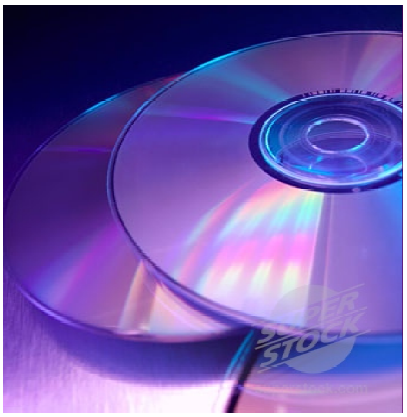
TOGGLE

THE MICROCOMPUTER TURN (ON)

MONTHLY NEWSLETTER FOR TACOMA-SEATTLE AREA MICROCOMPUTERUSERS

Volume 33 Number 4 September 2012 Issue #352

IN THIS ISSUE



UPDATE

Communications

In *Copyleft* the author discusses the state of the free public software movement, which started in the 1980s and continues in various Linux versions and elsewhere.

In *Power Line Networking* the author discusses the various ways that the internet access may be distributed throughout your home, including wired, wireless and power line connections. Pragraphs include *How Power-line networking works, The good and bad of Power-line networking, Security of data,* and *Availability.*

In *Better File Information With Windows* the author says: *''There is often a lot of information automatically recorded when you save a file. This information can be easily displayed and can prove to be useful when sorting/ categorizing files.''*

In *How to Tell If Your Cloud Provider Can Read Your Data* the author discusses the common practice of comingling data but using techniques that allow you to separate out your own stuff. He goes on to say: *''Not all services work this way, but the vast majority do.''* There's much more - read the article.

Operating System

In *Windows Live SkyDrive: An Office in the Cloud* the author says: ''A quiet, steady evolution is taking place in the data storage world. Soon CD's and external hard drives may be replaced by storage on the Internet, or, as we say, the ''cloud.'' In this era of mobile devices like smart phones, laptops, and tablets, it is natural for us to want to have access to the files and photos on our base computer when we are in some remote location.''

In *Adding Disk Space to Windows 7* the author suggests four options to consider if you are running out of disk space. He discusses three of the options but has no experince with the fourth: Enable dynamic disk management, which makes multiple disks appear as one, thus increasing the available space.

In *Screen Capture in Windows 7* the author found a little program called PicPick that does the job of screen capture.

In *Using Windows Task manager to Get Out of Potentially Harmful Situations* the author discusses how to use Task Manager to log off those pesky sites that won't let you go.

Software

In *Change of Allegiance - Does the Antivirus Software You Use Really Matter?* the author reviews his experiences with some well-known products.

COMMUNICATIONS NOTES & TIPS

Copyleft

Cal Esneault, President, Cajun Clickers Computer Club
(www.clickers.org) ccnewsletter (at) cox.net

We are all familiar with the term ''copyright''. This is where a government grants to the creator of an original creative work certain exclusive rights to its distribution and use in return for the public disclosure of the work. There is usually a time period for this protection (for example, life of the author plus 75 years). Common examples are art work, photographs, and music. With a few exceptions (such as ''fair use''), the copyright owners have strict control over the copying and distribution of such work unless they grant exceptions or specific permissions.

Although there is debate over the details, computer software can also be covered under copyright law. This can be more restrictive than patent law since ''inventions'' establishing patents require a more extensive proof of originality and usefulness and last for a shorter period of time (about 20 years). Proprietary software distributors solve any ambiguities by having users forfeit most of their rights immediately by requiring End-Use License Agreements (EULA's).

Originators of the concept of Free and Open Software (FOSS) wanted to ensure that their free work and any subsequent derivatives would have legal standing to continue to be free in the future. They created the play on-words term ''copyleft'' for using copyright law to provide copyrights which ensured the free distribution of their work and any derivatives thereof. This gained the term ''viral'' protection since, with certain legal language, any product which contained any part of this open code would render the entire project to be free and open. Thus, this piece of code would propagate like a ''virus'' and infect any piece of proprietary code.

The first widespread use of copyleft was conducted by Richard Stallman for the GNU General Public License (GPL). There have been several GPL versions:
1. GPLv1 (1989)
2. GPLv2 (1991)
3. GPLv3 (2001)

the numerical ratings, which mean little, but carefully read the comments, where it is easy to identify the balanced, knowledgeable comments from the petty whines.

In general, they allow the license recipient the right to use, study, copy, share, and modify the original code. Users must acknowledge the original author and distribute any modified software under the same restrictions obtained from the original license. The GPL license is the mainstay of Linux systems. The author has the right to have only parts of the software covered, or extend other limitations. The concept is that anyone using this ''free'' software is bound by its initial conditions as a minimum requirement.

There are alternatives to the copyleft approach. Copyright owners may freely give their rights away (''public domain''), or they may grant only certain rights (''permissive'' restrictions). For example, Apache and BSD have permissive licenses, and, users may use this free software and then combine it with their own software to create a new proprietary work. This, for example, is how Mac OS uses an earlier open version of a Unix-type OS with their own handiwork to create their own proprietary operating system (which, of course, you readily agree to by checking acceptance of the EULA!).

To protect the legacy of open software, the Free Software Foundation (FSF) was created in 1985 to ensure compliance with copyright protection established to maintain the open software conditions. They have attorneys to take legal action against anyone not following the open distribution of free software and also maintain a large set of copyrights and patents for community use.

Not everyone agrees that ''copyleft'' is the best approach (as no surprise, Microsoft Corp. objects to it). For example, inadvertently putting a small piece of open code into a large program could invalidate proprietary usage of the entire software package. Options exist, such as dynamic linking, which tend to minimize this problem. Future modifications of the GPL and permissive licenses continue to occur as technology advances and as originators of open source software seek to ensure its continuing legacy.

This article has been obtained with permission to reprint by non-profit or other user groups, with credit given to author, publication and user group.

Power-line networking

by Andrew Petrovic, Ottawa PC User Group, June 2012

Introduction

When an ISP provides an Internet connection to your home through a coaxial cable or DSL connection, it feeds into a modem unit (usually supplied by them) which will either have a router incorporated or will likely need to be connected to a separate router. Either way, the router has several network outputs that can supply one or more computers.

In larger homes where several people each have a computer in different rooms, there has to be a method to distribute this Ethernet network signal throughout the house. Even if there are no extra computers, several devices, such as Blu-ray and media distribution devices or gaming consoles can connect to the Internet via an Ethernet cable.

So what are the methods of distributing this network signal around the home? Here are the common ways:

♦ **Wired connections**. Here there are actual network cables running inside the walls of the home. Where the cable terminates there will be an Ethernet socket on the wall and you just

plug your device into it and go. This is by far the best method, but of course is the least convenient and most people don't want to go to the trouble of setting all this up. Also the wires and connectors are in a fixed position, so you must connect where the cable runs only.

♦ **Wireless.** This is a much more common method and the technology has improved over the years. There are drawbacks with it though. You must have wireless compatible equipment, such as a wireless router and also each device (desktop computer; laptop; etc) must be capable of using wireless. You also need some technical understanding of setting up wireless in order to make it secure, as the signal can be picked up around your neighbourhood quite easily.

♦ **Power-line.** This is an alternate method that uses the 110 volt power cables running throughout your house. The network signal rides on top of the power in the electrical wiring and can be picked up wherever there is a power outlet in your home.

How Power-line networking works

To make this work, you need to buy Power-line units - one for each network node. For example, you can locate one near to the existing network router. You plug the unit, which is a small box the size of two decks of cards, directly into the power outlet on the wall. Then connect an Ethernet network cable from this unit to an available network connector on your router.

You then take another unit (they are often sold as two units in a 'starter kit') and plug this into the wall outlet somewhere else in the house, where your remote computer is located. This computer then connects to that unit with a standard network cable.

Actually the basics of the technology is not that new - there were home intercom units years ago that worked by only needing to plug them into electrical outlets without a separate communication wire.

The good and bad of Power-line networking

Probably the main plus of Power-line networking is the fact that it's very easy to set up. There is no extra wiring to install and the end points can be anywhere that there is an electrical outlet. In addition, there is a minimal amount of technical know-how required to install it.

Wherever the network connection comes out, you can plug in other distribution switches or wireless units if you need to and make quite a complex network environment.

It's not absolutely perfect though, because in some older houses with older wiring it may not work very well. Even in more modern houses it is possible that if the end points of the network are on different electrical circuits (different phases) then it may not work, or speed may be reduced, although in my house, which is 13 years old, I was able to have the router and one Power-line unit in the basement and the other Powerline unit could be connected to any outlet anywhere in my house, on any of the three levels and never suffer more than a minimal loss in speed.

The older Power-line units did suffer from quite slow connections, but these days the technology has been improved to the point where the network speed can be typically 100 or 200 Mbps and recently up to 500 Mbps. For comparison, wired Ethernet in the home can go up to 970 Mbps and the fastest wireless up to 600 Mbps.

Note also that the unit should be plugged directly into the wall outlet and not through extension cables or power bars and especially not through any surge devices that could affect the signal quality. Also plugging into an AFCI circuit breaker line can reduce performance.

Security of data

One of the disadvantages of using a wireless connection is security. Unless you tighten up that security then you are vulnerable to outside 'hackers' picking up your signal and allowing them to access your data - both data being transmitted and data stored on your PC.

Power-line has the option of easily set up encryption. If you are just streaming video or audio around your home, then encryption is less important and you need the maximum bandwidth available. For data transmissions you need to set the security up, which is usually done by pressing a switch on one unit and afterwards pressing a switch on the other unit. Not exactly difficult. Encryption may slow down the network speed slightly because of the overhead involved, but it should not be significant.

It could be possible for your neighbours to pick up your Power-line signal if they have a compatible unit and are on the same electrical phase (perhaps more common in apartments than houses) though the distance the signal can go is fairly limited and the data encryption you can apply is quite strong, so should not be a reason to be concerned.

Availability

Most of the main computer suppliers stock Power-line products now. You can start off by buying a starter kit, consisting of two units, then if you need to expand the network you can buy additional units to add to your home wherever they may be needed.

The devices should also come with some software that you can install on your computer to manage your Powerline network. Accompanying instructions will detail exactly what software can be set up. The software may not be required to be installed for the units to work, but it does make life easier to use the software for renaming, testing and troubleshooting connections.

Better File Information with Windows Explorer - Sort your files more intelligently with a few simple clicks.

By Les Townsing, a member of the Melbourne PCUG, Australia
April 2011 issue, PC UPDATE
www.melbpc.org.au editor (at) melbpc.org.au

There is often a lot of information automatically recorded when you save a file. This information can be easily displayed and can prove to be useful when sorting/categorizing files.

Normally, when you open Windows Explorer (rightclick on the Start button and select 'Explore') you get displays indicating the file name, size, date modified, and other general information (see below).

If, however, we right-click anywhere on the Column Heading bar we get a lot of additional columns we can add. Depending on the type of files you can select some meaningful columns. If we are looking at picture files (jpg) some appropriate columns may be Date Taken, Dimensions or file size.

If you right-click on a file and select properties, you get to view all the possible information as well as the ability to edit some of the fields. You can now sort your files by any of the columns (just left click on the column heading). If we right-click on a file, we can select Rename and change the name to a more meaningful title rather than a bunch of numbers. These features may be more meaningful if we use music files as an example.

Unfortunately, some of the ''Ripper'' programs (programs that copy CDs and often convert the files to MP3s) get it wrong or leave a lot of stuff out, which can be quite annoying, particularly if it is the artist's name or the title of the song. When selecting a CD Ripper program this is one item worth checking.

Extra Tip

If you select a file (click on it) then hold down the shift key whilst clicking on another file then the system will select all the files in between and including the first and last file you clicked on. Now, if you right-click on any one of the selected files and choose properties, you can edit a field for all the selected files. This is no good for titles as every file must have a different name. However, it is good when you want to edit the album title or artist for a number of tracks.

Extra Extra Tip

Often the files you want to select are not consecutive in a list. No problem, hold down the control key then click on the files you want. As you click on the files they become marked as selected. You can then right-click on any selected file to edit the properties of all the selected files.

How to Tell If Your Cloud Provider Can Read Your Data

by Rich Mogull <rich@tidbits.com>
article link: <http://tidbits.com/e/12920>
Newsletter of the Hartford User Group Exchange June, 2012

With the tremendous popularity of services like Dropbox and iCloud there is, rightfully, an incredible amount of interest in cloud data security. Once we start hosting our most sensitive data with cloud services (or any third-party provider) its only natural to wonder how secure our data is when its in the hands of others. But sometimes its hard to figure out exactly _who_ can look at our information, especially since buzzwords like secure and encrypted dont necessarily mean _you_ are the only one who can see your data.

How Cloud Providers Protect Your Data -- In part because there are numerous ways cloud providers could protect your data, the actual implementation varies from service to service. All consumer cloud services are what we in the cloud world call _public_and are built for _multi-tenancy_.

A public cloud service is one that anyone on the Internet can access and use. To support this the cloud providers need to _segregate_ and _isolate_customers from each other. Segregation means your data is stored in your own little virtual area of the service, and isolation means that the services use security techniques to keep people from seeing each others stuff.

Practically speaking, multi-tenancy means your data is co-mingled with everyone elses on the back end. For example, with a calendar service your events exist in the same database as all the other users events, and the calendars code makes sure your appointment never pops up on someone elses screen. File storage services do the same thing: intermingling everyones files and then keeping track of who owns what in the services database. Some, like Dropbox, will even store only a single version of a given file and merely point at it from different owners. Thus multiple users who happen to have the same file are technically sharing that single instance; this approach also helps reduce the storage needed for multiple versions of a file for a single user.

Although multi-tenancy means co-mingling data, the cloud provider uses segregation techniques so you see only your own data when you use the service, and isolation to make sure you cant maliciously go after someone elses data when youre using the system.

The cloud providers databases and application code are key to keeping all these bits separate from each other. It isnt like having a single hard drive, or even a single database, dedicated to your information. That simply isnt efficient or cost-effective enough for these services to keep running. So multi-tenancy is used for files, email, calendar entries, photos, and every other kind of data you store with a cloud service. Not all services work this way, but the vast majority do.

Encryption to the Rescue? -- A multitenancy architecture has two obvious problems. The first is that if theres a mistake in the application or database the service runs on, someone else might see your data. Weve seen this happen accidentally; for example, last year Dropbox accidentally allowed any user access to any other users account. There is a long history of Internet sites (cloud and otherwise) inadvertently allowing someone to manipulate a Web page or URL to access unauthorized data, and the bad guys are always on the lookout for such vulnerabilities. <http://www.wired.com/threatlevel/2011/06/dropbox/>

The second problem, which has been in the press a lot lately, is that the cloud providers employees can also see your data. Yes, the better services usually put a lot of policy and security controls in place to prevent this, but its always technically possible.

One way to mitigate some of these concerns is with encryption, which uses a mathematical process coupled with a digital key (a long string of text) to turn your data into what looks like random gibberish. That key is necessary to decrypt and read the data.

Most cloud providers use encryption to protect your Internet connection to them (via SSL/TLS look for https URLs) so no one can sniff it on the network. (Unfortunately, some large email providers still dont always encrypt your connection.) Most of the time when you see encryption in a list of security features, this is what they mean. But encrypting data in transit is only half the battle what about your data in the providers data center? Encryption of storage is also necessary for any hope of keeping your data secret from the cloud providers employees.

Some providers do encrypt your data in their data center. There are three ways to do this:
1. Encrypt all the data for all users using a single key (or set of keys) that the cloud provider knows and manages.
2. Encrypt each individual users data with a peruser key that the _cloud provider_ manages.
3. Encrypt each individual users data with a peruser key that the _user_ manages.

By far, most cloud services (if they encrypt at all) use Option #1 - keys that they manage and that are shared among users because its the easiest to set up and manage. The bad news is that it doesnt provide much security. The cloud provider can still read all your data, and if an attacker compromises the services Web application, he can usually also read the data (since its decrypted before it hits the Web server).

Why do this level of encryption at all? Its mostly to protect data if a hard drive is lost or stolen. This isnt the biggest concern in the world, since cloud providers have vast numbers of drives, and it would be nearly impossible to target a particular users data, if the data could be read at all without special software. It also means that providers get to say they encrypt your data in their marketing. This is how Dropbox encrypts your data.

Option #2 is a bit more secure. Encrypting every users data with an individual key reduces, in some cases, the chance that one user (or an attacker) can get to anothers data. It all depends on where the attacker breaks into the system, and still relies on good programming to make sure the application doesnt connect the wrong keys to the wrong user. Its hard to know how many services use this approach, but when done properly it can be quite effective. The major weakness is that the cloud providers employees can still read your data, since they have access to the keys.

Option #3 provides the best security. You, the user, are the only one with the keys to your data. Your cloud provider can never peek into your information. The problem? This breaks... nearly everything. First of all it means you are responsible for managing the keys, and if you lose them you lose access to your data. Forever. Also, it is extremely difficult - if not impossible to allow you to see or work with your data in a Web page since the Web server cant read your data either. Thus it works for some kinds of services (mostly file storage/sharing) and not others, and _only_ for sophisticated users who are able to manage their own keys.

As is so often the case, these options reveal the tradeoff between security and convenience. **How to Tell if Your Cloud Provider Can Read Your Data** -- In two of the three options I listed above, the provider can read your data, but how can you tell for yourself if this is the case?

There are three different (but similar) indications that your cloud data is accessible to your provider:

* If you can see your data in a Web browser after entering only your account password, the odds are extremely high that your provider can read it as well. The only way you could see your data in a Web browser and still have it be hidden from your provider is if the service relied on complex JavaScript code or a Flash/Java/ActiveX control to decrypt and display the data locally.

* If the service offers both Web access and a desktop application, and you can access your data in both with the same account password, odds are high that your provider can read your data. This is because your account password is also probably being used to protect your data (usually your password is used to unlock your encryption key). While your provider could technically architect things so the same password is used in different ways to both encrypt data and allow Web access, that really isnt done.

* If you can access the cloud service via a new device or application using your account user name and password, your provider can probably read your data. This is just another variation of the item above.

This is how I knew Dropbox could read my files long before that story hit the press. Once I saw I could log in and see my files, or view them on my iPad without using a password other than my account password, I knew that my data is encrypted with a key that Dropbox manages. The same goes for the enterprise-focused file sharing service Box (even though its hard to tell when reading their site). Of course, since Dropbox stores just files, you can apply your own encryption before Dropbox ever sees your data, as I explained last year at Securosis. <https://securosis.com/blog/how-to-encrypt-yourdropbox-files-until-dropbox-wakes-the-f-up>

And iCloud? With iCloud I have a single user name and password. It offers a rich and well-designed Web interface where I can manage individual email messages, calendar entries, and more. I can register new devices and computers with the same user name and password I use on the Web site.

Thus, from the beginning, it was clear Apple had the capability to read my content, just as Ars Technica reported recently. <http://arstechnica.com/apple/news/201204/apple-holds-the-master-key-when-it-comes-to-icloudsecurity-privacy.ars>

That doesnt mean Dropbox, iCloud, and similar services are insecure. They generally have extensive controls both technical and policy restrictions to keep employees from snooping. But it does mean that such services arent suitable for all users in all cases, especially businesses or governmental organizations that are contractually or legally obligated to keep certain data private.

Doing It Right -- The backup service CrashPlan is an example of a service that offers flexible encryption to fit different user needs, with three separate options. (For more on choosing the appropriate encryption method for CrashPlan, see Joe Kissells Take Control of CrashPlan Backups.)<http://www.crashplan.com/> <http://www.takecontrolbooks.com/crashplan?pt=TB1121>

First, by default, your data is encrypted using a key protected by your account password. This still isolates and protects it from other users, while enabling you to view file information through the CrashPlan Web site and the CrashPlan Mobile app. But CrashPlans employees could still access your data.

Second, if you want more security, you can add a separate backup password that only you know. This approach still allows access through the CrashPlan Web site and the CrashPlan Mobile app, but CrashPlan employees cant see your data except (maybe) during a Web session after you enter your separate password. Attackers cant access your data either, though your password may be susceptible to brute force cracking or social engineering.

Third and finally, you can generate your own perdevice encryption keys, which CrashPlan never sees or knows about, rendering your backups readable only by you (or anyone who can beat the key out of you never underestimate the power of a wrench props to xkcd!). You could technically use a different encryption key on each device (or share, your choice) so that even if one system were to be compromised, it wouldnt allow access to backups from your other devices. Clearly, this is much more difficult to manage and well beyond the needs or capabilities of the average user (heck, even I dont use it). <http://xkcd.com/538>

So if you want to be certain that your data is safe from both attackers and the cloud providers employees snooping, look for services that offer additional options for encrypting data, either with a password or an encryption key known only to you. If such an option isnt available at the next cloud service you check out, youll know that the providers employees could technically read your data. And when the next big story of a cloud provider reading data hits the headlines, you can smugly inform your friends that you knew it all along.

OPERATING SYSTEM NOTES & TIPS

Windows Live SkyDrive: An Office in the Cloud

By Nancy DeMarte, a member of the Sarasota PCUG, Florida, December 2011 issue, Sarasota PC Monitor
www.spcug.org ndemarte (at) Verizon.net

A quiet, steady evolution is taking place in the data storage world. Soon CD's and external hard drives may be replaced by storage on the Internet, or, as we say, the ''cloud.'' In this era of mobile devices like smart phones, laptops, and tablets, it is natural for us to want to have access to the files and photos on our base computer when we are in some remote location. SkyDrive is Microsoft's password-protected, free online storage area, complete with abbreviated versions of popular Microsoft Office programs for editing the stored files. It is also equipped for sharing files with others and is a convenient way to transfer files from an old computer to a new one. Microsoft Office users should get to know Windows Live Sky-Drive as a solid option for online backup.

Online storage has been around for awhile, primarily purchased by businesses as a backup for large amounts of data. Carbonite, for example, is a well respected online storage company popular with businesses which also offers a package for home clients. The home client pays an annual fee of about $60 per computer to upload user-created files to a secure spot. Free online storage is not as common, but Google and Microsoft are competing for the title of most popular free cloud storage. I have used Microsoft's SkyDrive for a couple of years and have found it to be a user friendly, flexible service with many good features and being updated all the time.

Windows Live

Before we explore how SkyDrive works, let's take a minute to review the concept of ''Windows Live,'' of which SkyDrive is a part. Microsoft has been reworking the ''Live'' idea since 2005. It is a group of online services and software downloads which complement Microsoft's operating systems. When Windows 7 was introduced, several applications which had been part of earlier Windows versions were removed, among them Windows Mail and Photo Gallery. Instead, Microsoft offered a suite of programs and services called Microsoft Live Essentials and made it available for free downloads, as long as the person joined the Live community with a username and password. (I have belonged for years and have not received spam as a result.) Users can choose the programs they want from a long list. Many of these are online services, such as SkyDrive and Hotmail. Others are downloadable programs, such as Windows Live Mail and Movie Maker. All are free. Microsoft has announced recently that Windows 8 will have the Live Essentials package included with the system.

SkyDrive: Free Storage

SkyDrive lets a Microsoft Office user add Word documents, Excel spreadsheets, PowerPoint presentations, OneNote documents, and photos to a password-protected place on the Internet at skydrive. live.com. You can add a single file up to 100MB in size and can store a total of 25GB at no charge. These limits were recently raised, and the prediction is that storage space on SkyDrive may be unlimited very soon. Isn't competition great?

To add files to SkyDrive, you must first create a free Live account, then log on to SkyDrive and create folders to hold your files. You then select the files, including photos, from your computer and upload copies of them into these folders using an easy-to-follow wizard on the SkyDrive home page. You can even upload a whole folder at once as a local zip drive. Next you set permissions for each folder using a simple slider and folksy categories: Everyone (public), People I selected, People with a link, or Just me.

Once files are in SkyDrive, they can be deleted, organized, and renamed. Plus, they can be edited with the Office web apps, mini-versions of Office programs located on the SkyDrive home page, using any version of Office back to 2003. If you have Office 2010, you can open a file that you have stored in SkyDrive in the appropriate web app, and then click the ''Open in '' button to open it with your full version of program on your computer. If you have an earlier version of Office, you can download a plug-in program from Microsoft that allows you to open a file with your full program. I tried this on my laptop with Word 2007, however, and found it cumbersome. I guess they want us to buy Office 2010. As a workaround, you can always download a file from Sky-Drive to your computer for full editing capabilities.

Sharing Files

If you want to share a file, whether an Office file for a photo, on SkyDrive with someone, you can either send him a link or set the permission so he can view and/or edit it. I experimented by sharing a Word 2007 document with a friend who is not a member of Windows Live. In SkyDrive, I highlighted the file I wanted to send. From the Sharing menu, I clicked 'Send a Link'. An email message opened ready to address. It contained a link to the file with a spot for me to type a message. My friend received the message with no problem and merely clicked the link to go directly to the folder on SkyDrive. She now has permission to view documents in that folder.

Currently, the only Office web app that allows for shared editing is Excel. This involves editing a spreadsheet in SkyDrive with selected people. Names of those working on the file at the same time show up in the toolbar.

SkyDrive is greatly improved from its predecessor, Windows Live Workspace. I would expect it to get even better as the competition heats up with its rival Google. The reviews show that although Google made a huge push a couple of years ago, with its array of services like Google Apps and Google Calendar, Microsoft is catching up. Its latest version of SkyDrive, plus two new related synchronization services,

Live Sync and Live Mesh, are a good start. Microsoft now offers 25 GB of free storage compared with Google's 1 GB (although there is the option to purchase more). If you are a Microsoft Office fan, then you can't go wrong by giving SkyDrive a try.

Adding Disk Space to Windows 7

by Dick Maybach

The Rochester Computer Society, Inc. Monitor / June 2012

When buying a new PC, it's usually wise to equip it with the largest possible hard disk. Despite this, it's not uncommon to find that eventually it becomes uncomfortably full, leaving you with four options:

1. Save all your user data on an external disk, replace the system disk with a larger one, install Windows and all your applications from scratch, and restore your user data from the external disk,
2. Make an image of the current disk on an external drive, replace the current hard disk, and restore the image to it,
3. Add a hard disk and move some data folders to it, or
4 Enable dynamic disk management, which makes multiple disks appear as one, thus increasing the available space.

If your Windows 7 installation is corrupted by file system errors or malware, you must use option 1. If your system is working well, use option 2 (using the Windows 7 Backup and Restore tool), which is substantially easier and faster than 1. If your current system is working well, option 3 looks attractive, but there are significant issues, which I discuss below. I don't have the resources to test option 4, and I've learned from sad experience not to write about things I haven't done. If you are interested in dynamic disk management, see a good

book, such as Window 7 In Depth by Cowart and Knittel. However, this approach appears to be complex enough to make it useful only in a professionally-staffed computer center. I don't recommend it for home users.

Option 3, add a second hard disk and move some of the data folders from our home folder to it, looks attractive. Here, some data will reside on a different drive, call it D:, and unfortunately, some programs, for example iTunes, cannot access data on it. You can edit iTunes' preferences to declare that, iTunes Media, the folder that holds its music, resides on D:, but iTunes apparently doesn't look outside your home folder. There are probably other applications with similar flaws.

A procedure called grafting appears to offer a solution. It maps all the files on an auxiliary disk into a folder in your home folder, and any files you later add to that folder are stored on the grafted disk. The basic procedure is as follows:
- Copy all the files in the selected folder to the auxiliary disk;
- Delete the selected folder on the main disk; and
- Graft the auxiliary disk to a folder on main disk.

This indeed works on Windows 7, and after I did it, iTunes was able to find its files on the auxiliary disk, but operations were so flaky (see below) that I wouldn't do this on a PC that I actually used.

If you would like to experiment (not on the PC you use for TurboTax please), here is the procedure. Log into an account with administrator privileges, and open the Disk Management tool. (The easiest way is to tap the Windows key or click on Start, type disk manage and select Create and format hard disk partitions.) The screenshot below shows the result.

In this example, I graft NTFS-2 (F:) onto a folder in my home folder. Right-click on NTFS-2 (F:) and select Change Drive Letter and Paths Click the Add button, select Browse navigate to the folder where the original folder appeared (in my case C:\users\n2nd), click the New Folder button. The result is shown below.

Click the OK button and the Browse for Drive Paths window will close, then click OK in the Add Drive Letter or Path window, and close the Disk Management window. The disk NTFS-2 (F:) is now grafted on the folder C:\Users\n2nd\New Folder. If you had to log in as a different user to obtain administrator privileges, log out and then log back into your home account, in my case n2nd.

This seems straightforward, but there are several traps. The Disk Manager is quirky and not well documented. I needed several attempts to make the above procedure work, which isn't good for a tool that modifies your folder structure. Since you can graft an entire disk only to a single folder, if there are several large folders, you must partition the auxiliary disk and graft a separate partition to each folder. This is unfortunate, because you can't graft your entire home directory, as it contains system files that are always in use. Most disturbing is that when I finished and tried to make a full backup, including a system image, the procedure failed. Even if it had succeeded, I'm not sure I could have restored my system. Would the software try to put everything on the original (now too small) C: disk, or would it be smart enough to restore to both C: and F: and graft F: to a folder? This isn't something about which you want to be surprised when you have to restore your files.

My conclusion after all this is that Windows 7 is designed to operate from a single disk, as are some of its applications. In this respect, it's made a step backward from XP, where you could locate your My Documents folder on any disk, and even iTunes could find its files there. You can add additional disks to a Windows 7 system, but accessing files on them will be somewhat less convenient than if everything resided in your home folder. As a result, if you run out of disk space on a Windows 7 PC, the best course is to replace the disk with a larger one and port your system to it.

From the March 2012 issue of BUG Bytes, Brookdale Computer Users' Group, NJ.

Screen Capture in Windows 7

by Alan German, Ottawa PC User Group, July 2012

I always wondered what was left out of Windows 7 Home Premium in order to make it into the Starter Edition. Obtaining a netbook computer with Windows 7 Starter Edition installed gave me the chance to find out first hand.

One of the things that became apparent was that the Windows Snipping Tool, used to capture full or partial screenshots, was nowhere to be found. This set me on a hunt - to locate a free screen grabber - just so that I could create a screenshot with which to illustrate this article. Well, not really, but since I do take images off my display screen quite often, I need an easy-to-use and flexible screen capture utility.

One program that I found really easy to use, but with considerable power, is PicPick. This little utility loads itself into the system tray and is then always ready to jump to the task of obtaining a screenshot. There are many configurable options. Capture of the full screen, the active widow, or an outlined region can be specified, and a variety of file formats in which to store the screen image are available. The captured image is first loaded into the program's main window (see above) where a range of tools, including resize and crop, and the ability to add text and graphics to the image, are provided.

PicPick makes it easy to grab an image of any portion of the display screen, do simple editing, and then store the image to disk in BMP, JPG, PNG or GIF format. The program is free for noncommercial use.

Bottom Line

PicPick (Free for non-commercial use)
Version 3.0.3 Wiziple Software
http://www.picpick.org/

Using Windows Task Manager to Get Out of Potentially Harmful Situations

by Terry MacLennan
Sauk Computer Users Group, IL June 2012

There is an easy method of getting your computer out of two situations of potential harm. To do this, we will use the operating system's built-in program called the Task Manager.

The first situation is when you have too many programs running at one time and the computer locks up. This lockup can also be caused by a single program that for one Reason or another, fails to run properly. Reaching over and hitting the power button may seem to be your only option but there is a much better choice.

The second situation occurs when you are on a webpage and one of those realistic looking but totally phony ''security alerts'' pops up on your monitor screen warning you of imminent danger of viruses and other malware that ''it'' has detected on your computer. These scare popups trick many naive people into clicking on them only to find out that now their computer truly is infected and control has been lost. You are totally helpless when you have clicked on one of these so-called ''security'' scam programs.

You absolutely must not click anywhere on these pop-ups including buttons that say something to the effect of ''No Thanks,'' ''Decline'' or even ''Continue Unprotected.'' But, instead of clicking one of those, you may decide, almost instinctively, to click the ''X'' in the corner of the pop-up box. Doing any of these actions is almost like turning your house alarm off, opening the door and saying ''come on in'' to the masked bandit standing outside. Paying the ''bandits'' for their ''security program'' which is holding your computer hostage is an extremely poor choice. Do you really want to pay the thieves with your credit card and it's number?

But you are now stuck in a situation where you may try to click off the web page by clicking on its ''X'' in the upper right hand corner. But you soon find out that that won't work as you first need to close the window (the pop-up in this case) that is on top. Hard shutting down the computer by using the power button may seem to be your only option but again there is a better alternative.

Your best friend in both situations is the Task Manager. To open this built-in program, press and hold the CTRL and ALT keys with your left hand, then tap the DEL key with your right hand.

In Win XP, this will automatically open the Task Manager while with Windows 7 it will take you to a page with a list of options. Click the bottom option and it will open the Task Manager which looks nearly identical to the XP one. From here, everything is the same for both systems.

Along the top edge of the Task Manager is a row of tabs. Click the Applications tab, if it doesn't happen to automatically be on that tab. When you have opened it up, you will see a listing of all the programs and web pages that are running.

If your computer is locked up, look for any programs that are ''Not responding.'' Click the program one time to highlight it then click on End Task at the bottom. This should close the nonresponsive program and free your computer. If the computer remains locked up, use the same method to close all of the remaining Programs that are running then shut down as you would normally. Everything should be back to normal when you reboot the computer.

A hard shutdown with the power button is absolutely the last resort as this could potentially damage files. To close a web page with the dangerous fake security warning pop-ups, use the same method by highlighting the web page in the list then clicking End Task. This will safely shut down the web page with its pop-up without installing the malware ''security program.''

Originally published in The Computer Connection, the newsletter of the Sauk Computer Users Group

SOFTWARE NOTES & TIPS

Change of Allegiance - Does the Antivirus Software You Use Really Matter?

by Greg Skalka, March 2012 issue of Drive Light, Under the Computer Hood User Group, CA.

I just switched to a new antivirus program. I'd been a loyal user of my previous program for over five years, which seems like an eternity in the ever-changing computer software business. I've wondered for some time if it mattered which brand I used. Although there are probably dozens of antivirus programs available, some of which are even free, I have only ever used four. Am I using the best one? Is there a best one? Would I be wasting my time trying to determine the best one? And is what is best relative to my needs anyway?

I was surprised at the results of an informal survey taken at one of our recent general meetings. Our membership appears to use a wide variety of the available antivirus offerings. Around a dozen different vendors were being used by our members, with no one source having more than 10% of the market in our group. With the market apparently so fragmented, can one brand really be that much better than the others? I don't deny the importance of computer security. It is a common tenant of cyber security that every computer should run an antivirus program to protect against those threats. Microsoft believes this so much that every version of Windows since XP performs checks to see that an antivirus

program is installed and that the virus signatures are not out of date. I'd just like to see proof that the antivirus software is doing its job.

One of my problems with antivirus software is that, at least in my experience, it seldom finds any viruses. I've tried to be diligent in my regular computer maintenance, running antivirus and anti-malware software once each week and keeping the signatures updated. My anti-malware software will often find some kind of spyware or malware on one of my computers to quarantine or delete, but from all the probably hundreds of hours I've spent running antivirus scans, I've yet to find a virus. I do know viruses still exist out there in the cyber world, as I have seen others have them. My daughter had a virus on her laptop last year, and this month we found the Conficker worm on some network servers at the company I work for. Since I've not found any, could I be running just a placebo antivirus program?

I guess the effectiveness of antivirus software is something we may have to take on faith. I've never seen comparisons or reviews of antivirus software that evaluated the ability to detect or remove particular threats.

Usually the software's rating is based on less essential but more measurable parameters like ease of use, cost or manufacturer's reputation. With new virus threats appearing constantly (or so we are led to believe), how can a program's ability to quickly recognize something new be evaluated in advance? Selecting an antivirus program might be similar to choosing a religion, in that all you have initially is your faith in your choice, and you won't likely find out until much later whether you chose correctly.

I originally started out (over a decade ago) using Norton Antivirus, as it was one of the first and few of this type of program on the market. They also offered a lot of rebates on their products, so I could usually get my antivirus every year for free. I really liked the Norton Utilities, and so it was not long before I was using Symantec's Norton SystemWorks suite. I also really liked the ZoneAlarm firewall, and so used their free version for many years alongside the Norton suite. Eventually, however, Symantec came out with their own firewall program, and they made a decision that has me soured on their products to this day. Symantec made their Antivirus product incompatible with the ZoneAlarm firewall, probably to promote their own Norton firewall. This made me have to choose between them, and ZoneAlarm won. I don't think I've purchased a Symantec product since.

Around this time, ZoneAlarm came out with their own security suite, ZoneAlarm Internet Security Suite. It combined my favorite firewall with antivirus and antispyware. It was also usually available periodically for free after rebate (my favorite kind of software), so I used their suite on all my computers for at least five years. The ZoneAlarm antivirus never really impressed me, but at least it worked well with their firewall, and so I had faith that it was protecting me.

In the last year, however, the ZoneAlarm antivirus turned into a real nuisance. It became a drag on my computer's resources, slowing it down considerably while updating and while scanning. Every time my computer was started, the suite tried to check for updated antivirus signatures. This process took minutes to complete, and occupied the computer to such an extent that it was not possible to use it until the update was completed. This became very annoying, as it slowed my computer just as I was most interested in using it. If I wanted to boot my computer quickly to look up something on the Internet, it added additional minutes to my search time. It also suddenly went from a few hours to overnight and more to run an antivirus scan. I even tried (unsuccessfully) to disable the antivirus updates. Finally I had enough and decided to look for a new antivirus program. This also coincided with the end of my ZoneAlarm ISS subscription and the apparent end of their rebate deals.

During this time I had also used McAfee's antivirus briefly on a new computer that came with a free trial, and used it on the computers provided by my employer. I didn't think it was anything special.

A trusted reference was the deciding factor in my selection of a new antivirus program. Our group's webmaster has been using ESET's NOD32 antivirus software for many years, and had nothing but good to say about it. He claimed it used little hard drive space and ran quickly with little impact on computer performance. I considered using it in conjunction with the free version of the ZoneAlarm firewall, but a rebate deal on ESET Smart Security persuaded me to try another firewall program as well. I bought two of the three-user packs, and figured I was set for all my computers for the next year.

I soon found out why the ESET Smart Security 4 suite was offered at a discount, as within a month Smart Security 5 was released. I was allowed a free upgrade to version 5, but found upgrading from 4 to 5 had issues. It was much better to install version 5 from the web (using my normal activation information), as it allowed the installation on a drive other than the boot drive. The firewall also seemed to work better this way. I'm still learning about ESET's firewall, but their antivirus seems to live up to its reputation as easy on resources. I guess I have something new to have faith in.

Help Lines

HARDWAREHELP	Advisor No.
Reformat Hard Disk, FDISK	2,4,5
Install Hard Drive, CD-ROM/RW	2,4,5
Install Video Card	7
Partitioning Hard Drives	2
Internet/Intranet	6,7
Audio Cards	4
MPs Files, WMA Files, WAV Files	3,4
Burning CD's	3,5
Homesite	7
Net Objects	7

SOFTWAREHELP	Advisor No.
Win 95/98/ME/2K/NT/XP	2,3,4,7
Win 7	4,7
Microsoft Word	2,7
Microsoft Excel	4
Microsoft PowerPoint	4
WordPerfect	1,7
Norton/Symantec AntiVirus	2,3,6,7
Norton System Works	2,7
CompuPic / CompuPic Pro	3,7
Winzip, WinRAR	6
Ccleaner	3,4
Outlook, Outlook Express	2
Internet Explorer	2,7
RegSeeker	3,5
Instant Messaging	2
Installing Software after Reformatting	5
Deleting Files; Wiping	6

ADVISORS

Name	Phone	Hours
[1] Fred Shelton	(253)752-0120	Variable
[2] Bob Henkel	(253)537-6732	8A-8P any day
[3] Tom Stepanek	(253)922-7939	7-9P Mon-Fri
[4] Carl Tenning	(206)824-3843	6-9P Mon-Fri
[5] Oclad Wesley	(253)212-0352	6-9P
[6] Bob Thomson	(253)752-5582	Variable
[7] Ray Mills	(360)692-7568	6-9P Mon-Sat

TOG Sunset?

by Carl Tenning, TOG President

The "Tacoma Open Group For Microcomputers" is now over 31 years old. It started out in June 1981 as the Tacoma Osborne Group. After the IBM PC emerged, the name of the club was changed to "Tacoma Open Group For Microcomputers". In the last few years membership and meeting attendance have been declining. Meeting attendance was only eight in both July and August of this year and only six at the September 2012 meeting. An election of officers was supposed to be held at the May meeting of this year, but no one stepped forward to offer their services. Thus, we continue operating with the previously elected officers, President, Treasurer, Librarian, and Newsletter Editor. No one has filled the position of Vice President/Program Chairman for at least two years now. So, the question arises, should we continue on? The club, however, is on firm financial ground with sufficient funds to continue operation as we are now for about three even if we were to discontinue collecting yearly dues. Thus the proposal was made by the Treasurer at the September 2012 meeting to discontinue collecting membership dues beginning in January 2013. A vote on this proposal will be taken at the November 2012 meeting.

In the event that this proposal is approved, (1) membership dues will be terminated as of January 2013; (2) we will continue publishing the printed newsletter and it will continue to be mailed out to existing members; (3) new members will not receive a printed newsletter through the mail, but may elect to receive one at the monthly meeting; (4) the club will continue the TOG web site and will post the newsletter on that site, as it is now. Come to November 12, 2012 meeting to express your views and vote on this proposal**.**

Tacoma Open Group for Microcomputers (TOG)
New Member Application/Existing Member Change of Address Form

For **Tacoma Open Group** annual membership, send form (if needed) & **$25** to Bob Henkel., 10613 25th Avenue E., Tacoma, WA 98445.
Make checks payable to TOG

Please print or type. Date:_____ Sponsored by:_____

Member's Name:_____

Address: _____

City:_____ State:_____ Zipcode:_____Plus Four _____ Country: _____

Home Phone: (____) _____ Work phone: (____) _____ E-Mail Address _____

TACOMA MEETING

When: **Mon 10 Sept 2012 -7:00 PM**
Where: SE Tacoma Community Centre
1614 99th Street E.
Tacoma, Washington

From I-5 take Exit 127 (Hwy 512) to Portland Ave., north on Portland to 99th, left over tracks. Building is on south side.

Future Dates: 2nd Monday of Month

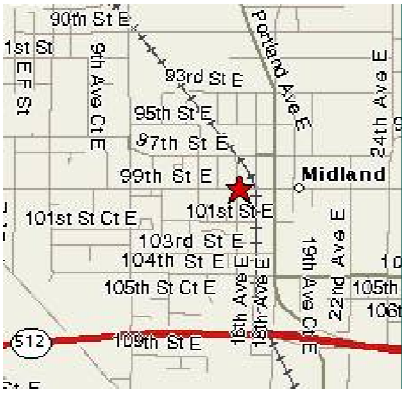
TOG BOARD MEMBERS

TOG Web Site: http://www.toggle.org

Deadline: 15th of this month to appear in next months' issue, if room

How To get To The Meeting

For those readers still unfamiliar with how to find our meeting place we have reproduced the map showing its relationship in Tacoma to Portland Ave S. and the 512 Freeway. The 512 Freeway can be entered from I-5 in Tacoma on the west or from Hwy 167 in Puyallup on the east. Proceed to Portland off-ramp and turn north to 99th Street. Some folks in the middle of Tacoma may prefer to take Portland southbound to 99th. At 99th turn west over the tracks and there you are!



TOGGLE

Tacoma OPEN Group for Micros
1808 Lenore Drive
Tacoma, WA 98406-1920

Change Service Requested

PROGRAMS

This Month's Meeting

This will be a regular monthly meeting. Meeting discussions are always interesting and the ever-popular Q&A (Question & Answer) period is sure to pique your interest, come up to your expectations and tickle your fancy. Come and share your own experiences, problems and discoveries.

The presentation at the meeting will be ''Windows 7 Tips & Tricks''. For those interested, the items presented may be copied at the meeting so be sure to bring a thumb drive or a blank CD-ROM to the meeting in order to obtain a copy of the presentation material and/or files. Carl says: Copies of the presentation are in three PDF files.