



News from

The GLORIOUS SOCIETY OF THE WORMHOLE

April 2025

Hello Worms

The meeting is on even if this is being sent out rather late. I again will not be able to join you but have high hopes for next month.

The TARC fest is next weekend and I will miss seeing you there also.

Bring your drink of choice and lunch if you want. We will not be cooking but we have access to the Chamber of Commerce kitchen which has a microwave and a toaster oven so you can heat up/cook what you bring.

DID YOU KNOW

An Italian banker, Gilberto Baschiera, is considered a modern-day Robin Hood. Over the course of 7 years, he secretly diverted 1 million euros to poorer clients from the wealthy ones so they could qualify for loans. He made no profit and avoided jail in 2018 due to a plea bargain.

DON'T TRUST SEARCH ENGINES

Hoe-To-Geek by Joe Fedewa

We've all heard the warnings: "Don't trust everything AI says!" But how inaccurate are AI search engines *really*? The folks at the Tow Center for Digital Journalism put eight popular AI search engines through comprehensive tests, and the results are staggering.

First and foremost, let's talk about how the Tow Center put these AI search engines through the ringer. The eight chatbots in the study included both free and premium models with live search functionality (ability to access the live internet):

- ChatGPT Search
- Perplexity
- Perplexity Pro
- DeepSeek Search
- Microsoft Copilot
- Grok-2 Search
- Grok-3 Search
- Google Gemini

This study was primarily about AI chatbot's ability to retrieve and cite news content accurately. The Tow Center also wanted to see how the chatbots behaved when they could not perform the requested command.

To put all of this to the test, 10 articles from 10 different publishers were selected. Excerpts from each article were then selected and provided to each chatbot. Then, they asked the chatbot to do simple things like identify the article's headline, original publisher, publication date, and URL.

The chatbot responses were then put into one of six buckets:

- **Correct:** All three attributes were correct.
- **Correct But Incomplete:** Some attributes were correct, but the answer was missing information.
- **Partially Incorrect:** Some attributes were correct, while others were incorrect.
- **Completely Incorrect:** All three attributes were incorrect and/or missing.
- **Not Provided:** No information was provided.
- **Crawler Blocked:** The publisher disallows the chatbot's crawler in its robots.txt.

As you'll see, the AI search engines were wrong more often than not, but the arguably bigger issue is *how* they were wrong. Regardless of accuracy, chatbots almost always respond with confidence. The study found that they rarely use qualifying phrases such as "it's possible" or admit to not being able to execute the command

Grok-3, for example, returned a whopping 76% of its responses "confidently incorrect" or "partially incorrect." Keep in mind that Grok-3 is a premium model that costs \$40 per month, and it performed worse than its free Grok-2 counterpart.

The same can be seen with Perplexity Pro vs Perplexity. Paying for a premium model—\$20 per month in the case of Perplexity Pro—doesn't necessarily improve accuracy, but it does seem to be more confident about being wrong.

Some AI search engines have licensing deals that permit them access to specific publications. You would assume that the chatbots would be great at accurately identifying the information from those publications, but that wasn't always true.

So, what does this all mean for you? Well, it's clear that relying solely on AI search engines for accuracy is a risky proposition. Even premium models with licensing deals can confidently spew misinformation. It's a stark reminder that critical thinking and cross-referencing remain essential skills in the AI age.

Be sure to check out the complete study at https://www.cjr.org/tow_center/we-compared-eight-ai-search-engines-theyre-all-bad-at-citing-news.php for all the fascinating (and alarming) findings.

*** GOOGLE AI CAN DETECT PHONE SCAMS IN REAL TIME ***

by John Lister

Google Pixel phones can now detect potential scams in text messages and voice calls in real time. The company says the technology runs locally on phones, meaning it shouldn't compromise privacy.

After a beta testing program, Google is rolling out Scam Detection for messages to any handset running **Google Messages**. This app is available for download on the Google Play Store and can replace the default messaging app on most Android phones. Users who install it gain access to Google's latest messaging features, including spam protection, end-to-end encryption, and AI-powered scam detection.

Google is also introducing a similar feature for voice calls. This will be available exclusively to users of the Pixel 9 series, the latest models of Google's own Android handsets.

Google hasn't disclosed the exact algorithms it uses to detect scams, likely to prevent scammers from bypassing them. However, it has shared some examples of how the system works.

1. If a caller asks the user to buy gift cards to make a payment, an immediate scam warning appears.
2. If a message contains suspicious links or phrases commonly used in phishing attempts, an alert is triggered.
3. The AI system can recognize social engineering tactics such as fake account recovery scams or impersonation fraud.

To reflect the fact the user will be on a phone call at the time, there will be a three-pronged alert:

1. **Audio warning:** A verbal or tone-based alert will notify the user.
2. **Haptic feedback:** A vibration will prompt the user to check for scam indicators.
3. **On-screen message:** A visual alert will explain why the call is flagged as suspicious.

Scam calls and messages have increased in recent years due to advancements in automation, artificial intelligence, and cheap access to phone numbers worldwide. Cybercriminals can now deploy robocallers and AI-generated phishing messages at an unprecedented scale.

According to the Federal Trade Commission (FTC), Americans lost **over \$10 billion** to fraud in 2023, marking a record high. This figure represents a 14% increase from the previous year.

The Truecaller Global Spam Report also found that spam calls affected **68% of smartphone users** worldwide, with scammers frequently impersonating government agencies, banks, and delivery companies.

Here are some of the most frequently reported phone scams in recent years:

1. **Impersonation Scams:** Fraudsters pose as IRS agents, police officers, or bank representatives, claiming that the victim owes money or has suspicious activity on their account.

2. **Tech Support Scams:** The scammer claims to be from Microsoft, Google, or Apple and tells the victim their device has a virus. They then request remote access or payment for fake repairs.
3. **Gift Card Scams:** The scammer convinces the victim to purchase gift cards (e.g., from Amazon, Google Play, or Apple) as a supposed payment for taxes, bills, or to release a prize.
4. **Romance Scams:** A fraudster builds a fake romantic relationship online and then asks for money for emergencies, medical bills, or travel expenses.
5. **Fake Delivery Scams:** A text message claims a package is undeliverable and provides a link to reschedule - leading to phishing sites designed to steal credit card or personal information.
6. **"Grandma, It's Me, and I'm in Jail" Scam:** A scammer calls an elderly victim and pretends to be their grandchild in distress. They may say something like, "Grandma, it's me! I'm in jail and need bail money right away!" The fraudster pressures the victim to send money urgently, often requesting wire transfers or gift cards to "pay legal fees" before the grandparent has a chance to verify the story.

Newest Model Only

Unlike some previous features that were made available to older Pixel devices over time, Scam Detection relies on advanced AI processing. Google explains that the Pixel 9 uses its AI tool, **Gemini Nano**, while older models use a smaller machine-learning model. Testing showed that Gemini Nano significantly outperformed the other model, leading Google to limit the full feature to the Pixel 9 series.

To address privacy concerns, Google has designed the system with safeguards. Scam Detection is automatically disabled when speaking to an existing contact. Additionally, a recurring beep will sound at the start and during flagged calls to remind the user that the AI feature is actively analyzing the conversation.

Google emphasizes that all scam detection processing happens directly on the handset. No data is recorded, stored, or transmitted to Google or any third party. This ensures that personal conversations remain private.

Additionally, the processing is done "**ephemerally**," meaning that audio is analyzed only in real time and is never saved, even locally. This approach ensures that user conversations are not logged or retrievable after the call. (Source: googleblog.com)

Both the message and call Scam Detection features are optional and can be switched off at any time, including during an ongoing call.

ASTRONOMERS CRACK THE CASE OF A MYSTERIOUS DEEP SPACE RADIO SIGNAL THAT REPEATS EVERY 2 HOURS

Space.com

Astronomers have cracked the case of a mysterious repeating radio signal that has been a mystery since it was uncovered last year.

The team tracked the signal back to a strange binary system containing a dead star or "white dwarf" and a red dwarf stellar companion. The radio pulse repeats every 2 hours and was first detected a decade ago. It came from the direction of the Big Dipper.

This new research indicates that the cause of this repeating radio signal is the magnetic fields of the white dwarf and its red dwarf stellar companion slamming together in this tight binary, designated ILTJ1101.

The team tracked the signal back to a strange binary system containing a dead star or "white dwarf" and a red dwarf stellar companion. The radio pulse repeats every 2 hours and was first detected a decade ago. It came from the direction of the Big Dipper.

This new research indicates that the cause of this repeating radio signal is the magnetic fields of the white dwarf and its red dwarf stellar companion slamming together in this tight binary, designated ILTJ1101.

Previously, long-period radio bursts like this one had only been traced back to neutron stars, meaning this work puts an entirely new spin on their origins.

"There are several highly magnetized neutron stars, or magnetars, that are known to exhibit radio pulses with a period of a few seconds," team member and Northwestern astrophysicist Charles Kilpatrick said in a statement. "Some astrophysicists also have argued that sources might emit pulses at regular time intervals because they are spinning, so we only see the radio emission when the source is rotated toward us.

"Now, we know at least some long-period radio transients come from binaries. We hope this motivates radio astronomers to localize new classes of sources that might arise from neutron star or magnetar binaries."

Team leader Iris de Ruiter from the University of Sydney in Australia first discovered the signal in 2024 when she was searching through archival data collected by the Low Frequency

Array (LOFAR). LOFAR is the largest radio telescope operating at the lowest frequencies that can be detected from Earth.

The pulse first appeared in LOFAR data in 2015, and after finding its first instance, de Ruiter found six more pulses from the same source.

These flashes of radio waves can last anywhere from several seconds to a few minutes. Despite the difference in duration, the pulses repeat regularly, once every two hours.

*** FAKE CAPTCHA WEBSITES HIJACK YOUR INFORMATION ***

Malwarebytes Labs by

There are more and more sites that use a clipboard hijacker and instruct victims on how to infect their own machine.

I realize that may sound like something trivial to steer clear from, but apparently it's not because the social engineering behind it is pretty sophisticated.

At first, these attacks were more targeted at people that could provide cybercriminals a foothold at a targeted company, but their popularity has grown so much that now anyone can run into one of them.

It usually starts on a website that promises visitors some kind of popular content: Movies, music, pictures, news articles, you name it.

Nobody will think twice when they are asked to prove they are not a robot.

But the next step in this method isn't what you would normally see. If you use the checkbox, you'll be forwarded to something that looks like this:

"To better prove you are not a robot, please:

1. Press & hold the Windows Key + R.
2. In the verification windows, press Ctrl + V.
3. Press Enter on your keyboard to finish.

You will observe and agree:

"I'm not a robot – reCAPTCHA Verification ID: 8253"

Perform the steps above to finish verification.”

While these instructions may seem harmless enough, if you follow the steps you will actually be infecting yourself with malware—most likely an information stealer. In the background, the website you visited copied a command to your clipboard. In Chromium based browsers (which are almost all the popular ones) a website can only write to your clipboard with your permission. But Windows was under the assumption that you agreed to that when you checked the checkbox in the first screen.

What the obstructions in the prompt are telling you to do is:

1. Open the Run dialog box on Windows.
2. Paste the content of your clipboard into that dialog box.
3. Execute the command you just pasted.

They are not lying about what you will “observe”, but what they don’t tell you is that that’s only the last part of what you pasted, and what you are seeing is not really part of the command but just a comment added behind it.

There are a few things you can do to protect yourself from falling victim to these and similar methods:

- Do not follow instructions provided by some website you visited without thinking it through.
- Use an active [anti-malware solution](#) that blocks malicious websites and scripts.
- Use a [browser extension](#) that blocks malicious domains and scams.
- Disable JavaScript in your browser before visiting unknown websites.

The clipboard access is triggered by a JavaScript function `document.execCommand(‘copy’)`. Disabling JavaScript will stop that from happening, but it has the disadvantage that it will break many websites that you visit regularly.

***BERKSHIRE HATHAWAY EMPLOYEES WIN BIG \$ ON MARCH
MADNESS PREDICTION***

NEW YORK POST by Aeryl Zilber

A lucky Berkshire Hathaway worker finally netted the \$1 million grand prize that Warren Buffett has been dangling to win the company's annual March Madness bracket challenge.

The unidentified employee, who works at Berkshire subsidiary FlightSafety International, picked 31 out of 32 winners in the first round — including an incredible 29 straight games.

There were actually 11 others who also managed to get just one game wrong in the opening round, but the consecutive wins were used as a tiebreaker.

Each of the 11 runners-up will still walk away with an impressive consolation prize of \$100,000.

Buffett has run the bracket challenge since 2016, but despite generous prizes, nobody had ever claimed the grand prize.

Remarkably, the winner's luck didn't stop in the first round. He continued the winning predictions — accurately picking 13 straight second-round matchups. Overall, the employee correctly identified 44 out of the first 45 games.

Statistically speaking, Berkshire Hathaway noted, the probability of achieving such accuracy by mere chance is approximately one in 780 billion, assuming each game had equal odds.

"I feel good that we sort of hit the sweet spot on this one," Buffett told the Wall Street Journal. He was referring to a decision he made several years ago to adjust the contest rules — making it slightly easier by no longer requiring absolute perfection from employees in the opening round.

Buffett, 94, has long expressed a desire to give away significant prize money through the contest, especially while he's still actively involved with Berkshire Hathaway. "I'm getting older," Buffett previously told the Journal. "I want to give away a million dollars to somebody while I'm still around as chairman." The financial magnate added that he expected the substantial reward to spark excitement "all over the place."

Interestingly, Buffett has yet to learn the winner's identity, as the employee chose to remain anonymous. FlightSafety International, a relatively small subsidiary within the Berkshire empire, employs fewer than 5,000 individuals — just a small fraction of Berkshire Hathaway's roughly 392,000-person workforce.

This landmark victory contrasts with Berkshire's previous contests, notably a public challenge launched in 2014, in which the conglomerate insured a \$1 billion prize for anyone who could correctly forecast all 63 NCAA tournament games. After that ambitious challenge proved impossible, Buffett simplified the requirements to predicting the initial 48 games correctly, yet a grand prize winner remained elusive until now.

Representatives from both Berkshire Hathaway and FlightSafety International were unavailable for comment.

CLUB MEETING and ZOOM

The meeting time is 1100 on Saturday morning at the Lurie Civic Building on the St Petersburg College campus in Seminole. Turn west at the light at 113th St N and about 92nd Ave N. It's the first building on the north side. Here is a link to a Google map: [Google Maps](#). There are a few parking spots in front the Chamber building but double parking is fine since we will be able to find the owner to move his vehicle if necessary. Alternately if you go another 100 yards past you can park in the college parking lot. We cannot run Zoom and a computer presentation at the same time. Below is the Zoom information, same as last month. The ZOOM meeting is limited to 40 minutes so I will start it early and restart it to cover the whole meeting.

Topic: Bill Williams' Zoom Meeting
Time: This is a recurring meeting Meet anytime

Join Zoom Meeting
<https://zoom.us/j/2737114584?pwd=d1BETHVOQ21vWWZXZ0lYQ0FIWWtldz09>
Meeting ID: 273 711 4584
Passcode: worm

CLUB NETS

Check in on the club net Thursdays at 1930 and 2000 (or at the end of the 2M net). 2M at 146.850 – with a tone of 146.2. Our 6M net runs after our regular 2M net on 53.150 – 1MHz offset 146.2 tone.

LOCAL NETS

MONDAY

1830 147.060+ no tone	St Pete ARC daily net	St Petersburg
1900 144.210 USB	CARS, vertical polarization	Clearwater
1900 147.135 +146.2	Zephyrhills ARC	Zephyrhills
2000 147.165+ 136.5	Brandon ARS	from Brandon
2000 50.135	Pinellas ARK	Pinellas County
2030 NI4CE system	EAGLE Net, NTS traffic net,	NI4CE system
2030 145.450	Pinellas ARK	Pinellas County

TUESDAY

1830 147.060 no tone	St Pete ARC daily net	from St Petersburg
1900 50.200 USB	6M net	Brandon ARS
1900 28.365 USB	10M Net	Clearwater
1900 NI4CE system	WCF Section VHF ARES	NI4CE system
1930 145.170 & 442.4 both pl 156.7	Pinellas ACS net	Clearwater
1930 444.900 +141.3	Sheriff's Tactical ARC	Tampa
2000 NI4CE system	WCF Skywarn net	NI4CE system
2000 147.105+ 146.2	Tampa ARC net	from Tampa
2000 28.365 USB	simplex	Brandon ARS
2030 NI4CE system	EAGLE Net, NTS traffic net	NI4CE system
2100 28.465 USB	10/10 net	from Orlando
1900 146.490 simplex	3 RD Tuesday monthly, Hillsborough Co ARES simplex Net	

WEDNESDAY

1830 147.060 no tone	St Pete ARC daily net	from St Petersburg
1900 147.165 + 136.5	Humpday Net	from Brandon

1930 52.020 simplex	Suncoast 6'ers	from St Petersburg
1930 NI4CE system	WCF Section Digital Info Ne	NI4CE system
2000 147.105 146.2	Greater Tampa CERT net	from Tampa
2000 146.97- 146.2	Clearwater ARS	from Clearwater
2030 NI4CE system	EAGLE Net, NTS traffic net	NI4CE system
2100 NI4CE system	Tampa Bay Traders Net	non-affiliated
0000-2359 HF Winlink	Winlink Wednesday Net https://winlinkwednesday.net/reminder.html	

THURSDAY

1800 146.52 simplex	Hillsborough ARES/RACES	North Tampa
1830 147.060 no tone	St Pete ARC daily net	from St Petersburg
1900 444.750 +146.2	Fusion net	from Tampa
1915 224.660- no tone	St Pete ARC	from St Petersburg
1930 146.6385 -127.3	Lakeland ARC	from Lakeland
1930 440.1 +162.2	Hillsborough ARES/RACES	from Tampa
1930 146.850- 146.2	Wormhole	from Pinellas Co
2000 53.150 -1MHz 146.2	Wormhole	from Pinellas Co
2030 NI4CE system	EAGLE Net, NTS traffic net	NI4CE system

FRIDAY

1830 147.060 no tone	St Pete ARC daily net	from St Petersburg
1900 3.830 LSB	Brandon 80M Net	from Brandon
2030 NI4CE system	EAGLE Net, NTS traffic net	NI4CE system

SATURDAY

0730 3.940 (7.281 Alt.) +/- QRM	WCF Section HF Net	from WCF
1830 147.060 no tone	St Pete ARC daily net	from St Petersburg
2030 NI4CE system	EAGLE Net, NTS traffic net	NI4CE system

SUNDAY

0800	3.933	Florida Traders Net	non-affiliated
1830	147.060 no tone	St Pete ARC daily net	from St Petersburg
1930	NI4CE system	WCF Section Net	NI4CE system
2000	147.550 simplex	550 Simplex Net	Pinellas County
2030	NI4CE system	EAGLE Net, NTS traffic net	NI4CE system
2100	144.210 USB	Clearwater ARS	vertical orientation

FOR SALE / WANTED

Anyone having something for sale or who might be looking for an item let me know. I will not print phone numbers or email addresses unless specifically told to since this newsletter might end up on the web. The exception is when I get the information off the web. If you are a member of the Wormhole then you can ask club members for the persons contact information. If you are not a member ... why not? OK, if you are not a member you can contact me at the email address at the end of this newsletter, I will give you the information to contact the person involved. If you want to see anything here and you are coming to the meeting let the seller know, maybe he can bring it.

FOR SALE,

See Bill AG4QX for the following: make me an offer.

*ICOM IC-W32A , 2m and 440 HT, AA battery pack	\$25
*Heathkit HD-1215 Phone patch looks ok	\$10
*Drake WV-5 wattmeter looks ok	\$75
*Cushcraft A4S, 10/15/20 4 element beam	\$250
*Cushcraft AV-12AVQ, 10/15/20 vertical	\$125
*Cushcraft A50-#S, 6m beam	\$125
*Cushcraft A-#WS, 17/12 WARC beam	\$250
*15000 V neon sign transformer currently used for Jacobs ladder	\$30

HAMFESTS

2025

April 12

TARCFest TARC Clubhouse, 22nd St at the river, 8AM-1PM, \$5 entry including tailgate, a few inside tables must be reserved in advance, talkin on 147.105 +146.2, license testing after, more info at <http://hamclub.org/>

May10

EPARS Hamfest, American Legion, 37745 Church Ave, Dade City, gate \$5, tailgate \$5, inside table \$10, talkin 146.880 (-.600) 146.2, contact Chris Bloxsom , AA4CB, PO Box 2199 St. Leo , FL 33574 or 224-221-5064 or aa4cb@yahoo.com, **Website:** <http://eparsonline.org>

May 16-18 Xenia, Ohio, Dayton Hamfest, tickets \$30 at the door, tailgate \$30, 10x10 booth \$705

May 24

WormFest 2025, Pinellas Park, admission FREE, tailgate free, Freedom Lake Park, 9990 46th St N, southeast corner of US 19 and 49th Street, 33782. Park opens at sunrise for vendor setup, hamfest starts at 0800. Talk-in on 146.850 – 146.2. All FREE! For a map and directions see <http://www.TheWormholeSociety.org> .

August 23

TARCFest TARC Clubhouse, 22nd St at the river, 8AM-1PM, \$5 entry including tailgate, a few inside tables must be reserved in advance, talkin on 147.105 +146.2, license testing after, more info at <http://hamclub.org/>

November 8

Pinellas Park, SPARCFest, admission FREE, tailgate free, Freedom Lake Park, 9990 46th St N, Southeast corner of US 19 and 49th Street, Talk-in on 147.060+ no tone. VE testing at 0900. Website has not been updated yet.

December 12 & 13

Plant City, the 2025 Tampa Bay Hamfest and West Central Florida Section Convention, Friday and Saturday, at the Strawberry Festival grounds, admission \$13, 16x40 ft tailgate space \$10, electric \$10, for information contact Bill Williams AG4QX, chairman@fgcarc.org or go to <http://www.tampabayhamfest.org> or you can just ask me, Jim or Dee at a meeting ;-)

2026

January 17

TARCFest TARC Clubhouse, 22nd St at the river, 8AM-1PM, \$5 entry including tailgate, a few inside tables must be reserved in advance, talkin on 147.105 +146.2, license testing after, more info at <http://hamclub.org/> Date not confirmed .



Fourth full weekend January	Winter Field Day https://www.winterfieldday.com/
Late January	Gasparilla celebration
Late February	West Central Florida Tech Conference http://arrlwcf.org/wcf-special-events/wcftechconference/
March/April	MS Walks
April	MS150 bike now named Suncoast Challenge http://www.citrustour.org/register.php
March/April	Mass Casualty Exercises
Late April	Southeastern VHF Society Conference, http://www.svhfs.org
Late April	Florida QSO Party
Mid May	March For Babies (was March of Dimes) https://www.marchforbabies.org/Registration/Events
Mid May	Annual Armed Forces Crossband Test
Mid-May	Florida Hurricane Exercise
Late May	Dayton Hamfest
May, Memorial Day Weekend	Wormfest
First weekend in June	Museum Ships on the Air
Fourth weekend in June	Field Day http://www.arrl.org/contests/announcements/fd/
Third weekend in August	International Lighthouse/Lightship Week https://illw.net/
September	Run for All Children's
Mid October	The Great Shakeout https://www.shakeout.org
October, 3 rd weekend	JOTA, Scout Jamboree-on-the-AIR (around 14.280MHz)
Early December	ALS bike ride in Walsingham Park
December, Second weekend	Tampa Bay Hamfest http://www.fgcarc.org/

North American QSO Party

Mode	Contest Weekend
CW	2nd full weekend January 1 st full weekend August
SSB	3 rd full weekend January 3 rd full weekend August
RTTY	last Saturday February 3rd full weekend July

YOUR WORMHOLE OFFICERS

Bill AG4QX is President and editor of this newsletter, the Vice President position is open, Treasurer is Jim KD4MZL, Paul KA4IOX is the Secretary, Dee N4GD is the Repeater Trustee and Mike KV0OOM is our webmaster.

YOUR WORMHOLE REPEATERS

53.150 -1Mz PL 146.2

442.625 +5Mz PL 146.2

146.850 - 600Kz PL 146.2

The Wormhole 2M and 440 repeaters are both now dual mode Yaesu DR-2X. FM analog as always and Yaesu Fusion, a C4FM digital mode.

The Wormhole website is at: <http://www.TheWormholeSociety.org>.

West Central Florida Section website: <http://www.arrlwcf.org/>.

The ARRL website is at: <http://www.arrl.org/>

This newsletter is written for The Glorious Society of the Wormhole, an ARRL affiliated amateur radio club located around the Seminole section of Pinellas County Florida. Anyone wishing to be added or removed from The Glorious Society of the Wormhole mailings please write to me at the address below and thy will be done.

73,

Bill Williams

AG4QX

[ag4qx AT arrl DOT net](mailto:ag4qx@arrl.net)