

Using AI Securely

A screenshot of the ChatGPT Plus announcement page. The background is dark purple. On the left, the text 'Introducing ChatGPT Plus' is displayed in a light green font. Below it, a smaller line of text describes the Plus plan as a subscription for ChatGPT, a conversational AI that can chat with you, answer follow-up questions, and challenge incorrect assumptions. A small button labeled 'Read about ChatGPT' is visible. On the right side of the image, there is a blurred screenshot of a chat interface with alternating green and purple horizontal lines representing text messages.

Introducing ChatGPT Plus

Introducing the Plus plan for ChatGPT, a conversational AI that can chat with you, answer follow-up questions, and challenge incorrect assumptions.

[Read about ChatGPT](#)

A Brave New World?

You are no doubt aware of the hype around AI, especially since the second half of 2022. Depending on your point of view, AI either represents a utopian future for humanity or a serious threat to our security and way of life. You may have used ChatGPT to do research, write an essay or translate a document. In this short course you will get an overview of AI, what it is, how it can improve our lives and what security issues it brings.

What is AI?

AI, or Artificial Intelligence, is a technology that enables machines to perform tasks that typically require human intelligence, such as problem-solving and decision-making.

In simple terms, AI mimics human thinking to solve problems and make smart choices, making it a powerful tool in various fields, including cybersecurity, healthcare, and transportation.

AI allows computers and machines to learn from data, adapt to latest information, and improve their performance over time, making them increasingly capable and efficient.

Aren't AI and Google the Same Thing?

While it is true that AI and Google are related, they are not the same thing. Google uses AI technologies in its search, mapping, and translation services (among many others) but AI itself is a broader concept that encompasses the development of intelligent systems that can perform tasks requiring human-like intelligence.

Why use AI?

- Increased Efficiency: AI automates repetitive tasks and processes enabling tasks to be completed faster and efficient.
- Improved Accuracy: AI can process vast amounts of data with precision providing reliable insights and predictions.
- Enhanced Personalization: AI technologies can tailor experiences based on individual preferences, leading to better customer service and personalized recommendations.
- Automation: AI can automate repetitive and everyday tasks, freeing up human resources to focus on more complex and creative aspects of their work.
- Advanced Problem-Solving: AI's analytical capabilities help tackle challenging problems in various domains, including healthcare, finance, and cybersecurity, providing innovative solutions for complex issues.

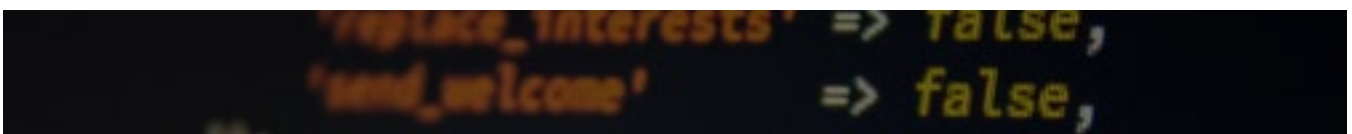




How AI Can Improve Security

- AI can enhance cybersecurity by enabling faster and more accurate threat detection and response.
- AI can leverage machine learning algorithms to analyse vast amounts of data in real-time.
- AI can detect anomalies that may go unnoticed by humans.
- AI allows the automation of security processes such as patch management for faster incident response.
- AI can trigger real-time alerts to reduce the potential impact of a breach.

These capabilities can help organizations to respond quickly when threats arise while minimizing financial loss or reputational damage. However, it is important to remember that as AI becomes more sophisticated so do the security risks associated with it. Therefore, prioritizing security measures during development and implementation is essential for any organization leveraging AI.





Data Protection Concerns

AI raises privacy concerns because it relies on large amounts of sensitive information. The collection, storage and processing of personal data raises privacy and security issues and may lead to data breaches or misuse.

- AI relies on vast amounts of data to train and improve its performance. Some of this data can be sensitive, and if not handled properly, can lead to privacy breaches.
- AI systems are subject to attacks from hackers and cybercriminals, who may exploit system vulnerabilities to gain unauthorized access to sensitive data.
- Major concerns include poor development processes, data breaches and identity theft, poor security in AI applications, data poisoning attacks, lack of transparency and explain ability.



Data poisoning aims to trick AI systems by intentionally supplying of misleading or bad data to impact the quality of AI.

Cybersecurity Concerns

The background image for the 'Cybersecurity Concerns' section shows a person's face in a dark, low-key setting. Their hands are raised to their face, and glowing green digital numbers and symbols, such as '240', '28', and '19', are superimposed over their skin, suggesting a digital or cyber theme.

The integration of AI in cybersecurity raises concerns about potential vulnerabilities and exploitation. While AI can enhance threat detection and defence, malicious actors could also use it to create sophisticated attacks that are harder to identify and combat.

- Unscrupulous actors may exploit vulnerabilities in AI systems to cause harm or security breaches.
- Phishing attacks are a common way for malicious actors to target individuals or organizations by exploiting these weaknesses.


- Hacking threats such as inputting bad or malicious data to fool AI into making wrong decisions.
- Inputting biased data to influence AI decisions.
- Unauthorized access: Hackers gain control over the AI infrastructure to steal data, manipulate systems, or deploy malicious AI models.
- Deepfakes: AI can be used to create realistic fake images, videos, or audio. These can be misused for spreading misinformation, impersonation, or defamation.



The term "deepfake" refers to a manipulated or altered media, such as images, videos, or audio recordings, which have been created using AI techniques. Deepfakes are known for their ability to generate highly convincing and often hyper realistic content that can be difficult to distinguish from genuine media.

Ethical Concerns





The advent of AI has raised some ethical concerns regarding its potential impact on privacy, bias, and human autonomy.

Big Data

As AI systems process massive datasets, privacy breaches and unauthorized data access become significant concerns.

Biased Management

Biases in AI algorithms, resulting from biased training data, can lead to unfair outcomes, perpetuating discrimination.

Biased data manipulation

AI systems can inadvertently inherit biases present in the data they are trained on, leading to biased decision-making or discrimination.

What can be done to minimize ethical concerns related to AI?

- Striking ethical guidelines that prioritize fairness, transparency, and accountability is essential to harness AI's potential while ensuring its responsible and equitable deployment.

- Ensuring AI is designed and used ethically requires transparency, accountability, and a commitment to mitigating biases to foster trust and responsible AI deployment.



Using AI Securely

Here are some tips to keep yourself and your organization secure when using AI in its various manifestations. Click on the forward or back arrows to view each tip.

Tip 1

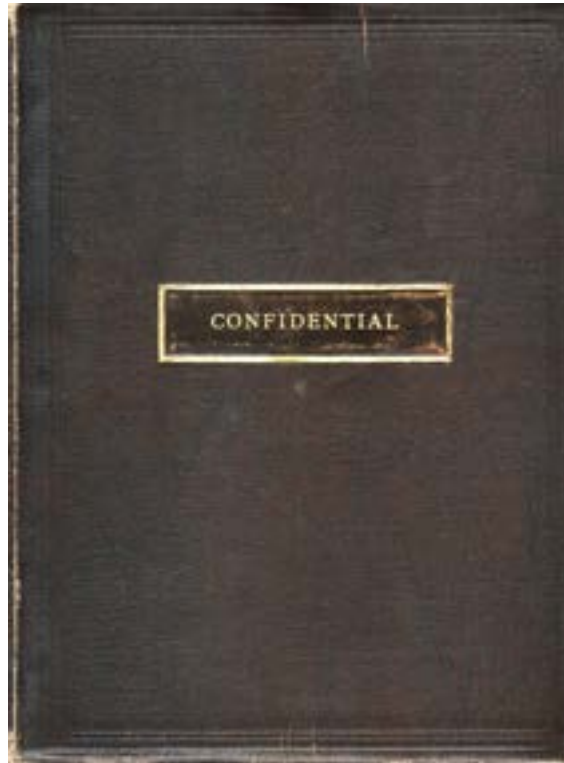
Choose your AI application carefully



Hackers are aware of the exponential rise in the use of AI applications and have responded by creating fake AI apps designed to distribute malware and steal data, so be sure to use legitimate applications only.

Tip 2

Don't input sensitive information



Never use AI for tasks that involve personal or sensitive information.

For example, it would be extremely risky to use Chat GPT to create a set of corporate policies and procedures, as any content you create will be stored on Chat GPT's servers in an unknown location. Chat GPT will use your information when responding to requests from other users, which means that your company's sensitive information may be exposed. In addition, uploading personal information may violate data protection regulations.

Tip 3

Garbage in, garbage out



The data you get from an AI app is only as good as the data it receives- if its data is out-of-date or incomplete, the content it generates could be wrong or inaccurate.

Tip 4

Be careful when coding



AI can provide software or application developers with a quick and easy way to generate code. However, AI-generated code can contain bugs or vulnerabilities that can lead to unsafe or unstable programmes or applications.

Tip 5

Be extra vigilant against cyberattacks

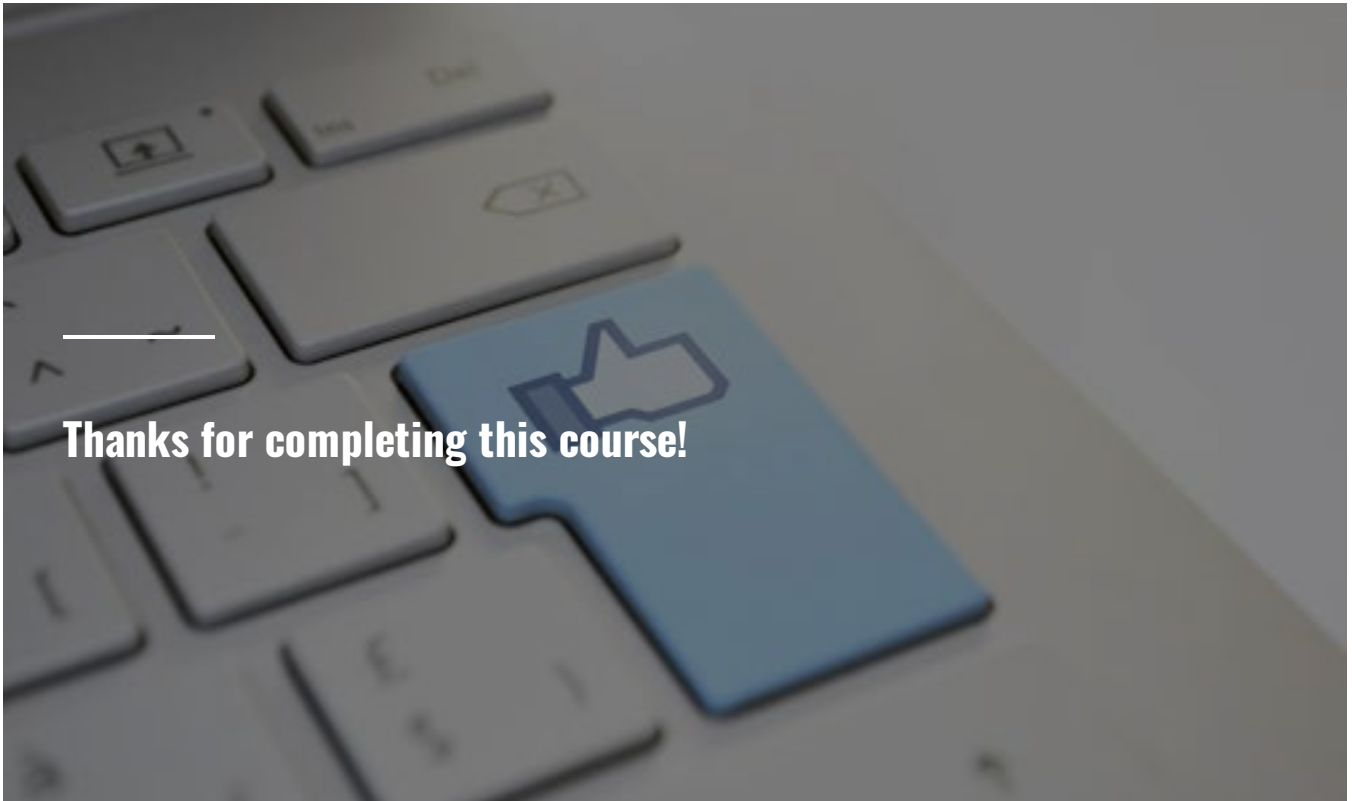


The advent of AI has made life easier for hackers and other unscrupulous individuals. They can leverage AI to generate millions of convincing emails that are much harder for both spam filters and humans to detect. These increasingly sophisticated phishing attacks can put you and your business at increased risk.

Summary

AI has the potential to immeasurably improve our working and personal lives. Unfortunately, it also makes life easier for those who try to exploit its potential. Always keep this in mind when using AI. Only use legitimate AI applications, do not enter personal or confidential information into a chatbot, and be aware of the increased likelihood of cyberattacks

Thanks for completing this course!



Explore our comprehensive course catalog today and embark on a journey of
lifelong learning!

Visit our website www.vigitrust.com

Email: info@vigitrust.com

