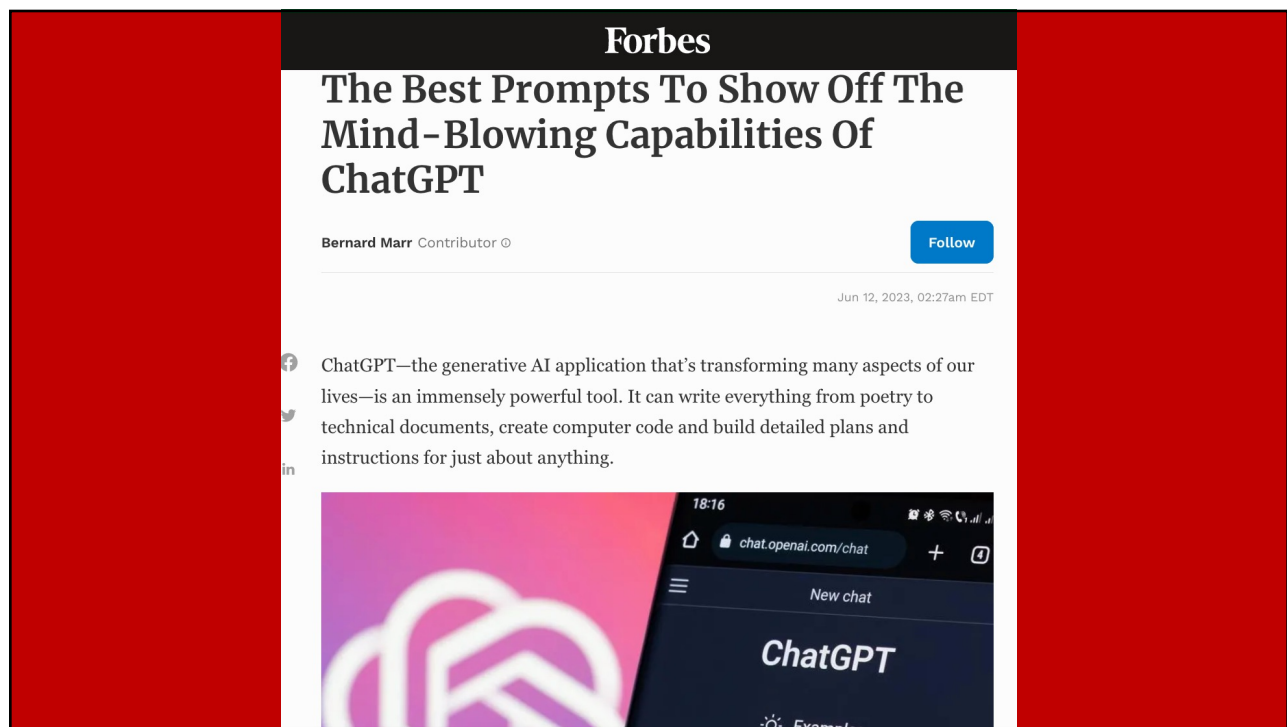




1



2

New AI Tools List

Created by Hasan Toor from Twitter

Productivity Tools <ol style="list-style-type: none"> 1. TLDV 2. Taskade 3. Notion AI 4. Microsoft Bing 5. Google Bard 	GPT-4 Free Tools <ol style="list-style-type: none"> 1. ForeFront 2. Merlin 3. WNR AI 4. ChatABC 5. Huggingface 	Academic AI Tools <ol style="list-style-type: none"> 1. Paperpal AI 2. Monic AI 3. ChartGPT 4. Trinka 5. Scholarcy
Sales AI Tools <ol style="list-style-type: none"> 1. Lavender 2. Regie 3. Warmer 4. Twain 5. Octane 	Coding AI Tools <ol style="list-style-type: none"> 1. 10web 2. Uncode 3. Dora AI 4. Durable AI 5. Replit 	Research AI Tools <ol style="list-style-type: none"> 1. Scholarcy 2. Consensus 3. Writesonic 4. Trinka 5. Paperpal AI
Chatbots AI Tools <ol style="list-style-type: none"> 1. Yatterplus 2. Typewise 3. Cohere 4. Quickchat 5. Kaizan 	Logo Generator Tools <ol style="list-style-type: none"> 1. Looka 2. Namecheap 3. Logo AI 4. StockIMG 5. BrandMark 	Text to Speech Tools <ol style="list-style-type: none"> 1. Panopreter 2. Speechelo 3. Synthesys 4. Speechify 5. Murf
Video Generators Tools <ol style="list-style-type: none"> 1. Pictory 2. Synthesia 3. InVideo 4. Veed.io 5. Colossyan 	AI Art Generators <ol style="list-style-type: none"> 1. GetIMG 2. Shutterstock 3. NightCafe 4. Artbreeder 5. Stablecog 	Startup AI Tools <ol style="list-style-type: none"> 1. Speak AI 2. AISEO 3. Lumen5 4. Spellbook 5. Olivia

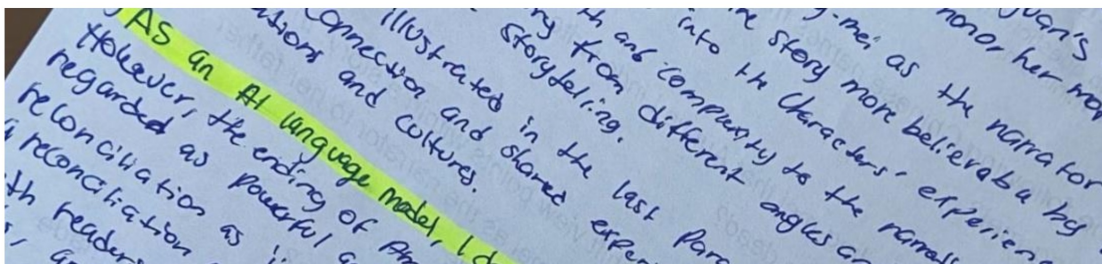
3

Class 7 Student Uses ChatGPT To Do English Homework. Gets Caught Because Of This Line

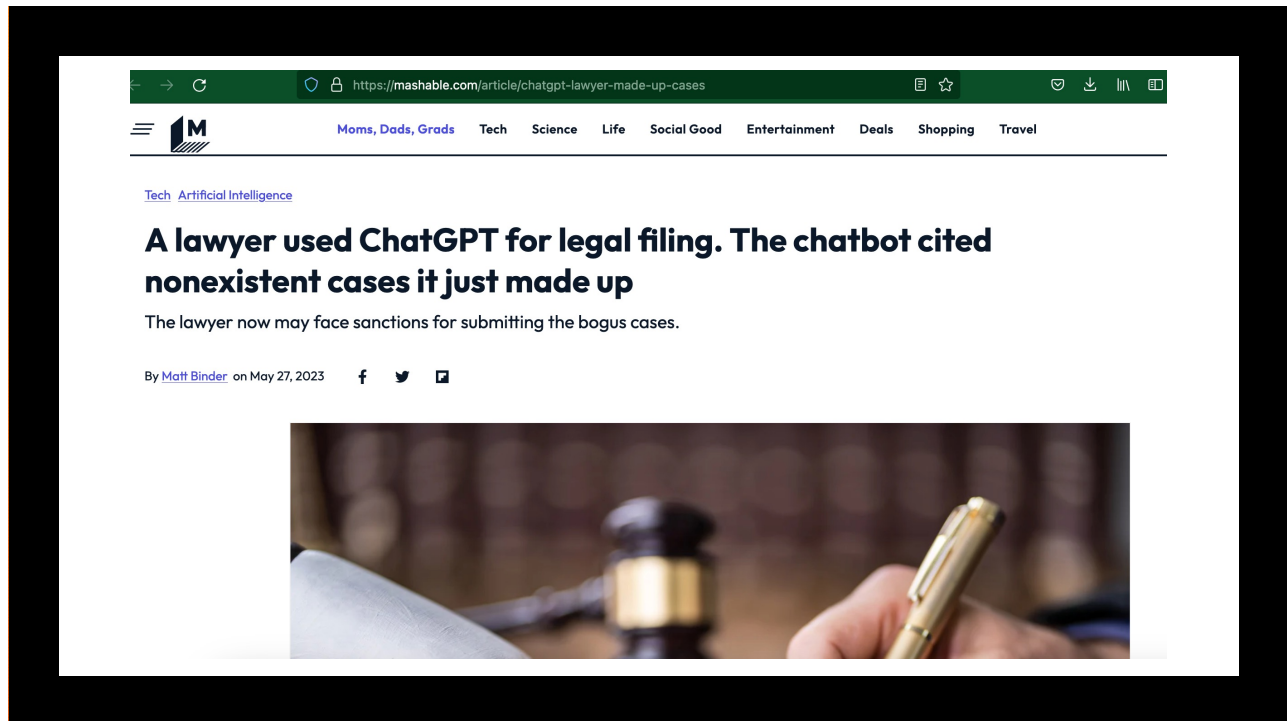


Isha Sharma

Updated on Jun 08, 2023, 01:57 IST - 8 min read



4




5

What about Cyber Criminals?

How might they use generative AI to up their game?

1. What are potential scenarios where generative AI poses significant cybersecurity risks?
2. What are the implications for traditional awareness and training drives?
3. How should organisations respond?



6

Scenario 1

- A hacker uses ChatGPT to generate a personalized spear phishing message
 - trained using your company's marketing material
 - plus phishing messages that were successful in the past

7

Scenario 2

- An AI bot calls an accounts-payable employee, in a (deep fake) voice that sounds like the boss
- After exchanging some pleasantries, the "boss" asks the employee to transfer thousands of dollars to an account to "pay an invoice."

8

Scenario 3

- Hackers use AI to realistically “poison” the information in a system, creating a valuable stock portfolio
- they can cash out before the deceit is discovered

9

What do these teach us?

- Up to now, most attacks used relatively unsophisticated high-volume approaches
 - Scattergun approach
 - Hoping that sheer volume will catch some people

10

Zombies ...

millions of persistent but brainless threats that succeed only when one or two happen upon a weak spot in the defensive barrier



11

Sometimes ...

- most sophisticated threats
- lower-volume attacks that require actual human involvement
 - E.g., Stuxnet



12

Now



13

What does this mean for cybersecurity?

- In particular, what does this mean for the humans in the socio-technical system?

14

Moving from **Human as Problem** to **Human as Solution** in Cyber Security

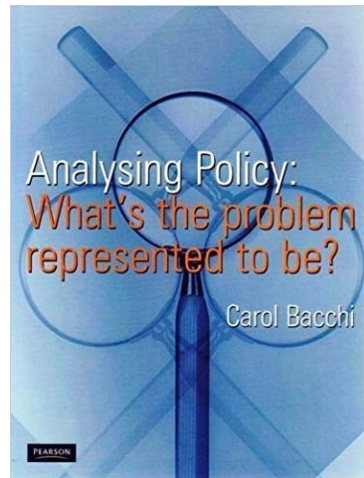


15

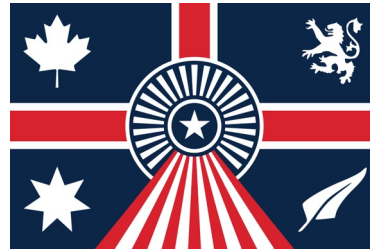
What's the
Problem in Cyber
Security?



16



17



18

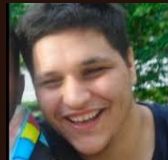
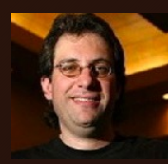
Top 5 Cybersecurity Companies (eSecurity Planet)

- Cisco
- Symantec
- Palo Alto Networks
- Check Point
- Microsoft



19

Published Hacker Statements

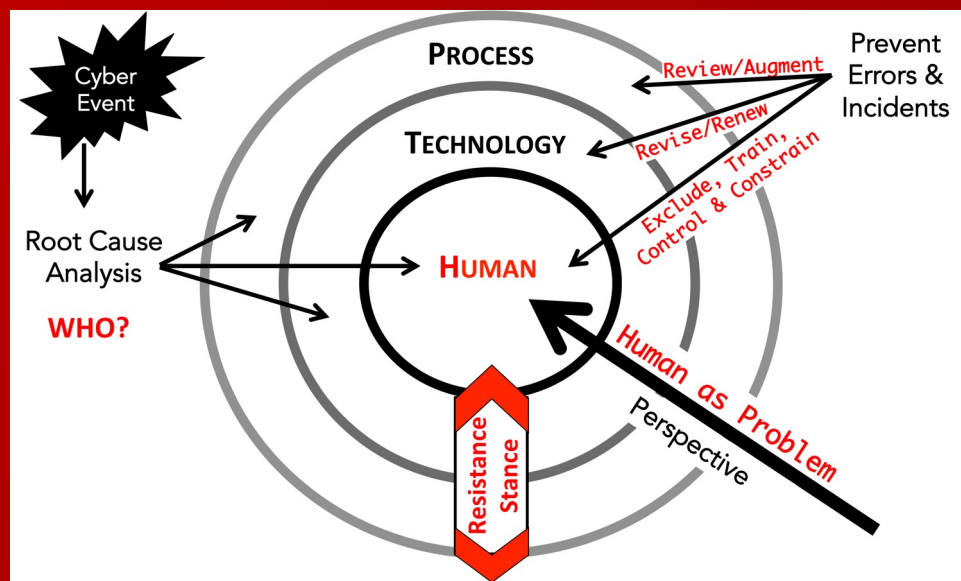


20

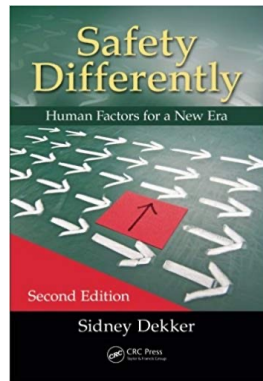
What's the Problem in Cyber Security?



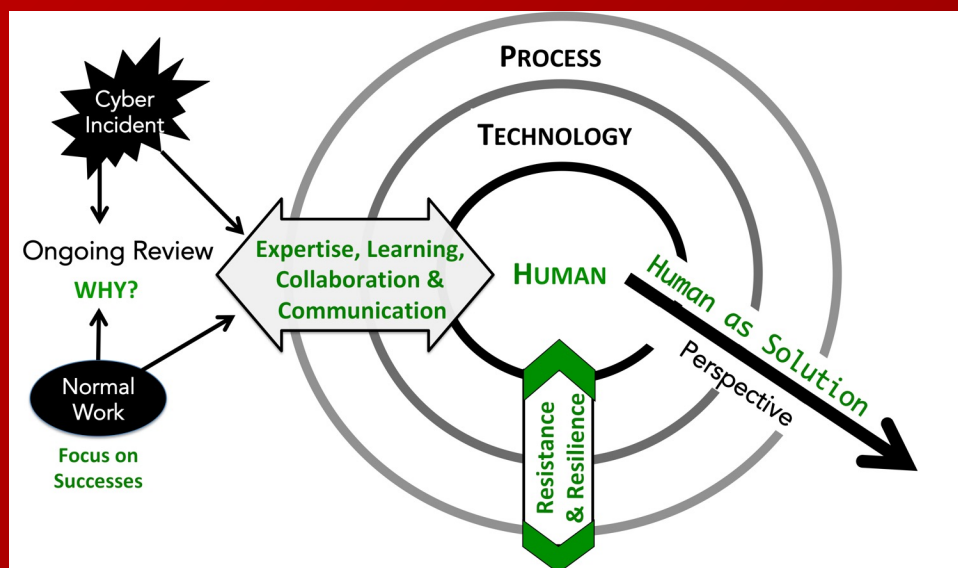
21



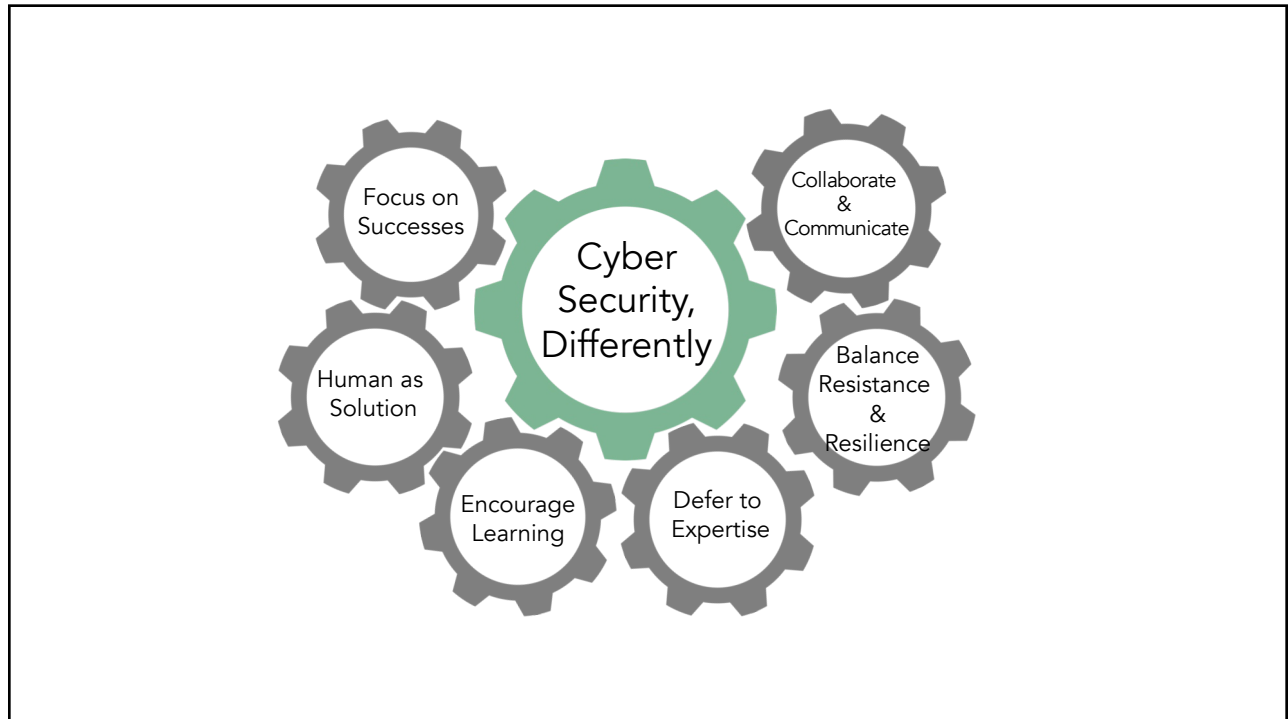
22



23



24



25

karen.renaud@strath.ac.uk



26