Chesapeake PC Users Group

# THE PRINTER

*Celebrating 25 Years of Users Helping Users*

## PRESIDENT'S CORNER

# HAPPY SNOW YEAR!

**Happy New Year Everyone!**

I hope everyone enjoyed the January meeting. We have a great set of meetings planned for the next few months, beginning with the February 0 no that the March meeting. Just a reminder, the elections will be taking place at the next meeting. I do plan to run for the office again, but as with all offices, it is up for vote.

I would encourage anyone who has an interest in helping to guide the Users Group to please run for an office. New blood is always welcome, and needed, on the Board of Directors.

**February 10th Meeting – Computer buying Tips and Tricks**

We are shifting the meeting around a little from last month. It seems that many people would like to replace their old computers, but have questions as to what to look for. Fran Damratowski will lead a panel on computer buying advice and present some of the highlights as to what to look for.

**March 10th Meeting – Windows 7 Tips and Tricks**

This meeting will be the lead into the formal Windows 7 course that Sam Shepherd will be teaching beginning April 6. As folks upgrade their operating systems, many would like to know how to use all of the new features. Sam will go over some of the more interesting points that will help folks right away. See the tentative Course Schedule on page .

**April 14th Meeting – PhotoBook design and layout by Mike Delucia**

**May 12th Meeting – Sketch Up by Kathy Walker and Bill Somers**

**June 2nd Meeting – Activating TechNet**

More details will be forthcoming about the later meetings and as always, your input is welcome for upcoming meeting topics.

***I hope to see you at the upcoming meetings!***

***Michael***

***ps - February's presentation will be postponed until March. So March's meeting will be a twofer.***

***Inclement weather - Remember to check the Anne Arundel County Public School website - www.aacps.org/ - for school closings at the first signs of the dreaded and much feared white stuff. You can even sign up for email alerts!***

# From the Wonderful Folks at Smart Computing

"Reprinted with permission from *Smart Computing*. Visit www.SmartComputing.com/Groups to learn what *Smart Computing* can do for you and your user group!"

• **Windows 7 Shortcuts:** In Windows 7, if you have several open windows, grab the top of the frame of one window and shake it back and forth. The rest of the open windows will minimize. The keyboard shortcut for the same function is WIN (the Windows logo key)-Home. Now press WIN-Down arrow to minimize the current window and WIN-Up arrow to maximize it. Pressing WIN-Right arrow or -Left arrow will dock the current window to the right or left edge of your Desktop.

• **Restart Your Computer For Better Performance:** Many users log off their computer every night as a way to try to keep unwanted people from accessing their files on the computer. Instead of logging off of your computer every night, restart it. In doing so, you will enable Windows to refresh itself and remove temporary files. It will also let your computer free memory and other resources that some of your hardware and software will not release, thereby making your computer work more smoothly and at a faster rate.

• **Going The Distance:** If your current router has trouble distributing Wi-Fi (or Wi-Fi at an adequate speed) to every room in your house, look for a model that has two or three antennas and MIMO (Multiple Input, Multiple Output) technology. These features can increase the range and reliability of your Wi-Fi signal, improving the distribution of Wi-Fi across large houses or to devices that are

# OFFICERS

***President***

**Mike Young.....(410) 551-4411**
**president@chesapeakepcusersgroup.org**

***Vice President***

**Mike Regimenti.....(301) 509-6091**
**vice-president@chesapeakepcusersgroup.org**

***Co-Treasurers***

**Kathy Walker (410) 410-266-6317 Bill Somers (410) 647-9429 treasurer@chesapeakepcusersgroup.org**

***Secretary***

**Kris Johnson.....(410) 544-8706**
**secretary@chesapeakepcusersgroup.org**

***Publisher/Editor***

**Mike Regimenti.....(301) 509-6091**
**editor@chesapeakepcusersgroup.org**

## CHAIRPERSONS

***Programs***

**Craig Barlow.....(410) 266-6829**
**programs@chesapeakepcusersgroup.org**

***Education***

**Sam Shepherd.....(410) 647-6077**
**education@chesapeakepcusersgroup.org**

***Membership***

**Margaret Duggan.....(410) 647-2722**
**membership@chesapeakepcusersgroup.org**

***Public Relations***

**Kris Johnson.....(410) 544-8706**
**pr@chesapeakepcusersgroup.org**

## SPECIAL INTEREST GROUPS (SIGS)

***New Users Group***

**Sam Shepherd.....(410) 647-6077**

***MidShore Computer Users Group SIG***

**George Ireland ..... (410) 745-2361**
**mscug@chesapeakepcusersgroup.org**

***Technology SIG***

**Mike Regimenti.....(301) 509-6091**
**internet@chesapeakepcusersgroup.org**

***Computer Refurbishing SIG***

**Fran Damratowski.....(410) 544-7047**
**refurbishing@chesapeakepcusersgroup.org**

***Webmeister***

**Mike DeLucia.....(410) 721-2991**
**webmeister@chesapeakepcusersgroup.org**


# OPERATING SYSTEM COURSE

## Tentative Course Schedule

The course will be given on eight consecutive Tuesdays starting on April 6, 2010. The class will meet in classroom ??? in the Severn River Middle School at 7:00 pm and will run to approximately 9:00 pm. The class will be taught using a single computer projected for all to see. The instructor will use Power Point as an aid to the lecture and the slides material will be available as a handout before class for note taking. The computer will also be available to demonstrate Windows 7. Cost of the course will be $50.00.

**Week 1 - April 6, 2010 (Tuesday after Easter)**

- Selecting your version.
- How to install and/or upgrade.
- Compatibility: Virtual Mode, XP Mode.
- User accounts & UAC.

**Week 2 - April 13, 2010**

- Compare the new look to the old: What are the choices?
- Start Menu: Customize, Jump List.
- Gadgets.
- Task Bar: Customize.
- Personalize the Desktop.

**Week 3 - April 20, 2010**

- Libraries, Folders, Documents, Files.
- Virtual Folders.
- Cloud computing.

**Week 4 - April 27, 2010**

- The new Windows Explorer: Understanding and using.
- Making it work for you.
- Customize Windows Explorer.

**Week 5 - May 4, 2010**

- New Search Tool: Use, Filter & Save.
- Configuring.
- Folder Options.
- Compressed Folders.

**Week 6 - May 11, 2010**

- Networking.
- Browsing the Web.
- E-mail.
- Live services.

**Week 7 - May 18, 2010**

- Performance tools.
- Monitoring.
- Improving memory.

**Week 8 - May 25, 2010 (Tuesday before Memorial Day)**

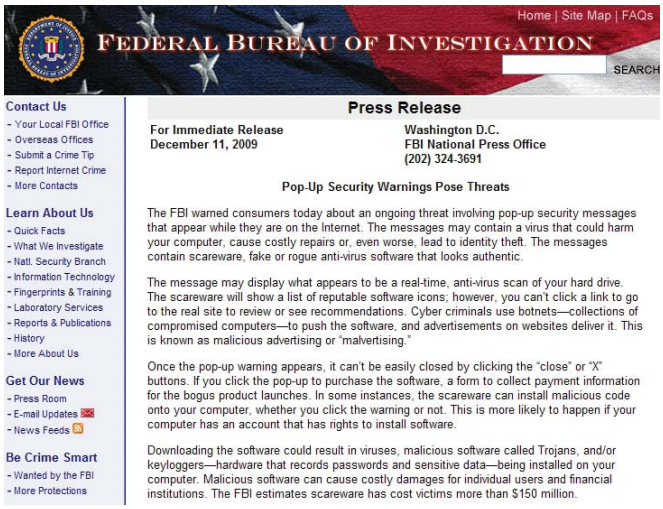
- File and PC backup.
- Troubleshooting.
- Third party tools, eg: Firefox, Security Essentials.

# Scumware and Scareware Warning and Removal

*by*
*Ira Wilsker*

WEBSITES:
http://www.fbi.gov/pressrel/pressrel09/pop-up121109.htm
http://www.usatoday.com/tech/news/2009-06-09-cybergangs-scareware-hackers_N.htm
http://www.networkworld.com/news/2009/101909-scareware.html
http://blogs.zdnet.com/security/?p=4297
http://online.wsj.com/article/SB123976230407519659.html
http://www.malwarebytes.org/mbam-download.php
http://www.malwarebytes.org/mbam/database/mbam-rules.exe
http://www.emsisoft.com/en/software/free/
http://download1.emsisoft.com/a2usb.zip
http://www.threatfire.com
http://www.microsoft.com/security/malwareremove/default.aspx

Many of you have had the experience of having a popup or window open on your computer that tells you that your computer is infected with a substantial quantity of viruses, worms, Trojans, and other forms of spyware. Typically, these warning messages, which may appear to be authentic Windows warnings, instruct the user to "click here" to remove the malware. Upon clicking, another window opens which solicits a fee, typically $29.95 to $49.95 (or more) to purchase software to remove the infection. The software being offered has an attractive and professional looking interface, and often carries a name that is intended to inspire confidence, sometimes even being similar to reputable product names that we have heard of before. Trying to close the window often results in the popup reappearing again, almost instantly. If we choose to ignore the warning or close it, it may continue to reappear whenever we click on a webpage, open our own already installed programs or security software, or randomly. These warnings may "scare" us, or become so intrusive that many of us will pay to purchase the recommended software to clean our computers of malware and restore the usability of our machines. By doing so, at a minimum, we just became the victim of a scam that according to the FBI has duped Americans out of an estimated $150 million.


Home | Site Map | FAQs
FEDERAL BUREAU OF INVESTIGATION
SEARCH

Contact Us
- Your Local FBI Office
- Overseas Offices
- Submit a Crime Tip
- Report Internet Crime
- More Contacts

Learn About Us
- Quick Facts
- What We Investigate
- Natl. Security Branch
- Information Technology
- Fingerprints & Training
- Laboratory Services
- Reports & Publications
- History
- More About Us

Get Our News
- Press Room
- E-mail Updates
- News Feeds

Be Crime Smart
- Wanted by the FBI
- More Protections

**Press Release**

**For Immediate Release**
**December 11, 2009**

**Washington D.C.**
**FBI National Press Office**
**(202) 324-3691**

**Pop-Up Security Warnings Pose Threats**

The FBI warned consumers today about an ongoing threat involving pop-up security messages that appear while they are on the Internet. The messages may contain a virus that could harm your computer, cause costly repairs or, even worse, lead to identity theft. The messages contain scareware, fake or rogue anti-virus software that looks authentic.

The message may display what appears to be a real-time, anti-virus scan of your hard drive. The scareware will show a list of reputable software icons; however, you can't click a link to go to the real site to review or see recommendations. Cyber criminals use botnets—collections of compromised computers—to push the software, and advertisements on websites deliver it. This is known as malicious advertising or "malvertising."

Once the pop-up warning appears, it can't be easily closed by clicking the "close" or "X" buttons. If you click the pop-up to purchase the software, a form to collect payment information for the bogus product launches. In some instances, the scareware can install malicious code onto your computer, whether you click the warning or not. This is more likely to happen if your computer has an account that has rights to install software.

Downloading the software could result in viruses, malicious software called Trojans, and/or keyloggers—hardware that records passwords and sensitive data—being installed on your computer. Malicious software can cause costly damages for individual users and financial institutions. The FBI estimates scareware has cost victims more than $150 million.

If it was only money that was lost, the damage would be bad enough, but the infection and hijacking that produced the popups and warnings in the first place may have also destroyed our existing antivirus software, deactivated our firewall, transmitted our vulnerabilities to unknown miscreants, and made our computers vulnerable to continued attacks. Purchasing, downloading, and installing this rogue software may possibly also open us up to even worse attacks such as turning our computers into spam sending zombies that can generate massive income for the zombie master. Other identified hazards of this software may include the installation of keylogging software to steal our usernames, passwords, and credit card information to be sold on illicit websites for criminal purposes including credit card fraud and identity theft. Simply put, your computer may physically be in your home, but for all practical purposes it belongs to some crook somewhere

*cont'd on Page 8*

*cont'd from page 4*

# Scumware and Scareware - cont'd

who in reality has control over it for nefarious and pecuniary reasons.

This may sound like science fiction or the theme of an action movie, but the scenario is a sad reality that has been repeated on millions of personal computers. The victims of this scam may have visited websites, often legitimate websites, that have been victimized themselves by hackers who installed the dangerous code that can infect a computer by simply opening a webpage, causing the malware to be loaded onto the victim computer. In some other cases the infection can occur by clicking on an apparently authentic looking online advertisement, opening an email attachment, or simply doing other online activities. A lot of the victims clicked on links posted on Twitter, YouTube comments, instant messages, links illicitly planted in search engine results, and ads posted on legitimate websites. Many of these "drive-by" infections are explicitly designed to evade antivirus and anti-spyware software, and once on the computer, may destroy the ability of the antivirus and anti-spyware to provide any future protection. The authors of this malware are smart, and if the legitimate security software is indeed neutralized, it will still appear to load and even update, as well as display the program icon in the tray by the clock, giving the user a false sense of security that his computer is still protected. Not just is the computer no longer protected, but some of the malware sends out invitations to other cyber crooks to visit the "buffet" of purloined computers and help themselves to the bounty of goodies that may be available, as well as allow them to install additional spyware and malware on the victimized computer.

Some of this illicit activity is done in a "multi-level marketing" or pyramid model where cyber criminals can pay the master crook for access, and then resell this access to others, who can then sell to others, each paying a fee or commission that is passed up the line to the master crook. This is not some obscure threat or risk that we face, but a very common occurrence. According to the security company F-Secure's senior researcher Mikko Hypponen, one of these master criminals recently ran a contest offering a $36,000 Lexus sedan to the top-selling affiliate. According to a report in USA Today, in 2008, "… SecureWorks researcher Stewart infiltrated a Russian group known as the Baka Software gang. He accessed documentation showing one affiliate earned $146,525 in 10 days by spreading promotions for a worthless program, called Antivirus XP 2008, to more than 154,000 people, and closing sales to 2,772 of them. Another record showed five top Baka Software affiliates earning weekly commissions averaging $107,604." In another example of the degree of infection, Microsoft reported that its Malicious Software Removal Tool found one specific fake security program on 4.4 million computers! There are hundreds or thousands of these rogue programs currently infesting countless millions of computers. This begs an answer to a rhetorical question; would you really want to give your credit card number and security code to a crook that is probably in Russia? If you fell for this scam, contact your credit card company immediately and tell them what happened; also ask them to chargeback the charges made on your card by the crooks.

If you feel that you have been victimized there are some free utilities that can likely detect and kill the malware. Since much of this malware will not be initially detected by the protective software on our computers, and may in fact neutralize the protection that we do have, simply performing a scan with the security software we already have may provide little or no benefit. It should also be noted that if the user cannot access the websites of the legitimate utilities that can detect and kill the malware, that is a sure symptom that the victim computer is under the control of the cyber crook.

I am now receiving daily emails and phone calls from people describing a similar problem, complete with the typical symptoms of a scumware or scareware infection. I have had very good

*cont'd on Page 6*

# Scumware and Scareware - cont'd

*cont'd from page 5*

results with a few free utilities that will likely detect and kill the malware, and remove it from our machines. While there can be no guarantees that they will continue to work well, they do have a proven track record, and so far, have fared well in this "cat and mouse" game where the cyber crooks keep developing something new, and the security companies have to come up with a way to detect and kill the infection.

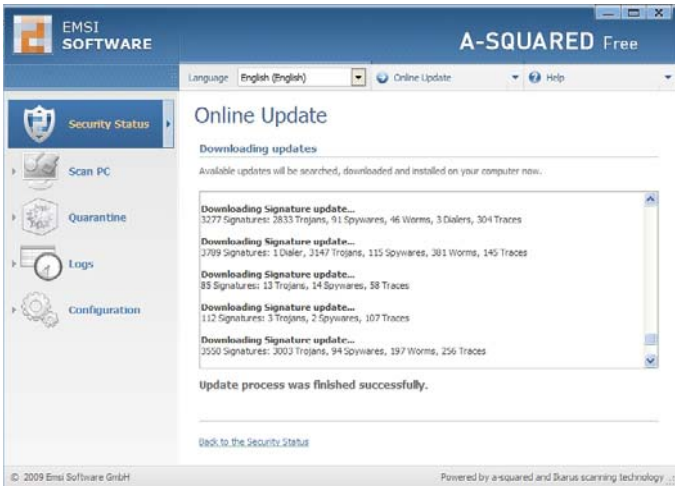

My first choice is Malwarebytes Anti-Malware, available for download from www.malwarebytes.ORG. I emphasized the ".ORG" because there have been knock-off websites with other upper-level domains designed to explicitly scam people looking for the authentic product. Malwarebytes has both a free version and a commercial version. As is customary, the paid commercial version has more features and capabilities, but the free version is fine for detecting and removing most malware. Download it (probably from a link redirecting the user to CNet's Download.com), install it, update it, and perform a scan. A quick scan will detect malware in the most common locations in just a few minutes, but a full scan will be much more thorough, and may take an hour or two to run. If the user cannot directly access the malwarebytes.org website, but is redirected somewhere else or totally blocked, then that is a sure sign that the computer has been hijacked. If this happens, download Malwarebytes to another computer, and copy it to a flash drive or CD, and install it from that media. It may also be a good idea to manually download the latest updated signature files (called "rules"), from www.malwarebytes.org/mbam/database/mbam-rules.exe, as access to the update server may also be blocked on the infected computer. Install the Malwarebytes on the infected computer, and then run the file mbam-rules.exe to update the software. If there is memory resident malware detected, Malwarebytes may direct the user to reboot the computer, and Malwarebytes will then automatically rerun at boot, killing the malware before it can load. Update it and rerun it frequently to help keep your computer clean of malware.


The other utility that I use along with Malwarebytes to detect and kill malware is A-Squared Free, available for download from www.emsisoft.com/en/software/free/. A-Squared Free has a commercial sister product, A-squared Anti-Malware (www.emsisoft.com/en/) with more features and a memory resident component that provides real time protection in addition to the security software already on the computer. Both versions also integrate a full featured virus scanner to detect more than most other scanners. Download one of the versions of A-Squared (the free version is adequate if the user only wants to detect and remove malware and viruses), install it, and update it.

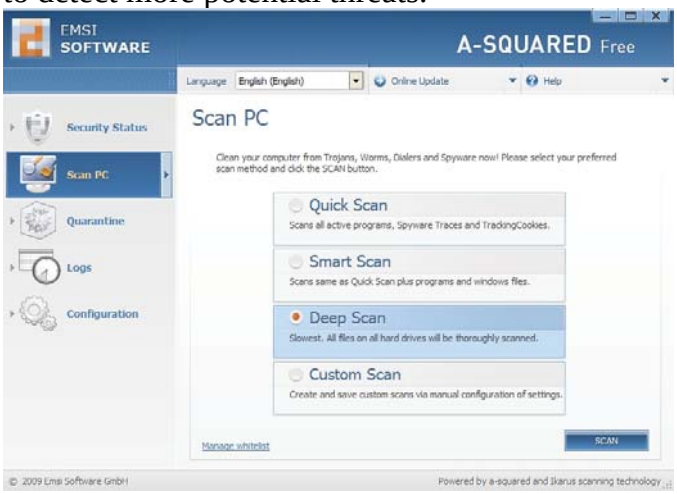
*cont'd on Page 7*

# Scumware and Scareware - cont'd

*cont'd from page 6*




Do a quick scan for a quick clean, and a deep scan to detect more potential threats.




A-Squared also detects fragments, or pieces of code that may be a threat. Since a detector as sensitive as A-Squared may occasionally detect a file and label it as a threat, but it is really a false-positive, I choose to initially quarantine anything that is found, rather than delete it. That way, I can recover any files that may have been misdiagnosed.


A-Squared is another product whose website is commonly blocked by malware, in order for the malware to protect itself from removal. If that happens, the A-Squared software can be downloaded to another computer, and copied to a flash drive or CD, and installed from that. An alternative designed explicitly for just such an occurrence is A-Squared Emergency USB Stick Files (download1.emsisoft.com/a2usb.zip). This version, which is kept up to date continuously on the Emsisoft website, is a 67mb download which contains all of the necessary files, is intended to be copied to a flash drive, and installed on the infected computer from that media.

After the computer is cleaned of malware, the user will often notice a marked increase in performance. Do not be complacent, because you may still be victimized even though your computer is likely clean. Since your logons, user names, and passwords may have been compromised, it would be a good idea to change them, and repeat the scanning process on a frequent and regular basis. It may also be necessary to reinstall your security software, as it may have been destroyed by the malware. Consider installing another layer of security that works in addition to your security software, and enhances your protection, making a re-infestation less likely. The paid commercial versions of Malwarebytes or A-Squared Anti-Malware would be good choices, or a freeware product such as Threatfire (www.threatfire.com) would provide enhanced protection in addition to the traditional security software.

***I've had the pleasure of working on several computers that have been infected with this type of scumware and I can tell you that it is no fun. A couple of times I've been able to remove the offending software, but on several others, I've had to reformat the hard drive and start from scratch.***

***Editor***

# Mozilla Firefox 3.6 Now Available

***Just a heads-up that Mozilla has shipped Firefox 3.6, the next version of its web browser.***

Mozilla, a public-benefit organization dedicated to promoting choice and innovation on the Web, today released Firefox® 3.6, an update to its popular, free and open source Web browser. The latest version of Firefox introduces cutting-edge features, support for a wide variety of Web standards, and access to more than 6,000 free add-ons that allow users to customize their browser to their liking.

Firefox 3.6 is more than 20 percent faster than Firefox 3.5 and includes extensive under the hood work to improve performance for everyday Web tasks such as email, uploading photos, social networking, and more. It also delivers new features like customizable browser themes called Personas, a ground-breaking Plugin updater, improved JavaScript performance, and enhancements to familiar favorites like the Awesome Bar for a better, more personal Web experience.

Firefox 3.6 was built by Mozilla's global community of passionate contributors, including thousands of experienced developers, security experts, localization and support communities, and hundreds of thousands of active testers. More than 350 million users worldwide enjoy Firefox's fast, secure browsing experience and unparalleled customization.

## What's new in Firefox 3.6:

Below are some of the coolest features of Firefox 3.6:

***Personas:*** Personalize the look of your Firefox by selecting new themes called Personas in a single click and without a restart

***Plugin Updater:*** To keep you safe from potential security vulnerabilities, Firefox will now detect out of date plugins

***Stability improvements:*** Firefox 3.6 significantly decreased crashes caused by third party software – all without sacrificing our extensibility in any way

***Form Complete:*** When filling out an online form, Firefox suggests information for fields based on your common answers in similar field

***Performance:*** Improved JavaScript performance, overall browser responsiveness, and startup time

***Open Video and Audio:*** With the world's best implementation of HTML 5 audio and video support, now video can be displayed full screen and supports poster frames

## What's New Under the Hood for Developers

Support for the latest HTML5 specification, including the File API for local file handling

***Font Support***: In addition to OpenType and TrueType fonts, 3.6 now supports the new Web Open Font Format (WOFF)

***CSS gradients:*** Supports linear and radial CSS gradients which allow for a smoother transition between colors

***Device orientation:*** Firefox 3.6 exposes the orientation of the laptop or device to Web pages

## How to get Mozilla Firefox 3.6:

Firefox 3.6 is available for Windows, Mac OS X, and Linux in more han 70 languages – more platforms and languages than any other browser! You can download Firefox 3.6 at www.firefox.com.

# *from the Secretary's desk*

## Minutes from the January 21, 2010 Board of Directors Meeting

**Attendees**: The Mikes Young, Regimenti, and DeLucia, Fran Damratowski, Sam Shepherd, Kathy Walker, Bill Somers, Kris Johnson

### OLD BUSINESS:

**February Meeting:** "Computer Buying Advice" with Fran Damratowski, "Windows 7 Tips and Tricks" with Mike Young and election of officers

**March Meeting:** "Windows 7 Tips and Trick"

**April Meeting:** "Photo Book and Book Making" demonstration" by Mike Delucia

**May Meeting**: "Sketch-Up from Google" presented by Bill Somers and Kathy Walker

**June Meeting**: "Tech Net Activation"

### SIGS:

**Technology**: Mike Regimenti will give a presentation of Firefox 3.6. Leo will be contacted to see if he is willing to conduct a workshop on "Macro for Excel" in March and April.

**CRSIG** – Fran reported that she has offered 10 low-end computers free to the County School PTA for distribution to needy families but has not received a reply from them yet. Fran also reported about the class at O'Malley and her findings about purchasing polo shirts for the club.

### Finances

The treasurers reported that the club is solvent. Kathy reported about the progress in getting a tax exempt card.

### NEW BUSINESS:

Sam gave an update of his class on Windows 7. He is planning to have an 8 week course starting on the Tuesday after Easter and running for 8 weeks. It will be held at the Severn Middle School and will cost $50. Five school members will be offered the class free of charge.

Sam reported that his laptop has been repaired free of charge.

Mike Young will be providing Smart Computing magazines, and Kris will be bringing some miscellaneous items for the members' only club raffle. Kathy will be providing an updated list of members in good standing.

Mike Young checked out club options from Tech Soup but has put off purchasing anything until the next meeting.

Meeting was adjourned at 9:15 p.m.

***Kris Johnson***

***Secretary***

Chesapeake PC Users Group

***Celebrating 25 Years of Users Helping Users***

**The Next Regular Meeting will be at**
**The Severn River Middle School**

## Wednesday
## February 10th, 2010

**Meeting will be held in the large meeting room.**
**It starts at 7:00 P.M. with club business and a short discussion period.**

***presentation on***
***Computer Buying Tips & Tricks***
***by***
## Frank Damratowski

CANCELLED

**Members and their friends are welcome to come, ask questions and become enlightened.**

## How to Find: Severn River Middle School

SRMS is close to the Arnold, MD campus of the Anne Arundel Community College. From Annapolis and points south, take Rte 2 (Ritchie Highway) north about 3 miles from the intersection of Rt. 50, **turn right on College Parkway**. At the first light, turn left on Peninsula Farm Road. (Of course, if you are coming from points North, you would turn left onto College Parkway) about a half-mile down the road the large SRMS school building, set back off a large two level parking lot, will be visible on your right. Park here and go to the main entrance. Signs will be posted to direct you to the **Large Group Room** where we will be meeting.

**How to find: The Technology SIG, A ChPCUG Special Interest Group****

**The meetings are held at the SRMS in the Library.**

Chesapeake PC Users Group

**1783 Forest Drive #285**
**Annapolis, MD 21401**

**FIRST CLASS**

## INSIDE THIS VERY ISSUE!

**President's Corner**
**Firefox 3.6**
**Secretary's Desk**
**Scumware & Scareware**
**... and a little bit more!**

**Note:** *The date above your name on the mailing label is the expiration date of your membership. Contact the Membership Chairman (page 2, column 2) to update.*

**Proudly Affiliated with**

NASA FEDERAL CREDIT UNION www.nasafcu.com

apcug