Space Coast Area Mensa

NEWSLETTER

Volume 40, Issue 3 **March 2022**

From Your LocSec

This newsletter can be thought of as an extended edition. Within these hallowed pages, I will be educating everyone on cybersecurity. This edition is just part 1 of that topic.

Cybersecurity is something everyone needs to be concerned with. It follows then that you need to be knowledgeable on the subject. I will be writing a series of articles over the next few editions of our newsletter to, hopefully, enlighten members on the threats that exist and how to protect yourselves from them. It has been said that the best defense is a good offense. That adage doesn't apply so much to cybersecurity. When it comes to cybersecurity, "The best defense is a better defense" because you can't really take an offensive stance..

.....

Our Discord server is maturing and I would encourage everyone to sign up.

Discord can be downloaded here: https://discord.com/download

Once you have a Discord account, please sign up with this invite:

https://discord.gg/s82uBqPTj4

This URL is set to never expire. Vetting members to the server might initially be a challenge so please set your Discord nickname to your real name to make that process easier.

.....

If you plan to attend any of the events scheduled for March, please RSVP directly to me so I have a head count and can make proper reservations when needed.

We have a three member team for CultureQuest this year. If you would like to join the team, just let me know. We need to register our team by March 31st.

Did you know that I post the newsletter, RVC column, Events, Recipe Corner, and Picture of the Month in Discord? I do. Neat, huh?

Jim Fitzgerald

Inside this issue:

RVC10—Thomas G. Thomas

The next meeting of the American Mensa Committee (AMC) will be held on Saturday, March 19, 2022 in Hurst, TX at the American Mensa headquarters. At the time I'm writing this column the agenda has not been finalized, but it's scheduled to be posted to https://www.us.mensa.org/lead/amc/meeting-reports/ by the end of February.

That said, it appears that the agenda will be packed. Because it's been a while since the last meeting in November, a lot of committee work has been underway in the interim. I expect there to be motions to create a pair of Task Forces which have already started working in anticipation of being approved (these being the Volunteerism Task Force and the Criminal Acts Task Force). The Communications Officer has been working on a number of motions regarding Internet Communications Services (which includes websites, email services and social media). The Gifted Youth Committee has been working on their Gifted Youth Coordinator (GYC) handbook, which hadn't been updated for many years. The Finance Committee has been working on the budget for 2022-2023,

RVC10—Thomas G. Thomas

(Continued from page 1)

which will be presented for approval by the AMC along with a motion to clarify our investment policies. A motion has been prepared to address concerns about the use of our membership lists. And these are just the ones I know about; others may be coming in over the next few days.

Aside from business to be conducted at the meeting, committees have been working on their projects. The Gifted Youth Committee kicked off their quarterly GYC roundtable in February. Simone van Egeren (Chair of the AML History Committee) posted an article in the February *Mensa Bulletin* discussing the work of the committee. The Events Planning Committee has been working on site selection research for the 2026 Annual Gathering. The Bylaws Committee has started to receive new updates for Local Group Bylaws. And there are many others I'm not aware of yet, but I expect that they will be reporting their progress via their quarterly reports at the link above.

_____

Moving to Regional activity, I attended the Central Florida Regional Gathering ("It's All Sun 'N' Games") over Martin Luther King Jr. Day weekend, this year being held at the CoCo Key Hotel and Water Resort in Orlando. As usual, Debbie Freeland did an excellent job of pulling it together after locating a venue on short notice, with the great assistance of Hospitality Chair Jennifer Keating and Speaker Chair Bill Keevan, along with the many speakers and game and tournament chairs.

I've noticed that several local groups have already started pulling together their CultureQuest® teams, but there's still time if your group hasn't joined in – or if your group has enough interest in a second team! Registrations can still be taken up to March 31.

_____

Local Groups have slowly started to hold in-person events again, although many members are still wary of group activities. As a reminder, the official position of American Mensa is to recommended that groups follow all CDC, federal, state, local, and venue requirements when hosting an event. As an aside and as a matter of courtesy, guests should follow the wishes of the host of an event, and conversely, hosts should make it known in advance whether or not they are requiring masks or vaccinations, especially for events to be held in private homes.

_____

Until next month (or until I see you online),

Thomas George Thomas
Email: RVC10@us.mensa.org
Facebook: https://www.facebook.com/thomas.g.thomas
https://www.facebook.com/groups/MensaRegion10/

Local History

Space Coast Area Mensa spans Brevard and Indian River counties. Here's a little info on how those counties came to be.

Brevard County: Established by an act of the Florida Legislature in 1854, actually signed into law by the Governor early in 1855. The initial boundaries of the new county incorporated all of what had been St. Lucie County. At that time, Brevard extended southward along the state's Atlantic east coast all the way down to present day Miami-Dade County in south Florida. The origin of the county's name is widely attributed to **Theodore W. Brevard**, Florida Comptroller at the time of the county's creation. In the decades after it was first established, the boundaries of Brevard County were amended several times. It took on its current shape in 1905.

Indian River County: Vero was settled by early pioneers in the 1880s. One of Vero's most notable early settlers was Henry T. Gifford. In 1887, he built a house which is now located near present-day City Hall. He operated a citrus grove business and established Vero's first mercantile store which also operated as a post office, express office and railroad ticket office. The story of how "Vero" got its name is often attributed to his wife Sarah who suggested the settlement be named for its Latin meaning, "to speak the truth." In 1893, the Jacksonville, St. Augustine and Indian River Railroad tracks reached the Vero settlement and Henry Flagler's dream of building a railway through to Key West was coming closer to fruition. Trains not only provided much needed farming, building and cooking supplies, helping to make Florida's wilderness more habitable, but improved commerce by providing faster transport of agricultural products and other goods.

In 1919, the City of Vero was incorporated. In 1925, a number of Vero's most prominent citizens successfully lobbied in Tallahassee for the creation of a new county that they named "Indian River." Vero was designated the county seat and was re-incorporated and re-named Vero Beach.

Cybersecurity — Part 1

By Jim Fitzgerald

The National Institute of Standards and Technology (NIST) defines cybersecurity as: **The ability to protect or defend the use of cyberspace from cyber attacks**. This is good stuff. Cybersecurity is our defense against cyber attacks in cyberspace. That's a lot of cyber going on. What is cyberspace? Again, from NIST: **A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.** As you can see, cyberspace encompasses areas well beyond just the Internet. When I see terms such as telecommunications and embedded systems, I immediately think of infrastructure; like dams, electrical grids, water, etc. Critical infrastructure in the United States lacks cybersecurity measures, which represents a national security risk. More than 85% of our infrastructure is privately owned, which adds to the complexity of securing our systems. Gas, water, electrical; all vulnerable to a outsider threat from a user anywhere on the Internet. I invite you to read Securing Cyber Assets: Addressing Urgent Cyber Threats in Critical Infrastructure published by The President's National Infrastructure Advisory Council. The 45 page document is available at: https://www.cisa.gov/sites/default/files/publications/niac-securing-cyber-assets-final-report-508.pdf

There have been numerous successful attacks around the world and numerous attempts which were thwarted. It is a cyber war and while no guns or missiles are being used, it is still a war and all wars carry a cost. At the 112th Congress, a hearing was held before the Subcommittee on Oversight, Investigations, and Management of the Committee of Homeland Security on April 24th, 2012. The transcript can be viewed at https://www.govinfo.gov/content/pkg/CHRG-112hhrg77380/html/CHRG-112hhrg77380.htm

Cyber attacks can be coordinated and sophisticated. They can be state sponsored, conducted by hacker groups, or even be just a lone actor. Targets are foreign governments, infrastructure, corporations, and individuals. The reason for this article is to get you, the reader, to start thinking about your own cybersecurity. We all touch cyberspace one way or another and that means cyber attacks are something you need to be aware of and this article, along with subsequent articles, is intended to help provide you with the tools to protect yourselves from the threats that are out there. They are real.

Phishing is a social engineering attack designed to trick the victim into revealing personal or sensitive information.

Provided information can be used to steal the victim's identity, access online accounts, access bank accounts, and so on.

When you are targeted by a phishing attack, there are normally some obvious clues which, once you recognize them, will help you avoid becoming a victim.

While phishing comes in various forms, let's discuss ***Email Phishing*** first:

Email phishing remains prevalent because it remains successful. Attackers use software to send emails to many thousands of addresses with a single click of the mouse. Only a few unwary recipients need to fall for the scam for the attack to be very profitable, the old 'throw a dart at the dartboard while blindfolded' concept.

Phishing emails will usually have the following characteristics:

- **Too good to be true** - Offers of an attractive reward for completing a survey or winning a prize are a couple of examples of something that is too good to be true. These will be attention-grabbing statements.
- **Urgency** - Many phishing emails will tie some urgency to their offer or deal. Others may warn that your account will be

(Continued on page 4)

FUN FACT

The saying 'Beware the Ides of March' is from Shakespeare's play "Julius Caesar" on the foretelling of Caesar coming to harm no later than the Ides of March by the seer Spurrina.

Cybersecurity — Part 1

(Continued from page 3)

closed if you don't act immediately. Cybercriminals do this to make you react and not give you the time to think about what you are doing.

- **Misleading hyperlinks** - Because hyperlinks can be composed with a friendly name (like 'My Profile', it is possible to make links that appear to be something they are not.
- **Attachments** - Any attachment from an unknown sender should immediately raise a red flag. Attachments of unrecognized file types should always be a cause of concern. Even known file types, such as .pdf or .jpg, can contain malware (malicious software) and should never be opened unless you know the sender or were expecting something from the person or company who sent the email. That brings up another issue, cybercriminals are always improving on their attacks and with so many people ordering from Amazon or Ebay, it is not unusual for us to receive emails from these companies. The cyber criminal is counting on these emails being so common that their victims let down their guard and go into a kind of autopilot. Every email you receive should be regarded as suspect.
- **Unknown senders** - Random emails from strangers really shouldn't happen very often unless you operate a business with a web front-end that is putting your email address out there. Businesses have an especially hard time because email is often the front door to the company and sometimes the only way to initiate contact, whether you are a valid customer or a cyber criminal.
- **Language:** Often, there will be typos and bad grammar in phishing emails.

How do you protect yourself from the email phishing threat? Follow these guidelines:

Preview Mode: Turn off 'preview' if your mail application, such as Outlook, supports it. Preview mode will open the email the moment you click on it in your inbox. With preview disabled, you must deliberately double-click it and it will open in its own window. We want preview disabled so you can see who the sender is and what the subject is without having to actually open the email. If it is from some random person or company you have never dealt with or the subject contains important sounding words like 'Important!', 'Hurry', 'Last chance', you are able to simply delete it without ever having opened it. Pro Tip: In Outlook, you can press shift+delete to permanently delete the email. This protects you from accidentally opening the email months later when you are rummaging around in the deleted emails folder.

Hyperlinks: For any emails you do open which look suspicious, especially ANY email dealing with a company you actually conduct business with, you can hover over a link and your email should show you what the actual link is. The text of the hyperlink in the email might say 'View My Account' but the underlying link may be to an entirely different site. Did you know that cybercriminals can easily set up web sites that look exactly like the company you use? Going to one of these fake sites and attempting to log in won't work but, the moment you entered your account credentials, they've got you. And that is all it takes. Some of these fake sites may use domain names very similar to the real company. You must look closely to see where the link will take you. Is it really amazon.com or is it actually amazom.com? These tricks are extremely effective because people are comfortable getting emails from amazon and they aren't scrutinizing the email at all. Cybercriminals are counting on your complacency for their attack to work.

Attachments: Any attachment can be a threat. Maybe .txt is still safe. Adobe .pdf format is not safe and neither is .jpg or .png. Having preview mode off really helps here because the picture will not display (meaning it was read by the computer) unless you have opened the email. Since images can be inline, just opening the email may read the image. In other emails, the image may be an actual attachment you must deliberately open. There is really no way to know which it will be until you open the email itself. One thing you can do in Outlook is to disable automatic download of images. This is an excellent protective measure making it much safer to open an email that you aren't sure is legitimate or not. If it is legitimate, all you have to do is right-click a broken image in the email and select 'download images'. The thing to recognize here is that you had control of all of it. You choose to open the email or not open it. You choose to load images or not load them. Anything that puts you in control of protecting yourself is a very good thing.

Too good to be true: "Congratulations! You've won a 90" LG 8K television!" You immediately feel kinda special. I mean, not everyone can win a 90" tv right? If you had really won something after having really participated in some survey or raffle to win that something, the operators would most likely be contacting you via phone. If they were to use email, it is unlikely they would use catchy

(Continued on page 5)

Cybersecurity — Part 1

(Continued from page 4)

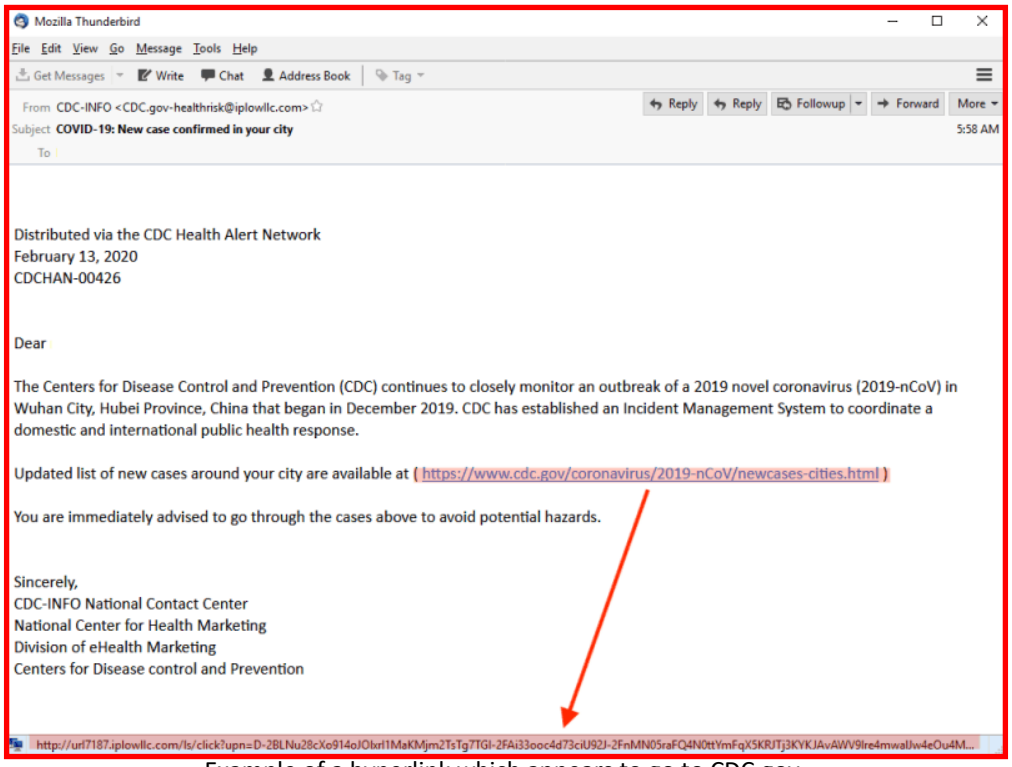
phrasing to notify you. A legitimate email would contain a professional subject line. I've personally turned down enough prizes to fill a barn. Don't fall for these scams. If you clicked on any links from these 'winning' emails, you would be taken to a site where you just need to sign into your financial site to verify your account and then your item will be shipped directly to you. It doesn't matter if you entered valid credentials or not because their site will just assume you did. All they want is your account username and password which will be changed before you can do anything about it. At least Amazon has taken steps to force you to authorize a purchase from a new device. That's some protection but it should not be relied upon as your sole defense.

Urgency: This is the big one really. Most malicious attacks require you to do something to compromise yourself. Putting urgency on whatever their scam is a great motivator to get people to do what you want them to do. "Act now! Last chance! Final Notice!" All of these are just ways to get you to do something without putting a lot of thought into it. The less you think about what you are doing, the more likely you are to fall victim to their scam. Any legitimate company would follow up email notifications with an actual letter if something became urgent. When in doubt, you can always call the company (assuming you actually do business with them) and ask if there is an issue with your account and explain the email you received. You can also go online and search for the subject line of any suspicious email and see if others are reporting it as spam or malware. Some companies, when they become aware of a phishing email becoming wide-spread, will post on the front page of their site what to watch out for. They do this because there is really nothing they can do to stop it, so they choose to educate their customers in the hopes that it saves them from becoming victims of the scam. A few seconds of your time to protect you from them. Totally worth it.

If you feel like the email is legitimate and you are just dying to click on that link, remember you are still in control. Just because they provided a convenient link for you to click on doesn't mean you have to use it. If Netflix is asking you to validate your account or update your credit card information, you can easily use our own bookmark for Netflix and safely go to the site that you are certain is the right one and securely log in from there. Once done, you can shift+delete that email because you no longer need it. You can also set a reminder on your calendar to notify you that your credit card will expire for auto-paymen in the month prior to its actual expiration.

All of your accounts should be set to multi-factor authentication. This means that in order to log into your account, you must provide

(Continued on page 6)



Example of a hyperlink which appears to go to CDC.gov.
When hovered over, the link shows it is actually going to a completely different web site.

Cybersecurity — Part 1

(Continued from page 5)

something only you have and something only you know or something only you are. These could be a credit card number (something you have), a PIN (something you know) or a facial/retina scan (something you are).

You can also leverage an authenticator application, which is a disconnected token, providing a one-time password or authentication code. This is a powerful method of protecting yourself. Just remember that a false site can look exactly like the real site. Always know what site you are opening and, if not sure, do a simple search for the site with some keywords added. Example: "is no-tascam.com legit" or "is malwaresafe.org safe".

Here are a few takeaway statistics:

- 92% of malware is delivered via email
- 98% of mobile malware targets Android devices
- MacOS malware has increased 165% in the last year
- 70% of malware payloads were ransomware
- Over 18 million web sites are infected with malware in a given week

A final tip, consider using your phone for email vetting. While mobile malware certainly exists, your phone cannot open very many attachments, which makes it safer to review email on a mobile device. If the email checks off boxes for the warning signs I've laid out in this article, you can just delete it right there on the phone and it will never reach your computer. This technique assumes you do not have your computer on all the time with your mail application open. Personally, I've not opened Outlook on my computer in over a year.

Well, that's it for Email Phishing. Below are some safe resources that you can visit to learn more about the cyber threats out there.

Next month, this series of articles will continue with other types of cyber threats and how you can protect yourself from them.

References and Further Reading

National Institute of Standards and Technology (NIST): https://www.nist.gov/
NIST Cybersecurity: https://www.nist.gov/cybersecurity
Phishing.org: https://www.phishing.org/what-is-phishing
Federal Trade Commission: https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams

Vintage postcard for Cocoa Beach

The Wright Brothers

By Steve Schneider

The Locals Thought They Were a Little Strange

Wilber (the elder brother) and Orville Wright were two clever and hardworking men who ran a modest bicycle shop in Dayton, Ohio. One should remember that the Wright brothers, "had no college education, no formal technical training, no experience working with anyone other than themselves, no friends in high places, no financial backers, no government subsidies, and little money of their own" (McCullough, 2015, p. 35). Nevertheless, they conquered heavier-than-air flight on an isolated, windswept beach, living in a shack they built themselves that had no electricity or running water. The locals found the Wright brothers' work amusing, but the time Wilber and Orville could spend in North Carolina was limited because they had to return from "vacation" to run the bicycle shop in Dayton.

Leading a small team of trusted friends and associates, they succeeded when those with much more money and support had failed. I believe the Wright brothers prevailed because of both their intelligence and leadership. They epitomized leading the "surgical team" discussed by Brooks (1995) in his classic work, *The Mythical Man-Month*. Wilber and Orville started their glider airframe designs in keeping with published data. However, much of the published information available on aeronautics was simply not correct (McCullough, 2015). Orville and Wilber constantly adjusted their approach in response to their own experimental findings. This was a highly Agile methodology that solved a problem that had challenged human beings since the days of Icarus.

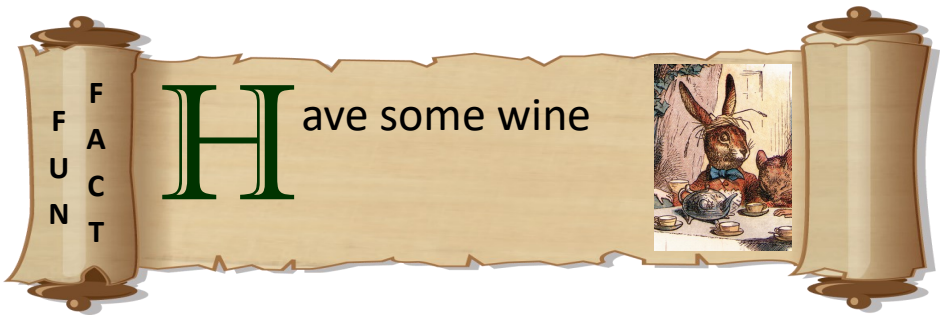
Samuel P. Langley, the head of the Smithsonian Institution, was working on the airplane at the same time as the Wright brothers. Langley had financial backers and large government grants. Everything was in his favor. However, while the Wright brothers concentrated on solving a problem, Langley wanted glory. He launched his "aerodrome" from a catapult on top of a large houseboat located on the Potomac in Washington, D.C., on October 7, 1903. His invention immediately fell into the Potomac, broke apart, and almost drowned the pilot. Years after the Wright brothers' successful flight, the Smithsonian made modification to Langley's original aircraft and fraudulently claimed that the failure was only due to the launching device. When Orville Wright originally offered to donate his aircraft to the Smithsonian, the Smithsonian refused to accept it. (The Smithsonian changed its mind years later, and the Wright Flyer is currently on display in the Smithsonian Air and Space Museum.)

The Wright brothers successfully flew on December 17, 1903. The goal of the brothers was to solve a problem, not make a fortune, and they showed true leadership in the process. They were not interested in becoming captains of industry. They saw themselves as inventors, not manufactures. Both brothers were remarkably unaffected by the fame and fortune that followed their invention. In a stunning quote, Wilber remarked, "A man who works for the immediate present and its immediate rewards is nothing but a fool" (p. 246). If only those in a position of influence and power today had that wisdom!

Wilber died on May 30, 1912, of typhoid fever, at the age of 45. Orville sold the Wright Company with its patents in 1918 and established his own Wright Aeronautical Laboratory to concentrate on research. Orville died on January 30, 1948, at the age of 77. He lived to see the sound barrier broken by a jet aircraft flown by Chuck Yeager in 1947. (By the way, Chuck Yeager died in 2020 at the age of 97.) I truly believe that no one embodies the spirit of inventiveness and leadership better than Wilber and Orville Wright, who are true American heroes.

Reference

Brooks, F. P., Jr. (1995). *The mythical man-month: Essays on software engineering, anniversary edition.* Reading, MA: Addison-Wesley.
McCullough, D. (2015). *The Wright brothers*. New York, NY: Simon & Schuster.



Volunteer Opportunities

Are you ready to help Space Coast Area Mensa? Got some down time from binging and looking for something to do? If you answered yes to either question, this is the page you've been looking for.

We are seeking a volunteer to be our **Public Relations Coordinator**. This would be a non-voting role with the following duties & responsibilities:

- Community Outreach: Shameless promotion of Mensa and Space Coast Area Mensa through social media and local newspaper/magazines.
- Provide notification to ExComm when our local chapter is promoted using social media, newspapers, local magazines, and other mediums.
- Announce testing dates/times/locations in coordination with our Testing Coordinator.
- Work with ExComm for any special announcements which have been determined to be worthy of special publicity beyond normal community outreach efforts.
- Work independently with the staff PR Coordinator at the National Office to leverage the resources and experience therein.
- Other duties aligned with the above as the position matures.

Sound good? Wanna help? Just send me, your LocSec, a short email saying you are interested in becoming the Public Relations Coordinator for our chapter. Really, it will be that easy.

Newsletter Submissions

To submit articles, events, SIGs, announcements, please email locsec@scam.us.mensa.org

All submissions must be received by the Editor before the 10th of the month preceding publication. Whenever possible, we prefer submissions via email.

Editor contact information is listed above

Upcoming Events

12 Mar: Geocaching at Wickham Park. 8:30 AM meeting at youth area (see map on page 10) **RSVP**

13 Mar: Brunch with the LocSec: 11:00 AM meeting at Bonefish Grill in The Avenue **RSVP**

14 Mar: ExComm Meeting: 5:30 PM meeting at Rotary Park at Suntree in Marlin Pavilion

Picture of the Month

Eau Gallie Causeway

Photo by: Jim Fitzgerald

For the high resolution image, visit the Picture of the Month channel on our Discord server

Have a Picture of the Month for the newsletter? Submit to locsec@scam.us.mensa.org.

All submissions must be the original work of the person submitting the image.

Geocaching Event

Meeting in the youth area (marked with red X in map below)

8:30 AM on March 12

You should already have an account on geocaching.com

Please RSVP directly to locsec@scam.us.mensa.org or on Discord

Wickham Park

Recipe Corner

Contributed by Eileen L.

Hearty Slow Cooker Chili

Make 4 (1 ½ C) servings

Preparation:

1 lb lean ground beef
1 medium onion, chopped
1 Tbs chili powder
1 tsp ground cumin
1 tsp cinnamon
1 tsp oregano
2 cans (16 oz each) diced tomatoes, undrained
1 can (15 oz) pinto beans, rinsed and drained
½ C prepared salsa
Salt and pepper
3 slices of cooked and crumbled bacon
½ C (2 oz) shredded cheddar cheese
3 Tbs sour cream
4 tsp sliced black olives

Directions:

1) Heat skillet over med heat.
2) Add beef and onion; cook until beef is browned and onion is tender. Drain fat.
3) Place beef mixture, chili powder, cumin, cinnamon, oregano, tomatoes, beans and salsa in slow cooker; stir.
4) Cover and cook on low 5-6 hours or until flavors are blended and chili is bubbly.
5) Season with salt and pepper to taste.
6) Add crumbled bacon
7) Optionally serve with cheese, sour cream and olives.

SPACE COAST AREA MENSA

Local Secretary	Jim Fitzgerald	locsec@scam.us.mensa.org
Deputy Local Secretary	George Rasley	asstlocsec@scam.us.mensa.org
Treasurer	Val Valek	treasurer@scam.us.mensa.org
Recording Secretary	Elizabeth Wilder	recsecretary@scam.us.mensa.org
Area Coordinator		
Brevard County	Jim Fitzgerald	locsec@scam.us.mensa.org
Indian River County	Bob Roth	
Testing Coordinator	Hank Rhodes	testing@scam.us.mensa.org
Testing Proctor	Julie Costopoulos	
Testing Proctor	Harold (Bud) Long	
Testing Proctor	Hank Rhodes	
Newsletter Editor	Jim Fitzgerald	locsec@scam.us.mensa.org
Calendar Coordinator	Jim Fitzgerald	locsec@scam.us.mensa.org
Discord Administrator	Jim Fitzgerald	locsec@scam.us.mensa.org
Webmaster	Karen Freiberg	webmaster@scam.us.mensa.org
Membership Chair	Julie Costopoulos	membership@scam.us.mensa.org
Scholarship Chair	Julie Costopoulos	scholarship@scam.us.mensa.org
S.I.G.H.T Coordinator	Karen Freiberg	sight@scam.us.mensa.org
Social Media Chair	Jim Fitzgerald	locsec@scam.us.mensa.org
Regional Vice Chair (Area 10)	Thomas G. Thomas	RVC10@us.mensa.org

Vacant Positions (volunteers needed)

Gifted Youth Coordinator
Publicity

Mensa Links

SCAM Web Site
http://www.spacecoast.us.mensa.org/index.html

SCAM on Discord
https://discord.gg/s82uBqPTj4

American Mensa
https://www.us.mensa.org/

Mensa Connect
https://www.us.mensa.org/connect/mensa-connect/

Your Membership Profile
https://www.us.mensa.org/my-mensa/my-membership-profile/

Receiving the newsletter electronically is easy. Just follow these simple steps:

1. Go to https://members.us.mensa.org/eweb/DynamicPage.aspx?webcode=CommPref
2. Edit the top box "Publication Preferences" and set 'Local Group Newsletter' to "Electronic" and click 'Save'