1783 Forest Drive #285
Annapolis, MD 21401

Chesapeake PC Users Group, Inc.

THE PRINTER

PRESIDENT'S CORNER

Happy New Year Everyone!

I hope everyone has a safe and joyous 2007! There are a lot of new technology developments that are happening this year. In addition to a new operating system from Microsoft, there are a lot of new hardware and architecture changes that will be taking place. And the Chesapeake PC Users Group it just the place to investigate the new developments. With your help, we can have some great upcoming meetings.

Secure Wireless Home Networking
(BRING YOUR NOTEBOOK!)

At the January 10 General Meeting, we will demonstrate how to securely install a wireless 802.11g home network. For this demonstration to work properly, it is important that we have participants. Please bring your wireless device (laptop, notebook, handheld, etc.) ***We will also be giving away to a lucky member, the wireless router used at the meeting.***

Listed below are a few tips to get things going. If you set up a wireless network, it is very important that you use all of the security capabilities of the devices. These include:

Use the strong (128 bit) WEP encryption built into the devices. Some products only support 64-bit encryption, but you should try to use wireless devices that support both 64 and 128-bit encryption. Use WEP for authentication ***and*** to secure the data being transmitted. This can reduce network throughput by 10-15% (for 64 bit) or 15-25% (for 128 bit). This is not bulletproof protection, but it requires significant effort to break. Someone would have to eavesdrop on ***a lot*** of your network traffic in order to effectively crack this encryption.

Secure your Router/Access Point. Make sure that you require a password for configuration of the router or access point. In addition, make sure you change the default password, as these are well known. You should physically secure your Access Point if possible, to prevent someone from performing a "hard reset" and setting the passwords back to their defaults.

If possible, disallow remote configuration. This requires you to plug directly into the Access Point/ Router in order to configure it.

Use MAC address-based association and access control. The MAC address is a unique identifier in a device, and by limiting access to certain MAC addresses, you can help lock out intruding computers. This can be done on our wireless router and our broadband router.

Use NetBEUI instead of TCP/IP for file and printer sharing. If someone gets access to your network, they won't be able to access your files, just your Internet connection.

Only share what you need to. You should share folders and files, not entire hard drives.

cont'd on Page 2

cont'd from page 1

PRESIDENT'S CORNER - cont'd

Secure your sensitive files with a strong password. Not a dictionary word, containing non-alpha numeric characters like: !@#$%^&*.

Use WPA to secure your network.

Almost all the Wireless Hardware that came out since the second half of 2004 is WPA-TKIP able. Upgrade from WEP to WPA might be available for a few selected older versions (check you Brand Website). To have a functional WPA on your Wireless Network, both Windows and the Hardware have to be WPA Enabled. Microsoft already posted the WPA update for WinXP.

Probably More Vista

With Vista expected to launch in January, we may have a visit from a Microsoft representative to demonstrate the operating system or Office 2007. If Microsoft does not attend the meeting, members of the users group may provide an updated view of the shipping operating system.

Winter Digital Photography

There are always many opportunities to take wintertime digital photographs. Processing the long shadows and high contrasts can be a challenge. Our March meeting is a good time to review processing the pictures that you took over the winter.

Combined Federal Campaign

The users group is an affiliate charity of the Combined Federal Campaign. For those of you who contribute to the CFC or know someone who contributes, please designate the Chesapeake PC Users group as one of your charities, we are number **3069**. With funding, we can really do a lot more with our meetings and organization.

See you at the meeting. Bring a Friend!

Michael

OFFICERS

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

Vice President
Mike Regimenti.....(410) 974-0649
vice-president @chesapeakepcusersgroup.org

Treasurer
Karl Richmond.....(410) 268-3860
treasurer @chesapeakepcusersgroup.org

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

Publisher/Editor
Mike Regimenti.....(410) 974-0649
editor@chesapeakepcusersgroup.org

CHAIRPERSONS

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

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

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

Public Relations Chairperson
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
Lee Wickline.....(410) 745-9932
mscug @chesapeakepcusersgroup.org

Technology SIG
Mike Regimenti.....(410) 974-0649
internet@chesapeakepcusersgroup.org

Computer Refurbishing SIG
Fran Damratowski.....(410) 544-7047
refurbishing@chesapeakepcusersgroup.org

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

The Chesapeake PC Users Group

The Chesapeake PC Users Group (ChPCUG) is a 501(c) 3 charitable organization that has been active in Maryland since 1984.

PC Computer users are assisted through education classes, monthly user meetings, a newsletter, an on-line forum, and the opportunity to participate in Special Interest Groups. ChPCUG collaborates with all organizations and government agencies interested in advancing computer knowledge for members of the local community.

One of the most important functions of ChPCUG is Computer Refurbishing. It began in February 1999 with the purpose of refurbishing computers for those individuals, families, schools, and nonprofit organizations unable to afford a new computer. Grants allow provision of computers at no cost to those unable to make a donation. A modest donation is requested from those able to provide it. Volunteers perform all refurbishing activities.

The activities of the ChPCUG are to promote computer literacy, challenge the digital divide, and enable recipients to have access to the vast storehouse of information available on the Internet.

As of 1 October 2006, the Chesapeake PC Users Group has now provided over 1300 computers to those in need. Since 2004, over 350 computer systems have been provided to elementary school students at no cost.

Please direct your Combined Federal Campaign contributions to:

Code #3069

Project File: Build a Vista Ultimate Capable PC!

Tools Needed for the Build

by
Fran Damratowski

Last month, Mike Young wrote about the opportunity to build a Vista capable computer from the ground up. Some tools will be needed to build the computer. You can do one of two things- buy a computer tool kit (I keep one in drawer next to my computer) or just bring the tools you have at home. You can see what a tool kit looks like, by doing a search for PC tool kit or computer tool kit. A small tool kit, 11 or 12, tools usually sells for $12 -$15.

The tools that you have at home and that will probably be all you need are:
two Phillips screw drivers #0 & #1,
two small flat bladed screw drivers 3/16 and 1/8,
two nut drivers 3/16" and 1/4",
small pliers,
some kind of long pickups for dropped screws.

I doubt we will need Torx drivers, if so possibly T1, T10, or T15.

You will be invited to build the computers at the CRSIG workshop because we have benches with electric power and hookups for the internet. Volunteers at the workshop bring personal items and keep them on their benches. We ask that you do not disturb these items. You will need to bring your lunch, we do not have a cafeteria.

Directions to the workshop

From Annapolis:
Go north on Generals Highway (Rte 178) behind the Westfield Mall past the Golf Course and past the Fairgrounds to Crownsville Road. It's about 4 miles from the Westfield Annapolis Mall. Turn left onto Crownsville Road.

From Rt. 97:
Take the Crownsville exit go several miles and turn right onto Crownsville Rd.

Go about three tenths of a mile on Crownsville Rd. and turn right onto Marbury Drive (baseball field on the corner). At the STOP sign turn right. Turn left immediately past the single story red brick building on your left as you make the turn. Our sign is on the corner of the building. Our entrance is around the corner from the sign. There is a small sign on the window of the door. Our red brick building is directly across the road from the white maintenance building.

Chesapeake PC Users Group

from the Secretary's Desk

Minutes of CHPCUG Board meeting on December 20, 2006

Attendees: The Mikes Young, Regimenti, & DeLucia, Sam Shepherd, Karl Richmond, Lee Wickline & Kris Johnson

OLD BUSINESS:

January Meeting: Wireless networking security by Mike Young & Yahoo Groups by Craig Barlow.
February Meeting: More Vista by Mike Young with possible input by Microsoft.
March Meeting: Digital Photography with Michael Alloy.
April Meeting: Possible presentation by Verizon on their Fios service.
May Meeting: Making Lightscribe CDs by Fran Damratowski.

SIGS:

Technology: Mike Regimenti's meeting on January 3rd will look at Google Calendar & a quick look at the PhotoshopSupport.com.
Mid-Shore CUG: Lee Wickline reported that all is going well. Mike Young & Mike Regimenti are planning to attend their January meeting.

Treasurer's Report: Karl reports the club is fiscally solvent.

NEW BUSINESS

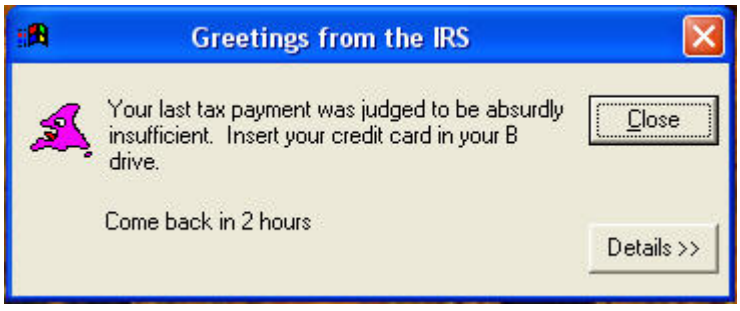
In response to Mike Young's suggestion that the club expand its charitable outreach groups, Kris suggested the Family Tree Organization as a possible group that could benefit from our refurbishing center. The Family Tree is an organization dedicated to improving our community by providing families with proven solutions to prevent child abuse and neglect through education and support. While they do have some paid staff, 78% of all contributions raised directly support their programs and services. Mike Young suggested that the Family Tree e-mail a detailed list of their needs and perhaps make a presentation at a board meeting.

Mike Young strongly suggested that the treasurer purchase Adobe GoLive for the webmeister.

Meeting was adjourned at 9:00 P.M..

Happy New Year!
Kris Johnson
Secretary

Coming in April...



Top 8 Tips for Wireless Home Network Security

Guide Picks
from Bradley Mitchell,
Your Guide to Wireless / Networking

Many folks setting up wireless home networks rush through the job to get their Internet connectivity working as quickly as possible. That's totally understandable. It's also quite risky as numerous security problems can result. Today's Wi-Fi products don't always help the situation as configuring their security features can be slow and non-intuitive. The recommendations below summarize the steps you should take, in order to importance, to improve the security of your home wireless LAN.

1) Change Default Administrator Passwords (and Usernames) ***(http://compnetworking.about.com/cs/wirelessproducts/qt/adminpassword.htm)***

At the core of most Wi-Fi home networks is an access point or router. To set up these pieces of equipment, manufacturers provide Web pages that allow owners to enter their network address and account information. These Web tools are protected with a login screen (username and password) so that only the rightful owner can do this. However, for any given piece of equipment, the logins provided are simple and very well-known to hackers on the Internet. Change these settings immediately.

2) Turn on (Compatible) WPA / WEP Encryption***(http://compnetworking.about.com/cs/winxpnetworking/ht/wpainwindowsxp.htm)***

All Wi-Fi equipment supports some form of "encryption." Encryption technology scrambles messages sent over wireless networks so that they cannot be easily read by humans. Several encryption technologies exist for Wi-Fi today. Naturally you will want to pick the strongest form of encryption that works with your wireless network. To function, though, all Wi-Fi devices on your LAN must share the identical encryption settings. Therefore you may need to find a "lowest common demoninator" setting.

3) Change the Default SSID ***(http://compnetworking.about.com/cs/wirelessproducts/qt/changessid.htm)***

Access points and routers all use a network name called the SSID. Manufacturers normally ship their products with the same SSID set. For example, the SSID for Linksys devices is normally "linksys." True, knowing the SSID does not by itself allow anyone to break into your network, but it is a start. More importantly, when someone finds a default SSID, they see it is a poorly configured network and are much more likely to attack it. Change the default SSID immediately when configuring your LAN.

4) Enable MAC Address Filtering ***(http://compnetworking.about.com/cs/wirelessproducts/qt/macaddress.htm)***

Each piece of Wi-Fi gear possesses a unique identifier called the "physical address" or "MAC address." Access points and routers keep track of the MAC addresses of all devices that connect to them. Many such products offer the owner an option to key in the MAC addresses of their home equipment, that restricts the network to only allow connections from those devices. Do this, but also know that the feature is not so powerful as it may seem. Hacker software programs can fake MAC addresses easily.

cont'd on Page 7

cont'd from Page 6

Wireless Home Network Security - cont'd

5) Disable SSID Broadcast ***(http://compnetworking.about.com/cs/wirelessproducts/qt/disablessidcast.htm)***

In Wi-Fi networking, the access point or router typically broadcasts the network name (SSID) over the air at regular intervals. This feature was designed for businesses and mobile hotspots where Wi-Fi clients may come and go. In the home, this feature is unnecessary, and it increases the likelihood an unwelcome neighbor or hacker will try to log in to your home network. Fortunately, most Wi-Fi access points allow the SSID broadcast feature to be disabled by the network administrator.

6) Assign Static IP Addresses to Devices ***(http://compnetworking.about.com/od/workingwithipaddresses/qt/staticipaddress.htm)***

Most home networkers gravitate toward using dynamic IP addresses. DHCP technology is indeed quick and easy to set up. Unfortunately, this convenience also works to the advantage of network attackers, who can easily obtain valid IP addresses from a network's DHCP pool. Turn off DHCP on the router or access point, set a fixed IP address range, then set each connected device to match. Use a private IP range (like 10.0.0.x) to prevent computers from being directly reached from the Internet.

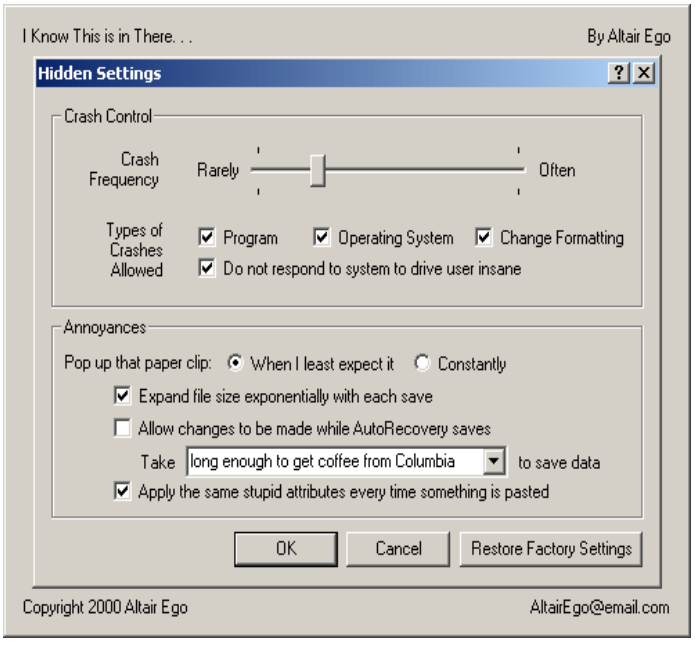
7) Position the Router or Access Point Safely ***(http://compnetworking.about.com/cs/wirelessproducts/qt/locate_aprouter.htm)***

Wi-Fi signals normally reach to the exterior of a home. A small amount of "leakage" outdoors is not a problem, but the further this signal reaches, the easier it is for others to detect and exploit. Wi-Fi signals often reach across streets and through neighboring homes. When installing a wireless home network, the position of the access point or router determines it's reach. Try to position these devices near the center of the home rather than near windows to minimize this leakage.

8) Turn Off the Network During Extended Periods of Non-Use

The ultimate in security measures, shutting down the network will most certainly prevent outside hackers from breaking in! While impractical to turn off and on the devices frequently, at least consider doing so during travel or extended periods off-line. Computer disk drives have been known to suffer from power cycle wear-and-tear, but broadband modems and routers can easily handle this treatment occasionally.

I Know This is in There...



Windows Vista Preview - Part II

Live taskbar thumbnails

Resting the mouse pointer over a taskbar item displays a live thumbnail of the window, showing the content of that window. The live thumbnail is displayed whether the window is minimized or not, and whether the content of the window is a document, photo, or even a running video or process.

See thumbnail views of the items in your taskbar by resting your mouse pointer on them.

Windows Flip and Windows Flip 3D

Windows Vista provides two entirely new features to manage windows: Windows Flip and Windows Flip 3D. Flip allows you to flip through open windows (by using Alt+Tab), providing a live thumbnail of each window, rather than just a generic icon and file name. Live thumbnails make it easier to quickly identify the window you want, particularly when multiple windows of the same kind are open. With Flip 3D, you can use the scroll wheel on your mouse to flip through open windows in a stack, and quickly locate and select the one you want to work with.

Use Flip to view and navigate more easily through open windows.

Use Flip 3D to navigate through open windows using the scroll wheel on your mouse.

Microsoft Vista Beta-First Look

by
Brian K. Lewis, Ph.D.,
Sarasota Personal Computer Users Group, Inc.

Many of the reviews that I have read on the early releases of Windows Vista have been done on "fast" hardware. Many times with 1- 2 GB of RAM. Knowing that many users of Windows XP will probably upgrade to Vista with their current hardware, I installed a Beta 2.0 copy of Windows Vista on an older machine. This computer has an Intel 1.3 GHz CPU and had 256 MB of RDRAM. I upgraded the RAM to 512 MB which is normal for many Windows XP users. The computer also has an ATA 40 GB hard drive and it did have a CD writer. However, when I went to install Vista, I found the installation disk was a DVD. I had to upgrade to a DVD unit. I did manage to find a Sony DVD burner at a very reasonable price. So, a word of warning for those interested in upgrading to Vista when the final version is available, you may have to have a DVD drive to install it. This review is based on my hands-on experience with Vista.

I installed this Beta version to the hard drive as a new installation. It saved the previous version of Windows and user files in one folder. Since I had no applications or personal information on the drive I was able to delete this folder after the installation was complete. I did note that the installation took more than 90 minutes to complete. I'm sure that this was partly related to the speed of this computer as well as the size of the operating system. Since this is a pre-release version, it probably contains debugging code which contributes to its overall size.

Once Vista was installed, it brought up a Control Center Window. This had icons for several items, one being hardware that wasn't installed and other to add a printer. There were also a Vista tutorial and an icon for new items in Vista. The first thing I tried was to see what hardware wasn't installed. The first item on the list was the ethernet card, next the sound system, then a "Simple Controller" which I finally figured out was the modem and a SCSI controller. To simplify things I removed the modem and the SCSI card. Then I tried to install the ethernet card. At that point I started getting the User Account Control (UAC) windows which required that I approve every step that might change the make-up of the computer. Every time I tried to install a driver I had several UAC windows to get through before I could get to the installation process. And this, in spite of the fact that I was running as the System Administrator.

Any of you who have set up Window XP Professional should be familiar with the Administrator and User Account system. On my XP Pro system, I have the Administrator account and a User account, both of which are password protected. I rarely use the Administrator account, instead I work in the User account. You might ask why I do this. The reason is that without the Administrator account running it is more difficult for Trojans or parasites to make changes to any of the system files on my computer.

That is assuming that they can get past the firewall in the first place. I have seen too many XP Pro systems where the user is always running in the Administrator mode which has allowed invasions of the system by Trojans/parasites. I have just cleaned out one system that was acting weirdly until I removed 295 parasites/Trojans. Whenever I need to install software on my XP system, I simply use the "Run As" command and enter the Administrator password. That way I don't have to change from the User mode to the Administrator mode.

cont'd on Page 10

cont'd from page 9

Microsoft Vista Beta-First Look - cont'd

However, this has all changed in Vista with the User Account Control. Even if you are logged on as the System Administrator, it requests your permission for access to anything related to the system or devices. Just to review the list of hardware in the Device Manager requires that you get permission to do so by clicking in the Permissions request window. When you try to install new software or drivers, you get a security window which requires your permission to let you continue. Then you get the UAC window, which requires that you verify that you know you are installing new software and that you think it is reliable. You even get a UAC window when you try to download and install Windows Updates. I have learned that there is a good reason for this security. According to one report I have read, it is possible for Trojans downloaded to your computer along with a web page, to inactivate your anti-virus, firewall and anti-parasite software. This can all be done in the background, if you are running in the Administrator mode. Then changes can be made to your system software that can affect the operation of your computer. The UAC in Vista is designed to prevent this from happening. Once I set up my User account, then I had fewer UAC windows show up. They occurred only when I wanted to install new software or drivers. The only thing I had to do then was to provide the Administrator password.

Since I didn't have drivers for the ethernet card, I had to search for one on the Internet using my XP computer. After some research, I was able to identify the make/model of the card. Then I found a driver on DriverGuide.com. I downloaded the zip file to my hard drive and burned it to a CD-RW. Then I transferred it to the hard drive on the Vista machine. Vista quickly extracted all the files for me. Then in the device driver, I clicked on "Update drivers" for the ethernet card and told it to search the drive for a driver. Low and behold, it did find and install the driver. Now, after some hard drive activity and approving the UAC to update the Network center, I was on the Internet.

The next thing I wanted was not my sound card driver. It was an anti-virus program. According to the Vista information site, only TrendMicro has an A-V program approved for Vista. However, I had noticed on the Avast Web site that they had a Vista compatible version of their A-V software. I went back to their web site and found that all versions of Avast are now Vista compatible. I downloaded a free Home Edition and installed it. Again, I had the UAC windows to get through to get the installation under way. After it was installed, I went through the Avast registration and my A-V program was operational. So far, the Avast is running normally and is doing its usual updates in the background.

I have been using the Windows Firewall as I "assumed" it was a two-way firewall. I have since learned that it is only an incoming firewall. I plan on replacing it with ZoneAlarm.

After a re-boot of the computer, Vista popped up a window and asked if it could install my multimedia sound card. I clicked on OK and the next window had two choices, one of which was to search the Internet for a driver. At this point I still had no indication as to the manufacturer of the sound card, so I selected the Internet search. In just a few minutes it changed from searching to installing the software. Then I had a window saying it had installed the software for the Creative Labs sound card. Now that, in my mind, is quite an improvement over previous Windows versions.

The one interesting aspect of the Creative installation is that Vista could not install a driver

cont'd on Page 11

cont'd from page 10

Microsoft Vista Beta-First Look - cont'd

for the game controller. As with most sound cards, there is a output for a game controller. For some reason, Vista was unable to install a driver for this output. It is now listed in the Device Manager as an unknown device. The sound card is listed correctly.

My next step was to set up a User account and shift out of the Administrator mode. That was accomplished quite easily through the Control Panel. So, once I was in User mode, I downloaded a copy of OpenOffice. When I started to install it, a UAC window popped up and I had to enter the Administrator password. Then the installation proceeded normally. Not really any different from the User mode in XP.

Vista has a Security software setup in the Control Panel, that is similar to that in XP. It shows the status of the firewall, anti-virus, updates and a new item, Windows Defender. This latter software is an anti-parasite package. It has a default setting to scan your hard drive every day at 2:00 AM. Since my computer is rarely turned on at that hour, I changed the setting to 5:00 P.M.. It is more likely to be running at that time.

The last step was to install two networked printers. I clicked on the "Add printers" icon in the Control Center Window. That brought up the Printer Installation Wizard. I selected a networked printer and told it to find the printer. Several minutes later it told me there were no networked printers. So I backed up and selected browse for printer. That took me through the whole network tree, but I did find the printer. When I selected the printer and went to the next window, a bright yellow warning popped up to tell me that "printer drivers can install viruses! Are you sure this networked computer is trustworthy?" Well, since it is my main computer, I decided it was trustworthy and clicked on the OK button. Then I got the usual UAC window. After entering the password, the installation was completed and a test page printed. I had to go through the same routine with the second printer. But at least both of them are installed and working.

The Vista computer is now part of my local network and I can share files with it. In fact, part of this article was written on the Vista computer using the OpenOffice I downloaded. I had intended to finish the article on that computer, but the hard drive died. I can't fault Vista for this, the computer is old and it was the original drive. So, when the new drive arrives, I will have to re-install Vista and all the drivers. Since I had activated this copy of Vista, it will be interesting to see what will happen when I have to activate the new installation.

Next month, I hope to tell you of my experience with the Vista interface. So, hang in there, more information on Vista will be coming.

Editor: Dr. *Lewis is a former university & medical school professor. He has been working with personal computers for more than thirty years. He can be reached via e-mail at bwsail(at)yahoo.com.*

Chesapeake PC Users Group

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

Wednesday, January 10th, 2007 Meeting will be held in the large meeting room. It starts at 7:00 P.M. with club business and a short discussion period.

There will be a Presentation on

Wireless Networking Security

by

Mike Young

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 parts 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 on to 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**
Meets the 1st Wednesday of each month at 7:00 P.M.

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!

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.*