WINNERS Notepad

WINdows usERS   September 2004

Help! I've been hijacked…

By Sherry Zorzi
Cajun Clickers Computer Club,
Louisiana.

First it was viruses, worms, and spam. Then came Trojans, spyware, and pop-ups. The newest scourge plaguing Internet surfers is browser hijackers, and one very nasty one is making the rounds in the Baton Rouge area, causing all manner of grief for local folks, including some Clickers members.

Browser hijackers are malicious programs that change browser settings, usually altering designated default start and search pages. The newest versions are going beyond messing with your browser settings. One of the worst, called "Cool Web Search" is particularly hard to remove.

Symptoms

How can you tell you have a browser hijacker? If your start page is suddenly different, that's a clue.

SP2 and Me

By Terry Currier

Well, as we said at the last meeting, the Service Pack (SP) 2 is out. In fact, Sunny downloaded it and brought CDs for our members at our August 14 meeting. I put the CD away, figuring to update my computers later. Time marches on, and Microsoft released SP2 to the public. I waited a couple of days and downloaded it from the Microsoft website. I figured that even though I had the CD, there may be something Microsoft added to the final version for downloading.

I did the expected thing. I clicked on Windows Update in Internet Explorer. It took me to the site, but it just would not go through. I kept getting "Error number: 0x80072EE2." Seems it just kept taking too long. So, I did the back door thing and went to the Microsoft site for downloading the file itself.

Was I worried? No, I have never had a problem with an update. My data was backed up (I thought), and Microsoft creates a restore if there are any problems, right? It's true that when doing service packs or installing new programs, Windows XP is supposed to create a restore for you.

So I started the update with the downloaded file. Once done, it needed to be restarted to complete the installation. I did so, but it just would not start up. I could not get it to come up into normal or safe mode. No problem, I just restored it to the last known working state. Well, that didn't work! Now what?
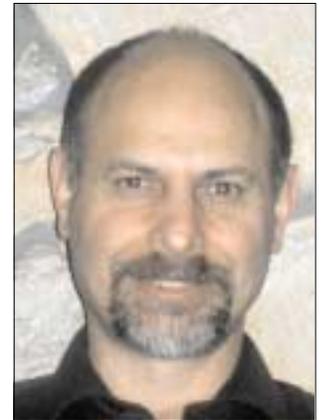
After many attempts that did not work, there really was only one thing to do. I had to reinstall (actually repair) Windows. Having done it once before, I was not too worried. I put in the CD and went through the process of having it repair the operating system. It wasn't long before I was back up. I got back into my computer but it was obvious that something was not right. Further checking showed it was stuck in limbo. It did not complete the update, but many of the SP2 files were in the Windows folder and they were not behaving.

My data is stored on my D drive and that was backed up. Of course, nothing happened to it. However, my Outlook data had not been backed up and it was not working, at all. I did have a backup from two months ago so I had to use it and lose two months. The operating system was more serious. There were two ways

Telephone Help Line

PROGRAM/SOFTWARE	NAME	PHONE	TIME
CompuServe	Cathy Grammer-Margolin	949-645-5950	6-10 p.m. & weekends
CorelDraw 5	George Margolin	949-645-5950	Most times
CorelDraw & Ventura & PhotoPaint	Sunny Lockie	949-644-0103	6-10 p.m. weekdays / 9 a.m.-10 p.m. weekends
Hardware	Jonathan Means	714-542-1653	6-9 p.m.
Internet	Cathy Grammer-Margolin	949-645-5950	6-10 p.m. & weekends
Novell, NT & Networking	Jonathan Means	714-542-1653	6-9 p.m.
Quicken & Quickbooks	Max Lockie	949-720-8170	6-10 p.m. & weekends
Windows 95,98,Me,Xp	Siles Bazerman	714-897-2868	9 a.m.-8 p.m.
Word for Windows	Cathy Grammar-Margolin	949-645-5950	6-10 p.m. & weekends
WordPerfect Windows	Sunny Lockie	949-644-0103	6-10 p.m. weekdays / 9 a.m.-10 p.m. weekends

General Meeting
September 11
Orange Coast College
9:00 a.m.-12:00 noon
in Science Room #149

Ritek - Advanced Media

WINNERS Notepad is published monthly by WINNERS, PO Box 9804, Newport Beach, CA, 92658. A subscription is included with all paid memberships in WINNERS. Other non-profit user groups may reprint *WINNERS Notepad* articles without prior permission, provided proper author, title and publication credits are given.

WINNERS, contributors and editors of *Notepad* do not assume liability for damages arising from the publication or non-publication of any advertisement, article, editorial, or other item in this newsletter. All opinions expressed are those of the individual authors only and do not necessarily represent the opinions of WINNERS, its Board of Directors, the *WINNERS Notepad*, or its editors.

PURPOSE

WINNERS, a computer association, is a volunteer organization providing a forum for sharing information and experiences related to Windows-based software, encouraging ethical use of computers and software, and offering service to our communities.

MEMBERSHIP

Annual membership is $20.00 for individuals; $5.00 each additional family member.

MEETINGS

WINNERS generally meets the second Saturday of each month from 9:00 a.m. to 12 noon at Orange Coast College in the Science Building, Room #149, 2701 Fairview, Costa Mesa.

FUTURE MEETING DATES

★ September 11
★ October 9
★ November 13
★ December 11

President's Message

By Steven Dela

By now, everyone has received an automated notice from Microsoft encouraging them to download the new Windows XP Service Pack 2 Update. This whopping 266MB compressed download is even a challenge for those using high-speed Internet access. For those using dial-up, it's an impossible task requiring over 15 hours of download time. The update is also available on CD, and can be ordered on the Microsoft site for the cost of shipping only.

All this worrying may be for naught, since many people are deciding to wait this one out until all the bugs are found and corrected. While this update has been touted as a cumulative patch of previous updates and a few new ones, few people believe it's the answer to all their problems.

Many of the message boards in the computing community are filled with stories on how this most recent update has changed their systems. There have been reported problems with some Dell notebook systems, anti-virus and utilities programs, naming routines, email clients, and games. Software companies are scrambling to verify the update does not cause any problems with their products and issuing patches when needed. For more information on some of the problems encountered, try visiting

http://www.pcmag.com

or
http://www.pcworld.com

for news and information.

Many IT departments in the private sector have issued instructions not to download the update. In fact, they have sent out a small program that is run on the local computer to disable the update notification so the update cannot be downloaded. Companies that did not take this precaution soon found their systems bogged down by users downloading the update and eventually system operation problems appeared on the update computers.

At the September meeting, if you have any positive or negative experiences with Windows XP SP2, please share them with the group during our random access session. That way, we can all learn what to expect and what to avoid when taking on this update.

New technology is currently launching that will take us to the next step in computer hardware. Terms such is BTX motherboards, and PCI Express bus will be important terms that you will need to know when buying your next computer. Come learn more about these by attending one of our general meetings.
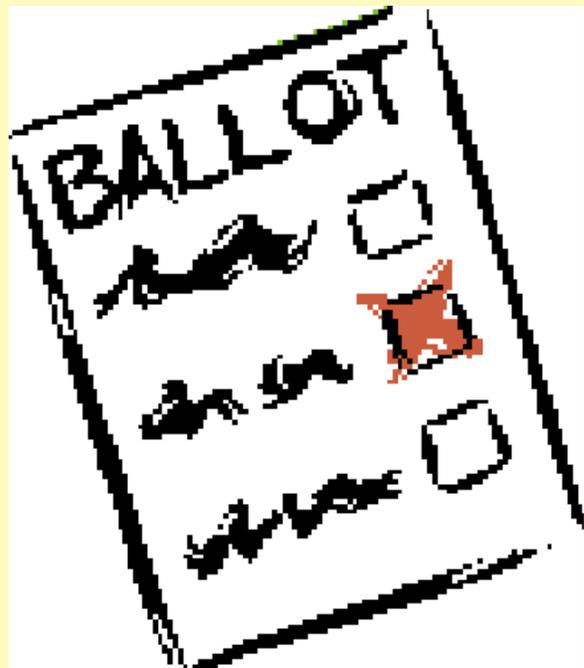
September also marks the first nominations for six Winners Board of Directors seats for a two-year term beginning in October. If you'd like to be nominated, please attend the September meeting to be nominated or relay in writing to any current board member your desire to serve. We'd like you to participate, and help Winners stay a productive and successful organization.

Steve

of fixing the problem, fully reinstall Windows, or try the SP2 again. I choose the SP2. Before doing so, though, I did a complete backup onto my external hard drive. I also backed up my data onto my second computer's hard drive. It may get me once, but not twice.

This time I used the SP2 from the CD, which worked including after reboot. Was I in the clear? No. My Sygate Firewall was not recognized, so the new Microsoft Security Center kept telling me I was in danger. I just clicked the message away. I would rather use the two-way Sygate Firewall than Microsoft's one-way. More serious was that my USB ports, including my media reader and Firewire, were not working. They were shown in the Device Manager, and Windows said they were working with no conflicts. Yet, if I put something on the USB port it was not read. I tried taking out the cards, rebooting, and then putting them back in, but that made no difference. So, after trying it that way, I deleted them from the Device Manager and rebooted. Upon starting up, Windows recognized there were new devices and reinstalled them. After that they worked fine.

It may be that I did had a problem but if so, it should checked itself and

not go through the process. I know there are some people having problems with it, but thankfully that is small. Microsoft offers a phone number for those who need help and cannot get online, call 888-772-4357.

The following is Rudy Wolf's process of installing SP2 from the CD we handed out.

I started at about 1:20 p.m.

The first activity was called inspecting, the next was performing an inventory. These seemed to take so long that I started to see how long each activity took on my computer.

At 1:30 it started to estimate space available.

At 1:34 it started to backup files (I left Norton AV on, so a couple of files took long enough so that the little AV window opened.

During this backup the screen went black for a few seconds but the backup continued.

At 1:48 it started installing files. Again, during this time the screen went black for several seconds but continued without problem.

At 2:08 it updated registry keys

At 2:08 it started finishing install. This included "running processes after install" and "performing cleanup."

At 2:19 a wizard window appeared with a Finish button and a

box that, if checked, would not allow Windows to restart.

At 2:19 I clicked Finish the Wizard window closed and nothing happened (at least not fast enough for me). I waited for a while and then initiated a windows restart using the Start button. After about 10 seconds, a dialog box opened informing me that an extraction program was not responding. I closed that program and when windows restarted, I got the blue screen of death, indicating that a driver (in my case umaxdrv.sys) was the cause of the problem. I no longer use my UMAX scanner, so I don't know why it would cause the problem since it is no longer active.

Anyway, I went through that twice to confirm that it was the same problem. I then used Go Back and restored my system to before the SP2 install.

I'm going to look to see where that UMAX driver is and see if I can get rid of it, then retry SP2 install.

The second time was the charm. However, in addition to being more patient at the end of the process I renamed the UMAX driver file before I started the second install.

The restart after install seemed to take forever. But this time I was patient and didn't interfere.

Often, the hijacker won't let you change your start page back to your preferred page. You might also notice a new "helper" toolbar added to your browser.

Another clue can be a changed search page. If you used to get MSN as your search page when you click the "Search" button but now some other page is coming up, you've likely been hijacked.

Some of the hijackers will load a page that looks like Google but isn't really Google—a particularly dastardly trick. Many will give unexpected search results. You may search for some innocent topic and get lots of results that lead to porn sites. If you search on "spyware" or the name of a hijacker program, the browser may either freeze up, or give you only benign results making it look like the hijacker program is a good thing.

Many folks who've been hijacked find that porn sites have been added to their favorites list. Some report pornographic files being downloaded. Some are being redirected to porn sites when mis-typing a URL (web address).

Other symptoms include pop-up ads even though you're running a pop-up stopper program. These pop-ups can appear more rapidly than you can close them and can freeze your system quickly. You may notice drastically reduced resources or messages that your system is low on resources or virtual memory. Or you may receive dramatically increased spam. Frequent lock-ups are a common complaint as is painfully slow performance.

Some of the hijackers can even disable your firewall, your anti-virus software or your spyware killers. Or they can prevent anti-virus software and spyware detectors from being updated.

In the past, we were safe from most Internet threats so long as we kept our anti-virus software updated and ran a firewall. Running Ad-Aware or Spybot Search and Destroy once a week or so cleaned up any spyware that had crept in but we never had much trouble. If we were smart enough not to download junk and not to open attachments, we were pretty safe. But times have changed and we must change our thinking too.

This recent rash of nasty stuff came in through a security hole in Microsoft Windows. Those who did not update Windows in a timely manner were sitting ducks for the Cool Web Search hijacker. From now on you must keep Windows up to date, especially with the so-called "critical updates."

Cure

The newest browser hijackers are particularly difficult to remove. You can try the following but be sure to follow the steps in order. If you don't know what you're doing, you should take the infected machine in to one of our local computer shops aIId let them fix it for you. It's possible to mess your computer up really badly while trying to remove a hijacker!

1. If you're running Windows ME, Windows 2000, or Windows XP, you must first turn off the system restore feature. Otherwise any problem you fix will just return when you reboot the computer. Search your Windows Help screens for instructions on how to disable System Restore for your version of Windows. Warning: You will lose all restore points you've previously made!

2. Download the Cwshredder tool from http://www.download.com

or any of the many sites that make it available. If you're infected with a hijacker, go to a non-infected machine to download your tools. Be sure you get the absolute latest version of Cwshredder since it is updated every few days. New variants of these hijackers appear at an amazing rate and you must have the latest Cwshredder to detect and clean them all.

3. Reboot your machine and run Cwshredder again.

4. Run Ad-aware. Be sure you update it first. If you don't already have Ad-aware, get it at http://www.lavasoftusa.com.

5. Reboot your machine and run Ad-aware again.

6. Run Spybot Search & Destroy. Be sure to update it first. If you don't have Spybot Search & Destroy, get it at http://www.safer-networking.org.

7. Reboot your machine and run Spybot again.

8. If everything seems to be clean now, be sure to turn Windows System Restore back on!

Don't let a browser hijacker ruin your tech-life! Keep Windows updated. Install and run a firewall. Install, keep updated and run anti-virus software. Install, update and run spyware cleaners. And encourage Congress to nail these hijacking jerks!

———

PC Annoyances Author Steve Bass

By Terry Currier

This is a collection of problems (annoyances) that many people have with their computer and computer programs. Steve states an annoyance and then tells you how to fix it. He separates the annoyances into seven chapters based on Email, Windows, Internet, Microsoft Office, Windows Explore, Music Video and CDs, and Hardware. For email, his annoyance is the person who replies to an email and includes all of the text from the previous message. I want to personally thank Steve for including that. I really hate seeing forwarding done through 10 different email addresses. For Outlook 2000 and 2002, click on Tools, Options and under the Preferences tab, select Email Options. Click on the drop-down list under "When replying to a message" and choose "Do not include original message." Please! He also lets you know of programs to help control spam getting into your email box.

Chapter 2: Windows

Something we need to know when Windows requires you to activate before you log on is that it looks at the file wpa.dbl, which logs your changes of components. Another great tip is adding Service Packs to your Windows CD.

Chapter 3: Internet

This chapter has good tips on the use of the Google search engine. One thing really worth getting is AM-DeadLink which you can download from
http://www.oreilly.com/pcannoyances

It looks at the Favorites you have saved and will go out and check to see if they are still live so you don't have to.

Chapter 4: Microsoft Office

If you use certain documents over and over again, go to page 84. This tip is one of the best for creating a work menu in Word that stores the documents you use the most. It's like having a favorites menu.
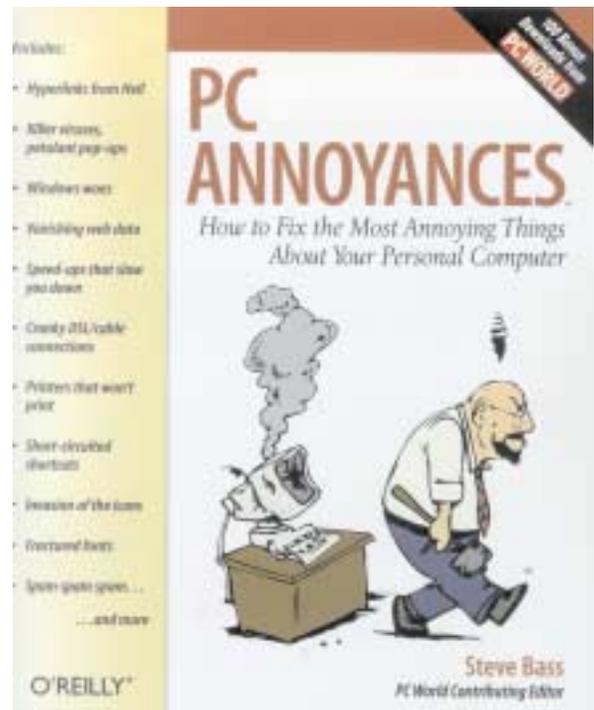
Chapter 5: Windows Explorer

Yeah, I use it when I have to. There are better browsers. Steve (and I) like PowerDesk from V Communications. The ease of use in changing the sort alone is worth the price. You can download a free version from the above web link.

Chapter 6: Music, Video, and CDs

Hey, did you ever have a set of songs you were listening to where one is real loud but the next is soft? Steve tells you there is a way to fix the problem by normalizing the volume as you play the music. Look under View, Enhancements, Cross-fading, Auto Volume Leveling.

Chapter 7: Hardware

The chapter has tips on trying to quiet down your computer and transferring phone numbers from Outlook to your digital phone, among others.

Steve gives good information with humor. He lists a lot of different software to enhance your computer experience. The book is the type you can use as a reference to check on why something is not working right. Well worth the money.

PC Annoyances $19.95 at
http://www.oreilly.com/catalog/pcannoy/

You can also catch Steve at the North Orange County Computer Club meeting Sunday, September 12, 1:00 p.m. at Chapman University.

Gadgets for Geeks

By Sherry Zorzi
Cajun Clickers Computer Club, Louisiana.

They say the only difference between men and boys is the cost of their toys, but the toys for gadget-geeks of any age or gender just keep getting better and, surprisingly, cheaper.

USB Flash Drive: These tiny solid-state devices are quickly replacing diskettes as the cheap and easy method for transporting or backing up data. A 256 megabyte flash drive will hold the equivalent of about 175 diskettes. That's about 3 hours of music or 1000 photographs, or thousands of common business documents – all in a $40 device the size of a Bic lighter.

Flash Watch: These watches include a built-in flash drive device. Just connect the watch to your USB drive via a built-in cable. Cost: under $100. Cool-factor: priceless.

Camera Phone: The trend these days is to go totally cellular. My new Motorola flip-phone (about $80 after rebate) has a camera, calculator, appointment book, voice recorder, alarm clock, text messaging, wireless web, games, and email. The sleek profile fits in any pocket or bag easily. Cellular coverage is getting better every year and service is becoming increasingly affordable.

Handheld Computer: Pocket PCs and Palms have been around for a long time, but the newest generation of both devices are slicker than ever. More than just a personal information manager, these tiny computers now include word processing and spreadsheet capabilities, play MP3 music files, handle multimedia and Internet connections, in some cases even play full-length movies. You'll pay about $200 at the low end and over $1,000 at the high end for a computer more powerful than the desktop of a few years ago that fits in your pocket.

Digital Camera: The novelty has worn off digital photography now. These cameras have improved so dramatically in quality and have become so affordable that they barely qualify as gadgets. The average digital camera today has 3-4 megapixel quality with 3X-5X optical zoom and will cost under $300. Mine goes everywhere with me. Within a minute of snapping a shot I can email it to a friend or upload it to my favorite photo-sharing website.

Satellite Radio: There are two flavors – XM Radio and Sirius. I've only tried XM, but all I can say is, "Wow!" Commercial-free music of any genre you desire – any time you want it. A scrolling digital display tell the title and artist of each tune, so no more sleepless nights trying to remember who sang that song that's been rattling around in your head all day. You can install XM Radio in your car and have an optional cradle in the house, making one subscription portable from home to road. Hardware is around $100.

MP3 Player: These music machines, of which the Apple iPod ($200-300) is the most recognizable brand, allow you to store many hours of music in a tiny portable device.

GPS: Portable global positioning systems use satellites to pinpoint your location to within one meter. Handheld devices are available or you can buy GPS add-ons to handheld computers. These are popular with hikers and sailors, but are also fun when traveling by car or to use in hobbies such as geocaching. A decent recreational GPS device can be purchased for $100-200.

Wireless Laptop: Intel's new Centrino technology combines integrated wireless LAN capability, improved battery life, and thinner, lighter design to make laptop computing what I always dreamed it would be. Imagine a laptop computer less than an inch thick and weighing less than 3 pounds. Add to that the ability to connect wirelessly to the Internet from thousands of "hotspots" around the country, including airports, coffee shops, even downtown Baton Rouge. That's a laptop to love, priced between $1,000 and $3,000.

No matter your age, gender, interests, or budget, there's a gadget somewhere for you to drool over. It's never too early to start making your Christmas wish list.

———

September 11   9 a.m. to 12 noon
Orange Coast College
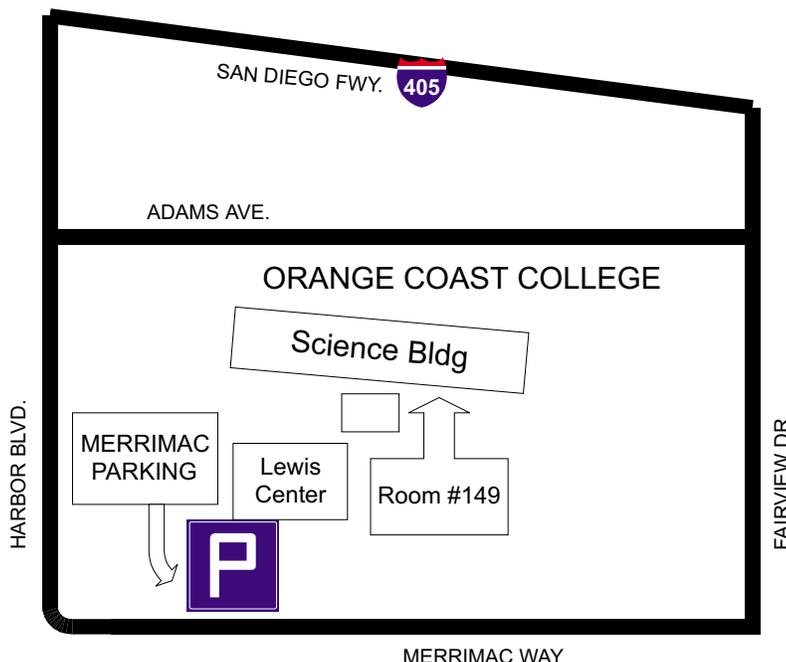## Science Building Room #149

Ritek - Advanced Media

Advanced Media is a subsidiary of RITEK Corporation, the world's largest optical media manufacturer. They just announced that they have begun production for a new double-layer DVD+/-R medium. The single-sided disc has 8.5GB of storage capacity—enough for up to four hours of DVD-quality video, 16 hours of VHS-quality video, or over 120 hours of MP3 audio. Compatible with all current DVD video players and DVD-ROM drives as well as new DVD+/-R DL drives, the disc is ideal for virtually any business or household application.

The Advanced Media RIDATA brand currently includes: CD-R/RW, DVD-R/RW, DVD+R/RW, DVD-RAM, flash cards and USB EZ drive.

RIDATA EZ Drive (USB Flash Drive) is a thumb-sized portable storage device that can store your essential data. The USB plug & play makes connecting to your desktop or notebook much easier. No power supply and no external cables are required.

SAN DIEGO FWY. **405**

ADAMS AVE.

ORANGE COAST COLLEGE

Science Bldg

HARBOR BLVD.

MERRIMAC PARKING

Lewis Center

Room #149

FAIRVIEW DR.

P

MERRIMAC WAY

PIG SIG:

After the meeting we will go to Niki's Indian Food at 3705 Bristol Street in Santa Ana. Rebecca Feinstein said the food is good, fairly inexpensive and there is something for everyone.