FOUNDED 1984
The Official Newsletter of THE
COMPUTERS ARE EASY USER GROUP

Abort, Retry, Ignore...

CAEUG Computers Are Easy User Group

February 2010 Suggested Retail Price $1.95 Volume XXVII Issue 2

Calendar of Events

!!! IMPORTANT !!!

*** * * NOTE * * ***
Confirmed 2010 meeting dates

February 27

March 27

April 24

May 22

Picnic Saturday June 19

**** ** ** ****
MEETING PLACE will be the Glenside Public Library

**** ****
Visitors Welcome

HOPE TO SEE YOU THERE!!
**** ****

CAEUG Meeting
:: Saturday February 27 ::

Norm Houbé will present 'Windows 7 Secrets'

New Win-7 Machine

By Larry Bothe
2/14/2010

Have you been waiting to buy a new machine because you wanted to avoid Vista? I was. In fact, I was even planning to wait for Service Pack 1 before taking the plunge. But my old XP machine was coming up with errors that only a reinstall of the operating system was going to fix, and since a reinstall is as much or more work as a new machine I decided to just go for it. Staples had a respectable machine (Compaq, dual-core 64-bit AMD processor, 3 gigs of RAM, 500-gig hard drive, Windows 7 Home Premium OS) on sale for $300 and I bought it in early December.

The actual setup and startup was a piece of cake. It's not hard to learn Win-7. Even though my new computer is actually fairly low-end, it is still much faster than the old one. The boot up is fast, and shutdown is very fast. I'm pleased with the performance. At $300 the new computer didn't come with any accessories other than a really crappy keyboard and mouse. That was OK by me; I didn't need any more low-end junk. I used my 22" LCD monitor and bought a Microsoft keyboard with a curved layout for an additional $20. Note that this keyboard is simply plug-and-play; no software to install. I have had trouble with Microsoft's whoop-de-do keyboard software in the past; I don't recommend it. My ancient Kensington

(con't on page 2)

TABLE OF CONTENTS

NO CD OF THE MONTH LIST FOR FEBRUARY DUE TO LACK OF SPACE. CD'S AND LIST WILL BE AVAILABLE AT THE MEETING ON FEBRUARY 27. SORRY FOR ANY INCONVENIENCE.

trackball mouse dated from around 1996, had no scroll-wheel capability, and the mechanical bearings were wearing out. I broke down and bought a new Kensington trackball with optical technology, 4 buttons, and a scroll ring ($68 from Amazon.com). I love it! The operation is unbelievably smooth. My venerable Altec-Lansing speaker system and recently-acquired Brother All-In-One printer-scanner-copier-fax complete my system.

This of course wouldn't be a story if I didn't have some problems to tell you about. Mine centered on obsolete software issues. I had the membership for an association I manage in a Parsons Technology program called Address Book. A-B was originally written for Windows 95 and has not been supported for years, so it shouldn't have been a surprise to me that it doesn't run in Win 7. The Professional and higher versions of Win-7 (there are 6 levels) have an XP mode you can run in, but Home Premium doesn't have it. After a brief foray into the database module of Open Office, which I found too complicated for me, I scrambled around to find another simple database program with a "front end" (user interface) for addresses and other information. I settled on Avanquest Database Professional, $40. It had several templates for entry of contact information, and allowed for customization (adding fields). It was a bit cumbersome, but I eventually got my data exported out of Address Book and into Database Professional. Some added fields and customized reports now provide me with the data I need to manage the association. There was one other program that wouldn't run in Win-7, but I got out of that by putting it on my wife's XP machine. The point of the obsolete software discussion is that you have to be wary of it in a move from XP to Win-7. Home Premium is the most widely offered version of Win-7 on new machines, and it doesn't have the XP mode. Home Premium does try to help you if certain software won't run. It asks what version of Windows it did run under, and then allegedly changes some settings to solve the problem. That routine was no help with either of my old programs. I considered upgrading my version of Win-7, but it costs $139 to go up to Ultimate (the highest level), with no choices in between. I decided that the new Avanquest software was my best solution.

There have been a slew of articles in the computer trade journals describing the features in Win-7, so I'll not repeat them here. Instead, I want to tell you about what I actually use, and one other "trick" I learned along the way. First, I have "pinned" several programs that I use most often to the Task Bar. That means they are always immediately available to me, and allow me to use the next feature I like, Aero Peek. If I hover the mouse over the icon in the task bar for a program that is open but minimized, it momentarily opens on the screen, and then minimizes again when I move the mouse away. I find that very helpful in not having to open and then minimize often-used windows.

In the same time frame that I was setting up my new machine I read an article online that described several "tricks" that I had not known about before. The one I like the best, and it's not limited to Win-7, is moving the task bar to the right or left side of your monitor. Think about this: Most of us now have a wide-screen (16:9 aspect ratio) monitor. Most productivity software is written for 4:3 monitors and the screen real estate on the right and left sides of your 16:9 monitor goes to waste. However, additional vertical space at the bottom is something you could use because that's the direction we go with full or additional pages. But your Task Bar is down there at the bottom of your screen taking up space. Why not move your Task Bar over to the right (or left) edge of your widescreen monitor? Just click and drag it to whichever side you think you might prefer. Mine is now over on the right, and after a few days to get used to it, I like it just fine. Now whatever I am working on goes all the way to the bottom edge of my monitor, and I don't have to scroll as much.

One other thing I did as part of my computer upgrade was to buy the Home & Student version of Microsoft Office 2007 ($80 from Tiger before Christmas, $140 right now). The newest version of MS Office I had was 2000, and that one didn't have PowerPoint in it, which is a module I need

(con't on page 3)

these days. Short version: I don't like MS Office 2007. It seems like they made it a lot more complicated and added "features" that most users don't need. I think it's called marketing. If you don't have a really good reason to upgrade to the 2007 version, don't do it. Open Office (**http://www.openoffice.org**) will do everything that MS Office does, for free, albeit somewhat more slowly.

I ran afoul of one known glitch in Win-7. If you add shortcuts to your desktop they may well disappear on you for some unknown reason at apparently random times. The problem has been traced to a maintenance routine that by default Win-7 runs every Sunday night. It deletes added shortcuts from your desktop. But the routine only runs if your computer is turned on at the appointed time. If not, then the routine runs the next time you turn the machine on; then your shortcuts go bye-bye. That's why the problem appears to be random, but it really isn't. To get out of it you simply disable the automatic maintenance routine in the Windows Task Scheduler. If you have the problem Google "Disappearing Shortcuts" and you'll find instructions on how to fix it.

Two final quick hints. Win-7 doesn't have Outlook Express included with it. Instead you download Windows Live Mail. I find it to work well, and you can easily import your contacts into it. Don't waste your money activating Norton or MacAfee, or whatever security program comes bundled on the new machine. Instead go to the Microsoft website and download the free Microsoft Security Essentials. It's all you need.

In my opinion it's OK to buy a Windows 7 machine now; you don't need to wait for the first service pack. Win-7 is faster and easy to use; you'll like it. The "pinning" and "aero-peek" features are useful. Be aware that some very old productivity software may not run under Win-7 unless the machine you buy has the Professional (or higher) version of Win-7 with XP mode. You can gain some useful real estate on your monitor by moving your taskbar to the right or left edge, and stay away from MS Office 2007.

Larry Bothe is an associate member of CAEUG and an honorary member of FVPCA. He was President of CAEUG for a time back in the 90's when he lived in the Chicago area. Larry presently resides in southern Indiana where he is retired from the plastics industry and currently teaches people to fly airplanes. He also performs pilot examinations for the FAA. He can be contacted at LBothe@comcast.net .

Minutes of CAEUG Meeting
January 27, 2010

Mike Goldberg called the meeting to order at 9:45 am.

There were 20 members in attendance and no visitors.

Old Business:

The Financial Report was not available due to Treasure, Lynn Johnson not being in attendance

New Business:

There was a CD of the month with many kilobytes of programs.

There were a number of issues discussed during the members Forum.

The Thumb Drives and lanyards were given to those members in attendance that had not received them in December.

There was a raffle of several items: A Canon Printer, a strong box, a Garrard turntable and stereo speakers, The Rendition DVD.

The next meeting will be on February 27, 2010. The presentation will be on Windows 7 tips.

The Picnic will be on 6/19/2010 at 11:30am.

The presentation at January's was made by Frank Braman on LINUX.

Respectfully submitted,
Al Skwara

LampPost 113
by John Spizzirri
February 21, 2010

I am going to depart from my usual citing and commenting on news in the computer sphere this month because of the gravity of this problem. It is malware sometimes called adware, ransomware, virusware, spyware, badware, cryptovirus, scamware, rogueware, and extortionware. It is a software that takes control of your computer or your data files and will not let you use it or see them without you paying a fee. I am not talking about PC Tools Spyware Doctor (1), ThreatFire (2), CyberDefender (3), or others like them. The companies making those programs advertise on radio, television, and the Internet. I, personally, do not like the way those companies operate. They diagnose a problem but then ask for money to fix the problem. You must listen to or read their ads closely to see that they only promised a diagnosis and nothing more. Malware on the other hand is picked up by going to some web sites or clicking on something in an e-mail or downloading and opening an infected file. My odyssey with malware started with a client calling me about their inability to use their computer and that pop-ups kept telling them that their machine was infected with numerous viruses and spywares. They were using Avast anti-virus software (4) with Spybot Search and Destroy anti-spyware (6). The client seldom updated either software. (Both should be updated at least once a week.) When I arrived at the client's home, I observed that the PC running XP Professional took about 10 minutes (by my watch) to boot up. The desktop background had been changed from a wedding photo to an electric green background color with a message on it that said the computer was infected with many viruses. I tried to open the Task Manager first by right clicking on the Task bar and selecting it from the pop up menu. I got an error message that stated, *"Application cannot be executed. The file taskmgr.exe is infected. Do you want to activate your antivirus software now."* To simplify subsequent references to this error message, I will use *ACBE* for "**A**pplication **C**annot **B**e **E**xecuted". I tried opening the Task Manager using Ctrl-Alt-Del key combination and got the same message (*ACBE*). I had never seen a situation where the Task Manager would not run. The client told me the only program that would run was Internet Explorer (they were using version 6). I tried to open Avast anti-virus program and got *ACBE*. The same happened with Spybot Search and Destroy also with Notepad. My next thought was to go to Trendmicro and download Housecall (6) to run it on the machine to eliminate the problem. I could not get to the Housecall web site nor could I get to any sites that would have anything to do with security, anti-virus, or anti-spyware. This symptom is common among some types of infections. It also prohibits updating anti-spyware and anti-virus programs. These crooks were very thorough. I questioned the client and found that they had gone from a normally operating computer to this, in the space of four days. They had tried various things before they called me. While we were talking, a screen popped up. The screen was very professional looking (See figure 1 on page 5). The client told me that they were continually getting that screen and another screen that was smaller having a red outline. Both screens said that a virus or viruses had been detected and that "real time protection" should be "activated". The client told me that if the PC was on for any amount of time with no keyboard activity, other windows would pop up with explicit ads for pornography sites. The client thought their son was responsible for the infection because of the porn. I was able to use an uninfected PC to search the Internet for Antivirus Live (the name of the malware). I found various web sites that explained what this infection was and how to get rid of it (7, 8, 9). The first thing I tried was to reset the proxy setting of Internet Explorer to avoid the Antivirus Live web site. I would reset them then try to get to a valid antivirus web site. To change the proxy settings in IE do the following;

(con't on page 4)

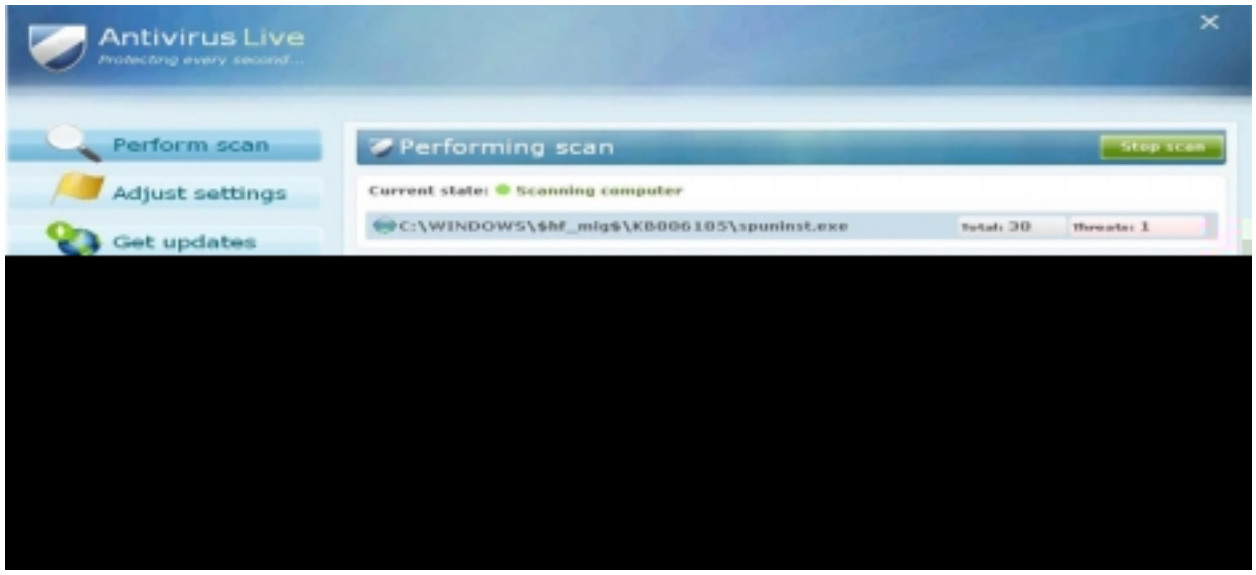


Figure 1

Run Internet Explorer, Click Tools --> Internet Options
Select Connections Tab and click to Lan Settings button
Uncheck "Use a proxy server" box
Click OK, Click Apply, Click OK
That did not work. As soon as I reset the settings, Antivirus Live would set them back again. I then tried to start the computer in safe mode by pressing the F8 key repeatedly during a resetart. I got the black screen with white lettering that lets the user select various methods of starting the computer. I first tried to start using the *"Last Known Good Configuration"*. That did not work. I then tried safe mode with networking. That did not work. I then tried safe mode. Safe mode was inoperative. Antivirus Live may have managed to prevent safe mode or something else may have been wrong with the machine. The next thing I did was get HiJack This (HJT (10)) using another machine. I copied it to a USB drive, twice. I renamed one of the copies iexplorer.exe. On the infected machine, I checked to make sure that Internet Explorer was <u>not</u> on the desktop. I copied both files on the USB to the desktop. If Internet Explorer had been on the desktop, I would have had to move it before copying the HJT files to the desktop because the file named iexplorer.exe would have overwritten the Internet Explorer program. I ran the HJT program and got the *ACBE* message. I ran the HJT program that I had renamed iexplorer.exe and it gave no error (Figure 2).

Figure 2

The Antivirus Live program had been fooled. HJT produced a log of the things it found. Most of the things it finds are necessary for Windows to run. Some of the things it finds are necessary for some startup programs to run. A few things it finds in an infected computer are dangerous. In the log's

(con't on page 6)

O4 section you may find entries like these;
O4 - HKLM\..\Run: [ekwdvdwk] C:\Documents and Settings\username\Local Settings\Application Data\username\gxymsysguard.exe

O4 - HKLM\..\Run: [RANDOM] %UserProfile%\Local Settings\Application Data\[RANDOM]\[RANDOM]sysguard.exe

O4 - HKCU\..\Run: [RANDOM] %UserProfile%\Local Settings\Application Data\[RANDOM]\[RANDOM]sysguard.exe

Note that the bracketed word [RANDOM] means 5 to 8 random alphabetic characters. The important part of the dangerous entries contain the word 'sysguard'. Once the offending lines are found, click the check box to the left of each offending line. When all the instances of 'sysguard' are found and checked, click once on the Fix Checked button. When it completes, close HJT. At this point, I should have been able to download Malwarebytes (the free version) here (see (11)). My client's computer would not let me. My client's computer displayed a screen like Figure 3.

Figure 3

I questioned my client who told me that the Internet Security 2010 was the first thing to come up. I wish I had known that there were multiple problems on the PC before I started. I downloaded Malwarebytes on another computer. Meanwhile a screen popped up like Figure 4 on my client's computer. I searched for Internet Security 2010 and how to remove it. It, too, requires a run of HJT. I found a site that explains the removal process here (12). I ran it and found entries similar to these;
F2 - REG:system.ini: UserInit=C:\WINDOWS\system32\winlogon86.exe

O4 - HKLM\..\Run: [winupdate86.exe] C:\WINDOWS\system32\winupdate86.exe

Figure 4

O4 - HKCU\..\Run: [Internet Security 2010] C:\Program Files\InternetSecurity2010\IS2010.exe
O10 - Unknown file in Winsock LSP: c:\windows\system32\winhelper86.dll
O10 - Unknown file in Winsock LSP: c:\windows\system32\winhelper86.dll
Again, I clicked the check box to the left of each offending line and clicked once on the Fix Checked button. I closed HJT. This seemed to cure most of the problems. I installed and ran Malwarebytes 'Quick Scan' Figure 5.

Figure 5

After it finished I clicked the 'Show Results' button and then clicked 'Remove Selected' see Figure 6 on next page. Once these bad files are removed, I installed and ran cCleaner (13) and fCleaner (14). After a reboot, the PC ran well. I updated Avast and Spybot Search and Destroy. I told the client to run complete scans

(con't on page 7)

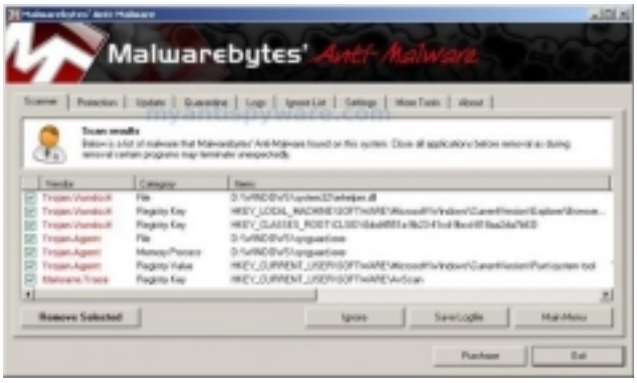


Figure 6

with both as soon as I left and at least every two weeks there after. I did further research and found these sites that explain in part what this type of rogue software does (15, 16, 17). I found that there are about 250 different versions (18) of this type of rogue programs with names like Malware Defense, Desktop Defender 2010, Security Tool, Cyber Security, PC Live Guard, Personal Security, Antivirus 2010, Antivirus PC 2009. You may notice that some of the names are similar to retail antivirus programs. These types of programs have been around for about four years. They have become much more sophisticated in the last year using slick professional looking pop up screens. These rogue programs are from Russia or Eastern block countries. They want you to buy the program so that they can get your credit card number. If you buy the program, I doubt that the program will fix your computer. The criminals have no incentive to undo what they have done.

Try this at your own risk:

If you wish to test the anti-virus software on your machine, go to this site (19). If your product is working properly, you will get a notice with the name of your product in the title bar warning you that the web site is rogue. Before you go to that site, back up your data files. When I went to this website, AVG found and stopped an infection and displayed this screen. See Figure 7.

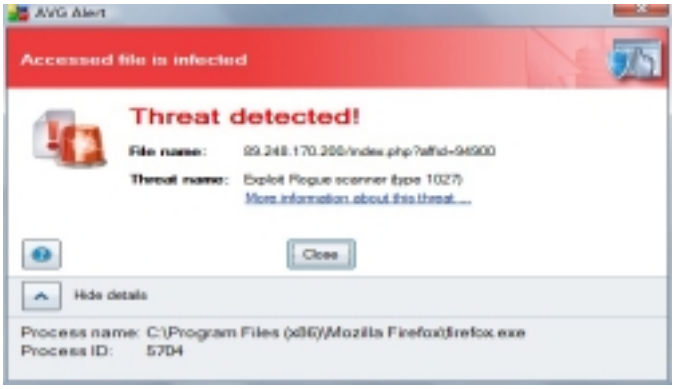


Figure 7

This web site might be down by the time you read this. Rogue web sites are shut down and reopened constantly.

Since my first encounter with this type of malware, I have seen three more instances of it. Helpful web sites that I used in the problem diagnosis were The Elder Geek (20), Bleeping Computer (21), How to Geek (22), 2-Spyware (23), 411-spyware (24), Geek Police (25), My Anti Spyware (18), McAfee Site Advisor (26), Audit My PC (27), and Youtube (28). In previous years I used Castlecops (29), which was run by voluteers. Microsoft (MS (30)) hired the leader of Castlecops and no one else had the time or inclination to keep it going.

1) **http://www.pctools.com/spyware-doctor-antivirus/download/?ref=google_pctools&gclid=CNDQvbWf9Z8CFRTyDAodEi3BZA**
2) **http://www.threatfire.com/**
3) **http://www.cyberdefender.com/**
4) **http://www.avast.com/index**
5) **http://www.safer-networking.org/en/index.html**
6) **http://housecall.trendmicro.com/**
7) **http://www.howtogeek.com/howto/8693/how-to-remove-antivirus-live-and-other-roguefake-antivirus-malware/**
8) **http://www.2-spyware.com/remove-antivirus-live.html**

(con't on page 8)

9) **http://www.myantispyware.com/2009/12/07/how-to-remove-antivirus-live-uninstall-instructions/**
10) **http://go.trendmicro.com/free-tools/hijackthis/HijackThis.exe**
11) **http://www.myantispyware.com/2008/08/28/malwarebytes-anti-malware-free-spyware-malware-trojan-remover/**
12) **http://www.bleepingcomputer.com/virus-removal/remove-internet-security-2010**
13) **http://www.ccleaner.com/**
14) **http://www.fcleaner.com/**
15) **http://www.2-spyware.com/ransomware-removal#parasites**
16) **http://electronics.howstuffworks.com/how-to-tech/how-to-remove-computer-virus.htm/printable**
17) **http://blogs.howstuffworks.com/2010/02/01/ransomware-holds-your-computer-hostage/**
18) **http://www.myantispyware.com/**
19) **http://89.248.170.200/index.php?affid=94900**
20) **http://www.theeldergeek.com/**
21) **http://www.bleepingcomputer.com/**
22) **http://www.howtogeek.com/**
23) **http://www.2-spyware.com/**
24) **http://www.411-spyware.com/**
25) **http://www.geekpolice.net/**
26) **http://www.siteadvisor.com/**
27) **http://www.auditmypc.com/**
28) **http://www.youtube.com/watch?v=NzbQrn7_xco&feature=related**
29) **http://www.castlecops.com/**
30) **http://www.microsoft.com/**

Between you, me and The Lamp Post that's all for this month.

Minutes of CAEUG BOARD Meeting
January 27, 2010

Mike Goldberg called the meeting to order at 12:18pm.

Those in attendance were Roger Kinize, Al Skwara, John Spizzirri, Billy Douglas, Mike Goldberg, and Kathy Groce.

Old Business:
-- Roger will buy 10 more thumb drives at $8.00 each to complete the delivery of thumb drives to members. Al will mail out thumb drives to those that have not received one.
-- Al will print some additional Coupons for Club publicity.

New Business:
-- The Picnic will be 6/19 2010.
-- Mike will contact Peter Nicchia to see if he will want to stand for election.
-- The February Presentation Topic will be WINDOWS 7 Secrets.
-- March Presentation Topic will be Optical Media.
-- In February we will need to appoint a nominating committee.
-- We will consider an Amendment to the Constitution to eliminate the Newsletter Mailing function; we are 100% digital newsletter delivery.

Respectfully submitted,
Al Skwara

CAEUG OFFICERS

President	Mike Goldberg
V.P. (Programs)	Roger Kinzie
Secretary	Al Skwara
Treasurer	L. Johnson
Newsletter Editor	Kathy Groce
Membership Chairperson & Circulation Manager	Pete Nicchia
Board Member	Billy Douglas
Webmaster	John Spizzirri

Reminder:
You'll get better, faster service if you use CAEUG in the subject of your e-mail.

ABOUT THE NEWSLETTER:

This printed version of our newsletter was laid out using **Adobe's Pagemaker Version 7.0** for Windows.

The opinions expressed in this newsletter are not necessarily those of the CAEUG Officers, members or other contributors. CAEUG, its officers, newsletter editor, authors or contributors are not liable in any way for any damages, lost profits, lost savings, or other incidental or consequential damage arising from the use of the information provided herein. Every reasonable effort has been made to confirm the accuracy of the contents of this newletter, but that accuracy is not guaranteed.

Permission is granted to reproduce any or all parts of this newsletter for personal use. Also granted is permission to reproduce for publication any part of this newsletter provided that a copy of the publication is mailed to CAEUG, immediately following publication and CAEUG is given credit.

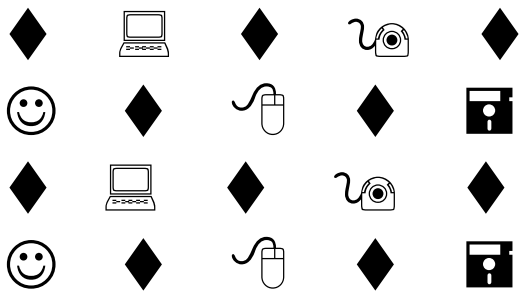
The CAEUG newsletter is published eleven times annually. Contributions by members are encouraged and will be gratefully acknowledged in the newsletter. We have a policy of exchanging newsletters with other users groups across the nation. Several CAEUG member articles have already been picked up and reprinted.

Beginner's SIG

Ask questions and discuss computer experiences
Such as:

1. New to Computers? (basic topics)
2. How to use the Web or download information
3. How to install hardware/software
4. Discuss how to troubleshoot hardware conflicts, learn boot up emergency tricks
5. What do you want to know??

SIG meets before regular meeting from **9:05 to 9:45**



MEMBERS HELPLINE

Any member with a specific expertise can volunteer to be on the Members Helpline.

Beginner Helpline . . . . . Billy Douglas

Beginner hardware problems . . . Dick Fergus

Hardware problems, ...2K, XP & Linux
. . . . . John Spizzirri

CD OF THE MONTH FORMAT: Is now available in **two** (2) flavors. The **Basic CD** will be packed with the standard items, while the **CD of the Month** will have NEW and updated items.

NEW Money Saving Offer for CD of the Month
Pre Order + Prepay = SAVE $$

The club will offer the CD of the Month on a pre order, prepaid basis. The charge will be $70.00 a year for 9 months. This is $20 annual savings over buying them for $9 each month. Lynn Johnson, the treasurer, will keep track of anyone placing a 9-month order.

MAIL Request - There will be a $2.00 mailing charge per CD

Membership Costs.....

	First Yr.	Renewal
Individual	$25.00	$20.00
Family	$30.00	$25.00
Corporate	$30.00	$25.00
Associate	$20.00	$15.00

CAEUG
P. O. Box 2727
Glen Ellyn, IL 60138

FIRST CLASS MAIL

---

* ! ** ! ** Notice Date information ** ! ** ! *

The next **REGULAR** meeting will be held at the **Glenside Public Library**
25 East Fullerton in Glendale Heights, Illinois
starting 9:45am next meeting on

Saturday February 27, 2010
Windows 7 Secrets

CONFIRMED Future Meeting dates for **2010** at Glenside Public Library
The following Saturdays ::
March 27, April 24, May 22, Picnic Saturday June 19

Meeting Location and Special Accommodations

The Glenside Public Library address is at 25 E Fullerton Avenue, Glendale Heights, Illinois. The Library location is Fullerton between Bloomingdale Road (stop light intersection) and Schmale Road (stop light intersection) on the south side of Fullerton. Fullerton is parallel to North Avenue (Route 64) and Army Trail Road. North Ave. is south and Army Trail is north of Fullerton. Please park away from the building. Thank you.

The meeting(s) are not library sponsored and all inquiries should be directed to Mike Goldberg at MikeGold60137@yahoo.com. Individuals with disabilities who plan to attend this program and who require certain accommodations in order to observe and/or participate in the program are requested to contact CAEUG president, Mike Goldberg at MikeGold60137@yahoo.com, at least five (5) days prior to the program, so that reasonable accommodation can be made for them.

Hope to see you there!