

HOW A BACK UP CAN BACK UP ON YOU!

I was panic stricken. I got a call from my co-editor on my other newsletter, the OnLine Connection. He was reviewing and proofing our January issue which I published three days before the end of 2011. He wanted to know if the half page blank space on page 2 was intentional or a mistake.

Even if is an online newsletter, it is not normal to leave any page partially blank unless it is the last page. Since he was reading the PDF version I suspected that the conversion process from to Publisher to PDF left out part of a page. There was only one way to find out: open the MS Publisher version of the newsletter and look at page 2.

So opened the January issue of the Online Connection and found it totally blank! After preaching to you all about file management over the past few years, how did I commit such a faux pas in file management. It was puzzling. The Publisher version was blank and there was no PDF version at all. How could that be? Did I misfile it?. I did a search but found nothing. It was impossible. I just don't make any such 'mistakes.' I looked like a fool to my co editor of the newsletter.

I generally practice what I preach. In a previous issue of the CCMV newsletter I described an effective back up procedure that that involves cloning the primary hard drive onto the secondary (second) hard drive so that in case of failure of the primary it is a simple matter to use the Setup function to switch the primary boot to the second drive and continue working.

I had not done that for months. In short, I worried because I really had no current back up and a failure now would be a total disaster. So a few days ago (about December 20) I did the clone back up and resumed working on the primary which included writing and finishing the OnLine Connection. But this morning on December 30 I decided to check out the secondary drive containing the clone to see if my backup worked OK.

The secondary booted up beautifully. When my co editor called I had forgotten that I was working with the cloned version. *(See next col.)*

This issue starts the new year of 2012 Confining my comments to this newsletter only, I'd say that I don't know what I am going to cover this new year. There is so much material available that I could fill 50 pages but there is only so much time available. I don't want to commit myself to specific specific topics. It is more fun for me to see what's appropriate for the time or to expand on what the President covers during the month. I assume that either (a) nobody is reading the newsletter or (b) every body is happy with it.

I will be 94 years old this month.

"As you are, I once was; As I am, you will be!"

(Continued from the left column)

I finally remembered that I was working with the cloned version! I shut down my computer and I used the Setup function to switch to the primary to boot up. I verified that I did Indeed have a MS Publisher version and a PDF version of the January 2012 OnLine Connection newsletter. And half of page 2 was blank!

I write about this because it is a lesson for you too. You don't have to install a secondary hard drive in your computer to create a clone. You can do it on an external hard drive which you all should have anyway if creating any kind of back up is important to you.

See the boxed message below about backups. I choose to use the internal secondary hard drive so that I do not have to face the hassle of putting the external in the computer to resume working. When my computer fails it is a disaster because of these newsletters.

A note about backups.

This newsletter reminds you again to clone your primary to another hard drive, either to an internal drive or an external drive. It is really better to provide the clone backup to an external hard drive so that the drive is not running constantly. Despite the low duty cycle of an external drive, the availability of the other internal drive in an emergency is attractive.



Are You a Sucker For Hoaxes?

By Frank Varano (*Italic are mine*)

(I got this from Early To Rise (ETR) on the Web. I wrote emails about this elsewhere many times but it is surprising to me how many people still fall prey to these hoaxes. Here is a direct quote from ETR on the subject:)

About Urban Legends and Hoaxes

Did you know that if you forward this ETR e-mail to 10 people, Bill Gates will send you \$100? And that if you pour Coca Cola on a piece of raw pork, dozens of worms will come crawling out?

Would you believe that if your cell phone battery is running low, just press *3370# and a small amount of secret reserved power will be released?

Well, actually, not a single one of these stories is true! And yet, every day, millions of people forward stories just like these around the Internet.

So the next time you receive a forwarded e-mail with a truly unbelievable story, plea for help, or commercial pitch, check Snopes.com before you do anything else. This website, the premier hoax-and-scam-exposing, urban-legend-busting watchdog on the Net, has been around since 1995.

(Some people don't like Snopes.com. I also have some reservations but it is pretty good and timely with its assessments. Snopes.com has changed its mind occasionally too.)

MORE ON BACK UPS

(HTG (How to Geek) on the Internet talked about backups recently when their readers came up with their own systems. In this article I want extract from their ideas to see methods others use to satisfy their back up needs.)

People store financial documents, family photos, letters, books (and newsletters) and other work projects in backups, digitally.

Redundancy is really storing things in more than one place. (How I do it is described in the sidebar in the next column.) Many readers of HTG used redundancy. They really had a lock on the key core principles of backing up.

No matter how minimally you use your computer, If you don't, as an absolute minimum, a simple USB 'stick' back up then you are vulnerable to an expensive restore effort by someone who will charge you an arm and a leg for the time involved to restore your computer. →

"All I need the computer for is to write and send emails." This is an expression I hear often. Admittedly, back up of personal information is minimal in that case. The only thing to worry about then is if the computer itself breaks down. But that 'only thing' is one, big fat hassle. You then have to use the restore files or restore disks. I avoid that like the plague. It is like being reborn again and going all through your life to get to where you are but you have to do it is hours not years.

Unless you absolutely don't care, I do recommend that the 'minimal' user have an external back up and clone your internal hard drive on it. I takes a lot less time to replace the internal hard drive with the external hard drive clone than it does to restore a hard drive.

What do others do for back up?

(This is extracted from what others do.)

Redundancy is key with dome users! If you don't change enough to warrant frequent backups, then use an external that to copy files to regularly.

Some save to two externals to get double redundancy so as to always have 3 copies of any given file.

Some burn DVDs. But there is nothing like an external hard drive to really hold a lot of data. A DVD is ok for a lot people who have only a gigabyte of personal data at any one time. (It really would not be enough for me.)

Some use offsite/offline storage and swear by it. But for a lot of users who don't have an enormous amount of data it seems smarter to put your money in equipment inhouse. I always feel queasy about storing anything that I need immediately somewhere else. Let me give you a weak analogy. →

AND HOW DO I BACK UP?

I have a primary internal hard drive, a second internal hard drive, an external hard drive and a USB 'Stick.' periodically I clone the internal primary hard drive onto the secondary internal hard which becomes immediately availability in case the primary fails. I also clone the primary internal hard drive onto the external hard drive also, but it is not immediately available.. It has to be installed when the primary fails.

I copy My Documents (which has everything I create) onto a big (16 Gig) USB Stick usually at the end of each day so that most I can lose is a day's work.

I depend on the cloned copy of my primary onto the external hard drive to be a partially redundant backup of My Documents. I don't always adhere rigidly to the backup plan. But this is essentially my setup..



Board of Directors

President,

Jim Richardson

PRESIDENT@ccmv.net

Vice Pres. - Larry McCuistioner
VP@ccmv.net

Secretary - Darlene Gayles
SECRETARY@ccmv.net

Treasurer - Chet Hartley
TREASURER@ccmv.net

Dir. at large - Jim Semanek

Help lines: **Windows XP**

Bill Oberg—672-3387

wobergr@verizon.net

MS Word, Excel & PowerPoint

Joannie Lenz—301-6226

Joannie@RainbowFlair.com

Club Meetings:

LOCATION AND TIME

2nd and 4th Tuesdays

11:00 a.m. to 01:00 p.m.

Public Library

Sun City, CA

Many free items and loaners.

Department Leaders

Membership

Diane Robinson

MEMBERSHIP@ccmv.net

Material Distribution

Dorothy & George Metcalf

GWDJM@Verizon.net

Shareware

Position Open, Need Volunteer

Newsletter

Editor - Frank Varano

Send comments and suggestions to

EDITOR@ccmv.net

Computer Lab

Technician

Jim Richardson

Web Site

www.ccmv.net

Jim Semanek, Webmaster

WEBGUY@ccmv.net

All newsletters are posted.

Read in PDF and in color

REGISTRAR@ccmv.net

Training Registrar

Darlene Gayles

**Teachers & Assistants
are CCMV members and
volunteers..**

Here is my analogy.

In those days (are they still here?) when people would rent freezer lockers, they would buy a whole side of a cow. and it was so much meat that it was necessary to store it where there was plenty of cold storage. But if you have a few pounds of ground beef, a couple of chickens and maybe a rabbit, it is prudent to use your own freezer compartment, assuming that you did have enough room.

Here is what one reader said: "I am the King of Redundancy when it comes to backups. For the most part, I have multiple copies of backed up data (five copies at the minimum). Mostly done on a daily and/or weekly basis by automated synch programs. I have two drive image backups that are replaced every three months. Since I have the install disks for most all my applications and cloud based storage for the downloadable software I've purchased, the data is the more important. Most of it is irreplaceable, hence the redundancy. I use a lot of CDR & DVDR disks because of their cost effectiveness. For the image backups, I have them on their own dedicated 2-1/2" USB External 500Gb drives."

(I think this user has gone overboard but we really don't know why he is so involved in backups. I have seen some fantastic computer systems in places I have visited. I would not say it is an obsession but I would say that it is his life and like many of us, we can get 'carried away' with our hobbies or work.)

Here is what [Nancy](#) does. She mixes it up with a combination of external drives and server storage like this:

1. I have a separate hard drive (WD MyBook) connected to my computer. I save all my data to this drive.
2. I use Windows Home Server to back up all four of my computers. The Server is built of mostly older parts; however, the motherboard, RAM and hard drives are all used for the first time in this machine.
3. I have several (8 or 9 at last count) jump/flash/thumb drives. I keep particularly sensitive data on these, so it's backed up three times. Redundant, but it works for me.

There is a lesson to be learned here. If your data isn't in separate locations it's not truly backed up. Assuming that it's important you, it should exist in at least three places and two of those places should be offline in some form (like an external drive or DVD set that you might keep in a fire safe).

Your data is primarily on your internal hard drive. The first offline location could be a second hard drive or an external hard drive. The second off line location could be a flash drive. The third offline location could be your DVDs. The fifth offline location could be Cloud based storage.

HTG readers didn't like Cloud based storage and I don't like it either although it is fine for businesses for a variety of reasons. The happy HTG readers who liked Cloud based storage generally were working with small amounts of files and that surprises me. I personally think that they are influenced by advertising.

(See next page)

Cash Flow for The Month

12/1/11 through 12/31/11

Chet Hartley, Treasurer

Income (\$):

Contributions	32.00
Investment Inc	1.11
Shareware Freeware	0.00
Textbooks Sales	20.00
Training & Income	0.00

Total Inc. 53.11



(Continued from page 2)

Some of the users were out of this world with backups. Although very interesting I doubt that many CCMV members would benefit from more on this subject except a few words on the off-line storage systems which is heavily advertised on the radio and TV. Therefore, you are exposed to the idea of offline storage.

1. **Dropbox** is a free service that lets you bring your photos, docs, and videos anywhere and share them easily.
2. **CrashPlan** provides online data **backup**, with free unlimited online storage for personal use, and remote **backup** and disaster recovery services for businesses.
3. Mozy is a secure online backing plan for \$5.99 per month.
4. Carbonite is 'Easy recovery. Secure, Unlimited Backup for \$59/Yr

Many readers noted that they used Dropbox for small but important files and most of them encrypted them before uploading. Dropbox, being an easy and free system was popular among HTG readers.

Although Carbonite and Mozy are widely popular online backup solutions, many readers had stories of being burned by them and transitioning to CrashPlan.

If the warnings we heard from various readers about the danger of cloud based storage are distilled down into a simple missive, it's this: don't trust the cloud as your only redundancy.

This is the end of the heavily modified article. It sort of confirms my own feelings about Cloud based systems. I like to keep the side of beef in my own freezer and if my regular freezer isn't big enough I'll get a big chest freezer like I had when I had a big house in Placentia.

When I think of backups I also think of probabilities which I studied in college. So what is the probability that your hard drive ever will fail? If you use the word 'ever.' then you must answer 100%. It will fail.

The proper question to ask is what is the probability it will fail in 5 years? I don't know but for

(Continued from left column)

For practical purposes you must assume that it will fail in 5 years. Since you don't know when it will fail you must reduce the probability of losing your data by storing your data offline. Now ask: what is the probability that both primary secondary storage will fail at the same time? This is where you think intuitively that 'that's not likely to happen.

You would be interested to know that there is field in engineering that deals with MTBF (Mean Time Between Failure) in the design of equipment. Well, you might say, don't feed me that engineering crap. Like it or not you do deal with it when you buy a hard drive with a warranty of 1 year or 5 years.

The design engineers give you a warranty period which is a result of their analyses of the equipment. If the designers know that the bearings will last 3 years then you can expect the warranty to be less than 3 years because it is less than the MTBF.

So, if you buy a hard drive that has a warranty of 3 years, you gotta assume that the probability is high that it will fail in 3 years. It is not necessarily 100%. Some will last longer. Some will fail earlier. Will it be yours? Most of them will last longer. But how much longer? The company doesn't want to issue RMAs for a lot of them but their analyses tells the company how many are expected to be returned out of each production cycle.

Heck, I don't want to belabor the point any more here. I just want you to believe that you have to increase the probability as close to 100% as possible that your data will not be lost. So there! Let's change the subject!

Calculator Plus for Windows XP

From counting on fingers to desktop calculators, figuring numbers has come a long way. Add value to your Windows XP calculator with Microsoft Calculator Plus, and run apps your old pocket calculator never dreamed of. Greg Shultz tells us about this free applet.

The Calculator applet that comes with Windows XP is basically the same as the one that came with Windows 3.0. If you've always wanted an updated Calculator applet with some more advanced features, you owe it to yourself to download and install [Microsoft Calculator](#)



Calculator Plus for Windows XP continued from page 4, second column .

Microsoft Calculator Plus has a vastly improved interface over the old version, and even sports a transparency feature that allows you to see through it when it is on the screen but not the active application.

If you prefer, you can change the interface to Classic View, so it looks just like the native Windows XP Calculator while maintaining its advanced features.

In addition to the Standard and Scientific views, Calculator Plus provides you with a very comprehensive Conversion view. In fact, there are 11 conversion categories, which include such items as Length, Volume, Weight, and even Currency. (To update the available currency values, pull down the Edit menu, and select the Import ECB Exchange Rates command.) While the layout and operation of the Currency conversion feature may behave erratically, it does work.

Keep in mind that Microsoft Calculator Plus, like the Microsoft PowerToys, is a free product and not officially supported by Microsoft.

How's that for a timely subject since you will be doing your beloved income taxes soon. I just want you to be cheerful about your taxes!

A computer joke for you

"A technician went to his customer's house and found that the monitor had to be replaced. The customer immediately freaked out and got very upset at the technician.

He wondered why as he put the monitor back down. Then she blurted out in a shaky voice, 'You can't take that monitor, all of my data is in there!'

And Don't Forget It!

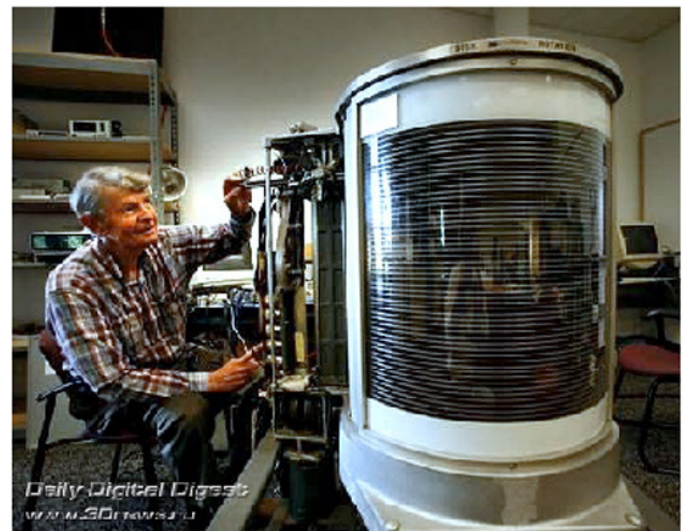
By Frank Varano

By virtue of the fact all of us have computers, I feel safe in giving you a web address for you to visit. Here it is;

<http://www.snopes.com/glurge/nodesks.asp>

This address was given to me by Andy Johnson, my good friend at The Club with whom I often discuss computers and to whom I often go for information. He thought I would be interested. Yes, I sure am and I think all of you will

(Continued at the bottom of next column.)

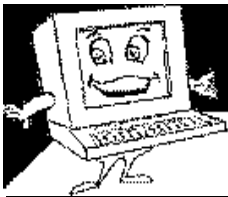


The picture is an early hard drive system. I wonder where the old stuff is now located?

(Continued from bottom of left column.)

be interested. Now, what is so unique about this web address?

I am not going to tell you here. Just rest assured that you will be surprised. And note that the URL is that of the Snopes outfit who is always debunking hoaxes. I'll leave you with that last hint. Go there, dammit! It's your homework. *End of this issue.*



Some Odds and Ends

Windows Explorer in XP

Windows Explorer allows you to view and work with the files and folders on your computer. Windows Explorer is useful for copying and moving files. The following sections explain how to use Windows Explorer.

Opening Windows Explorer

To open Windows Explorer, right-click the **Start** button, and select **Explore**.

The Exploring window opens.



Memo

I often worry that that these Odds and Ends might be too elementary to some of you, perhaps to a lot of you. I am tempted to 'push the envelope' in presenting material in these newsletters. Yet, in my everyday efforts to help others, I find that many do not even know about them. So I end up showing friends on how to do the simpler things that make you more efficient on the computer, not to show off how much I know.

Viewing files and folders

1. In Windows Explorer, click a folder on the left side of the window to display its contents on the right. Click the plus signs (+) to display more folders.
2. To change the size of either side of the window, click and drag the bar that separates the two sides. (Place the cursor on the line and poke around until you see a double ended arrow. Hold the mouse key down and drag the line to the left or right as needed.)

To quickly open a folder and display its subfolders, double-click the folder on the left side of the window.

Copying files

1. In **Windows Explorer**, select the file or folder that you want to copy.
2. On the **Edit** menu, click **Copy**.
3. Open the folder or disk where you want to paste the file.
4. On the **Edit** menu, click **Paste**. (To select more than one file or folder to copy, press and hold the **Ctrl** key and then click the items that you want to copy.)

(Continued on next page.)



(Continued from first page)

(And if you still have a Floppy)

Copying a file to a floppy

1. Insert the disk in the floppy disk drive.
2. In **Windows Explorer**, click the file that you want to copy.
3. On the **File** menu, click **Send To** and then click on the floppy drive (usually A:).

Creating a shortcut to a file

A shortcut is a link to a file. You can put a shortcut to any program, document, or printer on your desktop or in any folder and then double-click the shortcut to open the file. Shortcuts are quick ways to get to the items that you use often. For example, you can create a shortcut to your printer by using the right mouse button to drag its icon to the desktop. Then, to print a file, drag its icon onto the printer icon. Following are two different options you can use to create a shortcut.

Creating a shortcut on the desktop

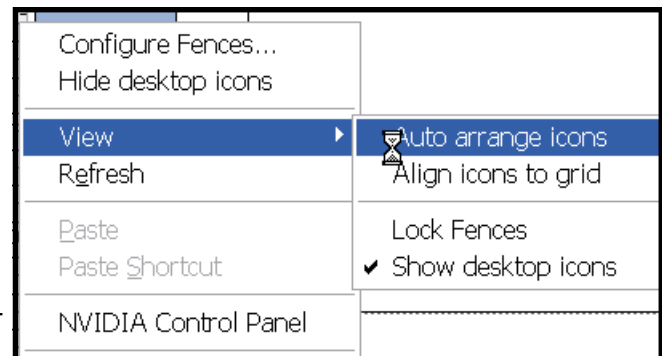
1. In Windows Explorer, select the file you want to link to.
2. Click **File** , **Send To** , and then click **Desktop as Shortcut** .
3. Find the shortcut icon on the desktop and drag it to where you want it.

Note

Some prefer to have the desktop icons in a grid which constrains a shortcut to a specific area with the other shortcuts. Frankly, I think it is a little ridiculous. If you have a bunch of icons on the desktop, that makes the icon time consuming to find when you needed it. See the picture on next page.

Bunch the desktop icons the way you want it

1. Right click on a blank space on the desktop to get a menu.
2. Click on **View**. To the right is the picture you get:
3. In the extended menu if any of the top three are checked, uncheck them.
4. Now you can move the icons around and bunch them according to categories. Later I will give you another tool that will help you in the bunching procedure.



Creating a shortcut in a folder

You can also place the shortcut in the current folder of the item for which you are creating the shortcut. After it is created, move the shortcut.

1. In **Windows Explorer**, select the file you want to link to.
2. Click **File** , and then **Create Shortcut** .
3. A shortcut for the item that you selected appears in the same folder as the item for which you were creating the shortcut.
4. Drag the shortcut to the place you want it in the left side of the **Windows Explorer** window

Note

In the picture above you will not get exactly the same menu as mine. Please note the reference to **Fences**. I will talk about **Fences** later in this newsletter.

In some previous issues of this newsletter I showed you how to work with two windows open at the same time with each window occupying part of the screen (usually half and half). The big monitors available today make that technique very useful. (On my dinky monitor it works but obviously not as well as.)

(See next



Board of Directors

President,

Jim Richardson
PRESIDENT@ccmv.net

Vice Pres. - Larry McCuistioner
VP@ccmv.net

Secretary - Darlene Gayles
SECRETARY@ccmv.net

Treasurer - Chet Hartley
TREASURER@ccmv.net

Dir. at large - Jim Semanek
Help lines: **Windows XP**

Bill Oberg—672-3387
wobergr@verizon.net

MS Word, Excel & PowerPoint
Joannie Lenz—301-6226
Joannie@RainbowFlair.com

Club Meetings:

LOCATION AND TIME
2nd and 4th Tuesdays
11:00 a.m. to 01:00 p.m.
Public Library
Sun City, CA

Many free items and loaners.

Department Leaders

Membership

Diane Robinson
MEMBERSHIP@ccmv.net

Material Distribution

Dorothy & George Metcalf
GWDJM@Verizon.net

Shareware

Position Open, Need Volunteer

Newsletter

Editor - *Frank Varano*
Send comments and suggestions to
EDITOR@ccmv.net

Computer Lab

Technician
Jim Richardson

Web Site

www.ccmv.net
Jim Semanek, Webmaster
WEBGUY@ccmv.net

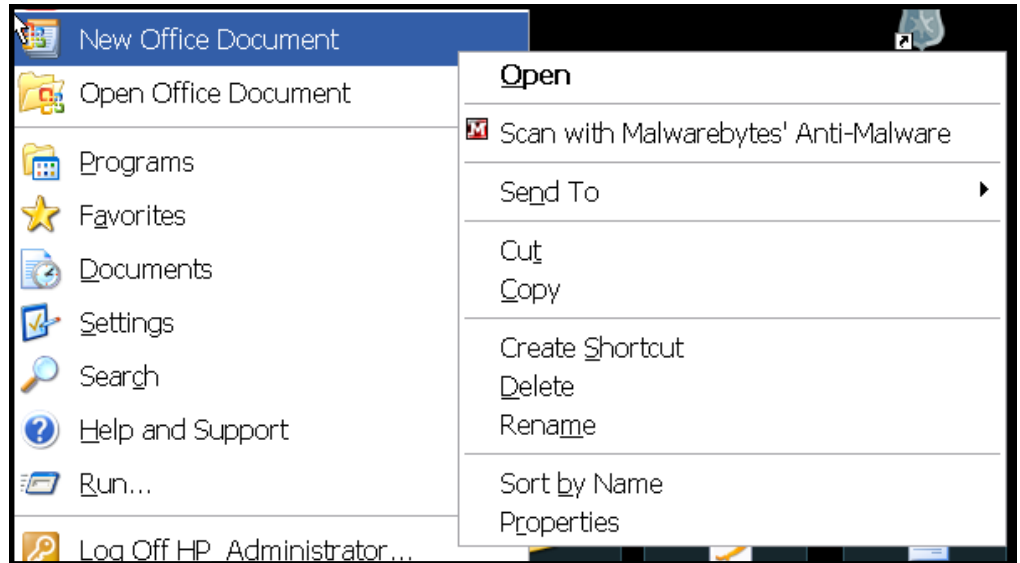
All newsletters are posted.
Read in PDF and in color

REGISTRAR@ccmv.net

Training Registrar
Darlene Gayles

**Teachers & Assistants
are CCMV members and
volunteers..**

Here is a picture of the menus for **Creating a shortcut on the desktop**. In this picture I wanted to put a shortcut of the **New Office Document** on the desktop. I right clicked on **New Office Document** to get the extended menu.. In the extended menu, the **Send To** option lets you create a short cut on the **Desktop** but also the **Create Shortcut** lets you create a shortcut right there in the **Program** list which you can drag to the **Desktop** or put it anyplace else, such as a second window open.



Thus, if you open any folder containing files, you can also create a short cut to one of the files and drag the shortcut it to elsewhere. For example, I have a large number of PPS shows wome of with have beautiful music but I want to have them quickly available on the desktop. To do this I createe the shortcuts in the folder that contains about 800 PPS shows, then dragged them into a music folder on the **Desktop**.

Note:

While manipulating files, folders and shortcuts you must be aware of difference between a short cut and a file that it is linked to. You can delete shortcuts with impunity, because you can always create another. But if you delete the file, it's gone to the Recycle bin and the shortcut at best will have a tenuous link to the file in the Recycle bin.

A file can be big as many megabytes but a shortcut is only about 1 or 2 KB. As a general rule store only shortcuts on the Desktop. And any files you put on the desktop should be there temporarily, like a holding bin for a downloaded installation program.

OK, Now lets talk about the Desktop Fence .

Some time ago I talked about desktop fences. They are called fences because each one acts like a corral holding like type of animal. In our

(Continued on the next page.)



(Continued from page 3)

analogy, our **Desktop Fence** can hold shortcuts serving similar functions. For example, Utilities, Anti Virus, Word Processing, Internet, Graphics, etc. You get the idea. The desktop fence is free. Here is how to get it.

In your Browser (**Internet Explorer** or whatever you use) type 'desktop fences download.' You will get a number of places that will handle the download but I want you to click on the Stardock one. It will look something like this::

[Stardock Corporation - Software - Fences](#)
Clear your **desktop** of clutter with **Fences** by Stardock ... Purchase/Download
www.stardock.com/products/fences - [Cached](#)

When you click on **Stardock Corporation—Software— Fences** Above you will see the picture below on that web page which gives you the free download. See the arrow pointing to **Free Download**.

Free for personal use!

No gimmicks, free is free.



- ✓ Create an unlimited number of Fence areas on your desktop
- ✓ Quickly hide/show your desktop icons with a double click
Patent Pending
- ✓ Customize the color and opacity of your fences
- ✓ Low profile, low system impact: Integrates tightly and cleanly with OS

Learn more about Fences...

Free Download

Cash Flow for Jan. 2012

Jan. 1 through Jan. 31

Chet Hartley, Treas.

Income (\$):

Contributions	95.10
Investment Inc	1.16
Tuition & Books	455.00

SUB TOTAL 551.26

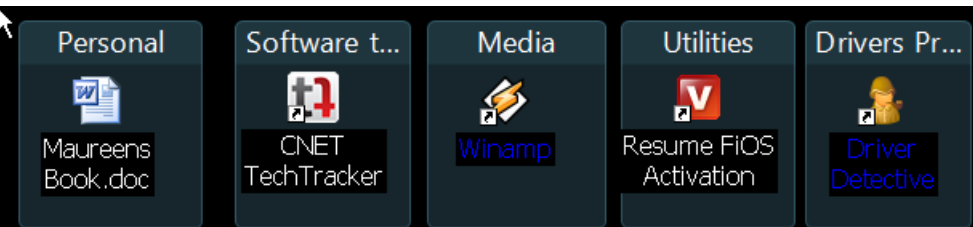
Expenses

Classroom Rent	45.00
Textbooks Buys	142.60

SUB TOTAL 187.60

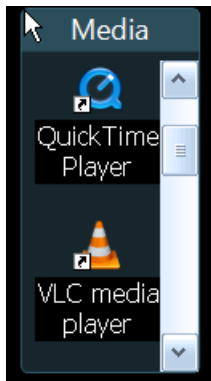
TOTAL 363.66

I'll leave the rest to you to figure out. It is pretty simple and below is a portion of my desktop using fences. These pictures will give you an idea on how to use the fences

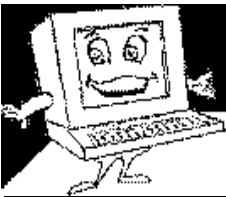


My Own Fences

Each of the **Fences** shown on the left has a scroll bar as in the **Fence** on the right. A **Fence** can be extended horizontally or vertically



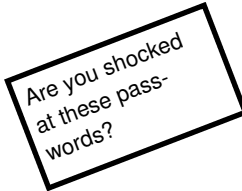
by grabbing any vertical or horizontal edge to enlarge it, up or down, displaying the shortcuts inside of the **Fence** and the scroll bar. The mouse arrow inside the **Fence** will display its scroll bar. *The scrollbar makes all shortcuts in the Fence accessible without enlarging the Fence.* Within a **Fence** shortcuts can be arranged with the most frequently used shortcut always visible as you can see in the picture above. The **Fence** system is an organized **Program** list. *The Fence allows you to sort the shortcuts by type and to arrange them by frequency of usage and to access them by scroll bar..* Without the **Fences**, the **Desktop** would be a night mare. END.



PASSWORDS (AGAIN!)

Top 10 Worst Passwords:

- | | |
|--------------|-------------|
| 1. 123456 | 6. princess |
| 2. 12345 | 7. rockyou |
| 3. 123456789 | 8. 1234567 |
| 4. Password | 9. 12345678 |
| 5. iloveyou | 10. abc123 |



Passwords

The subject of passwords is dear to my heart. Most people think of passwords as a horrible memory problem. It doesn't have to be so. (I wrote about it extensively in a previous issue of this newsletter.) I talk about it more in this newsletter.

Can you believe that people actually use such simplistic passwords? What do you use?

[Imperva](#) (my source for this article) has made several obvious recommendations, suggesting most users adopt passwords with at least eight characters and to mix those characters between upper and lower case letters, numbers, and symbols. Passwords should be simple enough that they won't be too easily forgotten, but the idea is to make cracking the code virtually impossible for either an unknown or known hacker.

Those are correct words defining a good password but a total disaster to remember. It is not easy to remember a password of totally random characters, numbers and symbols. It is bad enough to try to remember a password of letters only generated randomly. And if you have a different password for each occasion where you need it, merely typing the password in its box becomes a terrible waste of time and effort. I am a fast typist and I refuse to do it.

What do I use? For me I treat the password randomness of the password and (2) the actual box by typing or?

(1) For this part I have the random core heart until I get dementia. And just in case down somewhere but I'll forget where

(2) Typing the password where it is

So I use a password storage software pose is to enter password and other inboxes. Whenever the empty boxes appear when it is needed. **Roboform** itself the information for the first time. That

In order to follow the procedure I decide, I do have a core password of random password, by itself, it is a strong password, by itself, it is a strong password and to code of extra character(s) attached to my of the codes but they are written down someplace

With this method, I minimize the time and effort required to manually type not only the password but other information also as needed. Also I minimize the need to remember a bunch of passwords. To be sure I do follow my own procedure as in the previous issue but it is slightly modified to suit me.

But if you fail to enter the correct password (it should rarely happen), the identifying information (**Forgot Password?**) to prove who you are should be sufficiently obtuse so as to be nearly impossible for *any one else* to deduce. That is information only you know from an unforgettable event occurring in your own lifetime. One might be able learn it by searching your belongings after you get dementia. Frankly, at this point this subject becomes morbid. Reading "The Ten Worst Passwords" inspired this writing.

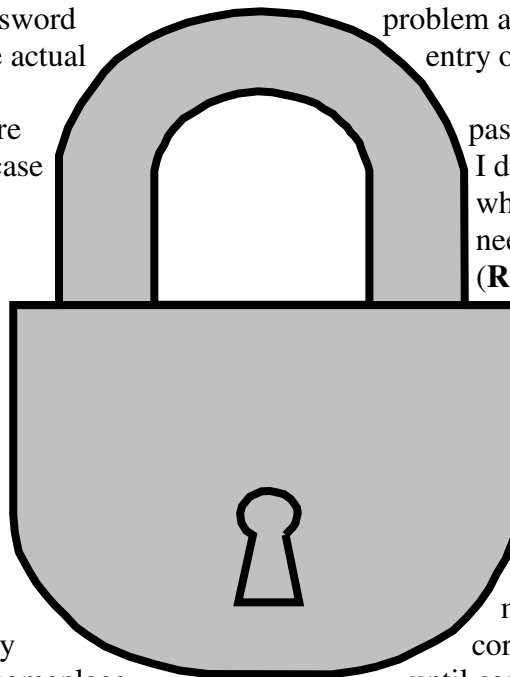
problem as having two parts. (1) The entry of the password in the password

password which I will know by I do get dementia I have it written when I do get dementia!

needed is a pain in the neck.

(**Roboform.**) But its sole purpose in the appropriate pear on a web page **Robo-** formation, including a password requires a password to access password is random.

scribed in my previous article random characters. The core word. But in order to distinguish make it even stronger, I use a core password. I memorized most until case I get dementia.





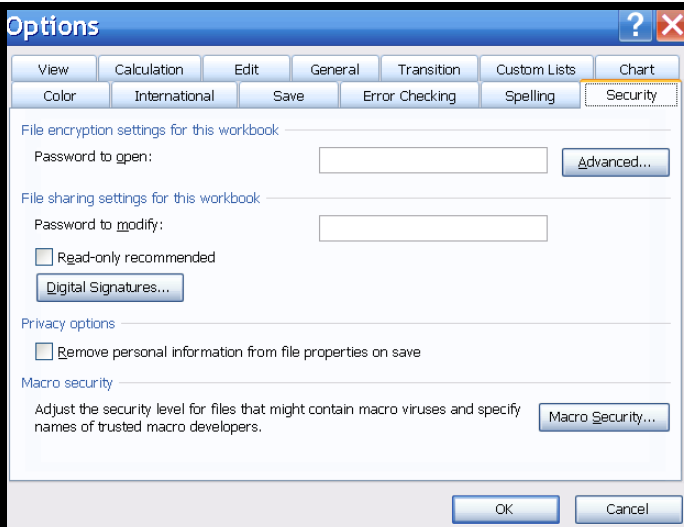
About Password Protection For a MSOffice File

He big question is 'Why would you even bother to protect a file? There are a couple reasons. If you have a spreadsheet showing your financial information, you may wish to keep it confidential from snooping relatives. Many places I go to help others on the computers, I find that I have to untangle the computer mess made by grandchildren and relatives sometimes.

Secondly, you may have some personal information that you wish to keep from prying eyes. Prying eyes? A husband or a wife may need to or want to keep some private information (not necessarily from his wife or her husband but) from visitor's eyes or from a computer repair person's eyes. In short, just ask yourself a simple question: "Do you want let anyone using this computer see this file?" Of course, if you answer 'no' then protect it from the casual snooper. This technique is not 100 percent fool proof. I'll have you know that I can recover lost passwords. It is unusual that a typical casual user would carry around with him such software.

In this article I am talking about Microsoft Office 2003' For Office 2007 or 2010 it may differ a bit.

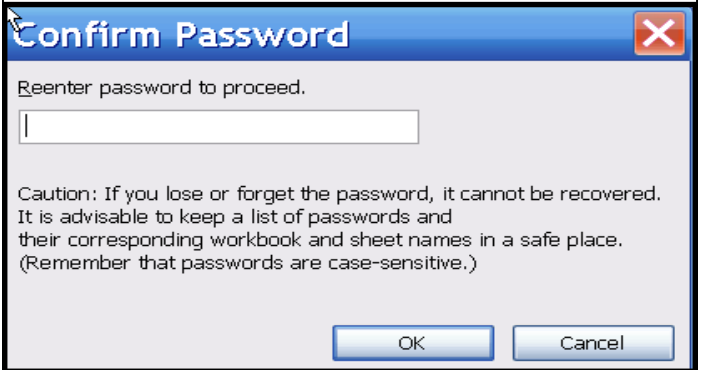
Let's say that you created a spreadsheet showing your investments and the month by month growth or attrition or whatever. It's nobody's business but yours. Let us further say that you created the file some time ago, updated it and now you want to protect it. Furthermore, you have some (snooping) relatives coming and they are computer literate. You are sure that they also will want use your computer to send emails. OK? Click on **Tools, Options** and then open the **Security** tab. Here is the **Options** window you will see:



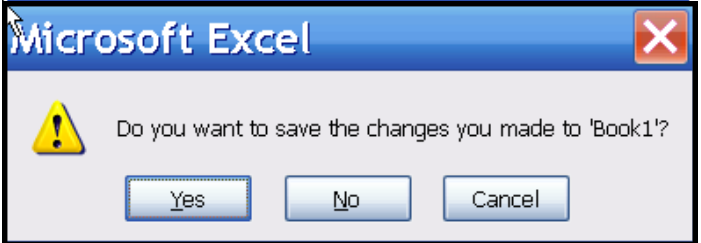
You have a box to type the password to open it and another password to modify the file. Don't bother with the second password. Having a password to open to open a file implies that you are also authorized to modify it.

If you are determined to create a thoroaly unique account use a silly password like "%TOPSECRET&" Your guests are not NSA (National Security Agency) people. A shrewd guest may guess "TOPSECRET" but not the extra characters. But read further. (See next column.)

When you click the **Save** button, you will be required to enter the password again and when you click **OK** the file will remain open. Don't let that confuse you.



When you click **OK** you will prompted if you want to save the file as shown in this window:



Of course, since you made a change you click on **Yes** so that you save it with the password attached. When you save it be sure you know where you put it *if it is a new file*. But if you already created the file It will return to its previous location when you click **Yes**. OK, now what about opening the file?

When you try to open the file you will be first presented with a window to enter the password. Here is what you will see when you try to open the file:

When you enter the password the file will open. Like magic, eh?"

In the band at the bottom **Fobiform** allows you to save the password or not. Clicking **Save** puts the



password in its catalog of passwords and other information to open the file. In order to create the above article I set up a temporary **Excel** file just for this purpose. I did not assign a name to the Excel file. Therefore the program itself assigned a default name for the file. The default name for the first **Excel** file is **Book1**

If you forget to name it you probably also forgot where you put it. If you fail to assign a name to a file you create, and you don't know where you put it, you can find it by searching for that default name.

Confusius say:

Wife who put husband in doghouse soon find him in cathouse. Man who drive like Hell, bound to get there. If you live in glass house change clothes in basement.



Board of Directors

President,

Jim Richardson
PRESIDENT@ccmv.net

Vice Pres. - Larry McCuistioner
VP@ccmv.net

Secretary - Darlene Gayles
SECRETARY@ccmv.net

Treasurer - Chet Hartley
TREASURER@ccmv.net

Dir. at large - Jim Semanek

Help lines: **Windows XP**

Bill Oberg—672-3387
wobergr@verizon.net

MS Word, Excel & PowerPoint

Joannie Lenz—301-6226
Joannie@RainbowFlair.com

Club Meetings:

LOCATION AND TIME
2nd and 4th Tuesdays
11:00 a.m. to 01:00 p.m.
Public Library
Sun City, CA

Many free items and loaners.

Department Leaders

Membership

Diane Robinson
MEMBERSHIP@ccmv.net

Material Distribution

Dorothy & George Metcalf
GWDJMJ@Verizon.net

Shareware

Position Open, Need Volunteer

Newsletter

Editor - Frank Varano
Send comments and suggestions to
EDITOR@ccmv.net

Computer Lab

Technician
Jim Richardson

Web Site

www.ccmv.net
Jim Semanek, Webmaster
WEBGUY@ccmv.net

All newsletters are posted on
www.ccmv.net.
Read in PDF and in color

REGISTRAR@ccmv.net

Training Registrar
Darlene Gayles

Teachers & Assistants
are CCMV members and
volunteers..

What About Privacy in Emails?

Gee, as long as we are talking about passwords, let's go to the realm of privacy in Emails. It does involve a password, of course. However, I'll go a step further. I want to show you how to make one of your email account private. It is private as far as the casual user who wants to snoop in your emails. Be aware, however, that what I say here is not 100% secure. Assuming the law is not in play in your email, it's OK. My primary purpose here is to give you some cloak of security regarding your email.

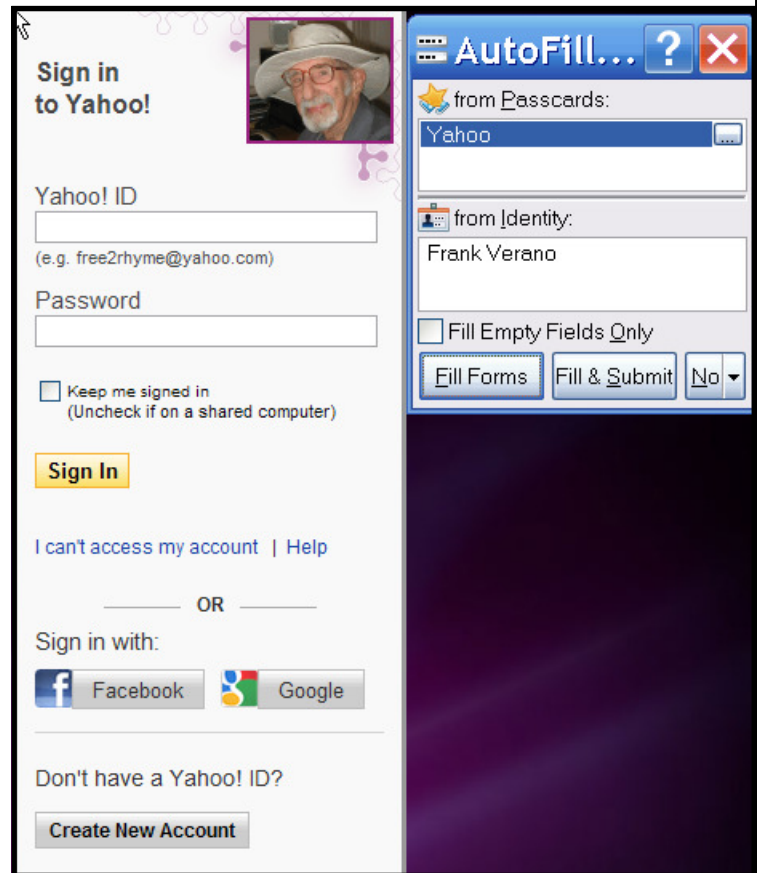
It is as simple as creating a new account that has absolutely no obvious reference to the account on your computer. That means, a casual user or (a repair person) does not even know it exists. Further, that secret account name and password is in your own head only. But your head, being fallible will need a crutch to help you remember.

(Keep in mind that you create such an account in Gmail too. The details vary on how to do it.)

Let's start by assuming that you have a Yahoo account. In this picture you can see that **Roboform** is poised to enter my account information in the left part of the window. In order to do that I click on **Fill Forms**.

Use a password handler like **Roboform** if you have to enter lots of other information besides

your username and password. Once you click on **Fill Forms** the Roboform part of the picture disappears. (See next page.)



How Roboform Works

Roboform in this picture above shows you how it works for you to reduce the amount of repetitive typing. As soon as **Roboform** sees blank forms, including usernames and password blanks this window pops up and generously offers to fill in the information for you. You must first manually enter the data in all the form blanks and then tell Roboform to **Save** it for you. **Roboform** then stores that data and associates that data with this particular website. In this case the only blanks are (1) Yahoo ID in the form of the email address and (2) the password blank.



Once I click on **Fill Forms** on the **Roboform** window, my email address and password is entered into the Yahoo form by **Roboform**. This is not my real Yahoo account.. I am using a fictional Yahoo ID account just to illustrate the procedure for this article. Not everyone will get the same sign in picture in Yahoo. This window will enter this article again later.

Click on **Create New Account** which appears at the bottom of the window to the right. You will get another Yahoo page where a number of functions are available but I show here only the pertinent part to create a new account. Here is where

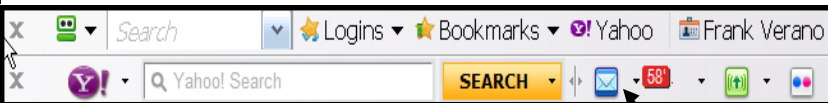
This

you type in the information for your new secret account. **PunkHead** is my self deprecating new ID. However, I selected the same password with added characters which is the only information I need to remember about the account Again I'll forget it if I get Dementia. I will show later how this works along with **Roboform**.

When you have filled out the **Re-type Password** block you will have to fill out one of those **captcha** code to prove that you are a human being and not a machine creating an account At the bottom of that page you must click on **Create Account** (not visible). After the account is created and you have control if it. Let's illustrate on how to access it so that it remains secret to you only. And perhaps it will die with you too.

Accessing Your Secret Account

Other Yahoo account users may access their email account differently. On my system, I open Internet Explorer to get to my Yahoo home page. I have also a Yahoo Toolbar. On that toolbar there is an icon for accessing my email account. Here is part of that tool bar:



I have an arrow pointing to the icon I am talking about. Click on this icon to open the **Sign in to Yahoo** window (see page three.) On my system **Roboform** windows pops up also and offers me the opportunity to fill in the form in **Sign in to Yahoo** window. I tell **Roboform** to fill in the window. But **Roboform** only has information of the existing account, not the fictional secret account. Therefore, a casual user only gets this far.

Roboform fills the form with the existing account information. To access the secret account I have to modify the sign in information as follows

- (1) change the ID from **FatHead** to **PunkHead** and
- (2) keep the same password or change it by adding one or more secret characters to it.

You can reduce the effort even further. Merely add a symbol or character to the ID and not change the password. At this stage, it is up to you to determine how much to change it. Remember it is in your head now. (Ask me for details on **Roboform**.) **Finis**

Note:

The feedback I get from others whom I help inspired me to write mostly about creating a secret account which seems like a good idea in light of the incidental exposure of email accounts to others. .

Cash Flow for Jan. 2012

Feb. 1 through Feb. 29

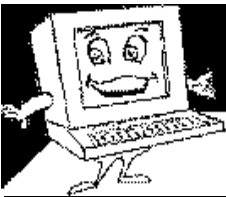
Chet Hartley, Treas.

Income (\$):

Contributions	81.00
Investment Inc	1.41
Text Books	15 00
Shareware-Freeware	10.00
SUB TOTAL	107.41

Expenses (\$)

Insurance	601.00
Classroom Rent	5.00
Textbooks Buys	0.00
SUB TOTAL	606.00
TOTAL	-498.59



Is Your Online Banking at Risk?

Extracted from Investing Answers

On Line banking is convenient, easy, and versatile. It is relatively safe but really, how safe is it?

You can do almost all of the transactions of your local bank branch quickly and easily with your personal computer or mobile device. And you don't use gas, you don't waste time driving, parking, filling out forms, and waiting in line. To me 'time' is money.

You can make deposits, transfer funds between accounts, view your checks (if you are still writing checks), view your checking history, pay bills online, send funds to a friend with just their email address and even get alerts from the bank when the credit card payment is due. And the list of options grows and grows. (But some of these things I will not do. More on that later.)

This amazing convenience also comes with risks. One (stupid or inadvertent) misstep and you could find your account has been accessed by online hackers, and in the blink of an eye your balance could be reduced to zero. (I wrote previously about using your debit card and credit card, and I also wrote extensively about passwords.)

We generally like to lump things we can do into numbered steps, so here are some of the best tips for safe online banking to ensure you're never putting your financial well being at risk.

Tip #1: Sign Up for Online Alerts. One of the best ways to keep track of your account activity is to sign up for account alerts through your bank's website preferences. Therefore you must look at your emails at least daily. Some of you don't. You can choose to be notified when your account drops below a certain balance, or if a charge appears over and beyond a certain amount, or if an external transfer has occurred on your account, or if a check you've written has finally cleared. When such activity is taking place that you didn't authorize or know about, the alerts will let you know either to your email inbox or via SMS messaging. And you can take action or not.

However, such increased communications from your bank inspire others to use techniques to fool you. You have to be darned sure you're reading legitimate email. Which brings us to the next tip.

Tip #2: Beware of Phishing Scams. Users are pretty much already aware that email scams do exist and they have only one purpose: to steal your login credentials. What bothers users more is an uncertain ability to determine that what the user sees in his Inbox is indeed a false email or if the link in the email is a legitimate one. You have to determine: "Is this or is this not legitimate?" This practice has now evolved into a more targeted scam, known as [spear phishing](#), which uses an email from a friend's hacked email account asking you to update your personal info.

The best practice when it comes to avoiding these scams is to *never, never, never* access your bank account from a link in an email. Always enter your bank's website directly through an address in the browser address bar. Type the address in the address bar or click on the bookmark that you yourself created when visiting the bank site. I like to resort to a grammatically distorted vernacular of mine, "Don't trust nobody!" Look for the "https://" at the beginning of the address. That means you are connected to an encrypted, secure network.



(Continued on next page)

About this issue

Just before I opened the template for the April issue of our newsletter I ran across an article which fits in nicely with the theme of our newsletters of late, namely, **Security**.

"This amazing convenience also comes with risks. One (stupid or inadvertent) misstep and you could find your account has been accessed by online hackers, and in the blink of an eye your balance could be reduced to zero."



(Continued from first page)

Also be sure to check the web address -- if it's not "your bank" .com, you may be on the verge of being hacked. Close out of your browser immediately.

Tip #3: Create a Unique, Complex Password. The original article said, "If you can remember your online password, it's not strong enough." I disagree with that quote from the original article. I refer you back to what I wrote a few months ago on passwords.

An optimal password is 10-14 characters long, combining upper case and lower case characters, numbers and symbols ideally. But not all sites have the same standards for passwords. Of course, "?IACpAs56IKMs" is a better password than "mypassword123." Most sites require at least 8 characters. A site may require only letters and numbers; some require upper and lower case letters; some may require at least two numbers; some don't want special characters. I could cite more standards. The answer to that problem is to have a core password, usually numbers and letters, that all sites will accept. Then have your special characters added to the core before or after or both. But you must have a system that is memorable to you. Again I refer you to my password issue.

You must write it down and keep it in a safe place. Don't store it in a document on your computer -- you're more likely to have your computer hacked with spyware than you are to have your home burglarized and your list of passwords compromised. If you do store your passwords on the computer be sure it is in a password protected software that can also be offloaded to a USB drive. The particular password to open the password protected software must be a good singular one.

I question the general advice to change your password and user name every few months. If you like fiddling around with changing a whole password and the attendant memory or logistic problem, go ahead. I don't. Likewise for your username. Choose a combination that is specific to you, but doesn't reveal your full name or anything about yourself. Think in terms of hackers, not your friends and family. How much can be obtained about you directly from your username? I don't recommend using your name. There are thousand of Lucy's. Yours might be Lucy5348. Think of what a very simple error would do to you.

Tip #4: Never Give Out Your Password to anyone. Your bank will not ask for your password over the phone or through an email. So if you receive a notification that you need to update your account, it is likely that it is a scam. Your password is your key to online safety; protect it like you would the key to your home.

Tip #5: Clear Your Browser's Cache. The cache on your Internet browser is a collection of passwords and online preferences that are stored when you visit a website.

Ideally, they make browsing the web faster, but they also reveal a lot about you if accessed by intruders. You can be selective about what you clear, but the best practice is to clear your cache every day, usually when you log off of your computer. If nothing else, clear your cache at least once a week. The best part is, it takes less than a minute to do it. Here's how:

Microsoft Internet Explorer 8.0

Choose "Delete Browsing History" from the "Tools" menu.

Make sure all of the [option](#) boxes are selected.

Select "Delete."

My USERID

My username for Verison.com is tmradius. It really stands for three mile radius and it was coined for me by a school teacher who rented a room in my house back in the 90s. She noted that I was not willing to travel farther than three miles from my home.

Following that theme, subsequently I used omradius for a second account (which stands for one mile radius), and then even later qmradius for my Yahoo account and later yet emradius for another account.

I suppose you guessed that the last two stand for quarter mile radius then even later eighth mile radius reflecting further reluctance to travel from home as I grew older and older and older. And older

(Continued on next page)



Board of Directors

President,

Jim Richardson
PRESIDENT@ccmv.net

Vice Pres. - Larry McCuistioner
VP@ccmv.net

Secretary - Darlene Gayles
SECRETARY@ccmv.net

Treasurer - Chet Hartley
TREASURER@ccmv.net

Dir. at large - Jim Semanek
Help lines: **Windows XP**
Bill Oberg—672-3387
wobergr@verizon.net

MS Word, Excel & PowerPoint
Joannie Lenz—301-6226
Joannie@RainbowFlair.com

Club Meetings:

LOCATION AND TIME
2nd and 4th Tuesdays
11:00 a.m. to 01:00 p.m.
Public Library
Sun City, CA

Many free items and loaners.

Department Leaders

Membership

Diane Robinson
MEMBERSHIP@ccmv.net

Material Distribution

Dorothy & George Metcalf
GWDJMJ@Verizon.net

Shareware

Position Open, Need Volunteer

Newsletter

Editor - Frank Varano
Send comments and suggestions to
EDITOR@ccmv.net

Computer Lab

Technician
Jim Richardson

Web Site

www.ccmv.net
Jim Semanek, Webmaster
WEBGUY@ccmv.net

All newsletters are posted on
www.ccmv.net.
Read in PDF and in color

REGISTRAR@ccmv.net

Training Registrar
Darlene Gayles

Teachers & Assistants
are CCMV members and
volunteers..

(Continued from the previous page.)

When the cache has been successfully cleared, the window should close on its own.

Tip #6: Never Access Your Bank Account From a Public Network. When you log on to a public network -- as in wi-fi access at a coffee shop or hotel -- your password, user name and possibly all of the information you type into your computer (key logging) is naked to anyone with even a little technological savvy. I know that the ubiquitous nature of laptops now and the temptation is great to take the risk. I certainly will not do it.

Only check your bank account on a secure network, such as the one at your workplace or at home where you have anti-virus protection and encrypted access. This leads us to tip number seven...

Tip #7: Use Anti-Virus and Firewall Protection. As a basic protection against malware and spyware on your computer, anti-virus software will regularly scan your computer for illegal programs intent on stealing your personal information. I almost feel embarrassed to even mention this since everybody knows that or should know that.

As an additional precaution, installing a LAN-based (Local Area Network) wi-fi router with password protection adds an additional layer of protection for your sensitive data, acting as a firewall to keep out unwanted visitors.

Windows user can download the free Avast Free Antivirus software, and those on a Mac can use the iAntivirus Free Edition. If you're not utilizing anti-virus software, download one of these programs today.

Tip #8: When in Doubt, Call Your Bank. If you're not certain that an email is legitimate or if you've noticed a questionable action in your account history, pick up the phone and call your bank's 24-hour online banking service. They'll be able to tell you if there are any items that require attention.

Additionally, closely monitor your online history for any unauthorized transactions. The sooner you can detect any possible compromises against your account, the quicker you can take action to remedy the situation.

The Investing Answer: As online banking becomes more commonplace, online scams that try to dupe you out of your login credentials are becoming more sophisticated. However, if you invest 20 minutes in these preventive measures, you can rest assured that your online accounts will remain safe.





PDF Editing

(Using a little known trick, you can take almost any secured PDF and "unlock" it for further edits and optical character recognition.)

I use Microsoft Publisher to write this newsletter. And when it is done I convert the newsletter Publisher file into a PDF format so that everybody I send it to can read it. I use one of the two free software that I have to convert the Publisher file to PDF. PDF is an Adobe software that allows you to read all the PDF files on your computer. It is free to everybody. (If you don't have it you can go to www.adobe.com to get it.

Occasionally, I need to make edits to the final PDF document like this newsletter when my proof reading fails me or when last minute changes come in. But up until now I always had to make the corrections to the newsletter while it is a Publisher document. Then I have to convert it again to PDF format. And that is time consuming and a pain in the left hearing aid.

Depending on where the PDF comes from, the PDF file may in fact be secured which means that no edits or changes can be made on the document (in the PDF form) for content integrity reasons. At this point, some engineers throw their hands up in dismay, knowing that they can't directly save the document out to a different format. Fortunately, some of the secured PDF's can be 'unlocked' using a 'print to file' trick. Actually, in using the trick the file is not unlocked, per se, but an unlocked equivalent is created that can be edited and manipulated to your heart's content.

First, open the document that you wish to unlock in Adobe Acrobat Reader and click **File**, then **Print**.

Next, in the list of printers, select "**Microsoft XPS Document Writer**" and then click **Print**.

If you try to use **Adobe's PDF** printer driver, it will detect that you are attempt-

ing to export a secured PDF out to a fresh file and it will refuse to continue. Even third party PDF print drivers tend to choke on such files. However, by using the **XPS Document Writer**, you effectively circumvent that check entirely leaving yourself with an XPS output. Now open the newly minted XPS file you have just created and simply repeat the printing process, only this time printing to PDF format

If you do not have a PDF printer to select in your list of printers, consider downloading and installing the freeware [CutePDF Writer](#) program or a program similar to it. This will allow you to set up a virtual printer that generates PDFs on the fly. (I have 4 G's in my computer.)

It is also highly suggested that you have enough RAM installed on the PC for best results. Sometimes if these files are big enough, it can take a considerable amount of time to finalize the export and your system memory can be completely overtaken.

For example, if you have to convert a 500 page secured doc to XPS and then back to PDF again, the export process can consume a lot of RAM (memory). In that case the computer's swap file is used extensively which can slow down the computer things considerably.

The other newsletter I write with a partner in The Club is often a 20 + page document. And when converting it to a PDF document, I keep my fingers crossed because these free programs are sometimes limited. It has not been a problem with my two newsletters, however. YET! Finis.



I have two PDF writers in my system that I use in creating this and another newsletter. Occasionally I have problems with converting the newsletter when I have pictures. Converting a file to PDF is apparently sensitive to the source of the pictures. When the source is in the computer itself it is OK. But if the picture is taken from a web page the PDF writer balks.

Cash Flow for March, 2012

March, 1 through March, 31

Chet Hartley, Treas.

(To be supplied in a later revision)

Income (\$):

Contributions 00.00

Investment Inc. 0.00

Text Books 00 00

Shareware-Freeware 00.00

SUB TOTAL 000.00

Expenses (\$)

Insurance 000.00

Classroom Rent 5.00

Textbooks Buys 0.00

SUB TOTAL 000.00

TOTAL -000.59



Is Your Online Banking at Risk?

Extracted from Investing Answers

On Line banking is convenient, easy, and versatile. It is relatively safe but really, how safe is it?

You can do almost all of the transactions of your local bank branch quickly and easily with your personal computer or mobile device. And you don't use gas, you don't waste time driving, parking, filling out forms, and waiting in line. To me 'time' is money.

You can make deposits, transfer funds between accounts, view your checks (if you are still writing checks), view your checking history, pay bills online, send funds to a friend with just their email address and even get alerts from the bank when the credit card payment is due. And the list of options grows and grows. (But some of these things I will not do. More on that later.)

This amazing convenience also comes with risks. One (stupid or inadvertent) misstep and you could find your account has been accessed by online hackers, and in the blink of an eye your balance could be reduced to zero. (I wrote previously about using your debit card and credit card, and I also wrote extensively about passwords.)

We generally like to lump things we can do into numbered steps, so here are some of the best tips for safe online banking to ensure you're never putting your financial well being at risk.

Tip #1: Sign Up for Online Alerts. One of the best ways to keep track of your account activity is to sign up for account alerts through your bank's website preferences. Therefore you must look at your emails at least daily. Some of you don't. You can choose to be notified when your account drops below a certain balance, or if a charge appears over and beyond a certain amount, or if an external transfer has occurred on your account, or if a check you've written has finally cleared. When such activity is taking place that you didn't authorize or know about, the alerts will let you know either to your email inbox or via SMS messaging. And you can take action or not.

However, such increased communications from your bank inspire others to use techniques to fool you. You have to be darned sure you're reading legitimate email. Which brings us to the next tip.

Tip #2: Beware of Phishing Scams. Users are pretty much already aware that email scams do exist and they have only one purpose: to steal your login credentials. What bothers users more is an uncertain ability to determine that what the user sees in his Inbox is indeed a false email or if the link in the email is a legitimate one. You have to determine: "Is this or is this not legitimate?" This practice has now evolved into a more targeted scam, known as [spear phishing](#), which uses an email from a friend's hacked email account asking you to update your personal info.

The best practice when it comes to avoiding these scams is to *never, never, never* access your bank account from a link in an email. Always enter your bank's website directly through an address in the browser address bar. Type the address in the address bar or click on the bookmark that you yourself created when visiting the bank site. I like to resort to a grammatically distorted vernacular of mine, "Don't trust nobody!" Look for the "https://" at the beginning of the address. That means you are connected to an encrypted, secure network.



(Continued on next page)

About this issue

Just before I opened the template for the April issue of our newsletter I ran across an article which fits in nicely with the theme of our newsletters of late, namely, **Security**.

"This amazing convenience also comes with risks. One (stupid or inadvertent) misstep and you could find your account has been accessed by online hackers, and in the blink of an eye your balance could be reduced to zero."



(Continued from first page)

Also be sure to check the web address -- if it's not "your bank" .com, you may be on the verge of being hacked. Close out of your browser immediately.

Tip #3: Create a Unique, Complex Password. The original article said, "If you can remember your online password, it's not strong enough." I disagree with that quote from the original article. I refer you back to what I wrote a few months ago on passwords.

An optimal password is 10-14 characters long, combining upper case and lower case characters, numbers and symbols ideally. But not all sites have the same standards for passwords. Of course, "?IACpAs56IKMs" is a better password than "mypassword123." Most sites require at least 8 characters. A site may require only letters and numbers; some require upper and lower case letters; some may require at least two numbers; some don't want special characters. I could cite more standards. The answer to that problem is to have a core password, usually numbers and letters, that all sites will accept. Then have your special characters added to the core before or after or both. But you must have a system that is memorable to you. Again I refer you to my password issue.

You must write it down and keep it in a safe place. Don't store it in a document on your computer -- you're more likely to have your computer hacked with spyware than you are to have your home burglarized and your list of passwords compromised. If you do store your passwords on the computer be sure it is in a password protected software that can also be offloaded to a USB drive. The particular password to open the password protected software must be a good singular one.

I question the general advice to change your password and user name every few months. If you like fiddling around with changing a whole password and the attendant memory or logistic problem, go ahead. I don't. Likewise for your username. Choose a combination that is specific to you, but doesn't reveal your full name or anything about yourself. Think in terms of hackers, not your friends and family. How much can be obtained about you directly from your username? I don't recommend using your name. There are thousand of Lucy's. Yours might be Lucy5348. Think of what a very simple error would do to you.

Tip #4: Never Give Out Your Password to anyone. Your bank will not ask for your password over the phone or through an email. So if you receive a notification that you need to update your account, it is likely that it is a scam. Your password is your key to online safety; protect it like you would the key to your home.

Tip #5: Clear Your Browser's Cache. The cache on your Internet browser is a collection of passwords and online preferences that are stored when you visit a website.

Ideally, they make browsing the web faster, but they also reveal a lot about you if accessed by intruders. You can be selective about what you clear, but the best practice is to clear your cache every day, usually when you log off of your computer. If nothing else, clear your cache at least once a week. The best part is, it takes less than a minute to do it. Here's how:

Microsoft Internet Explorer 8.0

Choose "Delete Browsing History" from the "Tools" menu.

Make sure all of the [option](#) boxes are selected.

Select "Delete."

My USERID

My username for Verison.com is tmradius. It really stands for three mile radius and it was coined for me by a school teacher who rented a room in my house back in the 90s. She noted that I was not willing to travel farther than three miles from my home.

Following that theme, subsequently I used omradius for a second account (which stands for one mile radius), and then even later qmradius for my Yahoo account and later yet emradius for another account.

I suppose you guessed that the last two stand for quarter mile radius then even later eighth mile radius reflecting further reluctance to travel from home as I grew older and older and older. And older

(Continued on next page)



Board of Directors

President,

Jim Richardson
PRESIDENT@ccmv.net

Vice Pres. - Larry McCuistioner
VP@ccmv.net

Secretary - Darlene Gayles
SECRETARY@ccmv.net

Treasurer - Chet Hartley
TREASURER@ccmv.net

Dir. at large - Jim Semanek
Help lines: **Windows XP**
Bill Oberg—672-3387
wobergr@verizon.net

MS Word, Excel & PowerPoint
Joannie Lenz—301-6226
Joannie@RainbowFlair.com

Club Meetings:

LOCATION AND TIME
2nd and 4th Tuesdays
11:00 a.m. to 01:00 p.m.
Public Library
Sun City, CA

Many free items and loaners.

Department Leaders

Membership

Diane Robinson
MEMBERSHIP@ccmv.net

Material Distribution

Dorothy & George Metcalf
GWDJMJ@Verizon.net

Shareware

Position Open, Need Volunteer

Newsletter

Editor - Frank Varano
Send comments and suggestions to
EDITOR@ccmv.net

Computer Lab

Technician
Jim Richardson

Web Site

www.ccmv.net

Jim Semanek, Webmaster
WEBGUY@ccmv.net

All newsletters are posted on
www.ccmv.net.
Read in PDF and in color

REGISTRAR@ccmv.net

Training Registrar
Darlene Gayles

Teachers & Assistants
are CCMV members and
volunteers..

(Continued from the previous page.)

When the cache has been successfully cleared, the window should close on its own.

Tip #6: Never Access Your Bank Account From a Public Network. When you log on to a public network -- as in wi-fi access at a coffee shop or hotel -- your password, user name and possibly all of the information you type into your computer (key logging) is naked to anyone with even a little technological savvy. I know that the ubiquitous nature of laptops now and the temptation is great to take the risk. I certainly will not do it.

Only check your bank account on a secure network, such as the one at your workplace or at home where you have anti-virus protection and encrypted access. This leads us to tip number seven...

Tip #7: Use Anti-Virus and Firewall Protection. As a basic protection against malware and spyware on your computer, anti-virus software will regularly scan your computer for illegal programs intent on stealing your personal information. I almost feel embarrassed to even mention this since everybody knows that or should know that.

As an additional precaution, installing a LAN-based (Local Area Network) wi-fi router with password protection adds an additional layer of protection for your sensitive data, acting as a firewall to keep out unwanted visitors.

Windows user can download the free Avast Free Antivirus software, and those on a Mac can use the iAntivirus Free Edition. If you're not utilizing anti-virus software, download one of these programs today.

Tip #8: When in Doubt, Call Your Bank. If you're not certain that an email is legitimate or if you've noticed a questionable action in your account history, pick up the phone and call your bank's 24-hour online banking service. They'll be able to tell you if there are any items that require attention.

Additionally, closely monitor your online history for any unauthorized transactions. The sooner you can detect any possible compromises against your account, the quicker you can take action to remedy the situation.

The Investing Answer: As online banking becomes more commonplace, online scams that try to dupe you out of your login credentials are becoming more sophisticated. However, if you invest 20 minutes in these preventive measures, you can rest assured that your online accounts will remain safe.





PDF Editing

(Using a little known trick, you can take almost any secured PDF and "unlock" it for further edits and optical character recognition.)

I use Microsoft Publisher to write this newsletter. And when it is done I convert the newsletter Publisher file into a PDF format so that everybody I send it to can read it. I use one of the two free software that I have to convert the Publisher file to PDF. PDF is an Adobe software that allows you to read all the PDF files on your computer. It is free to everybody. (If you don't have it you can go to www.adobe.com to get it.

Occasionally, I need to make edits to the final PDF document like this newsletter when my proof reading fails me or when last minute changes come in. But up until now I always had to make the corrections to the newsletter while it is a Publisher document. Then I have to convert it again to PDF format. And that is time consuming and a pain in the left hearing aid.

Depending on where the PDF comes from, the PDF file may in fact be secured which means that no edits or changes can be made on the document (in the PDF form) for content integrity reasons. At this point, some engineers throw their hands up in dismay, knowing that they can't directly save the document out to a different format. Fortunately, some of the secured PDF's can be 'unlocked' using a 'print to file' trick. Actually, in using the trick the file is not unlocked, per se, but an unlocked equivalent is created that can be edited and manipulated to your heart's content.

First, open the document that you wish to unlock in Adobe Acrobat Reader and click **File**, then **Print**.

Next, in the list of printers, select "**Microsoft XPS Document Writer**" and then click **Print**.



If you try to use **Adobe's PDF** printer driver, it will detect that you are attempt-

ing to export a secured PDF out to a fresh file and it will refuse to continue. Even third party PDF print drivers tend to choke on such files. However, by using the **XPS Document Writer**, you effectively circumvent that check entirely leaving yourself with an XPS output. Now open the newly minted XPS file you have just created and simply repeat the printing process, only this time printing to PDF format

If you do not have a PDF printer to select in your list of printers, consider downloading and installing the freeware [CutePDF Writer](#) program or a program similar to it. This will allow you to set up a virtual printer that generates PDFs on the fly. (I have 4 G's in my computer.)

It is also highly suggested that you have enough RAM installed on the PC for best results. Sometimes if these files are big enough, it can take a considerable amount of time to finalize the export and your system memory can be completely overtaken.

For example, if you have to convert a 500 page secured doc to XPS and then back to PDF again, the export process can consume a lot of RAM (memory). In that case the computer's swap file is used extensively which can slow down the computer things considerably.

The other newsletter I write with a partner in The Club is often a 20 + page document. And when converting it to a PDF document, I keep my fingers crossed because these free programs are sometimes limited. It has not been a problem with my two newsletters, however. YET! Finis.

I have two PDF writers in my system that I use in creating this and another newsletter. Occasionally I have problems with converting the newsletter when I have pictures. Converting a file to PDF is apparently sensitive to the source of the pictures. When the source is in the computer itself it is OK. But if the picture is taken from a web page the PDF writer balks.

Cash Flow for March, 2012

March, 1 through March, 31

Chet Hartley, Treas.

(To be supplied in a later revision)

Income (\$):

Contributions 00.00

Investment Inc. 0.00

Text Books 00 00

Shareware-Freeware 00.00

SUB TOTAL 000.00

Expenses (\$)

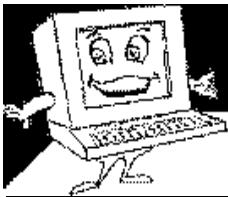
Insurance 000.00

Classroom Rent 5.00

Textbooks Buys 0.00

SUB TOTAL 000.00

TOTAL -000.59



How Do You Boil an Egg?

On second thought I think that is a stupid question. Most of you are retired, I think. If you are retired then you need an alarm clock or clock radio or something to make sure you get up in time to 'do your thing' and go to work.

On the other hand (we have a thumb and 4 fingers!) if you are indeed retired, you still need a timer. Why? Surely, not to get up in the morning. Perhaps you are not using any to get you up out of bed in the morning. But I can cite a good number of occasions where you need the time. I'll incorporate the occasions along with the material on the Egg Timer. Read on.

How to Boil and Egg.

Put a pan of water on the stove. I am sure that you know how big a pan to use and how much water to use. Once the water is boiling, lower the egg into the boiling water, set a timer for 9 minutes (for partially soft boiled egg,) and at 8 minutes remove from the fire (and turn off the fire.) At 9 minutes pour out the hot water. Now shake the sauce pan so that the egg bangs against the side of the pan which cracks the shell in many places. (See the side bar to the right of this writing.) Now fill the pan with cold water then peel the egg easily with your hands under cold water.

I really didn't need to tell you how to boil an egg. I wanted to illustrate that if you didn't keep track of the first 8 minutes, you get a different kind of a boiled egg. "Hey, that's only 8 minutes; I can remember that! Trust me!" So, do you really need to use a timer here? If you are staying in the kitchen you can keep an eye on the stove and it's only 8 minutes. If it is longer, nothing critical happens? However, it is time wasted, watching a pot boil! (Look, there is a well-worn adage for seniors that says, 'don't buy green bananas.' Well, at 94 years I find that downright insulting. I do buy green bananas. But I eat the really fast.) But what if you are not there in the kitchen?

Now consider the above scenario. First thing in the morning you are working on the computer, and you just clicked to download about 100 or more emails that piled up during the night. You know that will take some time. You haven't eaten breakfast yet, either. While you are waiting for the emails (and junk mail) to arrive you decide to put a sauce pan of water on the fire to boil a couple of eggs while the emails are downloading.

After putting a pot of water on the stove, you return to the computer. The emails have been downloaded. First, you are skimming through them. You read one, then another, then another..... and before you know it you have taken care of a most of the emails only to realize that you lost track of time and you forgot about that pot of water on the stove. The unique dry pot stink coming from the kitchen triggered your memory that you put a pot of water on the stove. You dash back to the kitchen and find that the pot is now very hot and dry.

It has happened to me. I am sure that it has happened to you. Except those of you who are otherwise perfect. In that case you don't need to read any further. Just twiddle your thumbs.

(See Next page.)

Extra!

In the past few days I had a tooth extracted. Therefore, in this issue I am not going to byte off any more than I can shoo.

When I do attend our meetings I usually sit in the back row so as to get a sense of how many are attending and how many of the back of the heads I am looking at are grey or bald. I am trying to asses what kind of audience we have. And thus what to write about in the newsletter.

I see a lot of heads with grey hair, indicating to me that the audience is in the 'senior' or 'near senior' category. I suspect some of you are still working but it looks like most are retired.

Therefore, the two items I want to write about in this issue may be very appropriate. One of the items is a simple 'Egg Timer' and the other is called 'Citrus Alarm Clock.' I ran across these two programs at CNET.COM.

Although you can use them and not pay for them, I thought both were worth the measly 5 and 10 bucks that the creator was asking.

I wrote this egg boiling instruction in another newsletter and I had a bunch of women in arms. They resented having a man tell a woman how to boil an egg. The whole story was a yoke on me



Egg Timer.

Here comes the solution, the Egg Timer. You can get it from CNET.com. Here is the **About** tab for Egg Timer. Note that it is only \$5. I read elsewhere in a review that it will not be turned off if you don't pay. Realistically, who is going to skip paying a mere 5 bucks?

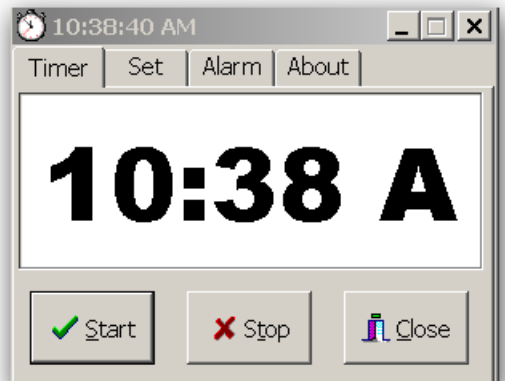
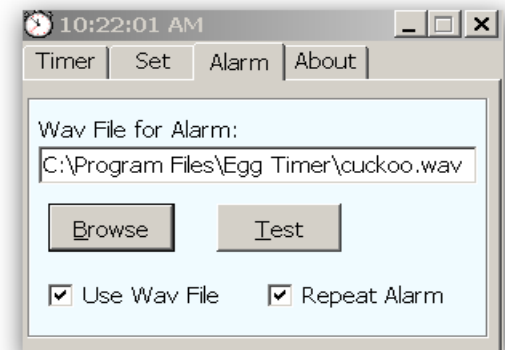
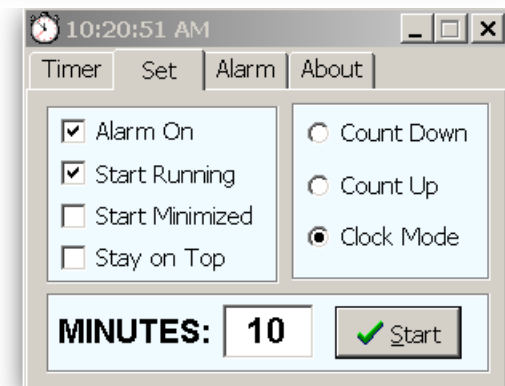
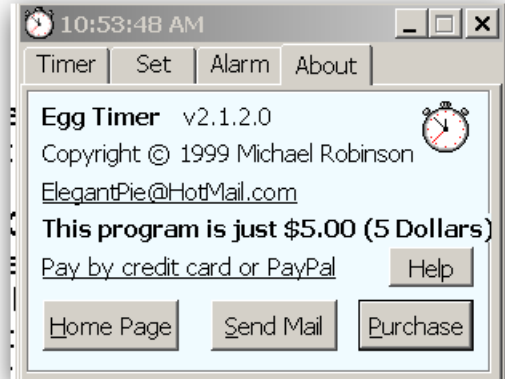
To get it, go to CNET.com and enter Egg Timer. There will be several. This one is Version 2.1.2. But look them over and pick out the one you think you'll like.

Let's look at the **Set** tab. I usually use the **Count Down** option so that if I need to remind me of an appointment or of a pot of boiling water on the stove I can be alerted so that I will not have a burned pot. Of course, you can **Count Up** too. If you have trouble counting beyond 10, this time will do it for you. If you keep the window on top you can keep an eye on it. (That is practically the same as watching the pot boil.) Generally, (at least for me) I need something to get me out of my stupor especially when writing for these newsletters. I can get so engrossed that I can lose track of time. Besides, I have trouble counting more than 10. Something has to get my attention.

Now let's look at the **Alarm** tab. How do you want to be alerted that the time set has elapsed? I chose to use the cuckoo.wave file which obviously comes with the Egg Timer. No, it will not slap you in the face to get your attention. You can dig down into your computer and select Nightingale Serenade (Sonata by Toselli not a translation.) Naturally you have to know where the path of the file (the location in your system.) Whatever you choose you have to know where it is and you have to tell Egg Timer where the file is located.

Finally, let's look at the **Timer** tab. This is where the **Count Down** or **Count Up** takes place or the **Clock Mode** showing the actual time. If any of you perfect people got this far in this write up then you can feel insulted, or feel good that at least you watch the time while you are working on the computer. I wish I were that perfect.

Just now I put a pot of water on the stove and set the timer for 10 minutes. (I need to get the first solid food in me after the tooth extraction.)





Board of Directors

President,

Jim Richardson

PRESIDENT@ccmv.net

Vice Pres. - Larry McCuistioner
VP@ccmv.net

Secretary - Darlene Gayles
SECRETARY@ccmv.net

Treasurer - Chet Hartley
TREASURER@ccmv.net

Dir. at large - Jim Semanek

Help lines: **Windows XP**

Bill Oberg—672-3387

wobergr@verizon.net

MS Word, Excel & PowerPoint

Joannie Lenz—301-6226

Joannie@RainbowFlair.com

Club Meetings:

LOCATION AND TIME

2nd and 4th Tuesdays

11:00 a.m. to 01:00 p.m.

Public Library

Sun City, CA

Many free items and loaners.

Department Leaders

Membership

Diane Robinson

MEMBERSHIP@ccmv.net

Material Distribution

Dorothy & George Metcalf

GWDJMJ@Verizon.net

Shareware

Position Open, Need Volunteer

Newsletter

Editor - Frank Varano

Send comments and suggestions to

EDITOR@ccmv.net

Computer Lab

Technician

Jim Richardson

Web Site

www.ccmv.net

Jim Semanek, Webmaster

WEBGUY@ccmv.net

All newsletters are posted on

www.ccmv.net.

Read in PDF and in color

REGISTRAR@ccmv.net

Training Registrar

Darlene Gayles

**Teachers & Assistants
are CCMV members and
volunteers..**

Citrus Alarm Clock

Ok I have another little program to use the computer instead of the alarm clock. First, I want to tell you a little true story about me and alarm clocks.

Way back in 1956 I moved to Reseda in San Fernando Valley (SFV) from San Luis Obispo where I was teaching Electrical Engineering subjects at Cal Poly. This was my first house and I was still a bachelor. I had a cat too. That's where the story begins.

I was working at the Jet Propulsion Laboratories as a loaner engineer for Motorola Research Labs in Corona. It was a long drive across SFV to work. That meant I had to get up early, like 6 am.

I had no alarm clock but I had a beautiful music system that was timed to come on about 5:45 am in the morning to one of the classical music station of that time (KCBH). Although the station was on all night, at precisely at 6:00 AM the station would begin a new broadcast day with a Roger Wagner chorale singing the Lord's Prayer which all of you are familiar with. Now you can read the box right below here.

My cat slept on the bed with me.

This was the time when a new broadcast band was just opened up by the FCC. It was assigned to FM (Frequency Modulation) type of radio frequency broadcast, (88 to 108 MHz) as opposed to AM (Amplitude Modulation,) occupying 550 to 1700 kHz.) You young squirts may not remember that.

Promptly, broadcast companies music catering to the classical music aficionados (including me) grabbed spectrum assignments for new stations because classical music was enhanced greatly due to the increased bandwidth that FM allowed to each station assignment. As a result stations playing classical music proliferated in the FM band, much to my delight.

But alas! The money was in the music of the day which (to me) was horrible. The classical stations were bought out broadcast companies and changed their format to the pop music and talk radio type of broadcast. To me it was like buying a Lexus to shop for groceries that wanted to make the most money.

There are two stations left that broadcast classical music. There is 1 one in San Diego and the other is a PBS University of Southern Cal. station. The latter depends on donations to stay in business.

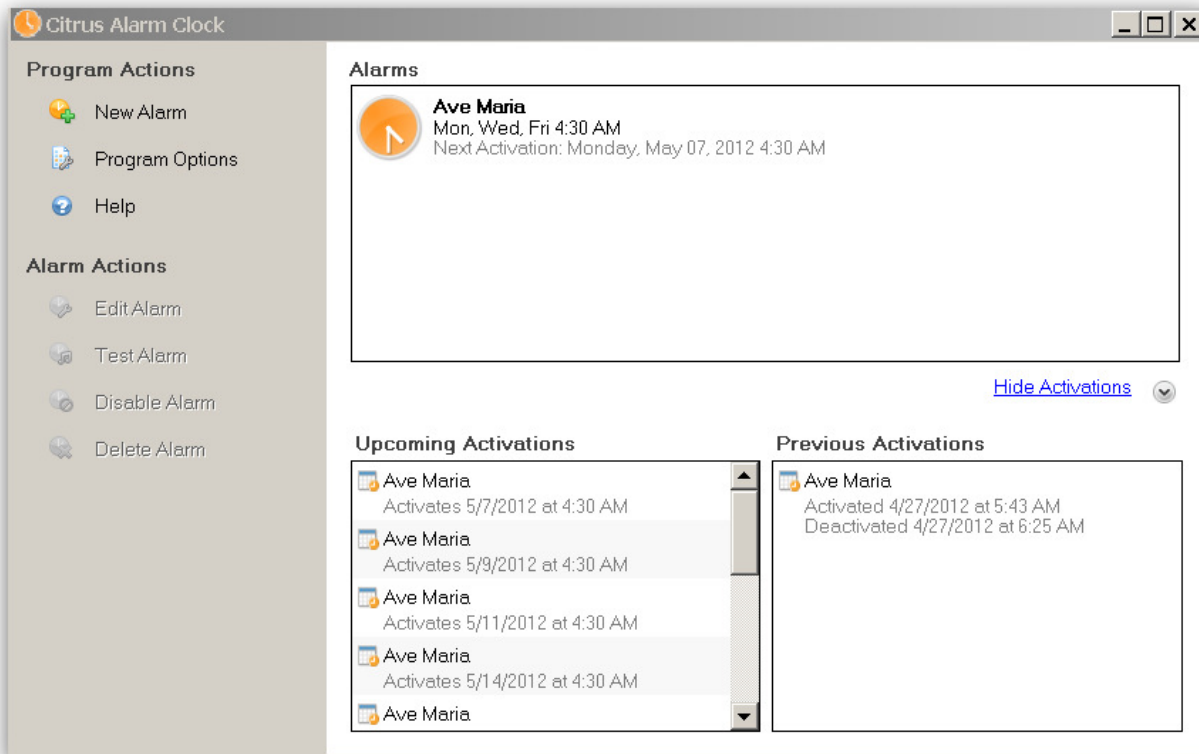
In those days I was very disciplined and when the music system played the Lord's Prayer, I would leap out of bed and head for the kitchen, feed the cat and myself. (But nowadays, I crawl out bed, reluctantly.) This is how I got into training cats for a hobby. (Now go to page 4.)

Technical Note: Armstrong invented FM radio but he really didn't understand the technical aspects of it. Radio engineers, in determining the bandwidth allocations used Fourier Transforms (a complicated mathematical method) to correctly determine the bandwidth available in FM Modulations which replaced Armstrong's simplistic assumptions, based on the AM (Amplitude Modulation.)



I noticed that my cat (Squeaky) would also leap off the bed and head for the kitchen. After all she was going to be fed! So I concocted an experiment. One morning I did not leap out of bed with playing of the Lord's Prayer. I stayed in bed. Instead my cat leaped out of bed and headed for the kitchen. I realize that the cat (and thus cats) do recognize sounds and can be trained to do various things. Subsequently I spent several years in this hobby. And some day I should tell about my 6 cats doing tricks. And also about video that was played on Betty Whites, Pet Set on a TV program long ago. That sure is a wild digression from this next topic.

Here is the basic window of the Citrus Alarm clock.



Go to CNET.com to get it. It is only 10 dollars. Instead of entering Egg Timer, enter Citrus Alarm Clock. When it comes up read the very thorough description of its functions which should tell you all about it.

I set it up at the house of a friend and it wakes her up with an orchestral rendition of Ave Maria, very appropriate for an early morning gentle introduction to a new day.

The above window is set to play Ave Maria to get me up at 4:30 on Mondays, Wednesdays, and Fridays when I go to the clubhouse to some my exercises.

I have a lap top in the bedroom and a good set of speakers there so that I can wake up in 'style.'

You might say that I practice what I preach and in this newsletter you might say that I certainly did preach a lot.

I prefer to use Music to wake me in the morning.. I never got over the Navy's general alarm to "Man the battle stations" which warns of impending battle situations. Though it's been seventy years, *I remember. (Finis.)*

Treas. Rpt for Two Months.

March. 1 through April 30

Chet Hartley, Treas.

Income (\$):

Contributions	117.00
Investment Inc.	1.99
Training, Books, Tuition	390.00
Shareware-Freeware	46.00

SUB TOTAL 554.99

Expenses (\$)

Classroom Rent	45.00
Textbooks Buys	0.00

SUB TOTAL 45.00

TOTAL 509.99