December 2008

WINDOWS USERS Notepad

WINdows usERS

Inside

Notice the January meeting due to a conflict (someone at the library beat us to the regular time) will be at a special time 1:00 - 4:00 p.m. on January 17

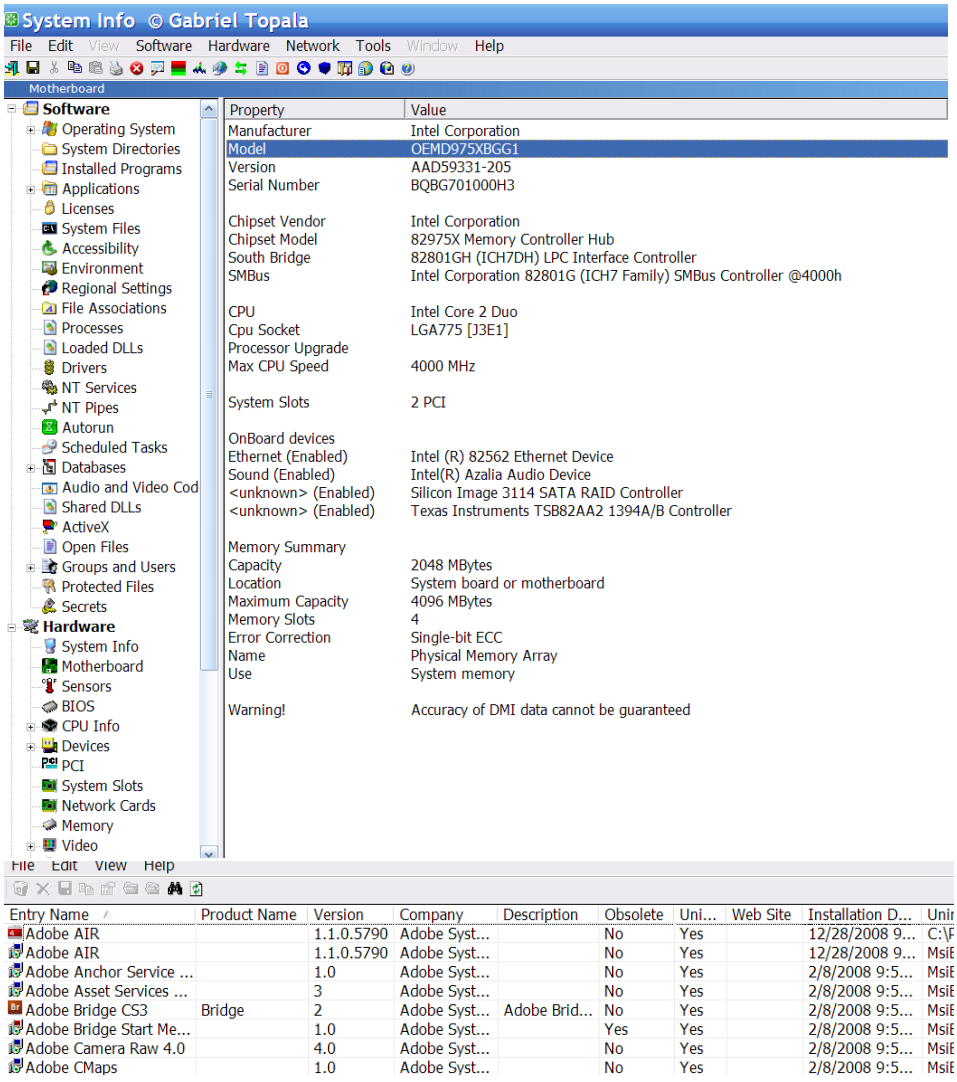
Fountain Valley Branch Library
17635 Los Alamos,
Fountain Valley
meetings on 3rd Saturday
10:00 am to 12:30 pm

Future Meeting Dates
January 17
February 21
March 21

Membership
Annual membership is $20 for indivduals: $5 for each additional family members.

December 2008 meeting

Terry Currier demonstrated some of his favorite utilities. Among these included SIW.EXE, a program that reads and presents to you just about everything about your computer. What motherboard you have, BIOS date, what DLLs you have loaded.



If you can't find you serial number for your Windows operating system it will tell you that also.

Most pictures will be about 2MB and tend to clog up mailboxes quickly. Use PhotoRazor to shrink them to a good size that will still show how cute little Timmy is. Just point it to what folder with pictures

you want shrunk and it will do that creating a new folder with the smaller sized – not changing the originals.

Myunistaller is my favorite way to uninstall a program. It doesn't just help you to uninstall a program it gives you a lot more information than Windows uninstall will. It shows the installation date and even the registry key to help you get rid of it if uninstalling it fails. My absolute favorite picture view program is the FastStone Viewer. Very fast and gives the user wealth of options and information about the picture. Scroll the mouse up and you see a thumbnails of the pictures within the folder. Go to the right and it gives information such as when the picture was taken and type of camera. Go to the left and resize, change the contrast, or even start a slide show. Scroll to the bottom and you can get rid of red eye, crop a picture and more.

A friend brought over a laptop with some really nasty spyware and asked for help in getting rid of it. He tried using some free program called Antivirus 2008. Problem was it was spyware. It would also not allow the computer out onto the Internet. I tried a couple of programs to remove it, but both would not do anything until it downloaded updates. I found Malwarebytes spyware remover and it worked great.

All of these can be found by using Google.com, and by the way all are free.

A clean house is a sign of a broken computer.

Surviving The Switch To Digital TV

By Andy Marken

At the stroke of midnight on Feb. 17, 2009 (now extended 30 more days), the analog transmissions that have beamed free television over the air in the United States for over half a century will disappear for good. They will be replaced by digital signals, many of which are already broadcasting, in what will be the most significant change to television since the introduction of color.

The "digital switchover" brings with it higher image quality, better sound and a level of versatility and flexibility previously unattainable through free television.
It also brings with it a number of significant headaches, as confusion over exactly who will be affected is inspiring panic in viewers fearful of being left behind in a haze of snow and static as the rest of the country moves into the future.
Many of those who will be affected know that the deadline is fast approaching, but are unsure of how to prepare for it. Thankfully, a solution is simple, easily attainable and won't cost you a dime.

There are two major reasons for the switch from analog TV broadcasts to digital TV. First, digital signals offer superior image quality and allow for the transmission of high-definition signals over the air. This means that a properly equipped HDTV can receive local high-definition broadcasts that will look about as good as what you'd get from cable or satellite television.
In Pictures: 10 Tips For Switching To Digital TV

Second, switching from analog to digital frees up real estate on the broadcast spectrum for other uses, as digital signals are more efficient and take up less bandwidth. Telecommunications companies like Verizon and AT&T have spent nearly $20 billion to secure the rights to the frequencies that were previously occupied by channels 52 through 69, in the hopes of using that airspace to improve their wireless communication networks.

What the digital switchover is actually doing is changing the language that TV broadcasters use to communicate with your television. Since 1941, televisions in the U.S. have utilized a set of broadcast standards laid out by the National Television System Committee. Big broadcast towers sent out information over the air using these NTSC standards and were picked up by the television antenna in your living room. Inside your TV, an NTSC tuner interpreted the information and properly displayed it on screen.

The digital switchover is introducing a new language, a new set of broadcast standards, this one designed by the Advanced Television Systems Committee. On Feb. 17, those broadcast towers are going to stop speaking NTSC permanently and start speaking ATSC. But unfortunately, your old television set doesn't know how to translate ATSC into moving pictures and sound. Just about all televisions manufactured and sold after Mar. 1, 2007 feature ATSC tuners, but if you purchased a television any earlier than that, chances are your TV won't be able to pick up over-the-air broadcasts once the switchover occurs.

The solution: A digital converter box, essentially an external ATSC tuner that sits on top of your existing television and is linked between your antenna and your TV. The ATSC signals are grabbed by the same antenna you've always used, then passed to the digital converter box that translates the ATSC signals into something your NTSC television can understand. They are easy to hook up and available at a wide variety of stores, including big box stores like Best Buy, Wal-Mart and Target, as well as online retailers.

Digital converter boxes cost between $40 and $70 on average, but since the digital switchover is being forced upon consumers, Congress has stepped up and created the "TV Converter Box Coupon Program."

Under this initiative, each American household is entitled to two $40 gift cards that can only be used to purchase a digital converter box. Individuals can apply at the official Web site for the DTV switch.
You can apply for coupons until Mar. 31, 2009; they expire 90 days after they are issued. You might want to apply for them sooner rather than later because the government has allocated a finite amount of funding.

TV viewers who pay for cable or satellite service need not worry. The digital switchover only applies to over-the-air broadcasts, so consumers who get their television directly from Comcast or DirecTV will not be affected at all, and service will continue uninterrupted and unchanged as the DTV deadline comes and goes.

There is, however, a subtler, unrelated analog-to-digital switchover taking place among cable companies, one that could affect subscribers. It has usually been possible to view a small number of basic cable channels by plugging the coaxial cable directly into a television set, bypassing a cable box entirely.

This was a quick and easy way to bring cable TV to many rooms in a home without renting multiple cable boxes. Unfortunately, this may not be possible in the near future. Cable companies like Comcast and Time Warner are slowly phasing out their analog cable services in favor of digital. By switching over, they free up more space on their cable networks that can be allocated to new high-definition channels and interactive services like "On Demand." The downside is that when all cable channels are converted to digital, renting a cable box will be required to see any channels at all.

Another point of confusion that retailers and manufacturers have been reluctant to clear up: consumers need not purchase an HDTV to weather the digital TV switchover.
In addition to the converter boxes, new standard-definition CRT televisions are still available, and they are required by law to include the necessary ATSC tuners. While an HDTV will allow viewers to take advantage of digital TV's high-definition potential, it's important to know that there is a lower-cost option available as well.

With the emergence of free, digital, over-the-air television that includes HD transmissions, it will be inter-

esting to see if Americans, the majority of whom now pay for their television service via cable or satellite, might see the benefit of switching back to the old rabbit ears. While the selection of over-the-air broadcasts will never be as comprehensive as pay services, that same glut of content is often cited as an annoyance--lots of channels that subscribers will never watch.

Of course, all this will depend on how smoothly the digital switchover goes, and whether or not people are actually able to see the improvements on their screen. With just a few short months to go, having the right knowledge to make it through is absolutely crucial.
In Pictures: 10 Tips For Switching To Digital TV == http://www.forbes.com/2008/12/04/digital-tv-switch-tech-personal-cx_mpb_1204digitaltv_slide_2.html?thisspeed=25000

See Also:

Ask This Before You Buy An HDTV -- http://www.forbes.com/personaltech/2008/10/07/buying-tips-hdtv-tech-personal-cx_mpb_1007hdtvtips.html

End of Article - End of Artic End of Article - End of Artic End of Article - End of Artic

Wireless Router Setup

By Bob Elgines, Editor, Colorado River Computer Club, Arizona
www.crccaz.com/
elginesz@rraz.net

How to change the setup or configuration of your Wireless Router and PC. First we need to get to your router after the original setup by bringing up Internet Explorer on your direct wired computer (Master) and typing in one of the code addresses below:

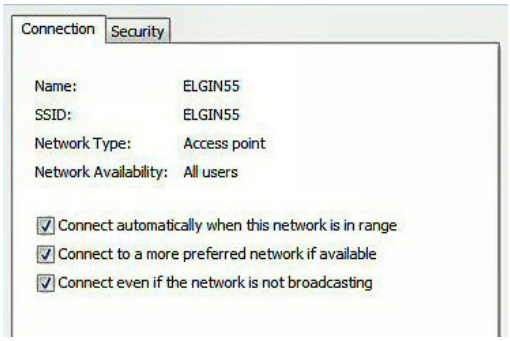
TYPE	CODE	USER	PASSWORD	CHNL
Belkin:	192.168.2.1	(No Name)	(Leave Blank)	6
D-Link:	192.168.0.1	admin	(Leave Blank)	6
Linksys:	192.168.1.1	(Leave Blank)	admin	11
Netgear:	192.168.0.1	admin	password	10

A login screen will appear, if you used your own login name and password then use them. If you lost them and you wish to reconfigure your router you will have to push the reset button for at least 30 seconds. This sets the router back to its defaults and you can use the default values above.

During your setup you may have seen "Number of DHCP users allowed", reduce this to the number of total computers in your network or that number plus one.

SSID is your wireless network name, for example, Linksys will broadcast "linksys". First, we want to rename your SSID and then hide it later. After changing the name, we need to reconnect with each wireless computer. To reconnect, right click the icon in the System Tray (or task bar-right).

Windows XP SP2 - Choose Available Wireless Networks / Change Advanced Settings. Click the Wireless Networks tab, click Add button in the Preferred Network section.
Type in the Network name you have chosen, then click OK twice.



Windows VISTA - Select Network and Sharing Center, then left click on View Status (located middle-right). Click on Wireless Properties button. Put check mark on "connect even if the Network is not broadcasting".

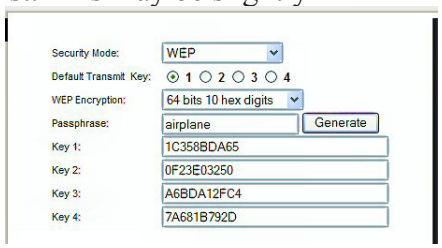
(Or go to START / CONNECT TO / click on your SSID and click the CONNECT button below. Then you can right click on your SSID and select Properties. This will get you to your Wireless Properties window where you can put the "check mark" and enter your Security code.)

Complete this on all of your wireless computers and remember how you got there!

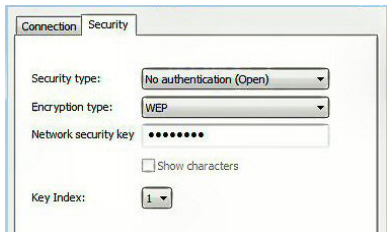
Second, now we can choose to stop your Router

from broadcasting your SSID by selecting disable to "SSID Broadcasting" in your router setup. All your computers should be reading the wireless connection.

Next step is to select a **Security** type, let us try **WEP** first. This may be slightly



different due to different manufactures. Usually you will find it under Security or Wireless tabs of your router setup. Select 64 or 128 bit encryption, then type in a word or phase and let the router do the coding by clicking on Generate. Select #1 and write down this code for your wireless computers. Go to the Wireless Properties window and click on the SECURITY tab. Then set the ENCRYPTION type to WEP and enter the security code you wrote down, click OK and Close. Key Index should remain on one.



Look at the Security Type by clicking the down arrow on the right. Note these are the other types of security allowed: WPA2-Personal, WPA-Personal, WPA2-Enterprise, and WPA-Enterprise. Most newer routers and computer can operate with this type of security and is considered better than WEP.

We completed a simple setup to supply a secured wireless connection. You can go further and use one of the WPAs if all of your computers will accept this. Just disable WEP and enable WPA and roughly go through the same process. You could also assign your MAC addresses, but how far do we have to go?

Following are definitions for MAC, DMZ, WPA, DHCP, and the router FIREWALL:

DHCP – Dynamic Host Configuration Protocol as a server assigns IP addresses to all computers on the network (in this case the router is the DHCP server).

DMZ – Dedicated Multi Zone exposes a computer directly to the internet with a IP address. Some games require this direct access. You could give a false address not used by your computers to send intruders to an address that goes no where!

FIREWALL – The router's firewall gives protection on data coming in, but not going out. If you wish full bi-directional protection you will have to use software and replace your windows firewall which is incoming only.

MAC – Media Access Control is a number related to the network adapter in a small network. LAN-MAC address is for your internal network and WAN-MAC address is used for router to modem connection. You can find your Client table (IP and MAC addresses) in your router's configuration utility.

WEP – Wifi Encryption Protection is the old security standard that can be used with either 64 or 128 bit encryption.

WPA – Wifi Protected Access is the latest network security standard, but if your equipment is over two years old you may want to checkout www.wi-fi.org web site for information. For full instructions on activating WPA see PC Magazine's step by step article at http://www.pcmag.com/article2/0,1759,1819544,00.asp

Things You'd Love to Say at Work, But Can't

- Do I look like a people person?
- Sarcasm is just one more service we offer.
- If I throw a stick, will you leave?
- Does your train of thought have a caboose?
- Whatever kind of look you were going for, you missed.
- Well, this day was a total waste of makeup.
- I'm trying to imagine you with a personality.
- Can I trade this job for what's behind door 1?
- Too many freaks. Not enough circuses.
- Nice perfume. Must you marinate in it?
- Chaos, panic, & disorder - my work here is done.
- How do I set a laser printer to stun?
- I thought I wanted a career, turns out I just wanted paychecks.

The Crabby Office Lady

Hey you, you clever, hot-under-the-collar person who can type faster than a cheetah can run. Think twice (or more) before popping off that tart e-mail message. Yes, there are ways to recall it — but sometimes they work and sometimes they don't. The best recipe to avoid embarrassment is to take out your frustrations in another manner.

Get the Crabby Office Lady's book
Read all the Crabby Office Lady columns
Get Crabby's columns via RSS
View Crabby's videos

Delay your crabbiness: Outlook features for itchy trigger fingers

Hey you, you clever, hot-under-the-collar person who can type faster than a cheetah can run. Think twice (or more) before popping off that tart e-mail message. Yes, there are ways to recall it — but sometimes they work and sometimes they don't. The best recipe to avoid embarrassment is to take out your frustrations in another manner.

I know you (because I am you):
You're hot under the collar and everybody knows that (and sometimes loves that) about you. And yes, you have a bit of an itchy trigger finger and you've been known to pop off an e-mail message that is, shall we say, less than diplomatic, and a bit more curt than you'd intended (sometimes — only sometimes). But before sending your clever and scathing message out there to the world, remember this: The pushing of the Send button lasts a moment; its effects can last a lifetime — or at least until you're back on the streets, looking for another job.
Outlook does offer a few ways to get that message back, but before I jump into that, I want to come clean: Nothing is foolproof. Certain conditions have to be just right in order for this message recall thing to work. For one, both you and your recipient have to be using Microsoft Exchange Server.
NOTE If you don't know what Exchange Server is (let alone know whether you're using it), I suggest you watch this helpful demo: Got Exchange? See how to check.

Using the Outlook recall feature
When you're using Outlook with Exchange Server, you have a few options when it comes to trying to recall a message.
1. If your unsuspecting recipients have not yet read this "oops" message, you can delete, or recall it. Again, this only works if they haven't already read the message.
NOTE You can also be notified if this recall attempt succeeds or fails for each recipient. If it's a lot of people we're talking about here, I'd forego this part.
2. You can recall the original message and replace it with a more, shall we say, gentle one.
NOTE If you decide to replace the original message with a new one, Outlook will automatically open up a new blank e-mail message so that you can reword your message — carefully this time.
You've done your best...but it's out of your hands
The success or failure of a recall depends entirely on the settings the recipients have in Outlook.
- If your recipients have Process requests and responses on arrival selected on their computers (in Outlook: Tools > Options > E-mail Options > Tracking Options), even if the original message — the one you tried to recall — has not been read, the recipient will be notified that something disappeared from their Inboxes. (And boy does that summon up curiosity.)
- If Process requests and responses on arrival is NOT selected on your recipients' computers, both messages, the original one and the new one, show up in the Inbox...and then fate steps in.

1. If the recipient opens the recall message first, the original message is deleted and the recipient is informed that you, the sender, deleted the message from his or her mailbox.
2. If the recipient opens the original message first, the recall fails, both the old and new messages are available, and you are left with egg on your face. Cluck-cluck.

There are many more variables when it comes to recalling messages. Sometimes it has to do with certain rules your recipients have set up, or, if you sent the message to a public folder, sometimes both the original and the new message show up in the folder (and live there for eternity).

I suggest you read some of the articles and view the demos I've referenced below about recalling messages, and see what may work for you. But again, my advice (if not always followed by myself) is to count to 10 before you send the message. However, if you've already sent it, realize that the message you just popped off in the heat of the moment is probably going to be read by someone before you've changed your mind and have had the opportunity to recall it.

- Demo: Take that message back
- How message recall works
- Recall or replace a message you've already sent
- Recall or replace a message after it is sent

Recalling messages to someone not using Exchange Server

You can't. I'm sorry, but you just can't. Therefore, I've created a list of things you can do to vent instead of sending that damaging e-mail.

1. Count to 10. Or 20. Or 100 if you have to.
2. Shout into your pillow (or, in your case, your chair's upholstery).
3. Close your office door (or, if you work in a cubicle, go to your car) and have yourself a good cry.
4. Head on over to the cafeteria or vending machine and gorge yourself on a good dose of medicinal chocolate.
5. Write to me (crabby@microsoft.com). I read all the messages I receive, and I never take them personally, ever.

"Experience is the name everyone gives to their mistakes." — Oscar Wilde

About the author

Annik Stahl, the Crabby Office Lady columnist, uses Office all day long. She gets her column ideas from your wild suggestions and demands, so if you're feeling demanding or just want to toss a comment her way, leave Crabby some feedback. If you have an Office tip you'd like to submit, send that to her personal mailbox at crabby@microsoft.com. (While she does read all of your e-mails, she can't offer personal assistance, so don't be offended by her curt auto-reply...)

End of Article - End of Artic End of Article - End of Artic End of Article - End of Artic

Internet Security: iFrame Attacks

By Brian K. Lewis, Ph.D., Member and Contributing Columnist, Sarasota PCUG, Florida
www.spcug.org
bwsail at yahoo.com

I'm sure that most of you reading the title of this article are asking "What is an iFrame?". Well, sit back, get comfortable and I'll tell you about the latest method hackers are using to steal information from you.

First the definition of an iFrame, which is shorthand for inline frame. That clears it up doesn't it? I guess I'd better add some more to that. An inline frame is code within a web page that permits a second page to be imbedded inside the first page. For example, they can be used to imbed an ad that is located on a different web site. One example is the clickable scrolling ad you frequently find on web sites. IFrames generally load after the main page and may sometimes have their own scroll bar. The iFrame may contain Javascript programming code which can permit interactive content. Some iFrames may be invisible and may contain code which can redirect the user to another page or download trojans or viruses.

Whenever your Internet browser sees an "iFrame tag" in the web page code it sets aside the space requested in the tag. It also goes out to the web page specified in the code to download the requested information.

So is this something new? I thought it was until I read a report in a tech newsletter (Windows Secrets) about an attack on the AskWoody web site. It turns out that iFrame attacks have been recorded since 2004. The first exploit implanted a worm on thousands of computers. The only thing that stopped it was a patch that Microsoft had to apply to Internet Explorer 6. In June 2007 over 10,000 pages were infected in Italy. In November 2007 Monster.com had to shut down as a result of an iFrame attack. Then, this year the AskWoody site had iFrame code added to its main web page. His research indicated that the code originated on a Russian web site, which subsequently disappeared. The code placed on the AskWoody web page linked to a web site in China and subsequently

to the Russian web site. This was all done by a short length of code that setup a single, invisible pixel on the web page. The code was designed to load data from the Chinese web site. Anyone with an unpatched IE 6 that visited the AskWoody web site would probably have been infected. However, it was never determined just what was being delivered by the offshore web site.

The worst part of this scenario is that the owner of the AskWoody web site did not find out about the iFrame exploit until he started receiving messages from someone who advised him that their AVG Resident Shield said his site was infected. That was followed by Google advising him that his site was infected and down rating the site. Google also provided a warning to anyone attempting to link to AskWoody warning them that visiting the site might infect their computer.

The question becomes, how did the iFrame code become attached to the web page? The code pages on web sites are generally password protected. Access to these pages for the purpose if making changes is controlled by the web site host and the hosting software. However, there are several programs available which enable hackers to take advantage of holes in web site security. Some of these are described as "kiddie scripts", indicating their ease of use. Others, such as Mpack, require a more sophisticated knowledge of programming. The problem is that thousands of respectable sites have been infected. The following are only a few that were reported in March 2008 by Dancho Danev's blog (a security information web site):

eHawaii Portal - ehawaii.gov - 992 pages
The World Clock - timeanddate.com - 944 pages
Boise State University - boisestate.edu - 471 pages
The U.S. Administration on Aging (AoA) - aoa.gov - 425 pages
Gustavus Adolphus College - gustavus.edu - 312 pages
Internet Archive - archive.org - 261 pages
Stanford Business School Alumni Association - gsbapps.stanford.edu - 157 pages
BushTorrent - bushtorrent.com - 147 pages
ChildCareExchange - ccie.com - 131 pages
The University of Vermont - uvm.edu - 120 pages
Hippodrome State Theatre - Gainesville, FL - thehipp.org – 112 pages
Minnesota State University Mankato - mnsu.edu - 94 pages
Medicare – medicare.gov – 12 pages

In many instances it appears that the hackers were able to "harvest" passwords which gave them access to these sites. Then, if the site did not have current input validation patches, the iFrame could be added to web pages. In some cases, home users may have been the source of the initial password theft. By use of a keylogger a hacker can obtain passwords to any protected site visited by the user. In other cases clicking on a banner ad that attracts you can result in the download of a bot, a trojan or other spyware. This is especially true if you are still running an unpatched Internet Explorer 6. It appears that Firefox is less vulnerable to these types of exploits. Also, clicking on an executable file in IE 6 generally results in running the file. In Firefox you are usually only given the option to down load the file. Obviously you should never download or run any file that you don't know or don't recognize. This is especially true when the site tells you that you need some kind of add-on or special viewer to see the information you want. This the type of social engineering being used to tempt users into downloading spyware.

There is also a danger related to the firewall you are using on your computer. A keylogger or other trojan needs to be able to report "home" without the user being aware that information is being sent out. This is done by opening a "back door" to the Internet; an outgoing port in one the thousands on every computer. If your firewall doesn't check on all outgoing data and requests permission for new unknown activity, then you will not be able to block the trojans back door connection. So it is very important that your firewall check both incoming and outgoing data. Then, anytime your firewall requests permission for a program, one you don't recognize, to connect to the Internet, just say NO.

There is one other recognized method for obtaining the information needed to get into web page code. Hackers can purchase web site administrator information on the black market. One software application used to hack web sites, Mpack, sells for about $1,000 US. The person behind this software is known as $ash in the Russian underground. The software exploits six flaws in Windows and Internet

Explorer. Thus for not a lot of money, hackers can obtain everything they need to exploit weaknesses in web pages.

As you can see, the iFrame attack is a real danger for those who surf the Internet. If you want to read more about these attacks, a Google search will provide you with tons of information. If you want to protect yourself from these attacks, your ability is limited. It is really up to your ISP and the web hosts to provide the security needed to prevent the web page intrusion of an iFrame. So what can a home user do? The following will help, but are no guarantee of protection.

1. Beware of pages that require software installation. Do not allow new software installation from your browser unless you absolutely trust both the Web page and the provider of the software.
2. Scan with an updated antivirus and anti-spyware software any program downloaded through the Internet. This includes any downloads from P2P networks, through the Web and any FTP server regardless of the source.
3. Use only a firewall that checks both incoming and outgoing data.
4. Beware of unexpected strange-looking emails, regardless of their sender.
5. Never open attachments or click on links contained in these email messages
6. Enable the "Automatic Update" feature in your Windows operating system and apply new updates as soon as they are available
7. Always have an antivirus real-time scan service. Monitor regularly that it is being updated and that the service is running.
8. OR another option would be to verify that the address is safe before going to it. You can do this by checking it at: http://linkscanner.explabs.com/linkscanner/default.asp

As you can see, for Windows users, the Internet is becoming more of a hazard to navigation. You, as a user, must always be cautious about clicking on links or accepting downloads. If in doubt, don't do it! If everyone practiced safe-surfing, it would be harder for the hackers to succeed.

Dr. Lewis is a former university and medical school professor of physiology. He has been working with personal computers for over thirty years; teaching, developing software and assembling systems. He can be reached at bwsail at yahoo.com.

End of Article - End of Article - End of Article - End of Article End of Article - End of Article

From the Sydney Morning Herald Australia comes this story of a central west couple who drove their car to K-Mart only to have their car break down in the parking lot.

The man told his wife to carry on with the shopping while he fixed the car.

The wife returned later to see a small group of people near the car.

On closer inspection she saw a pair of male legs protruding from under the chassis. Although the man was in shorts, his lack of underpants turned private parts into glaringly public ones.

Unable to stand the embarrassment she dutifully stepped forward and tucked everything back into place.

On regaining her feet she looked across the hood and found herself staring at her husband who was standing idly by.

The mechanic, however, had to have three stitches in his head.

Blonde Moment

A blonde was taking the tour of a national park not long ago. The ranger mentioned to the tour group that dinosaur fossils had been found in the area.

The blonde exclaimed, "Wow -- I can't believe the dinosaurs would come this close to the highway!"

Google Offers Free Medical Records Service

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

WEBSITES:
http://www.google.com/health
https://www.google.com/health/html/privacy.html
http://www.keyt.com/news/local/19222464.html

Google recently opened for free public access the beta version of its "Google Health" service at www.google.com/health. This service offers users access to a comprehensive user created database where the user can selectively store medical records. In addition to the storage of personal medical records, Google Health also allows for the importation of medical and prescription records from a variety of services, and the voluntary exportation of medical records to several diagnostic services. Google Health allows user approved physicians, hospitals, pharmacists, and other healthcare services to access the medical records.

To open a free account at Google Health requires registration; users with existing Google accounts may use their existing usernames and passwords for access. Once registered, opening the website at google.com/health offers the users an intuitive menu. The primary links in the center column of the page are:

"Add to this Google Health profile (Learn about your health issues and find helpful resources)"; "Import medical records (Copy and get automatic updates of your records)"; "Explore online health services (Find online tools for managing your health)"; and "Find a doctor (Search by name, location, and specialty)". On the left column of the opening page are hyperlinks to personal profile information, and the right column displays a profile summary.

Clicking on "Add to this Google Health profile" opens a menu with the headings "Conditions", "Medications", "Allergies", "Procedures", Test results", and "Immunizations". Under "Conditions" a condition or symptom can be entered in the search box, or the user can click on any condition in a lengthy alphabetical list to "Add" that condition to the user's profile. Many of the conditions have a "Reference" link that will provide more information on the condition, as well as any symptoms and treatments. The "Medications" heading allows the users to enter both prescription and non-prescription medications, vitamins and minerals, as well as herbal products. The search box displays selections as the product name is typed, or an alphabetical directory can be accessed. "Allergies", "Procedures", "Test results", and "Immunizations" are entered in the same manner as "Medications" and "Conditions", with a search box or alphabetical menu.

The main page selection "Import medical records" allows the user to securely import medical and prescription records form a variety of sources, including clinics, laboratories, and pharmacies. Included on the currently short list of such resources are Beth Israel Deaconess Medical Center, Cleveland Clinic, CVS Minute Clinics, Quest Diagnostics, Medco, RX America, Longs Drugs, and Walgreen's. It is clear in reading about the service that this small listing is in its infancy, as Google Health is trying to sign up additional partners. To experiment with importing data, I clicked on the link for the prescription manager Medco, which is utilized by my health insurance plan. Clicking on the "Link to profile" icon under the Medco listing opened the secure Medco website where I had to enter the username and password I use at Medco. Seconds after approving the transfer of my prescription history, it appeared on my Google Health profile under "Medications". The information transferred to Google Health by Medco was not just the prescriptions I ordered from Medco, but also recent prescriptions I filled at local pharmacies where insurance was claimed. Medco can automatically update my profile as new prescriptions are entered and filled. Items filled at local pharmacies under their respective $4 or $5 generic program, where no insurance was filed, did not appear on the Medco list.

The menu item "Explore online health services" opens a list of over a dozen services that offer online personal health services. These health services which can be linked to Google Health and utilize the information provided to Google Health (but only with the express consent of the user!) include

such well known services as the Cleveland Clinic, the American Heart Association "Heart Attack Risk Calculator", "MyCareTeam- Diabetes" diabetes management system (requires monthly or annual subscription), and several other services. While several of these personalized services are free, others are fee based. Most of the services listed require some form of registration in order to utilizes those services and integrate them with the users' Google health information.

The "Find a doctor" link opens a simple pair of search boxes, the first (left) of which is a directory of specialties, and the second box (on the right) is where the user can enter a zip code, city, or other information in order to generate a listing of physicians, chiropractors, and specialists that meet the selected criteria. The listings provided included physician or practice name, address, and phone number, as well as links to the practice website (if any), driving directions from Google Maps, and a link to "Save to medical contacts".

Once information is entered, a personal profile is created, and several analyses are made by Google Health. One that may be critically important shows up in the left column on the main page with the label "Drug Interactions" with a red exclamation point if there is a potentially dangerous interaction between prescription and non prescription drugs, vitamins, and herbals. On my personal page there is one advisory about a synergetic effect between two of my medications that says "Discuss with your doctor soon" (this effect is desirable in my case), and another interaction between three of my non-prescription medications that is labeled with a red icon "Requires immediate attention" (I already checked, and it is OK in my case).

In its privacy statement (www.google.com/health/html/privacy.html), Google Health explains the confidentiality of the information entered, and how it will not be released or shared with any third party without the express consent of the user. By my personal choice, I would be willing to allow my personal physician (if he participated), as well as any specialists or hospitals that I visit, to access my information. It could be a great time saver to allow them to access my medical records online, rather than me having to complete hand written forms at each office I visit. Because of its inherent completeness, this online "Personal Health Record" (PHR) can also be a life saver by providing healthcare establishments instant access to medical histories, medications, and allergies. By having a voluntary service, such as Google Health, Microsoft's upcoming competing service "HealthVault", or "Revolution Health" (bankrolled by by AOL's co-founder Steve Case), which can be securely accessed by health care providers, it becomes easy to create and maintain an accurate health profile for both the benefit of the user and healthcare providers approved for access by the user.

It should be noted that there are always security and privacy risks of posting sensitive information, such as health records, online. It is quite conceivable that hackers could penetrate the security of any establishment or server that contains or has access to sensitive personal information. While I know that they are not perfect, I basically trust Google Health with my information.

While there are many other "PHR" systems and services in use, often administered by corporations for their employees, others are offered by health insurance companies, as well as some regional PHR services, Google Health has the reputation and distribution (as well as the deep pockets) to create and securely maintain such a system, and sign up participating partners who are willing to allow the sharing of medical records.

I knowingly volunteered to post my medical records on Google Health. I hope the project succeeds, and more local physicians, pharmacies, labs, and hospitals partner with the service. As more healthcare providers transition to purely digital medical records, it will become easier to securely share this vital information.

Power Supply Tips

By Dan Hanson, the Great Lakes Geek, Computers Assisting People, Ohio
www.capinc.org/
Dan(at)magnuminc.com

We have all experienced the computer crashing seemingly for no reason. When it does, we blame Windows or a hardware problem or maybe a power surge or undervoltage. All are possible culprits but one often overlooked possibility is the power supply of the computer.

The power supply is the metal box with a cooling fan next to it. Typically it's in a back corner of the case and you plug your power cord into it. When you plug the power cable into the wall, the power supply converts the AC (alternating current) that runs through your home or office into the DC (direct current) that the computer needs.

If you bought your computer from a superstore or discount retailer it may a have low-cost, low-capacity power supply installed which may not be enough to handle all the things you do with your PC.

If you have upgraded your PC with newer or more components (like another CD or DVD player/burner, more RAM or another hard drive) then the power supply that came with your system may not be up to the task.

The physics of power supplies (ambient temperatures, 3.3V vs. 5V vs. 12V, etc) make it so that a power supply rated at certain wattage, say 300W, may not really provide that maximum wattage load. Some experts claim that power supplies are most efficient at 30-70% of their maximum capacity. So if you are nearing that maximum, you can be in for trouble.

Because the power supply gets a rush of AC (alternating current) when the computer is turned on and it heats and cools each time it is used, it is more prone to failure than many other components in your PC. You may notice a slight burning smell before it shuts down. Sometimes the cooling fan stops working and the system overheats.

Newer systems let you monitor the status of the power supply from Windows. Servers and other mission critical computers often have more than one power supply so that when one dies, the other kicks in and the system stays operational.

So what can you do?

Next time you buy a PC, don't just get a cheapo system with a sub-standard power supply unless you never plan on adding memory, drives or other components to the machine.

Take care of your power supply by keeping the cooling fan away from the wall or anything else that might block the air flow and make the fan work harder (and die sooner).

Keep the PC off the carpet or other surfaces where it may suck in particles and clog the fan. Cooler is always better with electronic components.

Periodically, blow out the fan and case with compressed air to get rid of dust and other particles that may clog up the fan and overheat the system components.

Add up the wattage of the components in your system to see if you are near the maximum of the power supply. E-mail us at dan@greatlakesgeek.com for a list of Estimated Power Requirements of common PC components.

If that is too difficult for you, look to see if most of the slots in the back of your PC are filled and if the drive bays in the front are being used. Those are indications that you may be close to maxing out your power capacity.

If you have a need, you can buy and install (or have someone else install) a new, heavy duty power supply. They come in several standard form factors to fit in most PCs. Warning this may not be a project for beginners though.

Get more tips at www.GreatLakesGeek.com

“Computune-up”

by Berry F. Phillips, member of the Computer Club of Oklahoma City
www.ccokc.org
bfdata(at)1access.net

Do you want your computer to run faster and increase your productivity? Of course; if you have major problems, you will need to contact your manufacturer and/or professional technical support. Many of those costly major problems can be prevented by doing “computune-ups” yourself. Yes, you can do it even without being a computer geek! My thanks to Microsoft for some of the information in this article.

“Computune-up” (Software)

1. Clean up your desktop! If you have not used a program for a year or one that you never use that came bundled with your system why not delete it. You will get more space on your hard drive in return.

2. Clean up your system tray to the left of time on your Taskbar! When you remove icons from your system tray that you rarely use, it will speed up your system since your computer has to locate those programs whenever you boot up. I love a little freeware program called Code Stuff Starter that shows you what is running and lets you easily turn those programs on or off.

3. Defragment your computer and your registry which will make your system run faster by consolidating fragments on your hard drive and registry. I use freeware programs like SmartDefrag and Aus Logics Registry Defrag and there are others available on the Internet.

4. Check your memory. The more programs you have running the more demand on your system memory (RAM). Adding more memory to your system will increase speed and is very easy to do without paying for expensive technical support. You can do it with minimal instruction or have a technically-oriented friend or club member do it since it only takes a few minutes to replace.

5. Keep your operating system updated and run utilities weekly! I strongly suggest you download needed freeware software for your system from “46 best ever freeware programs” thoroughly tested and rated with commentary.

“Computune-up” (Hardware)

1. Make sure your computer is unplugged before cleaning and not plugged in until your system is dry after cleaning!

2. Make sure you have the following tools available: a screwdriver, can of compressed air (available from a computer store), cotton swabs (not balls), rubbing alcohol, paper towels or anti-static cloths (available from a computer store), and water.

3. Clean the inside of your computer case! Using a screwdriver remove the side of the case opposite your motherboard. Touch as little as possible inside the computer, keeping fingers away from cards and cords due to static electricity. Blow air around all the components and along the bottom of the case, keeping the nozzle four inches away from your machine. Blow air into the power supply and into the fan from the back of your computer case. Blow air into the floppy disk and CD drives. Wipe the inside cover with a lightly moistened cloth before replacing it using your screwdriver. Clean every three months if your computer is on the floor or an especially dirty environment. Clean approximately every six to eight months in a normal environment.

4. Clean the outside of the case! Run a cotton swab dipped in rubbing alcohol around all the openings on the back of your case giving them one swipe with a dampened swab and one with a dry swab. Clean the remaining outside of your system. Do this whenever you clean the inside of your system.

5. Clean the mouse by taking out the screws and going inside with an alcohol swab. If there is a rubber ball, clean it with water, and let it dry. Then clean the outside of the mouse. Many mouse problems are simply caused by a dirty mouse.

6. Clean the keyboard! Turn it upside down and gently shake it and most of the crumbs and dust will fall

out. Blow air in and around the keys. Take an alcohol dampened cotton swab and clean the top and sides of the keys. Do this monthly; your keyboard gets very dirty and can even spread germs. If you have a laptop, follow the same procedure but take extra care with your machine.

7. Clean the monitor with a moistened paper towel or a soft lint-free cloth. (You can purchase monitor cleaning products from a computer store). Don't spray liquid directly on the screen but spray on the cloth. Wipe the screen gently to remove dust and fingerprints. (Never touch the back of the monitor). I suggest you purchase a special cleaning solution from a computer store for laptop computers.

If you have finished your "computune-up," you are on your way to being transformed into a computer geek! Do not be alarmed for the "geeks shall inherit the earth"! Bill Gates, chief geek and founder of Microsoft Corporation, has already made it; he is the role model for the rest of us!

Your Next Computer Will Be Green

By Marjie Tucker, Editor, Mountain Computer User Group, GA
www.mcug.org
mcug(at)dnet.net

With Europe leading the way, the computer industry is decidedly becoming "green." The Waste Electrical and Electronic Equipment (WEEE) and the Restriction of Hazardous Substances (ROHS) directives went into effect earlier this year. These two directives state that certain electrical and electronic equipment must cut down on hazardous
materials such as lead, mercury, and cadmium. They also give customers the right to return their equipment free of charge. Companies have several years to fully implement these directives, but the leaders have already started to make changes.

Dell, for example, is advertising Energy Smart workstations and notebooks that can reduce power consumption by as much as 78%. The Energy Smart configuration uses a default power setting that is designed to reduce consumption and energy costs right out of the box. In addition, the power supply, fan, and motherboard use significantly less energy to maintain cool internal temperatures.

HP is using 80 Plus power supplies to lower energy bills and AMD technology that reduces heat output and PC power consumption. In addition, they have already introduced an HP recycling program where you can trade-in or donate the products.
Government Initiatives Many U.S. government agencies have implemented standards and regulations to encourage green computing. The Environmental Protection Agency
launched an Energy Star program in 1992 and strengthened its requirements in 2006. In 2003 the California State Senate enacted the Electronic Waste Recycling Act and in 2007 President Bush issued Executive Order 13423 requiring all federal agencies to use the Electronic Products Environmental Assessment Tool when purchasing computer systems. In addition, a global consortium called The Green Grid was founded in 2007 by AMD, APC, Dell, HP, IBM, Intel, Microsoft, Rackable Systems, SprayCool, Sun and VMware.

Another initiative formed by a group of Global-minded IT executives, the Green Computing Impact Organization (GCIO), was created to be an active participant in transforming the IT community from an environmental liability to an Earth conscious example of responsibility. GCIO is a nonprofit organization that is based on environmental audit programs for consumers and small business homes with respect to general energy-efficiency programs (including lighting, heating, insulation, etc.). GCIO's mission is to educate and assist enterprise technology users in the design of environmentally aware and responsible information system operations. They help consumers become more environmentally responsible by reducing energy consumption and electronic waste in an effort to protect the Earth.

GCIO is sponsoring educational programs across the country and participating in a Green Computing Summit that will be held in Washington, DC on May 20th. The summit will address how public sector IT managers, procurement officials, and program managers public sector professionals can transform their IT and data center operations into more environmentally conscious yet efficient solutions. This conference will attract senior government IT professionals and their industry partners tasked with helping agencies become greener in the coming years. Attendees will represent federal, state and local governments, public policy organizations and suppliers to government. You can read more about this event at www.e-gov.com/EventOverview.aspx?Event=SGCS08 .

Features of Green Computing

Power management is the most popular method. The operating system of the computer can be set to directly control the power saving aspects of the hardware. It can automatically turn off the monitor or hard drive after a period of inactivity. Or, the entire system may hibernate, turning off most of the components such as even allow the user to manually adjust the voltages supplied to the CPU to reduce the electricity consumption and the amount of heat that is produced. As of July of 2007, all new Energy Star certified desktops must have a power supply that is at least 80% efficient.

Other features include using motherboard video output instead of a video card, hard disks that consume less power, flash based solid state drives that require fewer write cycles, and lower energy monitors. And, manufacturers of networking equipment are developing switches and routers that reduce energy costs.

Recycling Materials

Obsolete computers can be reused for charities, non-profit organizations, and developing countries. Parts from really old systems can be recycled through some recycling centers. Some recycling charges can be passed back to the manufacturers.

Recycling this equipment keeps the lead, mercury, and chromium out of our landfills. In addition, computer supplies such as cartridges, paper, and batteries can be easily recycled.

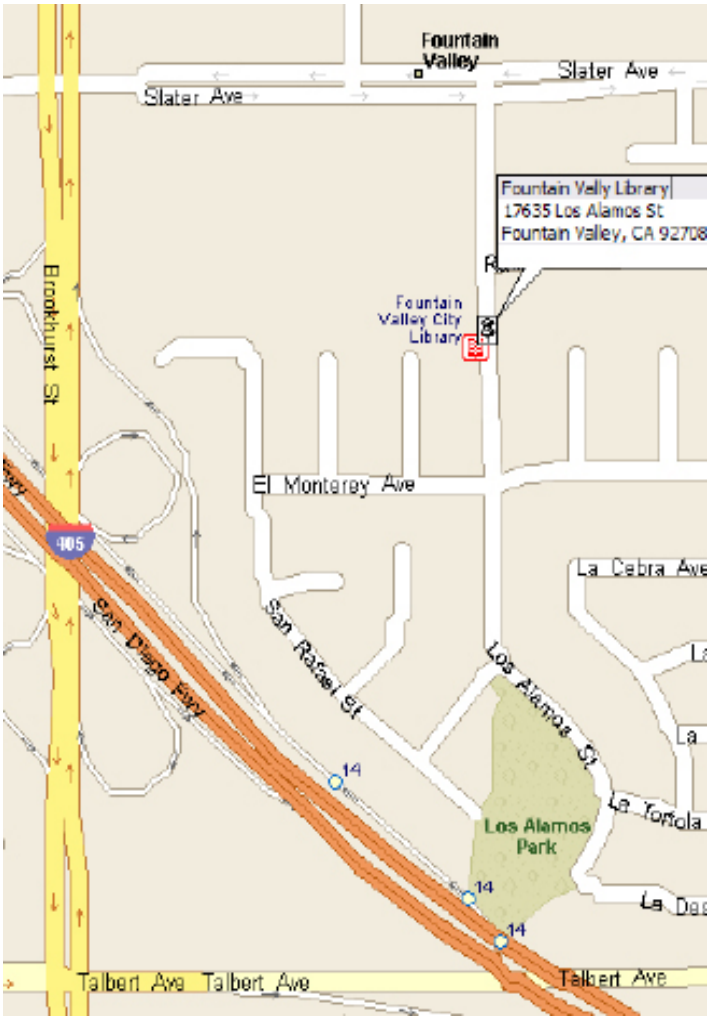
How Can We Work Greener?

Visit the website for Climate Savers Smart Computing at sww.climatesaverscomputing.org to view a three step program to go green. Here are the basic steps that they suggest:

Step One - Turn on Power Management. Since the average desktop PC wastes nearly 50% of the energy it consumes as heat, it makes sense to use the power management features that are built into Windows XP and Vista. The benefits? You will reduce your electricity bills and your energy footprint will be lowered as you reduce your greenhouse gas emissions. The Climate Savers organization predicts that the power management features on your computer can save nearly have a ton of CO2 and more than $60 a year in energy costs.

Step Two - Buy an energy efficient computer. Energy Star, the program designed by the U.S. Environmental Protection Agency, specifies the standards that equipment and appliances must meet to wear the Energy Star badge. You can visit their website at www.energystar.org for specifics. Basically an Energy Star compliant PC uses 15 to 25 percent less energy. This program is expected to save U.S. consumers and businesses more than $1.8 billion in energy costs over the next five years and prevent greenhouse gas emission equal to 2.7 million vehicles.

Step Three – Unplug from phantom power. As long as your computer is plugged in it still uses electricity, even while it is turned off or in standby mode. A computer that is turned off, but still plugged in, can use up to 10 watts. The Climate Savers estimate that you can reduce your electricity bills by as much as 10% by unplugging your appliances and electronics when they're not being used.



Membership application or renewal Form

Annual membership is only $20.00. Each additional family member is $5.00.

_____

Print Name:

_____

Address:

_____

City, Zip:

_____

Phone:

_____

Business Phone:

_____

Email address

Mail to

WINNERS - WINdows usERS
PO Box 9804
Newport Beach, CA 92658-9804

WINNERS - WINdows usERS
PO Box 9804
Newport Beach, CA 92658-9804

meets at
The Fountain Valley Branch Library
17635 Los Alamos
Fountain Valley
meetings on 3rd Saturday
10:00 a.m. to 12:30 p.m.

Notice the January meeting due to a conflict (someone at the library beat us to the regular time) will be at a special time 1:00 - 4:00 p.m. on January 17