http://www.tpcug.org

Bits of Blue

A Monthly Publication of the Tampa PC Users Group, Inc.

February in Tampa

Vol. 28 No. 2 February 2015

Meeting

Windows 10
by
Bob LaFave

Wednesday, February 11, 2015

6:30 PM

Pepin Distributing Co.
4121 N 50th Street
Tampa, Florida

INSIDE THIS ISSUE

Meeting Preview 1
Editor's Comments 1
Minutes 2
Taming the Password Beast 3
Picture of the Month 5
Links 5
Where is the Linux Desktop? 6
Map 8

Meeting Preview: Bob LaFave will demonstrate how to install Windows 10 Technical Preview. Bob LaFave will also conduct the usual Windows SIG for the first 30 minutes of the meeting.

Editor's Comments

By William LaMartin, Editor, Tampa PC Users Group
william@lamartin.com

It is nice to be able to welcome Dave Palmer as a contributor to the newsletter. He certainly knows a lot more about passwords than I. And I look forward to more articles in the future. Merle Nicholson has also been helpful in providing an article to fill out the newsletter so that all I need do is make a few comments.

Compared with last month, I have no problems to report. But I do have a complaint about what is happening at major and not so major websites. When I go to websites such as the New York Times and The Wall Street Journal, quite reputable organizations, I am amazed at all the processing my computer is doing. You can monitor this in the Task Manager's Performance tab. To see the actual traffic between your computer and the website, you can install the free program Fiddler and run it while visiting websites. You will be shocked at the volume.

In the first 15 seconds, the NY Times site's server had sent out

Comments........Continued on page 2

March Meeting: To be announced

* * OFFICERS * *

President: John Witmer (president@tpcug.org)	949-8007
Vice President : Kevan Sheridan (kevan@tpcug.org)	988-6480
Treasurer: Doug Mullis (dmullis@tampabay.rr.com)	234-9343
Secretary: Merle Nicholson (merle@merlenicholson.com)	879-3602
Member at Large: Ron Weinberg (rswjbr@verizon.net)	960-4132

APPOINTED (Volunteers)

Editor: William LaMartin (william@lamartin.com)	251-3817
Programs: Doug Mullis (dmullis@tampabay.rr.com)	234-9343

Home Page http://www.tpcug.org

Bits of Blue is published by the Tampa PC Users Group, Inc., a State of Florida registered non-profit corporation, to provide educational information about personal computer systems to its members. Our mailing address is P. O. Box 3492, Tampa, FL 33601-3492.

However, for business concerning this newsletter, Bits of Blue, please contact the Editor, William LaMartin, at 813-251-3817, or william@lamartin.com.

Technical information found in this publication is not necessarily compatible with your hardware and software, plus other errors or misprints could occur from time to time. Therefore, the use of programs, commands, functions or anything of a technical nature appearing in this publication will be at your own risk.

RENEWING YOUR MEMBERSHIP?

WE CERTAINLY HOPE YOU WILL

MAIL YOUR CHECK AND ANY
ADDRESS OR NAME CHANGES TO:

TAMPA PC USERS GROUP
PO BOX 3492
TAMPA, FL 33601-3492

$25 Individual $35 Family
$60 Corporate = 3 employees + $20 each add’l employee

Go to our web site http://www.tpcug.org and click on the About Us | Join link to join or renew online

Check the address label for your renewal month

Friend of the User Group

We acknowledge
Pepin Distributing Co.
for their support

Affiliations

Florida Association of User Groups

Association of Personal Computer User Groups

Minutes of the January Meeting

By Merle Nicholson, Secretary,
Tampa PC Users Group
merle@merlenicholson.com

The Windows Special Interest Group (SIG) opens our monthly meeting. The SIG moderator, Bob LaFave, introduces new or little-known products and technological developments for discussion by the group. He accepts questions and requests for help in solving problems from attendees. Bob covered a wide variety of PC subjects, starting with his new notebook computer with Windows 8.1 and touchscreen. He talked about an external USB FAX modem and the software “Windows FAX and Scan,” reassuring us that Windows 8.1 still has it included as standard.

He showed us what the Start-8 menu system for Windows 8.1 looks like and how to get it as a download. Last he led a discussion on a member’s problem with lack of sound while using Firefox.

Dave Palmer gave us a very comprehensive presentation on passwords and what criminals do to attack users and best practices on prevention. Since the presentation is included in this newsletter, we’ll just thank Dave for an excellent program, well-organized and thoughtful. It’s clear that Dave worked very hard and long putting this together and we’re the grateful recipients. ◆

Comments.......Continued from page 1

just over 200 http requests to various places, probably a little over 50%, of course, to the NY Times site itself. But the rest are to places such as ad.doubleclick.net, ckm-m.xp1.ru4.com, beacon.krxd.net, r.flite.com, b.scorecardresearch.com. And the list goes on. The Wall Street Journal is just as bad. The site of the New Orleans newspaper, the Times Picayune, produced over 1,000 http requests in the first 15 seconds. And it didn’t stop once the page was loaded. Periodically, another large batch would arrive. It is no wonder that,

Comments........Continued on page 8

Taming the Password Beast

By Dave Palmer, Tampa PC Users Group
dkp205@hotmail.com

In recent years cybercrime has become a growth industry. The tech-savvy criminals began developing and selling crimeware tools. Now it seems anyone who can operate a keyboard can buy a do-it-yourself malware kit for less than $100. Hacking into websites and stealing data has become a favorite, and lucrative, pastime.

But some of the data stolen was encrypted - usually passwords. How to decrypt, or “crack"”it? Cybercrime newbies found the necessary tools and how-to help forums on the web. Now they're off to the races.

Once a database of passwords is stolen, the criminals need to operate quickly – before the breached website discovers the data has been stolen and notifies users to change their passwords.

What do the hackers need?
Above all they need to work fast, and that means working smart. They need big lists of commonly used passwords like "LetMeIn" or "Password1" or "12345678." They need lists of words (called wordlists) commonly used in passwords. And they need to understand common password patterns. No problem, all those items are available online – usually for free. Did you know entire forums exist online to share stolen passwords and to assist in cracking them? In addition YouTube has many self-help videos aimed at new criminals and “password recovery specialists.”

Wordlists exist in many places on the Internet. Wordlists exist in multiple languages and can contain every word in Wikipedia, every word in Webster’s dictionary, first names, last names, sports teams, pet names and much more. Check out openwall.com/wordlists/. This paid wordlist has 40 million entries and contains commonly used passwords from 20+ languages. This database is 500MB in size. Another wordlist available at Crackstation.com contains nearly 1.5 billion words and is available for free or for a small donation.

RockYou changed everything
In late 2009 a gaming website called RockYou was hacked. It contained 14 million unique passwords. Unfortunately they were not encrypted; they were in plain text. Both legitimate security specialists and criminals quickly analyzed this treasure trove. Many common password patterns were discovered. This analysis changed password cracking forever.

Analysis of the RockYou passwords confirmed that nearly all capital letters come at the beginning of a password and almost all (90%) numbers and punctuation come at the end. Many other common patterns were revealed.

Password-cracking software is surprisingly easy to find, and often free. Several popular titles include John the Ripper, Cain & Able, Brutus, and oclHashcat. Most come with “rules” to test various patterns against a password database.

Rule-based attacks always begin with a wordlist. They can combine words, append endings, prepend beginnings and test common substitutions – like substituting 3 for E, 5 for S, 1 for L, etc. A rule, known as a "combinator" attack, runs two or more words together and either strips out all the spaces or leaves them intact. Other "mangling" and "hybrid" rules account for variations in capitalization, character substitutions, and other tweaks.

The cracking process
Experienced password crackers will begin by testing the database against a large list of common passwords (12345678, or Password1). Often that process alone will crack 15% – 20% of the passwords. The next step is to use a comprehensive wordlist to test dozens of password patterns (rules). Again a 15% – 20% success rate is possible. The last resort is to use a “brute force attack” to test every possible password combination for a specific number of characters: aaaaaaaa, aaaaaaab, aaaaaaac to zzzzzzzz.

Following Moore's Law, the power of computers is increasing quickly. In fact, performance of computers roughly doubles every 2 years. (www.mooreslaw.org/) Along with it, the ability of bad guys to “guess” or “crack” passwords is increasing too. (http://ow.ly/pkgvW) Expert crackers have learned to utilize the power of graphics cards, also known as GPUs, such as the AMD Radeon 7970 to boost the performance of their computers. During the recent presentation Merle added that this particular card has a total of 2048 processors on each card (!) and can run at the blazing speed of 6,000 GHz! It is capable of running billions of calculations (not guesses) per second. I believe that translates to around 8 million password guesses per second.

Why are longer passwords better?
Without getting too deep into the math, let me explain briefly why longer passwords are better. Imagine a 2-char-

Password.........Continued on page 4

Password.......Continued from page 3

acter password that is limited to numbers. Since each character can be any one of 10 possibilities (0-9), the number of combinations for a 2 character password is 102 or 10 x 10 = 100.

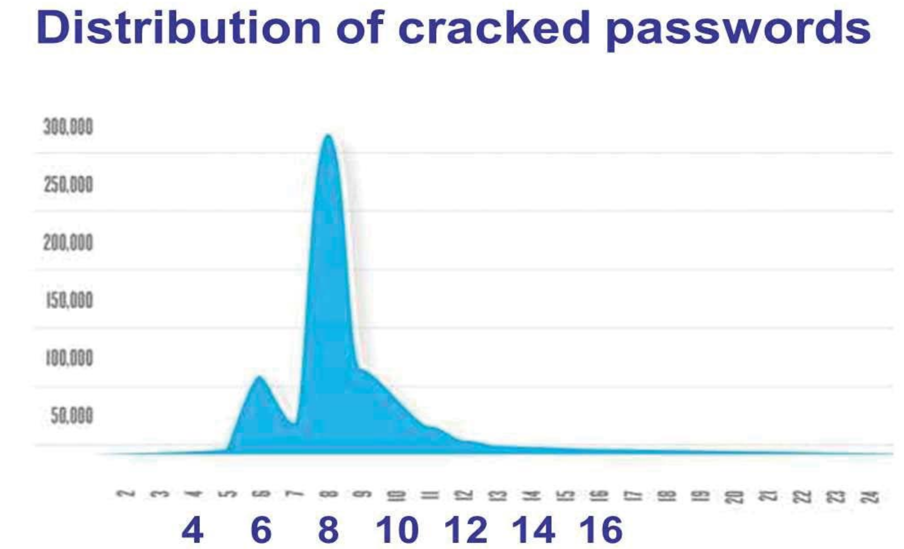
If we have another 2-character password that can include upper case letters (26), lower case letters (26) and numbers (10), the number of possibilities for each character jumps to 62 (26+26+10). The number of possible combinations is now 622, or 62 x 62 = 3844.

Let's try a 12-character password that uses upper case (26), lower case (26) and numbers (10). The number of possible combinations is 62 x 62 x 62 x 62 x 62 x 62 x 62 x 62 x 62 x 62 x 62 x 62 = 6212 or 312,000,000,000,000,000,000 possible combinations. In spite of the number of combinations, these passwords can still be cracked by a determined but patient criminal using brute force.

Password best practices

Passwords MUST be random – hackers are experts at testing for ANY pattern. The longer the password the better! The more complex the better! Passwords should include upper and lower case letters, numbers and, if possible, special characters. You absolutely MUST use different passwords for each account. Hackers have created software that can automatically check multiple accounts (banks, retailers, social media) for a single password.

The graph below shows a distribution of cracked passwords according the Internet security company Trustwave. It show that few people use passwords less than 5 characters or more than 12 characters. It also shows that passwords between 6 and 10 characters are often cracked.



https://gsr.trustwave.com/topics/business-password-analysis/2014-business-password-analysis/

Given that computing power doubles every 2 years, I would contend that 12 and even 14 character passwords are not currently safe. To secure sensitive accounts such as bank accounts or investment accounts, or even e-mail accounts, I would suggest using 18+ character passwords. 10, 12, or 14 character passwords could be used for less sensitive accounts such as the New York Times, etc. Given the state of password pattern analysis, I don't believe that passwords created by humans are safe even if they're longer than 12 characters.

Do not use whole words

Hackers are getting wise to people using whole word phrases for their passwords. They are starting to include multi-word phrases in wordlists like givemelibertyorgivemedeath(1). [(*) indicates a footnote at the end of the article.]

Are security questions a weak link?

If your security questions are more easily guessed than your password, you have a problem. If the website allows it, make up your own questions. If not, either make up your answers, use someone else's information, such as a spouse or simply use the correct answers but spell them backwards.

If you can create your own questions consider making them 1) safe so they cannot be guessed or researched, 2) stable so they do not change over time, 3) memorable so you can remember them, 4) simple so they are precise, simple, consistent, and 5) have many possible answers.

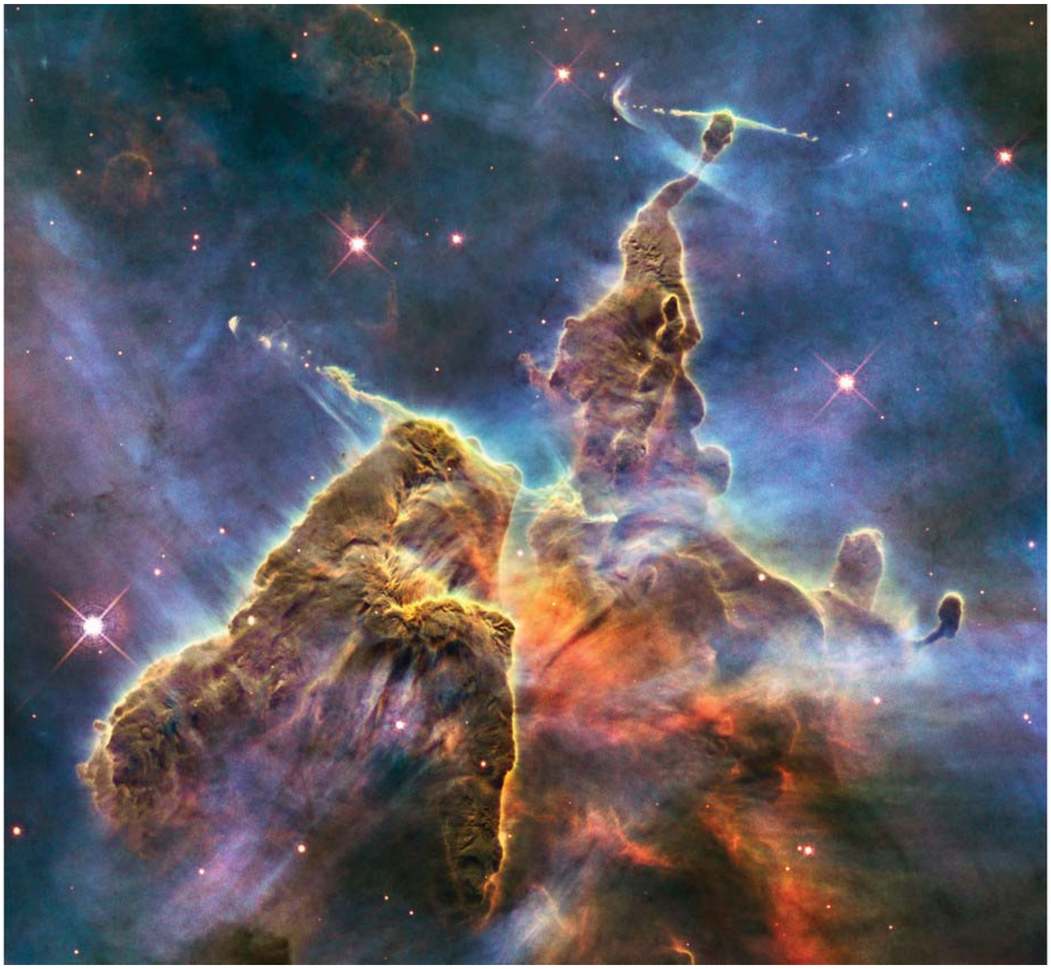
Consider using a password manager

A password manager can remember all your passwords for you except your master password. It can generate long random passwords. Most can auto-fill username and password boxes. Many can even log you in automatically. Most password managers are cross-platform – Windows, iOS, Linux, and mobile cross-platform. Some can also save other data beyond passwords. The basic version of most password managers is free. I suggest that you not use browser password managers as most are insecure to some degree.

A word about master passwords

Password.......Continued on page 6

Internet Picture of the Month



Images of outer space from the Hubble Space Telescope

From http://www.wsj.com/articles/star-studded-images-from-the-hubble-space-telescope-1422658561?mod=WSJ_article_EditorsPicks_6. “It may look like a fantasy film still, but this image is actually the top of a pillar of gas and dust. Located 7500 light years away, the pillar is three light-years tall.” Note that these are not the colors you would see with the naked eye. They are due to enhancements by NASA to emphasize certain features. The Hubble telescope has been in orbit for 25 years.

February’s Links

Tampa PC Users Group	http://www.tpcug.org
Windows 10 Technical Preview - CNET	http://www.cnet.com/how-to/windows-10-guide/
Florida’s Springs	http://www.floridasprings.org/
European Synchrotron	http://www.esrf.eu/
Mardi Gras in New Orleans	http://www.neworleansonline.com/neworleans/mardigras/

Password.......Continued from page 4

If you can create a completely random password that you can remember, use it. If not consider this system. Find a quote, a song lyric, a line from a poem, the Bible or a movie that you can repeat almost without hesitation. Use the first letter of each word and include all punctuation. The password will be much stronger if it includes numbers, punctuation and/or capital letters in the middle. If it doesn't contain them, figure out how to add them or find another phrase.

Here are a couple of examples to lead you in the right direction. I increased the font size so the characters underlined would show up better.

Ifi2abrof,Iwdddatfwh. – 21 characters – Johnny Cash
I fell into a burning ring of fire, I went down down down and the flames went higher.

Y,Amtssfa,Nilatth2s. – 20 characters – Beatles
Yesterday, All my troubles seemed so far away,
Now it looks as though they're here to stay.

Fascinating articles

In 2013, a tech-savvy journalist with no hacking experience attempted to "crack" a database of over 16,000 encrypted passwords. His editor gave him one day to find the resources, learn the tools and "crack" as many passwords as possible. The rules were he could use only consumer-level computers and free tools from the Internet. After some initial struggles Nate Anderson cracked over 8,000 passwords (47%) in one day.(2)

Not long afterward, Wired magazine asked 3 expert crackers to attack the same database. One spent only one hour and cracked 62% while using a single GPU card. One used a bit more than an hour and cracked 82% while using two GPU cards. The last cracker spent 20 hours and cracked 90% using a single GPU card.(3)

What I've learned

- Cracking tools are quite sophisticated and mostly free.
- Wordlists, online help,and other resources are easily available and mostly free.
- Computing power doubles roughly every two years.
- Cracking passwords is all too easy even for relative beginners.
- Human generated passwords (HGP) invariably have patterns embedded in them.
- Humans are not usually capable of generating completely random passwords.
- Wordlists, pattern analysis, and pattern-generating software can defeat HGP.
- Shorter passwords, whether created by humans or completely random, are simply not secure.
- The degree of difficulty in cracking passwords increases exponentially with the number of characters.

Conclusion

The only way to generate and remember long, completely random passwords for every account is to use a password manager.

References

(1) "How the Bible and YouTube are fueling the next frontier of password cracking" http://arstechnica.com/security/2013/10/how-the-bible-and-youtube-are-fueling-the-next-frontier-of-password-cracking/
(2) "How I Became a Password Cracker" http://arstechnica.com/security/2013/03/how-i-became-a-password-cracker/
(3) "Anatomy of a Hack"- http://www.wired.co.uk/news/archive/2013-05/28/password-cracking ◆

Where is the Linux Desktop?

By Merle Nicholson, Secretary,
Tampa PC Users Group
merle@merlenicholson.com

We all know by now that Linux is in wide use all over the world, just not on the desktop. It dominates phones (Android) and servers and even supercomputers. The top 20 supercomputers worldwide almost all use Linux. The one supercomputer exception uses Unix – an earlier version. And the millions of internet servers? Almost all Linux.

Chromebooks outsold laptops last Christmas season, and the year before. Linux is a dominating force in connected devices. So it's all around us, except for the desktop and for notebook computers – Chromebooks being the exception. Chromebooks are making great inroads in schools where the ability to control what gets installed ranks high, as does the relative resistance to malware and viruses, and obviously cost.

Computers with Linux OS pre-installed just aren't gener-

Lilnux........Continued on page 7

Linux.......Continued from page 6

ally available. Dell and HP have always sold them, but you won't find them in stores. With Dell, the cost differential with Windows OS is small, just $50; although if it were on a $500 computer that's 10%. And I suspect that the margin will be even smaller because Microsoft is now giving the OS software to manufacturers at a price close to zero. Look for an operating system called "Windows 8.1 with Bing."

First, let's state that there are no file or networking incompatibilities between Linux and Windows. Common files are fully interchangeable between the systems: Documents, spreadsheets, pictures, movies. This concern is even less important now that users' computer needs are evolving toward Internet-centric applications. The Internet browser is a great equalizer. You can even install some Windows programs in Linux using an emulator called WINE. For the technical-minded you can run excellent Virtual Machine software and then run any and all Windows software.

But there are some needs that have so far been unmet. The first that comes to mind is Intuit's TurboTax. If your tax needs are simple enough to use the online TurboTax, problem solved. Otherwise, there's no Linux solution. The second thing is a major trip planning and navigation software like Delorme Street Atlas. But most everything else is available in first-class applications like Office Suite, financial systems, photo and movie editing, publishing, CAD drawing and thousands of games. And to top it all off, nearly all these are available at no charge. There is a built-in software catalog program that helps you find and install everything.

I have yet to install Linux only to find I have a driver problem. The device drivers – except for some printers – are built in. And they work well.

Finally, let's address malware and viruses. There are some few known viruses that affect Linux. But the OS itself is constantly being updated to plug those exploits. Linux users don't use virus scanner software because the chances of getting one is much smaller than a Windows computer with the very best virus software installed. Statistically speaking, no one gets a virus with Linux.

So why would you consider a Linux desktop? What circumstances make it a viable option?

If you are currently running an old Windows OS. XP or earlier, you need to replace it now. Right now unless you are not connected to the Internet. Linux will run on an old system easily and much faster than Windows ever did. For free.

If you have a computer where you're up to your eyeballs in malware and can't fix it yourself, you're looking at a $100 professional repair. Save the bucks and give Linux a try first. If you can back up your data you have nothing to lose.

If you're just plain tired of fighting off malware and viruses or you feel you don't have the skills to do it, Linux is a good way to go. No yearly fees for virus scanners that work about 95% of the time anyway.

If you're looking for a simpler system with good protection for the kids in the house, you can't do better than Linux. You can control everything that gets installed and also know it's virus-free. Nothing gets installed without the administrator password. Just don't tell the kids what it is. The desktop and application launcher is actually closer in operation to an Apple iMac than it is Windows. It's simple and easy.

What are the issues?

Probably the biggest issue is deciding which of the many versions to install. If you count all the variations and branches, there are probably 250 or so choices to make. The most popular by far is Canonical Ubuntu with the standard "Unity" style desktop. This is a very good way to start because the base OS is being maintained by a large multi-national company. Alternately, there are some "flavors" of Ubuntu that replace the desktop appearance and controls, menus, settings and a unique selection of standard software. These all have the blessing and cooperation of Canonical. Each has a target audience like Eubuntu which is designed for children and schools. The website https://wiki.ubuntu.com/UbuntuFlavors details the differences of the nine flavors.

There are good instructions on how to make a bootable CD or flash drive with Linux and then run it on your computer without installing any software. This is a very good way to try it out to see if there are any hardware incompatibilities and to see if you really like it. You have nothing but a little time to lose.

There is a wealth of friendly web pages to help with all this. Start at http://www.ubuntu.com/ or https://wiki.ubuntu.com/ and proceed to http://www.ubuntu.com/download, a very good place to get installation guides and instructions; also "Ask Ubuntu" and "Ubuntu Forums." ◆

Tampa PC Users Group, Inc.
P. O. Box 3492
Tampa, FL 33601-3492

First Class Mail

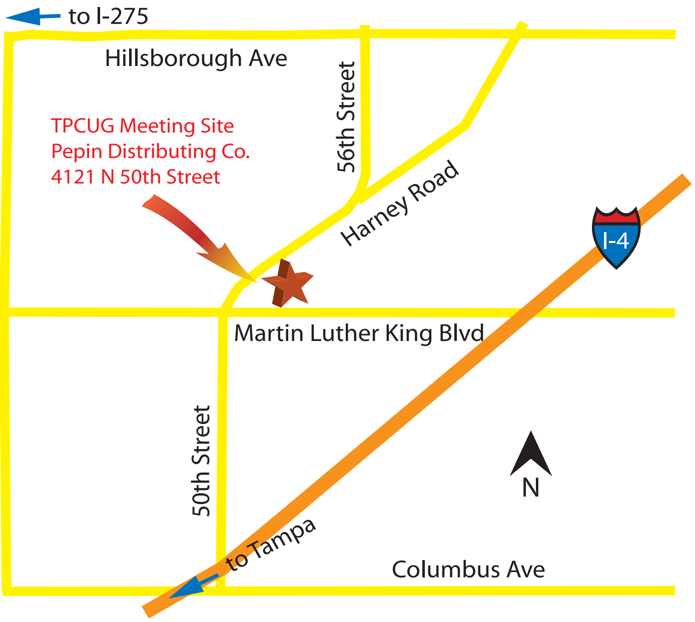
□ *Member: Your membership is up for renewal*

Comments........Continued from page 2

for sites such as these, our browsers are unresponsive at times. And it is getting irritating.

I am sure you have probably noticed at many sites now when you start viewing at the main page and then click on a link to go to another page at the site and then click the return button to return to the main page nothing happens. To get back to the main page (using IE), you have to either hold your cursor down on the back button to see a list of previous page and choose the main page or you have to find a link to the main page and click on that. I am convinced this is because of all the activity that is going on in the background.

What would be nice is a new browser that stripped out all that advertising and tracking stuff and just presented you with a web page containing text, images and whatever links were appropriate. Think we will see anything like that anytime soon? ◆


to I-275
Hillsborough Ave
56th Street
TPCUG Meeting Site
Pepin Distributing Co.
4121 N 50th Street
Harney Road
I-4
Martin Luther King Blvd
50th Street
N
to Tampa
Columbus Ave