PRESIDENT'S CORNER

.... And down the stretch we come

We've had some really great meetings lately. I think everyone has enjoyed them and we will end the current season with a presentation by Craig Barlow. There's a lot to look forward to in the autumn. With new hardware and operating systems coming out, it should be very exciting.

June 3 Meeting – Wireless networking

Before we break for the summer, Craig Barlow will discuss wireless networking your PCs, one of the more important aspects is securing your wireless connectivity. In addition, Craig will review the latest wireless technology and what it means to you. Please bring your laptop to this meeting. Your participation is necessary. Check out the *Top 8 Tip on Wireless Home Network* article on page 10. This article is reprinted from the January 2007 issue.

September 9 meeting – Windows 7 released!

While this date isn't set in stone, all signs point toward the release version of the Windows 7 operating system to be released by September. We'll have probably the first of many full meeting on this new operating system.

Meetings are really starting to become interesting so I hope that you can attend as many as possible. Also, I hope that you participate in the meetings.

As reported in the May issue of *The Printer*, WIndows 7 RC (Release Candidate) is now available to all TechNet subscribers and the general public.

http://www.microsoft.com/windows/windows-7/download.aspx

**Everyone have a safe and happy summer,
and I will see you in September!**

Michael

Flash Drive - cont'd

cont'd from page 7

For those of us who have standard non-U3 drives, there is now an alternative that provides for the same functionality. This alternative to U3 that will run on almost all contemporary flash drives is called "PortableApps", and can be found online at portableapps.com. According to the PortableApp website, "A portable app is a computer program that you can carry around with you on a portable device and use on any Windows computer. When your USB flash drive, portable hard drive, iPod or other portable device is plugged in, you have access to your software and personal data just as you would on your own PC. And when you unplug the device, none of your personal data is left behind." Dozens of portable apps are available, including the Firefox browser, OpenOffice office suite, antivirus software, games, password managers, and many other pieces of software. The Portable-App Suite is totally free, and does not contain any spyware or adware. In addition to the bundled suite, there are many other programs available, almost all free, which will run as portable apps. The PortableApp website keeps a running tally of new software that is available, including new releases and versions, as well as beta (pre-release) software. A simple click will install the selected software on the flash drive.

Now that many of us are routinely carrying flash drives, it is nice to know that they may be capable of doing much more for us than just transport data.

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) 268-3860   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 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
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

2

www.chpcug.org/   **ChPCUG dues are $40 per year**   **THE PRINTER**   **June**   *2009*

End to End Security for Your Home Network

by

Mike Young

The most important part of your home network is the data. For most people this will consist of financial data, legal documents, photos, video, and other personal documents. While this data will not cause a global calamity if it became compromised, it would cause a disruption in the lives of those who own this data.

When you consider the security of your home network, if it's one computer or a few computers, you should consider a layered approach to security. The security layers will be reviewed below. This method consists of a common sense approach to security. While every method may not be applicable to everyone, most will be.

Physical Security

Most people lock their doors and turn off the lights when they are not home. Be sure to do this with your computer also. When the computer is not in use, turn it off. Also turn off your network access equipment. This will minimize the risk of someone using your Internet connection when you are not around.

If you are in a location where the physical access may be compromised, invest in a cable to secure the computer to a surface (table, wall, etc.). Inspect the area and think what you would do to break-in and

Security for Your Home Network - cont'd

try to prevent this. If you are using a laptop, keep it as secure as your wallet when traveling.

Backup your data

There many ways to backup your data. You can use imaging software such as Ghost or Aconis.

Copy files to an external source (hard drive, flash drive, etc.). Backup your data to optical disc. A recent option is to use an on-line service to secure your data.

Whichever method you choose, your should backup your data on a regular interval, daily, weekly, monthly, whichever you prefer, just as long as you do it. If you have a security compromise, you will be able to retrieve some (if not all) of your data. This is also important if your hardware should become damaged or malfunction.

Secure your computer

It is important that you keep your computer up to date. The security patches that are released from Microsoft are important to apply to keep it up to date with known security vulnerabilities. You should also keep other software patched. While this may not be as automated at the process for the operating system, it is just as important.

You should install and update anti-virus and anti-malware software. Some people would include a software firewall, but personally I've found that the software firewalls are not that effective and take up more resources then they are worth. I do recommend that you change the default administrator password on your network router and use the most advanced security options with the router that are feasible.

Encryption

Encryption is and excellent method to prevent your data from being compromised. There are several areas that encryption should be used to secure your data.

Hard drive encryption. If your computer is stolen or misplaced, the data can be accessed very easily if the harddrive is not encrypted. There are several commercial programs available for encryption use, but one of the better programs is an open-source program, TrueCrypt. This is a full disc encryption program that is recognized as one of the best solutions in the industry.

4

Security for Your Home Network - cont'd

Wireless encryption. When you are connected wirelessly to your computer, you should ensure that you are using a type of wireless encryption. Preferably you should use WPA-2 encryption, WPA or at a minimum WEP should be used. This will help to prevent your data from being compromised over the air.

Internet encryption. Accessing webpages that have sensitive data should use encrypted methods. Usually this is SSL, which is an excellent, secure, protocol. Without getting into the technical details, you should ensure that you see the 'lock' icon in your browser.

Things That You Can Do With That Flash Drive

by
Ira Wilsker, APCUG Director; Columnist, The Examiner, Beaumont, TX;
Radio Talk Show Host
Iwilsker (at) apcug.net

\ This article has been obtained from APCUG with the author's permission for publication by APCUG member groups; all other uses require the permission of the author (see e-mail address above).

WEBSITES:
http://portableapps.com
http://u3.sandisk.com/download/Download_
no.asp
http://www.microsoft.com/windows/windows-
vista/features/readyboost.aspx

With the demise of the floppy disk, and the approaching demise of the CD disc for data purposes, the USB flash drive has become the defacto method of saving and transporting files between computers. These small USB drives are known by a variety of monikers, such as flash drive, pen drive, pin drive, and thumb drive. Since their introduction a few years ago, their capacity has increased, and their prices have plunged. They are readily available in the big box stores, discount stores, club stores, and online. The most recent ones I purchased for the holidays were 8 gig size (almost the equivalent of the data stored on 2 standard DVD discs, about a dozen CD discs, or about 5700 floppy disks), and cost under $15 each. In the after-Christmas sales, some 8 gig flash drives were advertised for $9 each (after rebate). This amount of non-volatile storage for the price was inconceivable just a few years ago. I thought

5

Flash Drive - cont'd

I was getting a bargain a few years ago when I bought my first flash drive, a 64mb Lexar, for $49, and now a drive with about 64 times that capacity is about one-fourth the price! I have co-workers and students who wear their flash drives on cords around their necks, where they are referred to as "geek beads".

Most of us use the drive simply for portable storage, the ability to carry files around with us, but in reality these flash drives can do much more than to simply be used for storage. Most of the USB flash drives on the market today comply with the USB 2.0 standard for high speed transfer, while there still are a few inexpensive, low capacity drives that are of the slower USB 1.1 speed standard, or only about 3% of the speed of the USB 2.0 drives. From a practical viewpoint, the user will not notice any significant difference in speed if small files are saved and read, but will notice a difference if large files are used.

There are some other standards for USB flash drives that many users may find beneficial, if their flash drives have the capabilities. Users of Microsoft Vista (Home Basic, Home Premium, Business, and Ultimate versions) may find it advantageous to purchase flash drives that are labeled as "ReadyBoost". According to Microsoft, "Windows Vista introduces Windows ReadyBoost, a new concept in adding memory to a system. You can use non-volatile flash memory, such as that on a universal serial bus (USB) flash drive, to improve performance without having to add additional memory "under the hood." If the drive is compatible with the ReadyBoost standard, some of the flash memory in the drive can effectively and temporarily be added to the RAM (memory) installed in the computer, with an improvement on performance. If the Vista user with a compatible flash drive right clicks on the flash drive letter displayed under "My Computer" or Windows Explorer, and then left clicks on Properties – ReadyBoost, Vista will recommend how much of the available memory on the drive can be effectively and safely utilized by Vista. Other data stored on the ReadyBoost drive is protected from damage, and will not be harmed if the drive is used as a ReadyBoost drive. Because of the higher performance requirements, ReadyBoost compatible flash drives are slightly more expensive than standard drives, but are often the least expensive way to add memory to a Vista computer.
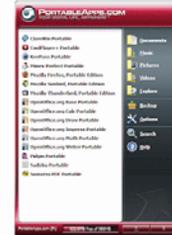

Another useful feature often found on a USB flash drive is known as "U3". Drives that are U3 compatible are labeled as such. A U3 powered flash drive allows the user to carry special versions of hundreds of programs on the flash drive that can be run directly from the flash drive with-

Flash Drive - cont'd

out being installed on the computer. This is an effective way to carry the actual software the user is familiar with, and run it on other computers. When unplugged from the computer, U3 leaves no data or other information left on the computer that was used. Some of the popular programs that come in U3 formats are the Firefox browser, Skype telephone, McAfee Antivirus (about $15), RoboForm Password Manager, OpenOffice (the comprehensive suite of office software including a Microsoft compatible word processor, spreadsheet, presentation program, database, and more, free), Thunderbird email client, and dozens of games. Most U3 drives come preinstalled with password protection and a "U3 Launchpad" which is a menu driven directory of the software on the U3 drive.

Twitter – What You Are Doing Right Now

by

Ira Wilsker, APCUG Director; Columnist, The Examiner, Beaumont, TX;

Radio Talk Show Host
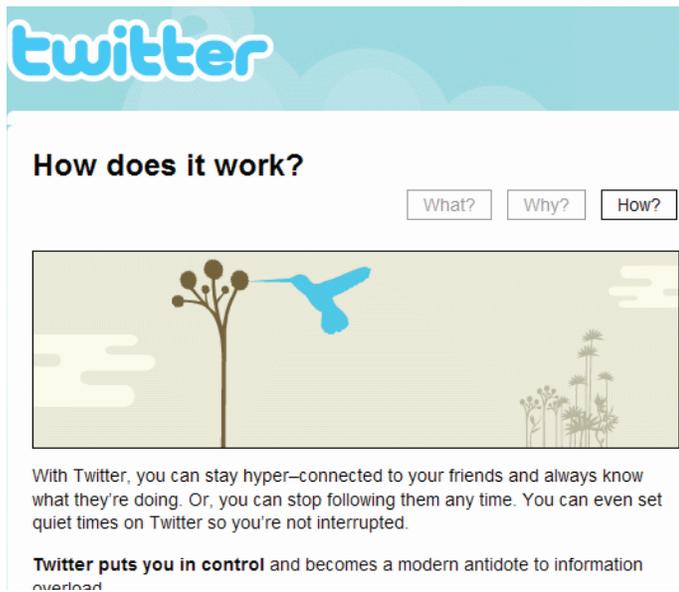
Iwilsker (at) apcug.net

WEBSITES:

http://www.twitter.com

Several of the readers of this column asked me, "What is Twitter?" following the media reports that senators and congress people were "Twittering" during recent presidential speeches. Twitter (the internet service and the person who does the posting) and Twittering or Tweeting (the posting of personal activities on Twitter) has become one of the most popular ways of communicating one's activities so that others can follow what is going on in the life of a Twitter. The service is self-described as, "Twitter is a service for friends, family, and co–workers to communicate and stay connected through the exchange of quick, frequent answers to one simple question: What are you doing?" According to some of the national media quoted by Twitter.com, "The New York Times calls Twitter "one of the fastest-grow-
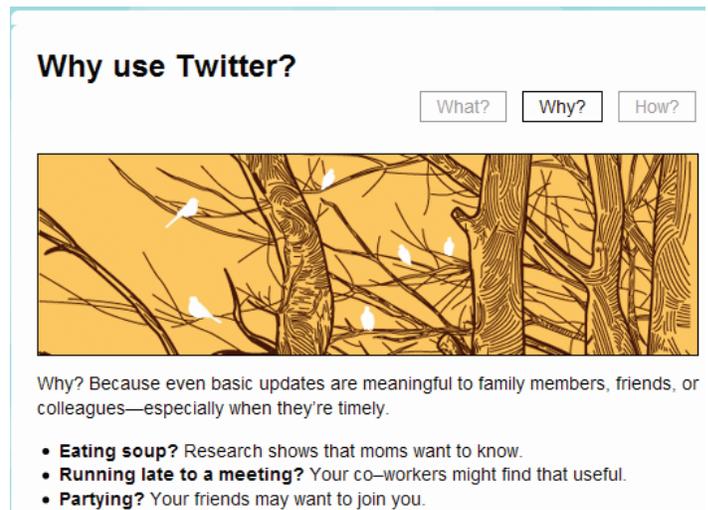
Twitter - cont'd

ing phenomena on the Internet." TIME Magazine says, "Twitter is on its way to becoming the next killer app," and Newsweek noted that "Suddenly, it seems as though all the world's a-twitter." One may wonder why a Twitter user would post his daily activities as they occur; Twitter explains it this way, "Why? Because even basic updates are meaningful to family members, friends, or colleagues—especially when they're timely."

How does it work?

With Twitter, you can stay hyper–connected to your friends and always know what they're doing. Or, you can stop following them any time. You can even set quiet times on Twitter so you're not interrupted.

Twitter puts you in control and becomes a modern antidote to information overload.

Just to experience the life of a Twitter, I went to www.twitter.com and signed up for a free account. The signup process was very fast and easy, only asking for me to create my user name, create a secure password, and entering my email address. After creating my account, I was given the opportunity to upload a photo of myself for display to anyone that views my Twitter page, and allow me to customize my page to control the way others view it. I entered my first short message that I was using Twitter, and it appeared on my now personalized webpage. Since messages and other postings are intended to appear as text messages on cell phones as well as on a webpage,

individual postings are limited to 140 characters, the maximum length of a text message (SMS) allowed on most cell phone systems. As I was typing this column, I posted a Twitter (message) that I was typing this column; if anyone is following my activities at this instant, he would receive this news as a text message on his cell phone, as an RSS feed on his computer, and email, or by simply viewing my Twitter webpage. On my view of my webpage is a text box where I can type my current activity, as long as I keep it under 140 characters, as shown by the counter adjacent to the text box. Postings can be made or received by computer, cell phone text message, Blackberry, or other communications device. Postings can also be received on any newsreader that uses the RSS format news feed.

Why use Twitter?

Why? Because even basic updates are meaningful to family members, friends, or colleagues—especially when they're timely.

- **Eating soup?** Research shows that moms want to know.
- **Running late to a meeting?** Your co–workers might find that useful.
- **Partying?** Your friends may want to join you.

Twitter makes it very easy to find friends who also Twitter. By clicking on the "Find People" icon, a window is opened that says "Find people". Follow them". To locate friends on Twitter, I chose to allow Twitter to access my email address book to determine if any of my current correspondents are on Twitter. Twitter can access (but only with your express permission) address books on

Twitter - cont'd

Yahoo, Gmail, AOL, Hotmail, and MSN. It will quickly scan the online address book, and match any email addresses in the address book against the millions already in the Twitter database. Twitter states that it does not save the email addresses and passwords, and does not send out emails to those located without express permission to do so. I also used the "Find on Twitter" feature to enter my last name to see if any of my relatives are on Twitter, and add them to my friends list. Just as a lark, I entered the names of some of our elected officials, and found that several of them do have Twitter accounts. If I want to invite friends by personal email, I can enter their email addresses in the "Invite by Email" box, and Twitter will send them an invitation.

If I want to add celebrities to my friend's list, I can click on "Suggested Uses", and a list of celebrities who Twitter will be displayed. By checking the box adjacent to their names, we can exchange Twitter posts and monitor each others' activities. Some of the more interesting celebrities and online services that can be added to anyone's Twitter friends list are the Jodrell Bank observatory, the Dell Outlet Store, JetBlue Airways Customer Service (monitors Twitter 24/7), the New York Times, 10 Downing Street (the official residence of the British Prime Minister), rapper M. C. Hammer, CNN Breaking News, Al Gore, John McCain, Whole Foods Market (Fresh organic tweets from Whole Foods Market HQ in Austin), Lance Armstrong, Britney Spears (Yes! This is the real Britney Spears!), George Stephanopoulos (ABC News Chief Washington Correspondent and Host of "This Week"), Women's Wear Daily, the Nightline TV news show, Martha Stewart, comedian and magician Penn Jillette, rapper 50 cent, and many more. The business and news outlets listed post breaking news or special deals to their Twitter friends. One that I added, being the na-

scent bargain shopper, is Woot.com, which posts one deeply discounted bargain each day in each of its merchandise categories.

Twitter, the company, is headquartered in San Francisco, and was founded in 2006. It is a small company, with only a few dozen employees, but has millions of members. It has a marketing model to generate revenue, but the revenue model has not yet been implemented, leaving all of the posts and web pages currently free of advertising.

I am not sure how much I will be using Twitter on a regular basis by posting my personal activities and short commentaries, but I will check my page occasionally just to see who is following my activities. The main purpose of Twitter is to answer the question, "What are you doing?" For those who want others to be able to know the answer in real time, they can do so with Twitter.

Top 8 Tips for Wireless Home Network

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.

Wireless Home Network - cont'd

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.

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.

11

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

Wednesday
June 3rd, 2009

**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

Wireless Networking

by

Craig Barlow

**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
Twitter
Fun with Flash Drives
Home Networking
MarketPro Schedule
 ... 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