http://www.tpcug.org

Bits of Blue

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

Vol. 29 No. 8 August 2016

August in Tampa

Meeting

Publishing Apps

& Windows Continuum

by

William LaMartin

Wednesday, August 10, 2016

6:30 PM

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

INSIDE THIS ISSUE

Meeting Preview: William LaMartin will discuss several topics: Publishing apps to Windows 10, Android and iOS; What is Windows Continuum; and creating videos from your photos.

Merle Nicholson will lead the Windows SIG for the first 30 minutes of the meeting.

Editor’s Comments

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

Last month I mentioned purchasing an iMac to enable me to create iPhone and iPad apps similar to my Windows 10 apps, some of which I had already extended to Android. Well, I now have two iOS apps in the Apple App Store: *Newspapers of the World* and *Computer Group Newsletters*. As time permits, I will add to that collection. Without a doubt, there are more hoops to jump through to create an iOS app than for Windows or Android. On Android and Windows, the first app is titled News of the World. The second app has all the TPCUG newsletters through 2015.

I had an iPad 2 around the house so as to be able to check the functionality of my iOS apps on a real device but thought that I also needed a small form-factor device. I purchased a used iPhone 5s for that purpose. It was an expensive month, especially considering that I make no money from these apps, considering it just a hobby. ◆

September Meeting: Merle Nicholson on Windows 10 Tips

* * OFFICERS AND BOARD MEMBERS * *

President: John Witmer (president@tpcug.org)	813-949-8007
Vice President : Kevan Sheridan (kevan@tpcug.org)	813-988-6480
Treasurer: Doug Mullis (dmullis@tampabay.rr.com)	813-234-9343
Secretary: Merle Nicholson (merle@merlenicholson.com)	813-879-3602
Member at Large: Ron Weinberg (rswjbr@verizon.net)	813-960-4132
Board Member: Dave Palmer (dkp205@hotmail.com)	813-789-0488
Board Member: Ed Cohen (CondoVacations@earthlink.net)	813-962-7800

APPOINTED (Volunteers)

Editor: William LaMartin (william@lamartin.com)	813-251-3817
Programs: Doug Mullis (dmullis@tampabay.rr.com)	813-234-9343

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 July Meeting

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

For July, we had a scheduling conflict for the meeting room and scheduled it a week early from July 13 to July 6. As a result, the meeting was poorly attended, quite a shame since our speaker was the ever-entertaining and informative Blain Barton, an employee of Microsoft. Blain has been there for us every year for quite a few years. Our gratitude goes to Blain for his continued support.

The Windows Special Interest Group (SIG) opens our monthly meeting. Merle Nicholson, the SIG moderator, 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. This month Merle demonstrated more Windows 10 settings challenges, including how to prevent Windows Store from hijacking your local account.

Our presenter, Blain Barton, was the July presenter. He always has something interesting to talk about on projects he’s engaged in at Microsoft. His main topic was about DevOps, a combination of the words Developer and Operations. It’s for “orchestration and automation technologies needed in the world of big data analysis, cloud and Agile rapid application development.” Blain is now engaged in the development and deployment of small applications. He explained his interaction with a business customer and modeling applications for them.

Thanks to Blain for an entertaining and useful presentation. ◆

Rethinking 2-Factor Authentication

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

I've taught various aspects of Internet Security for many years. I subscribe to many newsletters and newsfeeds. I have a number of Google Alerts to bring me information on a variety of related topics. As a result, I do a lot of reading. Like any good cub reporter, I like to confirm information I've read from one source with similar information from other sources, usually a number of other sources. In other words, I don't like to get fooled.

But I recently I got fooled. Or maybe lulled to sleep is a more accurate description.

Let me start at the beginning. 2-Factor Authentication (2FA) isn't new, but it's become a lot more popular over the last few years as hackers have more gotten more sophisticated and better at what they do.

Wikipedia (https://goo.gl/5QkXD) says 2FA is "… a method of confirming a user's claimed identity by utilizing a combination of two different components. These components may be something that the user knows, something that the user possesses, or something that is inseparable from the user." The standard example is the combination of an ATM(automatic teller machine) PIN (personal identification number) and a debit card. Something I know, the PIN, is combined with something I have, the card.

One popular method of 2FA is to use mobile phone-based two-factor authentication. This method of 2FA relies on the user inputting their user name and password (1st factor) into a website. The website responds by sending a one-time-valid, dynamic passcode via SMS (text) to the user's phone. Inputting the code (2nd factor) into the website authenticates the user and allows use of the website.

Many security-sensitive websites now have the ability to be configured to accept various forms of 2FA, including mobile/text 2FA. These websites include the Who's Who of technology: Google, Apple, Facebook, Yahoo, Amazon, Twitter and dozens, if not hundreds, more. All include mobile/text 2FA as well as other methods of 2FA. At least one site I'm aware of (https://www.turnon2fa.com/) offers specific instructions on setting up 2FA, including mobile/text, on many of these websites.

In addition, hundreds of articles have been published in the last few years touting the benefits of mobile/text- based 2FA. I'm sorry to say that the constant drone of this input put me to sleep.

Recently, while watching Steve Gibson's 'Security Now' broadcast on Twit.tv, I was jolted awake when Steve proclaimed that, in fact, mobile/text- based 2FA was INSECURE!

'What?' I thought. That seems to go against the advice of the entire technology ecosystem. His point, perfectly valid once I was roused from my comfortable acceptance, was that the phone system itself is not secure! But of course! My reading on privacy, tracking

Rethinking.......Continued on page 4

Rethinking..........Continued from page 3

and the shenanigans of the NSA and similar organizations around the word came racing back. Of course cell phones are not secure. I, like so many others, had not put the puzzle pieces together. That realization triggered another round of online research.

The information I ran across completely contradicts any thought that mobile/text 2FA could possibly be secure. Here are a couple of articles demonstrating that sophisticated hackers, as usual, are well ahead of us.

http://goo.gl/cNMrcq - 'Malware Bypasses 2-Factor Authentication' (2014) - "Criminals have been bypassing the Android-based two-factor authentication systems in use at 34 banks across four different countries, as part of a sophisticated spear-phishing and malware campaign…"

http://goo.gl/hAEERv - 'Two-Factor Authentication Bypassed in Simple Attacks' (2016) - This article concerns recent research that demonstrates "…practical attacks against both Android and iOS devices, showing how a Man-in-the-Browser attack can be elevated to bypass 2FA."

https://goo.gl/yr40pw - 'So Hey You Should Stop Using Texts for Two-Factor

Authentication' (2016) - This article points out several ways messages to mobile phones can get hijacked.

https://goo.gl/2mpUHk - In this recent (7/27/16) article the U.S. National Institute for Standards and Technology (NIST) says the SMS-based two-factor authentication would soon be discouraged citing a lack of security.

I also found the following academic paper. Dr. Wolfe should have added 'Let Me Count the Ways' to the title. This is an interesting read, 6 pages, and a bit scary.

http://goo.gl/SQ04ln - "The Insecurity of Mobil Phones" by Dr Henry Wolfe, a PhD specialist in computer security.

Rethinking..........Continued on page 8

Windows 10 Priority One for new installations Continued

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

This month, I'm adding a few more items to the changes that should be made to all Windows 10 installations. The main article is in last month's issue of Bits of Blue July 2016.

Note to readers: Instead of typing the URLs referenced in this article, go to the TPCUG.org website, and on the first webpage, open this current newsletter. There you'll find that all the links in this article are live. Just click on them.

But first, let's discuss the security of your computer. I've heard the argument many times that your computer is in your house and isn't accessible, so having a no password login or setting it to log into a default user account is acceptable. I'll disagree, and here's the reason why.

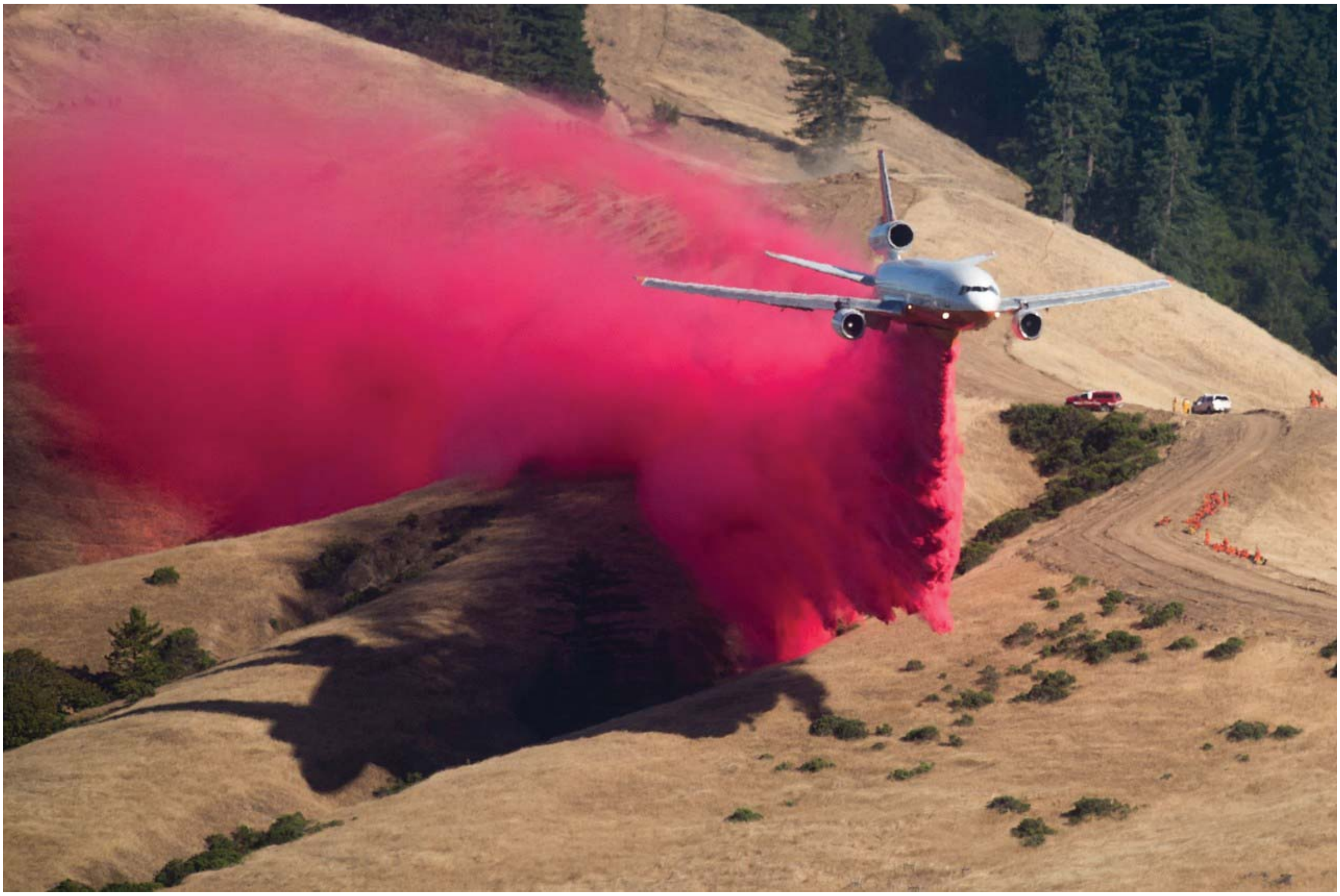
User Accounts

By default, on installation, the main user account has "administrative rights" which means that any user of this account can install and run any software unimpeded, including undesirable software as well as useful, intended software. All that needs to happen is to log into that account. The problem with this is software that comes into your computer from the Internet or software that has been piggybacked onto some other process that may or may not be initiated by yourself. Email attachments, hacked websites, software that you acquire thinking it's useful, PC help phone calls from people representing themselves as Microsoft employees .. all this is dangerous.

OK, well, what do you have to lose? Let's look at some worst cases; the situation where some ransomware changes the operating system to encode all useful files. Or gets your Amazon account or Visa card info. Or just wipes out the hard drive. Do you have a

Windows 10..........Continued on page 5

Internet Picture of the Month



Fighting a California Wildfire

From the Wall Street Journal, http://www.wsj.com/, in the Photos section.

“A plane drops fire retardant while battling the Soberanes Fire near Carmel Highlands last Saturday.”
Noah Berger/Agence France-Presse/Getty Images

Windows 10..........Continued from page 4

complete image backup stored where you can just re-image the hard drive using a boot CD or flash drive? Are your two- thousand photos backed up? Important documentation? Perhaps you can reinstall Windows and all your software from scratch. Do you have the original installation media? Do you have the CD installation keys? If you have Windows 7, do you want to then install the drivers for all your devices and also 260 updates?

If you believe you are fine with reinstalling Windows 10 after a disaster; you have documents and pictures in Google Drive, Dropbox or OneDrive; use a browser email implementation and do mostly internet, I’d sug-

Windows 10..........Continued on page 6

Windows 10..........Continued from page 5

gest you're not well served by Windows and should look at ChromeBox, ChromeBook, Linux (Ubuntu) or even MacBook. They're all much more secure, way cheaper (except Apple, which is much more expensive) far less trouble, and you can stop worrying about viruses and malware. My spouse and I both use Linux and Android for much of our everyday needs.

Compounding the user account situation on Windows 10 is that Microsoft obscures the route needed to create local accounts. All the buttons are there to route you to a Microsoft online user account and password. Yes local account links are there, and if you are not forewarned or are not using a well written tutorial, you'll miss them because they are just text, not a button, sometimes a different font color, sometimes not.

So what's wrong with using an online account? Wait a minute .. what? This is a login entry into your computer that malware, virus and ransomware can use to install on your computer, and you want to send it over the internet to Microsoft? Why would you do that? There is no other operating system that allows this. I can use my Android phone and tablet without logging into my Google Account, can't you? Yes, I do log into that gmail account, but it's not a condition of turning on the device. And obviously I don't have the level of concern about viruses.

If you like (insist on) an online Microsoft account to log into your computer, please change the security level to "standard". That's the only way there is to protect yourself. First, create an administrative level local account or activate the "Administrator" account. Use a good password, memorize it and use a password database like LastPass or Keepass. Don't tell anyone what that password is. Log into it once, then out, you may not need it again. Log into the main (MS online) account and change the security level to "standard". You may never use the administrator account again, but you'll use its password many, many times whenever a setting or a software installation requires it. You'll get to recognize the password prompt and it'll become routine. This will block out 95% of all viruses as well. All the details are covered in last month's article.

Number One problems with Windows 10 that you should fix right now.

See last months article for details.

1. Fix your login accounts. Activate or create a local Administrator account
2. Activate System Protection, System Restore
3. Fix the Boot into Safe Mode, activate the F8 on boot up.
4. Fix restart to BlueScreen
5. Manage Microsoft Updates (Win 10 Pro)
6. Disable as much Microsoft telemetry and forced advertizing as possible.

Turn off or uninstall OneDrive

In last month's article, I included one link to turn off OneDrive, the file storage and sync supplied for Microsoft users, and built into Windows 10. I personally don't use OneDrive, not that there's anything especially wrong with it. I have been using Google Drive for many years, and I really don't want to manage two cloud drives. There are three concerns associated with OneDrive. One is the System Tray icon, second the service itself is running in the background even though it's not being used, and third is the OneDrive drive shortcut in the left pane of all Windows Explorer windows.

This link from last month doesn't address the main problem - disabling the OneDrive service, but it is the least technical. https://support.office.com/en-US/article/Turn-off-or-uninstall-OneDrive-f32a17ce-3336-40fe-9c38-6efb09f944b0

This following link does everything, but by necessity is more complicated because Microsoft chose to not provide an accessible uninstallation or even an optional Windows Component for OneDrive. In fact, I've seen claims from Microsoft that it's a built in feature of Windows 10 and cannot be uninstalled. Bad Microsoft.
http://lifehacker.com/how-to-completely-uninstall-onedrive-in-windows-10-1725363532

More on Managing Updates

If you need a better reason to manage Microsoft Updates I have one you maybe haven't guessed.

If you can delay the installation of updates you can

Windows 10.......Continued on page 7

Windows 10..........Continued from page 6

have a chance to create a new restore point. This is important because every now and then there will be an update that cause enough havoc on boot up to keep you from using your computer. I'd wager this has happened to you at least once. Fortunately with Windows 10 Pro you can get notification that updates are available, you can then create a new restore point manually (if you have activated it), then allow the installation to proceed. Then, on a bad update you can use Safe Mode to restore the last good restore point.

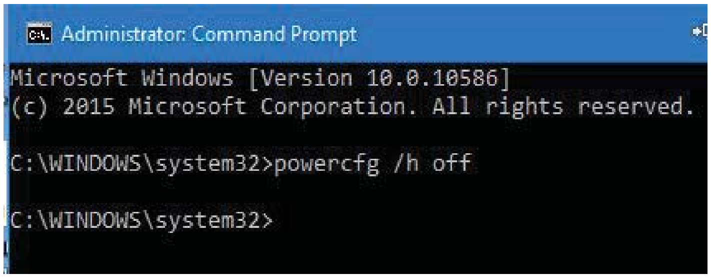
Fast Startup Power Option

It's a variation of the long standing Hibernate system available mostly for notebooks where the entire content of memory is saved to disk to be reactivated on next boot. But it went through some changes with Windows 10, became faster because it's been modified to save just the kernel (essential part) of memory. And it may be causing some problems on your computer. It may or may not be turned on. I would make sure it's turned off for several reasons. First, if you are booting from an SSD drive, it really has very little advantage and no further discussion is necessary because you're already enjoying fast boot up; make sure it's off. Problems it may cause are with USB devices not activating after boot because they haven't been awakened or updates becoming out of sync.

Turning Fast Startup off (or on) is available through the Settings: Settings, System, Power & Sleep, Additional Power Settings, Choose what the power buttons do, Change settings that are currently unavailable, Turn on fast startup (recommended). That's six steps, uncheck the box.

This link, http://www.howtogeek.com/243901/the-pros-and-cons-of-windows-10s-fast-startup-mode/, pretty much covers the subject except for one thing, and this is what I do to disable hibernate entirely which also erases the hibernate file from disk (hiberfil.sys). I would rather my computer do a complete reload at boot and not carry anything loaded in memory from the last session. I've encountered USB devices not working too many times, requiring that you first figure it out then unplug and reattach the device. My old USB scanner comes to mind. I boot from an SSD, in any case. I have tested this to see if there's any discernible difference and have found none.

In an elevated Command Prompt (Admin), enter: powercfg /h off



```
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>powercfg /h off

C:\WINDOWS\system32>
```

Lightning Strikes Again

By Bob Davis, Tampa PC Users Group
rob234@gmail.com

Lightning makes no sense some times. Although my computers and all the peripherals are on an uninterrupted power source, the other day a lightning strike killed my 4-port USB unit plugged into my laptop. Fortunately the laptop has 3 USB ports so I was able to hook all three important things back into it like the wireless mouse, the keyboard, and the printer. Next I went on to Amazon and ordered a replacement 4-port in case I need it.

I tried to print the invoice. That's when I found out the printer no longer communicated with the laptop. After testing all the USB ports on the laptop, I concluded the USB port on the printer was fried too. I thought about using the wireless feature but you have to use the USB port to set up the wireless feature. Go figure… End result, I needed to buy another All-in-One printer. I hate to throw the old 915 away. It still copies okay. I even think it will send and receive a FAX okay. It just won't talk to a computer so what would you do with it? I found it very inconvenient to dump a file to a thumb drive and take it to the desk top computer to print something. The work horse printer has always been the one hooked to the laptop.

Another problem is I just purchased a pile of spare cartridges for the fried Pro 915 printer. Contrary to what

Lightning.......Continued on page 8

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

□ *Member: Your membership is up for renewal*

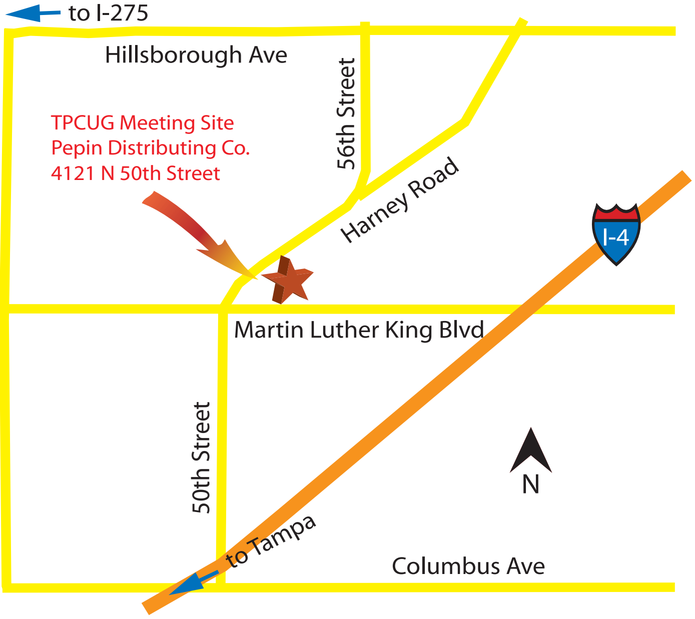
Rethinking.........Continued from page 4

In spite of the information above, I believe that if you're using texted codes on your cell phone as 2FA, the risk is relatively small. This is not (yet) a widespread threat. But if you're relying on mobile/text 2FA to secure your valuable accounts (banking, e-mail, etc.), it might be time to consider other options. The fact is, it's not secure. ◆

Lightning.........Continued from page 7

a professional printer user might say, I liked my little Lexmark Pro 915 All-in-One printer. (And what can I say – sometimes I go cheap.) Of course the Pro 915 printer is out of production and not available at a price I want to pay. I did some research and found the Pro 715 printer uses the same ink cartridges, and I was able to buy a barely used Pro 715. After updating the drivers, etc. I have a working printer again. The front panel is not as nice as the 915 but other than that, it's hard to tell any difference between the two.

I always say enjoy the journey, but some days are more enjoyable than others. Like the days when you don't have to buy another All-in-One printer. So now I am enjoying the journey again. ◆


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