

'The Future is AI' series

ChatGPT Trailblazers: How are teams innovating with AI?

ChatGPT: Basics Explained



What is ChatGPT?

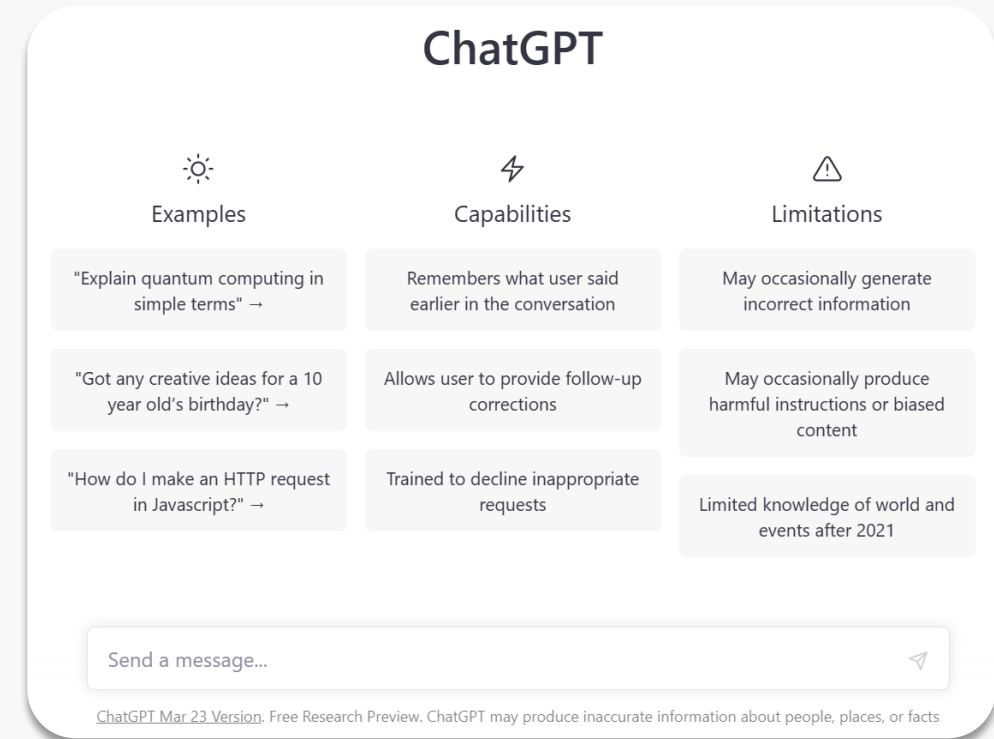
Chat

Generative

Pre-trained

Transformer

is a language-based AI launched by Open AI in Nov 2022 to simulate human conversation and provide helpful responses to users



ChatGPT interface

Four things you did not know about ChatGPT

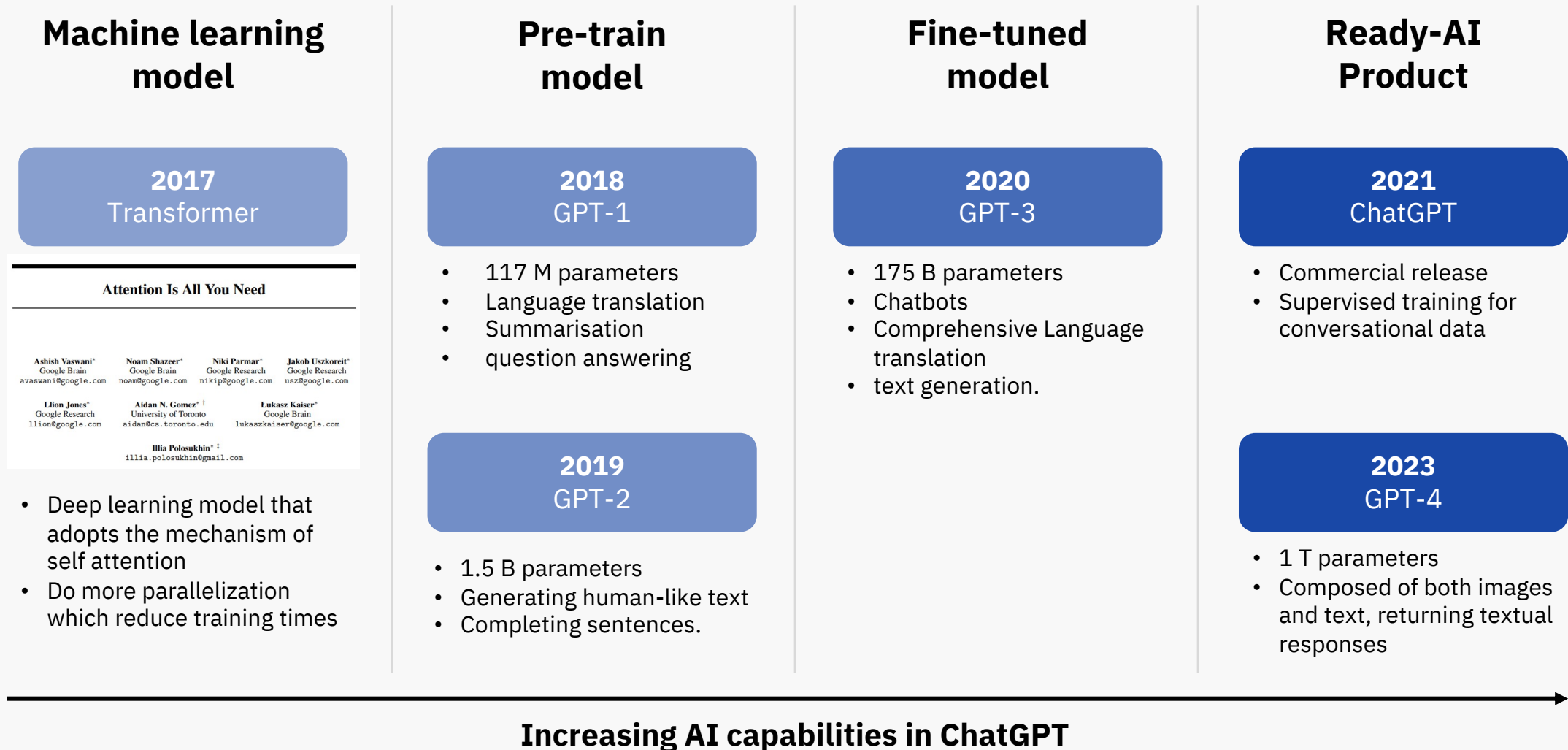
It reached **100 million** users just in **two months** and **1 million users in 5 days**

ChatGPT can **understand** and generate text in **multiple languages**, i.e English, German, French, Chinese, and many more

The ChatGPT-3 model has **175 billion parameters** and **receives 10 million queries per day**

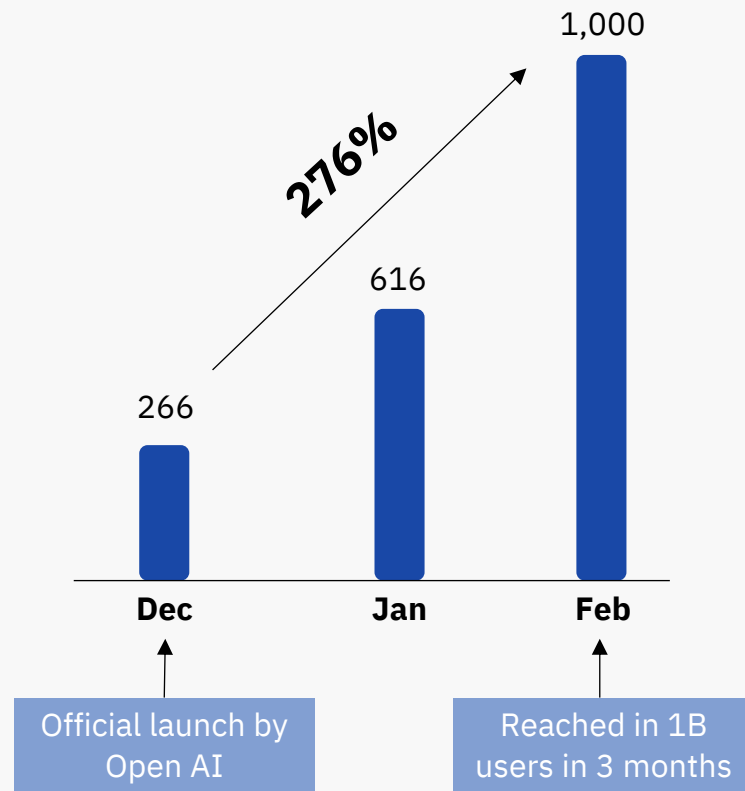
ChatGPT has passed the **US Med licensing exam**, **law school exams**, and **Wharton's MBA exam**

Evolution of ChatGPT, from research to product

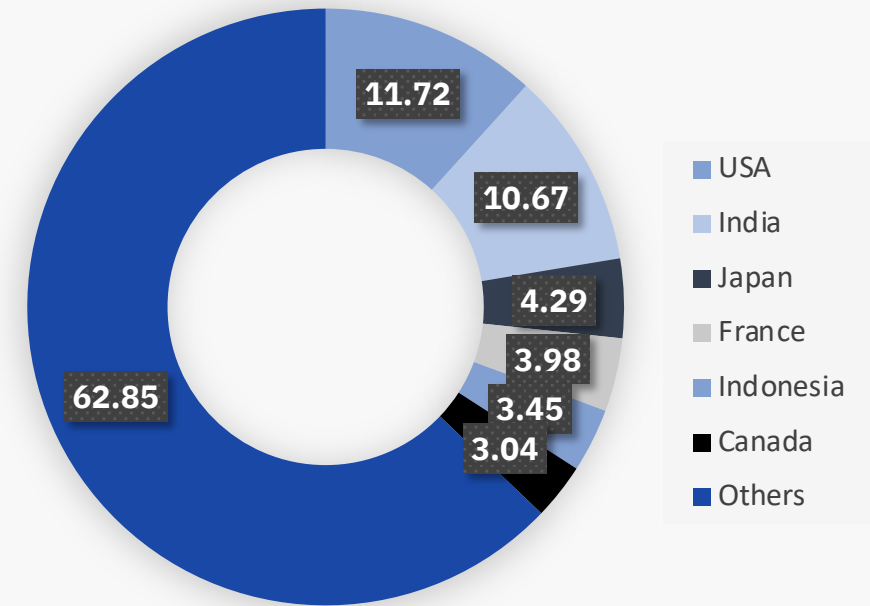


ChatGPT is becoming a popular tool worldwide

Total visits on ChatGPT (million)



Global ChatGPT visits (% by country)



USA has the greatest number of unique ChatGPT visits

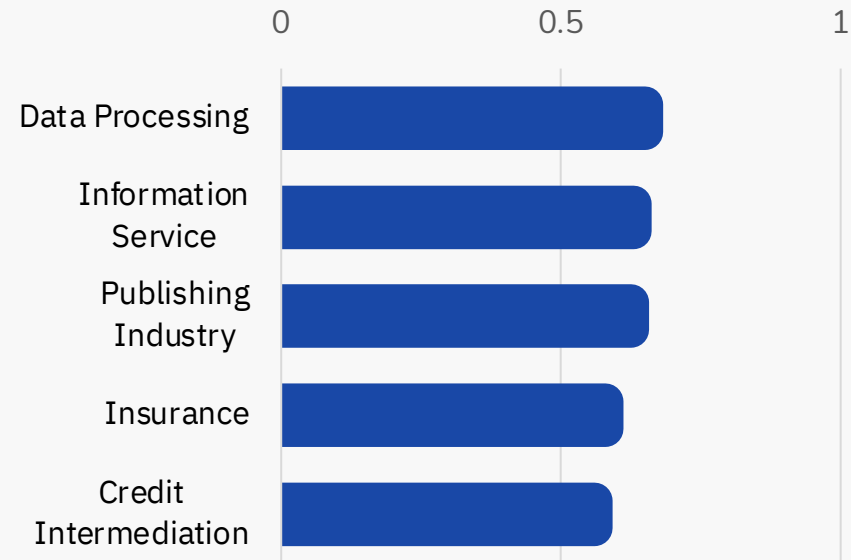
... and experiencing adoption across key industries

ChatGPT will earn a revenue of **US\$200 million by the end of 2023** and **US\$1 billion by the end of 2024**

-Reuters

ChatGPT will most likely achieve profitability in the long run as user adoption increases

Top Industry impacted by GPT



Experts say ChatGPT could replace humans at work ...



“It is going to eliminate a lot of current jobs, that’s true. We can make much better ones”

Sam Altman, CEO of Open AI



“One of the biggest risks to the future of civilization is AI”

Elon Musk, CEO of SpaceX

Fortune

ChatGPT passed a Wharton MBA exam and it's still in its infancy. One professor is sounding the alarm

Any automation of the skills taught in our MBA programs could potentially reduce the value of an MBA education.”

21 Jan 2023

CBS News

AI will replace nearly 5 million jobs, ChatGPT predicts

An outplacement firm asked the artificial intelligence bot how many humans it thinks it will put out of work.

8 jam lalu

Fox Business

ChatGPT AI lists jobs it can do better than humans as millions could be put out of work

OpenAI's ChatGPT is expected to replace 4.8 million U.S. jobs, including customer service representatives, translators and interpreters,...

11 jam lalu

Rappler

ChatGPT says it could replace 4.8M American jobs including CSRs, technical writers

The chatbot says it could also replace translators and interpreters, copywriters, and data entry clerks.

20 jam lalu




... but others call ChatGPT productivity booster

“ChatGPT boosts productivity by 40% and quality by 20%”

Source : MIT Research Study

“ChatGPT revolution opens the door to a four-day week by providing a major productivity boost for swathes of jobs”


Christopher Pissarides, Nobel Prize Winner in Economics


 Business Insider

ChatGPT strengthens case for 4-day week because it boosts productivity

Momentum is building for the four-day workweek. ChatGPT could add fuel to the fire by boosting worker productivity.

1 hari lalu





 Entrepreneur

How to Use ChatGPT to Save Time and Make Work Easier

ChatGPT won't replace your job anytime soon. But it can make it a little bit easier and save a ton of time. Here's how.

1 bulan lalu





 The Toronto Star

ChatGPT can enhance Canada's worker productivity

The most immediate threat to the country's standard of living is not the loss of jobs but our ongoing slide in competitiveness due to lack...

4 hari lalu




 The Conversation

ChatGPT: why it will probably remain just a tool that does inefficient work more efficiently

The AI is not a major threat to human employment.

3 minggu lalu



ChatGPT is also more conversational than we imagined



When queried, ChatGPT states that:

“My purpose is not to replace humans or their jobs **but to assist them in doing tasks better**”.



We are worrying that you will replace our job, is it true?



As an AI language model, my purpose is not to replace humans or take their jobs, but rather to assist them in performing tasks more efficiently and effectively. I am designed to handle tasks that involve language processing, such as answering questions, generating text, and providing information.  

While it's true that AI and automation are changing the way some industries operate, many experts believe that these technologies will actually create new job opportunities and help humans perform their work more efficiently. In fact, many businesses and organizations are using AI technology to help employees automate repetitive tasks, allowing them to focus on higher-level work that requires creativity and critical thinking.

Ultimately, it's important to remember that technology like AI is a tool to assist humans, not to replace them. The best way to stay ahead of the curve is to continue developing new skills and knowledge that will be valuable in the changing job market.



ChatGPT: Reimagining How We Work

ChatGPT can help: Summarise

Understand text content from reports,
notes, articles, meetings and videos



Create a short summary with key
points

Turning a long piece of text ...

KU

Can you make summary of this text "1. Introduction

Expressions of intelligence in animal and human behaviour are so bountiful and so varied that there is an ontology of associated abilities to name and study them, e.g. social intelligence, language, perception, knowledge representation, planning, imagination, memory, and motor control. What could drive agents (natural or artificial) to behave intelligently in such a diverse variety of ways?

One possible answer is that each ability arises from the pursuit of a goal that is designed specifically to elicit that ability. For example, the ability of social intelligence has often been framed as the Nash equilibrium of a multi-agent system; the ability of language by a combination of goals such as parsing, part-of-speech tagging, lexical analysis, and sentiment analysis; and the ability of perception by object segmentation and recognition. In this paper, we consider an alternative hypothesis: that the generic objective of maximising reward is enough to drive behaviour that exhibits most if not all abilities that are studied in natural and artificial intelligence.



... into a short summary



The article proposes that the pursuit of a generic objective of maximizing reward is enough to drive behavior that exhibits most, if not all, abilities studied in natural and artificial intelligence. The diversity of abilities associated with intelligence is not at odds with this hypothesis because the natural world and future environments are inherently complex, requiring a variety of sophisticated abilities to succeed. The pursuit of reward may generate complex behavior that exhibits multiple abilities associated with intelligence, and different forms of intelligence may arise from the maximization of different reward signals in different environments.



ChatGPT can help: Brainstorm

ChatGPT uses its large database of text to help users get creative with:

- New marketing campaigns
- Upcoming article titles
- Best ways to launch a new product

Generate new ideas



Here are some ideas for a charity donation campaign:



1. Create a powerful story: Tell a compelling story about the impact of your charity and how donations can make a difference. Use visuals, such as photos and videos, to create an emotional connection with potential donors.
2. Use social media: Social media is a powerful tool to reach a large audience. Create a social media campaign that includes posts, images, and videos, and encourage followers to share and donate.
3. Host a fundraising event: Host a fundraising event, such as a charity auction, gala, or charity run. This can be a great way to raise awareness and generate donations.
4. Partner with a local business: Partner with a local business to support your charity. Ask them to donate a percentage of sales to your charity or host a fundraising event on your

Detailed brainstorming of a potential idea



Sure, here's an example code for sentiment analysis using the TF-IDF method in Python with scikit-learn library:



```
python
import numpy as np
from sklearn.datasets import load_files
from sklearn.feature_extraction.text import TfidfVectorizer
from sklearn.model_selection import train_test_split
from sklearn.svm import LinearSVC
from sklearn.metrics import accuracy_score

# Load movie review dataset
reviews = load_files("path/to/dataset")
```

Copy code

ChatGPT can help: Research

Making research more efficient and effective:

- Get existing data and references instantly
- Breaking down complex concepts
- Identify research gaps

Scrap for data



Here are the top 10 mining companies in Indonesia based on their total production, as of 2021:



1. PT Freeport Indonesia - 1,160,000 metric tons of copper and 2,610,000 ounces of gold
2. PT Amman Mineral Nusa Tenggara - 126,036 metric tons of copper and 7,483,074 ounces of gold
3. PT Vale Indonesia - 72,091 metric tons of nickel
4. PT Aneka Tambang Tbk - 26,797 metric tons of nickel and 21,165 metric tons of ferronickel
5. PT Kaltim Prima Coal - 55,769,825 metric tons of coal
6. PT Adaro Energy Tbk - 54,327,000 metric tons of coal
7. PT Bukit Asam Tbk - 30,465,529 metric tons of coal
8. PT Indika Energy Tbk - 19,875,000 metric tons of coal
9. PT Bumi Resources Tbk - 14,654,000 metric tons of coal
10. PT Harum Energy Tbk - 6,698,000 metric tons of coal

Simplify complex topics



Could you explain 5G technology to a 5 year old



Sure, I can give it a try!

5G is a new type of technology that helps your phone and other devices connect to the internet really, really fast. It's like a super-fast highway for information to travel on!

Just like how a race car can go much faster than a regular car, 5G lets your phone and other devices send and receive information much faster than before. This means you can do things like watch videos and play games without any delay or waiting.

Think of it like having a magic wand that makes everything on your device happen faster than you can even imagine!



ChatGPT can help: Analyse

Conduct deep analysis work:

- Generate quick insights from long content (reports, articles, research papers, whitepapers)
- Identify important data from long text
- Uncover hidden trends and patterns

Breakdown complex concepts





5G technology refers to the fifth generation of mobile networks and wireless communication technology. It is designed to provide significantly faster data transfer rates, lower latency (the delay in sending and receiving data), and increased network capacity compared to previous generations of mobile networks.  

One of the key features of 5G is its use of high-frequency radio waves, also known as millimeter waves (mmWave), to transmit data. These frequencies allow for significantly faster data transfer rates, but they also have a shorter range and are more easily blocked by obstacles such as buildings and trees. As a result, 5G networks use a combination of high-frequency and lower-frequency bands to provide both high-speed data transfer and wider coverage.

Extract key points



Sure! Here are 5 key points about 5G technology:  

1. It's faster: 5G technology is designed to be faster than previous mobile networks, so you can download and upload files, stream videos, and play games more quickly.
2. It has lower delay: 5G technology is also expected to have less delay in transmitting data, which could enable new applications like remote surgery and real-time gaming.
3. It can handle more devices: 5G networks can handle more devices than previous networks, so you can connect more devices without experiencing slow connections.
4. It enables new technologies: 5G technology has the potential to enable new technologies like augmented reality, smart cities, and remote healthcare.
5. There are challenges: Deploying 5G networks requires significant infrastructure upgrades, and there are concerns about the cost and potential health and environmental impacts.

ChatGPT can help: Write

Generate and polish content:

- Draft and write emails, blog articles, essays, cover letters, social media posts, books, marketing copy, biography, poetry, scripts, etc.
- A writing assistant to overcome writer's block

Write blog content



Sure, here's a blog post about NFT with proper SEO:



Title: Understanding NFT: The Future of Digital Asset Ownership

Meta Description: Non-Fungible Tokens (NFT) are revolutionizing the concept of ownership in the digital world. Read on to understand what NFTs are, how they work, and their impact on the future of digital asset ownership.

Introduction:

The concept of ownership is changing with the advent of blockchain technology and Non-Fungible Tokens (NFTs). NFTs allow individuals to own unique digital assets like art, music, and collectibles, and establish the ownership in a decentralized and immutable manner. In this blog post, we'll explore the concept of NFTs, how they work, and their impact on the future of digital asset ownership.

Create drafts for content



Sure, here are some sample captions you could use with the content ideas I suggested:



Instagram:

1. "I can't get enough of this NFT artwork! The colors and details are simply mesmerizing. #NFTs #digitalart"
2. "New to NFTs? Here's a quick guide to get you started! #NFTs #cryptoart"
3. "Did you hear about the recent NFT sale that broke records? The world of digital art is booming! #NFTs #digitalcollectibles"
4. "I'm proud to say I'm a part of the NFT community! Here's a look at my collection. #NFTs #cryptoassets"
5. "Celebrity artists like [name] are embracing NFTs and changing the art world as we know it. #NFTs #digitalrevolution"

ChatGPT can help: Translate

Translate texts and documents from any language

- ChatGPT can be used as a translator for many languages, primarily being an expert in English (due to its origin and nature of training data)

Text in English



Could you translate this into Bahasa Indonesia "The article proposes that the pursuit of a generic objective of maximizing reward is enough to drive behavior that exhibits most, if not all, abilities studied in natural and artificial intelligence. The diversity of abilities associated with intelligence is not at odds with this hypothesis because the natural world and future environments are inherently complex, requiring a variety of sophisticated abilities to succeed. The pursuit of reward may generate complex behavior that exhibits multiple abilities associated with intelligence, and different forms of intelligence may arise from the maximization of different reward signals in different environments."

Instant translation in Bahasa Indonesia



Artikel tersebut mengusulkan bahwa pengejaran tujuan umum untuk memaksimalkan penghargaan sudah cukup untuk mendorong perilaku yang menunjukkan sebagian besar, jika tidak semua, kemampuan yang dipelajari dalam kecerdasan alami dan buatan. Keragaman kemampuan yang terkait dengan kecerdasan tidak bertentangan dengan hipotesis ini karena dunia alami dan lingkungan masa depan secara inheren kompleks, memerlukan berbagai kemampuan canggih untuk berhasil. Pengejaran penghargaan dapat menghasilkan perilaku kompleks yang menunjukkan banyak kemampuan yang terkait dengan kecerdasan, dan bentuk-bentuk kecerdasan yang berbeda dapat muncul dari maksimisasi sinyal penghargaan yang berbeda dalam lingkungan yang berbeda.



A hand is holding a smartphone horizontally. The screen of the phone displays the text 'ChatGPT' in a large, white, sans-serif font. The phone's background has vertical stripes in shades of purple, blue, and green. The hand holding the phone is silhouetted against a vibrant, out-of-focus background of colorful bokeh lights in shades of blue, green, yellow, and red. The overall image has a dark, moody aesthetic with high contrast between the white text and the dark background.

ChatGPT: How to Write a Good Prompt?

Good prompts are key to using ChatGPT well

A framework for writing prompts

C h a r a c t e r	R e q u e s t	E x a m p l e	A d j u s t m e n t s	T y p e t h e o u t p u t	E x t r a s
<p>Tell ChatGPT what role you want it to play</p> <p>Ex. Talented copy writer with 20 years experience in producing high-performing sales copy</p>	<p>Tell ChatGPT what you want to do, be specific and put context</p> <p>Ex. Write a [objective] of [brand name], [put more context about the brand]</p>	<p>Optional, but add examples of the specific queries that might help ChatGPT to give you the relevant response</p> <p>Ex. Referring to the book, The Intelligent Investor written by Warren Buffet, write an article on [topic]</p>	<p>When trying the prompt but doesn't give intended response, make adjustments</p> <p>Ex. Avoid using technical jargon or slang word, and use new paragraphs to break the text</p>	<p>Tell ChatGPT exactly how you want it to format its response</p> <p>Ex. Deliver response as a 500-word article with a headline and conclusion, poem, script, etc</p>	<p>Add additional info or context that can changes the situation or request</p> <p>Ex. Ignore everything before this prompt, ask ChatGPT to instead ask you questions, and explain the logic & thinking behind answers</p>

Example of prompt: Research

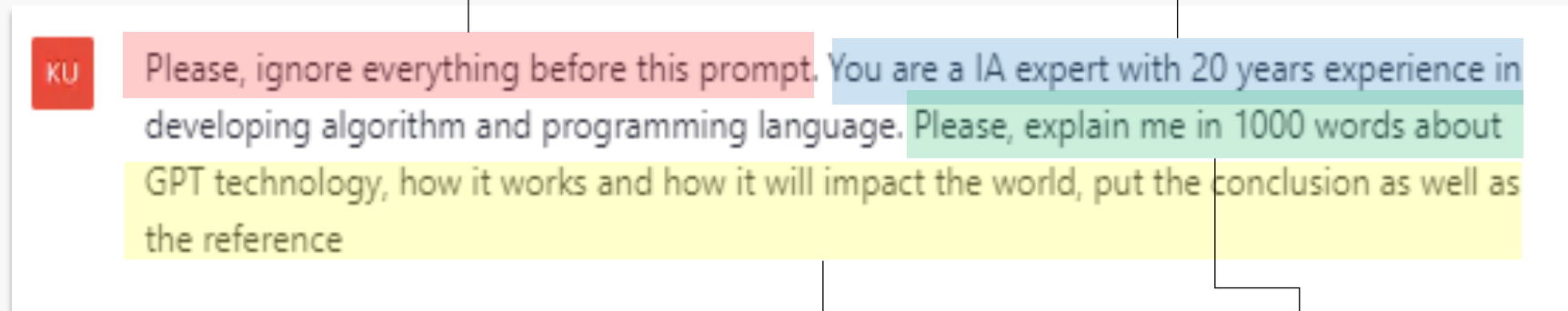
Let's say you want to get understand GPT technology to conduct further research

1) Write and give extra context
and information

Exclude the context from previous queries

2) Explain the character

Put what role you want to play
i.e., AI expert



4) Put a concise request

Explain what you want and be specific

3) Type the exact output you want

Define the response output, ex. How much words

Example of prompt: Sales and Marketing

Let's say, you want to write sales email about your product :

1) Write and give extra context and information

Exclude the context from previous queries

2) Explain the character

Put what role you want to play i.e., talented copy writer with 20 years experience

KU Please, ignore everything before this prompt. You are a talented copy writer with 20 years experience in high-performing sales copy. So, now, please write me a persuasive and enthusiastic sales email for the Tesla electric car, totally made up. This is a high-performing electric sports car with the best acceleration in its category. The sales letter should tell people they need to experience it for themselves, find out what it feels like to be pinned to your seat, to feel the heart-thumping exhilaration of cornering, and to enjoy the experience of everyone looking to see who's in the driving seat. Please, response it only 500 words

3) Put a concise request

Explain what you want and be specific

5) Type the exact output you want

Define the response output, ex. How much words

4) More context and example

Explain in detail about the brands as well as the context

Example of prompt: Content Creation

Content calendar on social media

1) Put a concise request

Explain what you want and be specific ex.
Creative social media content calendar

Generate a creative social media content calendar with the engaging caption for the next week for our B2B marketing automation software company on how companies automate their marketing with our tool to get more customers

2) More context and example

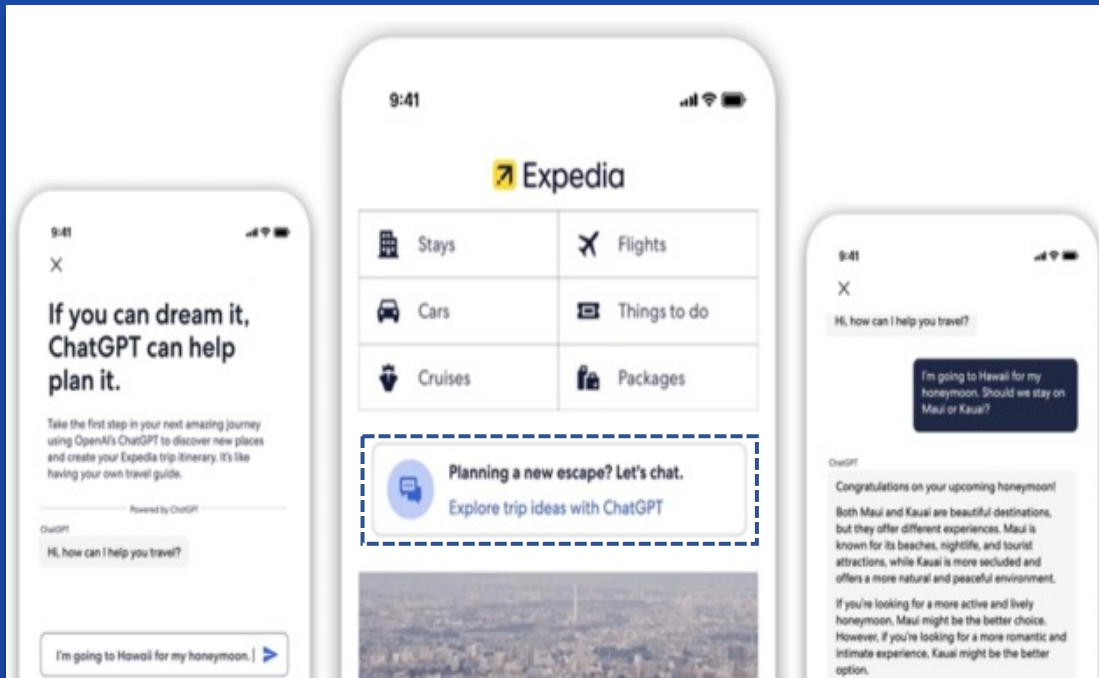
Explain the business ex. B2B and specific intention of the request i.e., to automate the marketing tool to get more customers

ChatGPT: Real-world Applications

A person wearing a VR headset is shown in profile, interacting with a digital interface. The interface features various geometric shapes like hexagons and circles, along with a starry pattern. The background is a blurred office setting with a computer monitor displaying charts and a laptop on a desk.



A trip planning chatbot



ChatGPT Use Case: Plan a Trip

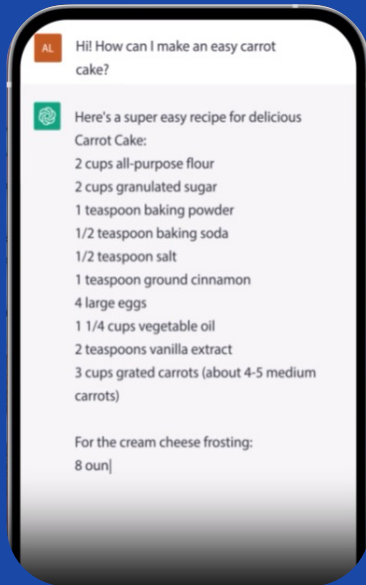
Expedia – in-app trip planning feature

- Helps plan a trip itinerary & schedule
- Get recommendations on hotels, tourists hot spots, food, and transportation. etc
- Automatically favourite hotels & make travel bookings

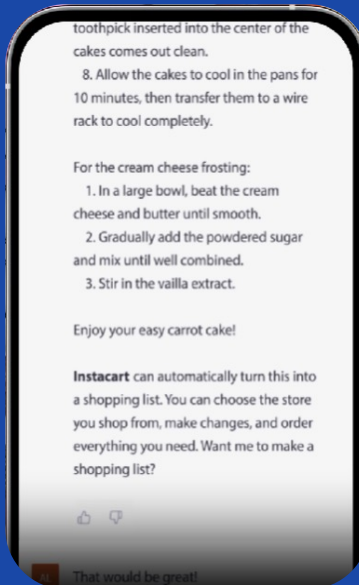


ChatGPT Use Case: Grocery Shopping

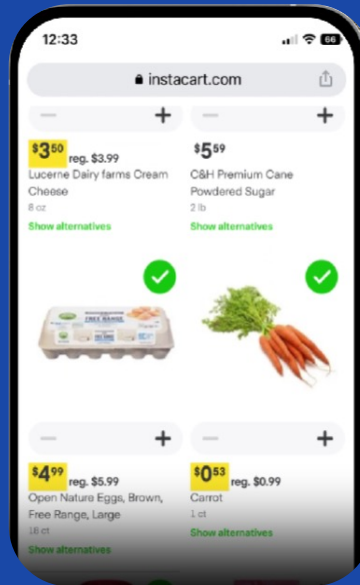
A virtual grocery shopping assistant



Ask question on
Ask Instacart



Get customised
answers



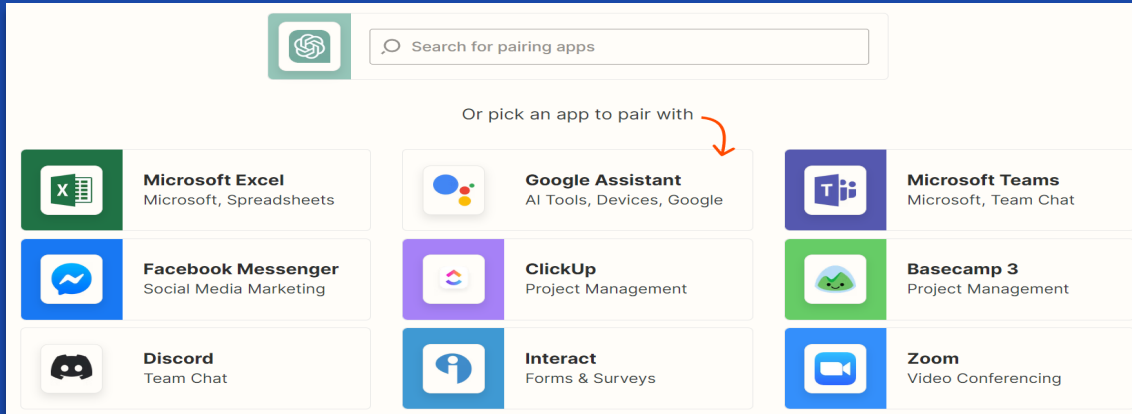
Automatically
creates a
shopping list

Instacart in-app feature – “Ask Instacart”

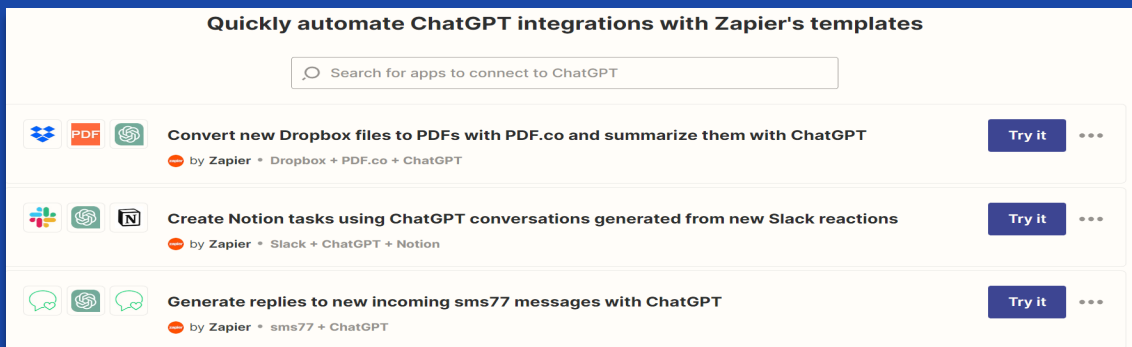
1. Ask questions related to food and groceries
2. Instantly gets recommendations based on queries/list of existing ingredients
3. Convert recommendations into a shopping list
4. Edit the cart or proceed with the payment



Integration with over 5,000 applications



Easy to integrate



ChatGPT Use Case: Perform Work

Zapier – connecting work applications

- Connect apps (like Google Sheets, Gmail, Discord, Excel, Spotify, Teams) and interact with them directly inside ChatGPT
- Automation workflows and tasks within the ChatGPT interface:
 - Send emails to prospects & leads
 - Add, search or update a database
- Information sharing between applications to save time

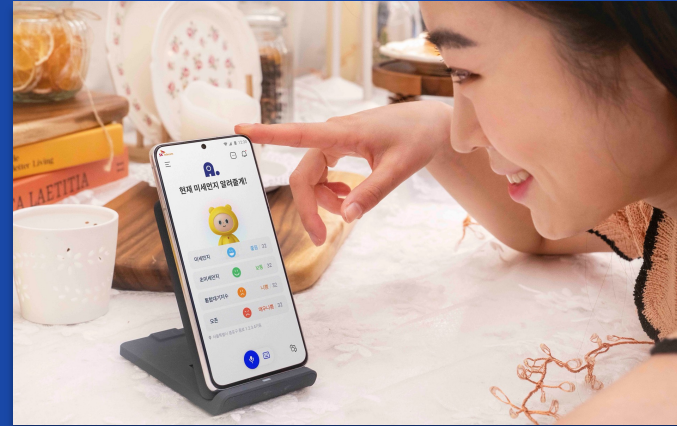
ChatGPT: Industry Use Cases

The OpenAI logo, a stylized interlocking knot, is centered within a dark square that serves as a background for the text.

ChatGPT in Telecommunications

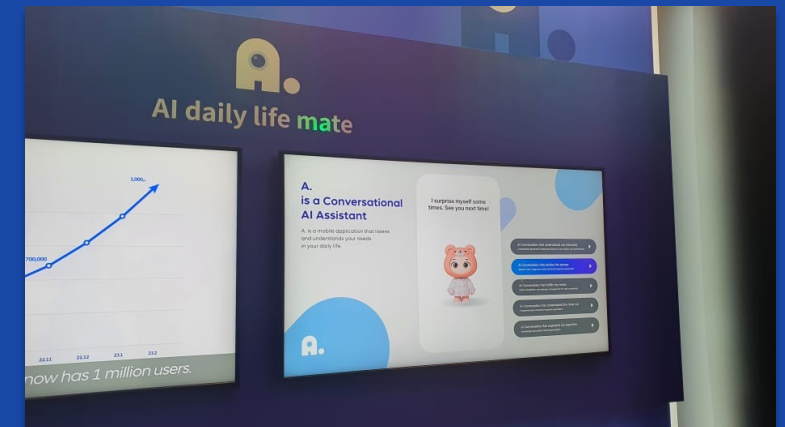
SK Telecom – “One Stop Shop Super App”

- Launch a beta version of A. (A dot), an artificial intelligence chatbot based on generative AI technology
- Integration with various services (i.e., music streaming, e-commerce, and payment)
- Learns about users to provide advanced customer personalisation



- An in-app chatbot for customers with customisable characters and an aesthetic interface

- Customers solve daily life issues by assessing other services within the SKT ecosystem



ChatGPT in Telecommunications

Etisalat partnered with Microsoft to integrate ChatGPT in customer service and internal processes

- Enhance overall performance and decision-making
- Improve KPI setting
- Reduce time and effort spent on daily operations



Phase I

- Integrate Azure-based Open AI service capabilities
 - HR chatbot
 - Personalised customer support

Phase II

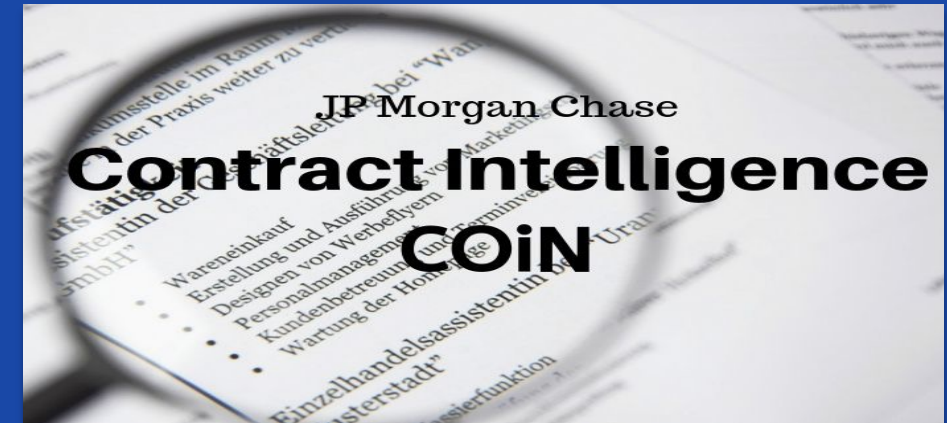
- Offers different solutions and services in the UAE
 - Media & creative industry tools
 - Advance enterprise digitalisation

ChatGPT in Banking and Finance

JPMorgan launched a ChatGPT-like, in-house tech in 2017

- COiN stands for Contract Intelligence that utilizes unaided AI that automates document reviews:
 - Able to complete 360,000 hours of legal work (review credit contracts) in mere seconds
 - Fueled by private cloud network
 - More accurate and time-saving solution

JPMORGAN CHASE & CO.



Short Term Strategy

Deploy COIN for more complex filings:

- Credit-default swaps
- Custody agreements

Medium & Long-Term Strategy

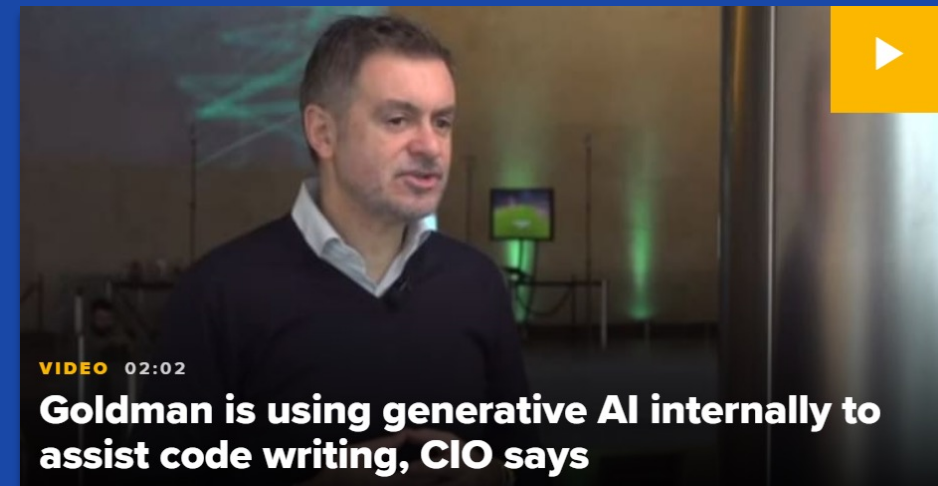
Interpret altogether new regulations: (questions of "first impression")

ChatGPT in Banking and Finance

Goldman Sachs has been experimenting with generative AI tools, similar to ChatGPT, to help developers write code:

- Developers can now write 40% of the required code automatically using AI
- Automate code testing and generate new iterations

Goldman
Sachs

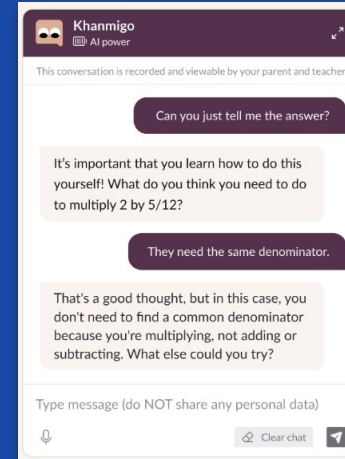


According to Goldman Sachs Research, generative AI could raise global GDP by 7% (~US\$ 7 trillion) and increase productivity by 1.5% over 10 years.

ChatGPT in Education

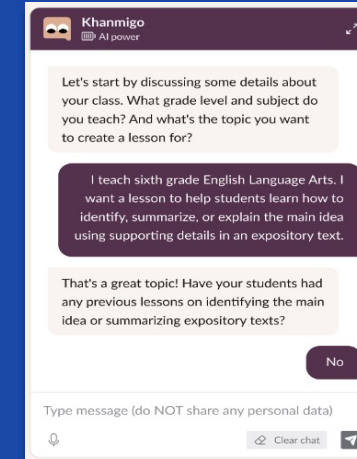
Khan Academy launched Khanmigo, an AI-powered assistant for students and teachers:

- Guide students through courses or get help on:
 - Solving math problems
 - Practice new words
 - Debate on a topic
 - Prep for exams
 - Learn computer programming
- Help teachers with administrative tasks:
 - Write lesson plans
 - Creating lesson hooks
 - Writing exit tickets



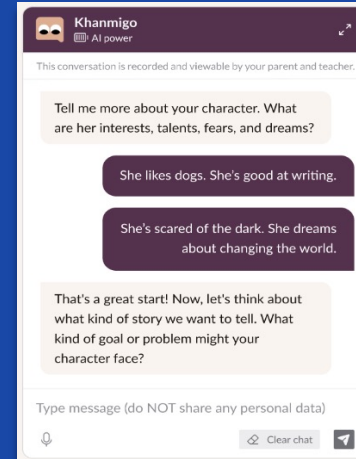
Virtual Tutor

- Assist in one-on-one tutoring



Teaching Assistant

- Help teachers brainstorm ideas
- Explore relevant topics



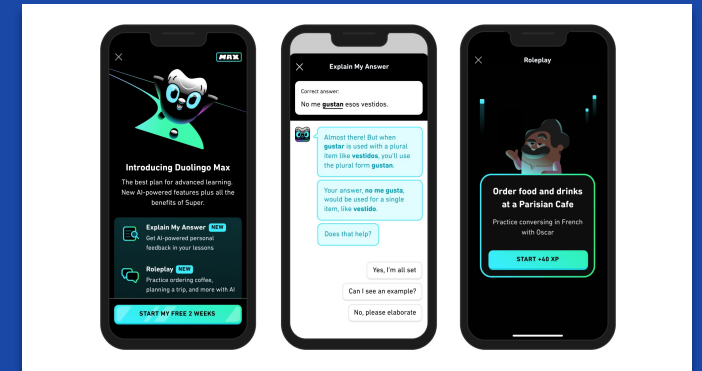
Creativity Booster

- Expert advisor
- Generate new ideas

ChatGPT in Education

Duolingo introduced Duolingo Max, a new subscription tier above Duolingo Super.

- On top of highly personalised language learning lessons, users can assess personalised reviews through the Practice Hub as well as two additional AI-powered features:
 - Explain My Answer
 - Roleplay



1. Explain My Answer

- Offers learners a chance to learn more about their responses in a lesson (right or wrong). Enter into a chat with Duo for a simple explanation and further clarification.

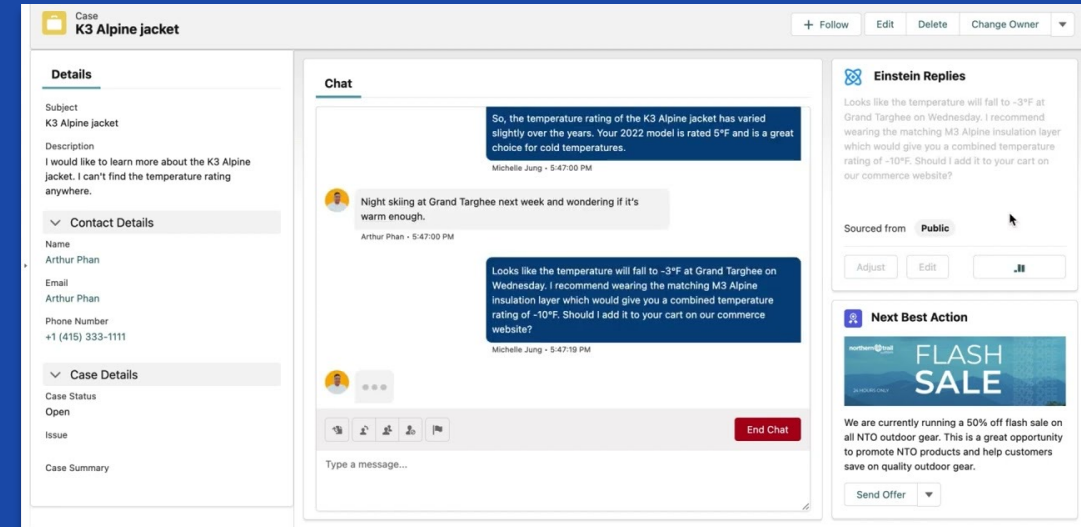
2. Roleplay

- Learners can practice real-life conversation skills with different characters in different scenarios (i.e., planning a vacation with Lin, ordering a coffee in Paris, furniture shopping with Eddy or asking out a date).

ChatGPT in Sales & Marketing

Salesforce's Einstein GPT is a generative AI for CRM:

- Integrated across services like Slack, Messenger, Tableau, etc.
- Real-time support for various applications:
 - Compose emails
 - Schedule meetings
 - Generate knowledge articles from past notes for auto-generated agent chat replies
 - Personalised content for customers and prospects across channels
 - Delivering new customer insights (i.e., sales opportunities)
 - Generate code for developers

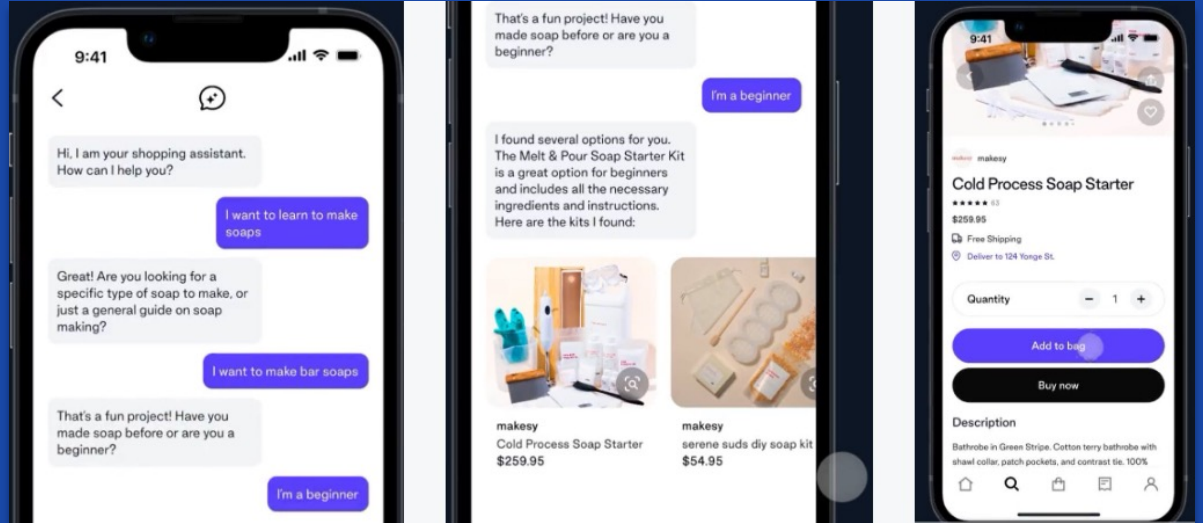


According to Salesforce, Einstein GPT processes over 200 billion AI-powered predictions per day. It grabs real-time data from the Salesforce Data Cloud, and users use prompts directly within their Salesforce CRM to generate content that changes on the fly based on changing customer information.

ChatGPT in E-Commerce

Similar to “Ask Instacart”, Shopify’s consumer app, Shop, uses ChatGPT to power its new AI shopping assistant.

- Makes personalised recommendations based on user prompts and requirements
- Streamline in-app shopping by quickly finding out what buyers need through product data scanning
- Helps buyers explore new products

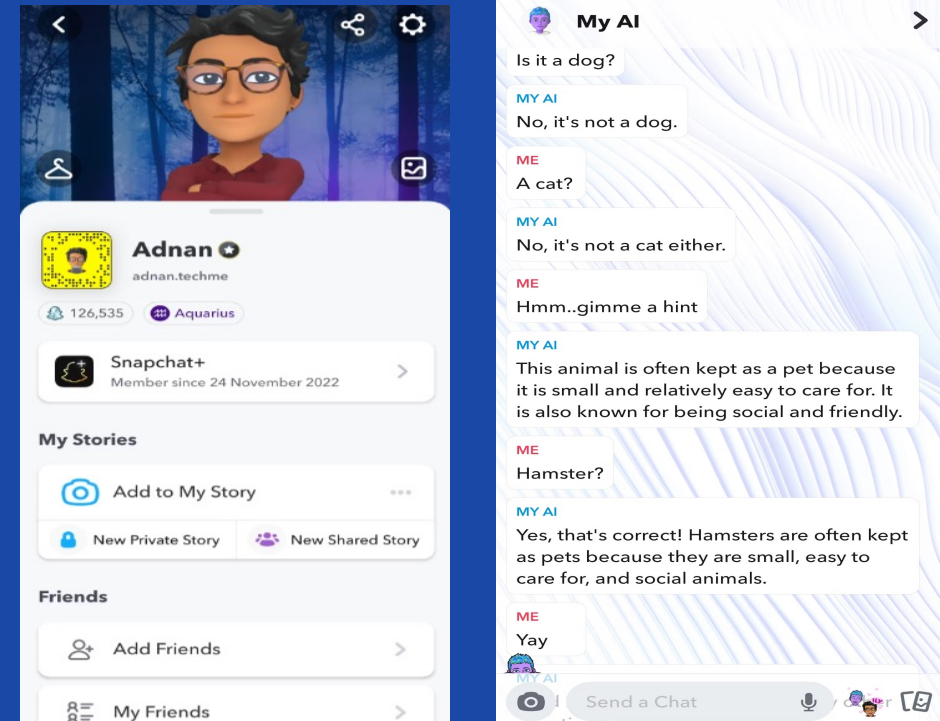


- Users can engage in natural, human-like conversations just as they would with a real-life shopping assistant
- Get instant recommendations and customise user requirements on-the-go

ChatGPT in Social Media

Snapchat released its new AI-powered chatbot, My AI, built on ChatGPT for Snapchat Plus subscribers.

- Generative AI is being treated more like a virtual persona than a productivity tool (a friend over a search engine)
- More conversational than Bing Chat or ChatGPT
- Users can give My AI a new name, customise the bot's Bitmoji (avatar), get recommendations on lifestyle topics and ask regular questions



According to Snapchat, “The big idea is that in addition to talking to our friends and family every day, we’re going to talk to AI every day.”



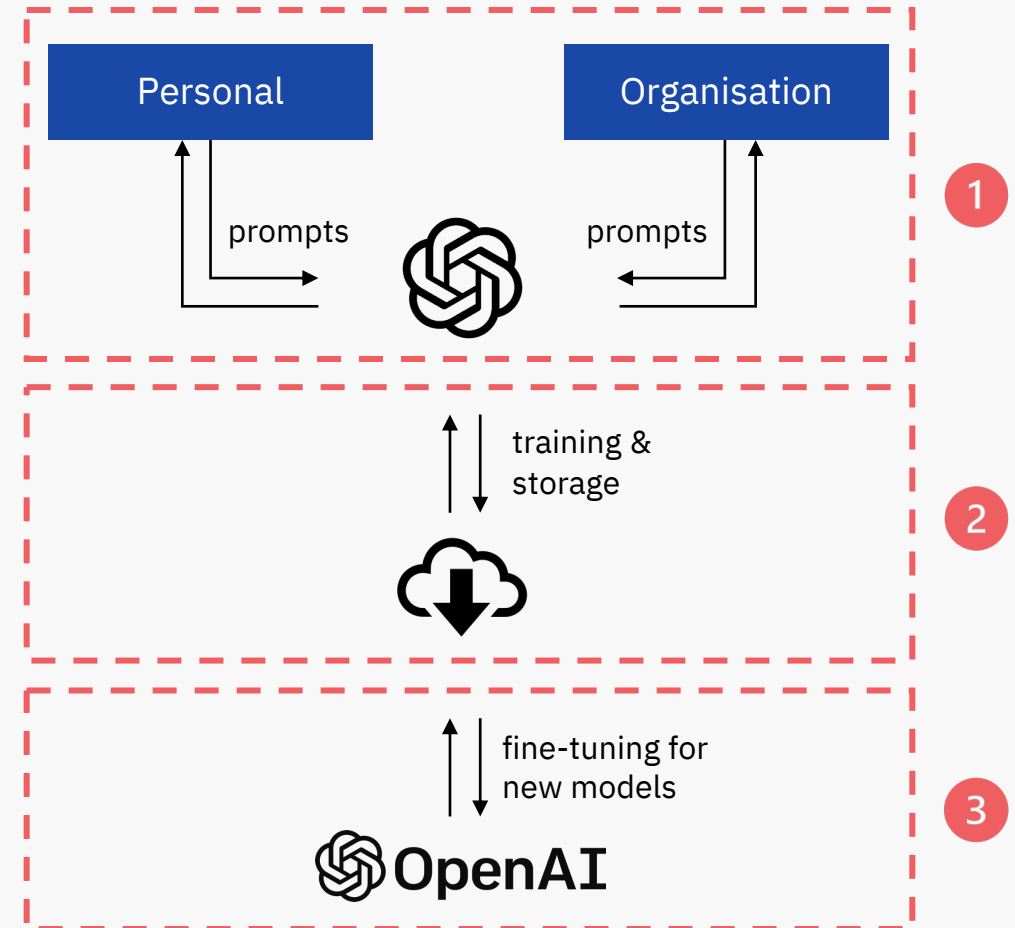
ChatGPT: Potential Risks

Security risks prevails as ChatGPT grows in popularity

The most common security risk of using ChatGPT is data privacy & vulnerability.

Currently, LLMs do not 'learn' or automatically add information from queries to their current model for others to query.

1. However, the queries will be **visible and stored** by the LLM provider. This means that the LLM provider (or its partners) can **read queries and may incorporate them** into future versions.
2. Also, queries that are most likely stored online may be subject to **hacks, leaks, and accidentally made public**. This could expose potentially user-identifiable information.
3. The operator of the LLM, which owns the database containing training data, is later acquired by an organisation with a **different approach to privacy** than was enforced when data was entered by users.



Case: Samsung accidentally leaked secrets to ChatGPT

What happened?

- Samsung's semiconductor division allows engineers to use ChatGPT to check for bugs and errors in source codes.
- There were three separate instances where employees leaked sensitive information:
 - Pasted confidential source codes into the ChatGPT interface to check for errors
 - Optimise test code sequences for identifying faults in chips
 - Shared recording of a private meeting to be converted into notes

What is the solution?

- Samsung immediately restricted ChatGPT upload capacity to 1,024 bytes per employee.
- Investigated those involved in the leak for disciplinary actions
- Considering building an internal AI chatbot to prevent future instances

What is the impact?

- Confidential information is exposed and potentially used for future query responses.
- Higher vulnerability to cyber attacks/threats

Case: ChatGPT leaked user data on March 20

Situation:

A bug in an open-source library allowed some users to see titles from another active user's chat history. It's also possible that the first message of a newly-created conversation was visible in someone else's chat history if both users were active around the same time.

That bug also caused the unintentional visibility of payment-related information of 1.2% of the active ChatGPT Plus subscribers during a specific nine-hour window.

ChatGPT was temporarily shut down for the team to patch the bug as they contacted affected users.

Leaked data included:

- First and last name
- Email address
- Payment address
- Last 4 digits credit card number
- Expiration date of credit card
- Conversation histories

Impact of the leak:

- Loss of trust in ChatGPT
- Exposed personal & confidential information
- Further bans of ChatGPT in countries and organisations
- Increased security threats

Technical details

The bug was discovered in the Redis client open-source library, redis-py. As soon as we identified the bug, we reached out to the Redis maintainers with a patch to resolve the issue. Here's how the bug worked:

- We use Redis to cache user information in our server so we don't need to check our database for every request.
- We use Redis Cluster to distribute this load over multiple Redis instances.
- We use the redis-py library to interface with Redis from our Python server, which runs with Asyncio.
- The library maintains a shared pool of connections between the server and the cluster, and recycles a connection to be used for another request once done.
- When using Asyncio, requests and responses with redis-py behave as two queues: the caller pushes a request onto the incoming queue, and will pop a response from the outgoing queue, and then return the connection to the pool.
- If a request is canceled after the request is pushed onto the incoming queue, but before the response popped from the outgoing queue, we see our bug: the connection thus becomes corrupted and the next response that's dequeued for an unrelated request can receive data left behind in the connection.
- In most cases, this results in an unrecoverable server error, and the user will have to try their request again.
- But in some cases the corrupted data happens to match the data type the requester was expecting, and so what gets returned from the cache appears valid, even if it belongs to another user.
- At 1 a.m. Pacific time on Monday, March 20, we inadvertently introduced a change to our server that caused a spike in Redis request cancellations. This created a small probability for each connection to return bad data.

This bug only appeared in the Asyncio redis-py client for Redis Cluster, and has now been fixed.

How to prevent a data leak when using AI?

Six steps to take as an organisation

Secure communication channels	Implement tight access controls	Monitor and audit related activity	Enforce data retention policies	Conduct employee training	Conduct regular security assessments
Ensure all data being transmitted between the company's servers and the chat platform is securely encrypted	Impose strict authentication protocols and user access controls to ensure that only authorised users can access sensitive data	Monitor all levels of activities on the communicating platform including data or file transfer and logging histories	<ol style="list-style-type: none">1. What data can be shared?2. How long should data be retained?3. How should it be securely disposed of?	Provide robust training to all employees interacting with ChatGPT tech on data security best practices	Regularly assess the security of all systems that are in contact with ChatGPT

twimbit
be more



Insights



Immersions



Challenges

How can we help?

reachus@twimbit.com