BAY BYTES

Greater Tampa Bay Personal Computer User Group, Inc.

Newsletter

Issue 6 June 2012 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/

Has Your Browser Been Hijacked?

By Bob Rankin

http://askbobrankin.com/has_your_browser_been_hijacked.html#ixzz1rZGm0VLd

A reader asks: Every time I open my browser, it goes to an unfamiliar search engine page, and when I search from the toolbar, it no longer uses Google. Was my browser hijacked somehow? If so, how do I get my settings back to normal?

Web Browser Hijacking

If your Internet Explorer, Firefox or Chrome browser suddenly behaves in unexpected or undesirable ways, it may have been hijacked. Browser hijacking is an attack by malicious software that changes your Web browser's settings. Some users who have been hijacked report popups or having searches redirected to pages for online casinos, weight loss products and even porn sites.

Here are some other symptoms that indicate you've been hijacked, and how to fix it ...

- Browser home/start page changed to an unwanted site.
- New favorites, bookmarks, toolbars, or desktop shortcuts that you did not add.
- Typing a URL into the address bar and being taken to some other URL instead
- You default search engine has been changed
- Inability to access certain sites, particularly anti-malware sites that might help you
- Your Internet security settings have been lowered without your knowledge
- Endless pop-up ads for things you don't want to see
- Sluggish computer response; malware often slows your whole system down

How does hijacking happen?

In many cases, the hijacking software is something you downloaded and installed, thinking it was something beneficial. Many hijack programs are written in ActiveX for Internet Explorer, so be very leery of requests to install ActiveX components. Other hijackers are buried in toolbars, add-ons, and even fake anti-malware programs.

Continued on the next page

See my related article on Fake Anti-Virus and Celebrity Scams to learn more about how some people are being tricked into installing malware. A hijack is not necessarily malevolent, some are just annoying. One example in this category is the Ask.com toolbar, an insidious annoyance that somehow keeps taking over the search functions of the browser on one of my home computers. But even if there's no malware, per se, you're still better off getting rid of these unwanted browser parasites.

Getting Back to Good

If you believe your browser has been hijacked, shut down your browser immediately. If you cannot close the browser in the usual way, press Ctrl-Shift-Esc to access Windows Task Manager, highlight your browser's file name in the Processes column (iexplore.exe, firefox.exe, chrome.exe) and click "end process" to close the browser.

Hijackers are one reason it is vital to have real-time anti-malware defenses in place at all times. If you're already running internet security software, obviously it didn't protect you from this particular menace. If the problem happened recently, System Restore may "undo" the problem and get you back to normal.

If that doesn't do the trick, reboot your system in Safe mode "with networking." This will load Windows with the minimum of startup options, hopefully omitting the hijacking software. You will need the network connectivity to download some anti-malware utilities. Then open your browser again.

Download one of these Free Anti-Virus Programs or another free anti-malware utility such as MalwareBytes Anti-Malware. Install the software and run a full scan on your system. Delete any suspected malware that it finds. Empty the Recycle Bin and reboot in normal mode.

Open your browser and put things back in order. Review and reset your home page, security settings, privacy settings, etc. Delete any unwanted favorites/bookmarks. Review the list of add-ons and uninstall any that look unfamiliar.

But Wait... There's More!

You're not done yet. Hijacking malware also likes to mess with registry settings.
See my list of Free Registry Cleaners to remove bad registry entries and close security holes in the registry.

The HOSTS file is another favorite target of hijacking software. The HOSTS file contains pairs of host names and their associated IP addresses. When a host name listed in the HOSTS file is requested by your browser, Windows directs the request to the associated IP address instead of looking up the host name in the DNS system. Hijack software may add entries to the HOSTS file so that certain sites are blocked or redirected to unwanted sites.

The HOSTS file is located at C:\WINDOWS\SYSTEM32\DRIVERS\ETC\HOSTS and can be opened with Notepad or your favorite text editor.
On Vista or Windows 7 you may need to open your text editor by right-clicking, then select "Run as Administrator". Make sure the HOSTS file includes ONLY the line "127.0.0.1 localhost" and any other pairs that you know you added yourself. Delete unwanted entries and save the HOSTS file.

To avoid browser hijacking, use real-time anti-malware defenses; don't give unknown websites permission to install software, toolbars, or ActiveX controls; and keep your browser's security settings on medium or high level.

If you've been hijacked, tell us how you fixed the problem. Post your comment or question below...

http://askbobrankin.com/has_your_browser_been_hijacked.html#ixzz1rZGm0VLd

Why does e-mail bounce? By Leo A. Notenboom

Email can bounce for many reasons. I'll look at several of the most common mail bounce messages, and try to interpret what they really mean.

Well, I'm afraid that there are *many* reasons why mail could bounce. In fact, there are so many ways how it could fail that sometimes I'm amazed that it works at all. But it definitely works most of the time, and one of the ways that it works is that very bounce message that you get.

You see, there's gold in that bounce message. It's not only telling you that your message didn't go through, but if you look a little closer, you'll see it's trying to tell you why.

Bounce messages can vary in format and in exact wording, depending on the mail server that's sending the message back to you. Different types of mail servers use different terminology. Some are quite geeky and difficult to understand. Others seem to take five paragraphs to tell you that you probably just mistyped the email address that you were sending to.

What I'll do here is list some of the most common messages, what they mean, and what you can do. Remember, though - a message that you get may not be worded *exactly* as I list it here. You'll have to look carefully at the bounce message that you receive and see which of these it's most like.

Examining a bounce

First, let's look at a couple of bounce messages. Buried in the all the geekery, I've highlighted a couple of important things:

```
    ----- The following addresses had permanent fatal errors -----
<somewhere@example.com>
     (reason: 553 sorry, relaying denied from your location [10.10.10.10] (#5.7.1))


    ----- Transcript of session follows -----
... while talking to smtp.example.net.:
>>>> DATA
<<< 553 sorry, relaying denied from your location [10.10.10.10] (#5.7.1)
550 5.1.1 <somewhere@example.com>... User unknown
<<< 503 RCPT first (#5.5.1)
```

Here's a bounce from another mail server which attempts to be more friendly:

```
Hi. This is the qmail-send program at example.com.
I'm afraid I wasn't able to deliver your message to the following addresses.
This is a permanent error; I've given up. Sorry it didn't work out.
```

Continued on the next page

```
ere@example.com>:
10.10.10.10. does not like recipient.
Remote host said: 550 MAILBOX NOT FOUND
Giving up on 10.10.10.10.
```

The messages "MAILBOX NOT FOUND" or "User unknown" are key and might actually be any of several different messages depending on the reason for the failure.

Common error messages

Mailbox Not Found, **invalid mailbox**, **User unknown**, **not our customer**: these are all saying pretty much the same thing. In the "someone@example.com" bounce examples above, the mail server "example.com" doesn't have an account for anyone with the email name "someone". A couple of common reasons:

- You typed the email address wrong. The single most common reason this error happens is simply that you made a typographical error in the email name. Check the entire email address for an error.
- It's an old email address that's no longer in use. Perhaps the person that you're attempting to email has changed their email address and you're using an old one which is no longer valid. Make sure that what you're using is up to date.

Mailbox unavailable: Nine times out of 10, this is the same as "mailbox not found." That other 10% of the time, it could mean that there's a problem with the recipient's email account. What kind of problem is hard to say. Check to make sure that you have the email address correct, wait a while, and try again; if it still bounces, try contacting the recipient some other way.

Mailbox full, or **Quote Exceeded**: sometimes this will show up as a part of a "Mailbox unavailable" message. It's fairly clear, though: your recipient has too much email and their server isn't accepting any more. This is common with services that have limits on how much mail you can accumulate. This can also be a sign of an abandoned account - someone's stopped looking at and cleaning out the email. In any case, you'll need to try and contact your recipient through some other email account, or some other way.

Host unknown, **Domain Lookup Failed**: this means that the mail server that you're attempting to use, the "example.com" part in the examples above, doesn't exist. A common reason is again, a typo on your part. Make sure that you typed it in correctly. Another reason is the ISPs that change their name. The largest example of this in recent memory has been "attbi.com" changing their name to "comcast.com". Anyone trying to send to an old "attbi.com" email address might get this message in return.

Unable to Relay: this is a terribly obscure error message, but also becoming more and more common as ISPs try to crack down on spam. Mail is sent by relaying email from one server to the next. There could be many servers involved, but typically, it's the mail server at your ISP relaying your email to the mail server at your recipients ISP.

In general, a mail server must "know" either the sender of an email, or its recipient, in order to safely transmit mail. Mail servers that do not enforce this requirement are called "open relays" and can be exploited by spammers to send out tons of spam.

Continued on the next page

Things get complicated because not all ISPs agree on what it means to "know" the sender of an email. All of these *might* result in an "unable to relay" message, depending entirely on the servers and ISPs involved:

- The From address might not match an account on the email server.
- The ISP might require that email comes via a connection (dial up or DSL) actually provided by the ISP - sending someone else's connection might not be allowed.
- The ISP might require you to authenticate before sending email and you haven't.
- A mail server somewhere could be misconfigured.

There's no blanket answer if "unable to relay" happens only occasionally. Double-check the email address that you're sending to, for starters.

Temporary Errors: errors like "no adequate servers", "Connection Timed Out," "Resources temporarily unavailable," and "Out of memory" all typically indicate a problem with a mail server that you probably don't have any control over. They are, in general, temporary, and should resolve themselves over time. *Look carefully at the bounce message*; the email server involved may continue to automatically try to deliver your email without any action required on your part.

Blacklist Filters: If you see messages that indicate your email was "blocked," or "listed in," and references to sites that have things like "spamcop," "dynablock," "blackhole," "spamhaus," and similar in their names, then your email was probably intentionally blocked because the receiving system thinks your ISP's mail server is a source of spam.

Various blacklisting services try to identify servers which are sources of spam. They then make that list available to ISPs, who in turn can block email coming from these sources. The problem is that criteria for addition and removal from these blacklists is vague, at best, and getting a server removed from blacklists can be very difficult. If this happens to mail that you send, get in touch with your ISP and explain that their server may be on a blacklist somewhere, and then try to use a different email address, or a different email account of your own, to contact your intended recipient. You might also tell your recipient that their ISP is improperly blocking legitimate email.

Content filters: Much like blacklists, content filters are an approach that many ISPs now implement to stem the tide of spam for their clients. Most will simply discard email that looks like spam, as I discussed in Why is my mail to this person not getting through?, but some servers will actually send a bounce. Phrases in the bounce message like "Message looks like spam," "Keywords rejected by the antispam content filter," "Scored too high on spam scale," and similar means that your email, for whatever reason, tripped the spam filters on the receiving end. Your email looks too much like spam.
What does it mean to "look like spam"? Here, again, things get vague. That definition will vary greatly based on how your recipient's email server has been configured. Obvious possibilities are the use of pornographic words or phrases, HTML formatted email, currently popular drugs being hawked by spammers, or even having something that looks too much like a sales letter or a scam. The best approach is to scan the bounce for any clues (sometimes there's more information), and then validate your recipient can get any email by sending a simpler message. Assuming that all works, then re-work your message as best you can to not look like spam.

Continued on the next page

How long is "a while"?

One of the most common solutions for just about any bouncing email problem (after checking that you're sending to the right address) is to "Wait a while and try again." The email system, while somewhat random, is also somewhat self-healing. If there's an email server with a problem, chances are it'll get fixed or eventually bypassed, especially if it belongs to a larger ISP. For temporary problems, as noted above, email servers will typically keep trying for up to four days before giving up.

My rule of thumb for trying email again is "one hour, one day, one week." In other words, try again in an hour. There are classes of problems that will resolve themselves that quickly. If that still fails, then I'll try again the next day. If that still fails (and my message can wait that long), I'll try again in a week. If that still fails ... I need to find another way to get my message to my recipient.

When a bounce isn't really a bounce

Be careful! There's a class of viruses these days that propagate by "looking like" bounce messages. They instruct you to open an attachment for more information. **Don't.** Especially if you don't recall sending the message in the first place. Don't open any attachment, especially one accompanying what looks like an email bounce unless you are *absolutely positively certain* that it's legitimate.

You may also be getting bounce messages for email that you didn't send. There's another class of virus that "spoofs" or fakes the From address on email messages; as a result, you could be getting bounce messages that have nothing to do with you. This scenario is sadly common and I've written about it in a separate article: Someone's sending from my email address! How do I stop them?!.

Everything bouncing?

Finally, if *every* email that you send bounces, then you probably have a different problem. Chances are your email client is misconfigured. Double-check outgoing or SMTP server settings and double-check with your ISP to ensure that you have them set correctly.

Is Your Internet Security up to Date?

Antivirus up to date?

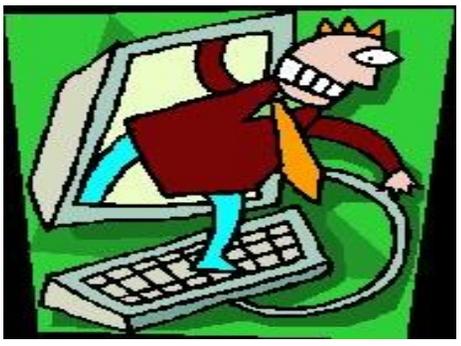
Firewall?

Windows up to date?

Spy Ware?

See how to protect your computer at:

http://gtbpcug.org/protect/



More about Internet Threats

Is Google Compromising Our Privacy?

By Sandy Berger, CompuKISS

www.compukiss.com

sandy (at) compukiss.com

Recently Google announced consolidating the privacy policies for all of its services. These include about 60 different services like the popular Google search engine, the Google-owned YouTube video website, Gmail, and the Android operating software for mobile phones. Because of the scope and popularity of these services, this move got the attention of everyone from state and federal representatives to advocacy and security groups. But more than anything else, it left consumers with a throbbing headache as they pondered how this would affect them and if they should be concerned enough to stop using Google services.

Data-protection agencies and lawmakers around the globe requested Google delay this implementation so they could review the new procedure but Google did not comply. The new privacy policy went into effect March 1, 2012.

Although Google states that this new privacy policy is aimed at making Google services easier to use, it doesn't take a rocket scientist to figure out that their primary aim is to target users with advertising that is relevant to their interests, making Google's ads more valuable. The aggregation of information from different areas enables Google to target the interests of their users more accurately.

Continued on the next page

For instance, if you search for gardening information with the Google search engine, play videos of how to plant seeds on YouTube, and get brochures of the latest horticultural offerings in Gmail, Burpee and other seed and plant companies may be willing to pay Google more to blanket you with their ads.

If you are interested in gardening you might actually be happy to see ads for gardening tools and seeds, but this is not really the point. The point is that we are putting private information about ourselves in the hands of others. The problem lies in two areas.

First are the unintentional consequences. As we recently saw in the proposed SOPA and PIPA legislation, even acts made with the best intention can backfire creating more harm than good. When you add that to the fact that technology is moving at the speed of light, we are becoming more and more data-dependent, and new ways to manipulate data are being invented every day, it gets a little scary.

Second, and possibly even more disturbing, is that power and money can corrupt even the most honorable people and companies. History tells this story over and over again. Google's informal corporate motto is "Don't be evil." Yet it was recently found that Google was circumventing the users' privacy settings in the Safari web browser. Even though the Safari browser was set to refuse tracking cookies, Google was adding hidden code that allowed it to implement browser cookies from third-party ad sites that Google operates. When this was made public, Google stopped the practice. But, other devious practices could be revealed or be implemented in the future. Believe me, this is only the tip of the iceberg.

Although Google's current proposed aggregation of data may be somewhat benign, what it will empower them to do in the future is problematic. With the use of data from mobile devices Google will be able to track our physical locations and actions. With data from our consolidated online profile they may be able to foresee our every move.

If you want a prediction of what this type of unseen tracking can do, check out the movie called "Antitrust." It was produced in the year 2000 when Microsoft was the big, bad, corporate entity. It shows what can happen when a company gets too much power, too much technology, and too much money. When you watch the movie, remember to add ten years of technology to the mix. In the year 2000 they didn't have the mobile technologies and data-tracking capabilities that we have now. If you watch this movie and really ponder how large and powerful Google has become, the throbbing in your head may become a much larger headache.

What the Summer Portends in New Tablets

http://www.computerworld.com

By **Matt Hamblen**

Apple, Google, Microsoft and Amazon expected to launch new models in coming months

Matt Hamblen, May 10, 2012 (Computerworld)

Summer 2012 promises to be the season of tablet experimentation on a grander scale than ever.

Just about every tablet maker, including Apple, is rumored (or expected) to announce (or launch) a new tablet version within roughly the next four months. The devices are likely to be smaller in the case of Apple and bigger in the case of Amazon.

Google is expected to announce an inexpensive tablet with hardware maker Asus at the Google I/O conference in late June, while a Windows RT tablet from Microsoft and new-found partner Barnes & Noble could be on tap for late summer or fall.

With so many different reports of new tablets surfacing, it's time to take stock of what's coming.

To begin, here are some general themes seen by analysts for what's coming in the next quarter:

Apple will grow stronger, even with new competitors like Microsoft. That's not a hard conclusion to reach, since Apple took 59% of the global tablet market in 2011, according to IDC, which expects Apple to dominate the tablet market through 2016, at least.

Google will attempt to regain control of a pure Android tablet. Having seen Amazon, with its Kindle Fire, and Barnes & Noble, with the Nook tablet, selling forked versions of Android that lessen dependency on Google services and apps, the company will want to step up its control over the mobile operating system it created. More vendors will lower the prices of their tablets to compete with the $200 Kindle Fire and the Nook.

More LTE-based tablets will emerge, offering faster wireless connections, even though customers currently prefer Wi-Fi-only models. A move to LTE will become even more likely once wireless carriers announce shared data plans, possibly this summer, that enable users to share smartphone and tablet data, possibly even across a workgroup or a family.
Tablet sizes will vary widely, with touchscreens ranging from 7 to 13 inches diagonally, although a 10-in. form factor will be dominant. The iPad has a 9.7 in. screen.

Here's what's on tap for this summer, in order of likely timing:

This month: Barnes & Noble and Amazon have already kicked off new TV ad campaigns for their current Nook Tablet and Kindle Fire models -- both of which have 7-in. touchscreens. They're hoping to appeal to people shopping for graduation gifts and to clear out inventory to make room for forthcoming models, analysts said.
May or June: Amazon is expected to launch a tablet that's larger than its 7-in. Kindle Fire, but IDC analyst Tom Mainelli said it's not clear whether it will be a 9.7-in. or 8.9-in. device.

Late June: In an announcement that will probably take place at Google I/O, Google is expected to unveil a $200 tablet called Google Play that will run Android 4.0 (Ice Cream Sandwich) using a Tegra 3 quad-core processor.

Continued on the next page

The Google Play would be built by Asus, possibly co-branded with Google or purely branded as a Google product. Its biggest distinction would be that it runs plain vanilla Ice Cream Sandwich, not the versions of Android seen in the Nook and the Kindle Fire.

August: Dominant tablet maker Apple is expected to launch a smaller version of the iPad, according to reports in Digitimes and elsewhere on Wednesday. These reports say the smaller iPad will be a 7-in. model, although Mainelli said it could be 7.8 in., just shy of two inches smaller than the current iPad.

Mainelli said the reports of a smaller iPad have credence. A smaller iPad, he said, "will help Apple gain traction in regions [like Japan] where the 9.7-in. tablet has been slower to take off because consumers think it's too big."

A smaller tablet would also enable Apple to offer a tablet at a lower price, possibly in the range of $299 to $349, while still maintaining to its historically high profit margins, Mainelli added.

"Once Apple owns every price point, from $299 to $829 [for the 64GB new iPad with Wi-Fi and 4G LTE connectivity], it's going to be very, very difficult for Android tablets and Windows 8 and Windows RT tablets to compete with Apple," Mainelli said.

Even today, Apple's prices have come down, with the 16GB, Wi-Fi-only iPad 2 model selling at $399, Mainelli added. That level of pricing is attractive to "cash-strapped consumers as well as educational buyers, who are embracing the iPad in a major way in some regions," he said.
By late summer, Microsoft is expected to make clear its plans for Windows 8 and Windows RT tablets, even if the devices don't ship until fall or later. Any announcement on that topic is expected to clarify whether Barnes & Noble and Microsoft, who recently became partners, will cooperate on a Windows tablet.
Also this summer, wireless carriers, such as Verizon Wireless and AT&T, are expected to provide more options for data packaging, where one monthly data plan would cover service across multiple devices, such as a tablet with a smartphone. That kind of data packaging could open up interest in LTE-ready tablets, offering the promise of faster video streaming and browsing.

Mainelli said Verizon is reported to be the first to offer such a data package. An AT&T executive at the CTIA conference also said tablets that combine Wi-Fi and LTE for an affordable price are in the planning stages. AT&T sold out of its Pantech Element tablet, a Wi-Fi-and-LTE device with a price tag of $399. Today, an iPad with LTE and Wi-Fi costs $130 more than a Wi-Fi-only model, not including the cost of a monthly service plan.

"Once carriers start offering the ability to use one data plan across multiple devices, then LTE on tablets become very interesting," Mainelli said. In addition to whatever new tablets may be announced in the coming months, there are other notable tablets that we know will begin shipping over the summer. They include the Toshiba Excite, the largest tablet at 13.3 in. and 2.2 lbs. It will go on sale June 10, starting at $650 for a 32GB model. It runs Android 4.0 and uses an Nvidia Tegra 3 quad-core processor.

While it's uncertain how well such a large tablet will sell, analysts agree that the Excite 13 is a sign of a fairly staggering amount of diversity in the tablet market.

The lighter Side

Acceptance Testing www.worldstart.com

Two young engineers applied for a single position at a computer company. They both had the same qualifications. In order to determine which individual to hire, the applicants were asked to take a test by the Department manager. Upon completion of the test, both men missed only one of the questions.

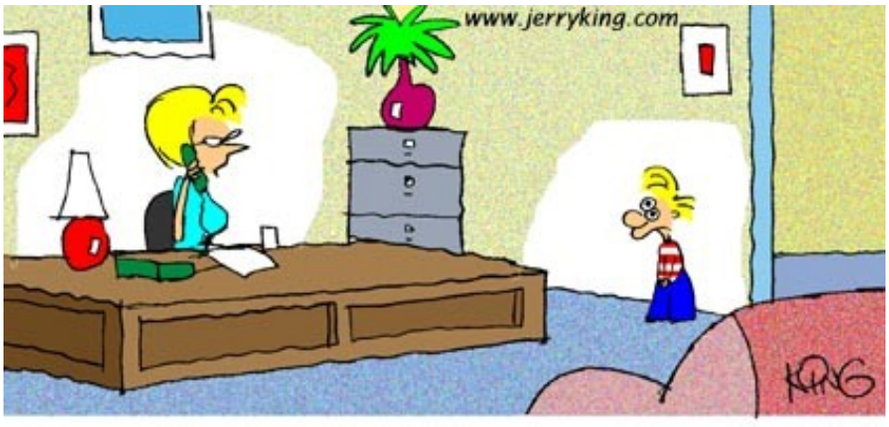
The manager went to the first applicant and said, "Thank you for your interest, but we've decided to give the job to the other applicant."

"And why would you be doing that? We both got nine questions correct," asked the rejected applicant.

We have based our decision not on the correct answers, but on the question you missed," said the Department manager.

"And just how would one incorrect answer be better than the other?" the rejected applicant inquired.

"Simple," said the Department manager, "Your fellow applicant put down on question No. 5, 'I don't know.' You put down, 'Neither do I.'"



"I'm sorry, but our Webmaster is currently unavailable. He has to go potty."

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