

May Newsletter 2010

Vol. 3 No. 5

It looks like spring has finally sprung. The yard could use some more work, but it will have to wait because I'm off to Spokane, WA. It is time for Bloomsday—an individually timed 10 K race. You start in shifts according to your “run” (a lot of us walk) time. The first group (they really run) usually finish before my group starts. It's still very chilly race morning and many folks buy second hand warm stuff. Before they start the race they throw their stuff into the trees. It gives a new meaning to clothes trees.

I will continue putting this newsletter together, but Denis Astrubel is now Vice President and will be running the Windows meetings. If you have suggestions or want to see a particular subject covered, email him at demmos@juno.com.

I recently attended a retiree conference in Las Vegas. One of the big topics was the new health care reform package. There is a lot of misinformation being circulated. While the coverage isn't all we hoped for, there are a lot of good things people can use. Lynn Woolsey is running a survey on her web site to find out what the people she represents think the most important provision is. Your choices are:

- Improve coverage for 419,000 Marin and Sonoma county residents with health insurance.
- Extend coverage to 42,000 uninsured residents in Marin and Sonoma counties.
- Give tax credits and other assistance to up to 121,000 families and 20,400 small businesses

- in Marin and Sonoma counties to help them afford coverage.
- Improve Medicare for 101,000 beneficiaries in Marin and Sonoma counties, including closing the donut hole.
- Allow 49,000 young adults in Marin and Sonoma counties to obtain coverage on their parents' insurance plans.

You can put your two cents worth in at www.woolsey.house.gov. To find out more of the true facts go to www.healthreform.gov, scroll down to the map and click on the State you are interested in. Please share this web site with your family and friends.



Southwest Computer Conference
June 4, 5 & 6, 2010—San Diego CA
www.theswcc.org

The Southwest Computer Conference is coming in June. To get the discounted registration fee you need to mail your form by May 15th. All platforms are covered—not just Windows or Mac. There are even door prizes for all platforms. By the way, everybody gets at least one door prize in addition to their bag of goodies and any freebies the vendors give out. Vendors also discount their prices. My one complaint is that I can't possibly see all the breakout sessions I'm interested in. This is one conference that is well worth the money.

—Beth

Neat Things You can do with a Flash Drive

by Vinny La Bash, Sarasota Personal Computer Users Group, Inc., Florida
vlbash (at) comcast.net www.spcug.org

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).

By now you're probably tired of reading about how much better Windows 7 is than Vista. me too, so let's spend some time examining some of the things you can do with a flash drive other than mere data storage. A USB flash drive consists of a flash memory data storage device integrated with a USB (Universal Serial Bus) interface. USB flash drives are easily removable, and much smaller than a floppy disk. They are rewritable, and usually weigh less than an ounce. There is a wide range of storage capacities with the most common being from 2 GB to 32 GB. Higher capacities up to 256 GB tend to be pricey.

One of the most useful things you can do with a flash drive is to run portable applications. Open Office, for example, is a free suite of programs that includes a word processor, spreadsheet, data manager, presentation tool, and drawing package. You can store the suite as a portable application, and run it on any computer that supports Windows. Firefox and Thunderbird are also available as mobile applications.

Having office applications, email, and an internet browser all pooled in a portable drive you can carry on a key chain is a powerful combination. If you want more go to www.portableapps.com for an open source platform that works with iPods and portable hard drives in addition to flash drives. The platform is not only free, but it's a full function site. You are not limited to a trial period or a limited function subset. There is no sign in requirement, and no necessity to provide even an email address. Go for it.

Everyone wants a faster system. With either Windows Vista or Windows 7, the built-in ReadyBoost feature can speed up your computer with a USB flash drive. ReadyBoost takes the storage space on a USB flash drive and converts it into an additional memory cache that supplements the main memory cache on your primary disk drive. It can do this because flash memory is faster than regular disk drives. It's faster because it has no moving parts, and you can get a noticeable improvement in response time. Implementing

ReadyBoost is simplicity itself. Insert the USB flash drive into the USB slot on your computer and follow the configuration prompts.

If you work or live in an environment where other folks have physical access to your computer you can use your flash drive to lock everyone else out of your PC. There is no built-in utility like ReadyBoost for this, but you can download a free tool called Predator from www.brothersoft.com that provides this function. Predator uses a standard USB flash drive as an access control device. After performing a short installation and configuration process, your flash disk becomes a key that will lock and unlock your PC. When you leave your PC remove the USB flash drive. This causes the screen to go blank while disabling the mouse and keyboard. When you ready to resume, put the flash drive back, and everything returns to normal. Move over, Mr. Bond, Predator is here.

All the preceding capabilities are very convenient, but how would you like to carry around a portable operating system? If you are willing to expend a little time and energy you can configure a USB flash drive to be a bootable Windows 7 drive. You will need a flash drive with a capacity of at least 8 gigabytes, and of course a Windows 7 installation disk. Start out by inserting your flash drive into its USB socket and inserting the Windows 7 installation disk in the optical drive. Please make a note of the drive letters. This is essential for successful installation.

Preparing the flash drive is the next step. Click on the Start orb and type: Diskpart

Pressing Enter opens a command window. (After typing a command at the command prompt always press Enter to execute the command.) At the prompt type: List Disk

You will see a list of all your hard drives, partitions, optical drives, card reader drives, and flash drives. Identify the optical drive that contains the Windows 7 installation disk and the flash drive you're working with. For this example we'll assume the flash drive is disk #4, also designated as G and the optical drive is disk #2, also designated as D.

At the command prompt type: Select Disk 4

Run the following commands:

```
Clean
Create
Primary
Partition Select Partition 1
Active Format FS=FAT32
Assign
Exit
```

This series of commands erased extraneous material from the flash drive, created an active primary partition, and formatted it with the FAT32 file system. The next step is to copy the Windows 7 installation files to the flash drive.

At the command prompt type: Xcopy D:*.* /S/E/F G

In this example D is the drive housing the Windows 7 installation disk and G is the USB flash drive. The command copies the installation files to the flash drive, and when it finishes you have a bootable Windows 7 flash drive. The last thing you need to do to make this work is go into the BIOS and make the first bootable device the flash drive.

Carrying a flash drive around is obviously far more convenient than carrying a DVD, and has the additional advantage of being faster than a DVD. This procedure also works for Windows Vista, but why bother when Windows 7 is here?

PC Don - The Senior Tutor

by Don Edrington , columnist for The Californian and San Diego' North County Times

Don shares his varied interest through www.pcdon.com and allows APCUG members to use his material

Limitations of Various Graphics Programs

Regarding some graphics programs I recently mentioned, Marie Anne Lorenzini wrote to say she couldn't find a way to lighten a photo's background in Irfan-view, and AI Roller said the "red-eye correction" feature in Picasa2 doesn't work very well.

Well, all graphics programs have certain strengths and weaknesses. Irfanview, as its name suggests, is mainly an image "viewer," while Picasa2 is mainly an "image organization tool."

Neither program has extensive bitmap-editing features, such as those found in very full-featured programs such as Adobe PhotoShop, PhotoShop Elements, Corel PhotoPaint, and Paint Shop Pro. In these programs, the "red-eye correction" tool does its job with extreme precision, while their "dodge" and "burn" tools allow you to lighten and darken selected areas of a photo.

There is no way I can give a detailed tutorial on programs like, say, PhotoShop Elements, but I can offer some tips to get you going. Let's start with the "**clone**" tool, which copies one area of an image onto a different area. Here's an example:

Using the "Clone" Tool

Let's say you have a snapshot of a two children wrestling on a park's lawn. However, a third child appears behind them, and you just want to see

your two in the picture. Let's further assume that grass is the main background seen in the shot.

With your clone tool you simply press ALT and click on an open area of grass. Next, "clone" some of the grassy area over the third person until he disappears. If this sounds complicated, you will be surprised to learn how easy it actually is. All comprehensive image editors have a clone tool. I'll give more photo-editing tips in the future.

Updated "Picasa" Picture Management Program Free from Google

Picasa, the free image management program has been recently upgraded and is available at www.google.com. What I like most about Picasa2 is its ability organize and display thumbnail views of all folders containing images. I've collected thousands of pictures over the years, and created many folders to hold them. Some of these folders have been copied and saved multiple times, meaning I have lots and lots of unnecessary duplications.

When Picasa2 displays a folder named, say, "July Beach Pics" seven times (each with 50 snapshots) I know I can safely delete five folders and leave one each of the others on my PC hard drive and on my external backup drive.

The program also has many photo-editing features found in other graphics applications, such as contrast and brightness options and "red-eye" correction. However, if you are serious about doing image-editing you might want to consider the 30-

day free trial of Photo-Shop Elements. Adobe PhotoShop has long been the program of choice for professionals; but its high price (\$649) and complex features have kept it from being much interest to the average family photographer.

Smart Computing Tip Of The Day

Smart Computing Magazine sends these tips via e mail. They also have them archived on their website:
www.smartcomputing.com

Things, Thinglets & Thingassoes

by Jack Lewtschuk, Columnist, Monterey Bay Users Group, CA
Blacklion (at) royal.net

<http://www.mbug.org>

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).

The Bad Guys are after Your Money

Well, that's nothing new.

Just as knowing the "computer language" is good to assist communication when seeking help or offering help to others, so is knowing the definition of words to describe cybercrime.

Just to better understand the nomenclature of cyber assaults, one has to be able to understand the lingo. I researched the Internet (some very helpful "e-letters") and came up with this handy list:

"Adware" - A piece of software that displays advertisements on a computer after the software is installed. Adware can be benign, as in the case of a free program that displays ads in a manner that is agreed upon in advance. Or adware can be a nuisance, displaying unwanted ads with no apparent way to remove the program. The nuisance variety is often silently downloaded along with some other desired software, such as a game or toolbar.

"Arbitrary Code Execution" - When a security vulnerability is discovered in a piece of software, sometimes it is said that it allows for "arbitrary code" to be executed on the machine. This really means that the vulnerability can be used to cause that program to execute ANY set of commands or instructions on that computer.

"Black Hat" - A "bad guy" or hacker who breaks into computer networks, creates viruses, sends spam, or uses unethical tactics to influence engine results.

"Ethical Hacker" - A "good hacker" who uses a variety of techniques to test the safety of a computer network or system software. Typically an ethical hacker (also known as a "White Hat") is hired by a company to see if there are any flaws in its systems that might allow Black Hats to gain entry.



Cartoon by Regina Doyle, MBUG-PC

"Botnet" - A collection of ordinary home and office computers that have been compromised by rogue software. The term "botnet" is short for "robot network" and describes the situation rather well. Computers that have been caught up in a botnet have been effectively taken over and can be used to perform almost any task by the person or persons who control the botnet. Botnets are controlled by criminals and other mis-

creants whose motives include spewing spam to sell products, operating financial scams, and crippling websites through coordinated attacks. (See "Denial of Service Attack".)

"Buffer Overrun" - This is a flaw in a computer program that occurs when the length of a user input is not validated. For example, if a program is expecting a 9-digit social security number as input, it should discard any input beyond the 9th character. If the program blindly accepts a longer input string, it could "overrun" the input buffer, thereby trashing some other part of the currently-

running program with the extraneous characters. In some cases, this flaw can be used to overwrite the existing program with code that comes from the input string. (See “Arbitrary Code Execution”.)

“Denial of Service Attack” - A concerted effort by one or more remote attackers that attempts to flood a web server or network with meaningless requests. A sustained, coordinated attack can render the target unable to service the legitimate users who are attempting to connect.

“Exploit” - A method of taking advantage of a bug or security hole in a computer program. It is possible that a hole may be known to exist, but no exploit has yet been created to capitalize on it.

“Malware” - Any form of malicious software. This can include computer viruses, spyware, worms, trojan horses, rootkits, and other software that is deliberately harmful, destructive, or invasive.

“Patch” - A fix for a software bug or security hole. When a bug is discovered, often there is a race by software vendors to provide a patch before an Exploit is created. Patches must be applied to the affected computers in order to prevent exploitation of the flaw.

“Phishing” - The act of stealing information using lies or deception as bait. Online scammers try to trick people into voluntarily providing passwords, account numbers, and other personal information by pretending to be someone they trust. An example of phishing is an e-mail that appears to be from a bank, asking recipients to log in to a rogue site that looks exactly like the real one. When the victim logs in, the operators of the fake site then have that person’s login credentials and can access his or her bank account.

“Rootkit” - A rootkit is a software tool (or a set of programs) designed to conceal files, data, or active processes from the operating system. Because of their ability to hide deep in the operating system, rootkits are hard to detect and remove. Although rootkits may not cause damage when installed, they are often piggy-backed with additional code written for the purpose of taking control of a computer, disabling certain functions, or spying on the user and reporting activities back to the rootkit creator.

“Scareware” - Software that is created for the purpose of tricking people into downloading or purchasing it, when in reality it is either unnecessary, marginally useful, or outright dangerous. Online ads that display fake warnings such as “Your computer may be infected—click here to

scan for viruses” or “ERROR! Registry Damage Detected—click to download Registry Cleaner” would qualify as scareware. Scareware programs often run a fake or cursory scan, then present the user with a list of hazards that must be corrected. Fixing these “problems” then requires the user to pay a fee for a “full” or “registered” version of the software.

“Skimming” - The act of stealing credit or debit card information while a legitimate transaction is taking place at an ATM (Automatic Teller Machine). Skimming involves an unauthorized device that is attached to the card slot of the ATM, which reads the magnetic strip as the card passes through. A hidden camera may also be used to capture the victim’s PIN (Personal Identification Number).

“Spyware” - Spyware is a type of malicious software designed to take action on a computer without the informed consent of the user. Spyware may surreptitiously monitor the user, reporting personal information to a remote site, or subvert the computer’s operation for the benefit of a third party. Some spyware tracks what types of websites a user visits and send this information to an advertising agency. Others may launch annoying popup advertisements. More malicious versions try to intercept passwords or credit card numbers.

“Trojan Horse” - A Trojan horse is a malicious program that is disguised or embedded within other software. The term is derived from the classical myth of the Trojan Horse. Such a program may look useful or interesting but is actually harmful when executed.

Examples may include web browser toolbars, games, and file sharing programs. A Trojan horse cannot operate or spread on its own, so it relies on a social engineering approach (tricking the user into taking some action) rather than flaws in a computer’s security.

“Virus” - A computer virus is a malicious self-replicating computer program that spreads by inserting copies of itself into other programs or documents, similar to the way a real virus operates. When the infected program or document is opened, the destructive action (payload) is repeated, resulting in the infection, destruction, or deletion of other files.

Sometimes the infected programs continue to function normally, albeit with the side effects of the virus; in other cases, the original program is crippled or destroyed.

“Worm” - A worm is a malicious computer program that is self-contained and does not need help from another program to propagate itself. It can spread by trying to infect other files on a local network or by exploiting the host computer’s e-mail transmission capabilities to send copies of itself to everyone found in the e-mail address book. Some even look in the cache of recently visited web pages and extract other e-mail addresses to target.

“Zero-Day Exploit” - An attack that tries to exploit unpatched security vulnerabilities. The term “zero day” derives from the fact that software ven-

dors sometimes have a window of time to fix a problem before an exploit is developed or before news of a vulnerability is made public. But when the exploit already exists before a patch is released, the vendors have “zero days” to fix it because users are already exposed.

“Zombie” - A computer that has been compromised and can be controlled over a network to do the bidding of a criminal or miscreant. Computers that have been caught up in a botnet are zombies and can be used by the controller of the botnet to send spam or participate in a coordinated denial of service attack.

Email Scams

by Vinny La Bash, Sarasota Personal Computer Users Group, Inc., Florida
vlabash (at) comcast.net www.spcug.org

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).

There are at least two dozen people in Nigeria that want to give me twelve million dollars. Imagine that! People are vigorously competing with each other to make me rich. You would think that after all the publicity over the last dozen years everyone would know about the Nigerian scam. Headhunters in New Guinea know about the Nigerian scheme. Lost tribes in the Amazon know about the Nigerian scheme. So why do the scammers keep doing it? Because people keep falling for it. Some folks want to believe, and nothing will stop them no matter what evidence sits in front of them.

Email scams like the one that keeps flowing out of Nigeria can be downright dangerous. Not only have people been scammed out of money, but in a few instances have actually lost their lives. That is a high price to pay for credulity.

Most unsolicited commercial messages (SPAM) may be annoying, but they do little more than eat up some bandwidth. The originators don’t want to harm you, just entice you to buy something. It’s sometimes called online advertising.

As the Internet evolves, so do the scammers. They have become more sophisticated at attempting to trick us out of our money, hand over personal information, reveal passwords, frighten us or make us believe in something that isn’t true.

For example, our current polarized political sys-

tem has generated distrust of government in some places. A band of swindlers has used these sentiments to construct an email that “warns” you that the Department of Homeland Security and the FBI believe that you are involved in either money laundering activities or somehow complicit in terrorist activity. Information like that, even if false, can make people uneasy.

Fortunately, the scammers have a solution. For the small sum of \$370 the Economic Financial Crimes Commission Chairman will send documentation certifying you as a proper upstanding citizen, thereby avoiding a messy prosecution and jail time. How could anyone pass that up? These government agencies must be terribly busy, and isn’t it a great comfort to know that they can resolve important matters by email if you’re willing to send them only a few hundred dollars?

Congratulations! You’ve won the lottery! There are many variations to this theme, but they all involve filling out a form before you can claim your prize. Don’t forget to include your social security number since they need to inform the IRS. What makes this scam so devious is that legitimate lotteries really do need this information. One thing that should puzzle you is how could you possibly win a lottery you haven’t entered?

Suppose you really did enter the contest or bought a lottery ticket, what then? Legitimate enterprises are aware of these scams and will almost always provide you with an alternate way of supplying the information. In other words, never be careless with personal information.

You receive an email informing you of a “problem” with your bank account. Strange, you don’t recall doing business with the bank. All you have to do to resolve the “problem” is click on the provided link and supply information that the bank already knows if you are a customer.

Tens of thousands of people receive these messages. A few may actually be customers of the bank. Some believing the email is real, click on the link, and are taken to a bogus site. Any information provided won’t be used to resolve any “problems”, but instead be used to clean out your bank account.

There are so many scams out there perpetrated by email it makes you want to give up in disgust. That would be understandable if there were no way to protect yourself, but many people forget the obvious: **Use Common Sense.**

When you get an email that asks you to be part of a plot to move large amounts of money offshore to your bank account by doing business with people you don’t know from a foreign country thousand of miles away, shouldn’t that arouse your suspicions?

Any text message that turns out to be an image should be suspect. The only purpose for turning text into images is to defeat spam filters. Be on your guard.

The bad guys are very creative and always seem to be one step ahead of everyone else. The FBI provides a service for citizens to receive the latest information about online scams. For more information on e-scams, please visit the FBI’s New E-Scams and Warnings webpage at <http://www.fbi.gov/cyberinvest/escams.htm>.

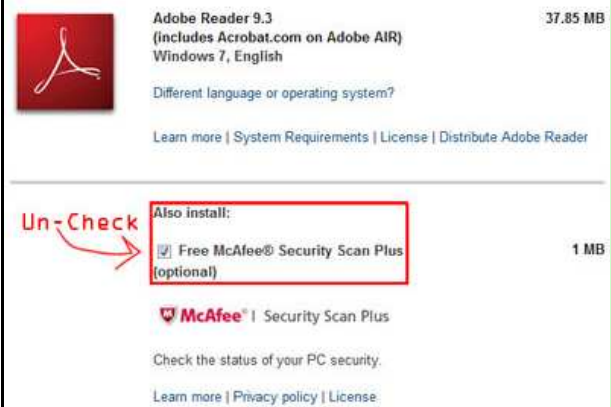
Here’s a heads up from Andrew at World Start:

Tag Along Software

Never heard of it, have you? That’s because I’m making a name for it right now. If anyone out there has tired to download a program like Adobe Acrobat or Flash Player, you may have noticed there’s now a pre-selected option to also install additional program like McAfee Security Scan.

You don’t really need that, do you?

Yeah, me either. So make sure you un-check it before you hit that download button.



I venture that we’ll be seeing more of this type of “tag along” software in the future, so always make sure to read carefully before agreeing to anything!

[fbi.gov/cyberinvest/escams.htm](http://www.fbi.gov/cyberinvest/escams.htm). Visit the site at least once a month to be aware of new and exciting ways scammers have to separate you from your money.

Smart Computing Tip Of The Day

Software On A Portable Drive

One of the cool things about mobile drives is that many of them come with portable applications, meaning programs you can run directly from a drive without installing anything on a public or borrowed computer you’re using. Not only does this make it more likely that you’ll be allowed to borrow a PC a second time, but it also lets you have the same settings and the same productivity software wherever you go. Another plus: Some portable browsers will let you access the Internet anonymously without leaving a trace of your activities on the host PC.

Smart Computing Tip Of The Day

Tabs In Web Browsers

The next time you need to have two Web pages open at once, or you want to be able to easily backtrack to a page you’ve already visited, utilize your Web browser’s tabbed browsing option. Instead of opening an entirely new window for each Web page you have open, this feature (available in most browsers) will add a tab to the top of your current Web browser window with another Web site page opened. When you want to toggle between the different Web sites you’ve visited, simply click on the tabbed Web page you want to see. Most Web browsers will let you open a new browser tab by pressing CTRL-T.

Travelin

by Gregory West, Editor for the Sarnia Computer Users' Group [SCUG], Canada
prospector16 (at) gmail.com www.scug.ca

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).

oad travelers.

Travelin

by Gregory West, Editor for the Sarnia Computer Users' Group [SCUG], Canada
prospector16 (at) gmail.com www.scug.ca

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).

oad travelers.

Travelin

by Gregory West, Editor for the Sarnia Computer Users' Group [SCUG], Canada
prospector16 (at) gmail.com www.scug.ca

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).

oad travelers.

Travelin

by Gregory West, Editor for the Sarnia Computer Users' Group [SCUG], Canada
prospector16 (at) gmail.com www.scug.ca

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).

oad travelers.

Travelin

by Gregory West, Editor for the Sarnia Computer Users' Group [SCUG], Canada
prospector16 (at) gmail.com www.scug.ca

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).

oad travelers.