BAY BYTES

Greater Tampa Bay Personal Computer User Group, Inc.

Newsletter

Issue 5 | May 2012 | 26th Year of People Helping People!

In this Issue

Single-Atom Transistor	*Cont.*	**2**
Computer password tips		**3**
What is Virtual Memory		**4**
What is Virtual Memory	*Cont.*	**5**
Facebook's privacy policy		**6**
Crime over the Internet		**7**
Crime over the Internet	*Cont.*	**8**
Things to look into...		**9**
The lighter side		**10**
Last minute news		**11**

Don't forget to visit our club's site at: http://gtbpcug.org

As well Don Miller's and Darrell Manns' :

http://www.dmanns.org/dmiller/

Researchers Develop Single-Atom Transistor

Article Date : February 21, 2012 http://www.pcmag.com

By **Damon Poeter**

Moore's Law could be safe for another decade or so. An international team of scientists has demonstrated a working transistor comprised of a single atom–nearly 100 times smaller than the 22-nanometer cutting-edge transistors fabricated by Intel.

More importantly, the research team led by Michelle Simmons of the University of New South Wales in Sydney was able to show a method for repeating the process with great accuracy and in a fashion that is compatible with the CMOS technology used in transistor fabrication today.

"This is the first time anyone has shown control of a single atom in a substrate with this level of precise accuracy," said Simmons, who worked with colleagues from the Korea Institute of Science and Technology Information, Purdue University, the University of Sydney, the University of Melbourne, and the University of New South Wales on the project.

The "law" associated with Intel co-founder Gordon Moore predicts a steady rate at which the density of transistors on silicon-based semiconductors increases over time. That steady procession of ever-smaller computer circuitry has held up for decades, but as the size of transistors approaches atomic scales, there have been serious questions as to whether Moore's Law can last much longer than another five years or so.

The work of Simmons and her colleagues could show a way to keep making microprocessor circuitry smaller and smaller through 2020 and beyond.

As they run up against atomic scales with ever-smaller circuitry, semiconductor manufacturers today are running up against problems affecting transistor performance that stem from quantum effects (basically, the fact that materials interact very differently at very small sizes) and a need for precision that may not be possible with the lithographic methods currently in use.

Continued on the next page

In recent years, advances in quantum computing have offered a viable path to smaller and smaller transistors, to be sure. But the new research might be the first strong sign that atomic-level transistor fabrication can be done in keeping with the part of Moore's Law that's often forgotten amidst the wonderment over tinier and tinier computer chips–that it be done cheaply.

Using a "combination of scanning tunneling microscopy and hydrogen-resist lithography," the team was able to "deterministically" place an individual phosphorus dopant atom "within an epitaxial silicon device architecture with a spatial accuracy of one lattice site," according to a paper published Sunday in the journal *Nature Nanotechnology*.

In layman's terms, that means the researchers are able to stick the phosphorous atom (used to "dope," or add an electron charge to a silicon substrate) precisely where they want to, whenever they want to.

That's important, because as transistors approach the size of atoms, it becomes hugely important to place each of those atoms very precisely. On larger scales, silicon can be doped with less accuracy and still produce the electrical current needed to switch between "on" and "off," the essence of what a transistor does and how it works.

As the researchers put it:

"Silicon technology is now approaching a scale at which both the number and location of individual dopant atoms within a device will determine its characteristics, and the variability in device performance caused by the statistical nature of dopant placement is expected to impose a limit on scaling before the physical limits associated with lithography and quantum effects are reached. Controlling the precise position of dopants within a device and understanding how this affects device behavior have therefore become essential."

Other scientists have created single-atom transistors in the past, but through a great deal of costly trial-and-error. The new research suggests that the first step towards a cost-efficient technique for creating single-atom transistors, a repeatable process, has been attained.

"I've learned that I thrive on stress.
That's why I started dating again."

Computer Password Tips and Strategies

By Jim Cerny, Director, Sarasota PCUG, Florida March 2012 issue, Sarasota PC Monitorww.spcug.org jimcerny123 (at) gmail.com

Most of us have several computer or internet “accounts” which provide us with many free services such as email, movies (Netflix), video communications (Skype), photo printing (at Wal-Mart, Walgreens, etc.), music (I-Tunes), banking, shopping, games, entertainment, books, and many more. In fact, your computer is the perfect window to the world and all the people and services in it! But each account you set up requires some sort of “ID” and a password. For example, your email account is your email address and it requires a password to access your email. Many other accounts will use your email address as your ID (so they can email you notices and ads) but will require another password. How do you handle all your accounts and passwords? Here are some helpful tips:

1. ALWAYS WRITE DOWN EVERY ACCOUNT AND PASSWORD YOU HAVE. I cannot emphasize this enough. Review this list every few months and make sure it is current. Keep it with you when you travel. Keeping them on a small portable “jump” drive is a good idea too. You may have set up your computer at home to easily access your email, perhaps telling the computer to “remember me” or your password for you, but when you travel or use another computer you will need your passwords! Personally, I do not ever allow my computer to “remember” any of my passwords – I enter the password from the keyboard each time I “log in” any account. That way, no matter what computer I am using, the way I access my account stays the same – I always enter my account and password.

2. Write down the internet address of the web page where you enter your account and password.
Many people use a “favorite” or an icon on the desktop to quickly get to the “log in” screen for their account. This is ok, but if you use another computer you will not have your shortcuts! So write down the web page address needed for each account.

3. The longer and more complex a password is, the safer it is. In fact, many services now require a password of 8 or more characters with some digits or other “non-letter” characters. Some accounts may require you to periodically change your password. But, hey, we are not spies guarding government secrets. Keep your passwords simple. Use unusual combinations which are easy for you but would be difficult for someone else to guess. Children’s names, birthdates, and home address numbers are too easy for someone to guess since such information can be obtained without too much effort. Instead, try the make and model of your first car, a childhood favorite game or toy, the name of your superhero, the nickname you gave to your worst in-law, etc. Get the idea? Easy for you but hard for someone else to guess, and impossible to find out without knowing you personally.

4. Yes, you can use the same password for multiple accounts. Now if someone really wanted to use your Skype account or read your email and they had a hint to one of your passwords, it would be much easier for them to guess your other passwords. So your security is reduced. But, honestly now, who would really want to steal your passwords anyway? Who would care? Well, ok, maybe for banking or credit card accounts I would be more careful, but for most other accounts I do not feel the need for a super secure password, so I do use the same password or a variation of it for several accounts.
In business, things are different. Most companies are very careful about computer and telecommunication security. But for personal home use, I think you can be much less paranoid.

But remember -- If your computer is repaired or replaced, or if you use another computer, you will need to have your passwords!

What is Virtual Memory?

http://www.askleo.com

Virtual memory is conceptually somewhere between RAM and hard disk space; it's disk space used to maximize the amount of RAM available to programs.

There's memory and then there's disk space. There's memory that's on disk, not to be confused with memory that looks like a disk. Disk that looks like memory? Isn't the disk a kind of memory? Or is it something else?

It *very* confusing, but we can clear a few things up. Disks and memory are fairly easy. Virtual memory is one way they overlap, and with a little explanation we can make that a little less confusing too.

(Note: the sizes of RAM and Hard disk mentioned below may seem small by today's standards, but the concepts *definitely* still apply. No matter how much RAM or disk space becomes commonplace we always seem to want more. .)

First let's review the basics: Memory versus Disk Space.

When a computer geek like me (or a computer salesman *not* like me) talks about computer *memory*, or RAM (for Random Access Memory), we're talking about a bunch of silicon chips in your computer that hold things like the operating system, the programs you're actually running right now, the document currently shown in your word processor, or the email you're typing up. Computers these days typically have somewhere between 128 megabytes (128 million bytes) and 4 gigabytes (4 billion bytes). What's important is that when you turn the computer off or if it crashes - *poof* - anything stored in RAM is gone. That's why when you're editing a document it's a good idea to save to disk often.

When we talk about *disks*, we're talking about the hard disk drives in your machine. Quite literally, a hard disk drive is typically made of several metal disks coated with a magnetic material not unlike a video or audio tape, or the strip on the back of a credit card. The disk spins at a fairly high rate of speed, and special "heads" can read, or record, a pattern of bits (1's and 0's) on the magnetic surface. The operating system assembles those bits into bytes, and the bytes into the files you might save, receive, or create. Disks do *not* lose what's on them when you turn off the power. Typical disk sizes these days start in the 20 to 40 gigabyte range and go as high as 250 gigabytes. It won't be long before we see the next step, the terabyte (one trillion bytes), on a single disk.

Compared to memory disks are much slower. Too slow in fact for your computer to work from directly. So the typical sequence of events is to load your program or document into memory from disk, have it run or be worked on in memory, and then either remove it from memory if it hasn't changed, or save any updates back to the disk.

Continued on the next page

Virtual Memory is simply the operating system using some amount of disk space *as if* it were real memory.

Exactly how virtual memory is implemented is complex and well beyond what I'd want to present here. But in an over-simplified nutshell it works like this:

You run programs that need memory. The operating system takes care of tracking which program is using what portions of memory, and allocating each program the amount of memory it needs.

- Those programs will need more memory as they do their jobs. Opening a large document may cause your word processor to request additional memory from the operating system in order to hold the document.
- *If* there isn't enough memory available to satisfy a request, the operating system may decide that another program's needs are less "important". Some of that program's memory will be freed, first by writing the contents to disk (the memory is "swapped out"), and then allocated to the program making the request.
- Later when the program whose memory was swapped out needs it back, that memory can be "swapped in" by reading it back from disk. This might cause memory from another program to be swapped out to make room.

Also remember that the operating system itself is also just a program. So it too will have need for memory. It can allocate memory to itself and its memory may get swapped out to disk as other needs arise.
As I said, disks are slower than memory, so if the operating system is doing a lot of swapping between the two it's going to slow your computer down. If that's happening frequently or if your computer seems to be "thrashing" or constantly swapping in and out from disk, then it might be time to add some memory to your machine. It can be one of the most cost effective ways to increase your system's speed.

_____ _____ _____ _____ _____ _____ _____ _____ _____ _____

Tip:
Cookies are great, especially if you don't want to type in a password every 30 seconds. Few people, however, like the kind of cookie that follows you from one website to another to report to advertisers on what you're looking at. But you can block those "third-party" cookies without getting rid of the useful kind.
For Internet Explorer, go to Control Panel, Internet Options, click the Privacy tab, and either choose a preset on the slider that blocks third-party cookies, or click Advanced, check Override automatic cookie handling, and check Block under 'Third-party cookies'.
In Safari, go to Edit, Preferences, Privacy, and set 'Block cookies' to From third parties and advertisers.
In Firefox, go to Firefox, Options, Privacy, and select Use custom settings for history from the drop-down menu. Uncheck Accept third-party cookies.
With Chrome, go to Options, Under the Hood, Content Settings, and check Block third-party cookies from being set.

Facebook's Privacy Policy

By Constance Brown, President, Canton Alliance Massillon User Group, Ohio March 2012 issue. The Memory Map http://.camug.com

Did you know that Facebook's privacy policy is more than 1300 words longer than the United States Constitution without the amendments? *That Facebook had 400 million registered users in May of 2010, half of whom login daily? That Facebook has ** 800 million users as of February 2012? That people spend more than 500 billion minutes there each month? How private are your communications on Facebook?

It used to be that you set up your privacy policy when you joined Facebook and could revise it from time to time. Now Facebook "has revised its privacy policy to require users to opt out if they wish to keep information private, making most of that information public by default. Some personal data is now being shared with third-party Web sites."

If you want to protect your privacy on Facebook, you have to engage a lot of buttons and select many controls. The new privacy policy itself is *45000 words long. To enjoy privacy you will need to press 50 buttons and make 170 selections. Not exactly easy and certainly time consuming. You will have to make sure to select to show information only "to me" or "to friends." You will not want to share with "friends of friends."

"Under the Account Settings option, in the Facebook Ads tab, two options are automatically turned on to share some information with advertising networks and friends. Anyone who wants to keep this information private must uncheck the boxes in that tab.

"Facebook has also added a feature, called community pages, which automatically links personal data, like hometown or university, to topic pages for that town or university. The only way to disappear from those topic pages is to delete personal data from Facebook."

**"Facebook does not sell user's information. They provide targeted advertisement.

From Richard Allan, Facebook policy director.

"Q. Do you ever think of selling any user information that's held in Facebook? [sic]

"A. No… Facebook has a business model. We looked at it and there are three ways you can run a service like ours.

"You could charge people subscriptions. And we decided early on, we didn't want to do that and we never will. That we're not going to charge people to subscribe to the service.

"The second way would be to sell data. And we looked at that and said that's not a very good business model because nobody will trust you.

"So the third way is to show people advertising. So they can use the service freely, but they get ads on the page. And that's what we do. Those ads are targeted according to your age, interest, where you live… but the advertiser doesn't get the data. They get to show the ad to you.

"Richard Allan is a former Liberal Democrat MP, a UK political party with a position of cultural liberalism and civil liberty. Now he works for Facebook, which is at the centre of a contentious debate on what role sites of its ilk play in free expression and free speech.

Is Your Internet Security up to Date?

Antivirus up to date?

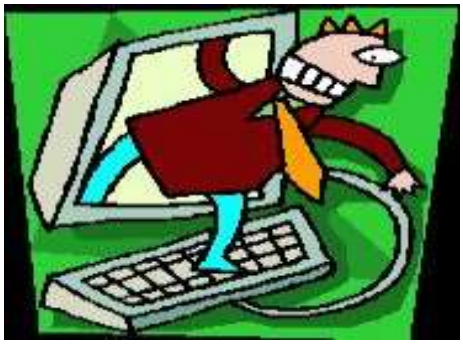
Firewall?

Windows up to date?

Spy Ware?

See how to protect your computer at:

http://gtbpcug.org/protect/



More about Internet Threats

Crime and Conflict over the Internet

By Greg Skalka, President, Under the Computer Hood User Group, CA president (at) uchug.org www.uchug.org

Recently my family and I were in Las Vegas and while we were there, another hacking incident hit the news. Zappos.com, an online shoe and clothing retailer, announced that they had been the victim of a cyber-attack. Being based in nearby Henderson, the reports on this company that I was previously unaware of (you can imagine how much online shoe buying I do) dominated the Las Vegas local news. Customer address, phone and email information had been stolen, but fortunately credit card info and account passwords remained secure.

This was just one more incident in an increasing trend of crime and conflict conducted over the Internet.

Reports of hacked computers and stolen commercial data have become commonplace. The Internet appears to be a prime medium for crime, with organized crime elements taking advantage of the easy access and anonymity. I've so far avoided being part of one of these data thefts from a major company that I've entrusted with some of my personal information, but it is probably just a matter of time until I'm a victim too. I'm also under siege on a smaller scale, receiving several scam emails every day. Most are such obvious scams that I almost have to laugh. Is the head of the FBI or Secretary of State Hillary Clinton really going to email me about claiming foreign funds I previously knew nothing about? I have seen some pretty realistic emails from banks (mostly ones I don't do business with, but a few that I do), advising me to click on a link to avoid a loss of account access. A little restraint and outside research show even the most polished of these to be fakes intended to trick you out of personal information or plant malware on your computer.

The worst of these online scams try to use your own friends and family to trick you into lowering your guard. I recently received an unsolicited email from my sister, which was also addressed to a number of other family members. It contained only a vague greeting and a link. I recognized it as a scam, but my wife did not.

Fortunately, it appears the link only led to a Viagra-peddling website, as repeated cleanings of her computer turned up no malware. It appears that someone gained access to my sister's email account and used it to send this message to everyone in her email address book. After receiving this sham email herself at work, she changed her email account password and sent a warning out to all her contacts. That showed good web etiquette. I receive similar emails periodically from a friend's account, but he never responds to my warnings about his email account being hijacked. If you lose control of an email account in this way, at least let the provider know so the account can be closed. If you simply abandon the compromised account, you'll likely leave a zombie account out there to continue pestering your friends.

Continued on the next page

In addition to the criminal element, the political conflicts of our world are starting to creep into the Internet.

While electronic personal communications can play a positive role in exposing repression around the world, and can be a tool for change towards more open and free political systems, the access to information can also be a weapon. Enemies of our country and way of life hack our government and commercial web sites to steal information and deny legitimate access. Our businesses and institutions may be under attack through the Internet by factions related to or agents of China, Russia or our middle-eastern adversaries.
Our own government has formed cyber warfare elements and acknowledges that future battles may include skirmishes in cyberspace. It is speculated that the Stuxnet worm, which appears to have targeted uranium processing facilities in Iran, may have been the product of U.S. or Israeli intelligence agencies. Palestinian hackers steal and release account information from banks and institutions in Israel, leading some in Israel to do the same with information on Palestinians.

Where will all this lead? I'd hate to see the "Information Superhighway" that was supposed to be our free and open Internet turned into the electronic equivalent of the highways in "Mad Max", where danger lurks everywhere and lawlessness abounds.

And speaking of laws on the Internet, we have recently witnessed online protests over U.S. Internet piracy legislation. A number of prominent web sites, including Google and Wikipedia, conducted partial shutdowns or redirections to protest pending legislation and solicit support from their users. The Stop Online Piracy Act (SOPA) and Protect IP Act (PIPA) are bills under consideration by the U.S. Congress to protect intellectual property. Opponents claim the proposed legislation would harm free speech and reduce technical innovation on the web. I acknowledge online piracy is a problem, but also don't want a solution at the expense of an open Internet. Hopefully our own government won't soon be in the censoring business.
We all have an interest in how this issue is resolved.

With all this conflict on and over the web, it makes me wonder if I'm taking all the reasonable measures I can to protect myself and my assets as I use the Internet. It is sometimes difficult to determine where "reasonable" fits in between "it won't happen to me" and a bunker mentality. As I've moved my finances and shopping online, I've realized I've become more dependent on the Internet. By conducting all my banking activities, including bill payment and monitoring of accounts, on the web, I hope I've not made myself more vulnerable in the process. Am I safer not having bank statements mailed to me, or am I now more open to theft by hacking or scams? How would I access my money in a web-only bank account if the Internet should for some reason go down?
It is great to be able to surf where I want, but does that surfing potentially expose me to malware that could capture my account information when I bank with the same computer? Is it paranoid to consider using a separate computer for banking and another for other web access?

It is exciting to think that the whole world can be accessed through that little RJ-45 Ethernet jack on your cable or DSL modem. It should also be sobering to consider that the whole world could be there in that connection.

Tablets of Clay

The crooks are not only after us on the Internet, but also in our electronics stores. Over this last Christmas, a number of iPad purchasers got the wrong kind of tablet. In Canada, a number of customers that purchased iPads at reputable stores like Best Buy and Wal-Mart later found the box contained not a tablet PC but a slab of modeling clay. In perhaps more than a dozen reported cases, it appears crooks purchased iPads at these stores with cash, replaced the items in the box with the same weight in clay and expertly resealed the boxes. The boxes were returned to the stores for refunds, and since they appeared to be unopened, they were replaced on the shelves to be purchased by unsuspecting customers. The first customer discovering this switch was thought to be a scammer by the store, but after additional cases were discovered, he was reimbursed and given an iPad.

Some things to look into…

Do you use Hotmail for email? Do you also have a Kindle Fire? Now there is an app that allows you to access your email from the Kindle Fire ...
http://tinyurl.com/7kne5qb

If you received a green envelope recently from Compliance Services, Tallahassee, stating the law in regard to corporate minutes, etc., and asking you to fill in a form, and send it along with a check for $125., it is a scam. You can check it out at ...
http://gingerreichl.com/2011/04/20/corporate-compliance-scam-annual-minutes-requirement/

You all know how important it is to do regular backups of your entire pc, so we won't belabor the point. To learn more about the program, you can also point your browser to Acronis' Web site at ...
http://www.acronis.com/homecomputing/products/trueimage/

With New Standard, Wi-Fi Could Become As Widespread As Cellular
POPULAR SCIENCE - NEW TECHNOLOGY, SCIENCE NEWS, THE FUTURE NOW | FEBRUARY 23, 2012 ...
http://pulse.me/s/6cYQv

The link below is a senior citizen father trying Windows 8 for the first time while his son video tapes the session. It runs about 4 minutes. This could be the reason more than half of the people who have tried Windows 8 preview would NOT recommend the new operating system to their friends ...
http://www.youtube.com/watch?feature=player_embedded&v=v4boTbv9_nU

XP still not running fast enough for you, this might help you to get some extra speed out of it ...
http://askbobrankin.com/make_windows_xp_run_faster.html

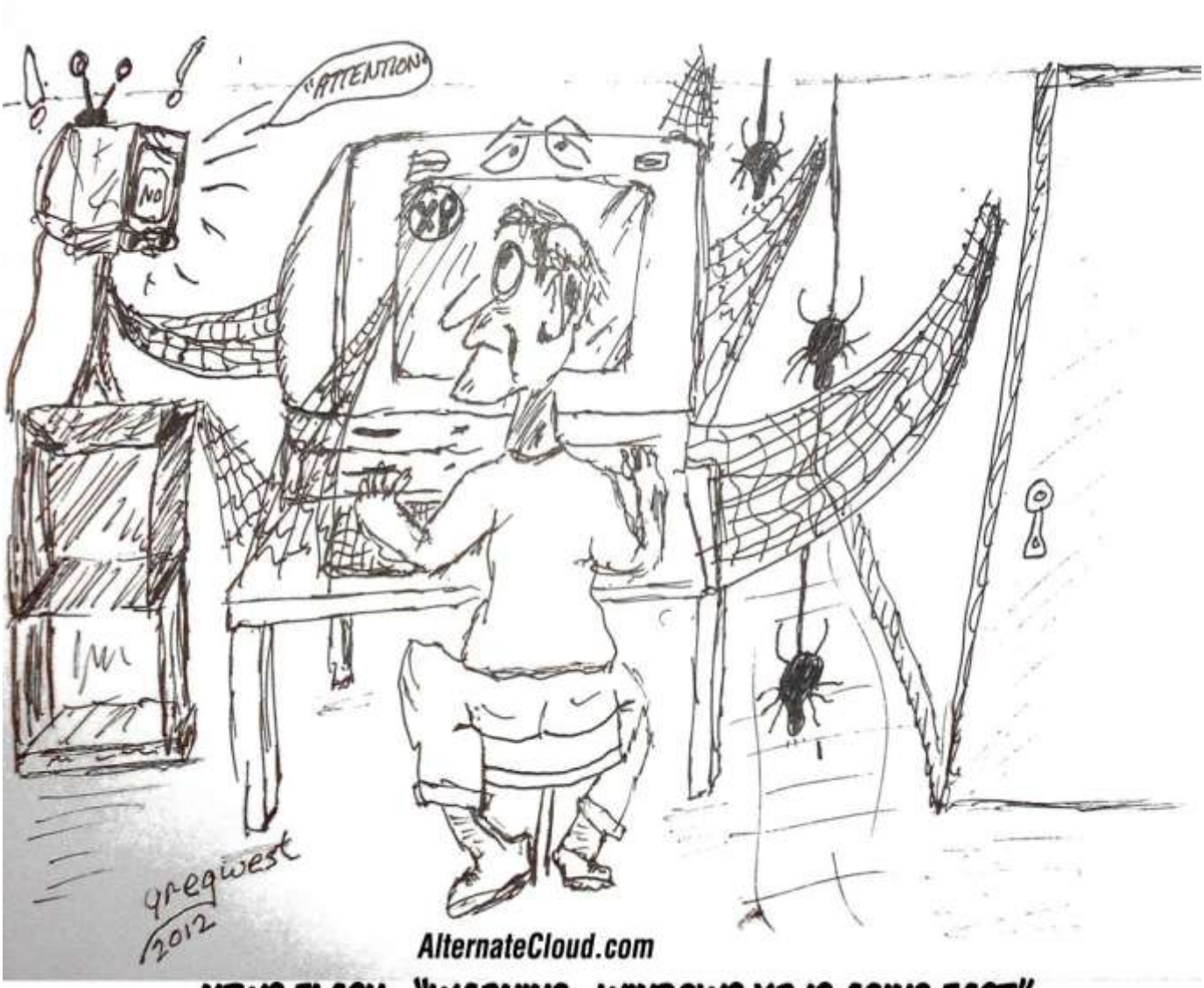
This also goes the same for Windows 7...
http://askbobrankin.com/speed_up_windows_7.html

If you need to access your own computer or someone else's from a remote location, you probably already know about GoToMyPC, which is often advertised on radio and TV. GotoMyPC's remote access service costs $20/month. But did you know that you can do the same thing for free? Here's how...
http://askbobrankin.com/free_alternatives_to_gotomypc.html

Unlike diamonds, hard drives are not forever. It's very likely that someday you'll start your computer, and instead of the familiar startup screen, you'll see one of these ominous messages: DISK BOOT FAILURE... NO FIXED DISK PRESENT... ERROR READING FIXED DISK... or HARD DRIVE FAILURE. Don't panic just yet, there may be hope for recovery of that damaged hard drive ...
http://askbobrankin.com/hard_drive_data_recovery.html#ixzz1qoVDeymF

Sometimes it seems obvious, sometimes not, but ultimately there's no way to prove that a computer is not infected. Best we can do is increase the odds ...
http://ask-leo.com/how_can_i_tell_if_my_computer_is_infected.html

The lighter side



NEWS FLASH... "WARNING...WINDOWS XP IS AGING FAST"

Some of the material appearing in this Issue was sent to the editor by other members of the GTBPCUG. Thank you.

Last minute news...

DNS Changer Malware

According to an article in the Saturday, April 21st issue of the Tampa Tribune, an ad scam has infected over half a million pc's. The malware redirects those pc's to Web sites other than the ones the users think they will be going to.

After an investigation some time ago, the FBI set up a safety net for those pc's, using government computers to help prevent Internet interruptions for those pc's. However, that safety net is now set to be discontinued by July 9th.

If you wish to determine if your pc is infected the DNS Changer malware, point your browser to http://www.dcwg.org, and click on "Detect" at the left or on the button next to it. When a new page comes up, click on the link next to "English" (http://www.dns-ok.us), wait a few moments, and if your pc is NOT infected, you will see a large green box, and underneath the green box will be "DNS Resolution = Green."

(Note: if for any reason you want to double-check that result, especially if your Internet provider is currently redirecting DNS traffic for its customers, read and follow the directions below the green box, which will take you to the FBI's web site.)

If instead of the green box you get a red logo, you'll be directed to Web sites where you can get tools to remove the malware infection.