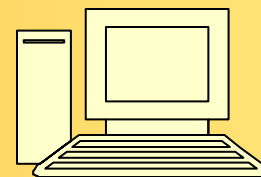


BAY BYTES

Greater Tampa Bay Personal Computer User Group, Inc.



Newsletter

Issue 12

December 2010

23rd Year of People Helping People!



In this Issue

Minutes of the meetings	2
Officer nominees 2011	3
SIG leaders for 2011	4
System crashes	5
.System crashes <i>Cont.</i>	6
Internet Security	7
Password removed	8
Vishing is on the move	9
Vishing is ... <i>Cont.</i>	10
Validate backups	11
Validate backups <i>Cont.</i>	12
The lighter side	13

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/](http://www.dmanns.org/dmiller/)



To all members

As we get closer to 2011, I want to extend my thanks to those members who renewed their commitment to continue serving our group as an officer or SIG leader next year. Especially to Gary Staley and Parker who were very constructive in getting our "old class room" back.

Since our group has close to 100 members, one would think it wouldn't be difficult to get a few members to help run our club for a year or two. This time it looks like the spirit of helping the club did prevail, for which I am most grateful and thankful.

As everyone knows, if the club doesn't actively take care of its membership, particularly potential new members, our group will inevitably wither away.

At this point let me thank "Brock" Brock, who volunteered to be our Vice President for 2011. Even so he is up north for about 5 month never the less it shows the sprit.

If you have never been one of the leaders in the past, PLEASE consider becoming one now or in the future. We still need a membership chair.

In conclusion, our group can continue to be as successful as it has been only if the members themselves see to it that the necessary leadership positions are filled.

In the meantime, my best wishes to everyone for the holidays and a healthy and prosperous 2011.

Your president,
Jo Ann Brawner

Class Meeting Report from November 2. 2010

During the class , Jerry Harris explained dual monitor setup in Windows XP and WIn7.

as well as customize desktop features in Win7.

AVG anti virus problems were also discussed.

Aconis introduced the 2011 version of True Image still at a discount for the members at: ugr.com

Class Meeting Report from November 9. 2010

At the 11/09 the Windows SIG kept Darrell Manns busy answering Windows related questions.

Again, anti-virus protection and hard drive backups were the most asked ones.

Class Meeting Report from November 16. 2010

Michelle Burgess, a member of the Tampa PC User Group,

as a special guest speaker presented the members with an introduction to Facebook and Twitter.

A well functioning anti-malware and anti-spyware program as well as a good anti-virus program updated to the latest version is a must to browse both sites safely.

Class Meeting Report from November 23. 2010

School vacation, no class.

Officer nominations for 2011 are:

President: Jo Ann Brawner



Vice President: Brock



Treasurer: Gary Staley



Secretary: Patrick Courtney

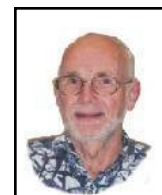


Membership:

Program Coordinator: Sherry Foecking



Web Master: Parker Monroe



Newsletter Editor Al Droll





Of course, also continuing their support to the club in 2011 are our SIG leaders:

Sherry Foecking with her expertise in MS Office and other office software related subjects.

Darrell Manns with his knowledge in Windows XP software, special programs and gadgets applied to the operating system.

Jerry Harris always has answers where the Internet and Networking are concerned. He also answers questions on other subjects as well.

Parker Monroe the all-round PC man seldom gets stuck with questions he does not have answers for.

Not to forget all the others filling in to lend a helping hand to make the evening a success.

Crashes come in all sizes

www.smartcomputing.com

Crashes come in all shapes and sizes. There's the freeze, of course, where everything just stops. And then there's everyone's favorite, the infamous "Blue Screen of Death," where the screen goes blue and displays all sorts of mysterious instructions. Once you see that, you know you're cooked.

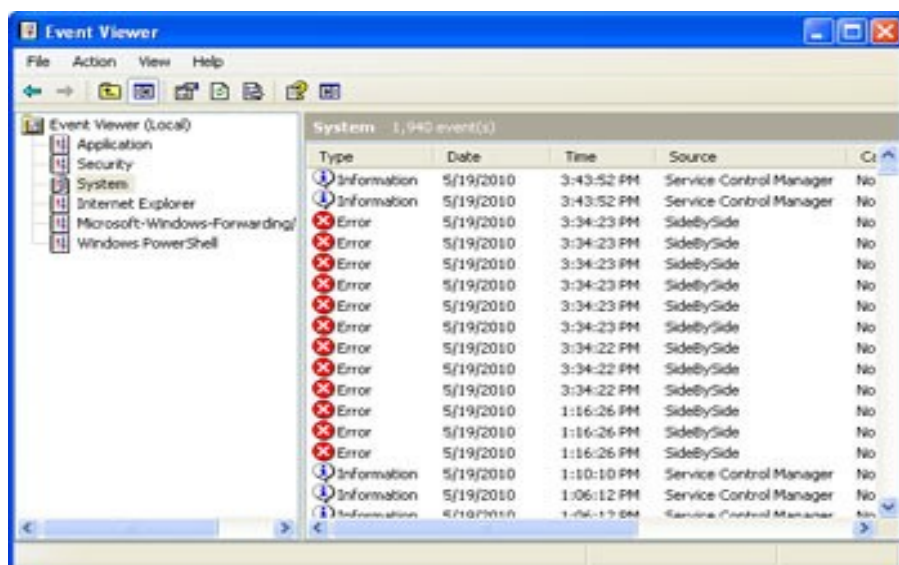
The first and most obvious response to a crash is to restart the computer. If your machine manages to reboot successfully, that's a positive sign. However, the crash may have left behind errors with the PC's registry.

The registry provides directions for every program on a Windows computer, telling your PC what to do next. If there's an error in your registry, your computer might not know what to do. It's probably not a great idea to try fixing the registry on your own. There is software that can do it for you; either [search for a free registry cleaner](#), or we recommend either [System Mechanic](#) or [PerfectSpeed](#), both of which include tools to fix a corrupted registry.

If your computer won't restart, your next move is to try restarting it in **Safe Mode**. Sometimes faulty drivers are the root cause of a crash -- rebooting the computer in Safe Mode disables most of those drivers in the hopes of getting the machine restarted, and perhaps recovering any lost data.

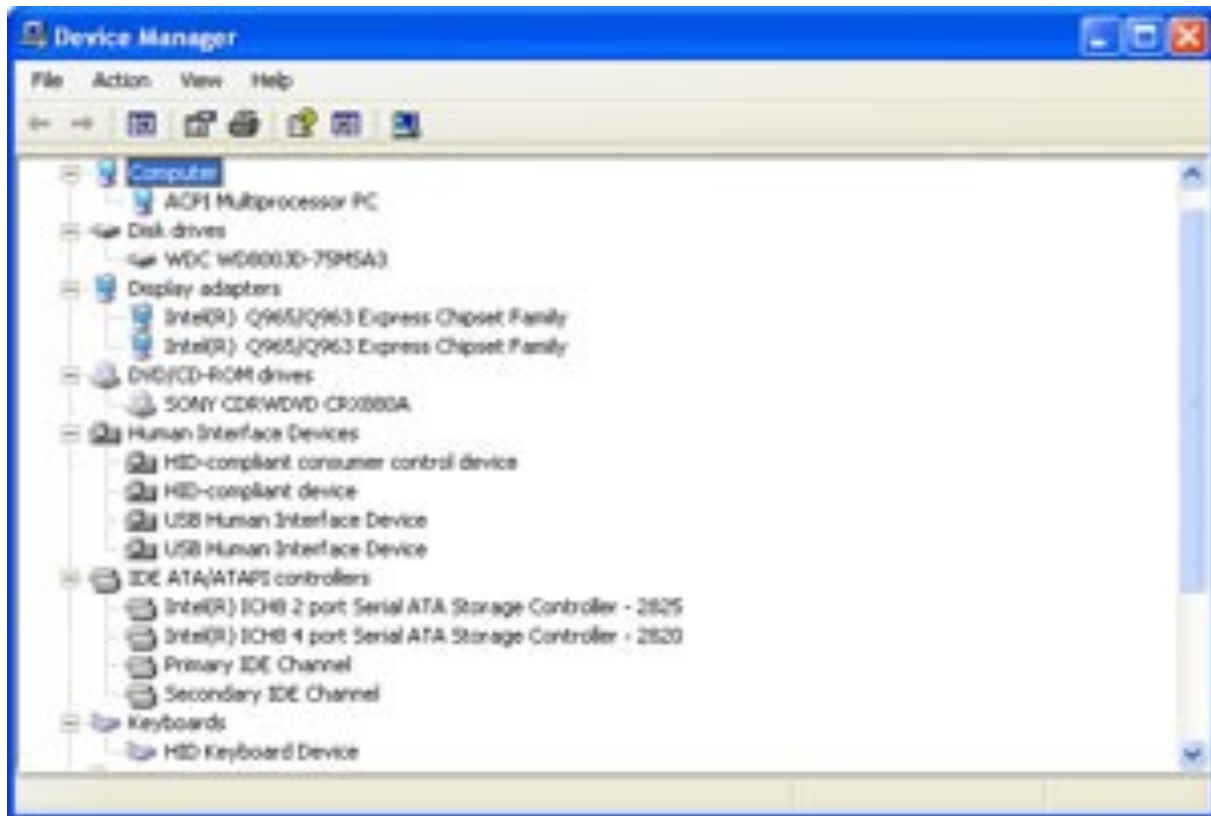
To reboot in Safe Mode, press the F8 key while restarting -- the **Windows Advanced Options** menu appears, providing choices in the **Boot** menu. Newer versions of Windows provide several Safe Mode options to choose from -- use the arrow keys (not the mouse) to make a selection, and press Enter.

Bear in mind that when the computer restarts in Safe Mode, it will look, feel and function differently than you're used to -- for example, it will display using fewer colors in a smaller screen resolution, and certain components won't work. In other words, you won't want to use the computer in Safe Mode for very long. Once you've successfully restarted in Safe Mode, work quickly to restore and back up any lost data, make any changes to your system setup and then reboot again normally.



While in Safe Mode, you can attempt to determine the cause of the crash to either disable or uninstall the culprit and avoid future trouble. Windows keeps track of the programs you're using in the **Event Viewer** -- this is a good place to look for the cause of a crash. Click **Start**, go to the **Control Panel**, and click on **Administrative Tools**. From there, double-click on the **Event Viewer** and choose the **System** section. Error symbols will be marked with a red exclamation point, suggesting which program (s) may have caused the crash.

Continued on the next page



Another guilty party could be the drivers that tell your computer's devices how to operate. To check your drivers for errors, click **Start** and then **Control Panel**. Click **System** and then the **Hardware** tab. Select the **Device Manager** to bring up a full list of your drivers; right-click on any one and select **Properties**. Errors will appear with a yellow "X" or an exclamation point, helping identify the cause of the crash.

If crashes continue to occur, your computer may have problems that require more than a do-it-yourself diagnosis and repair. In that case, we recommend [support.com provided by AOL](http://support.com.provided.by.AOL), which provides expert PC repair service remotely, over the phone.



"Okay your father managed to get a mouse. Now how do we use 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://www.gtbpcug.org/protect/>



More about Internet Threats

QUESTION:

www.komando.com

There is a lot of talk about the privacy dangers at public hotspots.

There seem to be a lot of threats out there right now. Is there one easy solution that can keep you totally safe?

ANSWER:

Criminals are always looking for new ways to get your money. Using a laptop at a public hotspot is particularly dangerous. I've offered tips to keep you safe on public Wi-Fi.

And I recently told you about a new threat, FireSheep. FireSheep can give a hacker easy access to your online accounts. You just have to log in while on a public network.

It's that easy to be hacked. The other threats may be a little more difficult to pull off. But, a hacker would have no trouble exploiting them.

This means that your information is incredibly vulnerable. Hackers can easily get at your online accounts or your files. And combating the crooks takes a fair amount of work.

Your best bet is to leave your important files at home. And you should make sure all your Internet communication is fully encrypted. Of course, it isn't always easy to follow these recommendations.

You usually need to have some important files on hand. And not all Websites support proper encryption. Fortunately, there is a solution that gives you the best of all worlds.

<https://www.eff.org/https-everywhere>

Getting rid of created password

www.komando.com

Q. I have Windows 7 on my new netbook. I foolishly set up a password. Now, I have to sign on each time I use it. Can I delete this? Thank you for all your help in the past. I will continue to learn with your expertise.

A. Well, that's easy enough to do. And having a password is actually a good thing. I'll discuss that in a moment.

Now, if you have a password, those plans could be OK. Odds are, the thief doesn't have the brains to crack the password. (The Windows password can be broken. But the thief probably just wants the hardware.)

Here's another example. With a password, you can set up a guest account. Let's say Aunt Gertrude comes to town. She's the family snoop. She asks to borrow the netbook to "check my gmail." You know she really wants to check YOUR e-mail.

Passwords are set up through User Accounts. They're easy to discard.

Click Start>>Control Panel>>User Accounts. Select your account. Click "Remove my password."

On the next window, enter your password in the box. Click Remove Password.

Passwords are easily removed in Windows XP and Vista, too. Click Start>>Control Panel. Double-click User Accounts. Click your account. Click "Remove the password." (In Vista, it's "Remove your password.") Click Remove Password.

I agree that a password can be a pain. When you boot up, you just want to use the netbook. You don't want to stop everything for a password. But there are good reasons to have a password. Let's say you're at a coffee shop. You get up to fetch your third 650-calorie blueberry muffin. You come back to find your netbook gone. Your secret plans for a perpetual motion machine with electro-hydraulic flywheel are on it.

Password Memorizer

If you struggle to keep track of multiple passwords, you can benefit from this program. It can organize and store all of your passwords in one place. All you have to remember is one code to access your passwords.

The program lets you categorize your passwords. For example, you could set up categories such as "E-mail accounts" or "Web site memberships." You can also name each user name/password pair to make them easier to find in the Password Safe list. One idea is to name them after their matching Web sites or programs.

Password Safe can produce strong passwords for you from scratch. Strong passwords such as "G9rt-qy5" are rarely used because they're so difficult to memorize. That's no problem with Password Safe. And passwords are kept in a secure file protected by Blowfish encryption.

Cost: Free

www.passwordsafe.sourceforge.net

Criminals have now gone 'vishing'

www.komando.com

You receive an e-mail from PayPal asking you to call. Your account has been compromised. Or, a company you don't know calls threatening collection. It's scary. Before you give out any personal data, there's something you should know.

You could be the target of vishing, or voice phishing. It's the latest twist on phishing scams.

Phishing attacks rely mostly on e-mail. You receive a message purportedly from a bank or a store. A problem with your account requires immediate attention.

The e-mail directs you to a malicious Web site. The site looks legitimate. The Web address even appears legitimate.

The site is designed to trick you into disclosing sensitive information. Or, it infects your machine with malicious software. Either way, you become a victim of credit card theft or worse.

Popular Web browsers incorporate anti-phishing tools. Unfortunately, criminals are one step ahead. They're using the telephone to catch you off guard.

Vishing leverages Voice over Internet Protocol (VoIP). Internet-based phone service makes it easy to spoof telephone numbers. Criminals can make a different name and phone number appear on caller IDs.

How do vishing attacks work?

There are several variations of vishing scams. In one attack, a criminal calls via telephone. Your caller ID displays the name and number of a reputable organization. Maybe it is a bank, store, government agency or Web site.

When you answer the call, a prerecorded message greets you. It directs you to another phone number. If you call, you're prompted to enter personal information via telephone keypad.

The key tones are captured and decoded. The criminals just got your information.

Another variation begins with an e-mail. Unlike with phishing messages, you're not directed to the Web. Rather, you're instructed to call a telephone number. You are tricked into revealing personal data.

Or, you receive a call from a spoofed number. This time, you speak to a real person. The person requests account numbers and other data.

The caller could invite you to join an online research network. You're paid to install special software on your computer. The software is spyware that steals sensitive information.

Some vishing attacks start with a prerecorded incoming call. You're directed to a Web site to resolve an account problem. The site is a phishing site.

Continued on the next page

How to spot a vishing attack

Vishing methods may vary. However, there are several hallmarks of vishing attacks.

First, the information presented in the attack is upsetting or exciting. For example, you could be threatened with a lawsuit over an unpaid bill. You may never have done business with the company.

Vishing attacks usually demand an urgent response. You allegedly run the risk of account closure or credit troubles. That is, unless you take immediate action.

You should also look out for false pretenses. The visher may ask you to take a poll. Then, you're directed to install a spyware program.

Vishing attacks usually aren't personalized. They probably won't reference a real account number. The visher may not even know your name.

How to protect yourself

Suspicion and vigilance are your best weapons. Be wary of incoming communications. Do not rely on caller ID to identify callers. E-mail addresses are not trustworthy, either.

Never give out personal information in these circumstances. Instead, call the organization to ask if the communication is legitimate. Check your account paperwork for the correct phone number.

You may have never done business with an organization. In that case, ignore the communication. It's your safest bet.



Set Validation for Acronis True Image Backups

by Parker Monroe

Many of our club members have purchased, and use, Acronis True Image backup software to store images of their computer on an external drive, but some are not aware that an essential part of the backup process is not being performed - making sure the backup has been "validated."

Validating a backup image, or what Acronis calls an archive, ensures that the backup image is actually error-free, and will be usable if and when needed.

Several members have, unfortunately, experienced the problem of having faithfully made backups of their computers, and have even noticed a message at the end of those backup routines stating that the backups were "successfully completed," only to find later, when they really needed to restore all or part of a backup image that the backup was corrupted.

To ensure that backups you create are not corrupted, the more recent versions of Acronis True Image software fortunately have a setting that tells the backup program to automatically perform a Validation after the backup is completed. Unfortunately (in my opinion), the publishers of Acronis True Image have chosen to leave that setting "off" in its retail versions when they are installed on computers, possibly because validation adds some time to the backup process.

I strongly recommend turning on that setting, so that every time you make a backup image, the backup program will then automatically validate that backup image. And, while that will add some time to the backup process, at least you will know that that backup image should be usable if ever needed.

Here's how to set two versions of Acronis True Image Home (that I have on my computers) so that Validation will run automatically after an image backup has been completed. Once you have made this setting, you will not have to set it again, unless you upgrade to another version of the Acronis backup program.

Acronis True Image Home 2010:

After bringing up the program, click on "Tools & Utilities" near the top of the program

Click on "Options"

In the left column of the window that opens, click on "Local storage settings"

Click on "Archive validation"

Left-click to put a checkmark in the small white box next to "Validate backup archive when it is created"

Click on OK to save the setting

Continued on the next page

Earlier versions of Acronis True Image:

For certain earlier versions of Acronis True Image, one cannot set validation (which Acronis used to call "checking") to run automatically, so one has to run it manually after completing a backup. For example, here are the steps to take for version 8 of Acronis True Image to "check" any backup image made with version 8 (and possibly even backups made with earlier versions).

Also, when doing a "check" on an earlier version image backup, be sure your external drive is already attached and turned on, and connected to your computer (usually via a USB plug), so you can find the backup image you want Acronis to check.

Acronis True Image Home 8:

After bringing up the program, click on the icon with the red checkmark on the toolbar. It is the 8th icon from the left

Click Next

In the Image Archive window, locate the drive that contains the backup image you have just created

In the list of backup images, click once on the backup image you want to check (validate) to highlight it

Click Next

Click Proceed to begin the checking/validation

To all members:

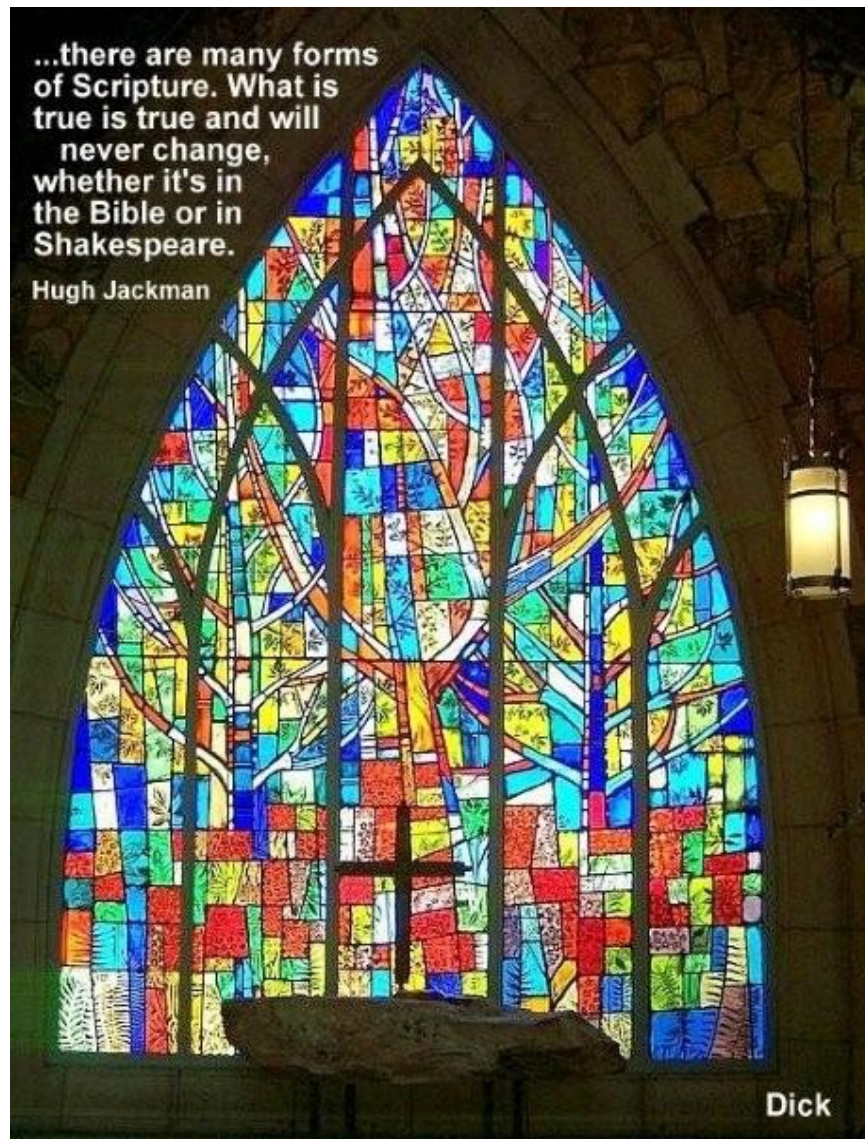
We received the following email today from the president of the FACUG (Florida Association of Computer User Groups), which our group is a member of.

The email notes that one can purchase a three-pack of Windows 7 Home Premium at a very good price of \$119.99, which means one could [upgrade](#) up to three pc's with legal copies of Window 7 for just \$40 per pc from Windows Vista or Windows 7. Be sure to run the [Upgrade Adviser](#) first!

Click on the link provided above, and at that Web site, if you wish to upgrade one or more Windows XP pc's, be sure to read what owners of Windows XP pc's need to do in order to install Windows 7.

Note: this very low price may not be offered for very long.

Parker



Legal Notice

Bay Bytes, Copyright © 2010, is the official newsletter of the Greater Tampa Bay PC User Group, Inc.(GTBPCUG). The information in this newsletter is intended to help our members. It has come from many sources and cannot always be verified. It is recommended that you obtain professional advice from software and hardware distributors, manufacturers, salesmen, or other professionals dealing with the subjects that appear in this newsletter. Unless specifically stated otherwise, the opinions expressed in Bay Bytes articles and columns are those of the individual authors and do not represent an official position of, or endorsement by GTBPCUG.GTBPCUG is not affiliated with any company, vendor or equipment manufacturer. Permission for reproduction of Bay Bytes in whole or in part is hereby granted to other APCUG user groups for internal, non-profit use, provided credit is given to the author, GTBPCUG Bay Bytes along with the copyright notice. Other reproductions require the prior permission of the editor. When published, please send a copy of your newsletter to

editor@gtbpcug.org or mail to P.O.Box 501, Brandon, FL, 33509-0501.