

# NATGUG News May June 2007

## Editorial

Gates has done it again, yes he's launched another Windows system which has built in problems, Firstly only the 32 bit version will run your old XP software, the 64 bit will not even run some of your old system or hardware drivers, secondly it has built in security to stop pirates, if it suspects you have fiddled with the system it slowly shuts parts of the system down and disables itself, if it gets it wrong though and you haven't fiddled with the system how do you put that right and stop your system disabling itself, I trust you will enjoy this security measure.

Reportedly there are 4 home and 4 business systems, although I have only spotted three Home Versions for sale, The Basic costing 179.99 Premium 219.00 and Ultimate 369.99, apart from the fact you will have to purchase a whole load of new versions of your software to run on Vista and the cost of the Windows software, the usual comments are coming from the experts, @You have to be rich, have more money than brain cells and lots of time on your hands to even want to purchase Vista.

Gates said he thinks 100 Million computers world wide will be running Vista in 12 months time although some computers will not run Vista at all the recommendation for system requirements are 512 MB Ram 800Mhz Processor 15 Gig hard disk space, remember ME required half a gig XP wanted 1.5 gig and now Vista requires 15 gig I can't wait to see how much space will be needed for the next new system.

Microsoft have pledged they will support XP until 2011

## Ergonomics for the Elderly

by Herbert A. Goldstein  
Sarasota FL PC Users Group  
[www.spcug.org](http://www.spcug.org) -  
[pcug@comcast.net](mailto:pcug@comcast.net)

[This article is reprinted from the 2005 March issue of "SYDTRUG News", newsletter of SYDTRUG Inc., PO Box 75, PANANIA NSW 2213, AUSTRALIA, where it was brought to you by the Editorial Committee of the Association of Personal Computer User Groups (APCUG), an international organisation to which SYDTRUG Inc. belongs. There is no restriction against any non-profit group using this article as long as it is kept in context, with proper credit given to the author.]

As baby boomers reach retirement age the ratio of employees to retirees will equalise over the next twenty years. Considering that the foundation of Social Security benefits is generated from the workers it is evident that benefits will be inadequate for future retirees. In order to endure, the elderly will be forced to keep working beyond the current retirement age.

As our increasing knowledge of the ageing process brings about breakthroughs in life extension technologies, the elderly will come to play a greater role in the productivity of our economy. Upcoming ergonomic developments will be critical in order to accommodate the elderly as viable and productive members of the workforce.

With the physical restrictions that naturally come with age we can expect that many elderly would be regarded as having disabilities and the ones who are not technically disabled could be considered physically and mentally compromised to some degree.

# NATGUG News May June 2007

Therefore, any workplace modifications that serve to overcome limitations in strength, coordination, endurance, sight, hearing and shift adaptability will accommodate the elderly into the workplace.

Visual restrictions can be overcome with a greater dependence on verbal communication with regard to instructions and assistive technology such as audio recorders. Labels should be in large, clear print with large, high-resolution computer monitors. Voice recognition software is also helpful.

Other modifications include paper holders and bookstands that allow for optimal positioning of written materials, voice mail systems for messages and raised edges along the sides of work surfaces to prevent objects from falling off.

In personnel with hearing limitations any audible information should be supplemented with some form of visual presentation. Whole body vibration transmitted to chairs should be minimised by utilising anti-vibration seating surface. Ambient noise should be minimised through workstation design, isolating noisy printers, sound dampening etc. Workers should have vibrating pagers, visual call indicators and sound amplifiers on telephones.

The elderly should have their work environment arranged in such a way as to avoid unnecessary reaching, lifting and carrying.

Storage systems with pull out shelves and workstation carousels help to keep frequently used materials within 18 inches of the body. Containers should be provided to break loads into manageable units and the employee should have the means to slide any materials over 2 pounds. Mechanical reaching devices should be available for accessing supplies beyond the reach of the worker.

With the preservation of their mental faculties and the advent of ergonomic innovations for staff, the elderly will find themselves continuing to play a dynamic and productive role in society into the later years.

## **Protection Against Virus Attacks Requires Routine of Preventive Practices**

by Gabe Goldberg -- CPCUG

[Reprinted from the 2005 March issue of "SYDTRUG News", newsletter of SYDTRUG Inc., PO Box 75, PANANIA NSW 2213, AUSTRALIA, where it was reprinted from the 2004 December issue of "Monitor", magazine of the Capital PC User Group, Inc., 19209 Mt. Airey Road, Brookeville MD 20833, U S of A]

People sometimes miss changes in the world around them, even in their home environment: the security fence sags, the guard dog ages and sleeps more, the alarm system stops working though its warning sign remains. We may feel safe and protected -- our castle may even look secure -- but appearances can deceive.

## NATGUG News May June 2007

For computers, anti-virus software combines the fence, dog, and alarm into a single handy package of protective services -- but those services take more frequent attention than the fence or alarm, and may need feeding nearly as often as the dog!

That's because anti-virus (a/v) software has a complex mission: detecting, quarantining, and eliminating computer viruses, worms, or other malicious programs (often called "malware"). Software is infinitely variable, limited only by the imagination of unfortunately creative nasty programmers. So today's new software virus was unknown when the a/v product you are now using was developed last month, last year, or even earlier.

At least there's some good news in how a/v software works. These programs are written to examine files being received (and sometimes transmitted) by your computer. So e-mail, music downloads, file transfers, floppy disks, etc., should all be automatically scanned for the presence of unwanted and dangerous stowaway software (check your a/v software to make sure appropriate protections are enabled!).

But how can year-old software detect a new virus? The answer is that the virus descriptions the a/v software uses for scanning can be updated separately from the software itself. You can think of virus profiles as "Wanted" posters hanging in the post office, which can be updated whenever there's a

new bank robbery. But just as there's not much benefit in having Jesse James' picture in your local post office, there's minimal protection offered by using last year's virus "Wanted" profiles!

Different approaches are advocated for keeping a/v software current. Some folks subscribe to (usually) free warning services from the government or a/v software vendors such as Symantec (Norton), McAfee, Sophos, etc. When alerts are issued about new virus discoveries, they update their a/v profiles and feel safe. In fact, it's often observed that most computer users just need to know that there is a new problem and that they should update their virus definition files immediately.

I disagree. I believe that specific problem warnings distract from following basic principles. Worry-upon-warning implies that there's no threat unless there's a warning. What if the threat arrives before the warning? It's much safer (and simpler) to follow basic rules:

- + Be cautious receiving attachments -- don't open attachments you don't understand or aren't expecting, or from someone you don't know. Don't click a virus attachment after being warned against it, "to see what would happen". The results won't be pretty.

- + Be cautious clicking web links received in e-mail. Verify that a link's apparent location is really the web site to which it points, because a link can be deceptive, spoofing the site to which it will take you. Most web browsers display the site

## NATGUG News May June 2007

associated with a link when you move the mouse cursor over the link without clicking it.

- + Install and run anti/virus software
- have it start automatically at PC boot, and set it to automatically scan arriving files.

- + Keep it current -- install new versions every year or two (often available free after rebates) and download software updates periodically.

- + Download new virus profiles regularly -- or, better, automatically, whenever the vendor makes them available.

- + Run a full virus scan of your hard drive at least weekly, using the (usually) built-in scheduling tool.
- + Carefully apply appropriate security fixes (software patches) to products such as Microsoft Office and Windows, and other applications.

These simple rules are akin to locking one's house, looking both ways before crossing streets, and not letting the gas gauge read 'Empty'. I don't find virus warnings useful because I always have security in mind, not just when I receive warnings.

Perhaps the most important step to take is understanding how virus threats, a/v software, virus profiles, and one's own computing habits and activities interact. Just as individual driving needs and

practices determine what we need in a car (e.g., powerful or gas/electric hybrid, automatic or standard transmission, performance or high-mileage tyres), PC applications determine security needs.

Someone frequently downloading games or music, or constantly seeking new shareware for tinkering, is at much higher risk than a person using a stable and small set of applications for e-mail, Web browsing, and desktop publishing. Unfortunately, even the latter person is at risk from viruses transmitted by e-mail and Web site booby traps. But risk increases with diversity of activity and applications, necessitating extra cautions.

Anti-virus software usually provides extensive configuration options controlling features such as when to start, what files to scan, when to fetch updates, and actions to take when virus software is found.

If your PC boots slowly and seems to be working hard before you start any applications, it may be scanning for viruses. (But, in fact, sudden slowing of the boot process may show signs of virus infection.) You may find it more convenient to schedule a weekly scan in the middle of the night than to have it delay every boot operation.

It's unfortunate that anti-virus software is a necessity of on-line life. Like seatbelts and door locks, it's best if a/v software never finds a problem to handle -- but when it

# NATGUG News May June 2007

does, it can prevent loss of irreplaceable data or having a PC become unusable without expensive repairs. Computer viruses are so increasingly common and virulent and a/v software is so inexpensive -- even free! -- that it's foolish and unnecessary to be unprotected.

Gabe Goldberg is a freelance technology writer, editor, and consultant, and currently serves as CPCUG's Outreach Director. He can be reached at [gabe@gabegold.com](mailto:gabe@gabegold.com).

## **Legal Bytes: It's the Slammer for a Spammer!**

by John Brewer  
Computer Club of Oklahoma City

[This article is reprinted from the 2005 March issue of "SYDTRUG News", newsletter of SYDTRUG Inc., PO Box 75, PANANIA NSW 2213, AUSTRALIA, where it was brought to you by the Editorial Committee of the Association of Personal Computer User Groups (APCUG), an international organisation to which SYDTRUG Inc. belongs. There is no restriction against any non-profit group using this article as long as it is kept in context, with proper credit given to the author.]

Spam is a nuisance. The cretins that engage in this sort of advertising deserve a fate of solitary confinement without Internet access and with rap music playing constantly at a high volume. A recent Virginia case has sent a message to the spammer community that should not be ignored. A jury in Leesburg, Virginia, AOL's home county, convicted two North Carolina spammers of sending spam through computers located in

Virginia. A third defendant was acquitted.

An article at Spamhaus.org reported the convictions. "Jeremy Jaynes of Raleigh, North Carolina, a prolific spammer who operated using the alias 'Gaven Stubberfield' and was listed by Spamhaus' ROKSO database as being the 8th most prolific spammer in the world, has been convicted of spamming using deceptive routing information to hide the source. A Virginia court recommended Jaynes spend nine years in prison for sending hundreds of thousands of unwanted e-mail messages. Virginia Attorney General Jerry Kilgore said Jaynes was found guilty under a Virginia state law that prohibits e-mail marketers from sending more than a certain amount of spams within a given time frame and prohibits the use of fake e-mail addresses.

Jaynes' sister, Jessica DeGroot, was also found guilty and fined \$7,500. An associate, Richard Rutkowski of eVictory Consulting (known to Spamhaus as being involved in "National Wealth Builders" spamming), was found not guilty.

A Loudoun County jury decided that Jaynes, 30, and his sister, DeGroot, 28, flooded tens of thousands of AOL e-mail accounts with unsolicited e-mail. The jury recommended that Jaynes spend nine years in prison and that DeGroot pay \$7,500 in fines for violating Virginia's anti-spam law.

Although both Jaynes and DeGroot lived in North Carolina, Virginia asserted jurisdiction because they

## NATGUG News May June 2007

sent messages through server computers located in the state."

SecurityFocus.com has reported other developments reference criminal prosecutions for spamming.

"A Los Angeles man who used other people's wi-fi networks to send thousands of unsolicited adult-themed e-mails from his car pleaded guilty to a single felony Monday, in what prosecutors say is the first criminal conviction under the federal CAN-SPAM Act. [Note: the Virginia prosecutions were under Virginia state law, CAN-SPAM is federal law.] In a plea agreement with prosecutors, Nicholas Tombros, 37, faces a likely sentencing range stretching from probation to six months in custody, assuming he has no prior criminal convictions. Sentencing is set for December 27th.

Tombros drove around the Los Angeles beachfront suburb of Venice with a laptop and a wi-fi antenna sniffing out unsecured residential access points, which he then used to send thousands of untraceable spam messages advertising pornography sites."

An FBI spokesperson said earlier this month that Tombros obtained the e-mail addresses from a credit card aggregation company where he used to work, but officials have not revealed how they caught the spammer.

The CAN-SPAM Act, which took effect January 1, 2004, doesn't criminalise unsolicited bulk commercial e-mail, but it does prohibit most of the deceptive practices used by spammers.

Tombros was charged under a provision that prohibits breaking into someone else's computer to send spam. Also outlawed is the practice of deliberately crafting spammy (Note: spammy ?) messages to disguise the origin; materially falsifying the headers in spam; spamming from five or more e-mail accounts established under fake names; or hijacking five or more IP addresses and spamming from them.

A first-time violator faces up to one year in federal stir for a small-time operation -- three years if he or she meets one of several minimum standards of bad behavior, like leading a spam gang of at least three people, sending over 2,500 messages in one day, or using 10 or more falsely-registered domain names.

Assistant U.S. attorney Wesley Hsu, who prosecuted Tombros, says he believes the spammer is the first to be convicted under CAN SPAM. "It is my understanding that it is, in fact, the first," said Hsu.

But even without the spam-fighting legislation, Tombros' drive-by spamming technique would likely have put him afoul of existing computer crime laws, said David Sorkin, an associate professor at the John Marshall Law School. "It sounds to me like this could very well have been prosecuted under other statutes."

The Tombros case is one of a handful of wireless hacking

## NATGUG News May June 2007

convictions federal prosecutors reeled in this year.

In June, a Maryland man with a grudge against a Connecticut-based patent firm pleaded guilty to using unsecured wireless networks at homes and businesses in the Washington D.C. area to penetrate the company's computers and deliver anonymous threats and extortion demands.

The same month, two Michigan men, Brian Salcedo and Adam Botbyl, pleaded guilty to conspiracy charges stemming from a scheme to steal credit card numbers from the Lowe's home improvement chain through an unsecured wi-fi network at a suburban Detroit store. A third man later pleaded guilty to a misdemeanor for using the same access point to check his e-mail."

Spamhaus is a company located in the United Kingdom. It offers an anti-spam service based on a database that collects information and evidence on known spammers and spam gangs, to assist ISP abuse desks and law enforcement agencies. Spamhaus states that approximately 200 spam operations account for 90% of all spam. The following information is found on the Spamhaus web site.

"90% of spam received by Internet users in North America and Europe can be traced via redirects, hosting locations of web sites, domains and aliases, to a hard-core group of around 200 known spam operations, almost all of whom are listed in the ROKSO database. These spam operations consist of an estimated 500-600 professional

spammers loosely grouped into gangs ("spam gangs"), the vast majority of whom are operating illegally, and who move from network to network seeking out Internet Service Providers ("ISPs") known for lax enforcing of anti-spam policies. These are the spammers you definitely do NOT want on your network.

Many of these spam operations pretend to operate 'offshore' using servers in Asia and South America to disguise the origin. Those who don't pretend to be 'offshore' pretend to be small ISPs themselves, claiming to their providers the spam is being sent not by them but by their non-existent 'customers'. Some set up as fake networks, pirate or fraudulently obtain large IP allocations from ARIN/RIPE and use routing tricks to simulate a network, fooling real ISPs into supplying them connectivity. When caught, almost all use the age old tactic of lying to each ISP long enough to buy a few weeks more of spamming and when terminated simply move on to the next ISP already set up and waiting."

Unfortunately there is nothing simple about modern spamming operations. Hopefully, the criminal prosecutions will continue until the spammers get the message.

John Brewer practices law in Oklahoma City, is a member of the Governor's and Legislative Task Force for E-Commerce, and enjoys issues relating to eBusiness and cyberspace. Comments and questions are welcome and can be emailed to [Johnb@jnbrewer.com](mailto:Johnb@jnbrewer.com).

# NATGUG News May June 2007

## **Hard Drive HouseKeeping Is Vital**

by Dennis Schulman  
Tampa Bay Computer Society

[This article is reprinted from the 2005 March issue of "SYDTRUG News", newsletter of SYDTRUG Inc., PO Box 75, PANANIA NSW 2213, AUSTRALIA, where it was brought to you by the Editorial Committee of the Association of Personal Computer User Groups (APCUG), an international organisation to which SYDTRUG Inc. belongs. There is no restriction against any non-profit group using this article as long as it is kept in context, with proper credit given to the author.]

For those of you who surf the net on a regular basis - and that includes those who use dialup access as well as cable or DSL - it is absolutely crucial that you take your hard drive housekeeping more seriously than you ever thought necessary. Many users think that by having a suite of utilities, such as Norton or McAfee, that you are protected. You might be, but I seriously doubt it for so many reasons I won't go into it now except for three:

You use auto update and auto scan. This requires that your computer be on-line at the time to run the auto update. In the case of cable or DSL, that is possible, but the computer has to be on at the time also. In the case of dialup, the computer won't go on-line unless your password is saved and used automatically. That, of course, defeats keeping friends and annoying children from messing up the computer without your knowledge. So, you might want to run your antivirus update manually, just to make certain it worked and there were no errors.

The second reason is based on the fact that if you did not clean house before scanning, you risk the possibility of the antivirus finding a virus it could not delete or quarantine and you did not know it. You also risk the possibility of not knowing if the auto update was not run successfully for one of many reasons (and time and space won't permit that discussion at this time) and consequently your subsequent full system auto scan may not be able to recognise the latest nasties you have managed to acquire.

There is a third, more obtuse, reason. If you don't really know if your system is truly clean and clear of all the bad stuff, how will you know what to do when you get a message that says something to the effect: "It has been determined that your computer has been sending messages infected with the \_\_\_\_\_ trojan horse virus to what appears to be the e-mail listing of your address book. If you do not take appropriate action immediately, your e-mail service will be discontinued. If your anti virus program has failed to protect you, please download the following trojan horse removal tool and run it immediately."

So, here is a housekeeping procedure I use - which is manual - because then I am more certain that I know the status of my files than most of the "suite" programs. And it doesn't use much - if any - of my system resources except when I use it. Just in case you think you have all the utilities you need, let me comment that I am not an expert on your system, but I spend more time now than ever before on systems that have too many over-burdensome utilities that are truly

## NATGUG News May June 2007

unnecessary and in some cases more dangerous than what they claimed to be designed to do. What I am proposing is basically using 3 little free utilities that only work when invoked, along with utilities that already come with your computer.

Run Disk Cleanup (under System Tools under Accessories on the Programs menu) and process all options (don't worry about compressed files, but do them at a later time when you have nothing else to do, since it could take quite a while if you haven't done it the first time.)

Clear your browser cache. In Internet Explorer go to Tools, Internet Options. Delete cookies and delete all off-line files. In Netscape Communicator go to Edit, Preferences, Advanced, Clear Memory Cache and Clear Disk Cache.

Open Windows Explorer (right-click on My Computer, select Explore), select the folders/View option and select show all files except system files. You can leave it this way. Find any folders called tmp, temp, or cookies. Unless you have a good working knowledge of what cookies you need or do not need, you probably don't need the contents of any of the temp, cookies, or temporary internet folders except the index.dat file (you might want to save the contents of the History folder)

Empty the Recycle Bin

Update and run the latest core version of Adaware SE Personal Edition (currently version 1.05). Once the scan is complete, click on

an object found, right-click a lined item and select all, click next and remove all.

Update and run the latest version of Spybot (currently version 1.3). Before running the scan, run immunise. Then run Look for Problems. Once problems are found, select them all and click on Fix Problems.

Note: Some spyware may be associated with programs you want to use, so read the help section for a further understanding of the features and options on both of these programs. These spyware objects detector utilities can be downloaded from [download.com](http://download.com) or [majorgeeks.com](http://majorgeeks.com).

There is a third utility, called a hijack remover. There are many available, but I like CWS shredder.exe (current version 2.00) (use [www.google.com](http://www.google.com) to find the program). Just make certain you are not on-line and that your browser is not open when you run it. You may be surprised and pleased if it finds something and fixes it (generally really bad stuff).

Now you should be able to update and run your antivirus more successfully than ever before. The only catch is that it takes time. Once you figure out about how much time each step takes, you can determine whether you can walk away and come back later when it is done.

I recommend running HouseKeeping at the end of every day you go on-line - if you can manage it. Otherwise, run it every 3 days for certain.

# NATGUG News May June 2007

Now, if you know your computer is clean and pure, then this is the only condition to justify running the defragmentation utility (once a week or twice a month). Defrag does not "fix" anything. It enhances the performance of a healthy environment. If you attempt to defrag a "sick" system, you could make it worse to the extent that the computer will fail to boot or run. If you have Windows 2000 or Windows XP, you can run defrag directly. If you have Windows Me, 98, or 95, run it in Safe Mode. I prefer running Defrag in Safe Mode as I have a UPS and the computer can complete the defrag, even if the lights go out in the house.

Now that you have successfully learned the housekeeping routine and understand its importance without the need for complex and sometimes dangerous free software utilities that can cause conflicts, you can set up the program scheduler to run your housekeeping routine for you and just check up on it from time to time to see that it is accomplishing your wishes.

Feel free to e-mail me for further details and other fine, free utilities available for keeping your hard drive and system performing at its best.

Dennis Schulman, known as the PC Miracle Man, has been a practicing field consultant in Largo, Florida for over 22 years. He has been a member of the Tampa Bay Computer Society for over 15 years and was the editor of its sometimes 40-page newsletter for 5 years. He can be contacted at [dschulman@myrapid sys.com](mailto:dschulman@myrapid sys.com).

## Tech News

by Sue Crane  
Big Bear Computer Club

[This article is reprinted from the 2005 April issue of "SYDTRUG News", newsletter of SYDTRUG Inc., PO Box 75, PANANIA NSW 2213, AUSTRALIA, where it was brought to you by the Editorial Committee of the Association of Personal Computer User Groups (APCUG), an international organisation to which SYDTRUG Inc. belongs. There is no restriction against any non-profit group using this article as long as it is kept in context, with proper credit given to the author.]

U.S. dictionary publisher Merriam-Webster says "blog" topped the list of most looked-up terms on its Web site during the last 12 months. The word will now appear in the 2005 print version of Merriam-Webster's dictionary, defined as "a Web site that contains an on-line personal journal with reflections, comments and often hyperlinks." However, Oxford University Press says "blog" is already included in some print versions of its Oxford English Dictionary and has entered mainstream usage. According to an Oxford University Press spokesman, "Now we're getting words that derive from it such as 'blogosphere' and so on." According to the Pew Internet & American Life project, a blog is created every 5.8 seconds, and blog analysis firm Technorati estimates that the number of blogs in existence now exceeds 4.8 million.

CDW, a national technology solutions provider recently announced that its Tech Twister technology makeover contest. The company's teaming up with IBM, Intel and Linksys to offer small businesses a chance to win a complete technology makeover. Tech Twister is open to any small

## NATGUG News May June 2007

business with five to 100 employees. Go to CDW's Web site and fill out the on-line application to enter the contest

[http://www.cdw.com/Webcontent/land/page/techtwister\\_110804.asp](http://www.cdw.com/Webcontent/land/page/techtwister_110804.asp).

All entries must be completed and received by 5pm PST on February 15, 2005. The winners will be chosen during the months of December 2004, January 2005 and February 2005.

In a sign that wearable technology is gaining greater acceptance, the Gap on Thursday introduced a fleece jacket with a built-in radio for kids. The Hoodio has a control keypad located on the sleeve and a hood that conceals the speakers. Xybernaut sells a wearable, 1.9-pound computer with an 8.4-inch touch screen. And MP3 players are now in sunglasses. Oakley's Thump line is available in seven combinations of lenses and colors. The shades have earphones and lenses that flip up and down. Meanwhile, NanoHorizons has developed socks containing silver and gold nanoparticles, which kill foot odor and bacteria.

NanoDynamics has come up with a golf ball that can correct its own flight path so it flies straighter than conventional balls. The design of the ball -- and the materials it's made of -- serve to better channel the energy received from the club head and thus correct a wobble or slight drift. The company believes the ball complies with the rules of the United States Golf Association. It will provide samples for testing and USGA approval in January or February. Earlier last year, Easton Sports announced it was developing a set of bike components made from carbon nanotubes that would be stronger

and lighter than conventional parts. And other companies have developed nano tennis balls that don't lose air and golf shafts constructed with nanomaterials.

During the string of hurricanes that hit the U.S. last summer, satellite phones were often the only reliable means of communication, because they use orbiting satellites rather than landlines and cell towers to transmit signals. "They cover such a broad area, I can use it anywhere," says one Iridium customer. "The call may get unclear, but if you wait about five or six seconds, it gets better. A cell phone would just drop the call."

Microsoft's new small business software gives you financial info at a glance. Looking to offer small businesses an integrated approach to accounting, contact management and general productivity, Microsoft announced that a beta version of its newly announced small business management product is now available for testing

Kawada Industries in Japan, has been putting the final touches on a large biped Robot that can do what no humanoid its size has done before: lie down, get up, and help a human carry light loads, like suitcases and briefcases.

Passwords will soon be a thing of the past according to Microsoft Chairman, Bill Gates. Gates predicted that people will soon rely on other ways of verifying their identity. "A major problem for identity systems is the weakness of passwords," Gates said. "Moving to biometric and smart cards is a

## NATGUG News May June 2007

wave that is coming, and we see our leading customers doing this."

Japanese electronics giant TDK has developed a tough new coating named Blu-ray that makes DVDs scratch-proof. In a test conducted by CNET News.com, a DVD treated with TDK's coating survived a determined attack with a screwdriver and a Sharpie permanent marker with no effect on playability.

Researchers at the Toho University School of Medicine in Tokyo have found that long hours spent in front of a computer screen may increase the risk of glaucoma in near-sighted people. The research is based on a study of 10,000 workers in Japan, with results correlated to data on how many hours were spent on the computer and pre-existing visual problems, such as myopia. Scientists said they believe the optic nerve in myopic people might be more vulnerable to computer-caused stress.

Watch for hefty increases in annual subscription rates for antivirus software as major Security companies encourage subscribers to upgrade to full Internet Security Suites which include firewall, anti-spam and anti-spyware as well as anti-virus.

Cyber Terrorism - A Portent of Things to Come

by Ira Wilsker  
Golden Triangle PC Club

[Reprinted from the 2005 April issue of "SYDTRUG News", newsletter of SYDTRUG Inc., PO

Box 75, PANANIA NSW 2213, AUSTRALIA, where it was reprinted from the 2004 November issue of "The Voice of FCUG", newsletter of the Fairfield County Computer Users Group Inc., 280 Main Street, Westport CT 06880-2408, U S of A, where it was reprinted from the 2003 September issue of "Bits & Bytes", newsletter of the Tampa Bay Computer Society, where it was a reprint of an article supplied by the Editorial Committee of the Association of Personal Computer User Groups (APCUG), an international organisation to which SYDTRUG Inc. belongs. There is no restriction against any non-profit group using this article as long as it is kept in context, with proper credit given to the author.]

This week is a more serious column than is typical for me. As I type this, the news is heavy with warnings of terrorism and terrorist attacks. While the news is emphasising possible attacks on our physical infrastructure, including business, government and transportation, there has been almost nothing published in the mass media about another potentially devastating terror attack: an assault on our cyber and electronic infrastructure. To those involved with cyber security this is not news, but something we have been trying to train and prepare for, as well as inform others of the risks, so that they can also prepare, and harden, their systems.

According to Dr. Magnus Ranstorp, the Director of the Centre for the Study of Terrorism and Political Violence at the University of St. Andrews, Scotland, and a CNN consultant, Al Qaeda is very

## NATGUG News May June 2007

involved in the use of computers and the Internet to promote its cause. In his published report "Al Qaeda in Cyberspace: terrorism challenges in the information era" he describes some of Al Qaeda's cyber activities. Al Qaeda uses the Internet as one of its primary methods of communication, recruitment, mobilisation, and propaganda. It is also used for theological teaching, and hidden communication between its covert cells. It is well known in security circles that Al Qaeda uses the free e-mail services of Yahoo and Microsoft's Hotmail to communicate using a variety of innocuous user names, and apparently non-sensitive e-mails. Al Qaeda uses common vernacular as disguised code words, often with prearranged meanings, as well as the practice of "steganography", or hiding messages in plain sight, typically in an image that would not otherwise attract any attention. By remaining in open sight, and without any unusual content that would attract attention, Al Qaeda can exchange information that is nearly impossible to identify in a timely fashion.

According to John Hamre, Deputy Secretary of Defense under President Clinton, many of the notebook computers belonging to Al Qaeda operatives captured or otherwise seized, had significant information about the programming and operation of "supervisory control and data acquisition" (SCADA) systems commonly used in industry to control electrical, pipeline, refinery, power company, and other automated systems. By cracking into these often underprotected systems, a potential terrorist can effectively

take control of those systems. The implications of this vulnerability are enormous, and the potential for economic and other damage is incalculable.

Osama bin Laden is no stranger to computer security, and is personally well educated and experienced in dealing with computer security issues. He is reported to have [created] a hacker school involving the faculty in the electronics department during his university education. He was also instrumental in creating a "cyber university" in Pakistan with an emphasis on SCADA systems controlling water utilities, pipelines, nuclear power plants and dams, according to John Hamre.

The infamous terrorist group Hezbollah also has contemporary information and the talents and abilities to launch electronic attacks against the soft American and European infrastructure; Israeli infrastructure has already been hardened, making such attacks there much more difficult by Hezbollah, according to Dr. Ranstorp. He also states that Al Qaeda will likely coordinate a cyber attack with a conventional terrorist attack, enhancing the economic damage and resulting in crippling losses.

Professor Yonah Alexander, director of International Center for Terrorism Studies, a recognised leading expert on terrorism, stated "We can expect to see an escalation in terrorism on a global scale with a continuation of conventional acts of terror". There will also be a move towards the use of non-conventional weapons "and cyber-terrorism, whereby

# NATGUG News May June 2007

perpetrators will try to disrupt power supplies and air traffic, for example, at the touch of a button."

I am not disclosing anything here that is not already well known in security circles, and that has not already been widely disseminated on the Internet and in written form in the various Al Qaeda and other terrorist training manuals.

We as businesses, government, consumers and citizens, need to be aware of the threats we face to our sensitive and often "soft target" infrastructure, and take necessary and appropriate steps to harden our systems. From an individual's viewpoint, we must all be certain to have current and frequently updated antivirus, firewall, and anti-spyware software installed on our computers, and verify that it is properly functioning. Our personal computers can be taken over by zombies placed on our machines by viruses and trojans, and used to launch "distributed denial of service" (DDOS) attacks, where millions of computers simultaneously launch an attack against countless servers, web sites, governmental entities, and other such facilities, effectively shutting them down. Similar attacks can also be launched from personal computers against some of the SCADA systems controlling our vital systems.

Information on protecting our systems is readily available and often free on the Internet. There are many web sites [discussing] the so-called "info war" and what we can do about it. One excellent site is the British Information Warfare site at <[www.iwar.org.uk](http://www.iwar.org.uk)>, which has hundreds of links to American,

Australian, British, Canadian, and other resources, including many free government-produced booklets, and information from private businesses and other organisations. The left column on the site has a directory of topics that covers these critical areas, ranging from home computer security, to hardening corporate SCADA systems.

Regardless of our personal political beliefs, it appears that terrorism is a fact, and cyber terrorism is a very real threat. Using a now common cliché, it is not a matter of "if", but a matter of "when".

## Index

|   |         |
|---|---------|
| Editorial                                       | Page 3  |
| Ergonomics for the Elderly                      | Page 3  |
| Protection Against Virus Attacks                | Page 4  |
| Legal Bytes: It's the Slammer for the Spammer ! | Page 7  |
| Hard Drive House Keeping Is Vital               | Page 10 |
| Tech News                                       | Page 12 |
| Cyber Terrorism – A Portent of Things to Come   | Page 14 |