BAY BYTES

Greater Tampa Bay Personal Computer User Group, Inc.

Newsletter

Issue 1 | January 2013 | 26th Year of People Helping People!

In this Issue

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/

What will happen to Windows XP

zdnet.com

There are just 500 days left until Microsoft officially terminates all support for the incredibly popular Windows XP operating system (OS).

When it happens, the event will mark a major transition for the software giant, and could present big problems for the half billion computers still running the aging OS.

Once these 500 days come to an end, Windows XP will no longer be updated or have any security vulnerabilities patched by the Microsoft development team. Over time, that will tend to make the operating system highly vulnerable to hacker attack.

You can think of this 'end to upgrades' much the same as your home security company announcing to the world that it was disabling your alarm.

One Million Upgrades Per Day Required

If current XP users are to remain under the umbrella of Microsoft upgrades and security patches, approximately one million of them will need to upgrade to Windows 7 or Windows 8 each and every day for the next 500 days.

Many experts see that as unlikely to happen, and worry that so many computers being left unsupported could result in the biggest security scare in a generation or more.

The biggest threat is posed to the enterprise crowd, including private businesses and public agencies that have refused to move ahead from Windows XP.

They will need to sign up for Microsoft's 'Software Assurance for Volume Licensing' program soon, or risk putting their users' information at risk.

Continued on page 12

Why shouldn't I post my email address in a public forum?

Spammers harvest email via a variety of means. One of the most common is to simply surf the web and look for anything that might be an email address.
So many discussion forums and technical assistance sites, including yours, ask for an email address to post comments, and yet friends tell me never to put my real address in.
Sometimes I need to include my email address as part of my comment or question, but I'm told that's even worse! Why is that, and what should I do?

The why is easy.

The what to do? Not so much.

Why is it a bad idea? In a word, spam.

Anything that will put your email address on to a publicly accessible web page will, in all likelihood, cause you to start getting more and more and more and more spam. Why? Because one technique that spammers use is to visit all the web pages that they can, and collect anything that looks like an email address to add to their mailing list.

Here's an example: muchspam@ask-leo.com - now that I've published that email address on the web on this page, even though it's the *only* place that email address has or will be officially mentioned, it will now start getting spammed.1 Just because it was published on a web page, and it looks like a valid email address.

So when you include your email address in an on-line posting - say on a discussion board, or even in a comment here on Ask Leo!, you're almost literally *asking* for spam.

Don't do it.

In my case, you'll notice that in order to post a comment on Ask Leo!, you're required to provide an email address. But notice also, that that email address is *not* published on the web page (in my case, if you use a valid email address, it's simply a way for me to follow up with you directly should I have a question about your comment). But *be careful* - not all weblogs and discussion forums hide your email address. Many turn right around and put it on the web page for all to see. Including the spammers.
Before you post *anywhere* be sure you know what's going to happen to your email address when you do. Are you a member of a mailing list? Does that mailing list have an on-line archive? Then your email address *may* be available to the spammers for harvesting. Ever post on Usenet? The email you used is probably already in the spammer's lists. An early Usenet post "before I knew better" is the reason my wife gets hundreds of spam per day.

So use a fake address - or better yet, don't use one at all.

Continued on the next page

Now, what if you *need* to post your email address in a publicly accessible place? There are several techniques for obfuscating the address. Here are a couple of my favorites:

askleo *at* gmail.com
askleo@gmail.seeohem

The first you've probably seen already in other places. It simply requires that you, as a human, realize that the " at " needs to be replaced with "@". My fear is that this technique is also fairly easy to decode by computer, and the spammers will soon catch on.

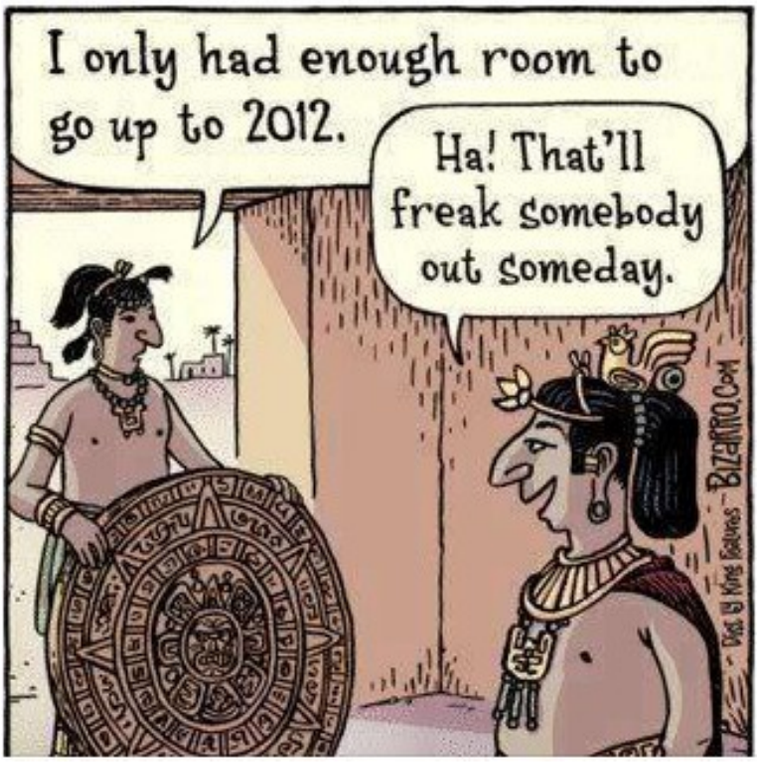
The second requires some thought. If you sound out "seeohem", you'll realize that it sounds like c, o, m. "com". Hence you realize that the ".seeohem" really means ".com" and can make that translation when you type in the email address.

The biggest drawback to these approaches is that the email links are not clickable. Anything you can click on to get an email address, the spammers can use to harvest it. Even copy-paste doesn't work, for exactly the same reason.

But protecting yourself from spam is important. And not asking for more, is even more important.

1: A check in 2012 shows this address is indeed still regularly getting spam. Even though it was mentioned exactly once, only here.

Comments & updates at: Why shouldn't I post my email address in a public forum?



A newly-unveiled password-cracking system can reportedly guess billions of unique passwords every second. At that rate, it's entirely practical to have the device attempt every possible eight-character Windows password.

The password-cracking system is a Linux-based graphical processing unit (GPU) 'cluster' that uses a special type of virtualization software which allows it to use not one, not two, but 25 Advanced Micro Devices (AMD) Radeon graphics cards.

350 Billion Passwords Guessed Each Second

That kind of GPU power enables the cluster to guess passwords at an astonishing rate: 350 billion passwords per second. That's roughly four times faster than once thought possible.

In fact, experts estimate the device could actually guess every eight-character password, including those containing combinations of letters, symbols, and numbers, in just five-and-a-half hours. (Source: cnet.com)

This method of simply guessing computer passwords is known by security experts and hackers alike as "brute forcing".

In the past, brute forcing of passwords was possible, but not practical because it would have taken years or even decades to run through all the possible passwords.

Thankfully, hackers are not the ones who have developed this device. Instead, it's the work of Stricture Consulting Group, a security firm specializing in password cracking.

Stricture's chief executive officer, Jeremi Gosney, unveiled the cluster at last week's "Passwords^12" conference in Oslo, Norway. (Source: arstechnica.com) Although it's unlikely hackers have a tool like this at their disposal, Gosney and other security experts believe people with criminal intentions could develop similar devices in the future.

Experts: It's Time for Longer, More Complex Passwords

According to Gosney, the advent of this password-cracking cluster gives a signal that everyone should start thinking about developing much longer and more complicated passwords.

Infosecurity, an online security magazine, insists that eight-character passwords "are no longer sufficient," and that only by using longer passwords including both letters and numbers will people "help prevent brute forcing." (Source:nbcnews.com)

Where possible, security experts like Kaspersky Lab's Dmitry Bestuzhev suggest using a much longer combination of letters, numbers, and symbols to construct passwords. Furthermore, Internet users should refrain from using the same password more than once.

Sophos Labs security expert Paul Ducklin sees the cluster's unveiling as "yet another reminder that security is an arms race." For the average Internet user, winning that arms race requires taking password construction more seriously. (Source: nbcnews.com)

Restoring Your Computer with Windows System Restore

One of the features that was introduced into Windows as of Windows XP is an invaluable resource called System Restore.

We've all seen the program installations that flash a message that they're creating a Restore Point. Windows makes a Restore Point whenever you install a new driver. It also makes a restore point periodically based on elapsed time.

While System Restore and its Restore Points do not protect data files, it protects Windows' system files and the Windows Registry. That way, if you install something that totally messes up Windows, whether it's a new program or drivers for new hardware, you can easily restore Windows to the way was recently (as long as you have not turned off System Restore). However, Windows does a good job of hiding the tool for actually using those restore points.

The route to find the System Restore tool is:

Start > All Programs > Accessories > System Tools > System Restore.

After we click the Next button at the bottom of this introductory window, we get the following dialog box. This is where you will set all your options to use a Restore Point.

The first thing to note is that three restore points are displayed. By default, only the latest restore point is shown.
To show all the restore points (three in this case) put a check in the checkbox that says Show more restore points.
A button on the right-hand side, Under the listing of available Restore Points, allows you to check to see which programs will be affected by the rollback to that Restore Point.

Affected programs may have to be uninstalled and re-installed. For Windows itself, you'll have to run Windows Update again to get those system updates (since you will have restored the original files). When you have selected the Restore Point that you want to use, click the Next button.

This dialog box gives you one more chance to decide whether or not you want to run the System Restore with that Restore Point.

Fortunately, Windows will make a Restore Point just before the restoration. That way, if it doesn't work, you can restore back to where you were (and try to solve the problem some other way)

Windows Defender is just a new name for Microsoft's well-known and free software: Security Essentials. One of the best new security features in Windows 8 is that the operating system will enable Windows Defender whenever it fails to detect some other antivirus program.

Windows Defender in Windows 8: OEMs Cry Foul

pcworld.com

Microsoft's decision to include Windows Defender in Windows 8 has aroused lots of anger among computer manufacturers, who are paid hefty sums by antivirus companies in exchange for installing trial versions of their software on the manufacturers' new PCs.

In order to keep manufacturers (or 'OEMs') happy, Microsoft allows them to disable Windows Defender in order to install their trial-version antivirus software.

However, there is a problem with this approach: if a third-party antivirus program (from companies like McAfee, Symantec, or Kaspersky Lab) trial subscription runs out, Windows Defender may not automatically see the lapse of computer protection and jump into action.

And that will leave your PC vulnerable to viruses and malware.

How to Activate Windows Defender

Fortunately, you can manually activate Windows Defender after a trial antivirus software package has expired.

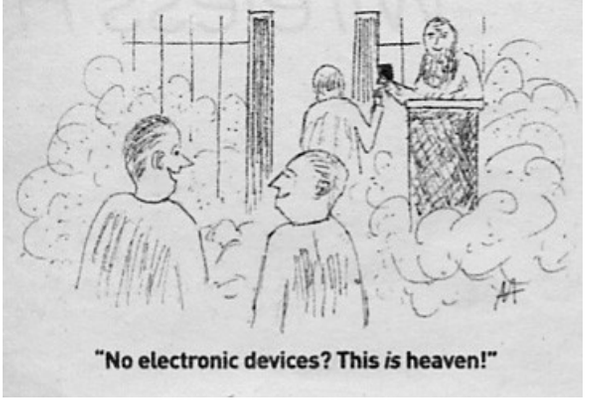
To do this, first go to Windows 8's new Start screen and type in the command 'Windows Defender' (no quotations).

When the Windows Defender icon appears, click on it.

If Windows Defender is disabled, you'll be warned that Windows is "At risk" with a big red 'X'.

To enable Windows Defender, go to the Settings tab at the top of the Windows Defender window. Select and enable 'Real-time protection' and then click 'Save Changes.'

If the "At risk" warning is no longer visible, you know Windows Defender is working properly.
Once Windows Defender is activated, you can immediately run a system scan by clicking 'Scan Now.'
However, it's recommended that users first download the latest Windows Defender protection tools by clicking the 'Update' tab.



Is Your Internet Security up to Date?

Antivirus up to date?

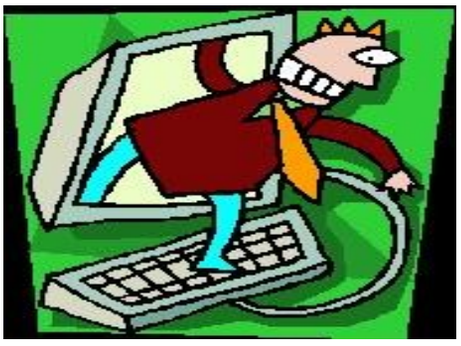
Firewall?

Windows up to date?

Spy Ware?

See how to protect your computer at:

http://gtbpcug.org/protect/



More about Internet Threats… *and about other Malware, Spam and Users beware*

User beware

From a member

Remember the ink jet printer scam of a few short years ago, where you had to purchase the original printer manufacturers replacement ink cartridges? That's because the printer manufacturer imbedded proprietary circuitry in their ink cartridges and printers. If the replacement cartridges you purchased did not have the circuitry imbedded, the printer would not work.

Well, fast forward to today. Some laptop manufacturers now include proprietary identification circuitry in their battery packs; the laptop won't charge the replacement batteries unless it sees this special identification circuitry. HP is one company that apparently is using the proprietary circuitry. I'm sure other companies will follow suit. That means instead of buying a 3rd party replacement battery for about $30, you will need to purchase the original manufacturers replacement battery for more than $100. If you are planning on purchasing a new or used laptop, suggest checking this out.

That famous Latin phrase comes to mind: caveat emptor (let the buyer beware).

Online or Local Backup: Which is Best?

When it comes to backups, you have two fundamental choices: local or online backup. Local means making backup copies on removable or external media that you keep nearby. With online backup, you're transferring your files over the Internet to a remote server. Here are the pros and cons for online backup, local backups, and two things you MUST back up, in addition to your hard drive…

The Best Way to Back Up Your Files

http://askbobrankin.com

There are trade-offs when considering online backup or a do-it-yourself approach in your home or office. Local backup is secure while you are doing it. When you copy data from your computer to a DVD, a flash drive, or an external hard drive, no one else can steal it. Local backup is faster than online backup, because your Internet connection is not nearly as fast as your backup drive's data transfer rate. The initial full backup with an online backup service Mozy or Carbonite can take days or weeks, depending on how much data you have, and the speed of your Internet connection.

The downside of local backup is mainly before and after the actual backup process. Adhering to a regimen of regular, orderly backup sessions is hard for many people. Keeping multiple backup sets adds clutter and work. If you backup on DVDs, you have to swap discs, label them, put them in protective sleeves, and find someplace safe to store them. And if you use an external hard drive, should you have more than one backup image?
When you need to restore data from backup copies, there is the problem of remembering where the right discs are. And there's always the question of what happens in the event of a fire or flood. Keeping your backup media in a fire-proof safe is a good idea, but safes can be stolen. If you keep your backup copies in a safety deposit box or an off-site location, the time and hassle of retrieving them can be significant.

One good strategy is to make backups to a set of external hard drives. One stays connected to the computer for automatic daily backups, and one stays in a fire-proof safe. Once a month, you swap them. This way, you always have a complete, up-to-the minute backup, and another one that's safely stored away and at most a month old. If you need help getting started with a local backup system, see my related article Free Backup Software.

What About Online Backups?

Online backup services eliminate many of these hassles. You can configure backup sessions to run when your computer is otherwise idle, and backups will be made even if you forget about them. When you need to restore selected data, a Web interface helps you find the right backup copy and choose just the file(s) you want to restore. What's not to like about online backup?

Cost is the first downside of online backup. Most online backup solutions give you a few gigabytes of backup storage space for free to get you to try them. But for a complete system backup, five gigabytes or even ten is often not enough.

Continued on the next page

Then you have to pay monthly storage fees which can range from ten dollars upward.

Security is another big concern. But I'd argue that the online servers used to store copies of your files are MORE secure than the typical home or office environment. Online backup services employ strong encryption, 24/7 physical security, and have plans to protect against fire, flood and other natural disasters. They're also certified and audited by independent agencies. Chances are, the computer in your home is much more vulnerable. See my related article Are Online Backup Services Safe? for a more complete discussion on how online backup providers keep your data safe.

Speed is another consideration. The online backup process can run while you are asleep, but when you need to restore data you usually want it in a hurry. Even if you subscribe to the fastest broadband service available, Internet traffic jams can slow your online backup and restore sessions to a crawl. And if you need to restore a full backup, the sheer volume of data will make this a lengthy affair.

CrashPlan is an online backup service that helps you avoid the long wait times when making your initial backup, or if you need to do a full restore. They'll send you an external hard drive for your first backup. After you mail it back, all your backups are incremental, over the Internet. And if you need to restore an entire disk (or just a lot of data) you can use CrashPlan's "Restore to Your Door" service, and have your backup drive mailed to you.

Some online backup services to try include Mozy, Carbonite, iDrive, and CrashPlan. Check out my article comparing these offerings in Carbonite, Mozy, or Crashplan? Then try one or more, taking advantage of their free storage allowances, until you find one that suits your needs.

My Backup Strategy, and Other Considerations

Personally, I use a hybrid approach which combines both local backups and online backup. Using external hard drives, I make a full backup weekly, with daily incremental. I then make separate backups of selected important files and folders. And I also backup my backup, so it's never just in place. That's where the online backup component of my strategy comes into play. You can read more about how I do all this in Save Your Bacon With Acronis True Image Backup.

Oh, and don't forget that your hard drive is just one part of the backup task. Your webmail, social media accounts, and everything on your mobile phone needs protection, too. See Have You Backed Up Your Online Accounts? and How to Backup Your Smartphone for help completing your backup strategy.

Got something to say about backup options? Post your comment or question below…

Read more: http://askbobrankin.com/online_or_local_backup_which_is_best.html#ixzz284NDY2E6

The lighter side

USB Problems with Windows XP

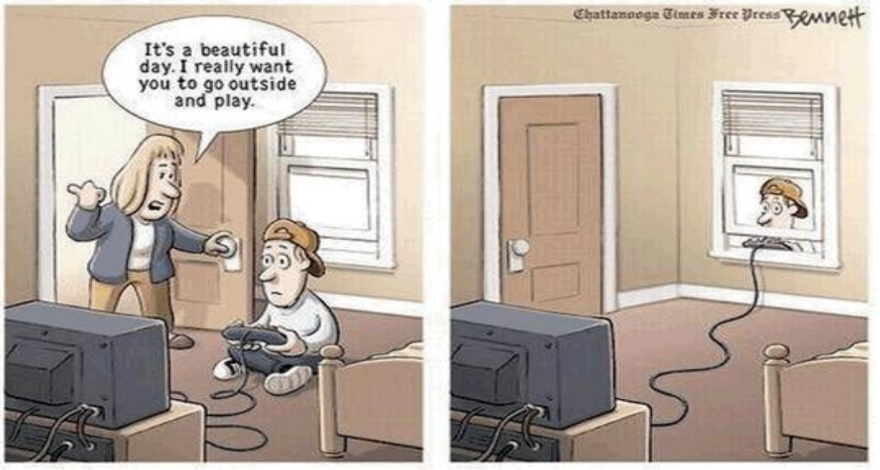
http://www.terryscomputertips.com/

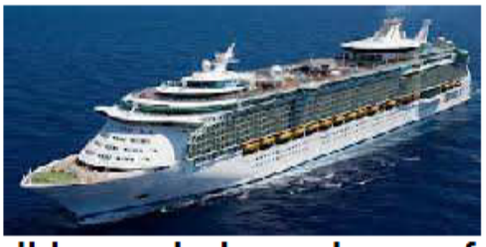
Long-time subscriber Dave Volente wrote with a question about USB and Windows XP issues he was experiencing:

> *Hi Terry.*
> *I'm still running good old XP Home on my two desktops and Pro on my laptop, all "networked" and everything shared in front of me on the same desk. Have numerous USB items (back-up drives, card readers, webcam, etc), so many, in fact that I also have loads of powered hubs to run them all. However, I've never had much luck with reliability as far as USB is concerned on ANY of the machines.*
> *External drives regularly vanish while transferring data for back-up (errors like "cannot find file", etc. — especially between machines, it seems). Items seem very fussy about where they're plugged in and are often not recognized or come up as "unknown device".*
> *When the drives re-appear at random (sometimes with the wrong drive letter), their properties (such as sharing and system restore, that I normally leave off on external drives) have been altered. A Google with "unreliable USB" seems to throw up folk with much the same problems.*
> *Is there an ultimate answer to this USB hassle? It has never seemed a very robust way of running peripherals to me!*

I wrote back to David to give him some consoling thoughts. David is experiencing one of the non-joys of the way Windows XP handles USB connections.

Windows XP installs drivers on a USB port by USB port basis. If you connect a device to one port and install the USB drivers, that port will already be set up the next time you plug the USB device into it.
The problem comes when you plug the USB device into a different port the next time. Windows XP isn't smart enough to adjust by itself. When you plug the device into a different USB port, it will install drivers for that port.
When you have a bunch of USB powered hubs and plug/unplug USB devices routinely, you have to remember which USB port you're using for a specific device and use that port. Or, alternatively, you can put up with Windows thinking it's a new device each time you plug it into a different USB port.





Royal Caribbean - Independence of the Seas

Saturday, December 7, 2013 - Sunday, December 15, 2013

The Florida Association of Computer User Groups (FACUG) is presenting its Fourth Technology Conference@Sea

There is no better vacation bargain than a cruise and no better cruise bargain than this one. Add to it a full-fledged Computer and Technology Conference on the high seas and it becomes an outstanding event not to be missed. Be a part of FACUG's fourth annual Conference@Sea on what promises to be another outstanding SAIL-A-BRATION!

The amazing bargain cost of the 9-day/8-night cruise starts at $579.67/person + tips including the FACUG $75 early-bird incentive refund. The FACUG Technology Conference will be on the Royal Caribbean Independence of the Seas; sailing on Saturday, December 7 to Sunday, December 15, 2013. FACUG is doing the work so we can offer this outstanding rate and amenities to you. See the Royal Caribbean website (www.rccl.com) for more information about the ship. Cabin rates are below (pp/double occupancy).

Cabin	# Cabins	Cruise minus $75 E/B refund	+ Port Charges	+ Taxes & fees	= Total/person
Interior N	17	$268	$200	$111.67	$579.67
Interior M	21	$277	$200	$111.67	$588.67
Interior L	42	$285	$200	$111.67	$596.67
Atrium PR	47	$311	$200	$111.67	$622.67
Interior K	48	$404	$200	$111.67	$715.67
Oceanview H	4	$379	$200	$111.67	$690.67
Oceanview G	5	$514	$200	$111.67	$825.67
Balcony E1	15	$744	$200	$111.67	$1,055.67

Pre-paid gratuities $93.20/person and travel insurance $59/person ($89/balcony) are additional.

Sailing from Fort Lauderdale, calling on Philipsburg, St. Maarten; Basseterre, St Kitts; San Juan, Puerto Rico and Labadee, Haiti then returning to Fort Lauderdale. This offer is valid for a limited time only. The Technology Conference@ Sea registration fee is $95/person for members of a FACUG or APCUG club ($120 for non-members) and also $95 for the second person in the cabin who need not be a club member. The early-bird refund is $75 per conference attendee.

Included in the conference fee are many extra perks including a Welcome Bag full of goodies, two Meet & Greet cocktail parties which are a big hit every year and a few additional surprises.
The $250/person cruise deposit is completely refundable until September 7, 2013 when the balance is due.

There will be buses from several locations around Palm Beach County to the Port of Fort Lauderdale and back for about $15/person each way. We will look into buses from other points in Florida if there is sufficient demand. Last January we did 200+ occupied cabins with 400+ people. After the cruise, a survey was taken and 3/4 of the responders, including spouses, rated the event an "A". It was called a great balance between conference time and party time. Ask your friends who were there. If you are interested in sailing with us at the above early-bird rates, you first need to register for the conference by following the directions below and then book your cruise with the booking agent noted on the other page.

I am including my $190/couple ($95/single) conference registration check refundable until June 1, 2013.

Please fill out the following form and place it into an envelope with your check. Mail to:

John Witmer; FACUG Treasurer, 3312 Sheehan Drive, Land O' Lakes, FL 34638-8036.

Once this is done, send an email containing the completed information below to president@facug.org with a cc to treasurer@facug.org to time-stamp your submission, since Royal Caribbean has limited our number of attendees.

Then call booking agent Dean Leblanc (866-606-2067) to book your cruise.

DATE: _____ COMPUTER & TECHNOLOGY CLUB: _____

NAMES OF BOTH PEOPLE: _____

EMAILS: _____ PHONE #: _____

Check #_____ Amount _____ - 2013 FACUG CONFERENCE CRUISE

For more cruise information, call booking agent Dean LeBlanc at Cruise Buyers Choice toll-free: 866-606-2067.

For more conference information, email facugcruise@ariesmart.com.

Continuation from page 1

Upgrades to Boost Microsoft Business

The countdown to the end of XP support should prove beneficial to Microsoft, which can assume that at least a large portion of the 500 million Windows XP users will pay to upgrade to Windows 7 or the brand new Windows 8.

Observers expect that most enterprise users will go for Windows 7, and that many home consumers will opt for Windows 8. (Source: thenextweb.com)

So, why have these users waited so long to upgrade?
Many users remain attached to Windows XP. For the enterprise crowd, upgrading is an incredibly expensive process. Not only do organizations need to purchase new Windows licenses, but they must also train employees to use the new OS.

That takes lots of time and can become a major drain on productivity. Microsoft has played into these decisions to put off operating system upgrades by repeatedly delaying its termination of support for Windows XP.
But this time observers believe the extended lifeline will finally reach its limit.

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