devcon
MIDWEST

AI to benefit all humanity

# ChatGPT: Caveat Emptor

**ca.ve.at emp.tor** *noun*, *Latin*: let the buyer beware

nvisia
connect. build. enable.

Any sufficiently advanced technology is indistinguishable from magic.

~ Third Law, Arthur C Clarke

nvisia
connect. build. enable.

# Show of hands

Who has not tried ChatGPT yet, for work?

# Show of hands

Who uses ChatGPT Plus?

nvisia
connect. build. enable.

# Show of hands

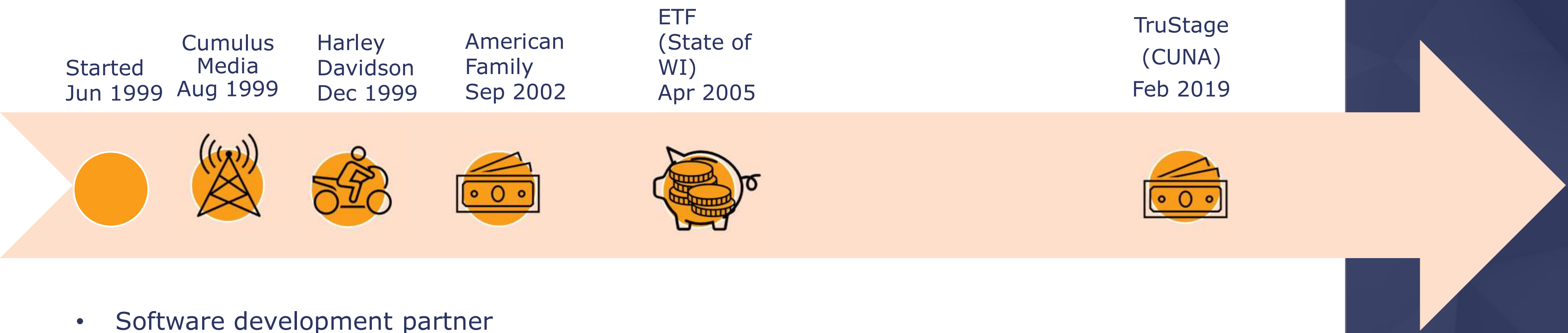
Other OpenAI products?

## Naveen VK

**Technical Director**

**naveen@nvisia.com**

nvisia
connect. build. enable.



Started
Jun 1999

Cumulus
Media
Aug 1999

Harley
Davidson
Dec 1999

American
Family
Sep 2002

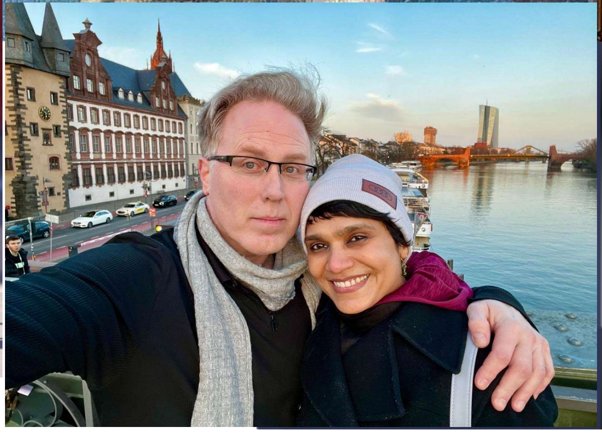
ETF
(State of
WI)
Apr 2005

TruStage
(CUNA)
Feb 2019

- Software development partner
- Offices: Chicago-IL, Milwaukee-WI, Madison-WI
- Offerings: Agile Leadership, Creative/UX, DevOps/Cloud, Product Management, Software Development
- Industries: Financial Services, Insurance, Government, Healthcare, Manufacturing, Travel, etc.

nvisia
connect. build. enable.

# I’m also really into…

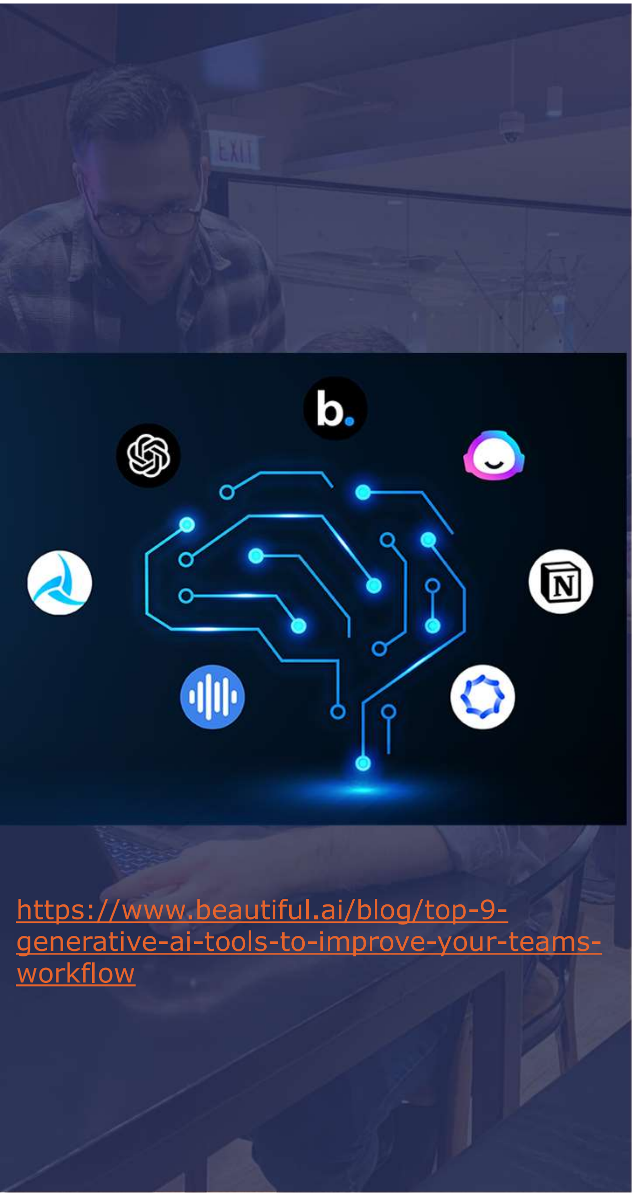


in Naveen VK
navnoon
f Naveen VK

nvisia
connect. build. enable.

# OpenAI

**AI benefits all humanity**



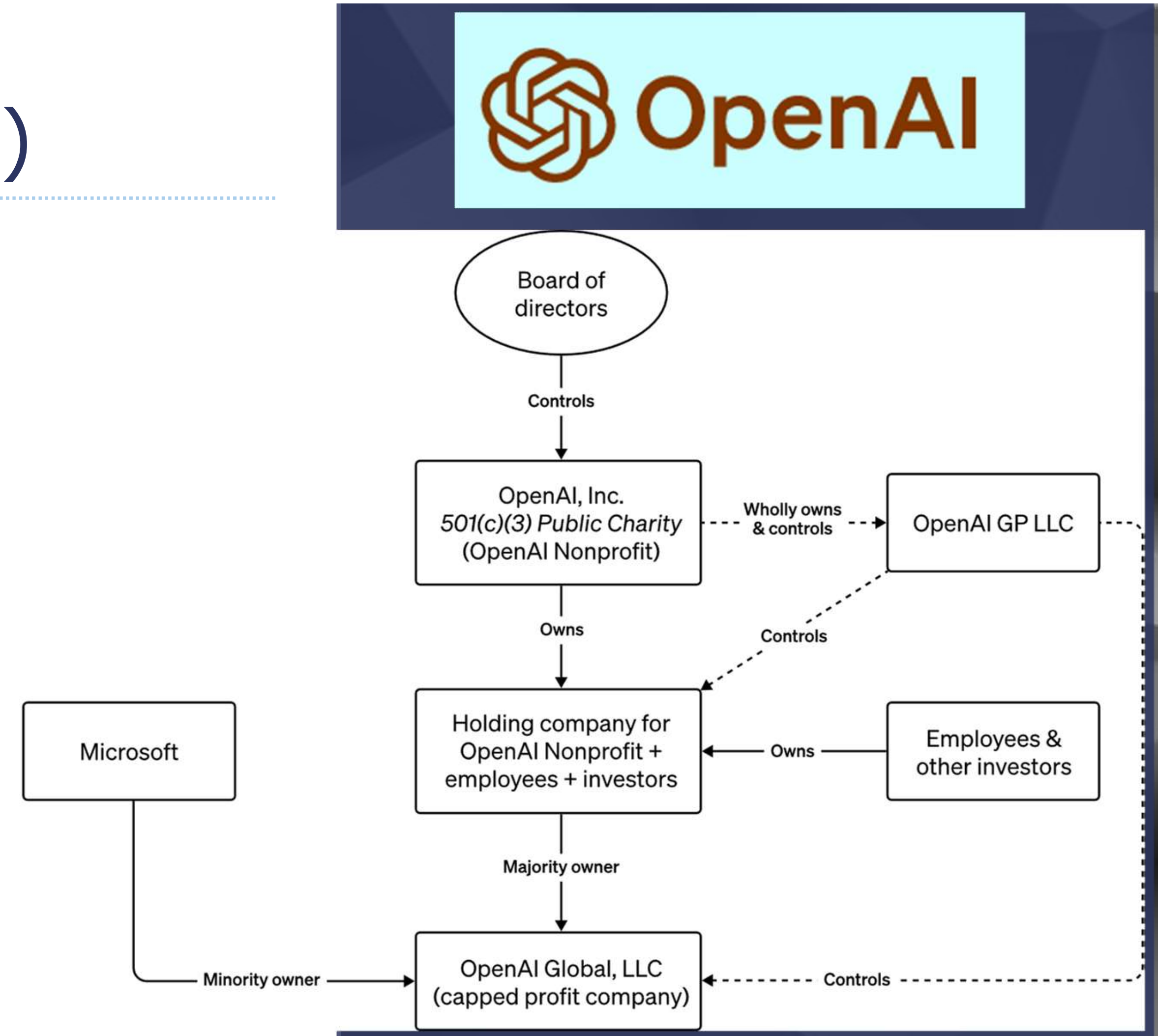
https://www.beautiful.ai/blog/top-9-generative-ai-tools-to-improve-your-teams-workflow

# Generative AI (GAI)

- AI for generating text, images, music, art, video, data, code, etc.
- Uses Neural Networks like Transformers
- Generates original content based on training data
- Some GAI tools
  - ChatGPT
  - GitHub Copilot
  - MidJourney

# OpenAI (openai.com)

- GAI R&D company
- Mission: “To ensure AI benefits all humanity”
- Started: 2015 as a non-profit
- 2019 “capped profit” arm in partnership with MS
  - 100 x investment



# OpenAI Products

- APIs and Libraries
- **ChatGPT**/**Plus** – Chatbot
- **DALL.E** – Creates images from text
- **CLIP** – Creates text from images
- **Whisper** – Speech to text. Translates many languages to English
- **Jukebox**, **MuseNet** – Create music

nvisia
connect. build. enable.

AI will either be the best, or the worst thing ever to happen to humanity.
~ Stephen Hawking

# ChatGPT

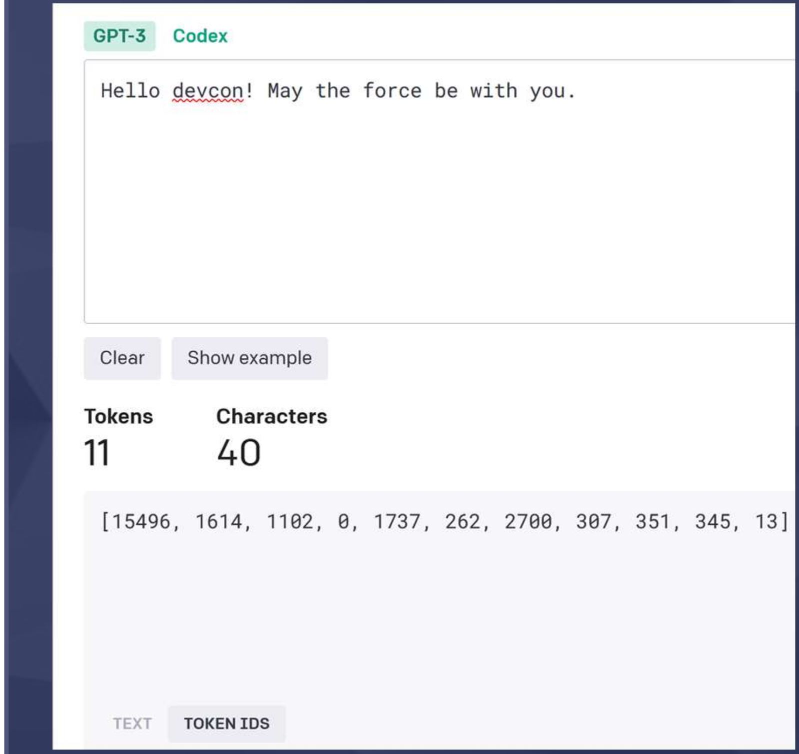
## GPT 3.5, 4

# Audience participation

When did you first use ChatGPT? For what?

# Key concepts

- **GPTs** (Generative Pre-trained Transformer)
  - Transformer model trained to understand natural language
  - Text inputs are called "prompts"
  - Produces conversational text output
- **Embeddings**
  - Vector (floating point numbers) representation of data/text
  - Preserves content/meaning
  - Used for searching, classification, clustering, etc.
- **Tokens**
  - Chunks of text, common sequence of characters



```
Hello devcon! May the force be with you.
```

Tokens 11

Characters 40

```
[15496, 1614, 1102, 0, 1737, 262, 2700, 307, 351, 345, 13]
```

https://platform.openai.com/tokenizer

# Transformer Model Architecture

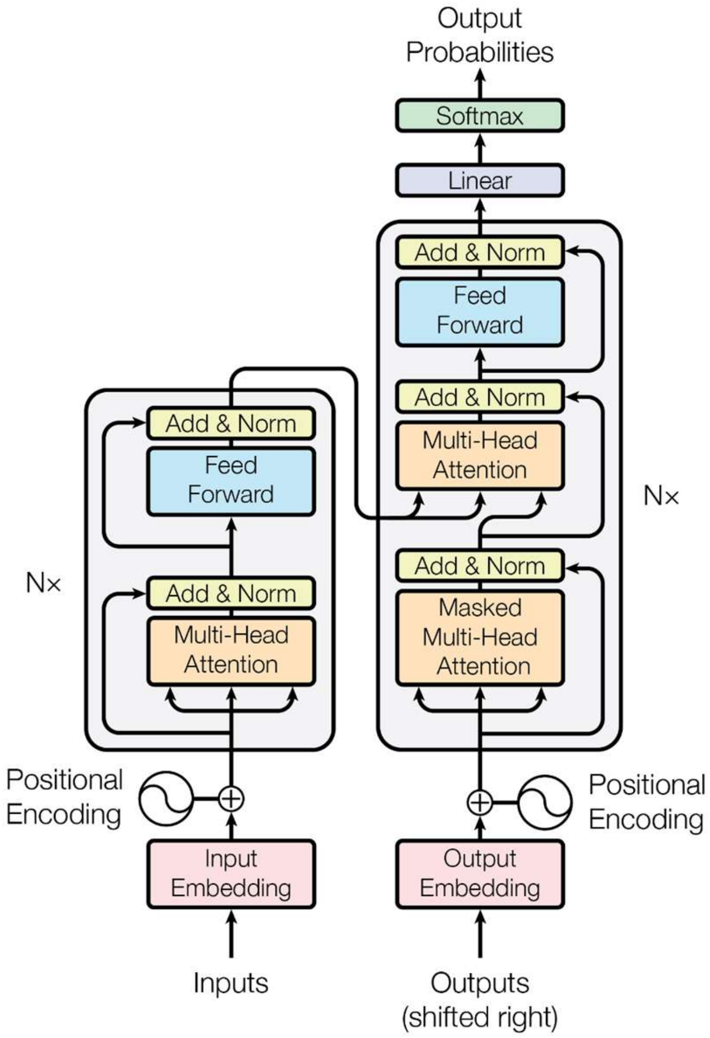


Figure 1: The Transformer - model architecture.

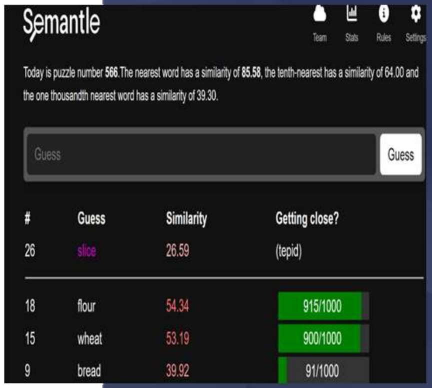
**"Attention is all you need"**

**2017**

https://arxiv.org/abs/1706.03762

# How does ChatGPT work?

- Transformer model: captures patterns, contextual relationship between words in the input text, parallel processing
  - Model was trained on large collections of text (Sep 2021)
- 2-step training process: pre-training and fine-tuning
  - In pre-training, predicts next word in the sentence
  - In fine-tuning, generates human-like, conversational responses
- Prompt engineering: prompts/instructions for desired output
  - Example: Explain passive loss carryover IRS
- Beam search: generates most probable sequence of words
- Positional encoding: provide info on position/order of words

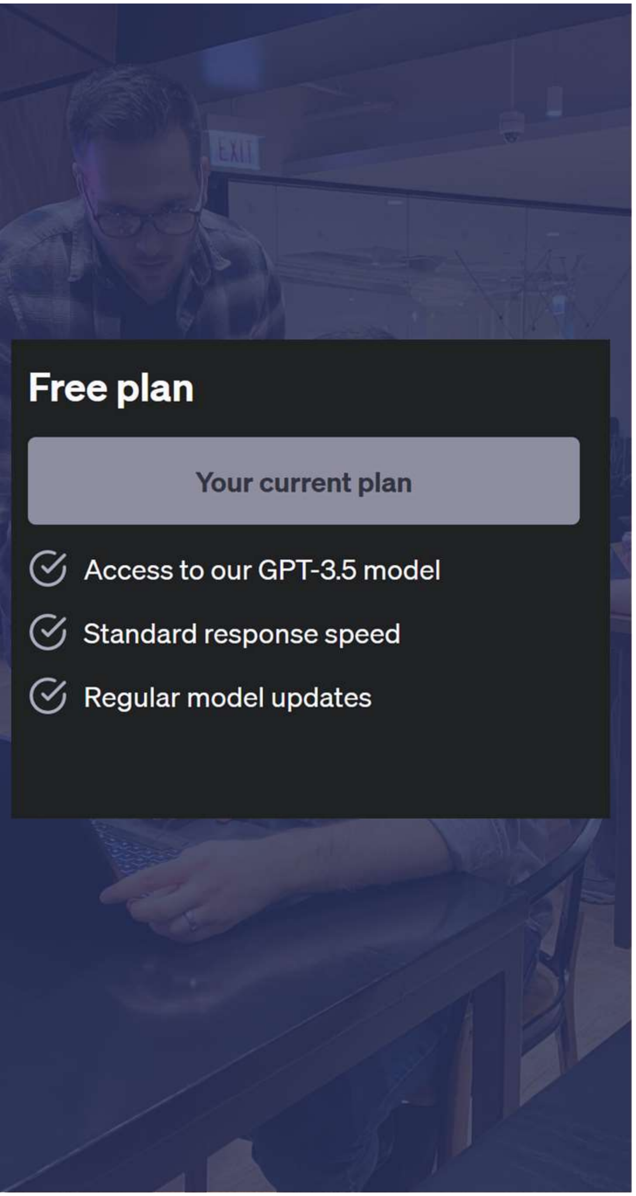


Today is puzzle number **566**.The nearest word has a similarity of **85.58**, the tenth-nearest has a similarity of 64.00 and the one thousandth nearest word has a similarity of 39.30.

| # | Guess | Similarity | Getting close? |
|---|---|---|---|
| 26 | slice | 26.59 | (tepid) |
| 18 | flour | 54.34 | 915/1000 |
| 15 | wheat | 53.19 | 900/1000 |
| 9 | bread | 39.92 | 91/1000 |

You know nothing, *Jon Snow.*
*~Ygritte, A storm of swords*

nvisia
connect. build. enable.



Free plan

Your current plan

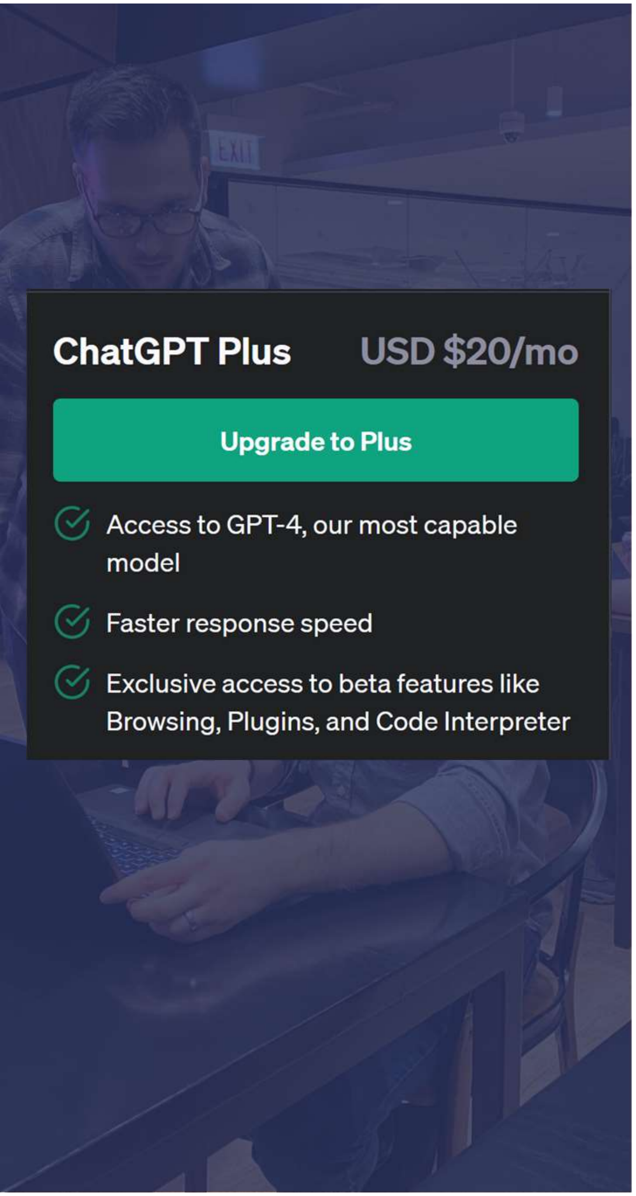
- Access to our GPT-3.5 model
- Standard response speed
- Regular model updates

# ChatGPT

- November 2022
- Uses GPT-3.5
  - 12 layer transformer model
  - 175B parameters
- Trained on books, articles, websites
  - Last updated September 2021
- Maximum 4096 token limit for input and output
  - Around 819 words, average 5 letter words
- Only text-based input and output

# ChatGPT Plus

- February 2023
- Uses GPT-4
  - 24 layer transformer model
  - 100T parameters
- Trained on text and images
  - With human feedback
- Subscription service
  - $20/month
- 25K word limit
- Can process both text and images



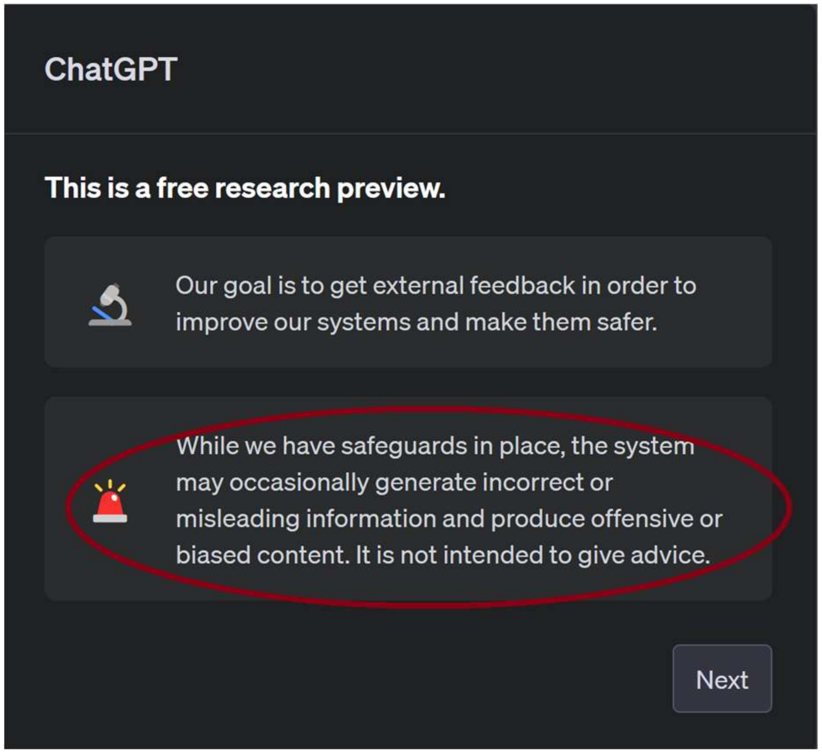
**ChatGPT Plus** USD $20/mo

- ✓ Access to GPT-4, our most capable model
- ✓ Faster response speed
- ✓ Exclusive access to beta features like Browsing, Plugins, and Code Interpreter

caveat emptor *noun, Latin: let the buyer beware*

nvisia
connect. build. enable.

# ChatGPT login screens

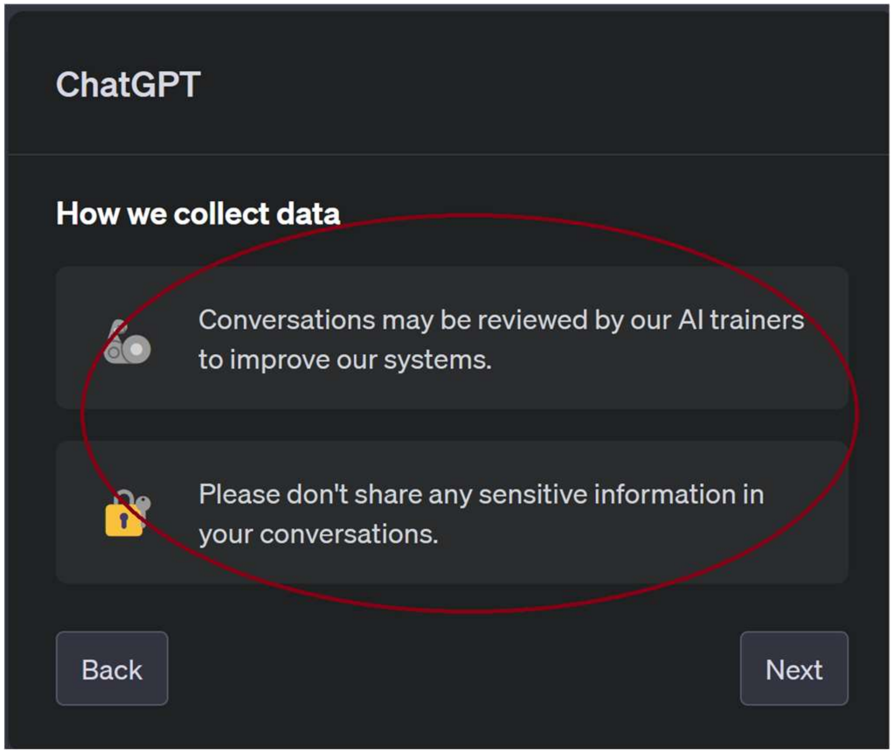


ChatGPT

**This is a free research preview.**

Our goal is to get external feedback in order to improve our systems and make them safer.

While we have safeguards in place, the system may occasionally generate incorrect or misleading information and produce offensive or biased content. It is not intended to give advice.



ChatGPT

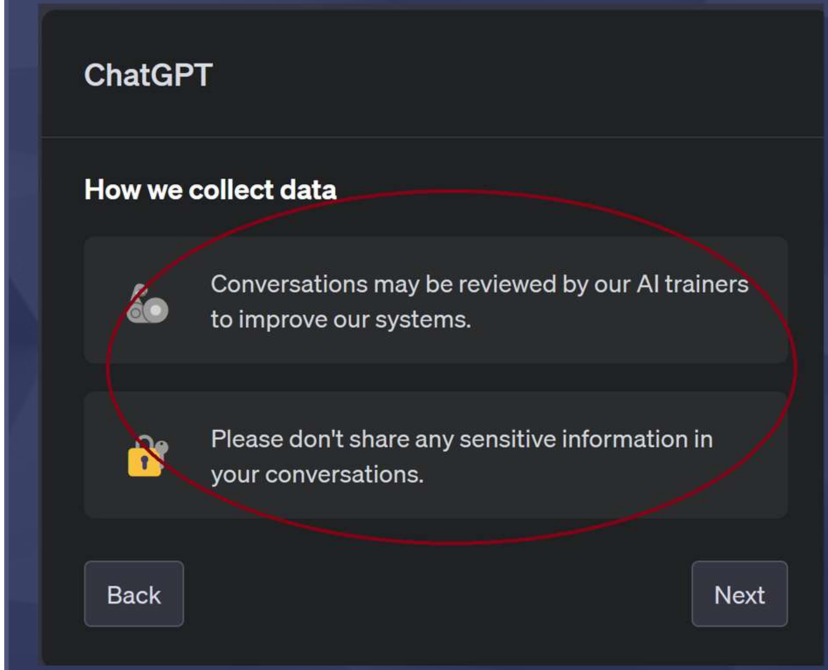
**How we collect data**

Conversations may be reviewed by our AI trainers to improve our systems.

Please don't share any sensitive information in your conversations.

# Some issues with ChatGPT

- Hallucinations
  - Responses look accurate, convincing, plausible, and coherent but are completely fabricated and fictional
- Privacy, cybersecurity concerns
- Training data is outdated (09/2021)
  - Does not cover all topics and all languages
  - Susceptible to bias
- Limited memory
  - Loses context in long conversations
- Inappropriate, biased content
- Attribution, copyright, responsibility
- [https://cdn.openai.com/papers/gpt-4-system-card.pdf](https://cdn.openai.com/papers/gpt-4-system-card.pdf)



ChatGPT

How we collect data

Conversations may be reviewed by our AI trainers to improve our systems.

Please don't share any sensitive information in your conversations.

nvisia
connect. build. enable.

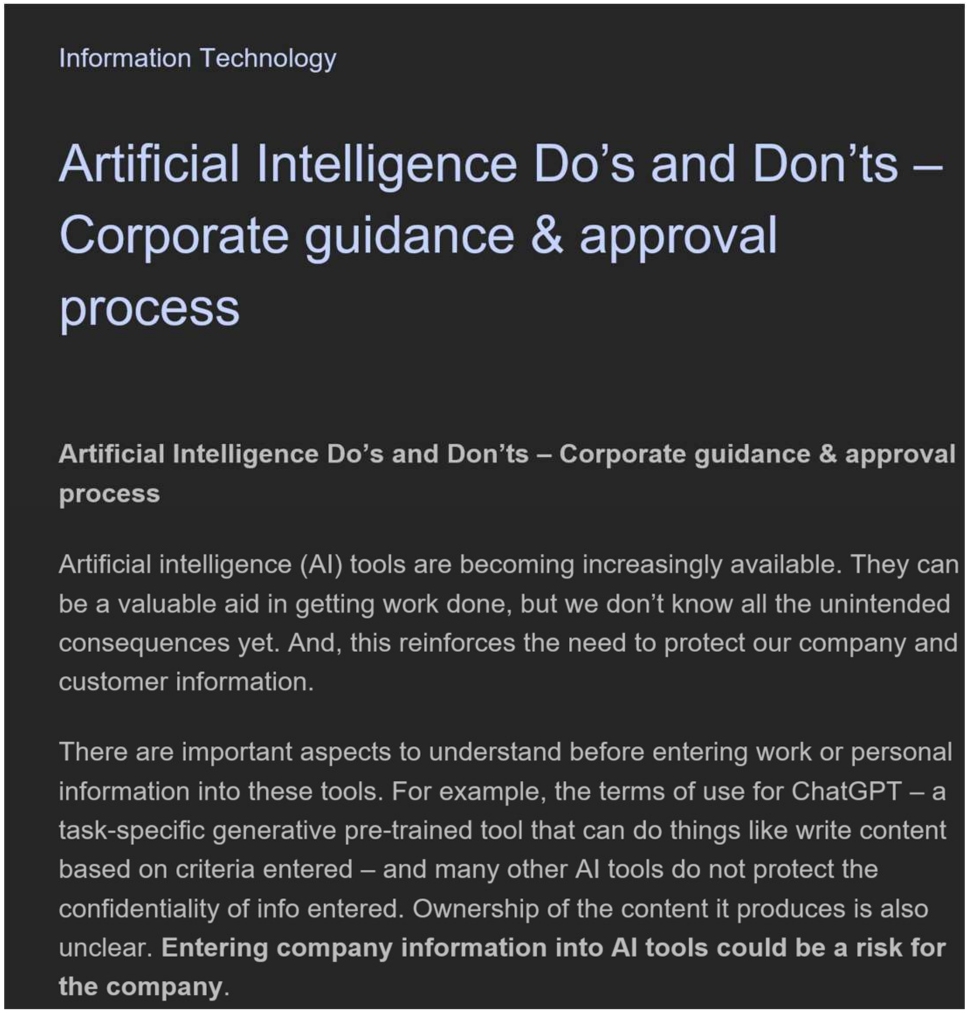
# ChatGPT negative press ☹

- AI content not eligible for copyright: 2/22/23
  - https://www.reuters.com/legal/ai-created-images-lose-us-copyrights-test-new-technology-2023-02-22/
- ChatGPT banned in Italy over privacy concerns: 4/1/23
  - https://www.bbc.com/news/technology-65139406
- FTC investigating ChatGPT over potential consumer harm by generating incorrect information about them: 7/13/23
  - https://www.npr.org/2023/07/13/1187532997/ftc-investigating-chatgpt-over-potential-consumer-harm
- ChatGPT's accuracy degrading over a few months: 8/1/23
  - https://arxiv.org/pdf/2307.09009.pdf
- Lawyer apologizes for *fake court citations* from ChatGPT: 5/28/23
  - https://www.cnn.com/2023/05/27/business/chat-gpt-avianca-mata-lawyers/index.html
- Samsung software engineers put proprietary code in ChatGPT: 4/7/23
  - https://www.pcmag.com/news/samsung-software-engineers-busted-for-pasting-proprietary-code-into-chatgpt
- Open AI classifier shut down: 7/20/2023
  - https://openai.com/blog/new-ai-classifier-for-indicating-ai-written-text

# ChatGPT is still awesome!

nvisia
connect. build. enable.

## Company Policy



Information Technology

# Artificial Intelligence Do’s and Don’ts – Corporate guidance & approval process

**Artificial Intelligence Do’s and Don’ts – Corporate guidance & approval process**

Artificial intelligence (AI) tools are becoming increasingly available. They can be a valuable aid in getting work done, but we don’t know all the unintended consequences yet. And, this reinforces the need to protect our company and customer information.

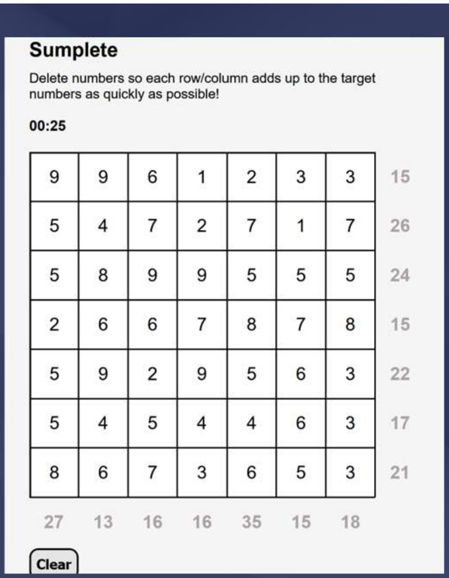
There are important aspects to understand before entering work or personal information into these tools. For example, the terms of use for ChatGPT – a task-specific generative pre-trained tool that can do things like write content based on criteria entered – and many other AI tools do not protect the confidentiality of info entered. Ownership of the content it produces is also unclear. **Entering company information into AI tools could be a risk for the company**.

# ChatGPT: How companies are using it?

- CaseText: GPT-4 trained AI legal assistant
  - Casetext - CoCounsel
- GAI strategies for Platform Engineering & Cloud Engineering
  - ProdConWI 2023 talk by Kyle Anderson, GE Healtcare
- FrontDesk Inc: automate workflow, data entry, wiki bot/slack
  - Frontdesk Inc. | About | Short-Term Stays (stayfrontdesk.com)
- Bend Health: generate chart notes
- AmFam: summarize reports (police, body shop) in claims
- UW Credit Union: boilerplate code, process automation

# How I use ChatGPT?

- Research for this presentation
- Draft generic content
- Code snippets/pseudocode
- MS-Excel formulas, Regex expressions
- IRS tax terms, medical terms, trivia
- My boyfriend uses it for everything
    - Specific lists, statistics, ordering
    - Obscure facts
    - Recipes

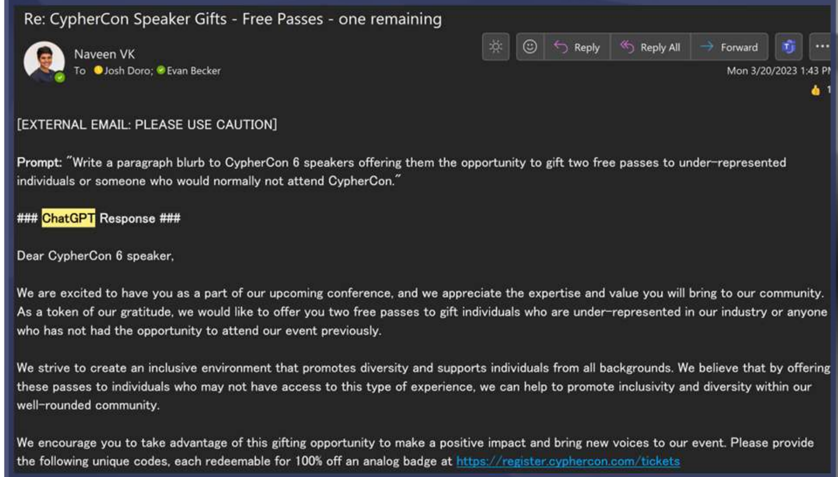


**Sumplete**

Delete numbers so each row/column adds up to the target numbers as quickly as possible!

00:25

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 9 | 9 | 6 | 1 | 2 | 3 | 3 | 15 |
| 5 | 4 | 7 | 2 | 7 | 1 | 7 | 26 |
| 5 | 8 | 9 | 9 | 5 | 5 | 5 | 24 |
| 2 | 6 | 6 | 7 | 8 | 7 | 8 | 15 |
| 5 | 9 | 2 | 9 | 5 | 6 | 3 | 22 |
| 5 | 4 | 5 | 4 | 4 | 6 | 3 | 17 |
| 8 | 6 | 7 | 3 | 6 | 5 | 3 | 21 |
| 27 | 13 | 16 | 16 | 35 | 15 | 18 | |



Re: CypherCon Speaker Gifts - Free Passes - one remaining

Naveen VK

To Josh Doro; Evan Becker

Mon 3/20/2023 1:43 PM

[EXTERNAL EMAIL: PLEASE USE CAUTION]

**Prompt:** "Write a paragraph blurb to CypherCon 6 speakers offering them the opportunity to gift two free passes to under-represented individuals or someone who would normally not attend CypherCon."

**### ChatGPT Response ###**

Dear CypherCon 6 speaker,

We are excited to have you as a part of our upcoming conference, and we appreciate the expertise and value you will bring to our community. As a token of our gratitude, we would like to offer you two free passes to gift individuals who are under-represented in our industry or anyone who has not had the opportunity to attend our event previously.

We strive to create an inclusive environment that promotes diversity and supports individuals from all backgrounds. We believe that by offering these passes to individuals who may not have access to this type of experience, we can help to promote inclusivity and diversity within our well-rounded community.

We encourage you to take advantage of this gifting opportunity to make a positive impact and bring new voices to our event. Please provide the following unique codes, each redeemable for 100% off an analog badge at https://register.cyphercon.com/tickets

# Prompt: Best uses of ChatGPT for s/w devs

- Code assistance and generation
- Debugging support/help
- Learning new tech
- Algorithm and Data Structure explanations
- Code review and refactoring
- API/code documentation
- Prototyping and pseudocode
- Parsing and text processing
- Brainstorming tech solutions
- Writing enhancements
- Natural language interfaces
- Writing automated testing
- Error message interpretation
- Database queries and management
- Project planning
- Feature ideation
- Deployment and DevOps
- Design and architecture ideas
- Interview preparation
- Learning and self-education

Prompt Engineering

# ChatGPT: Tips for better response

- Prompt engineering
  - Be clear and specific with the query
  - Provide context, instructions to help the model understand the query
  - Mention the perspective that is desired
- Iteratively refine or restate context/query ☺
- Correct, if response is incorrect
  - My boyfriend says thank you, please, etc.
- Ask open-ended questions
- Try “temperature”, “max tokens” parameters
- Experiment and learn

# ChatGPT: The Do's ✓

- **Use common sense**
- Follow your company's policy
- Boilerplate/non-proprietary code snippets or pseudocode
- Learning aid for established programming languages, algorithms, tools and frameworks
- Summarizing technical documents or non-proprietary code
- Emails
- Documentation

- Transparency, attribution to content generated by ChatGPT
- Be aware of legal standards
- Get user consent if using GPT or OpenAI APIs in user-facing apps
- Be aware of copyright, trademark, Intellectual Property rights
- Be aware of ethical guidelines
- **Verify the information provided by ChatGPT**

# ChatGPT: The Don'ts

- **Don't share anything you want to keep private**
- No sensitive data, PII, PHI
- No proprietary information
- No trade secrets
- No private financial data
- No credentials/secrets
- Do not use ChatGPT as a trusted source

- No training the model with incorrect/false data
- No spamming the model
- Other
  - Not for financial, investment, medical or legal advice
  - Not for mental health support or therapy
  - No hateful, abusive, offensive, violent, or harmful requests
  - No inappropriate, explicit, or adult content

# Key take-aways

- ChatGPT is just another tool.  Use it.
  - Prompt engineering, practice makes perfect
- If you want to keep something private/proprietary, don't put it on ChatGPT
- Use ChatGPT as a starting point (like Wikipedia)
  - Learning
  - Information
- **Verify! Verify! Verify!**

Making a thousand decisions, even the wisest make mistakes.
~ Old Chinese Proverb

nvisia
connect. build. enable.

**Naveen VK**
**Technical Director**
**naveen@nvisia.com**

# Thank you! Questions?

Naveen VK
naveen@nvisia.com
naveenvkm@gmail.com

in Naveen VK
navnoon
f Naveen VK