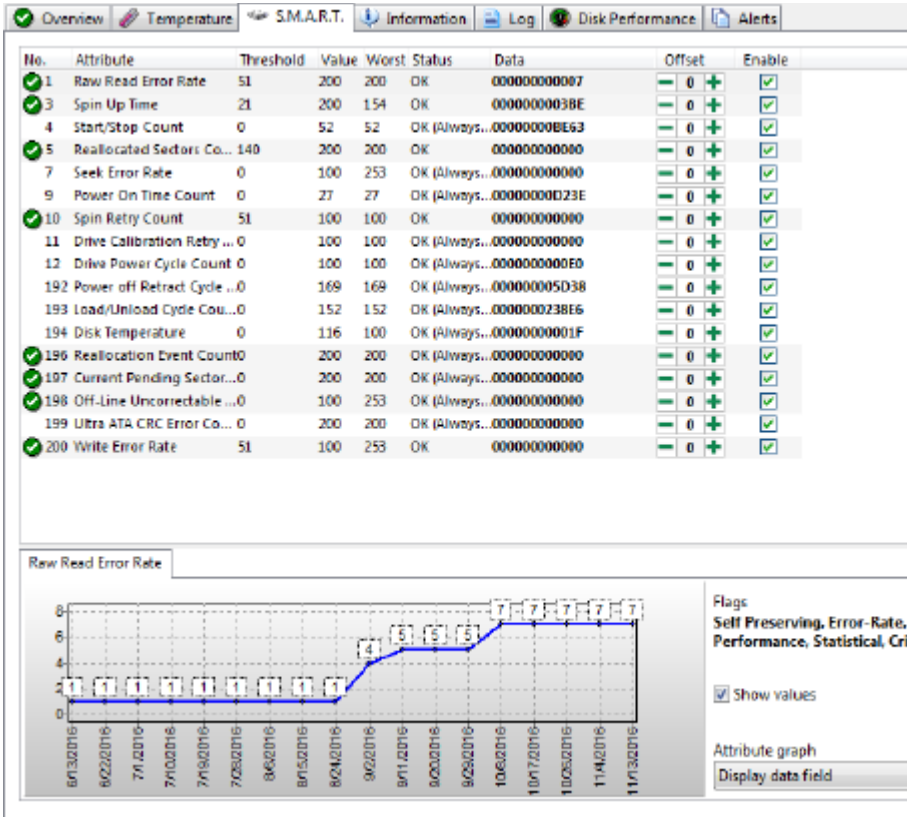


HDS can be used for maintaining one's at-a-glance comfort level (I like all my drives described, "The hard disk status is PERFECT”). Problematic or weak sectors were not found and there are no spin up or data transfer errors. No actions needed.") and for drilling into drive history (temperature patterns, various sorts of errors, performance information, and more.

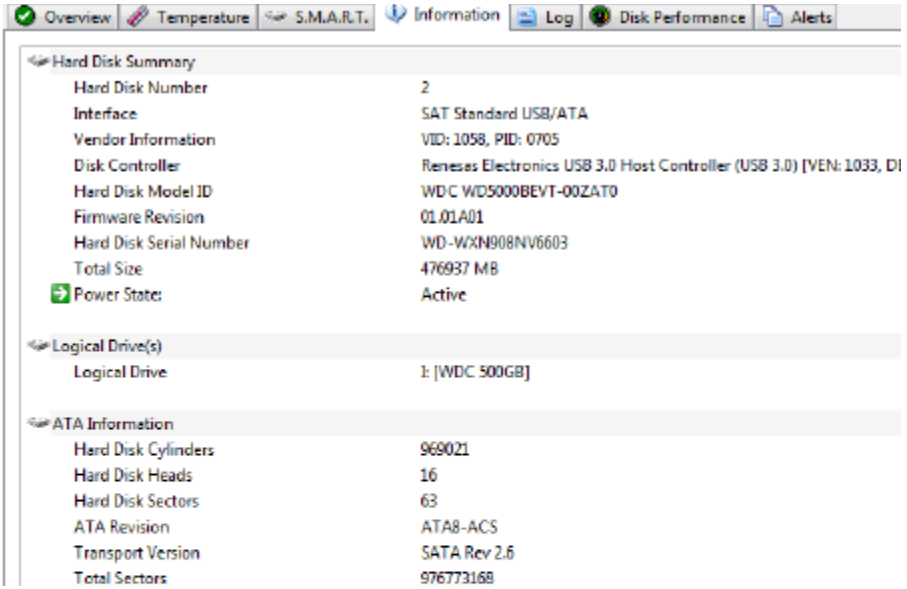
For many years, hard drives have included S.M.A.R.T. technology -- https://en.wikipedia.org/wiki/S.M.A.R.T. -- described as "a monitoring system included in computer hard disk drives (HDDs) and solid-state

drives that detects and reports on various indicators of drive reliability, with the intent of enabling the anticipation of hardware failures". But annoyingly, most operating systems don't easily make that information -- and recommendations or warnings – available. At least twice, based on such warnings, I've been able to replace drives in the process of failing before any data was at risk. So, I'm a firm believer in having software running to disclose drive information while there's time to act on it.

S.M.A.R.T Display



Information Display



HDS is developed/maintained/supported by a dedicated developer who's passionate about his product and brilliant at both tech support and answering questions about product usage. It's available at a bargain price for lifetime license (no renewal or subscription costs, free version upgrades) and a worthwhile investment in both knowledge and comfort.

* * * * * * RANDOM TIDBITS * * * * * *

Apple just removed hundreds of fake shopping apps from the App Store

By Caitlin McGarry, staff writer, Macworld

Counterfeit apps masquerading as huge brands like Zappos and Nordstrom are sneaking into the iOS App Store.

Just in time for the holiday shopping season, the iOS App Store is seeing a deluge of fake shopping apps branding themselves with designer names in hopes of trapping gullible buyers. Apple is now stepping in to remove the counterfeit apps, which are sneaking in by changing the content after Apple's approval or by resubmitting apps under different names and

credentials after being outed as fraudulent.

After reports of apps using reputable companies' names to shill their fake wares in the App Store surfaced in the *New York Times* and *New York Post*, Apple removed hundreds of offenders. But hucksters keep coming back: The *Times* found that an app called Overstock Inc. was trying to convince shoppers that it was Overstock.com by selling clothes and Ugg boots. Apple killed the app, only to see it return the next day, because sketchy developers are finding new ways to bypass the company's traditionally tough app review process.

But the company is doing its best to crack down on developers who use existing brands' names to submit fake apps, an Apple spokesperson told the *Times*.

"We strive to offer customers the best experience possible, and we take their security very seriously," said Apple's Tom Neumayr. "We've set up ways for customers and developers to flag fraudulent or suspicious apps, which we promptly investigate to ensure the App Store is safe and secure. We've removed these offending apps and will continue to be vigilant about looking for apps that might put our users at risk."

Shopper beware

So what's the harm of installing a fake app? If you try to buy a product, at best you'll be frustrated by app crashes or annoying pop-up ads. At worst, you'll hand over your credit card info to a sketchy company and never receive the item you ordered.

How to tell if a retail app is legit: How many reviews does it have? How many previous versions have been released? Does the language sound like it was written by an adult professional with a good grasp of English? If any of the above seem suspect, go to the store's website and see if you can find an App Store link directly from the source.

Excerpt from www.macworld.com, November 7, 2016. Permission to reprint this article was not obtained.

December's presentation of 'Free, and Alternatives to Free, Software' presented (via Skype) by John Kennedy of the East-Central Ohio Technology Users Group was a hit. I make this statement by observing all the note taking that was going on during the meeting. Fortunately, John has been kind enough to give us a pdf copy of the slides. I put a copy on my cloud storage at 'www.tinyurl.com/tonydel-rcsi-newsletters'. Later, the same slides will appear on our club website.

In a nutshell, for remote tech assistance, John prefers Teamviewer (using Skype for audio) vs GoToMyPc or LogMeIn. LibreOffice is a very good choice for a Microsoft compatible office suite. Additional online cloud suites are Google Docs, Office Web, and Open365. Check through the slides to find PDF readers and editors, browsers, screen capture software, anti virus selections, DVD burners, firewalls, backup programs, etc. I have used many of the programs for years, but John mentioned quite a few that I may have heard of, but wasn't sure if they were any good. He has saved us a lot of trouble, by testing out many choices and giving us his opinion as to what works and which he feels are good choices. Please feel free to contact John with questions, comments, suggestions or even better -- more free software that you've found: lccs.freejohn@gmail.com.

Rochester Computer Society, Inc.
Membership Form, *please print*

___ New Member ___ Renewal

Dues are $35 per year for active membership, $25 for full-time high school/college students or associate members (available to those who live more than 25 miles from Rochester or who do not drive at night).
Separate and bring to a meeting or mail this section, along with a check to: RCSI, 2 Bambi Lane, Rochester, NY 14624

Name _____

Address _____

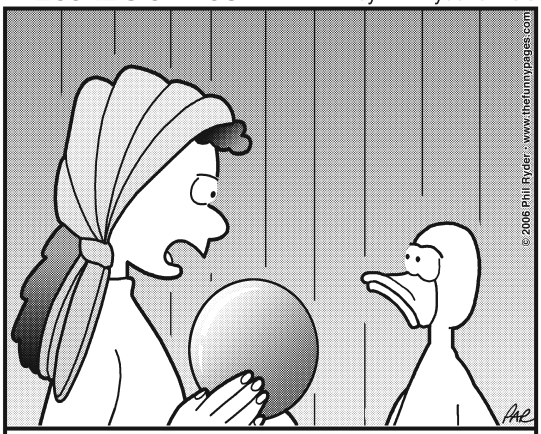
City _____ State _____ Zip _____

Phone _____ Email _____

Website _____

_____ Please, do not publish my address, phone number, or e-mail

THE JOKE'S ON YOU by Phil Ryder & **YOU**



"You've been cursed! To remove it, lie in my oven for 2 hours at 350 degrees."

- Frank Monaco • Coconut Creek, FL

Some benefits of membership:

Informative monthly meetings	Topical speakers
Question periods, solve user problems	Software help
Door prizes and giveaways	Free want ads
Monthly newsletter	

You use a computer at: ___ home ___ work

You consider yourself a: ___ novice ___ beginner ___ competent ___ expert

You are joining to: ___ learn about computers ___ get help with problems ___ learn about software ___ share your expertise

Can you volunteer for one of the many small jobs that keep the group going? ___ Yes ___ No

Would you be willing to help others use programs that you are familiar with? ___ Yes ___ No

What are some of your topics of interest, that we might use in a future presentation?

RCSI Officers

Pres: Steve Staub 429-9877
srstaub1@rochester.rr.com
VP: Mark S. Lawson . . . 544-5377
mslawson51@peoplepc.com
Treas: Dennis P. McMahon
denmac733@gmail.com
. 235-1260
Secretary: www.rcsi.org

Board Members at Large

Jan Rothfuss 347-6020
jan_rothfuss@hotmail.com, 9/19
Tony Dellelo 734-6149
tonydel@techie.com, 9/18
Bob Avery 385-4491
webmaster@rcsi.org, 9/17

Standing Committees

Membership: . . . . . Steve Staub
Monitor editors: . . . . Tony Dellelo
Sally Springett, 1936-2016
Linux SIG: . . . Carl Schmidtmann
unixgeek@faultline.com
Webmaster: . . . . . Bob Avery
Programs: . . . . . Tony Dellelo

Planning Meeting

Held on 1st Tuesday of each month at 7 pm, at St. John's Meadows, Briarwood building.

Newsletter Printing

The December newsletter was printed at St John's/Chestnut Court with the help of Don Wilder (computer and printer operator). *We will try and print on the 1st or 2nd* ***Thursday morning****, following the monthly meeting.*

Computer Recycling

Some Residential Drop off Locations: **Call first**, to find out what is accepted, especially for 'tube type' tvs or monitors.

Goodwill Industries of the Finger Lakes:
885 Long Pond Road (Greece)
376 Jefferson Road (Henrietta)
1807 Nathaniel Poole Trail (Brockport)
1200 Fairport Road (Fairport)
2 Commerce Drive (Victor)

Society of St Vincent DePaul,
1754 Norton Street (Rochester)

Amvets Thrift Store,
400 Jefferson Road (Henrietta)

Sunnking electronic waste collection event, on Saturday, January 28, from 9:30 to 1:30 pm, and sponsored by Senator Gallivan – East Aurora, NY, at the Parkdale Elementry School,
East Aurora, NY.

Our Meeting Place

St John's Meadows at Johnsarbor Drive, is on the left, past Clinton Avenue, when going West on Elmwood Ave. The opening in the white fence is Johnsarbor Drive. At the 'T', turn right. The meeting is in the first building on the left – **Briarwood**.

6:30 Help's Half Hour
7:00 Business
7:15 Main Presentation
our meetings end between 8:30 and 9:00 pm

Our meeting place can change. Please check our website before each meeting. **www.rcsi.org**

NONPROFIT ORG
US Postage
PAID
Rochester, NY
Permit No. 1537

See your address label for your membership EXPIRATION DATE!

CHANGE SERVICE REQUESTED

Monitor
Rochester Computer Society, Inc.
2 Bambi Lane
Rochester, NY 14624