The Rochester Computer Society, Inc.
Since 1982

MONITOR

Vol. 30, No. 10 October 2012

Next Meeting
Tuesday, October 9

Inform Your Investing Using Computers II
Dennis MacMahon

Contents

apcug Member of the Association of Personal Computer User Groups

Secure Your Wireless (WiFi) Connection

by Ira Wilsker

Almost all newer laptop computers as well as tablets, smart phones, video game consoles, and home entertainment systems utilize WiFi as a primary or secondary method of connecting to the internet or some other network. According to published reports from several sources, the majority of home internet users have some form of WiFi in their homes, and WiFi is very commonly used in business, commercial, and academic environments. While the

basics of WiFi security apply to almost all WiFi networks, home users have become especially vulnerable because many have never implemented anything more than the minimum default security settings when installing and setting up the hardware.

The Wi-Fi Alliance (www.wi-fi.org) defines WiFi as any "wireless local area network (WLAN) products that are based on the Institute of Electrical and Electronics Engineers' (IEEE) 802.11 standards."WiFi is a fancy radio device that sends and receives streams of data through the air, just as any other 2-way radio device. As consumers, we often see the presence of WiFi in terms of its standard designations, such as 802.11b, g, or n (as in 802.11n), each of these terms indicating the speed, bandwidth, and channels available under those industry standard protocols. While new speeds and protocols are always being developed and tested, the fastest and most powerful of the current widely available standards is 802.11n, which is capable of a theoretical speed of 540 Mbps. A portion of the standard provides for downward com-patibility, meaning that devices made for one of the newer standards, such as the "n" standard, must also be capable of communicating with lesser devices, such as the "b" and "g" standard devices.

For home use, most of us have some form of WiFi access point, typically either a free standing device directly connected to the internet, integrated with a wired (Ethernet) router, integrated with some form of modem (common with cable and D.L. internet services), or as a combination unit of "all of the above." In my home I have a major name-brand integrated unit that combines a broadband modem, 4-port router (four Ethernet ports for Ethernet cable connected devices), a USB port to connect a printer or other USB devices to the network, and an 802.11n wireless WiFi with MAMO (Multiple-Input-Multiple-Output technology) for improved performance. Purchased from one of the big box electronics stores for about $70, my multi-function device replaced the less-capable modem supplied by my internet service provider (ISP), and offers more features, speed, and security than the one provided by my ISP.

For me, enhanced security was one of the primary reasons for replacing the older technology modem provided to me from my ISP just a few years ago. This older broadband WiFi modem from my ISP incorporated the mid-speed 802.11g wireless access point, with archaic security and encryption capabilities. Being fully cognizant that home (and business) WiFi networks are common targets of hackers and crackers, I wanted to harden my system from attack, and the newer integrated WiFi access point offered far superior protection than did my ISP provided unit.

One of the first requirements of a reasonably secure WiFi network is to implement the best encryption available on that particular device, such that unauthorized individuals who pick up the WiFi signal will only find random garbage, rather than a useful stream of data. Since only WiFi devices with the proper encryption key can exchange readable data, enabling the best type of encryption compatible with both devices (access point and remote device) will help protect the personal WiFi network from intrusion. Unencrypted WiFi leaves the entire network open to attack which can be used to steal personal data, passwords, user names, credit card information, and other information that can be illicitly used for a variety of malevolent purposes, including identity theft. At a minimum, an unencrypted home WiFi network works like a free open network at a coffee house, where anyone can "leach" (steal or otherwise use) your internet access, slowing your connection, as the crooks are using your bandwidth. This "leaching" or theft of internet service may lead to unintended consequences, as it is not unknown for illicit drug dealers, pedophiles and child pornographers to use an innocent persons unprotected WiFi in order to conduct their evil enterprises; if law enforcement tracks the bad guys, it typically leads to the innocent WiFi owner, rather than the miscreant who purloined the system.

A common game of hackers and crackers is "War Driving" (en.wikipedia.org/wiki

/War_driving) where people with WiFi computers and some readily available software drive around an area picking up and recording the locations of all detectable WiFi networks, and posting the locations on a GPS coordinated electronic map. Even Google compiled a massive listing of WiFi networks as its specialized vehicles traveled up and down virtually every street in the country for its Google Maps "Street View" service, creating a massive firestorm with privacy and security specialists. While Google has graciously removed public access to its "war driving" database, there are a myriad of websites that post the maps and data found by amateur War Drivers, such that anyone can easily locate and tap into an unencrypted WiFi system. Parallel to war driving is war chalking, war walking, war jogging, and war bicycling, which is common in densely developed urban areas. The simplest iteration of these is to use chalk on the side of a building or sidewalk to show the presence of a vulnerable WiFi system, telling anyone on the street about the unfettered broadband internet access, compliments of an often unwilling provider. There is actually a standardized list of chalk symbols indicating the type and availability of WiFi signals, these symbols being available from en.wikipedia.org /wiki/War_chalking.

Virtually all WiFi access points offer some form of encryption. During the initial setup of the WiFi system, the user is often requested to select an encryption method, or else "no encryption" is often the default setting, making the network accessible to anyone within range. The most common forms of encryption for WiFi access points are WEP, WPA, and WPA-2. WEP (Wireless Encryption Protocol) is the oldest and least secure of the common encryption methods; while only having slight degradation in performance and speed, it is virtually useless against all except the least sophisticated hackers, with instructions on how to crack and defeat WEP being readily available on the internet. WPA (Wi-Fi Protected Access) is better than WEP in terms of security, but degrades performance a little more than WEP. On most contem-porary home WiFi access points, WPA-2 is the best of the commonly available encryption methods, but is slower and requires more computing resources then WPA; except for the most bandwidth intensive uses, the majority of users will not really notice the slightly slower performance of WPA-2.

Another security trick embodied in almost all WiFi access points is the "Hide SSID" setting. SSID means "Service Set Identifier," also called "Network Name." At a minimum, the user should change the network name to some meaningless name that is not readily connected to the particular system. The reason for changing from the factory default name (often the name of the manufacturer, such as "Linksys") to a nondescript name is that there are online directories with default encryption and password settings for unmodified WiFi access points; hackers can easily break into networks that are only using the factory default settings. An even better trick, if available on the WiFi access point, is to totally hide the SSID, meaning that the network name is not openly transmitted, and only those in range who know the network name can connect to it. While not foolproof or totally secure, hiding the SSID is a simple way to make it more difficult for hackers to find your network. If war driving through your neighborhood, hackers may likely miss networks with a hidden SSID, while picking up the other, possibly more vulnerable neighborhood networks.

Another feature that can be enabled to restrict unauthorized access to your home network is "MAC address filtering" (Media Access Control). Every device that can connect to the internet has a unique MAC address, usually a series of about six two-digit alphanumeric characters separated by periods. While MAC addresses can be counterfeited or spoofed, filtering only allows selected devices, as indicated by their individual MAC addresses, to access the network. By entering the authorized MAC addresses into the filter, and enabling the filter,

only those approved devices can connect to the network. Likewise, the filter can prevent specific devices from accessing the network.

On my laptop computer and on my smart phone I can see several nearby homes that have WiFi, some of which are not properly encrypted and accessible to anyone within range for any purpose, including illegal or other illicit activities. I cannot easily see networks with a hidden SSID. The unprotected household WiFi networks are so vulnerable, when one neighbor had his home broadband connection out of service, and was waiting for the ISP to come and repair it, he illegitimately used another neighbor's WiFi until his was repaired. Do you really want someone else using your network without your permission or knowledge? Secure your WiFi, or face the possible consequences.

Websites:

http://www.makeuseof.com/tag/7-important-features-wireless-router
http://compnetworking.about.com/od/wirelesssecurity/tp/wifisecurity.htm
http://wiki.answers.com/Q/How_do_I_change_my_wireless_network%27s_security_settings
http://en.wikipedia.org/wiki/WiFi
http://www.wi-fi.org
http://en.wikipedia.org/wiki/War_chalking
http://www.blackbeltjones.com/warchalking/warchalking0_9.pdf (Pocket War Chalking Card)
http://en.wikipedia.org/wiki/War_driving

Why Is Printer Ink So Expensive?

Reprinted from *PCWorld*

The short answer: Because printer manufacturers can get away with charging you that much. Without ink, your printer is just a big paperweight, and companies like Canon, HP, and Lexmark know it. That's why they can afford to sell printers for under $100; they're betting that most printer owners will continue to invest in ink cartridges that may cost $20 to $40 a pop over the course of several (or many) years. Third-party refilled or remanufactured ink cartridges may be a lower-cost alternative, but some are messy to install or deliver inferior print quality.

That's because printer ink is surprisingly difficult to replicate. But perhaps we shouldn't find this difficulty so surprising. Even consumer-grade printer ink is a technological marvel–capable of remaining fluid at extremely high temperatures, and then drying instantly on paper after being shot through a tiny nozzle at a speed of roughly 30 miles per hour. Good luck getting your ballpoint pen cartridges to match those requirements!

Of course, printer ink is less expensive if you buy a printer that matches your printing needs. Melissa Riofrio, *PCWorld* senior editor and printer aficionado, has spilled plenty of ink in the process of reporting on the printer industry over the years; her testing suggests that purchasing a more expensive printer ($200 or above) is usually a smart decision if you print more than 250 pages per month, as ink and toner replacements for expensive printers tend to cost less than replacement cartridges for cheaper models. However, if your print output is less than that, stick with the cheapest printer that meets your needs.

Flash Memory Survival

by William Tracy

Just how tough is an HP 1GB Flash Memory Drive? In Glendale, a unit has been tested. In August 2010, Bill Tracy left an HP in his Dockers when he washed his clothes. Could the HP survive this kind of abuse?

The HP was in his front-right pocket when it endured the mishandling. The Speed Queen commercial washer was set in Normal Permanent Press so dockers were washed in hot water at 110 Degree F. using 1 cup of Tide Detergent powder. Following the wash and rinse cycles, the trousers also went through a full high-speed spin cycle to wring out the wetness.
Then the Dockers were thrown into a Speed Queen Commercial dryer where it collided with steel surfaces. At some point the HP escaped the Docker pocket and endured harsh crashes inside the Dryer. Afterwards, the HP End Cap was still attached.

When the Dryer stopped, all the clothing was removed but the defiant HP stood up leaning against the wall like John Wayne after a gun fight. The solitary figure was immediately identified and removed from the Dryer. But there was serious doubt about any memory left in the unit.

However, when plugged into a Dell computer USB port, all the recorded data was still there. Nothing was missing. It had survived.

So now we know. HP Flash Memory Drives are indeed tough! Can any of the other manufacturers make that boast?

From TUGNET, the Users Group Network, La Crescenta, CA.

LinkedIn Helps You Fill the Seats at Your Next Event

posted by Wayne on the net

At the end of summer our thoughts typically move back into work mode full force, as we attempt to finish the year strong. Sometimes this includes hosting business-related events.

Many people have not even discovered the LinkedIn Event Application, let alone all the other features that can help them boost attention and ultimately attendance at their event. Thus, I thought I would share my best practices for using LinkedIn to promote events.

13 Ways to Effectively Promote Your Upcoming Event Using LinkedIn

Start by using the LinkedIn Event Application to actually post the event details so the event can be found if LinkedIn users are searching for events in your area.

Events is an optional application that you download by selecting the "More" tab on the top toolbar and scrolling down to "Get More Applications." Go through the download process, and then you will be able to add your event to the LinkedIn calendar for all to see and RSVP.

After individuals RSVP, a status update goes out to their network, and the event entry remains on their profile for all future reviewers of their profile to see. You will be amazed how many people will become aware of your event because they see an entry about your event on other people's profiles.

When creating the event on LinkedIn, you get a chance to tag the event with two different things — keywords that describe the event and titles of the people you think should attend the event. You get 20 keywords and 20 titles; so don't be stingy. Think about all the different titles and keywords people may use, not just the ones you use regularly.

Immediately after creating the event, LinkedIn will prompt you to share this event with a selected group of your connections. This is a great feature to get the word out to people you think would benefit from the event.

During the time leading up to the event, you will want to periodically visit the event page and use the "Share" button to re-invite connections or invite additional connections who were not previously invited. You can also use the "Share" button to share to your groups, your Twitter account, and individuals not even on LinkedIn directly via their email.

Leading up to the event, use your Status Box several times in order to promote the event. Change up the topic of the update and include information like the theme of the event, venue, speakers, etc. Use a URL shortener, like budurl.com or tinyurl.com, to link them directly to the LinkedIn event. This will enable you to use more of your 148 characters for your comments.

Start a discussion to promote your event in the LinkedIn groups that would most likely attend the event. Do this multiple times leading up to the event date. Change up the discussion/comments to generate interest. Always include the link to the event details.

Use the Advanced Search to prepare a list of people you will contact directly, via phone or email, by using keywords (probably the same tags you used above).

Go to the Advanced Search in the Event Application and see if there are any similar events going on in the area, and review the RSVP list to see if you should directly invite any of those individuals to your event. You will need to either be connected to that person directly or through a group. This is just another benefit of joining several regional super groups like Link Up Milwaukee or the Milwaukee Business Professionals Group.

Ask a few of your closest connections who have already RSVP'd for the event if they would consider either inviting some of their connections or using their Status Update to promote the event.

Ask a few of your most connected connections to "Like" or "Share" your status update on their homepage or with their connections or groups.

If the event is far enough in the future, consider starting a group just for the promotion of the event, and be sure to post updates to the agenda, speakers, RSVPs, and solicit input from the group members.

Upload a pdf version of the event brochure into your Box.net files. You may want to mention this in your Summary section so people realize that it is there.

Create a short video promoting the event. This could include clips from last year's event, an interview with the keynote speaker, testimonials from attendees of previous events, etc. This video can then be put on the profiles of all the board members, committee members or others involved in the event in either the Website section (as a hyperlink) or in the SlideShare or Google Presentation Application.

You may want to consider adding a statement in your Summary that would say something like, "See the Google Presentation below for a video of what you can expect at this year's benefit gala."

Do You Have a Digital Estate Plan?

by Bob Rankin

What will happen to your email, Facebook, iTunes and Amazon accounts if you die? It's an uncomfortable question, but leaving it unanswered can be vastly more distressing and costly for your loved ones who survive you. Here are some tips on setting up a digital estate plan...

You Can't Take Them With You...

Recently, there was a rumor that actor Bruce Willis was planning to sue Apple for the right to leave his iTunes music collection to his children. There was also a story about Steve Jobs

being reincarnated in a parallel world. The Willis rumor was debunked, and I'm pretty sure that Steve won't be checking his email any time soon.

Sooner or later, we'll all kick the bucket, buy the farm, or shed the mortal coil. But when you go, what will happen to your online accounts? You may or may not be content to just leave your Gmail or Facebook account dormant. You may have photos or documents in cloud storage. What if you have money in your Paypal account? And will your surviving relatives have the keys to your online banking or investment portfolio?

Also keep in mind that email and social network accounts can get hacked. Families and friends have been traumatized by spam sent from the accounts of the deceased. It can be difficult for survivors to get online accounts shut down after someone dies. Sometimes, it requires an expensive lawsuit or other court action.

Facebook, Twitter, Gmail, and some other major online services have procedures for handling the accounts of deceased members. In most cases, they require faxed copies of a death certificate, the photo ID of the requestor, and a notarized statement of authority. But Amazon, Grooveshark, Foursquare, and many others don't publish any infor-mation about dealing with deceased members' accounts. The DeceasedAccount website offers a handy guide to the deceased-member policies of many online services.

The simplest solution is to write down all of your accounts and their login credentials, then give that list to someone you trust. Of course, you'll have to remember to constantly update that document when you change passwords or create new accounts. But what if you don't trust anyone with all of your digital keys, at least while you're still alive?

Digital Estate Planning Tools

DeadmansSwitch.net lets you send emails after you die. An email to your executor, for instance, might contain a list of accounts and passwords or a full-blown digital will and testament. The service sends a check-in email to you every so often; you confirm that you're still alive by clicking on a reply link. If you don't reply within 60 days, you are presumed to be dead and your stored emails are sent. The free version supports up to two recipients. For a one-time fee of $20, you get up to 100 recipients and the ability to customize the check-in intervals and reply deadline.

SecureSafe.com adds cloud storage to the posthumous email solution. You can upload documents and other files that will be sent to recipients upon your presumed death. Each file gets assigned to a beneficiary, so you can leave different things to different people. The free version supports storage of up to 50 account passwords, while paid versions provide more storage space and security such as two-factor authentication that beneficiaries must provide to access their bequests.

The Digital Beyond is a news and information site devoted to digital estate planning. It offers a directory of services similar to those mentioned above; links to news articles on the subject; and a book called, "Your Digital Afterlife" that can help you consider what your digital legacy should be and set it up according to your final wishes.

What do you want done with your email after you die? Many people want a relative to login and send a message to all contacts with their news of their passing.

Should your Facebook page be closed or converted into a "memorial page"? How much money do you keep in Paypal, and who should get it when you die? How about your digital

photos stored on Flickr? Do you have a blog or website that may need to be closed down? These and many other questions are worth answering before you go.

Amazon "Glacier" Offers Ultra Low Cost Backup Storage

by Ira Wilsker

Amazon has developed a well earned reputation as a seller of goods. Originally an online book seller, Amazon diversified into consumer and institutional goods, digital books and music, and a variety of other services. Recently, Amazon announced what may be the lowest cost, commercially available "cloud" data storage for long term archival or backup services. Amazon has enormous data capacity, with countless servers and related data storage located in many places around the globe. With the price of data storage plunging precipitously, Amazon has entered the commercial data storage and backup business. As Amazon has had a reputation of supplying goods at highly competitive prices, this new backup service, known as "Glacier" substantially undercuts its competitors in terms of price, with storage being available for as little as a penny per gigabyte per month; at that price a terabyte of storage (1024 gigabytes) would cost only $10.24 per month at the base rate. According to a recent article in "Digital Inspiration," If your hard drive has 100 GB of data – videos, photos, and other important files – that you would like to preserve forever, you can transfer all these files to Amazon Glacier and the annual bill would just be a little over $10."

"Glacier" is an appropriate moniker, as this service is intended to be long term "cold storage," rather than storage that is frequently accessed. According to Amazon, there are no up-front costs to set up a storage account and you "Pay only for what you use. There is no minimum fee." While anyone may use Glacier, it is most appropriate for large agencies or businesses, rather than for personal data storage. For those who desire rapid and frequent access to stored data, Amazon offers its "S3" backup and storage service, which is much more expensive. Using the same 100 GB example above, storing that amount of data on S3 would cost about $150 per year, compared to Glacier's $10 per year, but on S3, the data is much more accessible.

Because of its geographic diversity, as Amazon sells its goods and services in many countries, Amazon offers this Glacier storage at five locations, Virginia, Oregon, California, Ireland, and Tokyo. Glacier is designed to be an extremely low cost service that provides secure storage of data for backup and archiving. Glacier is not intended to be used like a hard drive, where data can be quickly accessed and processed, but is instead intended for data that is infrequently accessed, and where immediate access to stored data is not necessary; Amazon says that it may take "several hours" to retrieve data from this system. There is no minimum or maximum amount of storage that must be purchased, and all of the data, regardless of quantity or size, is stored for as little as a penny per gigabyte per month with the user only charged for the space actually used, and an additional fee for data that is accessed or downloaded. There are no advanced or other up-front charges to use Glacier, and the user may freely increase or decrease storage space as needed, again only paying for space that is actually used. There is a very nominal one-time data transfer fee for transferring your files from your personal drive to Glacier, called an "Upload and Retrieval Request" of five cents per 1000 requests, meaning that 10,000 files can be uploaded for a one-time charge of fifty cents.

For those who have a large volume of data that needs to be securely stored in Glacier, but who do not have adequate bandwidth or upload speed to efficiently send Glacier massive amounts of data, Amazon offers an alternative to uploading the data via the internet. The user can send Amazon a digital device, such as a hard drive, USB flash drive, or other form of digital media; Amazon will then upload the files directly into its S3 servers, and then return

the device to the user. Once on Amazon's S3 servers, the data can be quickly transferred to the more cost efficient (but less accessible) Glacier service, or remain on the more expensive S3 servers. Amazon charges a flat rate of $80 to copy a storage device, plus $2.50 per hour of loading time, so larger capacity devices are more cost efficient for the user. Using the same 100 gb example above, Amazon would charge about $85 (complete) for it to load the 100 gb drive to the server; the $80 device fee, and about 2 hours of load time at $2.50 per hour. there are no limits on how many devices can be sent to Amazon for uploading.

From the user side, Amazon provides the "AWS Management Console" to setup the storage, and upload data. AWS is an acronym for "Amazon Web Services," a web based utility that, "...provides convenient management of your computer, storage, and other cloud resources." Data is stored in Glacier as "archives" which may contain a single file, or many files, and is uploaded as a single unit or archive. In order to store data in Amazon's Glacier, a vault is created and named. While the volume of data storage is unlimited, the user is limited to creating a maximum of 1000 vaults in each of Amazon Glacier's five regions (Virginia, Oregon, California, Ireland, Tokyo). Into each vault the user can upload countless archives, with the 40TB limit per archive. The archive packages are securely stored and organized in virtual "vaults." These vaults are created by the user using the AMS Management Console. Each archive is limited to 40 terabytes, and there is no limit to the number of archives that can be stored on Glacier. The vaults are heavily encrypted (AES-256), and accessible by using Amazon's "IAM" Identity and Access Management service.

According to a blog posting by Werner Vogels, Amazon's chief technology officer, "The service redundantly stores data in multiple facilities and on multiple devices within each facility." Amazon claims that with the redundant storage in the cloud, files will have an "... average annual durability of 99.999999999%," meaning that if 100 billion files or other objects are stored in Glacier, only one will be lost in any year.

Since Glacier is intended as stable, long term cold storage, retrieving files and data from Glacier is slower, and entails some cost. To retrieve an archive from Glacier requires that a job is initiated, which may take three to five hours to complete. There may be a fee for retrieving data in excess of 5% of the amount of data stored; up to 5% of stored files may be retrieved each month for free. Past that 5% free data retrieval cap, Amazon charges 12 cents per gigabyte downloaded, for the first 10 terabytes, with a descending rate for downloads greater than that. There is also a three cents per gigabyte fee for deleting newly uploaded files within 90 days.

Amazon offers a variety of other data storage and retrieval services, one of the most popular being its Simple Storage Service, known as S3. As stated previously, the data stored on the S3 servers are more accessible than they are on Glacier, but at a price. S3 offers a Free Usage Tier, where new Amazon Web Services (AWS) customers receive 5 GB of Amazon S3 storage, 20,000 Get Requests, 2,000 Put Requests, and 15GB of data transfer out each month for one year. Beyond the Free Usage Tier, up to a terabyte of storage is available for 12.5 cents per gigabyte per month for redundant storage, and 9.3 cents per gigabyte per month for a reduced redundancy storage system; the rate decreases significantly with larger volumes of storage. There are no inbound fees for uploading data to S3, but there are fees for downloading data, starting at 12 cents per gigabyte, again decreasing with volume.

There are some free alternatives available for remote backup and storage; Microsoft offers its free SkyDrive service (skydrive.live.com), with a 7 GB limit on free storage (users who signed up earlier this year had a 25 GB limit), and Google offers its Google Drive (drive.google .com), free for the first 5 GB of storage. Several other online services also offer free online

backups with various limits on the amount of free storage. There are many other sellers of commercial backup services, with varying prices and services.

With the three most important words in computing being, "Backup!, Backup!, Backup!." Amazon, Google, Microsoft, and other providers of backup services provide a cost effective and secure alternative to the more traditional on-site backup methods. These cloud based backup services are very worthy of consideration.

WEBSITES:
https://aws.amazon.com/glacier/
http://www.labnol.org/internet/amazon-glacier-for-online-backup/25000/
http://en.wikipedia.org/wiki/Amazon_Glacier
http://www.webmonkey.com/2012/08/amazon-glacier-backup-all-your-data-for-pennies-a-month
http://www.zdnet.com/amazon-launches-glacier-cloud-storage-hopes-enterprise-will-go-cold-on-tape-use-7000002926/
http://aws.amazon.com/s3/
https://skydrive.live.com
https://drive.google.com

VIPRE

by Susan Kennedy
TUGNET, CA

What, you ask, is VIPRE? The name is an acronym for Virus Intrusion Protection and Remediation Engine. More simply, VIPRE by GFI Software Inc. (formerly Sunbelt Software) is a product line that includes both a stand-alone antivirus program and a more comprehensive internet security suite.

Dodi Glenn, Product Manager for GFI, started by asking us "What is malware? What dangers are out there?" Malware includes adware, bots, dialer programs, keyloggers, rogue anti-virus programs, rootkits, and spyware along with the usual viruses, worms, and Trojans. He described malware as having "gone wild" with a huge increase in recent years. The purpose is no longer to damage people's computers; the motive today is almost 100% financial. Cyber criminals want access to your computer, your passwords and account information, and thus to your money! Besides stealing from your accounts directly, crooks make fortunes in selling credit card information. Much of this criminal activity originates in Russia and China.

Top threats include various forms of Java script. Some of the threats he named are the System Restore Rogue and S.M.A.R.T. Repair that may harm your hard disk drive.

A few threats created by governments have escaped into the world at large. We probably all know of the Stuxnet virus, believed to have been created to wreak havoc with Iran's nuclear program, but coming along today is Duqu, first spotted in September 2011. Another is Flame, a program developed by the CIA, NSA, and Israeli military, to attack nukes in the Middle East. For those of you who are fluent in high-level "geek-speak," GFI produced a video (33 minutes) on their analysis of Flame at http://vimeo.com/44382073; it's pretty heavy on the technical stuff.

Another type of threat involves social engineering, and many of these come out of India. One example spoofs Microsoft's tech support center, where a person calls on the telephone to tell you of a problem with your computer that he can fix if you just allow him remote access. The Better Business Bureau published an article you can read at http://tinyurl .com/7noulky. You can also see videos on this threat on YouTube by searching for Microsoft Service Support Center.

Where does this malware come from? Today it's mostly social networking (e.g., Facebook), online games, and email or through "portals" you access either for games or chatting in forums.

Malware (including spam) gets into your email through hacked web sites you visit, instant messages (such as posting on Facebook), and what are known as "exploits" in valid programs such as PDF, Java script, and Flash Player.

One threat few recognize is the "lost" flash drive. If you find a flash drive dropped in a parking lot or lying on a library table, for example, the natural instinct is to plug it in to a) see if the owner's name is available or b) just to see what might be on it. Don't do it! That drive may have been left intentionally because it was deliberately infected with malware (such as a keylogger or remote dialer) that will infect your computer when you try to access the info.

Dodi then described the steps one should take if your computer becomes infected or you suspect it may be.

< Be sure you have a good up-to-date antivirus program on all machines before you access the internet.
< Scan all your machines if you are on a network.
< If you discover a worm or virus on one machine, unplug it from your network.
< Get VIPRE Rescue from http://live.sunbeltsoftware.com or http://live .vipreantivirus.com; then restart your machine in Safe Mode and run the Rescue program. When the report displays, any entries in red are serious threats that must be removed.

Some other good anti-malware programs that Dodi recommends (many free) are Malware Bytes (www.malwarebytes.org)

< Super Anti-Spyware (www.superantispyware.com)
< TDSS Killer (www.super.kaspersky.com/)
< ComboFix (www.bleepingcomputer.com/download/anti-virus /combofix) and
< HijackThis (from any of several sites such as www.majorgeeks.com or www.filehippo.com.)

How can you prevent these threats from getting to your computer?

< Keep Adobe Flash Player and Java updated.
< Disable Java scripts from running in Adobe.
< Disable the function that lets your browser open PDF files automatically.
< Keep your operating system patched and updated.
< Use a reliable anti-virus program or internet security suite.

Some other tips Dodi offered include:

< Don't click links that you find in emails or on web sites; or at least do so with great caution.
< Be very wary of attachments to emails, even from people you know. The bad guys may have "spoofed" your friend's email address and sent you malware.
< Use a "site advisor" such as Web of Trust or MacAfee's Site Advisor. These program add-ons check web sites to see if they are safe and secure for you to visit. Web of Trust (WOT) (www.mywot.com) is one that works in all browsers. It is community driven; that is, it is run by its users. When you are checking a web site, a red circle means the web site is infected.
< Watch your mobile devices (tablets, smart phones, ebook readers) as carefully as your main computer. "Lookout" and VIPRE Mobile for Android are free programs for this. VIPRE Android also backs up your contacts and has a locator should you misplace your phone. (Kindle readers run on Android, but VIPRE Mobile is currently restricted by Amazon.)

A new threat is those ubiquitous QR codes that are popping up everywhere. The Norton security program warns of bad QR codes.

Following these tips will not protect you 100%—nothing can, but they will go a long way to keep your internet experience safe.

Presented at the Southwest Technology & Computer Conference, San Diego, by Dodi Glenn, VIPRE Product Manager, GFI Software (with Kathy Wattman, Product Marketing Manager). Courtesy of APCUG.

Webpage Font Size Too Small? Think about Screen Resolution

by Phil Sorrentino
Sarasota PCUG, FL

Anyone who has taken our basic computer classes knows that the font size can be changed just by selecting the appropriate text and then selecting the desired text size, usually from about 8 points to 72 points. And if you were in one of my classes you know that a point is 1/72nd of an inch. That's right; a 72 point selection will print text, on a printer, one inch high.

But everything you see on the screen is not as easy to control as the font of the text of a word processing document. There are, typically, no font size selections on a webpage when you're surfing the web; although you can make some font selections if you are using Internet Explorer. This selection is made by double clicking Tools, then selecting Internet Options. The "fonts" selection is toward the bottom of the window. Here you can select "default" fonts to be used if the webpage does not determine a font. But, practically speaking, you probably will never use these fonts, so don't rush to change these selections. (Other browsers probably have similar selections.) The size of the font that you see on your monitor is determined by settings that are determined by the webpage, and settings on your display graphics adapter. The webpage settings are determined by the webpage designer; the browser just follows the webpage's direction. The display graphics adapter settings are adjustable and are located in the "Display" Control Panel.

In Windows 7, a quick way to get to the Display control panel is to right-click on any empty space on the desktop, select "Personalize," and finally select "Display" (lower left). At this point you can select "Smaller" (the default type size), "Medium,", or "Larger." Because these settings depend on the Screen Resolution that is set, if you choose Medium or Larger you may be alerted that "*Some items may not fit on your screen if you choose this setting while your display is set to this resolution*." So screen resolution is involved in determining the font size and is an important parameter to understand, so that you can make the best choice.

Screen Resolution is generally defined in terms of pixels. A pixel is a picture element. (There is a technical difference between pixels and dots depending on different displays, but for simplicity, for this discussion I am going to use the term dot in the place of pixel.) So Screen Resolution, then, is the number of dots that can be displayed on the screen. It is usually indicated by two numbers, first the horizontal number of dots, followed by the vertical number of dots, for example, 640x480, 800x600, 1024x768, or 1920x1080. (Yes, if you multiply the horizontal and vertical numbers, you get the total number of dots displayed on the screen.) These four resolution settings are also called VGA, SVGA, XGA, and HD-1080. (There are a whole host of screen resolutions that can potentially be used, and are summarized at http://en.wikipedia.org/wiki/Display_resolution. The chart shows the most common display screen resolutions.) The HD-1080 resolution is also the standard used in High Definition Televisions, which is typically referred to as 1080p. So, if you are looking for a display that will show High Definition movies the way they were intended to be shown, make sure your Display Adapter is capable of showing at least 1920x1080.

The Screen Resolution control can be reached easily by right-clicking in any empty space on the desktop, and then selecting "Screen Resolution." (Or by clicking the start button, followed by selecting "Control Panel," followed by selecting "Display," followed by selecting "Adjust resolution" {upper left}.) The current screen resolution is shown as "Screen Resolution:," in the middle of the Screen Resolution window. The Screen Resolution slider control can be accessed by clicking the downward facing triangle next to the resolution that is currently selected. The Screen Resolution slider controls the resolution of the display and hence the size of text on the

screen. The number of selections on this control is determined by your display adapter and your particular monitor. You may have from 2 to many selections. The selections on the slider range from "Low" to "High." (Click on a different resolution on the bar to see a preview of the changed setting in the "Change the appearance of the display" box, (notice how the box representing the screen changes size and shape), then if you like it, click "Apply," if you don't like it try another, or click "Cancel.") Moving towards "High" puts more "dots" on the screen; however, this typically makes the size of objects smaller. Decreasing this setting (moving towards Low) usually makes things larger, but you might start to lose the right side of some web pages. (If you can't easily read the right side of a webpage, you might increase this setting, but things will probably get a little smaller. Try a setting with a few of your favorite web pages and see what setting is the best compromise.)

If you are still wondering what setting to use, click on "What display setting shall I choose?" and you will be treated to a help screen that further discusses screen size and screen resolution with some recom-mendations for appropriate settings for different display sizes. Note also, that you can easily get to the "Display Font Size" screen (discussed above) by clicking on "Make text and other items smaller or larger."

If you were wondering why the shape of the screen changes with resolution, it is because the resolutions that are supported by the display adapter cover the older 4x3 aspect ratio and the more current 16x9 (wide angle) aspect ratio. The 4x3 aspect ratio is what we inherited from seventy years of analog TV screens. All TV screens, before HD, were built with this aspect ratio. Aspect ratio is typically described by horizontal x vertical. So a 4x3 TV screen has 3 vertical increments for every 4 horizontal increments. (Academic observation for math majors: this always formed a 3x4x5 triangle. A 25 inch TV had a 25 inch diagonal with a 20 inch horizontal and a 15 inch vertical.) The more current 16x9 wide angle aspect ratio screens provide more viewing in the horizontal. For every 3 vertical increments there are 16/3 or 5 1/3 horizontal increments showing a wider angle view.

Screen Resolution is the key to getting a comfortable view of your favorite web pages. If you need to, try some different settings. If you still aren't happy, maybe try another Graphics Adapter, if we're talking about a desktop. If we're talking about a laptop, you're probably going to live with those currently provided. It is just about impossible to change the graphics adapter on a laptop.

From the August 2012 issue of PC Monitor*, newsletter of the Sarasota PCUG, FL. Courtesy of APCUG.*

What's New in Firefox Version 15?

by Bob Rankin

Firefox has always been an infamous memory hog, grabbing ever-larger chunks of RAM the longer it runs. In this release, Mozilla developers have tackled one of the biggest causes of this problem: third-party add-ons. Many add-ons retain copies of Web pages even after a page's tab is closed, thereby wasting increasing amounts of memory. Firefox 15 detects such shenanigans and frees up memory. Fewer crashes are another benefit of this housecleaning.

More sophisticated graphics are possible in Firefox 15. This version supports the WebGL standard, enabling 3D graphics and complicated textures. Enhanced graphics will surely become widespread, but their main application will be browser-based gaming. New APIs (application programming interfaces) give game developers better control over the timing of their interactive graphics, down to thousandths of a second.

I guess that would be important for a simulation of Olympic running or swimming, where margins of victory are often measured to within a few hundredths of a second. Mozilla has released a couple of demo games online: BrowserQuest and BananaBread.

Music lovers and teleconferencers will benefit from Firefox 15' s support for the Opus audio codec. Opus provides better audio compression rates than MP3, Ogg, or ACC formats, so audio files will be smaller and download faster. Also, Opus supports dynamically adjustable bitrates, and both pre-recorded and live interactive applications.

The auto-update feature in Firefox has been refined to make it less intrusive. Updates to the current version are now downloaded silently in the background, and applied faster when Firefox is restarted. You no longer have to deal with the "Firefox Update" dialog box and "Firefox is installing updates…&" messages. Users will be relieved, given Mozilla's more aggressive update schedule these days.

Developers will appreciate the Javascript debugger built into Firefox 15. It includes several UI enhancements that make finding snippets of code easier. A "Responsive Design View" helps developers test code on multiple devices, i.e., desktop monitor, smartphone, without actually having to view a page in a particular device.

Mobile Twinsies?

Firefox for Android got some badly needed features in this release. Text selection, find in page, and search suggestions bring the Android version more into line with the desktop version's features. Tabs can now be closed by swiping, and you can view the desktop version of a Web page through a menu button. Tablet support has also been added, with tabs appearing in a sidebar.

If you want Firefox 15, it's quite simple to get it. Firefox users can click on the Help button, then select About. The latest version of Firefox will start downloading instantly. If you're currently using IE, Chrome or some other browser, you can also get Firefox 15 at Firefox.com.

Of course, there are many subtle tweaks under the hood of Firefox 15, some of them dealing with important but obscure security issues. It's always best to keep your software up to date.

A few months ago, I finally got tired of Firefox, because it would become sluggish or crash due to the enormous amount of memory it was consuming. It wasn't uncommon for me to open the Task Manager and find that Firefox was holding onto over a GIGABYTE of memory! Shutting down and restarting the browser fixed the problem, but only temporarily.

So I made an effort to switch to the Google Chrome browser. Chrome seems to chug lots of RAM, too (about half as much), but it doesn't crash and seems generally speedy. But with Firefox 15's promise to manage memory better, I'm giving it another chance to impress.

The Tip Corner

by Bill Sheff
Novice SIG Coordinator, Lehigh Valley Computer Group, PA

Shift+Space Web Browser Navigation

Here is a way to make navigating pages in your web browser a little easier. Instead of using the Page Up and Page Down keys, you achieve the same results by pressing your Space Bar to go a page down and pressing Shift+Space to go a page up.

What Is Pinning and how do I do It?

Pinning is keeping items within a window in the same place for easy access. Programs, applications, web sites, etc. can all be "Pinned." For Example: The Windows Start Menu is divided into two sections. The top half of the menu is reserved for pinned items. Since I use

Excel and Word almost every day, I keep them pinned, making them accessible at the click of a mouse at any time.

How does one do this? Simply right-click on an icon on your desktop and choose "Pin to Start Menu." That's it.

What happened to Normal View in Word 2007 and 2010?

If you're using either Word 2007 or 2010 and preferred working in the Normal view, then you're probably wondering what happened to it. If you went to the View tab of the Ribbon it is not there. Well, it was not deleted. They just renamed it Draft view. Now all those page separations are gone. Unfortunately when you reopen the file it again opens in the Print Layout view.

So how do we tame Microsoft to open in the Draft view every time? Click on File and choose Options then Advanced on the left. On the right scroll all the way down to the General section. Locate and select the "Allow opening a document in Draft view" option. Click OK. When you open a file that you saved in Draft view it will still be in Draft view.

From the July 2012 issue of the The LVCG Journal*, newsletter of the Lehigh Valley Computer Group, PA. Courtesy of APCUG.*

I'm Thinking about Getting a Tablet Computer

by Bill Armstrong
Lehigh Valley Computer Group, PA

Question:

I am *thinking* about getting one of these tablet computers, but have oodles of questions so I thought I'd start here (rather than bugging sales people until I know a bit more).

Are there any additional costs to use for internet access. (i.e. like a cell phone on a per minute plan)? Are "apps" part of the deal using a tablet (we are not into smart phones either at this point)? Is there a cost to use an App (other than cost to download if it was not free)...such as checking mail, weather, interactive games? Would I be able to get my e-mail? One I am looking at mentions Gmail...which I do not have? How do I get virus (etc.) protection? How secure using a wireless hot spot?

Answer:

I do not have a tablet, but I do have a smart phone (Android). Internet access through the cellular network requires a monthly access fee with a carrier, so yes, there is a continuing cost. That is why most of the tablets sold are Wi-Fi (not cellular). The Wi-Fi only tablets are less expensive to purchase initially (since they do not have the circuitry for cellular communications). My plan with Verizon to get internet on my phone costs an extra $30 per month (over the cost of the cell phone plan for voice phone calls).

Apps are elective for you. I have some, but not a huge number. They give me weather info, stock market info, gasoline prices locally, movie listings, etc. Apps come in both free and paid versions. Once acquired, there is usually no additional cost to use them, forever. Most apps that require a fee up front are low cost, such as $0.99 up to $3 or maybe even $5. Some, I guess, are more expensive, but I have never paid for the expensive ones.

If you have Wi-Fi at home, a tablet will work on the Wi-Fi network very nicely. That is how most people use them. When you go out around town, you will find many businesses offer free Wi-Fi. I used the free Wi-Fi at Panera Bread today in Whitehall. You should be able to get your email when connected to the Internet over Wi-Fi. I'll bet your email service has a method of retrieving your email over the web.

Virus protection is available for the operating systems (OS) that tablets run. I have such a program for my smart phone, for which I paid. It's a good idea to have one. The app store for

your tablet's OS will offer many. Just search for anti-virus. Wireless hotspots (public Wi-Fi) are not secure. Period. That being said, I use them all the time. I just don't do any banking or money or credit card transactions. I wait until I am home, on my password protected Wi-Fi system.

Be sure to view a few screen sizes, to see what is good for you. The iPad is about 10.1 inches (measured diagonally), and many consider that size to be ideal for them. Other popular sizes are 7.7 and 7.0 inches, and 5 inches. View a website or two to see how they look.

My smart phone is large for a phone, about 4.65 inches. It's small but usable for viewing a website. I have to use a two-finger spreading action on the screen to enlarge the view, so I can read it easily. If using the Android OS, I recommend a tablet that uses Android 4.0 or later (called Ice Cream Sandwich or ICS). This OS makes scrolling and making the view larger/smaller very easy and intuitive and smooth.

I use my phone for getting email, viewing websites, checking the weather, checking my calendar (where I put all my appointments and "to do" list), checking facts on Wikipedia, getting news, reading tech articles, getting stock market info, etc.

From the May 2012 issue of the LVCG Journal*, newsletter of the Lehigh Valley Computer Group, PA.* Courtesy of APCUG.

Society News

Help's Half Hour
Led by Nick Francesco
by Jan Rothfuss

Q: A member using a Dell desktop, continues to get viruses. She has had to take it in for re-building twice now. She is using MacAfee.
A: Be sure that your anti-virus programs are being updated – daily is best. The viruses are getting more vicious, too. Nick suggested AVG or aVAST as they are effective and free.
Q: A member is using an Acer Laptop. Can it be set so that his kids need a password to use the internet?
A: You must set up the computer so that it needs a password. Be sure to logoff when your session is done. NetNanny is a guard software that can be used to request a password before internet access. That way both the kids and yourself would need to enter a password.
Q: What is the main goal of today's viruses?
A: They are trying to take over your machine. They want to hide inside your machine. They are also seeking to find identity information like bank accounts. You can tell that this is happening by using a program like Malwarebites. Viruses used to be written by novices. Now they are paying money for virus generation. It is a big business.
Q: Is it true that MACs do not get viruses?
A: Not true! The very first virus was on a MAC.
Q: What is the best method for backing up my data files?
A: First you must know where the files are located – like Outlook. You can backup your files on websites such as Carbonite. For $5.00 per month you then select what will be backed-up. You can also set up your own system using a separate hard drive. Many members added that they back up their files to two locations – using both a belt and suspenders. Another option is to use the net – Google allows you to store items if you use them.
Q: I want to thank you for your Security Tango. It has saved me a couple of times.
A: Yes, there is some additional software included now. He is trying to keep up with the viruses as they become more sophisticated.
Q: One member asked - when using Googledocs, it automatically saves as I type. What if I need to 'undo'?

A: Nick went online and checked the settings. It did not appear that it is an option.
Q: When you store things in GoogleDocs, is it safe? Do they look at your files? Who owns the rights to the material?
A: Google does not really care about your content. They do track you by number, knowing what selections you have made and then tailor your future ads. You are the owner of your data. You own the copyright.
Q: What is the advantage of using GoogleDocs?
A: All of my documents are available to me – regardless of which computer/tablet is being used. Also multiple users can access the same file at the same time.

Our new and glamorous mugs are now available for sale. At $5 each you can't do better. If you fancy giving a presentation you can receive one as a thank you gift.

The Lighter Side

"I predict the Internet will soon go spectacularly supernova and in 1996 catastrophically collapse." –Bob Metcalfe, *InfoWorld*, 1995.

He also said: "When Windows 2000 gets here, goodbye Linux."