BAY BYTES

Greater Tampa Bay Personal Computer User Group, Inc.

Newsletter

Issue 6 | June 2013 | 27th 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/

...most people are security aware, but not so security savvy!

http://www.pctools.com

The results of PC Tools global survey of 4500 users are in! While consumers are aware of potential sources of infection, 74% of people are not aware of the need for behavioural based protection against online threats.

This leaves them at risk from new and unknown threats on social networking sites, instant messaging services and other online communication and networking tools. As many as one in five do not understand the potential impact of some of the more dangerous attacks like zero day threats, while 41% of respondents use only one or two passwords across all the sites they visit online and 8% use only one password for all sites, suggesting respondents are not so security savvy!

On the other hand, research showed that a significant proportion of people are aware of the need for some level of security protection for their PCs with 57% saying that they have a security suite installed and 64% having their security software configured to update automatically as new information becomes available. A savvy 84% will always take action when they receive a security alert from the software they've installed, while 37% will verify a received link before following it...great work people!

While it's promising to see that most respondents are security aware and have installed security products on their PCs, it seems users may be bloating their systems by installing too many security solutions.

Stop Facebook from infecting your computer

http://www.komando.com

If there's one guarantee on the Internet, it's that there will be no shortage of security concerns on Facebook. Facebook invades your privacy, uses you in ads, misuses your Likes and could cost you your job. That's only counting threats from Facebook itself!

Since it has more than a billion members, it only makes sense that hackers and scammers would target Facebook. People spend hours on the site and reveal all sorts of private information. That only makes a criminal's job easier.

Based on information you've probably posted, a scammer could steal your bank information. They could even recreate your Social Security number or load your computer with a nasty virus. These are the dangers you face every time you log into Facebook.

It's unlikely that you want to close your Facebook account. That's fine, because you don't have to. You just need to know what to look out for to stay safe when you're using the site. I know a few ways to have all the fun with none of the security risks.

It goes without saying that you should double- and triple-check your Facebook privacy settings. Make sure you haven't missed any. One crack in your security can lead to a hacker unraveling everything.

Security software can help, too, if you accidentally click on a scam link. You'll find plenty of free options for that in my security center. These can catch a virus before it becomes a major problem on your computer.

It won't catch everything, though. You have to be vigilant and know exactly what scams to watch out for. There are sites like Snopes and Facecrooks that will show you some. Every Facebook user should read my roundup of the most popular Facebook scams, too.

There are even some third-party apps that scan your profile for scams. Social Media Scanner made by anti-virus company ESET, is a powerful one to try.

None of these will protect you if you're not using Facebook safely, though.

For starters, be careful what you post and what you look at on Facebook. Never post your full date of birth, address, phone number or any other revealing things about your life. Make sure your friends aren't posting that information, as well.

Speaking of your Facebook friends, don't assume everything they post is safe. They could be a victim of a scam or could have been duped. If you see a questionable post by them, ask them if they posted it. They may not even know it's there.

Try to ask them in person, if you can. Hackers taking over an account and posing as someone else isn't unheard of. If you ask them over Facebook while a hacker is in control of their account, you could be inviting trouble.

Would you know what do if a hacker took over your account? With a cool head and the right knowledge, you can take it back and stop it from happening again.

A data breach from a company you do business with could end in a hacked account. Here are a few easy ways to get your hacked account back.

If you use the same password on multiple accounts, those are all at risk. Create secure, easy-to-remember passwords for every account you use.

Hackers aren't afraid to use your information to try to steal your identity. Protect your ID from hackers and scammers without paying a dime.

See more at: http://www.komando.com/tips/index.aspx?id=13976

How to Test Internet Speed

with Charlie McKeague

Testing your internet speed can reveal whether your connection is capable of playing videos and games at top quality. Watch this About.com video to learn how to test internet speed.

Transcript: How to Test Internet Speed

Today I'll be showing you how to test your Internet connection speed.

Why Is Internet Speed Important?

If you're browsing the web and pages take a while to load, or a video you want to watch has trouble playing, your Internet speed could be the cause. You can test your bandwidth though by using free websites. These sites allow you to see if your connection matches up to what your Internet service provider promised you.

Speedtest.net Can Test Internet Speed

A free and trusted site is Speedtest.net. Simply load the site, and click the Begin Test button. Once this is clicked you'll get three results. Your ping speed, your download speed, and your upload speed. It's a good idea to test twice, or three times for best results. Your will likely end up with different results each time as activity on your network can influence your speed. The Speedtest results give you a general idea of what your connection speed is at the time. Ookla is the company behind Speedtest.net and most of the other testing services as well.

Test Internet Speed With Your ISP

Another way to go about testing is to check your connection with your service provider.
Your provider likely uses Ookla as well. The PC Support guide for About.com has the major providers listed, you can go there to find your provider and your connection speed between it.

Use a Consumer Broadband Test to Test Internet Speed

The U.S. government also has a test you can use by going to Broadband.gov.
Click on "Consumer Resources" and then on "Consumer Broadband Test". You'll have to fill out some information about where you are testing from first. This test is also provided by Ookla, and you'll need Java to run it. Once you enter your information you'll be able to begin a test. When you're done with your Ookla test you'll be asked if you'd also like to be tested by M-Lab. Try this too.

These tests are a great way for you to keep an eye on your connection speed, and they're easy and free. Remember though if you're downloading or uploading something you're bandwidth will be affected, so it's best to test when there's minimal activity on your network.

http://compnetworking.about.com/od/speedtests/Speed_Test_Internet_Network_Connection_Speed.htm

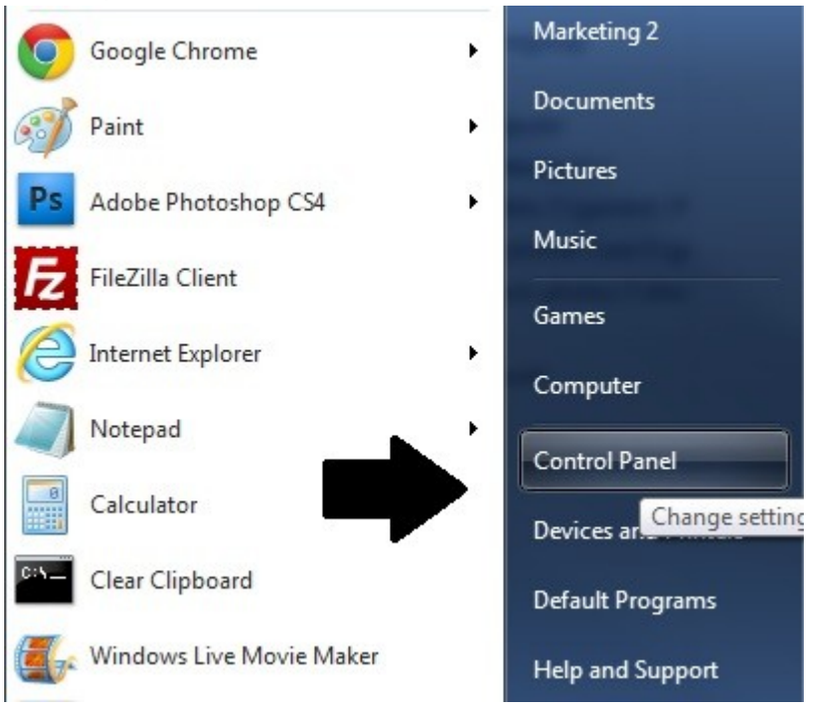
Another well known speed test site is http://www.speakeasy.net *and select Atlanta as a location.*

Editor

Making Windows 7 Easier To Read

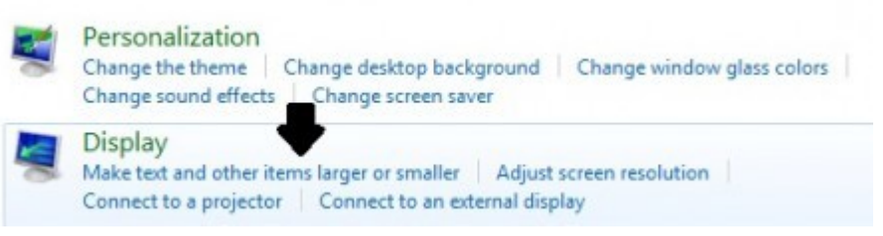
http://www.about.com

If you're finding it difficult to read things on your computer because they look too darn small on your screen, there's a quick way to make things easier to see in Windows 7. Open the Start Menu in the lower left and select **Control Panel**.



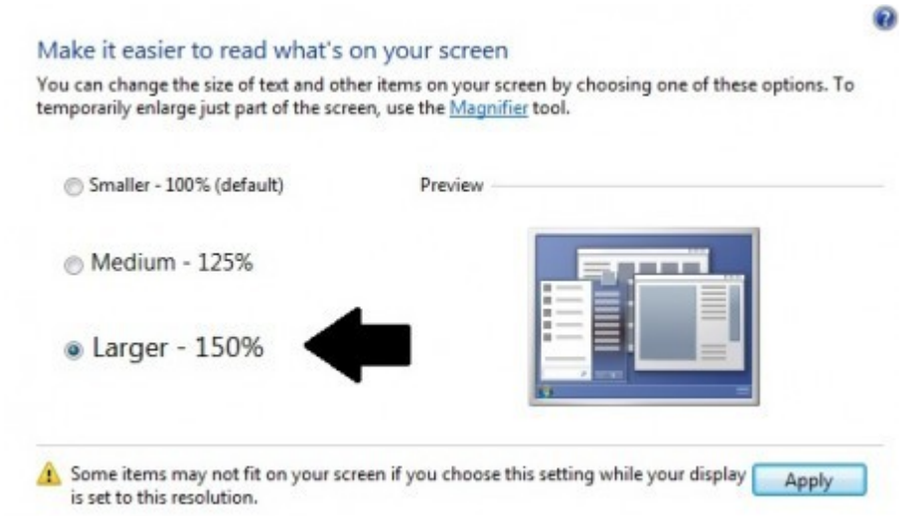
Then choose **Appearance** and **Personalization**.

Select the option to **Make text and other items smaller or larger**.

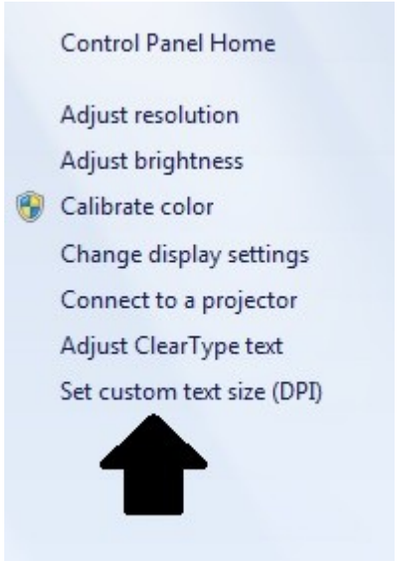


You'll have the option to decide how much larger you would like to make things. Making text larger can affect the display of some items. You might have difficulty getting everything to fit on a page.

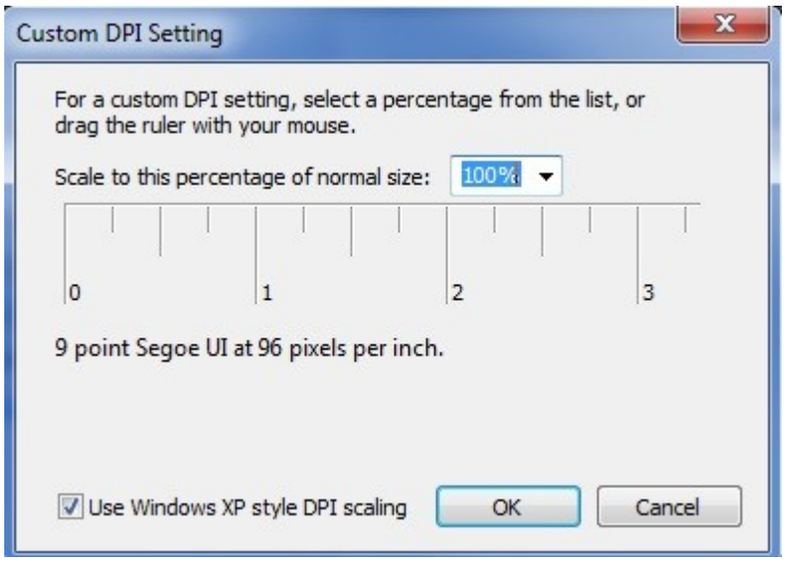
Continued on the next page



You can choose from the presets of 125% or 150%. This is how text would appear at the default setting of 100%.



You can select a size from the drop-down menu or drag your mouse along the ruler.



You will need to shut all of your programs and log off Windows for the changes to take effect.
Hope this makes things a little easier on the eyes. If you find you don't like the larger display, just follow the steps again and change the setting back to 100%.

Getting your data off a dead laptop

http://www.komando.com

Q: I just had an old laptop pass away. It wasn't a surprise. I'm pretty sure the hard drive is still good. I would like to transfer the data from it to one of my other computers. I've been looking at external hard drive enclosures. Will they work on a laptop disk,
or is there a better solution that you recommend?

A: Geez, Steve. It wasn't a surprise? Why didn't you back up the darn thing?
Assuming the hard drive is still good, you can retrieve the data. In fact, you can continue to use the laptop drive. It would work as an external drive. Or, you could install it in a desktop. (Most laptops only hold one internal drive.)
Before you invest in hardware, check with some computer stores. They will remove the data for you. That should be fairly cheap, assuming you don't have much. Most stores charge at a per-gigabyte rate. They would probably just burn it to a disc.
However, you might want to continue using the drive. Remember, though, laptop parts are less robust than their desktop cousins. So the drive might not last as long as you'd like.
With that in mind, I found external enclosures online starting at $10. As solutions go, that will be hard to beat. You cable these things to your computer, using either USB or FireWire.
Be sure to buy an enclosure for a 2.5-inch hard drive. An enclosure for a 3.5-inch desktop hard drive won't work.
Windows should see the drive right away. Go into Windows Explorer (Start>>All Programs>> Accessories>>Windows Explorer). The laptop drive will be listed under Computer.
You can drag the folders and files to your internal hard drive. Your old laptop drive could also be used for storage. Drag rarely used files from the internal hard drive. Again, I wouldn't count on the old drive lasting forever.
If the replacement computer is a desktop, you have an additional option. You could certainly use the old drive externally. You just need an available external port. But if that offends your sense of neatness, mount it internally.
I found adapters online for less than $10. They allow you to plug the laptop drive into a 40-pin cable. This works on an IDE setup. This is the old-style way of connecting hard drives and motherboards. You'll recognize it because it uses ribbon cables.
Double-check that you have an IDE port in your desktop. If you don't, stick with the external arrangement.
Now, Steve, really, are you doing backups? If not, you know very well that you should be. If nothing else, you could use your old drive for backups.
However, I'd get the backups off-site. If you're burglarized or your house burns, the backups will be safe. The obvious choice for off-site backups is Carbonite, one of my advertisers.
Carbonite is automatic. That's very important. If people are involved in the backups, they'll eventually stop doing them. Once Carbonite is set up, it backs up in the background. It never needs additional human involvement.

You can sign up for a free 15-day trial through my site. When you purchase the service, you'll receive two months free.

When it comes to hard drives, I've got lots more information:

--Clean up your hard drive
--Check the health of your hard drive
--Copy and wipe your hard drive

Backing up an iTunes library

http://www.komando.com

Q*. My son has an iPhone. His iTunes collection is 13.3 gigabytes. All of this is stored on our comuter's hard drive. I would like to back up the music. What method do you recommend? Should I back it up online or use a thumb drive? Or are there other options?*

A. Your question is troublesome, Larry. You see, 13.3 GB is not a particularly large amount of data. So, there's nothing terribly difficult about backing up this data.

But the fact that you're posing the question worries me. It sounds like you're not backing up at all. If not, you're asking for trouble.

In seconds, your important documents, e-mail and other data could disappear. And you might never get it back.

So, I fear you have more to worry about than the music. You need a plan for backing up your entire system.

You have many options. Let's look at the advantages and disadvantages of each. Choose the one that works best for you.

CDs/DVDs

Discs are a quick and easy way to share data. They're also good for making music CDs and DVDs for standalone players.

However, CDs and DVDs are not suitable for backups. Their storage sizes are relatively small. You can fit a paltry 800 megabytes on a CD. With DVDs, this is upped to 8.5GB. Your son's music collection would overwhelm either.

Capacity isn't their only problem. The real catch is that they're not very reliable.

Optical discs can be scratched or broken. However, the main worry with burned discs is deterioration.

When you burn a disc, a laser heats a media layer within the disk. Over time, that layer changes, making the disc unusable.

If you truly value your data, skip these discs.

Flash drives

Flash drives are handy for transporting data. They're small and can be put on a keychain or in a pocket.

Furthermore, they're highly reliable. They're less susceptible to drops and falls than other media. The biggest physical threats to flash drives are theft and loss.

Continued on the next page

Also, storage capacities are limited. Thumb drives top out at 64GB, although 128GB ones are on the way. You'll pay a premium for a 64GB thumb drive.

Flash drives are an excellent choice for backups.

Wondering how long a flash drive will last? Good question! You'll find the answer in my quick tip.

Hard drives

Hard drives are probably the most popular backup solution. These days, they're ridiculously inexpensive. You can pick up a 1 terabyte external drive for about $100.

You can get an external hard drive for even less. That assumes you don't mind doing a little tinkering. Of course, the most popular solution may not be the best. Such is the case with hard drives. They are relatively fragile. Drop one, and it's toast.

Even if you're careful, a hard drive will fail over time. I wouldn't trust a hard drive past five years. Many fail much sooner than that.

There are many pros when it comes to hard drives. However, their high failure rate should give anyone pause.

Online services

An online service is probably your best option for backups. I use Carbonite to back up my computers at home and the office. (Carbonite is one of my advertisers.)

With Carbonite, you don't need to worry about media failing. And, with unlimited backups, storage capacity isn't a problem.

Online services also add additional layers of protection. Your data is stored off-site. So, you don't need to worry about a fire or other disaster taking your data. And, backups are performed automatically. With Carbonite, backups become a set it and forget it affair.

I get a lot of questions about Carbonite. Most are about security. That's a valid concern when you're storing data off-site.

Carbonite is serious about security. You can learn more about Carbonite's security and encryption features in my handy tip.

Carbonite has a special offer for my listeners. You'll get two months free if you use my sign-up page, Carbonite.com/Kim. That's in addition to the standard 15-day free trial.

You'll want to make sure you're backing up all the right files. Otherwise, you'll be in for a shock when your computer fails.

Finally, some of the data you're backing up is probably sensitive. You don't want this data compromised. I have a great free download on my Web Site that will help you encrypt it.

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 Spam, Malware and Users beware

Internet Security

Collected from various sources by the editor from the Internet

Internet safety seems like an oxymoron these days with all the threats aimed at our computers. Staying safe online doesn't have to be difficult, and this article covers the basic steps that every computer user should take.

The phrase "Internet Safety" often seems like an oxymoron. Every day we hear of new threats aimed at our internet connected personal computers which seems to just make it that much harder to actually stay safe while connected online.

Knowing how to stay safe online has become a practical requirement these days for anyone using a computer connected to the 'net. Fortunately, a few relatively simply steps and a little education can go a long way to making sure that your internet experience is both safe and secure.

1. Use a Firewall - If you do nothing else, you must use a firewall. Firewalls act as a type of barrier between your computer and the Internet, preventing remote computers from connecting to yours unless you explicitly allow it. A firewall can be a simple device such as a broadband router, it could be a feature of your operating system such as Window's own built-in firewall, or it can be a full featured software package that you purchase and install on each computer. Which one you choose is less important than making sure you have one and that it is enabled and deflecting threats.

2. Back Up - Failing to back up your computer, or at least your critical data, is perhaps the most common mistake I see being made today. And sadly it can also be the most costly regret you'll have when, not if, disaster strikes. If malware hits or hardware fails often your best if not your only resort will be to recover your system from its most recent backup. Don't have one? Then you might be severely out of luck. I regularly hear from people who've lost all of their data due to a malware infestation or a hardware failure. If nothing else, invest in a large external USB drive and a good backup utility and start backing up regularly right away.

3. Keep Critical Software Updated - Every day people experience problems that could have been completely avoided had they simply kept their operating system and other PC software up to date. Both Windows XP and Vista make staying up to date very easy with "Automatic Updates" and I definitely recommend that it be turned on. Similarly, most other software and applications will now also check for updates and notify you, as new ones are available.

Continued on the next page

Make sure your system and applications are checking for updates regularly and installing them as automatically as possible.

4. Educate Yourself - No matter what else you do, no matter what other protections you put in place, malware authors can bypass it all if they can fool you into doing something you shouldn't. The problem, of course, is that "what you shouldn't" isn't always immediately obvious. That's why it is so important to educate yourself on how to detect and avoid their attempts. In short: be skeptical. Don't open email attachments or instant messenger downloads unless you're positive they're safe. Don't click on links in email unless you're positive that they're taking you to where you expect them to. Don't download and install software without first checking it for malware. Don't ignore security warnings unless you're sure it's OK. Use strong passwords and never share them with anyone.

5. Scan for Viruses - Even with the best of intentions, viruses happen. Even with the firewall in place, the operating system up to date, and a healthy knowledge of what is and is not safe, sometimes something slips through. That's where you'll need a good anti-virus tool. There are many to choose from but the key factors boil down to this: select a reputable tool, enable its "real time" monitoring if you're at all uncertain of yourself or others using the computer, configure it to scan your hard disk completely once a day, and make absolutely certain that it's downloading the latest anti-virus information daily.

6. Protect Yourself from Spyware - Much like viruses, spyware can also occasionally make it through your defenses. Spyware is often relatively benign from a pure safety perspective - spyware doesn't often erase your hard drive or send Spam, for example. However spyware does represent an intrusion, often presenting ads or modifying other programs in ways you didn't expect or ask for. And at its worst, spyware lives up to its name, spying on you and capturing potentially sensitive information. Anti-spyware utilities operate a little differently than anti-virus, so you'll want to make sure that you have a good spyware scanner in addition to your anti-virus tools. Like those tools, you'll want to make sure that it's downloading the latest spyware information daily as well.

7. Secure your Wi-Fi - The default configuration of most Wi-Fi equipment, and certainly the easiest configuration to set up, is completely unsecure. That means that anyone within range of your Wi-Fi equipment can monitor what you're sending to and from the Internet - including your account IDs and passwords. The same is true in most Internet cafes and free Wi-Fi hotspots. There are two steps you must take. First, at home, make sure you enable WPA security. This will require a password to connect to your wireless network, and will encrypt all the data so it cannot be monitored. (The older WEP security is no longer sufficient, as it is easily cracked.) Second, when you're using an open unsecure Wi-Fi hotspot, take care to only access sensitive resources through encrypted connections. That means making sure that any web page you're visiting that requires personal information is connecting via an https connection. It also means that you shouldn't be downloading or sending email via your POP3 or SMTP based email program unless you know those connections are configured to use encryption as well, since by default they do not.

Bonus Step: Understand Physical Security - An old saying that I've found myself repeating to people more and more in recent years is this: "if it's not physically secure, it's not secure." All of the preceding tips are for naught if someone else who doesn't understand these steps can use your computer and accidentally download malware. It's all for naught if someone with malicious intent can walk up to your computer, reboot it, install software or hardware and walk away without your noticing. It's all for naught if your computer can be stolen. Take care to understand just how physically at-risk you might be and take appropriate actions. Don't let others use your computer until you're comfortable with their understanding of the risks. Don't leave your computer unattended if you can't trust the people who might be able to touch it. Consider encrypting data on your laptop or other computer if it can be lost or stolen.

Everything I've outlined might at first seem overwhelming. The good news it that most of these steps are things you'll need to do only once, and then consider infrequently thereafter. And to put it perhaps into a little bigger perspective they're not nearly as overwhelming as the impact of an actual security problem if it happens to you. The practical reality of the situation is simply this: we as individual computer users need to take the responsibility of the steps required to Stay Safe Online.

People helping People … and themselves

Last September I purchased an OCZ 120 GB SSD for my home built desktop PC running Windows 7. I had backed up my mechanical Western Digital HD with Acronis software, and then restored that backup onto the SSD. The speed increase was VERY noticeable, probably cutting disk read/write times by 1/3. The PC boots up VERY fast from a cold boot using Windows 7 64-bit Ultimate, probably taking only 1/3 the time when compared to the mechanical WD drive.
Now for the bad news. After 2-3 months, the SSD drive crashed. I was frustrated, but having a good backup available I simply did a quick restore and all was back to normal, for a while.
The next month, the SSD drive again crashed. This happened 3 times and 2 months ago I sent the SSD back to OCZ for repair under warranty (1 year). OCZ sent me a refurbished 120 GB SSD, which I installed and restored from backup. This second drive performed flawlessly except for one little item. Every time I put the PC in the sleep mode, the drive would crash into the blue screen of death (BSOD). I could not figure out what could possibly be wrong.
Why would Windows 7 work just fine with all applications, but crash into the BSOD when hibernating? Before I called OCZ and complained, I tried something.

I did a quick format on the SSD and installed Windows 7 from scratch. For anyone who has ever done this you know it takes hours and hours to download and install all of the updates, plus all of your software, documents, pictures, etc. But the net result was the SSD now performs flawlessly. No more hiccups or crashes. Now I have a VERY fast computer with an even faster hard drive.
After everything was running smoothly with all updates installed, I reran the Windows 7 experience index. The hard drive transfer rate jumped from a paltry 5.2 to 7.3.
My motherboard maxes out at 3 GB/sec transfer speed, but the SSD supports 6 GB/sec.
So, one of my next projects is to upgrade my motherboard, memory and CPU to SATA 3 and 6 GB/sec transfer speed.

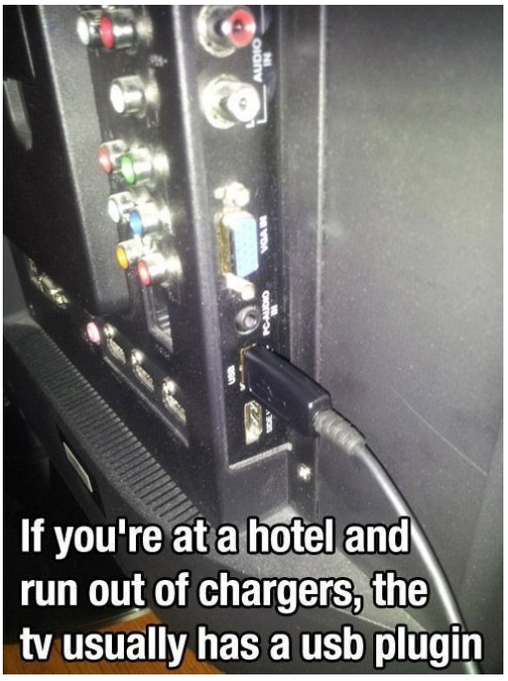
On a similar note, I read with great interest today's article by Fred Langa on backing up and restoring SSD to/from mechanical spinning platter drives. Fred also discussed the anti-wear routines that SSD drives use to "that prevent data from being written to the same locations on the drive, over and over again."

If you want to speed up your computer regardless of its age or operating system, you can't go wrong with a solid state hard drive. Your computer will easily be 3 times faster with an SSD drive.

Charlie

The lighter side

Collected from the Internet



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