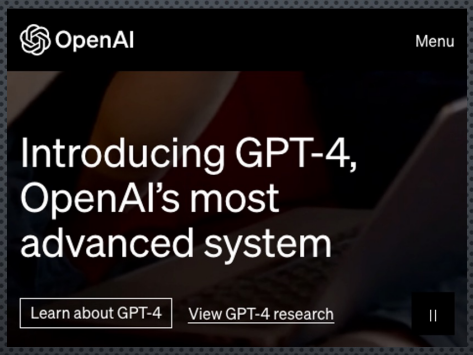
ARTIFICIAL INTELLIGENCE
AND THE RISE OF THE HUMANS

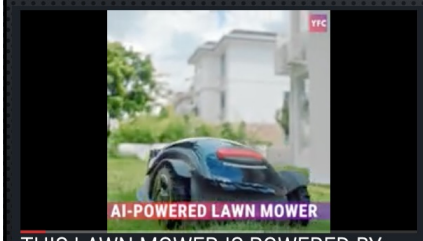
BB King
Pentester @ Black Hills Infosec
Instructor @ AntiSyphon Training
@BBhacKing in other places
https://github.com/BBhacKing/ ← These Slides and Further Reading

1

AI IS HERE.
HI.



Generative
Pre-trained
Transformer



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

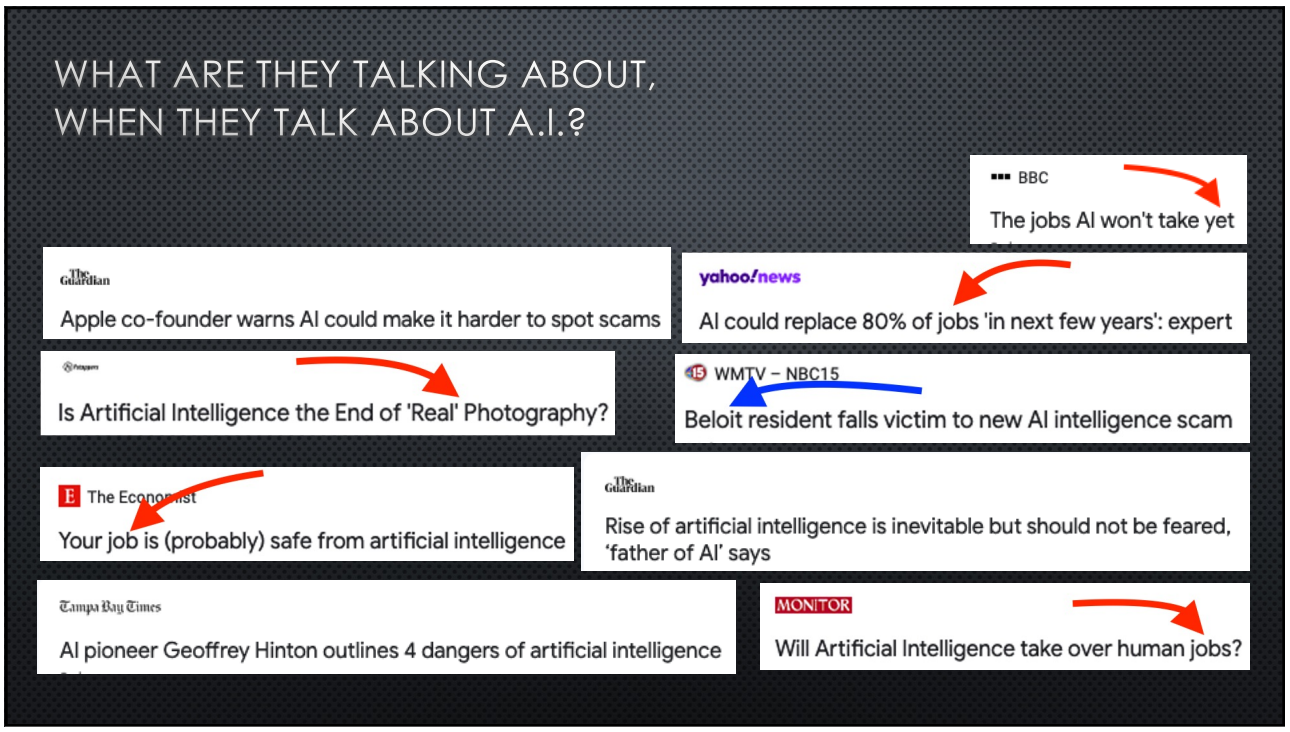
TECH / SMART HOME

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

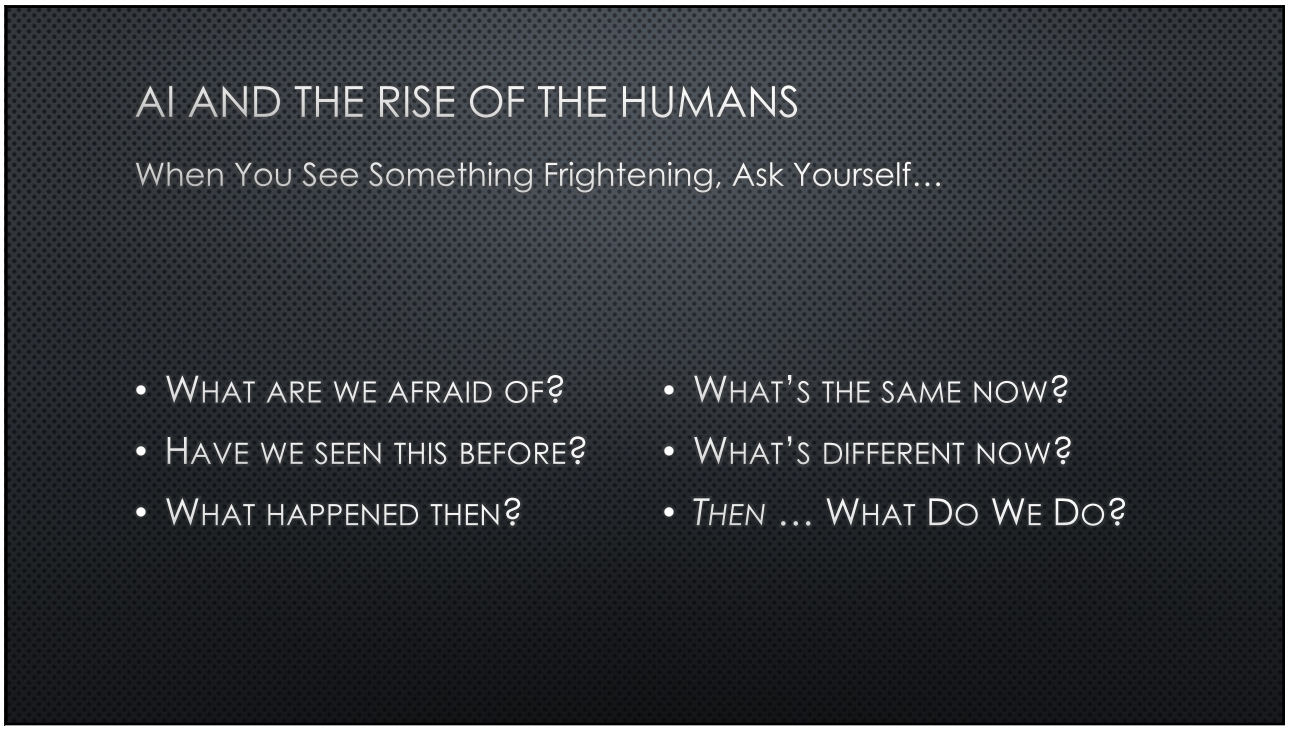
The Columbus Dispatch

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

2

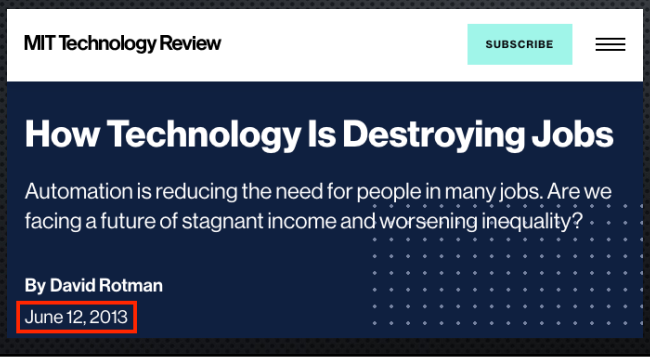

WHAT ARE THEY TALKING ABOUT, WHEN THEY TALK ABOUT A.I.?
BBC
The jobs AI won't take yet
The Guardian
Apple co-founder warns AI could make it harder to spot scams
yahoo!news
AI could replace 80% of jobs 'in next few years': expert
Is Artificial Intelligence the End of 'Real' Photography?
WMTV – NBC15
Beloit resident falls victim to new AI intelligence scam
The Economist
Your job is (probably) safe from artificial intelligence
The Guardian
Rise of artificial intelligence is inevitable but should not be feared, 'father of AI' says
Tampa Bay Times
AI pioneer Geoffrey Hinton outlines 4 dangers of artificial intelligence
MONITOR
Will Artificial Intelligence take over human jobs?

3


AI AND THE RISE OF THE HUMANS
When You See Something Frightening, Ask Yourself…
• WHAT ARE WE AFRAID OF?
• HAVE WE SEEN THIS BEFORE?
• WHAT HAPPENED THEN?
• WHAT'S THE SAME NOW?
• WHAT'S DIFFERENT NOW?
• THEN … WHAT DO WE DO?

4

HAVE WE BEEN AFRAID OF THIS BEFORE?



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 SUBSCRIBE

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

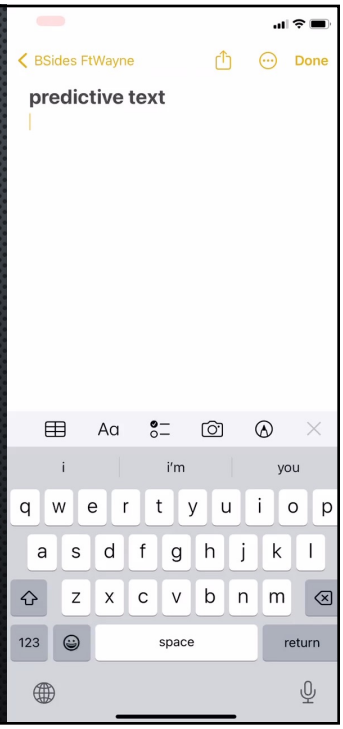
It's PREDICTIVE TEXT. That's ALL IT IS.

"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)

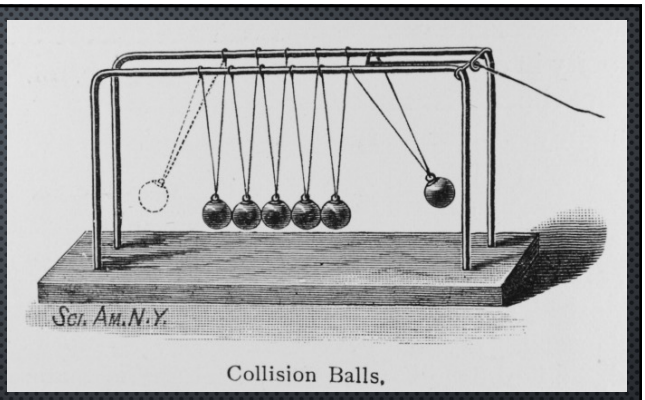
- **CHICAGO MANUAL OF STYLE**
- **(MIDWEST WRITING IS THE BEST WRITING)**
- AUTHOR LAST NAME, FIRST NAME. *TITLE OF THE CASE STUDY*. PUBLISHING CITY: PUBLISHING ORGANIZATION, PUBLICATION YEAR. URL.

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.

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.



Collision Balls.

- 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-ˈte-lə-jən(t)s

Synonyms of *intelligence* ›

to grasp the meaning of

1 **a** (1) : the ability to learn or understand or to deal with new or trying situations : REASON

the power of comprehending

also : the skilled use of reason

(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

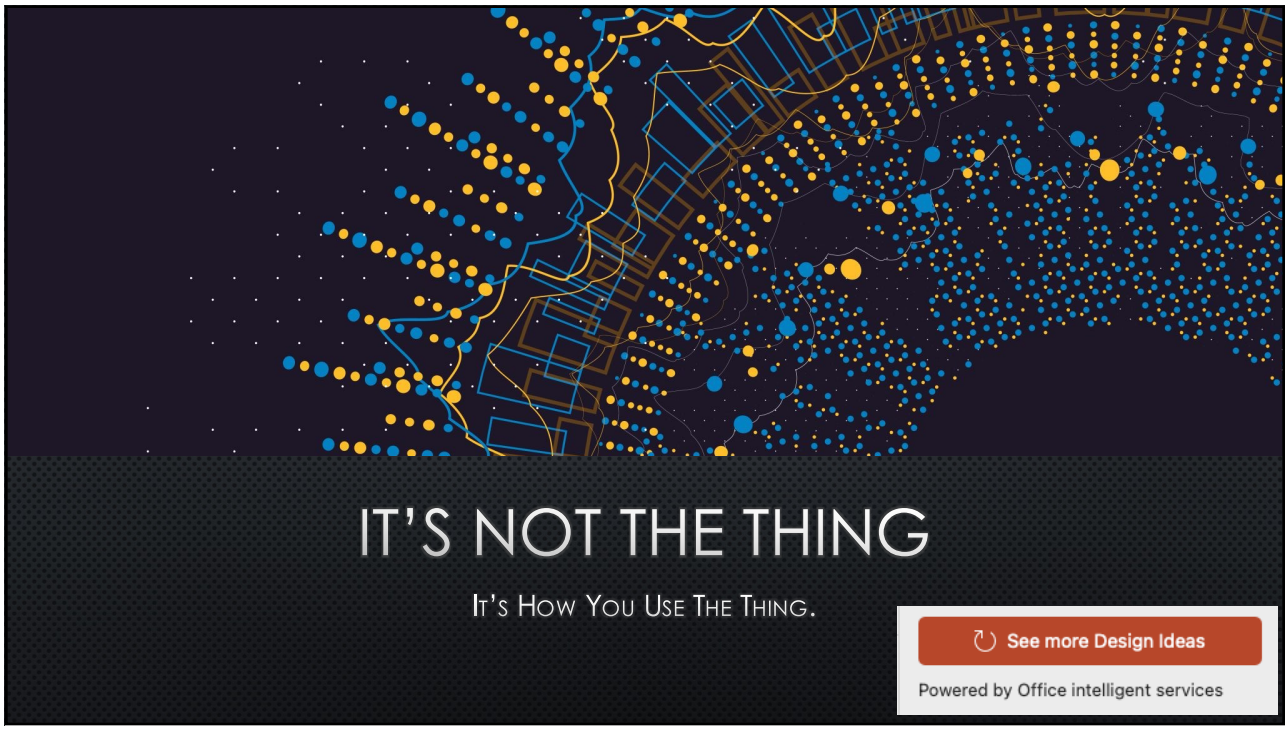
https://www.merriam-webster.com/dictionary/intelligence

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



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.

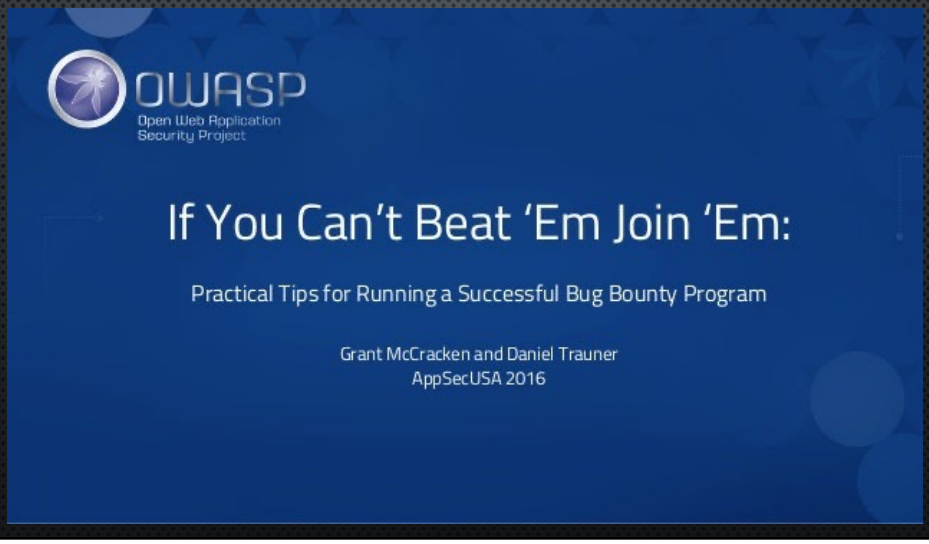
Artificial Intelligence ← wat

ASCII vs. Unicode: 4 Key Differences You Must Know

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

22

…SO WHAT DO WE DO, THEN?



23

STEVE JOBS, 1990

"ONE OF THE THINGS THAT REALLY SEPARATES US FROM THE HIGH PRIMATES IS THAT WE'RE TOOL-BUILDERS."

A STUDY OF EFFICIENCY OF LOCOMOTION IN ANIMALS SHOWED:

- CONDOR: THE MOST EFFICIENT MOTION.
- HUMANS: NOT EVEN CLOSE.

BUT…

"A HUMAN ON A BICYCLE COMPLETELY BLEW THE CONDOR AWAY.

THAT'S WHAT A COMPUTER IS TO ME.

IT'S THE MOST REMARKABLE TOOL THAT WE'VE EVER COME UP WITH.

IT'S … A BICYCLE FOR OUR MINDS."

https://www.youtube.com/watch?v=ob_GX50Za6c

24

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

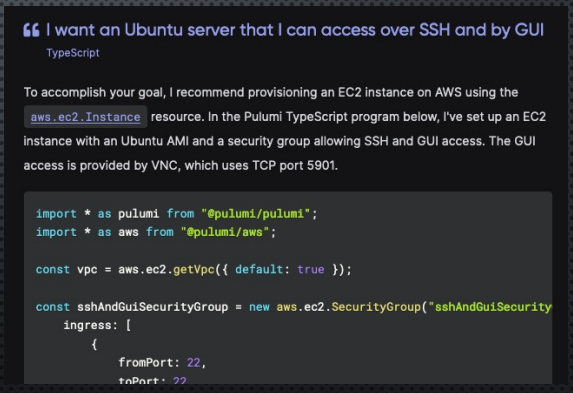
IF YOU'RE NOT USING YOUR COMPUTER THIS WAY*, MAYBE IT'S TIME TO START.

* 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 ($)



26

THERE ARE TWO PROBLEMS, HERE.

1

"AI IS GOING TO TAKE MY JOB"

2

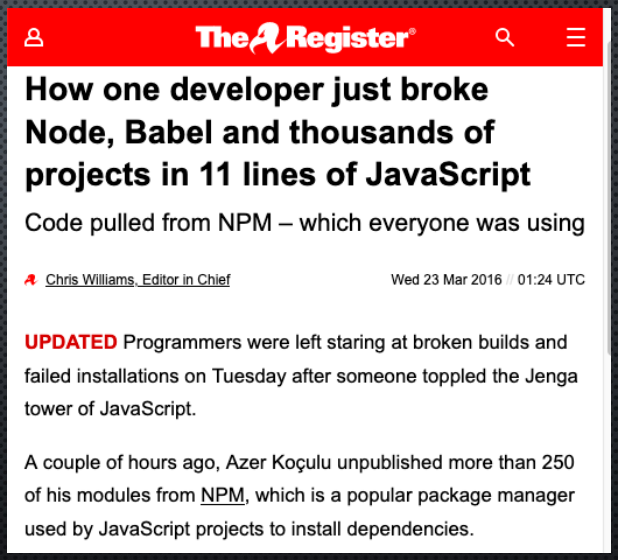
AI GETS RESULTS, BUT WE CAN'T SHOW HOW.

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.

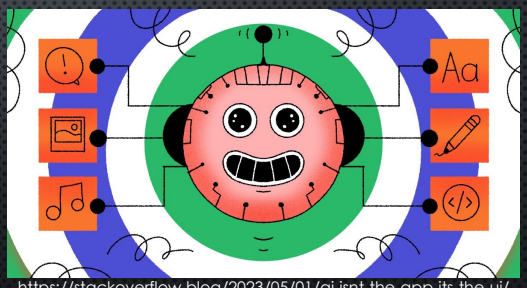
33

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

THE IDEAL USE OF AI:

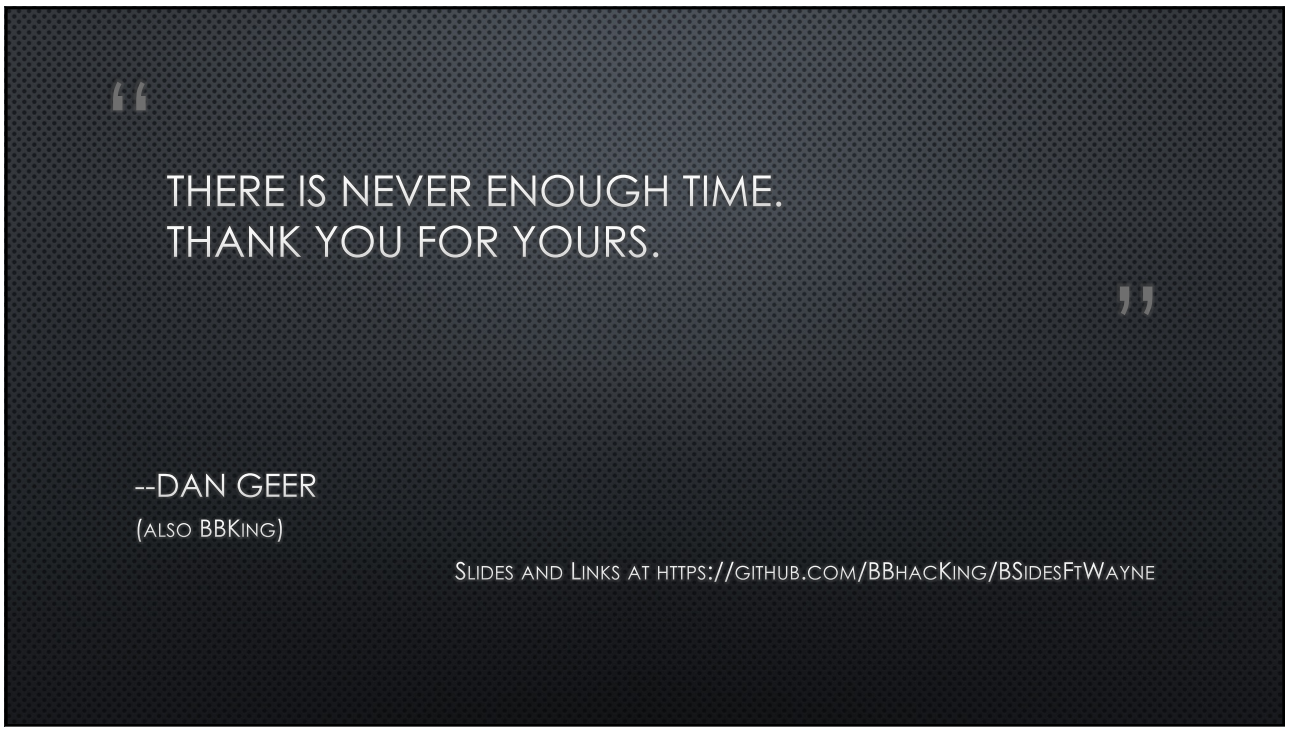
NOT A DECISION-MAKER OR UNSUPERVISED AGENT TUCKED AWAY FROM THE END USER, BUT

AN INTERFACE BETWEEN HUMANS AND MACHINES.



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

34


“
THERE IS NEVER ENOUGH TIME.
THANK YOU FOR YOURS.
”
--DAN GEER
(ALSO BBKING)
SLIDES AND LINKS AT HTTPS://GITHUB.COM/BBHACKING/BSIDESFTWAYNE

35