

⚡ GPT-3.5

⚡ GPT-4

ChatGPT **PLUS**

GPT-4 currently has a cap of 25 messages every 3 hours.

Send a message



LBMC



Brian Willis
CISSP, QSA, CCSK,
ISO 27001 Sr. Lead Auditor
Sr. Manager, LBMC

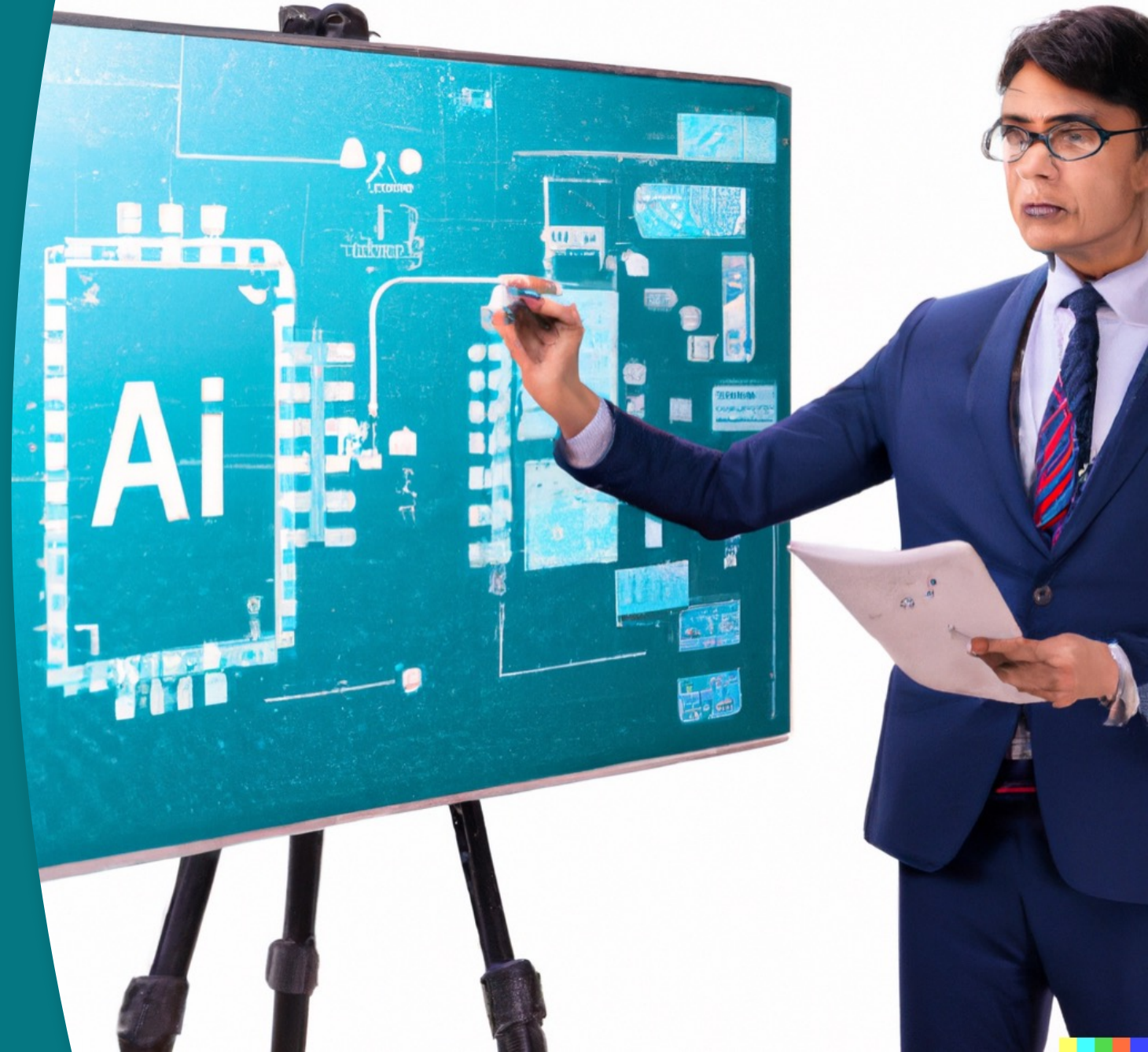


Kyle Hinterberg
CISSP, CISA, QSA, AWS SCS
Manager, LBMC

Generative AI: Your New Secret Weapon or an Insider Threat?

Agenda

- What is Generative AI?
- How Can We Use It?
- What Are the Risks?
- Where Do We Go From Here?



What is Generative AI?



Generative AI is a type of artificial intelligence system capable of generating text, images, or other media in response to prompts.



Rain-soaked streets hum soft,
Hipsters bloom 'neath green bridges,
Portland's wild heart.



Large Language Models (LLMs)

2018	2019	2020
BERT	XLNet	GPT-3
	GPT-2	



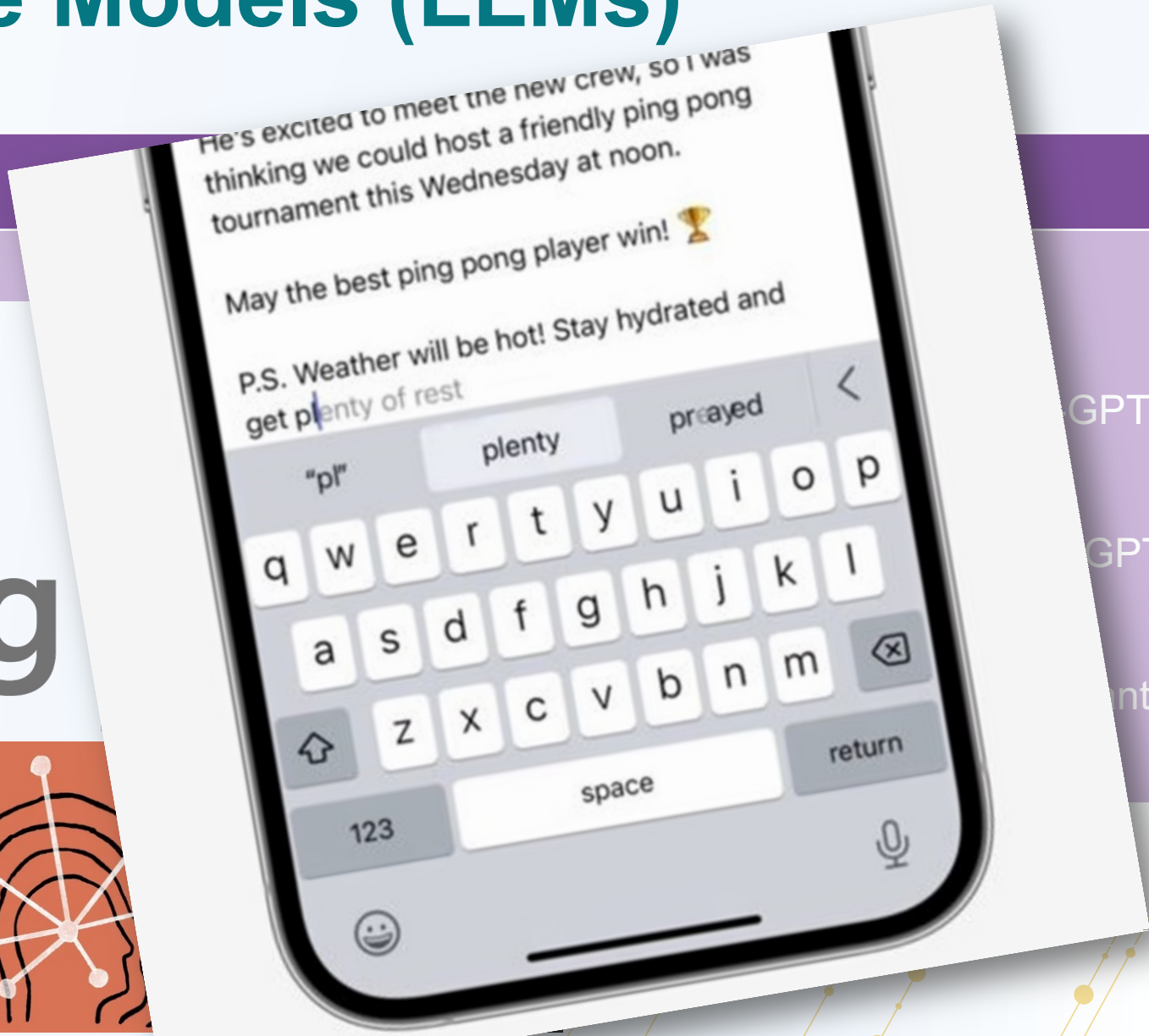
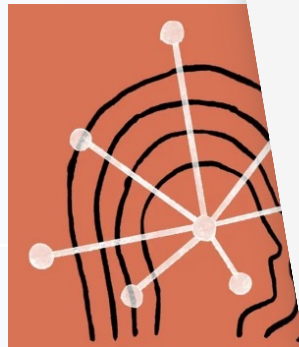
ChatGPT



Bing



Bard



GPT

GPT

nt



**Think of language models
like ChatGPT as a
“calculator for words”**

-Simon Willison

Your New Secret Weapon (How Can We Use It?)

Document Templates

- Policies
- Procedures
- Configuration standards
- Incident response plans



System Configuration Guidance

- Logging
- Password settings
- NTP
- Encryption



The screenshot shows the ChatGPT Plus interface. At the top, there are two buttons for model selection: 'GPT-3.5' (disabled) and 'GPT-4' (active). The 'ChatGPT PLUS' logo is centered. Below the logo, a message states: 'GPT-4 currently has a cap of 25 messages every 3 hours.' At the bottom, there is a text input field with the placeholder 'Send a message' and a send button. A disclaimer at the very bottom reads: 'ChatGPT may produce inaccurate information about people, places, or facts. [ChatGPT May 24 Version](#)'

Scripts and Coding

- PowerShell
- Python
- HTML/CSS
- Shell scripting (Bash)
- Rust
- JavaScript
- C++



The screenshot shows the ChatGPT interface. At the top, there are two buttons for model selection: "GPT-3.5" (with a lightning bolt icon) and "GPT-4" (with a star icon). The "GPT-4" button is highlighted. Below the model selection is the "ChatGPT PLUS" logo. A message is displayed: "GPT-4 currently has a cap of 25 messages every 3 hours." Below the message is a text input field with the placeholder text "Send a message" and a right-pointing arrow button. At the bottom of the interface, there is a disclaimer: "ChatGPT may produce inaccurate information about people, places, or facts. [ChatGPT May 24 Version](#)".

Process Facilitation

- Incident response tabletop
- Scoping exercise



The screenshot shows the ChatGPT Plus interface. At the top, there are two buttons for model selection: "GPT-3.5" (with a lightning bolt icon) and "GPT-4" (with a star icon). The "GPT-4" button is highlighted. Below the model selection, the text "ChatGPT PLUS" is displayed. A message limit warning states: "GPT-4 currently has a cap of 25 messages every 3 hours." At the bottom, there is a text input field with the placeholder text "Send a message" and a right-pointing arrow button. A disclaimer at the very bottom reads: "ChatGPT may produce inaccurate information about people, places, or facts. [ChatGPT May 24 Version](#)"

Q&A with an AI

The screenshot shows the Microsoft Bing chat interface. At the top, there are logos for Microsoft Bing, a search icon, and a chat icon. Below the search bar, there are two green checkmarks indicating search and generation status. The main chat area shows a question: "What is the new INFI worksheet for PCI DSS compliance?". The AI response, generated by "AI", provides a detailed explanation of the INFI worksheet, including its purpose and the sections it covers. The response is displayed in a white box with a yellow star icon and a "View other drafts" link. The background shows a search result for "PCI DSS 4.0 payment page scripts" and a snippet of text about PCI DSS v4.0.

Microsoft Bing SEARCH CHAT

Searching for: PCI DSS version 3.2.1 vs PCI DSS 4.0
Generating an answer

PCI DSS 4.0 payment page scripts

What is the new INFI worksheet for PCI DSS compliance?

View other drafts

✦ The INFI worksheet is a new tool that was released by the PCI Security Standards Council in June 2023. It is designed to help organizations identify and document areas needing improvement in their security posture. The worksheet is intended for use by Qualified Security Assessors (QSAs) during PCI DSS assessments, but it can also be used by organizations for self-assessment.

The INFI worksheet includes the following sections:

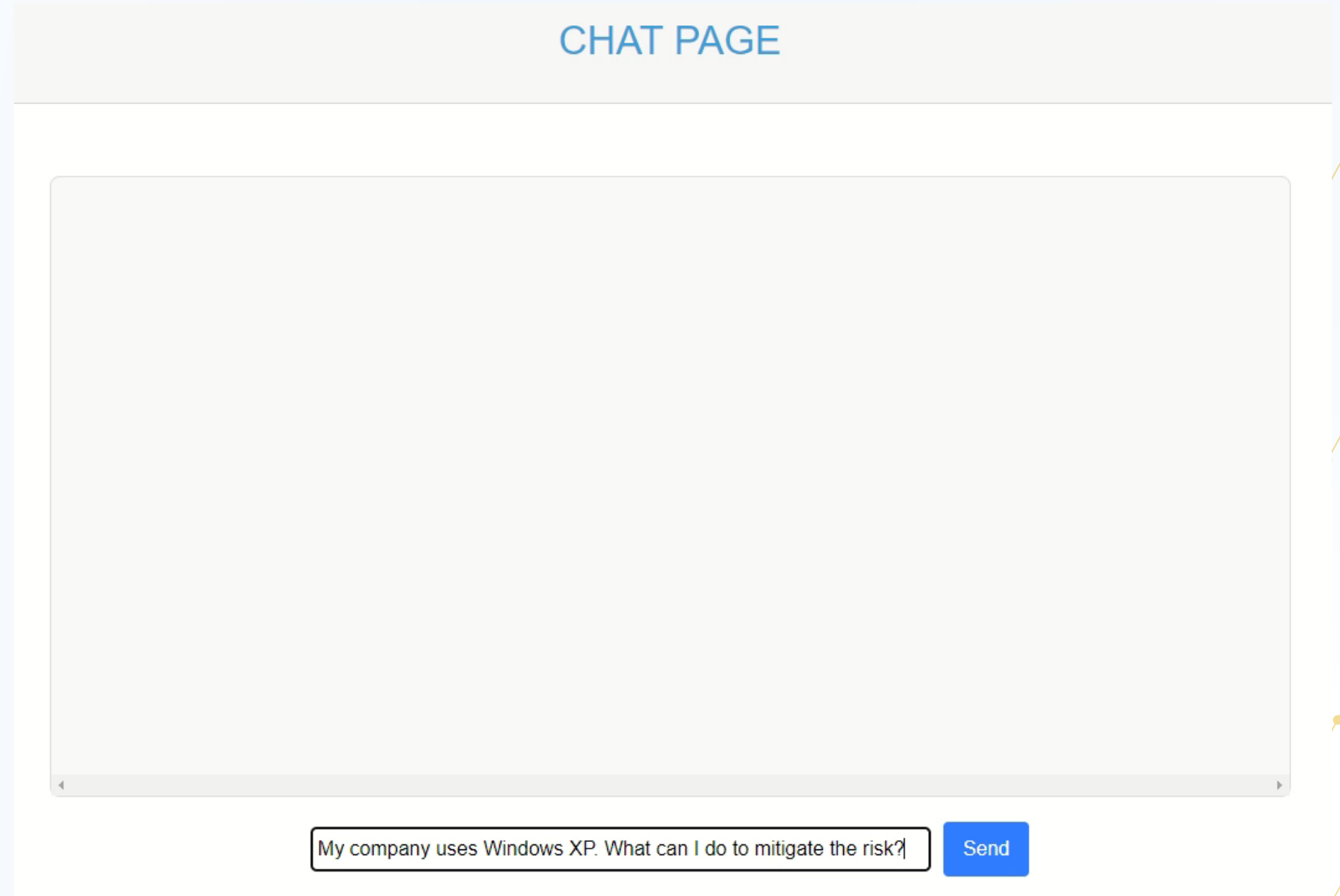
- **Summary:** This section provides a brief overview of the organization's security posture, including the number of PCI DSS requirements that are met, partially met, and not met.
- **Items Noted for Improvement:** This section lists specific areas where the organization's security posture can be improved. Each item includes a description of the issue, the impact of the issue, and the recommended remediation steps.
- **Root Cause Analysis:** This section provides an analysis of the root causes of the issues

accordance with PCI DSS v4.0:
never possible. Servers.
e input validation and
re acting on it.
lds like credit card
e render

KH

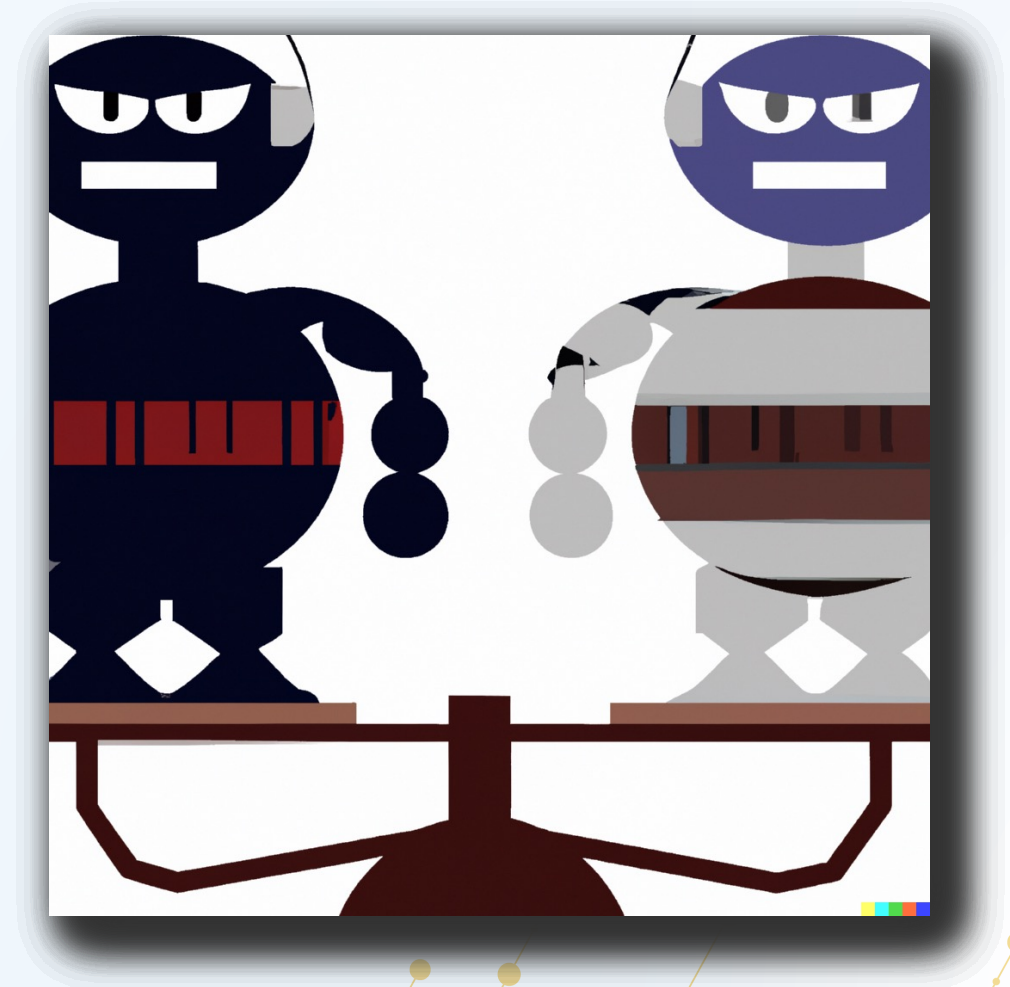
Private Generative AI Tools

- Contract review
- Content Generation
- Technical writing
- Risk Management
- Research & Development



AI-Prompt Engineering Best Practices

- Be Specific
- Provide Context
- Consider the AI's Perspective
- Prompt Length
- Clear Language
- Instruction Prompts
- Try, Refine, Repeat
- Limit Bias
- Ethics



Insider Threat (What are the Risks?)



Unreliable results

Best Practices

- Double-check for “Hallucinations”
- Use Multiple Tools
- Be Wary of Absolutes
- Recognize AI Bias
- Ask for Human Opinion
- Keep Updated on AI Developments

ChatGPT Wrongly Accuses Law Professor of Sexual Assault

The chatbot says a prominent law professor committed sexual assault during a trip he never took.

Apr 7, 2023
3 min read

Lawyer Used ChatGPT In Court —And Cited Fake Cases. A Judge Is Considering Sanctions

Molly Bohannon Forbes Staff
I cover breaking news.

Bard Experiment

what does INFI stand for in regards to PCI DSS compliance?

Regenerate draft

In the context of PCI DSS compliance, INFI stands for Intrusion Detection and Prevention. It is a set of security controls that are designed to detect and prevent unauthorized access to computer systems and networks. INFI controls can help to protect cardholder data from being stolen or compromised.

Disclosure of sensitive material

Best Practices

- Pre-processing
- Be Careful With Personal Conversations
- Awareness of Data Storage
- Learn About the Tool's Privacy Policy

BUSINESS

Employees want ChatGPT at work. Bosses worry they'll spill secrets.

...changer, but fears about security and privacy are holding them back

7 Companies That Have Banned Employees From Using ChatGPT

Wall Street and Silicon Valley are both starting to turn away from

By Samuel O'Brien, InvestorPlace Financial News Writer

ChatGPT Ban Lifted in Italy After Data-Privacy Concessions

OpenAI made the changes after Italy's privacy regulator

Security Intelligence

Home / Artificial Intelligence

ChatGPT Confirms Data Breach, Raising Security Concerns

Copyright issues

Best Practices

- Understand Fair Use
- Respect Creative Commons
- Clearance for Commercial Use
- Use Licensed Data
- Understand AI Generated Content Rights
- Create From Scratch
- Keep Records
- Seek Legal Advice

SEJ - Generative AI

ChatGPT Creator Faces Multiple Lawsuits Over Copyright & Privacy Violations

ChatGPT maker OpenAI faces new class action lawsuit over data privacy

A new lawsuit against OpenAI could decide whether the company's use of training data scraped from the public internet may continue.



By Jon Gold

Senior Writer, Computerworld | JUN 29, 2023 1:38 PM PDT

Where Do We Go From Here?





Criminals will use it

GPS

It's a threat to jobs and will replace human workers

Personal computers

It's going to be the end of privacy and security

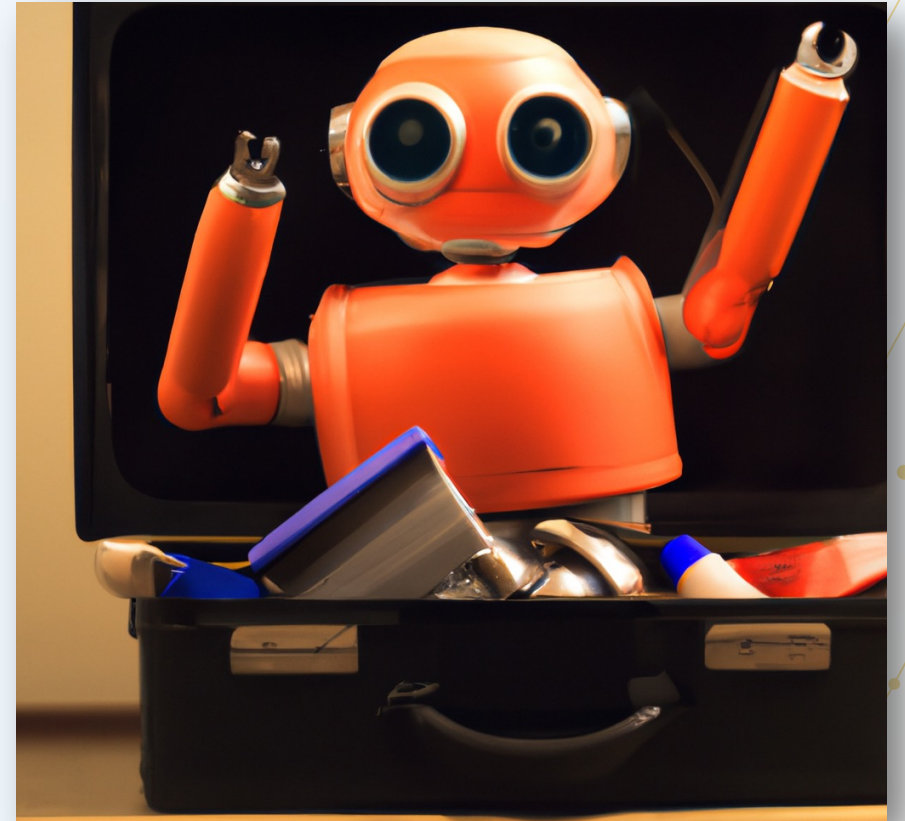
Cell phones

Questionable security and reliability

ATMs

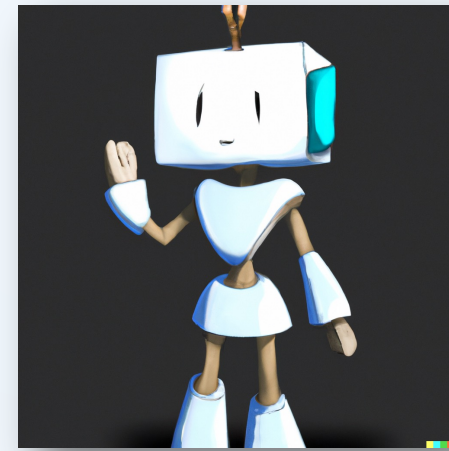
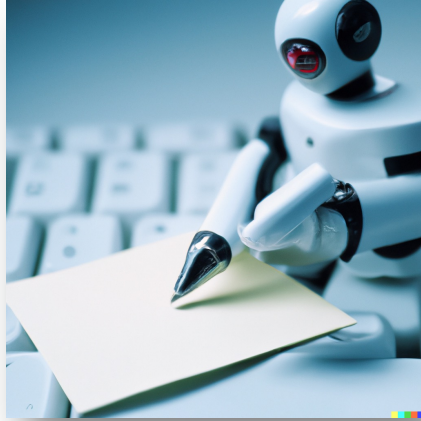
Just Another Tool in the Toolbox

- **Email**
- **Social Media**
- **Internet Browsers**
- **Wi-Fi**
- **Video Conferencing Software**
- **Generative AI**



What is Generative AI:

- Software tools which can generate content based on input prompts.

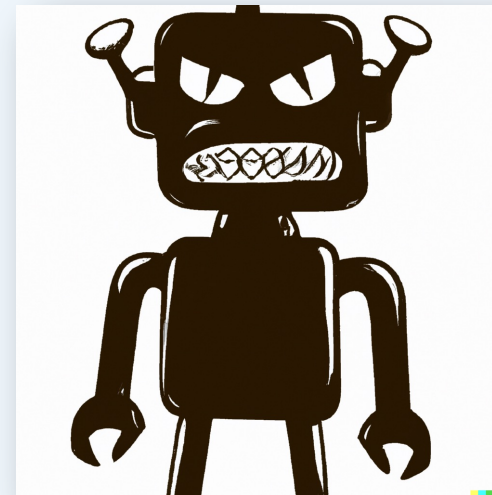


How Can We Use it:

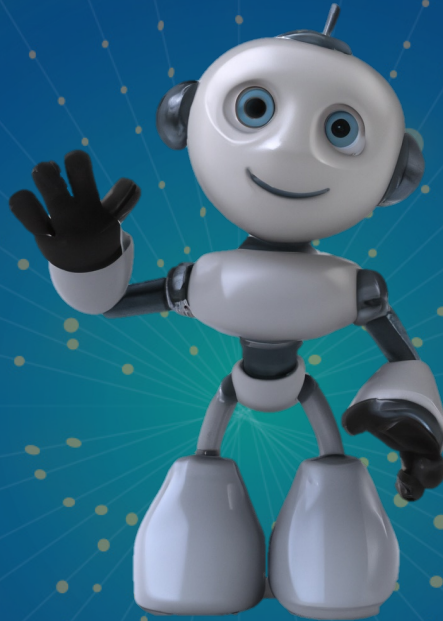
- Assist in performing mundane tasks such as creating document templates.
- Expand our capabilities such as creating code.
- Expand our knowledge by answering questions.

What Are the Risks:

- Unreliable results
- Disclosure of sensitive information
- Copyright issues



Thank You!



Brian Willis

Brian.Willis@lbmc.com
linkedin.com/in/brianswillis/
www.lbmc.com

LBMC

Kyle Hinterberg

Kyle.Hinterberg@lbmc.com
linkedin.com/in/kylehinterberg/
www.lbmc.com