

ARTIFICIAL INTELLIGENCE AND THE RISE OF THE HUMANS

BB KING

PENTESTER @ BLACK HILLS INFOSEC

INSTRUCTOR @ ANTI-SYPHON TRAINING

@BBHACKING IN OTHER PLACES

[HTTPS://GITHUB.COM/BBHACKING/](https://github.com/BBHACKING/) ← THESE SLIDES AND FURTHER READING

1

AI IS HERE.
HI.

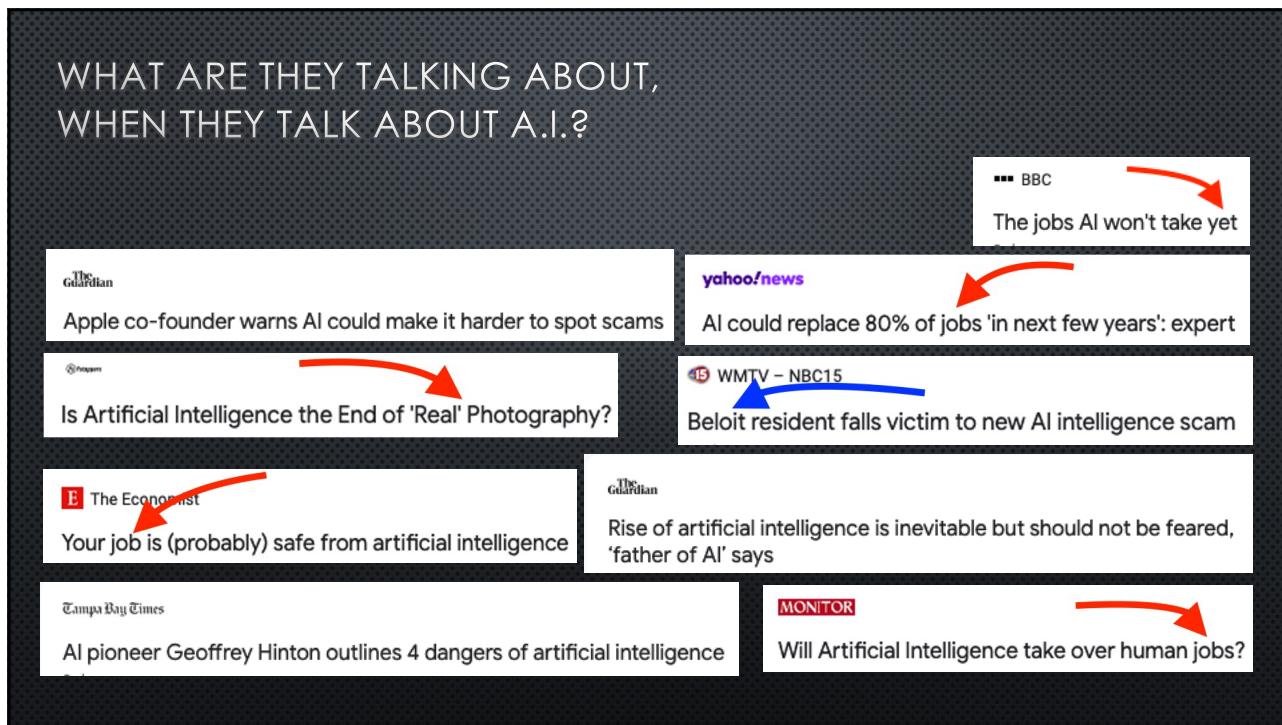


THIS LAWN MOWER IS POWERED BY
ARTIFICIAL INTELLIGENCE AND
DOESN'T NEED A REMOTE CONTROL

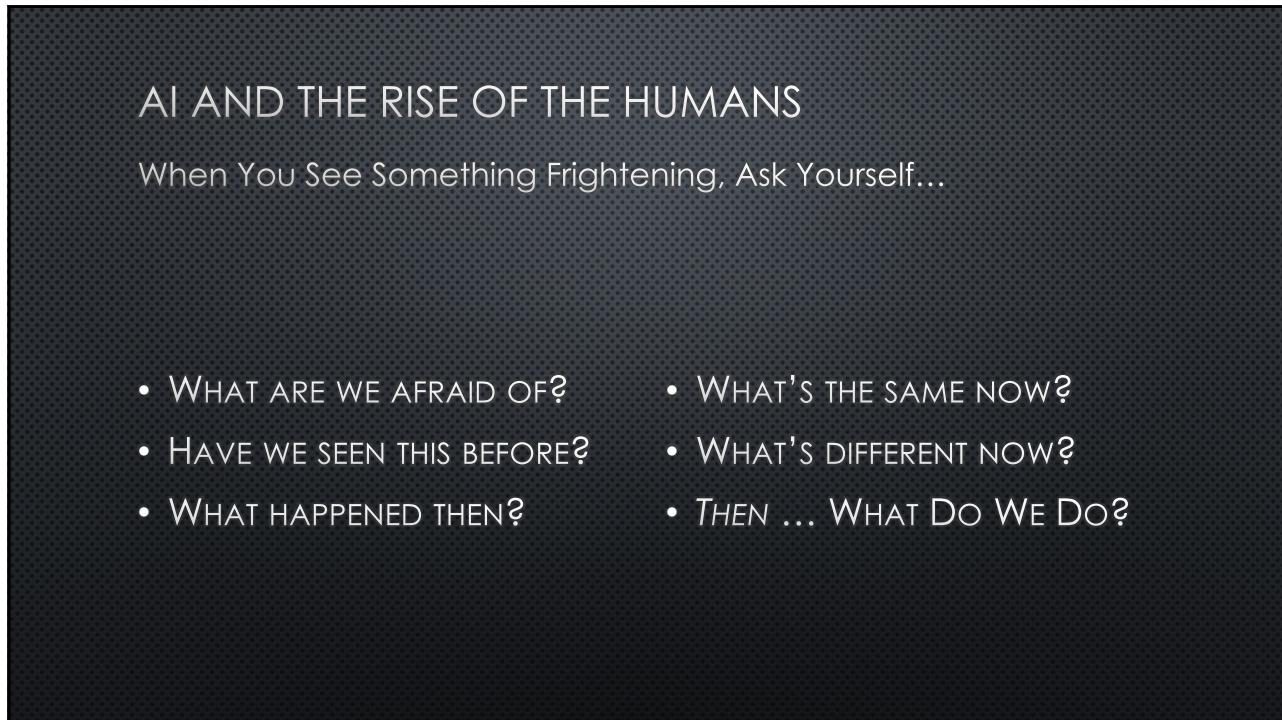
TECH / SMART HOME
Oral-B's new \$220 toothbrush has AI to tell you when you're brushing poorly / \$220 is double my yearly dental hygiene budget

The Columbus Dispatch
Wendy's to launch drive-thru AI program at Columbus area location

2



3



4

HAVE WE BEEN AFRAID OF THIS BEFORE?

IDEAS.TED.COM

BUSINESS

Will automation take away all our jobs?

Mar 29, 2017 | David Autor

MIT Technology Review

SUBSCRIBE

How Technology Is Destroying Jobs

Automation is reducing the need for people in many jobs. Are we facing a future of stagnant income and worsening inequality?

By David Rotman

June 12, 2013

Forbes

FORBES > INNOVATION > CONSUMER TECH

Technology Has Already Taken Over 90% Of The Jobs Humans Used To Do

Jan 18, 2018 | Last Updated: Jan 18, 2018

This article is more than 5 years old.

5

Computers replaced “computers” 50 years ago and yet spaceflight is still a thing.

How we do computation is different.
Going to space is still the reason.
Still like space?
There's still a place for you.

<https://www.nasa.gov/feature/jpl/when-computers-were-human>

6

YES, WE HAVE BEEN AFRAID OF THIS BEFORE

- SOME JOBS LOST THEIR VALUE.
- OTHERS WERE TRANSFORMED.
- AND WE ARE BETTER OFF NOW.

THE “HOW” CHANGES. THE “WHAT” AND THE “WHY” ... LESS SO.

7

WHAT'S THE SAME?

- WE ARE STILL HUMANS
- WE ARE STILL BAD AT PREDICTIONS
- WE STILL ... NEGATIVITY BIAS
- OR MIDWESTERN POLLYANNA!

WHAT'S DIFFERENT?

- ALL OF US CAN PLAY WITH IT
 - FOR GOOD OR ILL
- REGULATIONS WILL FAIL
 - THE REALLY BAD OUTCOMES DON'T COME FROM THE RULE-FOLLOWERS.

8

**THE SAME:
LET'S MAKE RULES.**

TIME
TECH • ARTIFICIAL INTELLIGENCE
European Union Set to Be Trailblazer in Global Rush to Regulate Artificial Intelligence

TECH
Elon Musk and other tech leaders call for pause on 'dangerous race' to make A.I. as advanced as humans
PUBLISHED WED, MAR 29 2023 8:23 AM EDT | UPDATED WED, MAR 29 2023 11:30 AM EDT
<https://futureoflife.org/open-letter/pause-giant-ai-experiments/>

The Atlantic
Never Give Artificial Intelligence the Nuclear Codes

ANNALS OF ARTIFICIAL INTELLIGENCE
THERE IS NO A.I.
There are ways of controlling the new technology—but first we have to stop mythologizing it.
By Jaron Lanier
April 20, 2023
<https://www.newyorker.com/science/annals-of-artificial-intelligence/there-is-no-ai>

9

THE SAME:

YOU'RE IN INFOSEC.

**SOMEONE
IS GOING TO ASK YOU
TO MAKE SENSE OF
WHY THE COMPUTER IS DOING THAT.
AGAIN. STILL. ALWAYS.**

10

They'll ask if we can *trust it*.

They'll ask if it's *lying*.

They'll ask *how* it came up with
whatever the h*ck
it came up with.

11

YOU ALREADY KNOW ENOUGH

INFOSEC IS MOSTLY JUST ASKING, "HOW DOES THAT WORK, REALLY?"

LET'S DO THAT. RIGHT NOW.

12

ChatGPT and Large Language Models

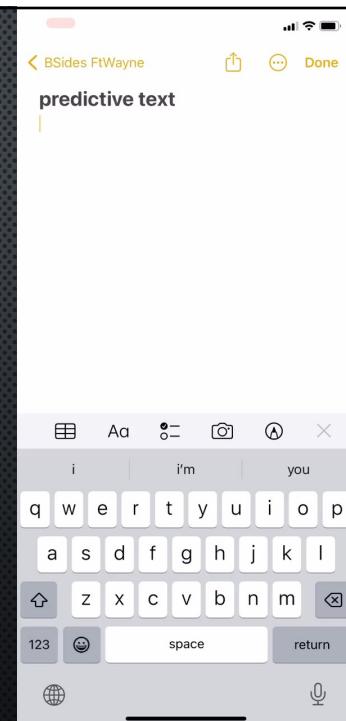
IT'S PREDICTIVE TEXT. THAT'S ALL IT IS.

"GIVEN THE WORDS SEEN SO FAR, WHAT'S THE NEXT MOST LIKELY WORD?"

ALL OF THAT IS BASED ON THE DATA USED TO TRAIN IT. "LARGE LANGUAGE"

WE COULD TALK ABOUT PROBABILITY DISTRIBUTIONS AND TOKENIZATION AND
DISCONTINUOUS PHASE SHIFTS (WHICH IS WHAT JUST HAPPENED WITH CHATGPT)

BUT WE DON'T NEED TO, SO LET'S NOT.



13

PREDICTIVE TEXT.
THAT'S ALL.
READY?

14

EXPLAIN THIS.

"references" means "citations"

15

HOW TO CITE A STUDY (THERE'S A FORMULA)

Hill, Linda A., Tarun Khanna, and Emily Stecker.

HCL Technologies (A).

Boston: Harvard Business School, 2008.

<https://www.hbs.edu/faculty/pages/item.aspx?num=34784>.

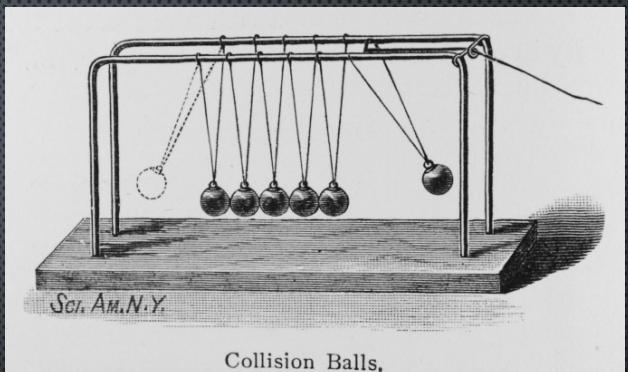
- **CHICAGO MANUAL OF STYLE**
- **(MIDWEST WRITING IS THE BEST WRITING)**
- AUTHOR LAST NAME, FIRST NAME. *TITLE OF THE CASE STUDY*. PUBLISHING CITY: PUBLISHING ORGANIZATION, PUBLICATION YEAR. URL.

When AI "makes up references" it's doing the only thing it can do.
It's just more obvious that there's no intrinsic meaning this time.

16

IT'S JUST PREDICTIVE TEXT.

- IT IS NOT ANSWERING QUESTIONS.
- IT IS NOT EVEN COMPOSING SENTENCES.
- IT IS ONLY GUESSING AT WHAT'S NEXT.
- ITS "ANSWERS" ARE NOT ANSWERS.
- THEY'RE MORE LIKE "REACTIONS"
 - AS IN NEWTON'S THIRD LAW OF MOTION: ACTION/REACTION
 - *THERE IS NO INTELLIGENCE IN A.I.*



17

intelligence noun

in·tel·li·gence (in-tel-i-jəns) (t)s

Synonyms of *intelligence* >

- 1 a (1) : the ability to learn or understand or to deal with new or trying situations : **REASON**
 - also : the skilled use of reason* → *the power of comprehending*
 - (2) : the ability to apply knowledge to manipulate one's environment or to think abstractly as measured by objective criteria (such as tests)
- c : mental acuteness : **SHREWDNESS**
- b **Christian Science** : the basic eternal quality of divine Mind

<https://www.merriam-webster.com/dictionary/intelligence>

18

GENERATIVE A.I. WILL NOT TAKE YOUR INFOSEC JOB.

- THERE IS NO LYING BECAUSE THERE IS NO *INTENT*.
- AND WITH AN LLM, THERE CANNOT BE.
- THIS THING IS NOT ... CANNOT BE ... YOUR ENEMY.
- **IT WILL CHANGE YOUR JOB.**
 - AND YOU HAVE SOME INFLUENCE OVER HOW.
 - ESPECIALLY RIGHT NOW, WHILE IT'S NEW.

19



IT'S NOT THE THING

It's How You Use The Thing.

 See more Design Ideas

Powered by Office intelligent services

20

AMAZON, TO THE SHOCK OF NOBODY...

Amazon Throws Down Gauntlet in Artificial Intelligence Market; Develops AI-Based Ads

Amazon plans to build AI tools to create visuals for advertising mediums on its platform.

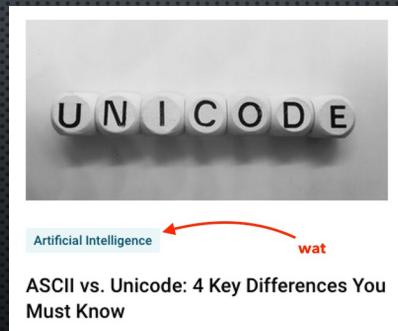


Anuj Mudaliar Assistant Editor - Tech, SWZD

May 9, 2023

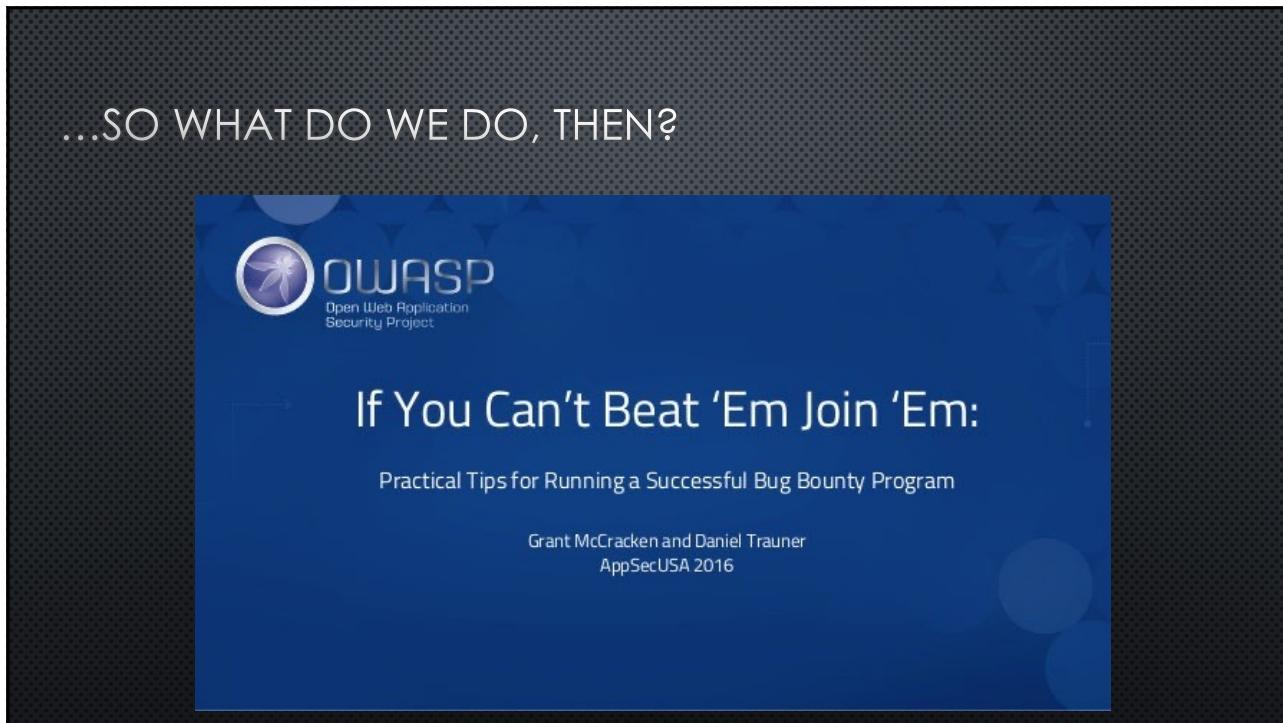
21

UNICODE IS NOT AI.
ASCII IS DEFINITELY NOT AI.
THE DIFFERENCES BETWEEN THEM?
ALSO NOT A.I.

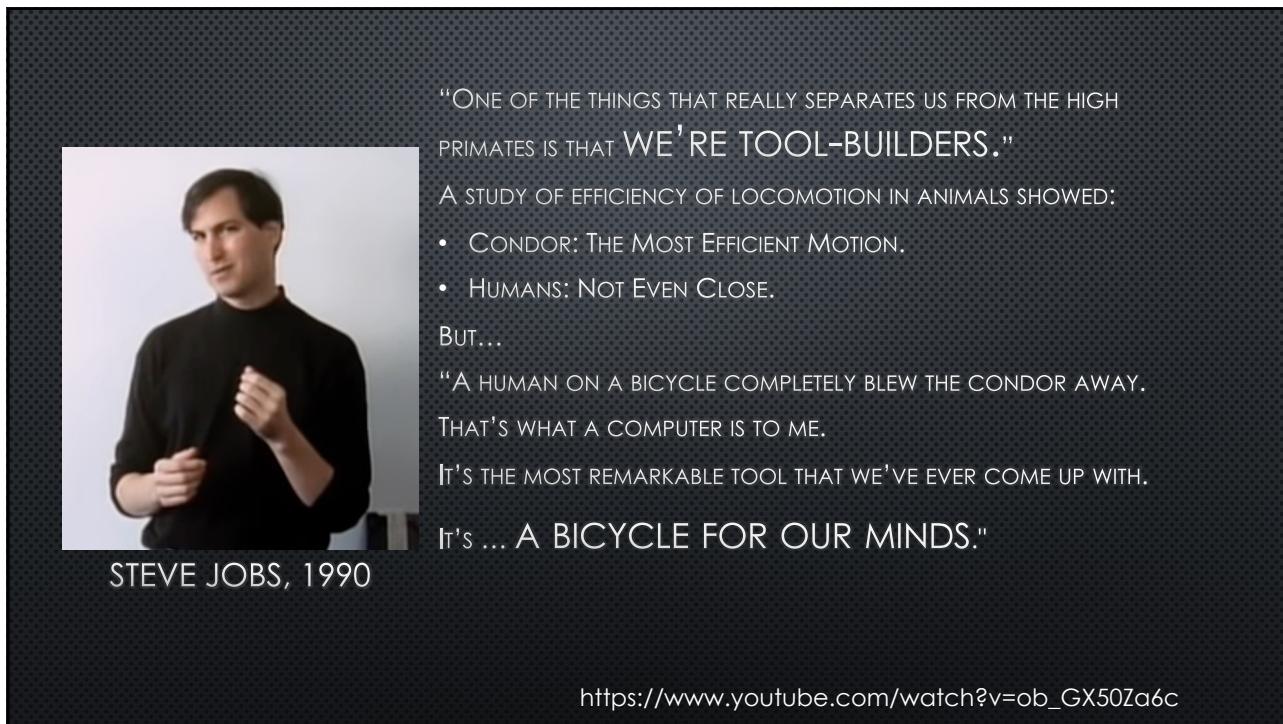


<https://www.spiceworks.com/tech/artificial-intelligence/articles/ascii-vs-unicode/>

22



23



24

PLEASE UNDERSTAND:
THAT WAS NOT YOUR AVERAGE BIKE, OR CYCLIST.

IF YOU'RE NOT USING YOUR COMPUTER THIS WAY*, MAYBE IT'S TIME TO START.

* DELIBERATELY. SKILLFULLY. INTENTIONALLY.

TO DO THINGS YOU CAN'T OR WON'T DO "BY HAND"

TO DO THINGS BEYOND THE OBVIOUS AND STRAIGHTFORWARD.

25

WHERE ARE THESE BICYCLES?

- CHATGPT, OBVS
- KHANMIGO (KHAN ACADEMY)
 - IN PILOT PHASE
- PULUMI AI (INFRA... AS CODE)
- CODY (SOURCEGRAPH)
- GITHUB CO-PILOT (\$)

 I want an Ubuntu server that I can access over SSH and by GUI

TypeScript

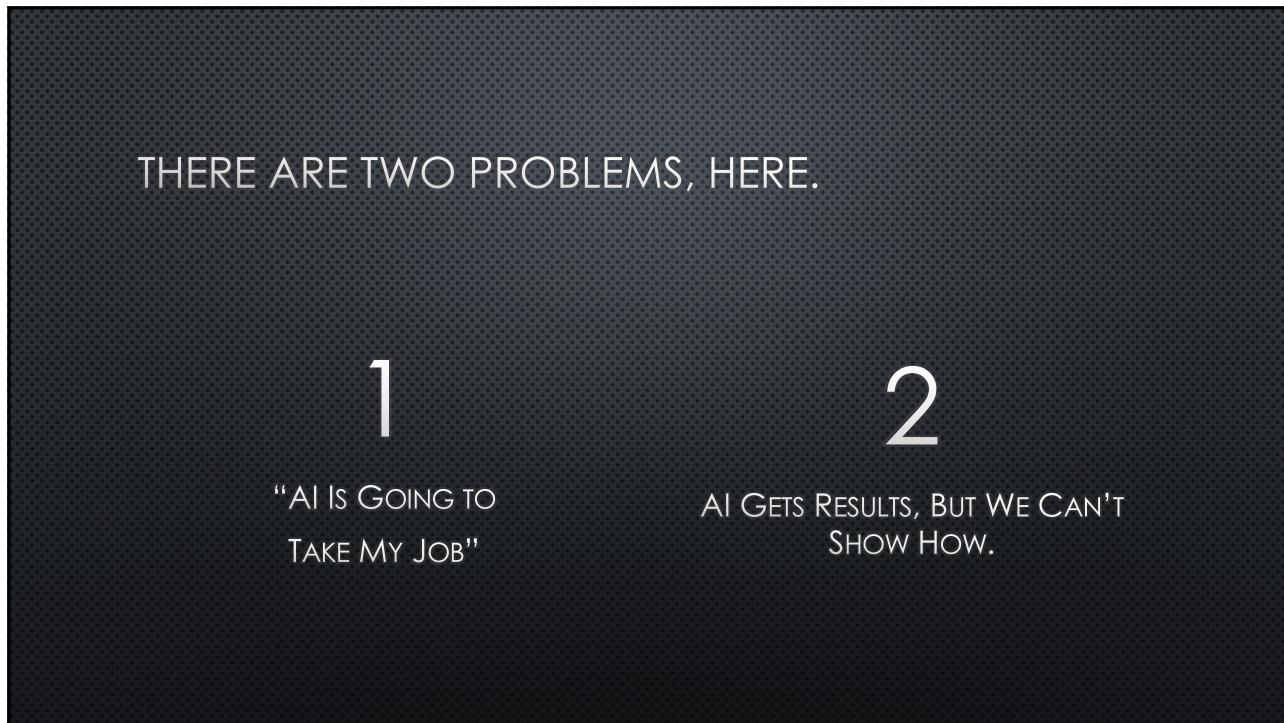
To accomplish your goal, I recommend provisioning an EC2 instance on AWS using the `aws.ec2.Instance` resource. In the Pulumi TypeScript program below, I've set up an EC2 instance with an Ubuntu AMI and a security group allowing SSH and GUI access. The GUI access is provided by VNC, which uses TCP port 5901.

```
import * as pulumi from "@pulumi/pulumi";
import * as aws from "@pulumi/aws";

const vpc = aws.ec2.getVpc({ default: true });

const sshAndGuiSecurityGroup = new aws.ec2.SecurityGroup("sshAndGuiSecurityGroup");
  ingress: [
    {
      fromPort: 22,
      toPort: 22,
```

26



27

NUMBER TWO FIRST:
DETAILS ASIDE, THERE'S
NOTHING* NEW HERE.

NOBODY HAS KNOWN WHAT THEY'RE DOING
FOR A LONG, LONG TIME, NOW.

HUMANITY WON'T ABANDON AI — OR ANYTHING
ELSE — JUST BECAUSE WE DON'T REALLY KNOW
HOW IT DOES WHAT IT DOES.

The Register

How one developer just broke Node, Babel and thousands of projects in 11 lines of JavaScript

Code pulled from NPM – which everyone was using

Chris Williams, Editor in Chief | Wed 23 Mar 2016 | 01:24 UTC

UPDATED Programmers were left staring at broken builds and failed installations on Tuesday after someone toppled the Jenga tower of JavaScript.

A couple of hours ago, Azer Koçulu unpublished more than 250 of his modules from [NPM](#), which is a popular package manager used by JavaScript projects to install dependencies.

*Well, it is worse with AI, but it's not a new kind of problem.

28

DON'T LET IT TAKE YOUR JOB.
LET IT MAKE YOU BETTER AT YOUR JOB.

IGNORING IT IS THE ONLY WRONG ANSWER.

29

REMINDER: THIS IS NOT NEW.
WAF AUTOCONFIGURATION IS AI.
(OK, IT'S ML ... JUST PLAY ALONG)

- **MONITOR MODE:** WATCH “NORMAL” TRAFFIC – TAKE NOTES.
- **ALERT MODE:** USE WHAT YOU’VE LEARNED – HIGHLIGHT ANOMALIES.
- **BLOCKING MODE:** USE WHAT YOU’VE LEARNED – BLOCK ATTACKS (I.E., “ANOMALIES”)

30

A.I. IS A TOOL. IT'S NOT USEFUL WITHOUT HUMANS.

- SOMEONE HAD TO IDENTIFY THE PROBLEM (THIS IS A HUMAN)
- SOMEONE HAD TO FIND A SOLUTION (THIS IS A HUMAN, USING TOOLS. AI IS A TOOL.)
- SOMEONE HAS TO IMPLEMENT IT (THIS IS A HUMAN)
- SOMEONE HAS TO DEBUG IT, MAINTAIN IT, MODIFY IT, BE RESPONSIBLE FOR IT
 - YES: HUMANS, AGAIN.
 - ALWAYS WITH THE HUMANS...

31

YOUR ROLE IN ALL OF THIS
SAME AS IT EVER WAS

32

USE THE TOOLS.
LEARN HOW THEY WORK.
LEARN HOW THEY FAIL.
SHARE WHAT YOU LEARN.

WATCH WHAT OTHERS DO.
ADOPT THE GOOD.
AVOID THE BAD.

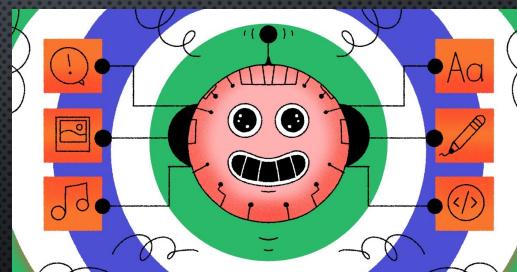
FIND A GOOD NON-DIGITAL HOBBY.

33

A USEFUL THOUGHT:
AI ISN'T THE APP. IT'S THE UI.
ISAAC LYMAN, STACK OVERFLOW BLOG

THE IDEAL USE OF AI:
NOT A DECISION-MAKER OR UNSUPERVISED AGENT
TUCKED AWAY FROM THE END USER, BUT

AN INTERFACE BETWEEN
HUMANS AND MACHINES.



<https://stackoverflow.blog/2023/05/01/ai-isnt-the-app-its-the-ui/>

34

IF YOU
REMEMBER
NOTHING ELSE,
REMEMBER THIS:

35

YOU ARE NOT
AN IMPOSTER
IF YOU ARE
DOING THE WORK.

IT IS NO SYNDROME
TO RECOGNIZE
YOUR LIMITS.

**You're Not an Imposter.
You're Actually Pretty
Amazing.**

by Kess Eruteya

January 03, 2022



HBR Staff/Getty Images/master1305

<https://hbr.org/2022/01/youre-not-an-impostor-youre-actually-pretty-amazing>

36

“

THERE IS NEVER ENOUGH TIME.
THANK YOU FOR YOURS.

”

--DAN GEER

(ALSO BBKING)

SLIDES AND LINKS AT [HTTPS://GITHUB.COM/BBHACKING/BSIDESFTWAYNE](https://github.com/BBHACKING/BSIDESFTWAYNE)