Treasure Coast Macintosh® Users Group

Living and playing with iOS, watchOS, macOS and tvOS devices!

Mouse Tales Newsletter

June 2017 • Vol. 30 - 6

MEETING

Thursday, June 15

LOCATION - Children's Services Council • 101 SE Central Parkway, Stuart 34994
• In the Green building between Unity Church and Bridges Montessori. Click on this map link - **http://tinyurl.com/clq2mkk**

5 - 8 P.M. "Here To Help"

Bring your laptop, iPad or iPhone and enjoy a format with Beginners tables throughout the room, where you can just join any group:

• iPad	• Basic Help
• iPhone	• Email & Internet
• iPhoto	• How can I ...

6:30 - 8 P.M.
• Red, Yellow & Green Buttons
• Finder Preferences

Join us for some really helpful instructional videos and follow along to learn how it is done.

See you there!

• Early Front Page Edition •
http://www.tcmug.net

MISSION: *Since **1988**, TCMUG has provided a forum for Apple users by creating a member network to share information and offer support in the evolving world of technology.*

On June 5, Apple held the **2017 Worldwide Developers Conference** to introduce 6 big announcements (and more):

1. watchOS 4
2. macOS High Sierra
3. New iMacs and MacBook Air / MacBook Pro refreshes
4. iOS 11
5. iPad Pro 10.5
6. Apple HomePod speaker

WWDC17

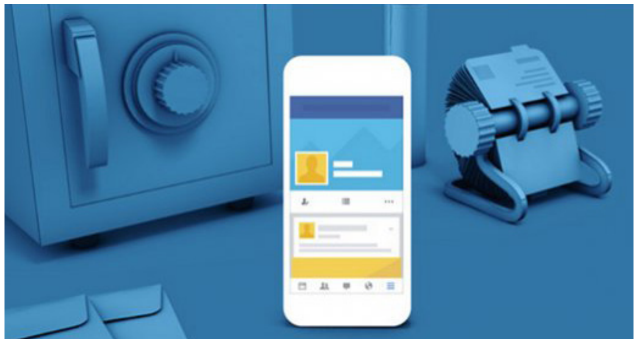
Apple WWDC17 - Watch the keynote -
https://www.apple.com/apple-events/june-2017/

Also cruise the main site for more product info:
https://www.apple.com

IN THIS ISSUE -

How to Secure Your Facebook Account

by Matt Klein 1/24/17



Choose a Strong Password

Make sure it is long (12 to 14 characters or longer), a mix of characters, and contains no personal information, since those can be easily can be socially engineered.

Most importantly, though, don't use this password anywhere else on the internet. You should use a different password for every single account you have, and ideally, they'd all be random strings of characters.

Lastly, beware of attempts by others to obtain your password through nefarious methods. Don't follow untrusted links, such as those sent in e-mails, that ask you to enter your password.

All the settings we'll refer to in this article can be accessed using a web browser by clicking the little arrow in the upper right corner and choosing "Settings" from the drop-down menu, so do that now.

In the mobile app, tap the "More" button in the lower-right corner, then scroll to and tap on "Settings". From the resulting pop up, choose "Account Settings".

You can change your Facebook password from the Password section in the Privacy settings. Use your password generator and password manager to store the password in a safe place, and you're good to go.

Use Login Approvals

Believe it or not, a strong password is not enough to really secure your account. These days, it's just as important to turn on a security feature known as **two-factor authentication**.

The principle behind it is simple: You sign in with something you know (your password), and something you have—which is usually your phone. After entering your password, Facebook will send a code to your phone that you type in on the site, to confirm that you are who you say you are. This feature can be enabled from **Settings > Security > Use two-factor authentication.** Check the box next to "Require a login code to access my account from unknown browsers".

This feature can be disabled at any time. We recommend, however, that you leave them on and get used to using them. It's an essential security feature of just about every service these days.

Enable Login Alerts and See Who's Logged Into Your Account

You'll find them under **Settings > Security and Login > Get alerts about unrecognized logins.**

You can either choose to get a notification on Facebook, over email, or as a text message. The next time anyone logs in from an unrecognized device or browser, you'll be notified.

Head to **Settings > Security > Where You're Logged In,** and click **"End Activity"** for any unfamiliar devices or locations. If you don't want to go through and review every session on the list, click **"End All Activity"** to log out from all devices on the list.

Note: if you log out from a session, you'll still be able to log in on that machine without entering a Login Approval code. You can revoke access for any Login Approvals—say, if your laptop or phone gets stolen—from **"Recognized Devices" in the Security settings.** Just Remove any browser or device that you've previously approved, then click **"Save Changes".** The next time that device tries to log in, they'll need a Login Approval code again.

Audit the Apps that Have Permission to Access Your Facebook Account

Head to **Settings > Apps** and take some time to remove anything that looks suspicious or no longer use.

To remove an app, just hover over it and click the "X" on the right-hand side.

Alternatively, you can click the "Edit" button (right next to the Remove button) to change what information you provide to an app.

At the bottom of the Apps Settings screen, you can change settings for a number of different items - what each of these settings means:

• Apps, Websites and Plugins

Turning this off will disable Facebook integration with third-party apps, websites, and plugins entirely. That means you won't be able to do stuff like log in with your Facebook account from websites or applications, games, and other things.

Click the "Edit" button to learn more and to disable this feature.

>>>>> continued

• Game App Notifications

Hate getting notifications from friends who play games and want you to play? Turn those off here.

• Apps Others Use

When you connect an app to your account, it can sometimes see information about your friends. Thus, when your friends use apps, they can sometimes see information about you. Click Edit on this section to change what your friends' apps can see about you.

These categories all appear to be an opt-in type of deal—so you can safely leave them unchecked—but it never hurts to know what's what.

• Old Versions of Facebook for Mobile

This setting controls the privacy of anything you post using old, outdated versions of the Facebook mobile app. Basically, if you're not using a BlackBerry or some other dinosaur of a device, you don't have to worry about this.

• Peruse the Rest of the Security Settings

The settings we've highlighted so far are the most important settings everyone should use. The rest of the security settings are up to you, but it's worth going through and checking out which might be useful for you.

Trusted Contacts

Hopefully you'll never get locked out of your Facebook account. If you're using a password manager, you'll never forget your password. And even if you do, you can always reset your password… as long as you have access to your email account.

If, for some reason, you lose access to all those things, Facebook's "Trusted Contacts" feature can help, as long as you set it up ahead of time. Trusted Contacts allows you to pick **three to five friends** you can call if you can't access your account. They then will give you the codes necessary to get back in.

Just head to "Your Trusted Contacts" on the security settings page to set this up.

Be sure to give your trusted contacts a heads up that you're using them, and if anything ever goes down, they should make sure that it's you calling before handing over the keys to your account.

Public Key

Most users won't use this, but if you're interested in encrypting notification e-mails "end-to-end" from Facebook, you can add your OpenPGP public key with this option.

This may be a little advanced, and perhaps you don't even receive notification e-mails, but if you do, and you want to encrypt them, then you can learn more about it.

Profile Picture Login

This is a newer feature that Facebook introduced, which lets you just click your profile picture in lieu of typing your password.

Thus, anyone with access to your browser can click on your picture and log into your account. This is probably a bad idea, so we **don't recommend turning this on.**

Legacy Contact

Ever wonder what happens to your Facebook when you die? That's what Legacy Contacts are for. You set someone (like a spouse or family member) as your legacy contact, and if you die, they can do stuff like pin posts to your Timeline, respond to friend requests, and update your profile picture. They cannot post anything to your Timeline or view your messages.

The legacy contact option is important because once you're gone, hackers can potentially access your account and you won't be around to prevent or respond to intrusions. Alternatively, you can choose to have your account deleted upon your demise.

Deactivate Your Account

This deactivate option is typically used to give you a break from Facebook, but is also useful if your account is hacked. It's simple enough, just click "Deactivate", enter your password, and read through the instructions to go through with it.

Lastly, don't neglect basic, general security practices either. If you log into your account from a public computer or on someone else's device, make sure you **always log out** and, if you can, **clear the history when you're done** (or, better yet, use the **browser's private mode**). Never leave yourself logged into your account, even if you walk away for just a few seconds. Make sure your computer and browser are always up to date, and have good virus and malware protection installed at all times. ■

TCMUG Note: Since Facebook updates information, go to Settings and check out the latest choices to protect your security.

How to Remotely Access Your Computer from Your Phone

by Cameron Summerson

There comes a time in nearly every computer (PC) user's life when they need a file from their computer…and it isn't nearby. Fortunately, there's an easy way to remotely access your computer directly from your phone or tablet. While there are many options out there, here are your two best options.

Option One: Chrome Remote Desktop (Windows, Mac, Linux, Android, iPhone)

This has been my personal go-to for remote access ever since it was first released some years ago. It's quick and easy to use, completely painless to set up, and works on pretty much any device across the board.

Of course, it does have its caveats, like the fact that **you have to be a Chrome user.** While there are a lot of Chrome users out there, I get that there are also quite a few users who just aren't into Google's browser, and that's okay—we'll talk about another good option for you guys down below. But if you use Chrome, this is probably your easiest option.

How to Set up Chrome Remote Desktop

First, you'll need to install the Chrome Remote Desktop extension in your browser. It's available from the **Chrome Web Store**, and the installation takes all of a few seconds.

Once installed, you'll launch the app from Chrome's app menu—it should be the first link in the bookmarks bar. From there, just look for the Chrome Remote Desktop link.

The first time you launch it, you'll have to enable remote connections to the computer by installing a small utility. The process is very straightforward, and Chrome will guide you through the whole thing.

When the utility has been downloaded and installed, Chrome Remote Desktop will prompt you to enter a PIN. Make it something easy for you to remember, of course, but difficult for anyone else to figure out!

After you enter the PIN, it will take a few seconds to enable the remote connection. Once it's finished,

your computer—whatever its name is—will show up in the list.

From there, you can easily access any of your connected computers from any other computer or mobile device you're logged into. NOTE: Chrome Remote Desktop has to be **set up before you need it**—you can't do it remotely!

How to Connect to Your PC with Chrome Remote Desktop

Now that everything is all set up, you'll need to download the Chrome Remote Desktop app for your phone (Android or iOS). Fire it up to get started—I'm using a Google Pixel XL here, but the process should be largely the same regardless of which device you're using.

As soon as you launch the app, it should show a list if your computers. Tap the one you need to connect to.

It will request your PIN here, as well as offer the option to always allow connections from this device without a PIN…which I honestly don't recommend doing. If something were to happen to your phone, you don't want any would-be wrong doers having access to both your phone and your computer, after all.

With your PIN entered, tap **"Connect."**

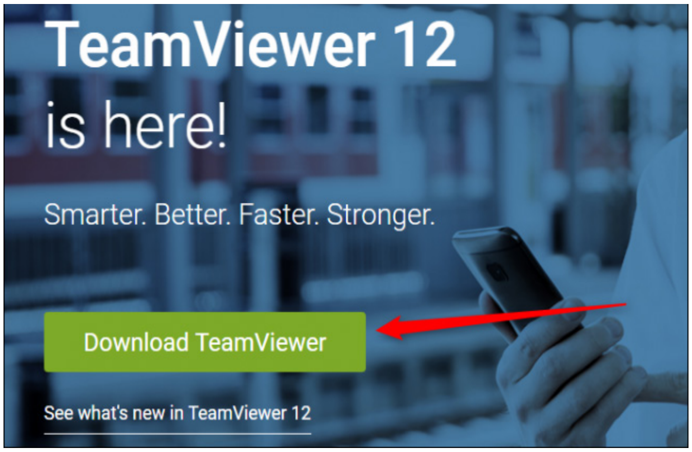
Boom. The connection will be instant. Use your finger as the mouse and tap to click.

When you're finished, just tap the **"Stop Sharing"** button at the bottom. The connection will be terminated. Easy peasy.

Option Two: TeamViewer (Windows, Mac, Linux, Android, iPhone)

It's not that hard to set up and use, but I'll warn you now, Chrome Remote Desktop is a lot simpler. And TeamViewer's complexity means it takes a lot more work to keep secure—something you absolutely need to do if you're going to use it. If you don't, you're basically leaving the door to your house unlocked, which is bad.

>>>> continued



https://www.teamviewer.com/en/download/mac/
https://www.teamviewer.com/en/download/ios/

How to Set Up TeamViewer

First, head over to the TeamViewer website and download the latest version of the program. It's a big green box on the main screen, so it's hard to miss.

During the installation, you'll need to select your installation type and use case. TeamViewer is free for personal use, so if you're just doing this on your personal computer, use that option. If you're using it for corporate use, though, be honest here.

The installation will just take a few minutes, and you'll be ready to get started.

By default, TeamViewer will provide you with a remote ID and PIN, but this is only useful if you're actually in front of your computer—the idea here is that you can provide that to someone else so they can remote access your computer. It doesn't do a whole lot of good if you're out and about and need remote access to your own system, though.

For that, you'll need to set up a TeamViewer account and connect your computer to it. To get that set up, click the "Sign Up" button in the small right-hand window. Of course, if you already have a TeamViewer account, you can just sign in.

Once you have your account all set up and ready to go, you'll also assign a password to this particular computer. Again, make it something easy to remember but hard to figure out. And now would be a good time to tweak these security settings as well.

How to Connect to Your PC with TeamViewer

To access your PC, install TeamViewer's mobile app on your Android or iOS device, then fire it up. Tap the "Computers" button at the bottom, then sign in to the account you just created.

After that, tap on "My Computers," which will show a list of all the computers currently attached to your TeamViewer account.

Tap the one you'd like to connect to. The remote connection will take a minute to get established, but after that you'll be ready to roll.

The bottom of the interface (again, on the phone) will show a quick list of things you can do: close, keyboard, actions (like keyboard shortcuts), Windows, TeamViewer settings, and hide. These are super useful settings for more than just simple tap-and-click uses, and one area where TeamViewer has a leg up on Chrome Remote Desktop.

When you're finishing doing your thing, simply click the X button (or "back") to close the connection.

How to Transfer Files Back and Forth with TeamViewer

But wait, there's more! If you're just trying to grab a couple of files, there's another option here: you can use TeamViewer's File Transfer system.

With the app logged into your TeamViewer account, tap the "Files" option at the bottom, then "Remote Files."

After you log in, tap the "My Computers" button, then select the computer you need to access.

From here, it's pretty straightforward: navigate through the file system, and tap the checkbox beside the files you'd like to transfer. With the files selected, tap the "My Files" button at the bottom, then the little paper icon at the top to transfer the files to the desired location.

When you're finished, just tap the back button to disconnect. That's really all there is to it.

There are countless other options for remote access out there, but these are two of the best cross-platform options that should work no matter what kind of computer or phone you have.

While I admittedly use Chrome Remote Desktop for all of my remote needs (which are generally rare), I concede that TeamViewer is clearly the more powerful option here. The file transfer option is brilliantly executed and easy to use. Just make sure that, if you want to take advantage of TeamViewer's power, you take the necessary steps to secure it. ■

Identify and report phishing emails and other suspicious messages

If you believe that your Apple ID has been compromised, please visit your Apple ID account page to change or reset your password immediately. If you need more help, contact Apple.

How to identify a phishing attempt

Scammers often use messages and notifications that are designed to look like they're from a legitimate company or a person that you know to try to trick you into sharing your password, credit card, or other personal information with them. Phishing scams can come as an email, text, or even a phone call or web page.

• The sender's email address doesn't match the name of the company that it claims to be from.

• The message was sent to an email address or phone number that's different from the one that you gave that company.

• A link appears to be legitimate but takes you to a website whose **URL doesn't match** the address of the company's website.

• The message starts with a generic greeting, like "Dear valued customer" — most legitimate companies will include your name in their messages to you.

• The message looks significantly different from other messages that you've received from the company.

• The phone call is unsolicited and the caller claims to be an Apple employee or support representative. Callers might use flattery, threats, or name-dropping to pressure you to give them information or money.

How to avoid phishing scams

• Turn on **two-factor authentication for your Apple ID**, so that your password alone is not enough to access your account.

• Learn more about security and your Apple ID. Use a **strong password**, pay attention to notifications about your Apple ID, and always keep your contact information secure and up to date.

• Never share temporary verification codes, that are used by Apple to verify your identity, with anyone.

• Learn how to verify that your browser is securely connected to iCloud.com and other sites. Pay attention to warnings about **expired certificates** or untrusted connections.

• Don't click any **link** in or reply to an **email or text** without verifying the sender. Instead, go to the company's website, find their contact information, and contact them directly about the issue.

• Don't click any **link or button** on a website without making sure that the address (URL) of the the company's website appears to be correct.*

• Don't open or save **attachments** from unknown senders. If you receive an attachment that you weren't expecting, contact the company to verify the contents.

• If you're not sure about the source of a **browser pop-up window,** avoid clicking any links or buttons in the window.

• Always confirm the **caller's identity** before you provide any sensitive information. If you get an unsolicited call from someone **claiming to be from Apple**, hang up and contact us directly.

Report phishing attempts and other suspicious messages to Apple

To report a suspicious email, forward the message to Apple with complete header information. In macOS Mail, select the message and choose **Forward As Attachment** from the Message menu.

These email addresses are monitored by Apple, but you might not receive a reply to your report.

• If you receive what you believe to be a phishing email that's designed to look like it's from Apple, please send it to **reportphishing@apple.com.**

• To report spam or other suspicious emails that you receive in your iCloud.com, me.com, or mac.com Inbox, please send them to **abuse@icloud.com**.

• To report spam or other suspicious messages that you receive through iMessage, please send them to **imessage.spam@apple.com.**

• If you receive a suspicious message about your account activity in the iTunes Store, App Store, or iBooks Store, please contact iTunes Support at **www.apple.com/support/itunes/store**.

On your Mac, hover your pointer over the link to see the URL in the status bar. If you can't see the status bar in Safari, choose **View > Show Status Bar. On your iOS device, touch and hold the link.*

~ apple.com

How to block ads on your iPhone or iPad

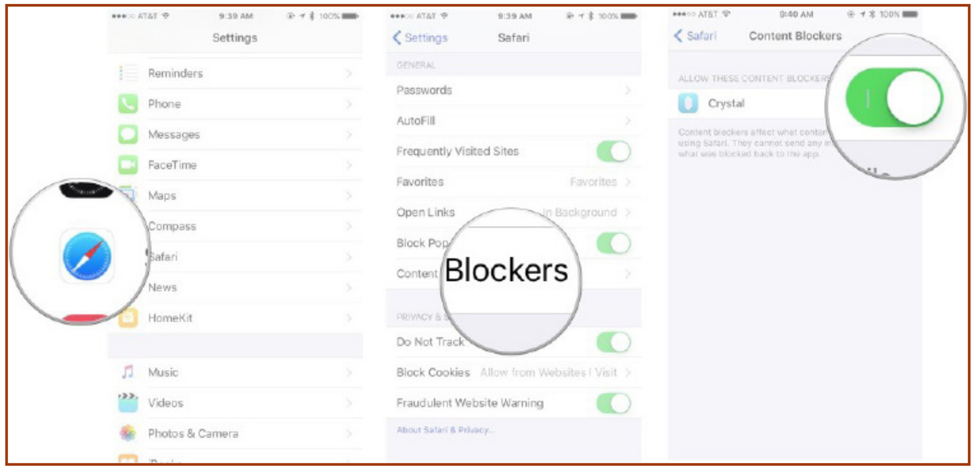
by Serenity Caldwell 7-16-16

Want to take advantage of iOS's support for content blockers? The Web has gotten messy. Whether it's ads, social widgets, or spoilers you want to avoid, you can make it a little less distracting by downloading and enabling content blocker widgets. Here's how to do so on your iPhone, iPad, or iPod touch.

Where can I block ads?

Only in Safari (or an app using the Safari View Controller). You'll also need a device with a 64-bit processor to deal with the background work, which currently includes:

- iPhone 7 & 7 Plus
- iPhone 6s & 6s Plus
- iPhone 6 & 6 Plus
- iPhone 5s
- iPad Air & 2
- iPad mini 2 & 3
- iPod touch 6



While older chipsets could run content blockers, they won't run them fast enough for Apple, and content blockers are all about speed. So, that means content blockers won't work with iPhone 5c, iPhone 5, iPhone 4s, iPad 2, iPad 3, iPad mini, iPod touch 5, or with apps that use the old UIWebView or WKWebView controllers.

How to block ads on your iPhone, iPad, or iPod touch

1 - Download your Content Blocker of choice from the App Store. We like **Crystal** - https://itunes.apple.com/app/id1022177308

You may not see the Content Blocker option in the Settings app without an applicable app installed.

2 - Open the Settings app.

3 - Go to Safari > Content Blockers.

4 - Enable the blockers of your choice.

And that's it! To disable a blocker, you can just return to this screen and turn off the switch next to it. ■

2017 MEMBERSHIP

Joining the Treasure Coast Macintosh Users Group will keep you from missing out on the best local Apple resource since the mouse — including the ***Monthly Meetings* • *Newsletter* • *Help Sessions*** and more! Membership is just $30 a year per family - getting your colorful newsletter by e-mail.

❑ $30 Yearly Dues

Check payable to: TCMUG (or Treasure Coast Macintosh Users Group)
Mail to: 1819 SW Willowbend Lane • Palm City FL 34990

Name(s) ____________________
Address ____________________ Apt. ______
City ______________ State ________ Zip ________
Home Phone ______________ Cell ______________
Email address ____________________
Birthday (ex. Sep.24) His ________ Hers ________ Retired? _
__ Beginner __ Intermediate __ Advanced __ Genius
Computer model(s) ____________________
Most used programs ____________________
__ Photos __ Web design program: ______________
__ Photoshop __ Quicken __ Skype __ FaceTime
__ FileMaker __ InDesign __ Microsoft Office

Pay dues by Credit Card at - http://www.tcmug.net

Check what devices and items you use:

__ iPhone __ Time Machine
__ iPad __ Preview
__ iPod __ Pages (layouts)
__ iMovie __ Keynote (slides)
__ Messages __ Numbers (data)
__ iDVD __ iBooks
__ iTunes __ 2+ computers

What help content would you like to see in TCMUG meetings & newsletter: ____________________

Officers

President, Newsletter, Website • Chris Kilbride
(772) 283-5646 • president@tcmug.net

Vice President & Publicity • Mark Weinberg

Hospitality • Anita Farrell
• Moe Goldy

Instructors • Paul Bendeck
• LC Campbell
• Guy Reer
• Holly Tucker

Palm Beach Liaison • Dave Sochrin

Photos & Graphics • Richard Lewis

Technical Advisor (Apple) • Bob Jorritsma
(772) 398-0748 • jorritsma@mac.com

Video Production • Bill Farrell

Helpline

1Password 201-0264 • Mark Weinberg mark@tcmug.net
Comcast 370-6407 • Bill Farrell - after 12PM bill@tcmug.net
DEVONthink Pro Office • mark@tcmug.net
DropBox 370-6407 • Bill Farrell - after 12PM bill@tcmug.net
FileMaker 283-5646 • Chris Kilbride chris@tcmug.net
iDVD 398-0748 • Bob Jorritsma bob@tcmug.net
iMovie 370-6407 • Bill Farrell - after 12PM bill@tcmug.net
InDesign 283-5646 • Chris Kilbride chris@tcmug.net
Internet 398-0748 • Bob Jorritsma bob@tcmug.net
MagicJack 370-6407 924-1084 • Bill Farrell - after 12PM bill@tcmug.net (MagicJack)
OS X 398-0748 • Bob Jorritsma bob@tcmug.net
Photos & Graphics 287-4948 • Dick Lewis dick@tcmug.net
Weebly Website • Chris Kilbride

A variety of programs for Beginners to Advanced Apple enthusiasts.

2017 CALENDAR

Jan. 19 • Feb. 16
March 16 • April 20
May 18 • June 15
July 20 • Aug. 17
Sept. 21 • Oct. 19
Nov. 16 • Dec. 7

**All located at the Children's Services Council Auditorium*

• BOARD OF DIRECTORS •
**** 2017 ****

• MONTHLY VIDEOS •
http://www.youtube.com/user/tcmug/videos

MEETING LOCATION

Children's Services Council • Stuart
http://tinyurl.com/clq2mkk
101 SE Central Parkway, Stuart • (772) 283-5646 •
Green building between Bridges Montessori & Unity Church.

West Palm Beach Apple Store - Gardens Mall:
http://www.apple.com/retail/thegardensmall/

West Palm Beach Apple Store - Wellington Green:
http://www.apple.com/retail/wellingtongreen/

Find Out How:
http://www.apple.com/support/sitemap/
https://www.apple.com/support/macbasics/

Manuals for Computers, iPhones & iPads:
http://support.apple.com/manuals/

MEETING INFO

(772) 283-5646
http://www.tcmug.net

$30 Yearly Dues per family may be paid in person (cash or check), by mail or credit card (tcmug.net)

MAILING ADDRESS

Treasure Coast Macintosh Users Group (TCMUG)
1819 SW Willowbend Lane
Palm City FL 34990