The Villages Computer club

The next meeting of the VCC will be at Hacienda, Friday 4/6/2012 (Good Friday) at 1 pm.
A presentation, INTERNET SECURITY, will be presented by Peter Cronas and John Campbell.

The same presentation will again be presented the following Friday 4/13/2012 at Lake Miona at 1 pm.
****

Computer Plus will meet on Thursday April 5th at 1:00 PM
at Laurel Manor Recreation Center.

What you can do with Microsoft Live Gallery, Movie Maker and DVD Maker? Fred Benson will show how to use these programs
to manage photos, make slideshows and videos and burn DVD's.

Come and see things you may not know about these programs.

Android Phones and Tablets: May 3rd

We are going to have an Android Phones and Tablets session on May 3rd and we are looking for a few folks who would like to
join us up front to answer questions or participate in the program presentation. The purpose is to cover "introduction" to settings,
"APPS" that you use or like, Security and Email. There will be a general introductory Power point to start us off. If you would
like to help please contact Pete R pjrdbs@msn.com or see him at the next meeting.

New Programs / Presentations

If you would like to suggest any new programs or presentations for C+ or would like to present one please email Pete Rosendahl
pjrdbs@msn.com or Fred Whitson fdwhitson@aol.com

We also welcome your comments, suggestions, ideas and anything we may want to improve.

For more information please contact Pete Rosendahl at pjrdbs@msn.com
****

Batten the Hatches

The spate of recent worms makes it clear that way too many people aren't keeping their PCs secure.

For example, many of these worm type viruses spread itself by email or by direct infection via unguarded network ports. But any good Anti-Virus tool, and some high-quality desktop firewalls like ZoneAlarm, defang hostile inbound mail attachments: This would have closed off email as an infection vector for this kind of attack.

Any decent firewall--- even the Microsoft Windows Firewall--- can block the port probes that "inbound" worms like this use to seek new local victims, totally closing off that infection vector. And the better desktop firewalls also alert you to suspicious *outbound* activity from your PC, so even if your PC were somehow infected, you could still see what was going on, and prevent your machine from infecting others.

This worm was designed to take advantage of a Windows security hole for which a patch had been released (via a "Critical Update") a month *before* the worm surfaced! This is a worm that should have gone nowhere.
But clearly, huge numbers of systems still are running unpatched, unprotected, and wide open; millions of PCs were thus needlessly compromised. Of course, the usual "it's Microsoft's fault!" cry went up. And while some problems *are* Microsoft's fault, I don't see how we can pin this one on them. People whose PCs were infected in this outbreak had ignored a "Critical Update" AND/OR were running unprotected by desktop firewalls AND/OR were running without up-to-date antivirus tools. Those are voluntary choices, and (as many found out) ones with bad consequences.

Many readers are running very well-protected computers. But if you have coworkers or friends who are leaving themselves open or if you're not well protected yourself--- this may help:

<u>First,</u> stay patched. I know some users worry about applying Critical Updates, because they sometimes do cause new problems. Up to a point, that kind of caution is a good thing.

Assuming you have a good antivirus tool and a good firewall running to protect you from the most-frequent infection vectors, then it can make sense to wait a few days after a Critical Update appears to see if others have trouble with it. But it rarely makes sense to wait weeks or months before applying a Critical Update. They're called "critical" for a reason.

And please note that you can apply the Critical Updates as soon as they appear, if you have a good backup process. Then, if something doesn't work out, it's no big deal because you can undo the change in a matter of minutes.

For that matter, you usually can apply Critical Update right away

anyway: Although some Critical Updates have caused trouble, most of them work exactly as they should.

Five steps to keeping your computer protected against viruses

- **Keep your operating system up-to-date.**
- **Run your virus scan program regularly**
- **Update your virus definition file often**
- **Use a personal firewall program**
- **Set-up your programs correctly**

****
*

Spyware

It is imperative that you keep spyware out of your computer. At the very least, it can slow down your computer. At worst it can cause harm to your computer and to programs in your computer as well as feed personal information back to it's creator.
****

Zapping Bad Cookies. Not all cookies are bad. But the bad ones - spy cookies in particular - can be very irritating. You can end up on spam lists. Your personal information could go to somebody you've never heard of. Your Web-surfing habits could be collated. Not good.

The best, fastest, easiest way to protect yourself from spy cookies is with a two-prong approach. First, you should install a bad-cookie catcher. Second, you should double-check your Internet Explorer settings to make sure most irritating cookies don't get through.

One effective bad-cookie and adware blocker is a program called Malware bytes. It can be downloaded FREE.

Download FREE Malwarebytes to your Download folder on your computer.

Click here: Download Malwarebytes Anti-Malware - FileHippo.com
(The download button is to the right top corner of the download page)

1. Open the DOWNLOAD folder and doubleclick the Malwarebytes file to install it.
2. Click the Malwarebytes file in the startup tray to open it, and select Update from it's menu bar and Check for Updates below on the left.
3. Restart your computer and doubleclick the Malwarebytes icon in the startup tray.
4. Run a FULL Scan on all files.

Note1: The FREE Malwarebytes does not update and run a scan automatically, so be sure to always update before running.

Note2: It is a good idea if you are having trouble and suspect malware, update Malwarebytes and your anti-virus program and run them from SAFE MODE as some such malware is loaded into your computer prior to the loading of Windows.

Open in Safe Mode by pressing the Power button on your computer and begin immediately tapping the F8 key. Select Safe Mode with networking. Once windows opens in Safe Mode, open the Malwarebytes and run a full scan(update before running). Next, run a full scan with your anti-virus program.

****
****

VIRUSES SUSPICIOUS FILES

A reader writes: "Anyone who really wants to play it safe should scan their documents before sending them. That would at least give them some peace of mind--knowing that at least they tried to make sure the item did not have a virus. Of course, if the software does not detect a virus that's present, there is nothing you can do, but at least you tried to be proactive about it. People should also look at every attachment to an e-mail as a potential virus. That's why I always scan my attachments, at home and at work.

"In general, I would scan any Word or Excel document, as they are susceptible to macro viruses. I would definitely scan anything with an .exe [extension]. I doubt anyone would ever send me anything with a .vbs extension, so I probably would delete that. In the case of any other oddball file attachment, I would look closely at the file type. In other words, if I do not normally have people sending me .txt files, I would probably look at that as a red flag."

Any email containing a single hyperlink, I delete as this is often the way a worm sends itself from an infected computer using the addresses in that address book. It also often selects one of the names in the address book to show as the SENDER of the email.

****

Who's lying? Who should we believe? Is this a Catholic issue or is it a Constitutional 'rights' issue?

http://online.wsj.com/article/SB10001424052702303816504577311800821270184.html?mod=ITP_opinion_0

****

Jmax

Jmax's Website http://www.jmaxbits.com/

Jmax Bits Newsletter is now posted each Monday & Thursday on the website. You have the option for a .pdf or a .rtf file.

1.For help with a computer problem, put HELP in the subject line and give me info about the computer you're using, if you know it.

2.To view or print Jmax Bits Good Services List in the Villages area, click link www.jmaxbits.com

3. To sign up for the non-computer newsletter, send an email to VLGSClassifieds@aol.com. Put SUBSCRIBE in the subject line. To send an Ad, place AD in the subject line.

4. The Villages Computer Club's web page: Click here: Welcome To The Villages Computer Club
To add your name to the VCC announcements list, send email to TheVCC-subscribe@yahoogroups.com

5. Fred Benson's website www.thevillagescomputerbasics.com