NAVIGATING A.I. SAFELY

PROTECTING YOUR BUSINESS

CONTENTS

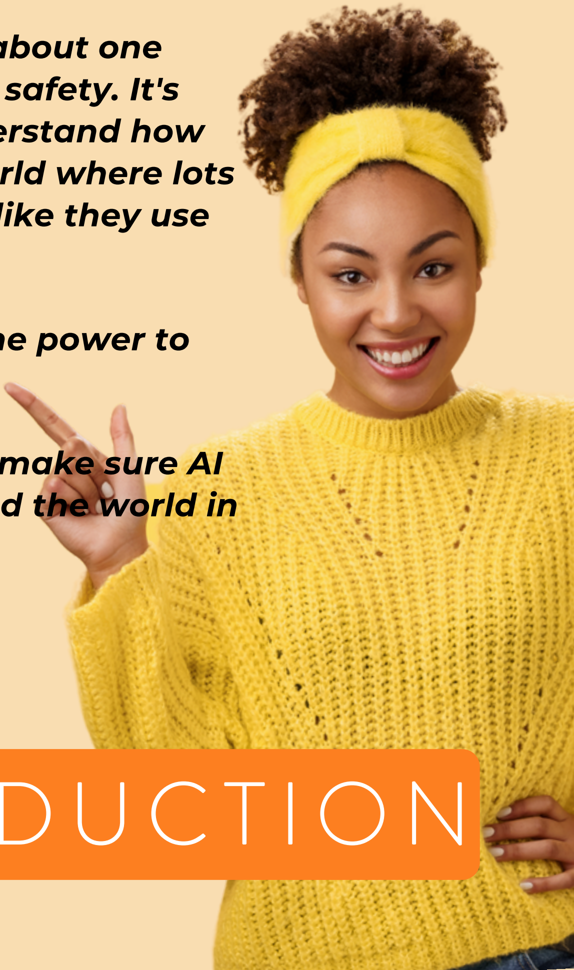
INTRODUCTION

Technology is moving very quickly, and one big part of this change is artificial intelligence (AI). AI is making big changes for businesses and people. AI can do things like make processes smoother and give personalized help. But as AI gets bigger, there are more problems to think about.

This eBook talks a lot about one important thing for AI: safety. It's very important to understand how to keep AI safe in a world where lots of people are using AI like they use their phones.

Remember, we have the power to use AI the right way.

Let's work together to make sure AI helps your business and the world in a good way.



Understanding AI problems and their effects is crucial to protect your business and personal interactions in a world driven by AI

Adversarial Attacks: Bad actors can take advantage of AI weaknesses to mess with the data AI uses, causing it to give wrong results. For instance, hackers might add confusing information to AI face recognition software, making it unable to recognize the right person.

Model Inversion Attacks: Attackers can use AI results to figure out private information about people. For example, if an AI recommends a personalized diet plan based on someone's medical history, attackers could study the suggestions to guess the person's medical background.

Data Manipulation and Poisoning: If hackers tamper with the data used to teach AI models, it can make the AI produce incorrect results. For instance, if the data used for self-driving cars or traffic signals gets messed up, it could cause deadly accidents or chaos on the roads.

Algorithmic Biases: Sometimes, AI algorithms unintentionally show bias because they were trained on biased data. This can lead to unfair or unjust decisions. For example, an AI loan approval system might deny loans to specific people if the training data has unfair information about them.

AI-Powered Attacks: Attackers can use AI's abilities to plan big attacks, like using ransomware or tricking people with phishing emails. For example, cybercriminals might use AI chatbots to create perfect phishing emails that don't have the usual mistakes like grammar errors.

Deepfakes and Impersonations: AI-generated deepfake videos can spread false information, fooling people and causing fraud or harm to someone's reputation. For instance, in today's world where many banks use online KYC (Know Your Customer) checks, malicious people could make incredibly realistic videos using someone else's voice and image to open accounts for illegal activities.

POTENTIAL ISSUES AND CONSEQUENCES

Navigating AI Safely: Protecting Your Business

Xact IT Solutions
There are no IT problems.. only IT solutions

As AI becomes a crucial part of our modern lives, it's incredibly important to use it safely and responsibly. Here are some basic AI safety guidelines to keep in mind:

Choose Wisely: Select AI tools from well-known and trusted sources.

Verify Trustworthiness: Opt for technologies that have a strong track record of security and addressing vulnerabilities.

Fortify Access: Strengthen security by using strong, unique passwords and enabling two-factor authentication.

Stay Updated: Keep your software current by promptly applying security updates to prevent potential threats.

Guard Permissions: Be cautious when granting AI applications access to sensitive information and personal data.

Prioritize Privacy: Regularly review privacy policies, adjust settings, and limit data sharing to maintain control over your information.

Prioritize Privacy-Centric Choices: Choose AI tools that prioritize protecting user privacy and data.

Beware of Scams: Stay alert for phishing attempts and dishonest AI apps that could put your data and devices at risk.

Rely on Safe App Stores: If you're searching for AI apps on app stores, only download them from official app stores to reduce the chance of security problems.

Think Critically: Be careful when relying on AI-generated recommendations, especially for important decisions.

Back-Up Data: Regularly make copies of critical data to safeguard against AI malfunctions or cyber incidents.

Stay Informed: Read trustworthy journals or publications by staying up-to-date with the latest AI developments and security risks.

A.I. SAFETY

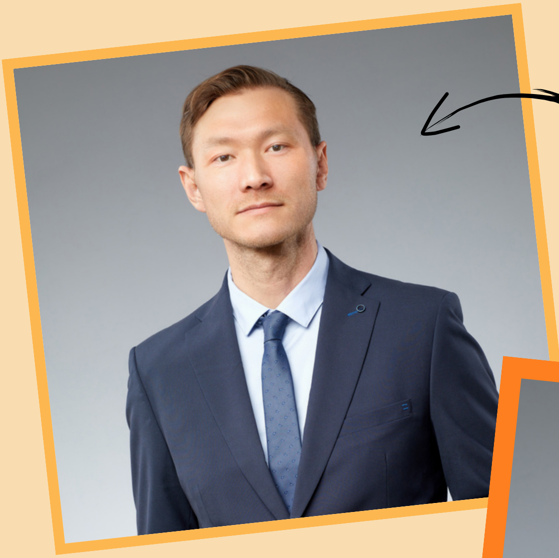
PRACTICES

As you bring AI into your business and personal life, always keep in mind the importance of using it responsibly. Our team is here to assist you at every stage of your journey. Whether you require guidance on AI safety practices, seek dependable AI tools, or have inquiries about the changing AI landscape, feel free to reach out to us anytime. We're just a message away and ready to help.

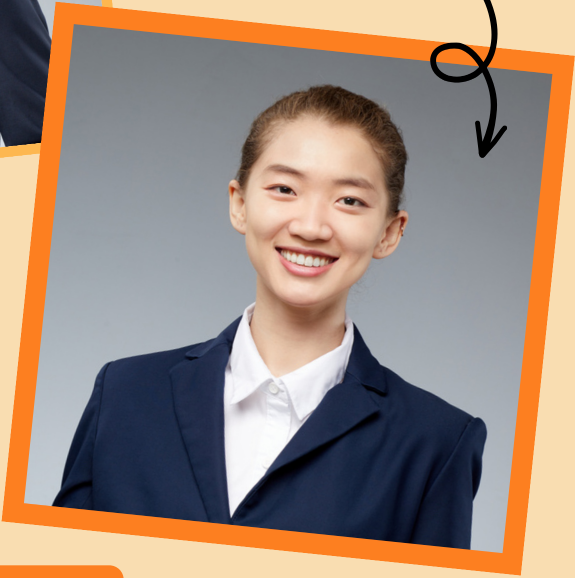
☎ **856-282-4100**

READY TO EMBRACE A.I.'S POTENTIAL?

Can you find the red flag in these two pictures?



What's wrong with these two?



SPOT THE

RED FLAGS

Use the hints to unscramble the words.

TUNOIAMAOT

HINT: Using AI to complete tasks instead of humans.

VCTEDIEPE IA

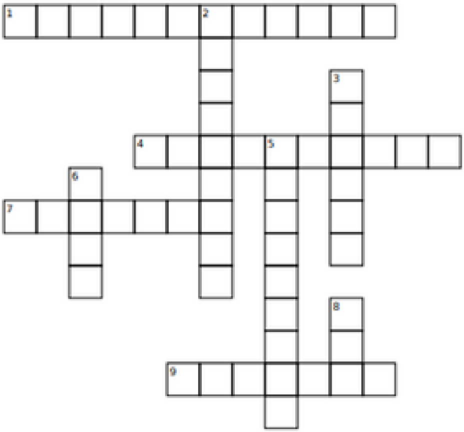
HINT: These types of applications may compromise your data or devices

GOIGESSUNTS

HINT: Data offered by AI platforms.

WORD SCRAMBLE

Use the hints to unscramble the words.



Down:

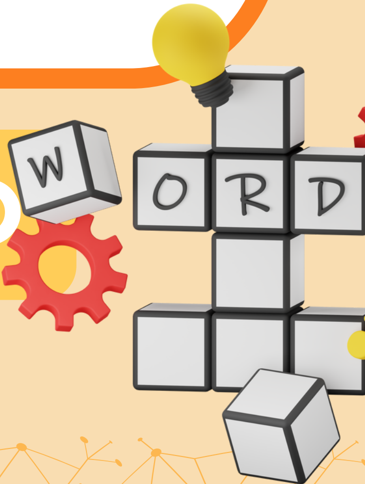
2. A set of rules a machine follows to do a task.
3. Its versatility and array of robust libraries make it the go-to programming language for chatbot
5. Famously said by Arnold Schwarzanegger's character from the future, "My CPU is a ________ processor; a learning computer.
6. a Major AI bot competitor created by a search giant
8. The famous AI who said, "I'm sorry, Dave.

Across:

1. function of artificial intelligence that imitates the human brain by learning from how data is structured
4. Its versatility and array of robust libraries make it the go-to programming language for chatbot creation.
7. a Popular AI chatbot used for generating content
9. Adobe's latest entry into the AI art space

CROSSWORD

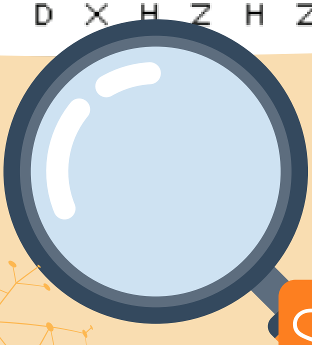
PUZZLE



CHATBOT
COGNITIVE COMPUTING
PREDICTIVE ANALYTICS
MACHINE INTELLIGENCE

IMAGE RECOGNITION
DEEP LEARNING
DATA MINING
TURING TEST

O	T	S	M	E	M	X	F	R	F	E	G	C	I	E
A	S	W	B	V	V	I	F	F	V	U	N	T	N	C
U	A	M	M	W	M	I	Q	I	A	U	I	R	T	D
T	O	B	T	A	H	C	T	E	R	O	T	V	E	G
G	D	Z	G	G	C	C	R	I	V	W	U	P	L	N
I	V	E	S	C	I	H	T	F	N	O	P	T	L	I
H	B	B	E	D	D	R	I	U	V	G	M	U	I	N
E	S	O	E	P	G	N	F	N	R	G	O	K	G	R
T	B	R	M	I	N	I	N	G	E	I	C	C	E	A
E	P	I	F	N	Y	V	Y	B	X	J	N	F	N	E
S	Q	Y	K	U	Z	E	D	L	C	V	L	G	C	L
T	H	E	J	A	N	A	L	Y	T	I	C	S	E	A
N	O	I	T	I	N	G	O	C	E	R	V	M	T	K
J	A	B	K	B	Q	U	V	U	C	Q	P	A	O	I
S	Y	B	D	X	H	Z	H	Z	W	B	D	X	Q	O



WORD SEARCH

Spot the Red Flags!

Both models are not human. They were created with AI software. Deep fakes use AI to manipulate videos and images to create a digital representation of the target person. Don't believe everything you see. Always check the sources

Word Scramble

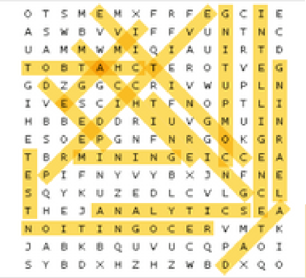
Automation
Deceptive AI
Suggestions

Crossword

DOWN
2. Algorithm
3. Python
5. Neuralnet
6. Bard
8. HAL9000

ACROSS
1. Deep Learning
4. Turing Test
7. ChatGPT
9. Firefly

Word Search



```
O T S H E M X F R F E G C I E
A S W B V V I F F V U N T N C
U A M M W M I Q I A U I R T D
T O B T A H C T E R O T V E G
G D Z G G C C R I V W U P L N
I V E S C I H T F N O P T L I
H B B E D D R I U V G M U I N
E S O E P G N F N R G O K G R
T B R M I N I N G E I C C E A
E P I F N Y V Y B X J N F N E
S Q Y K U Z E D L C V L G C L
T H E J A N A L Y T I C S E A
N O I T I N G O C E R V M T K
J A B K B Q U V U C Q P A O I
S Y B D X H Z H Z W B D X Q O
```

ACTIVITIES

KEY