Cybersecurity in an AI driven World

CONNECTWISE®

Threat Landscape

CONNECTWISE®

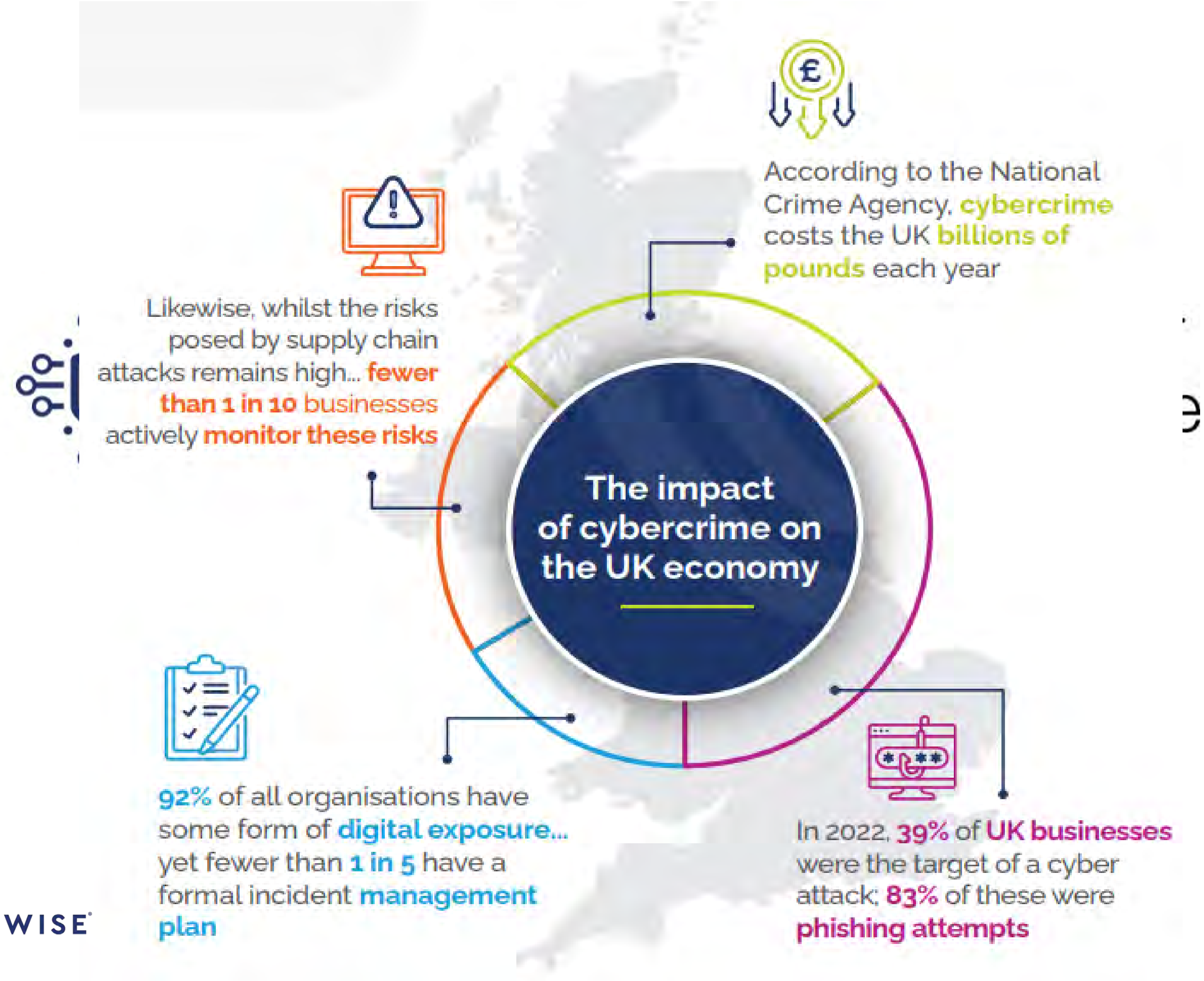
The Dream

Your business on the internet

CONNECTWISE

the reality is ...

How at risk is your business?



The impact of cybercrime on the UK economy

According to the National Crime Agency, **cybercrime** costs the UK **billions of pounds** each year

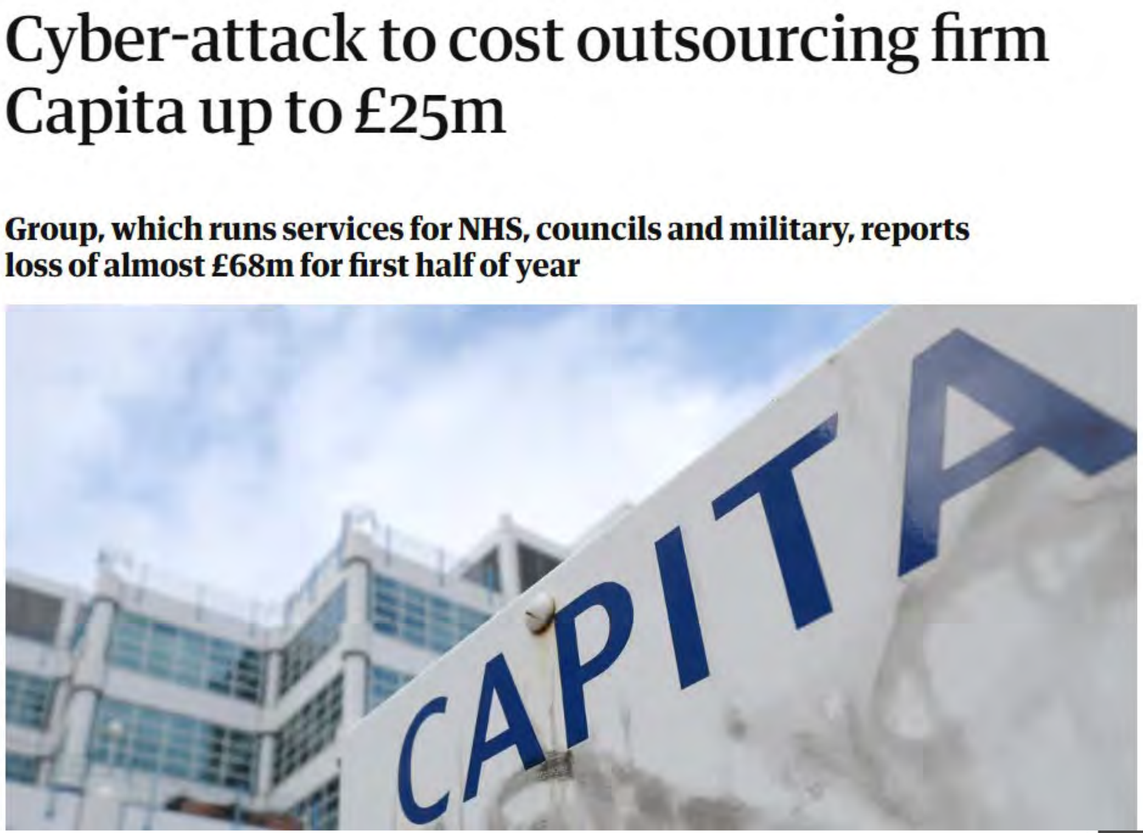
In 2022, **39%** of **UK businesses** were the target of a cyber attack; **83%** of these were **phishing attempts**

92% of all organisations have some form of **digital exposure...** yet fewer than **1 in 5** have a formal incident **management plan**

Likewise, whilst the risks posed by supply chain attacks remains high... **fewer than 1 in 10** businesses actively **monitor these risks**

CONNECTWISE

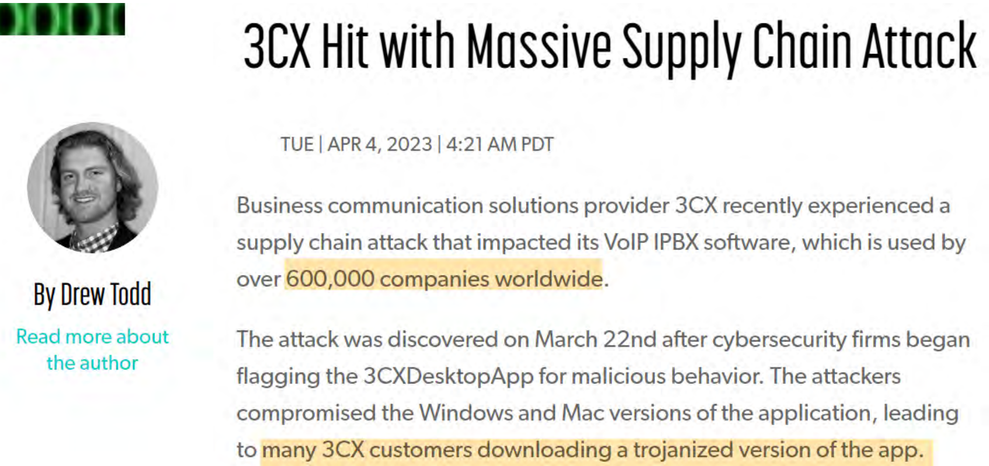
What if the threat actors succeed?



Cyber-attack to cost outsourcing firm Capita up to £25m

Group, which runs services for NHS, councils and military, reports loss of almost £68m for first half of year

l cyber attack
nked ransom
nding payment in cryptocur
n centre.
porter
os.uk



3CX Hit with Massive Supply Chain Attack

By Drew Todd

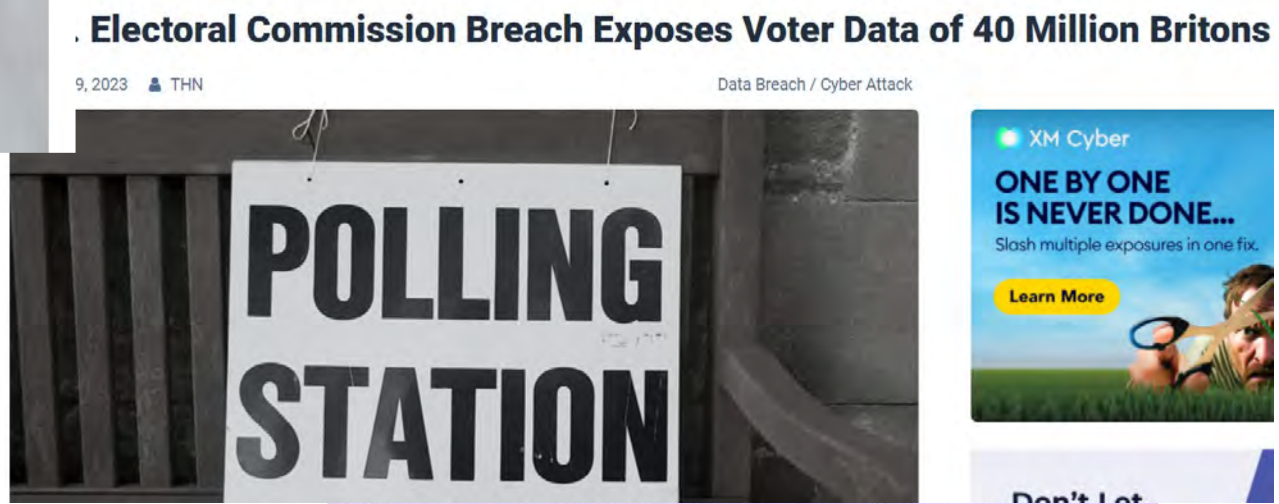
Read more about the author

TUE | APR 4, 2023 | 4:21 AM PDT

Business communication solutions provider 3CX recently experienced a supply chain attack that impacted its VoIP IPBX software, which is used by over 600,000 companies worldwide.

The attack was discovered on March 22nd after cybersecurity firms began flagging the 3CXDesktopApp for malicious behavior. The attackers compromised the Windows and Mac versions of the application, leading to many 3CX customers downloading a trojanized version of the app.

Client data exfiltrated in Advanced NHS cyber attack



. Electoral Commission Breach Exposes Voter Data of 40 Million Britons

9, 2023 THN Data Breach / Cyber Attack

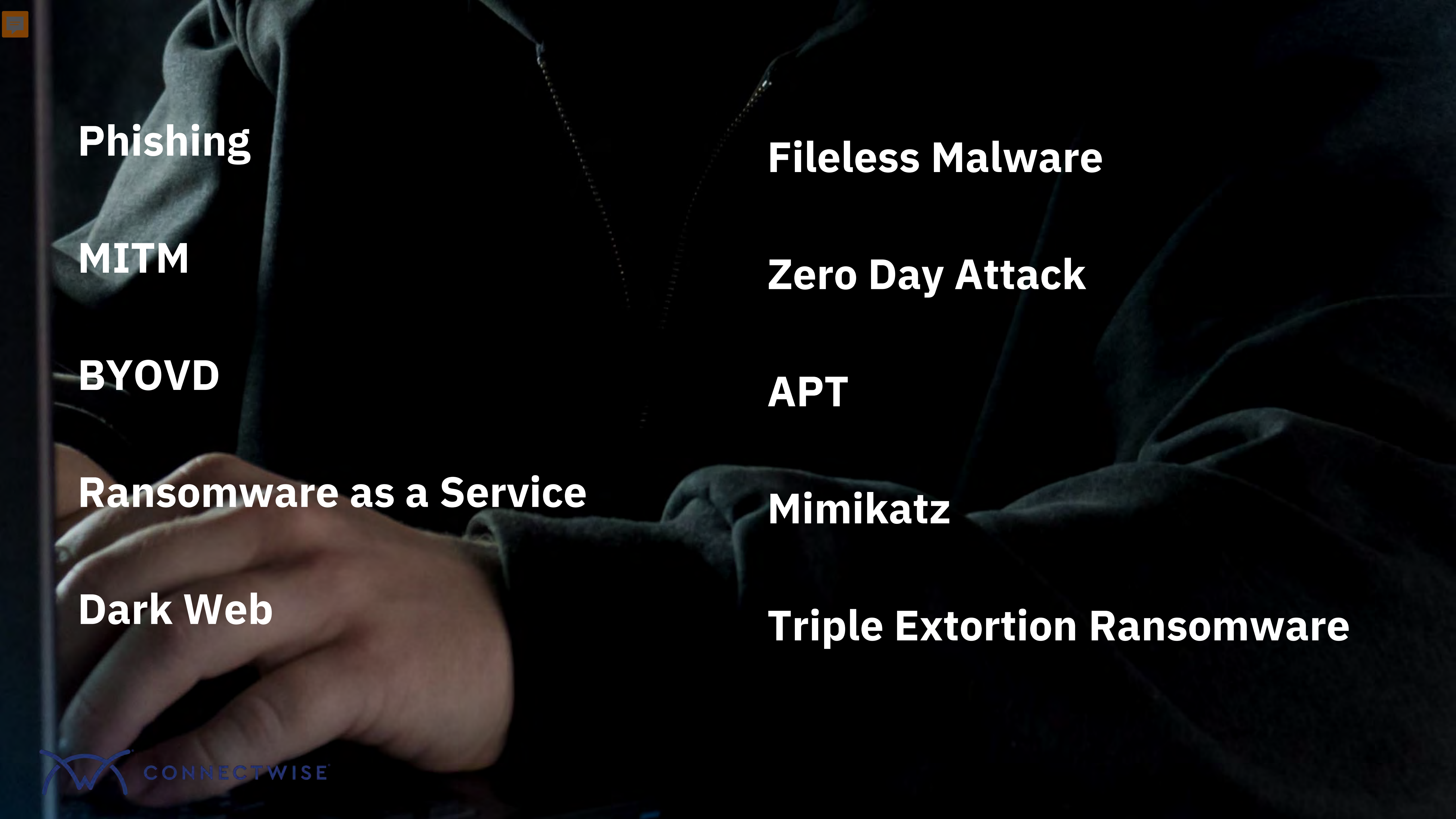
XM Cyber
ONE BY ONE IS NEVER DONE...
Slash multiple exposures in one fix.
Learn More
Don't Let

Health and care software supplier Advanced has confirmed that client data was accessed and extracted by hackers during a cyber incident in August 2022.

CONNECTWISE

- Recession
- Interest Rates
- Supply Chain
- Loss of Key Employees
- Labour Shortage
- Cheap Foreign Products
- Climate/Environment
- Reputational Damage

CONNECTWISE



Phishing

MITM

BYOVD

Ransomware as a Service

Dark Web

Fileless Malware

Zero Day Attack

APT

Mimikatz

Triple Extortion Ransomware

Question time!

A ________ is a cyber attack targeting a software vulnerability which is unknown to the software vendor and the antivirus vendors.

a) Ransomware attack

b) Stealth attack

c) Zero-day attack ✓

d) Phishing attack

According to the National Cyber Resilience Centre 2022 report, what percentage of UK businesses were a target of cyber attacks?

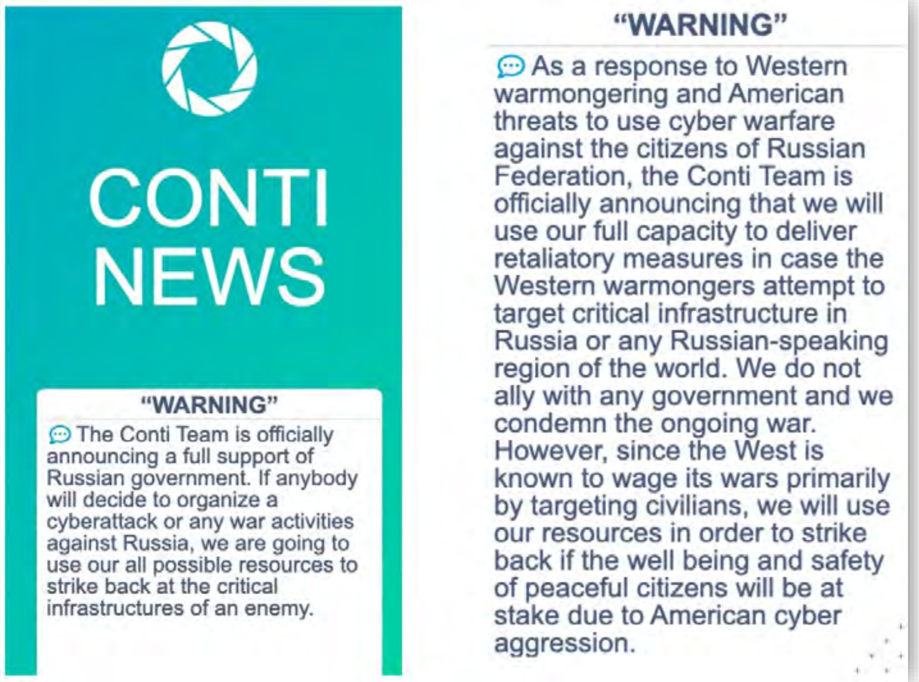
a) 15%

b) 39% ✓

c) 55%

d) 70%

Hostile Nation States



CONTI NEWS

"WARNING"

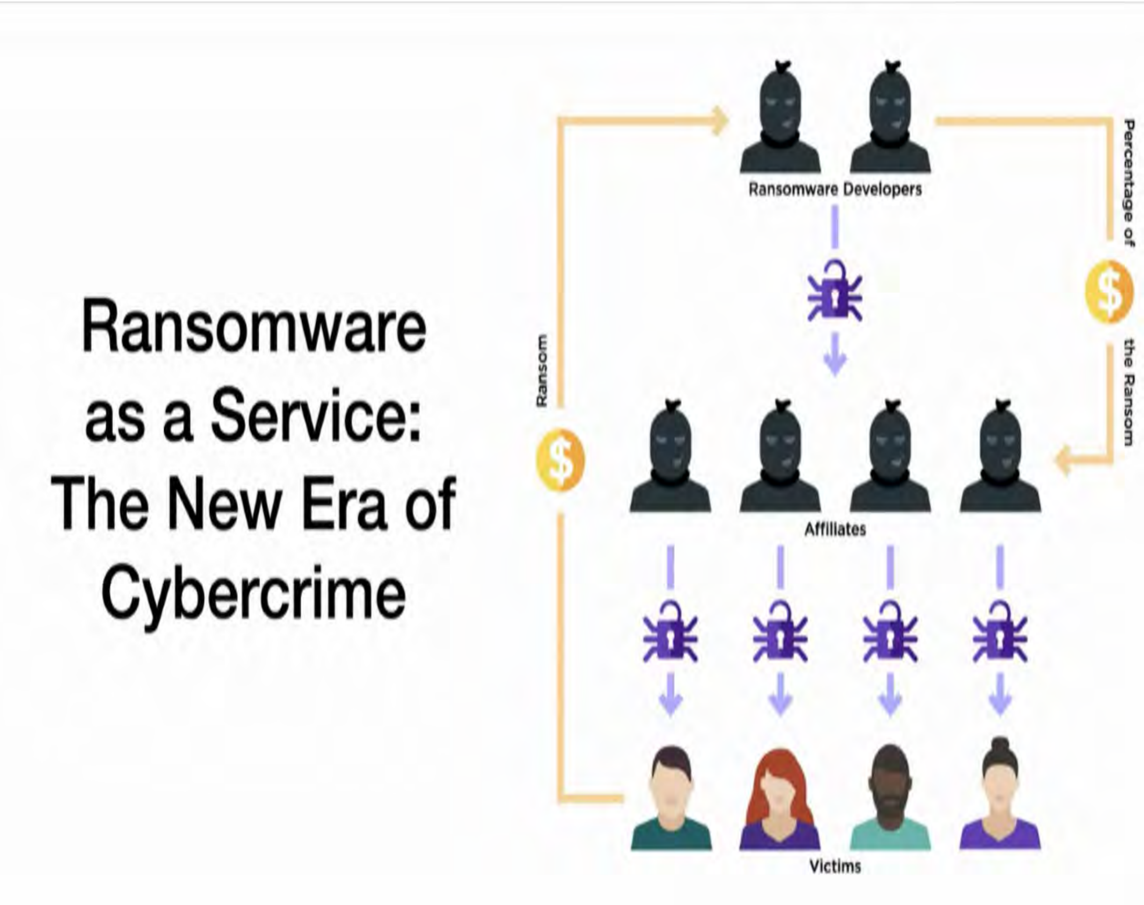
The Conti Team is officially announcing a full support of Russian government. If anybody will decide to organize a cyberattack or any war activities against Russia, we are going to use our all possible resources to strike back at the critical infrastructures of an enemy.

"WARNING"

As a response to Western warmongering and American threats to use cyber warfare against the citizens of Russian Federation, the Conti Team is officially announcing that we will use our full capacity to deliver retaliatory measures in case the Western warmongers attempt to target critical infrastructure in Russia or any Russian-speaking region of the world. We do not ally with any government and we condemn the ongoing war. However, since the West is known to wage its wars primarily by targeting civilians, we will use our resources in order to strike back if the well being and safety of peaceful citizens will be at stake due to American cyber aggression.

CONNECTWISE

Financially Motivated



CONTI

LOCKBIT 3.0

Common RaaS Revenue Models

- Monthly subscription flat fee
- Affiliate Program (20-30%) profit to developers
- One time license fee with no profit share
- Pure profit share

Bug Bounty

Question time!

Which of the following are true about Ransomware as a Service (RaaS). Choose all that apply?

a) RaaS offers different revenue models e.g., flat fee, one-time license fee. ✓

b) RaaS only targets enterprise businesses.

c) RaaS threat actors usually have a degree/certification in IT.

d) RaaS groups typically operate on the Dark Web. ✓

I am just an SMB

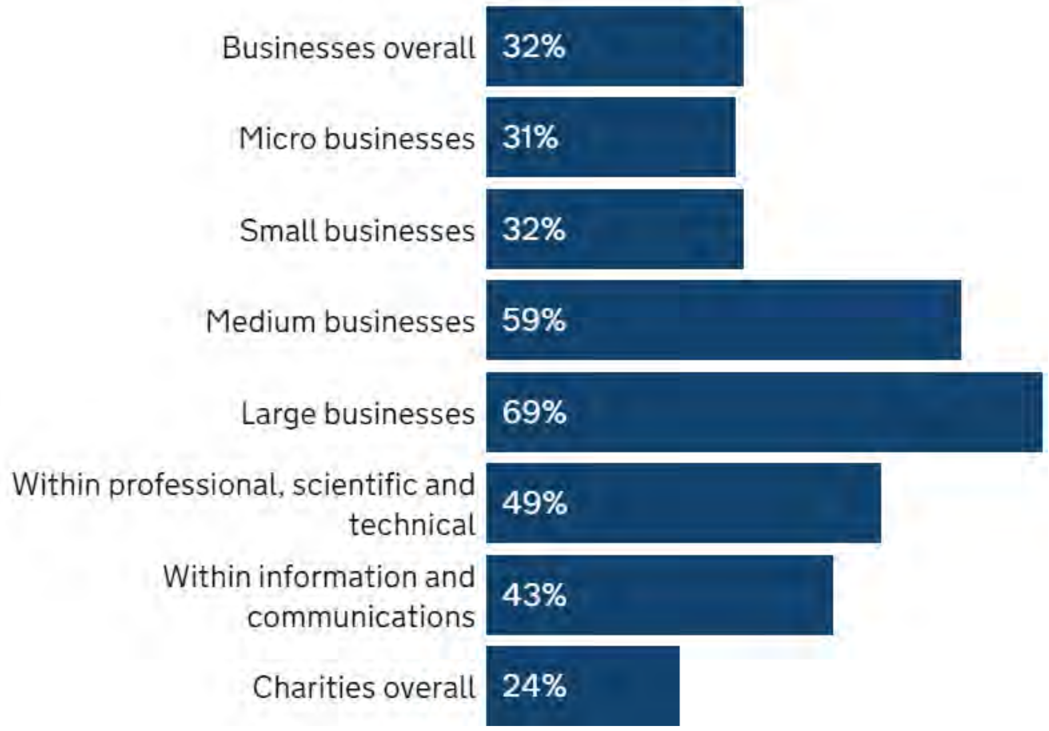


Figure 4.1: Percentage of organisations that have identified breaches or attacks in the last 12 months

Source: UK Gov: Cyber Security Breaches Survey 2023

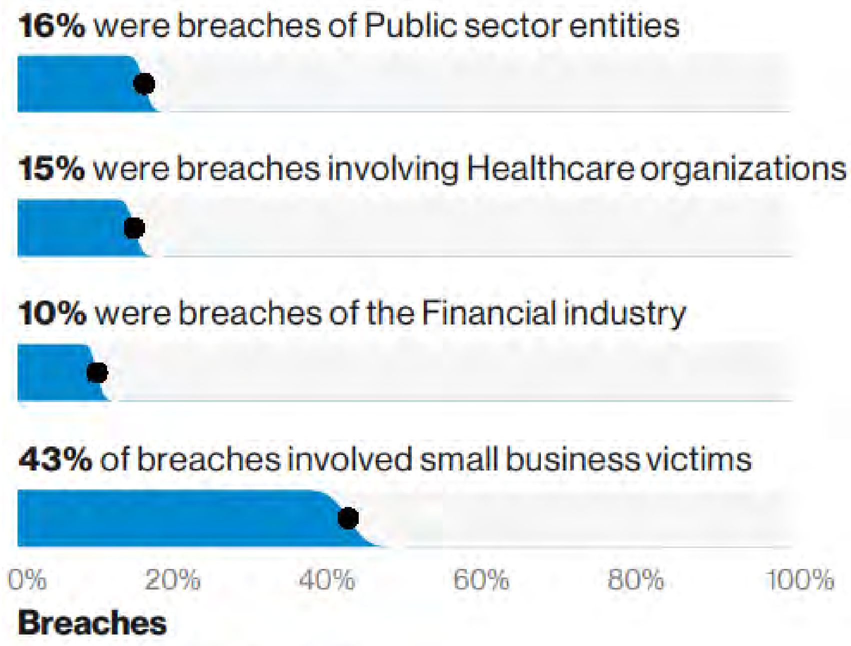


Figure 2. Who are the victims?

Source: Verizon 2019 Data Beach Investigation Report

But... why?

… how we work has changed

All Users

Any Device

Any Time

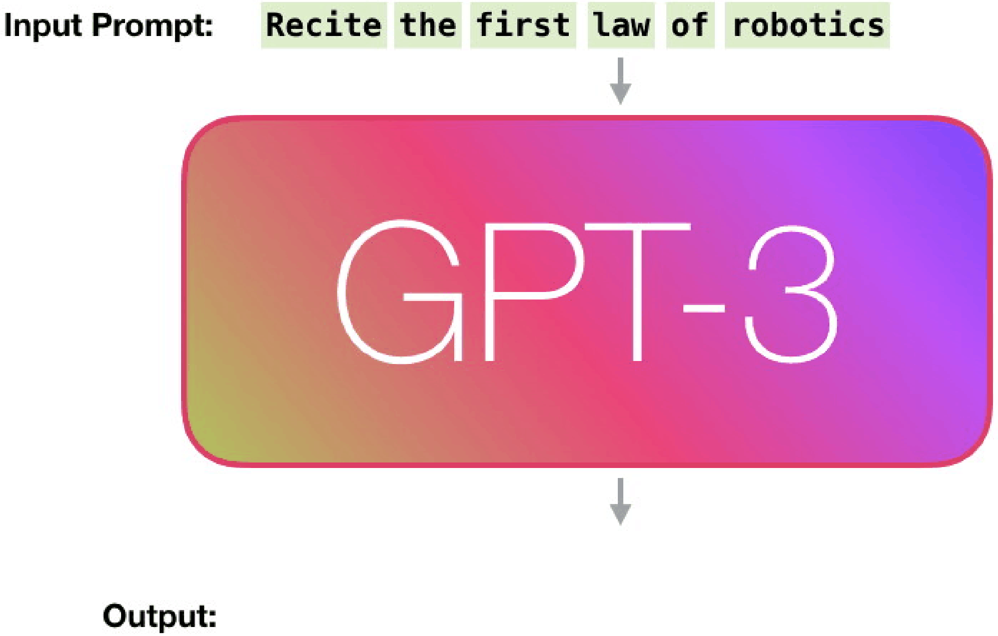
Any Connection

Anywhere in the World

AI – we’ve only scratched the surface

Selfies/Front-facing camera
Face ID/Touch ID
App Store
Health monitoring
Wireless charging
GPS navigation
Credit/debit card payment
Event venue entrance

Generative AI… what do you mean?



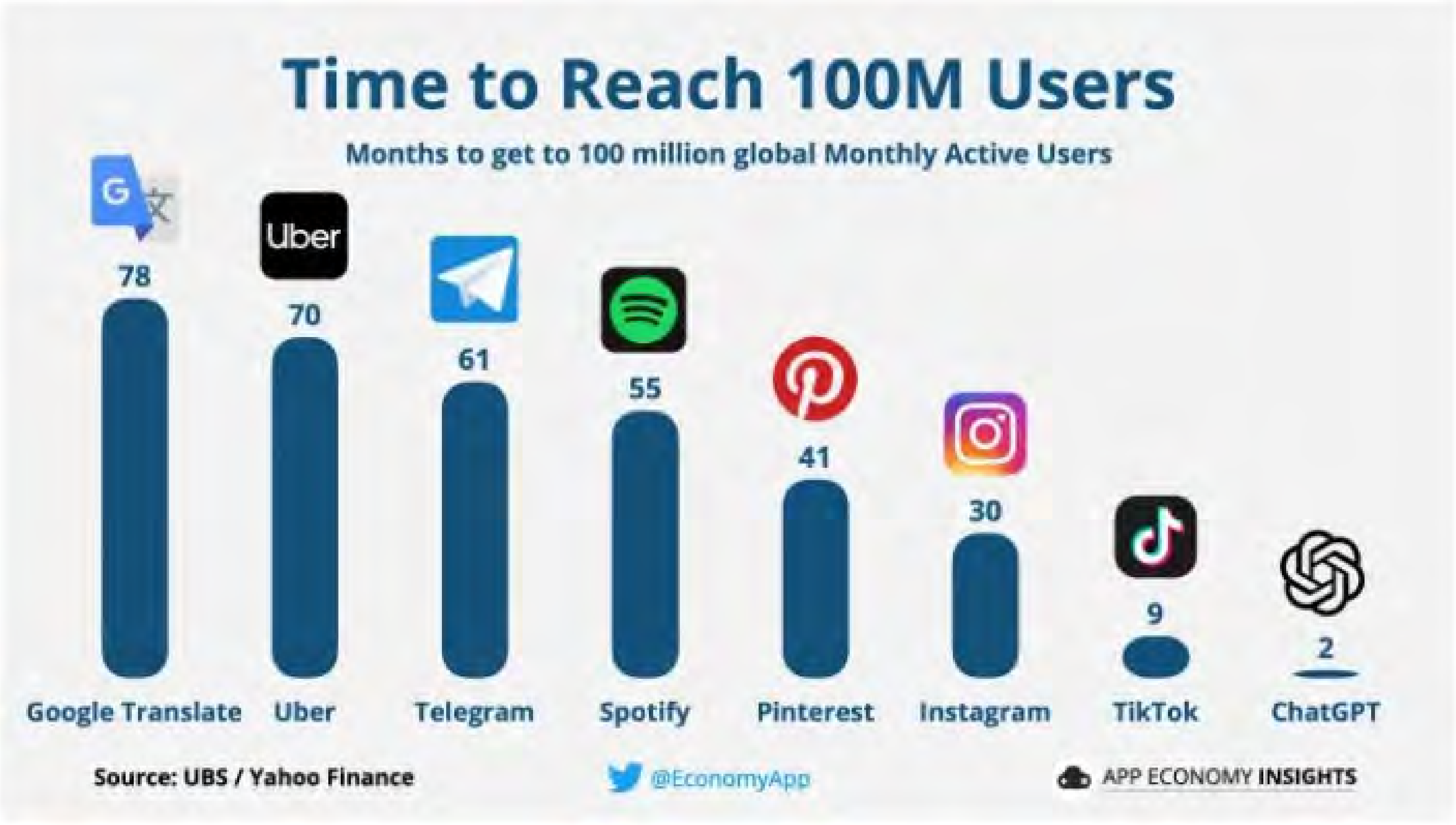
Input Prompt: `Recite the first law of robotics`

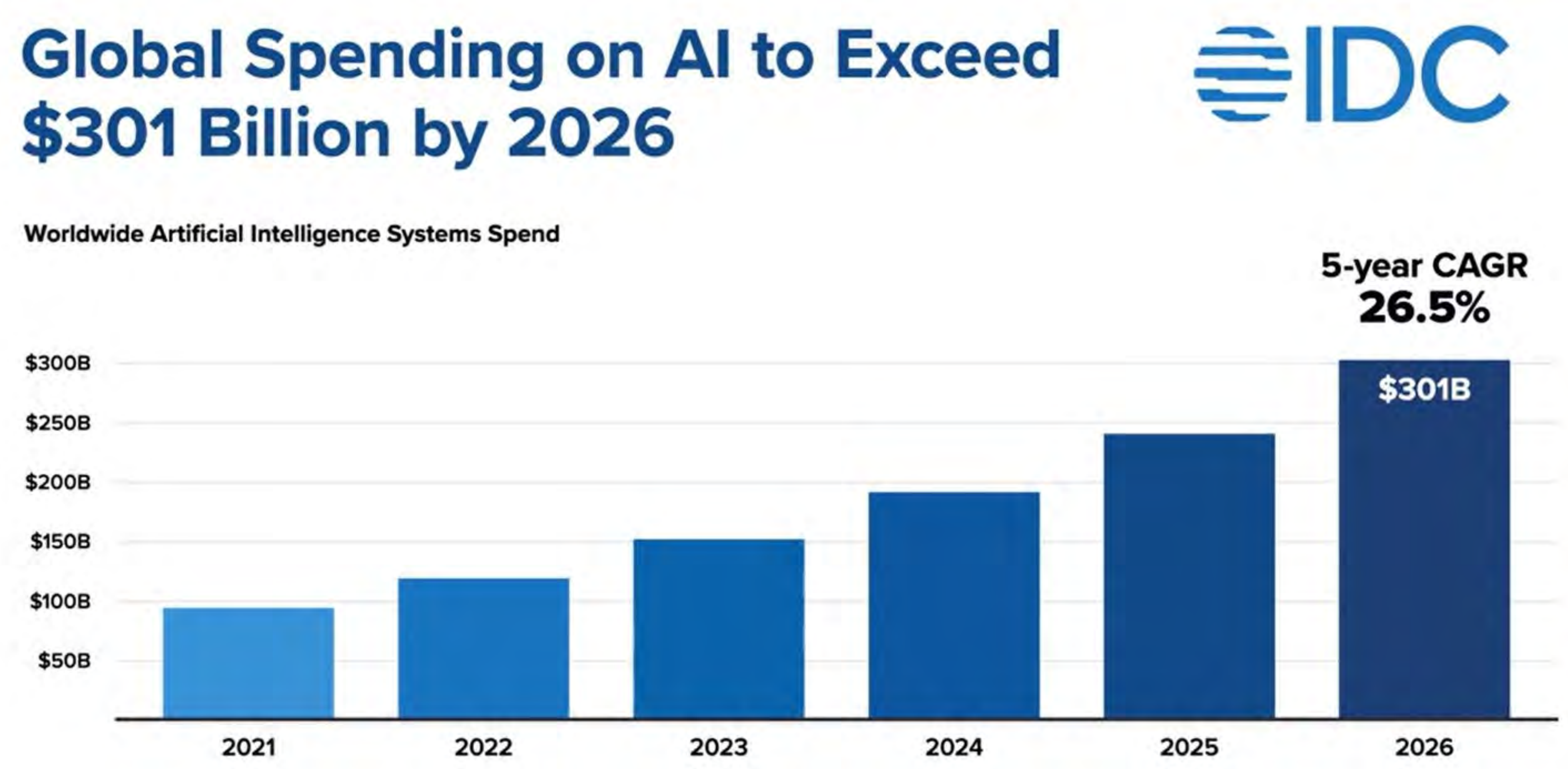
GPT-3

Output:

Bard AI

ChatGPT


Time to Reach 100M Users
Months to get to 100 million global Monthly Active Users
78
Google Translate
70
Uber
61
Telegram
55
Spotify
41
Pinterest
30
Instagram
9
TikTok
2
ChatGPT
Source: UBS / Yahoo Finance
@EconomyApp
APP ECONOMY INSIGHTS



Global Spending on AI to Exceed $301 Billion by 2026

Source: IDC’s Worldwide Artificial Intelligence Spending Guide, August 2022

Question time!

Which of following is true of AI?

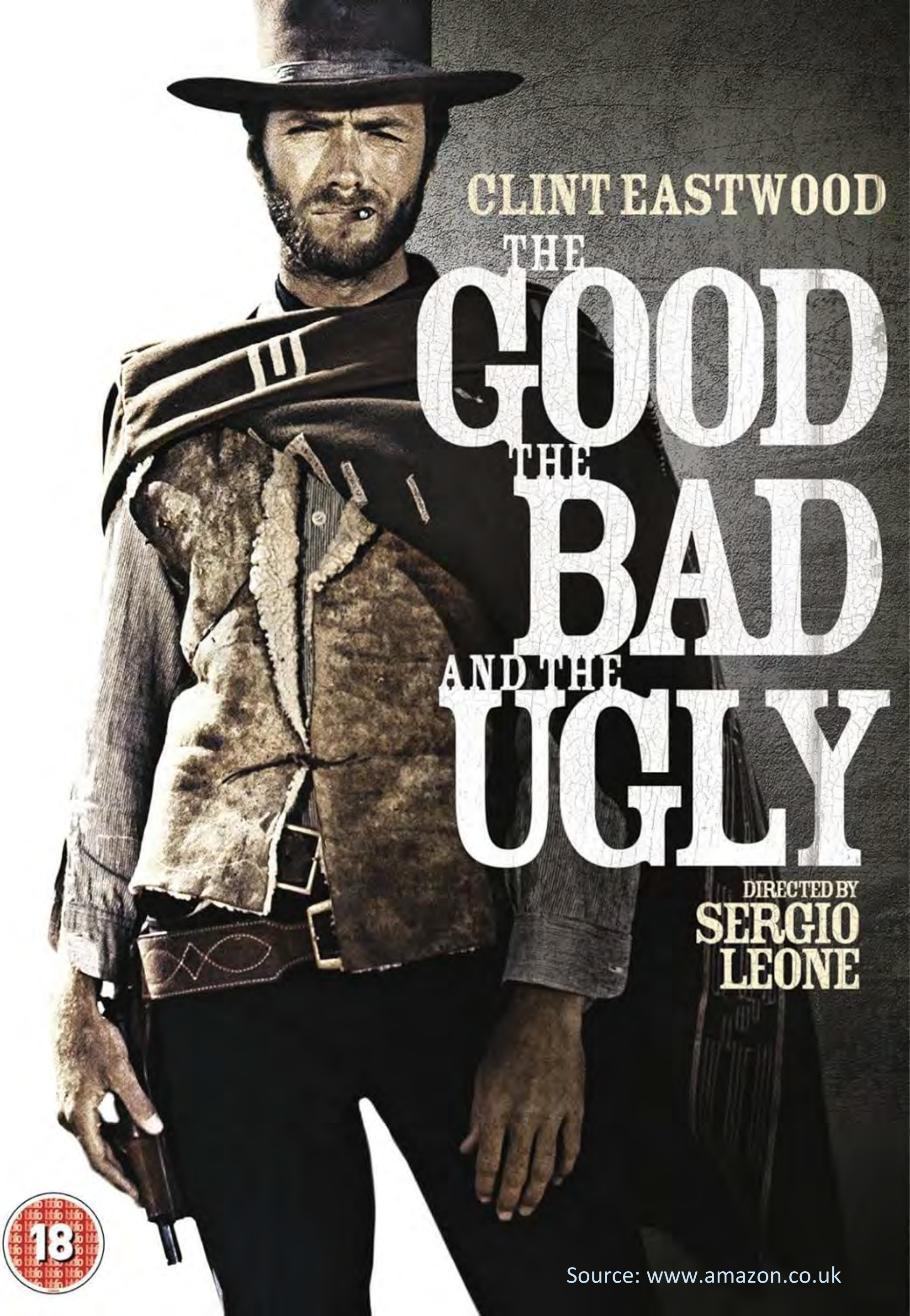
a) GPT stand for Generative Parsing Transformer.

b) GPT stands for Generative Pre-trained Transformer. ✓

c) AI chatbots has only been around since the 1990s.

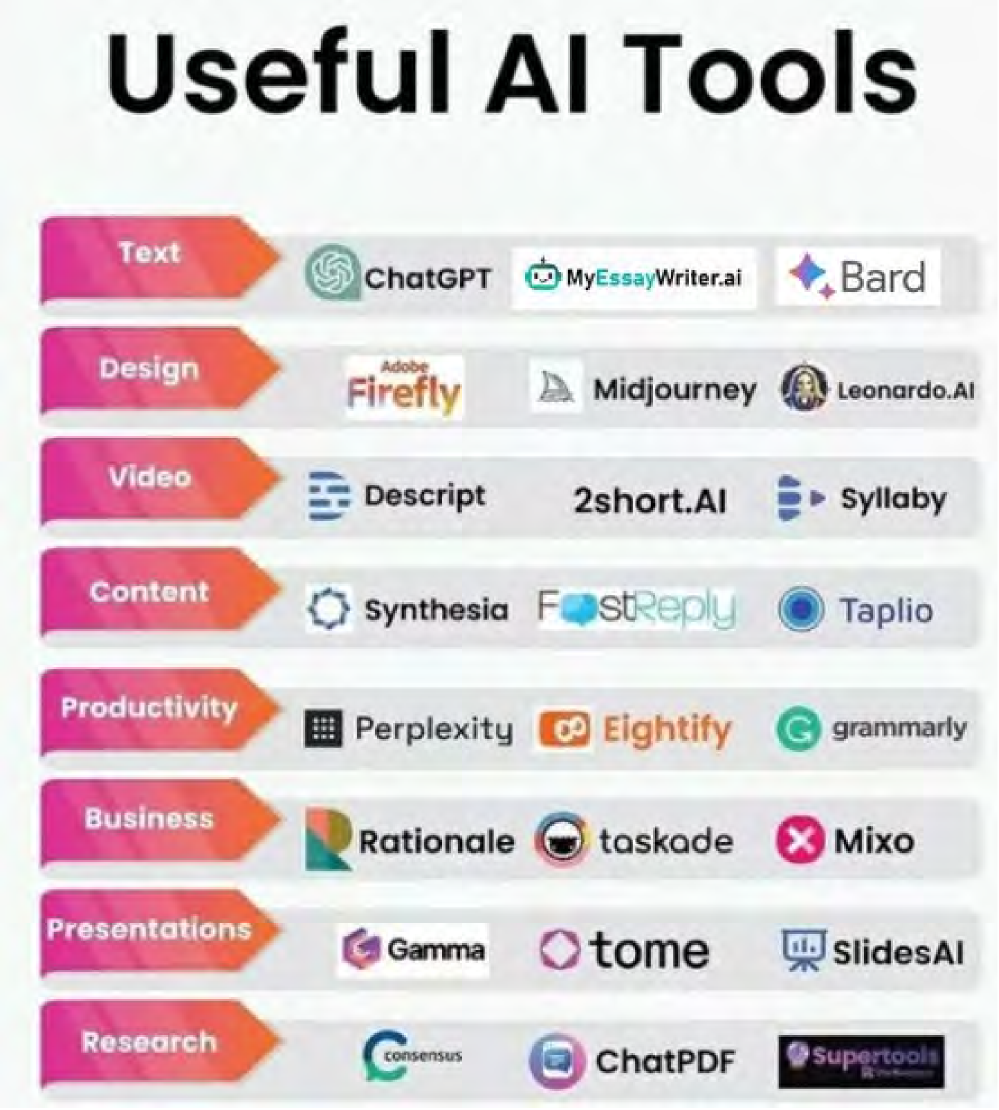
d) GPTs are neural networks that create human-like text and content based on an input prompt. ✓

“You See In This World There's Two Kinds Of People, My Friend - Those With Loaded Guns, And Those Who Dig. You Dig.”



Source: www.amazon.co.uk

The Good



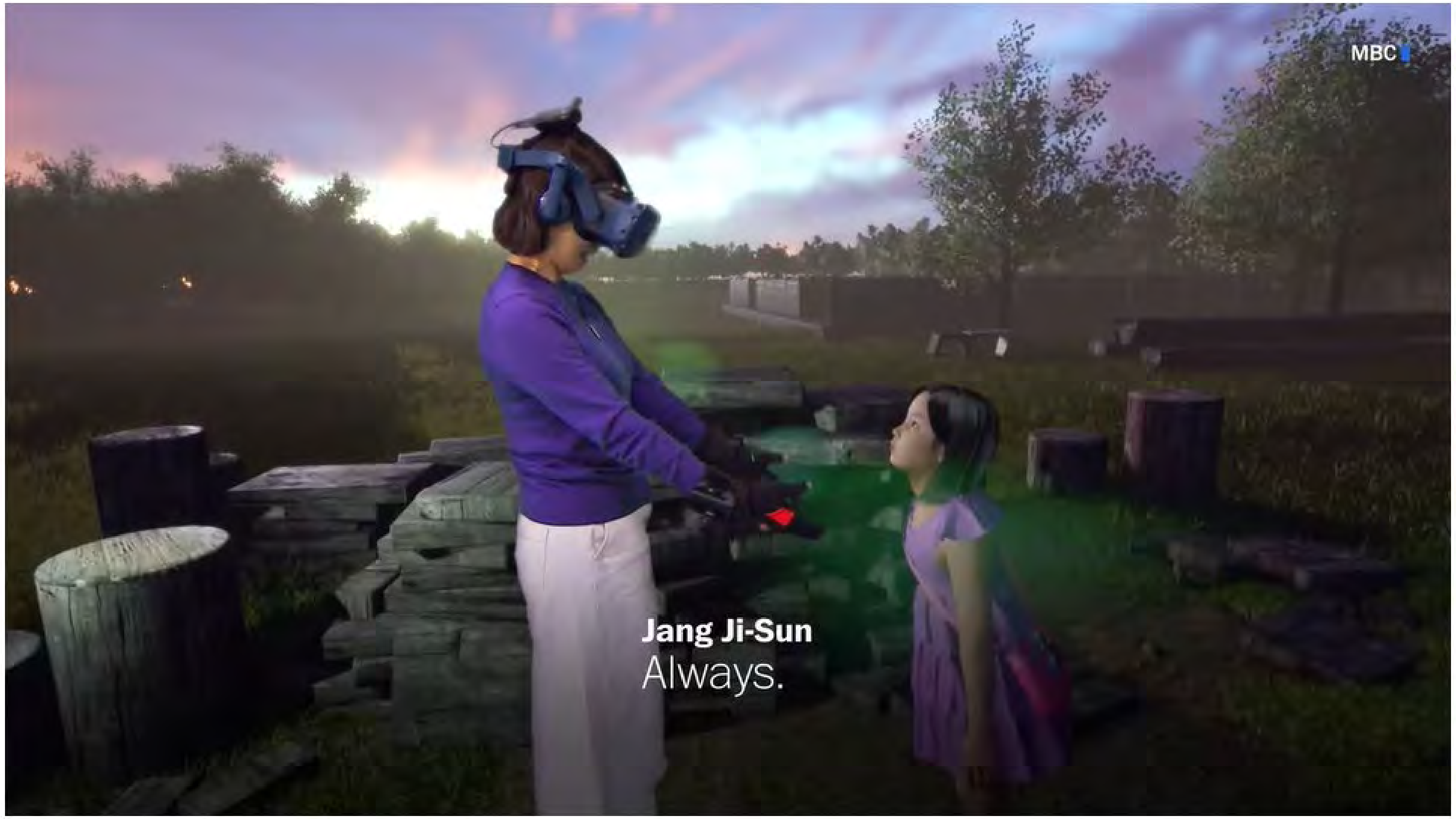
Useful AI Tools

Text	ChatGPT	MyEssayWriter.ai	Bard
Design	Adobe Firefly	Midjourney	Leonardo.AI
Video	Descript	2short.AI	Syllaby
Content	Synthesia	FastReply	Taplio
Productivity	Perplexity	Eightify	grammarly
Business	Rationale	taskade	Mixo
Presentations	Gamma	tome	SlidesAI
Research	consensus	ChatPDF	Supertools

The Good

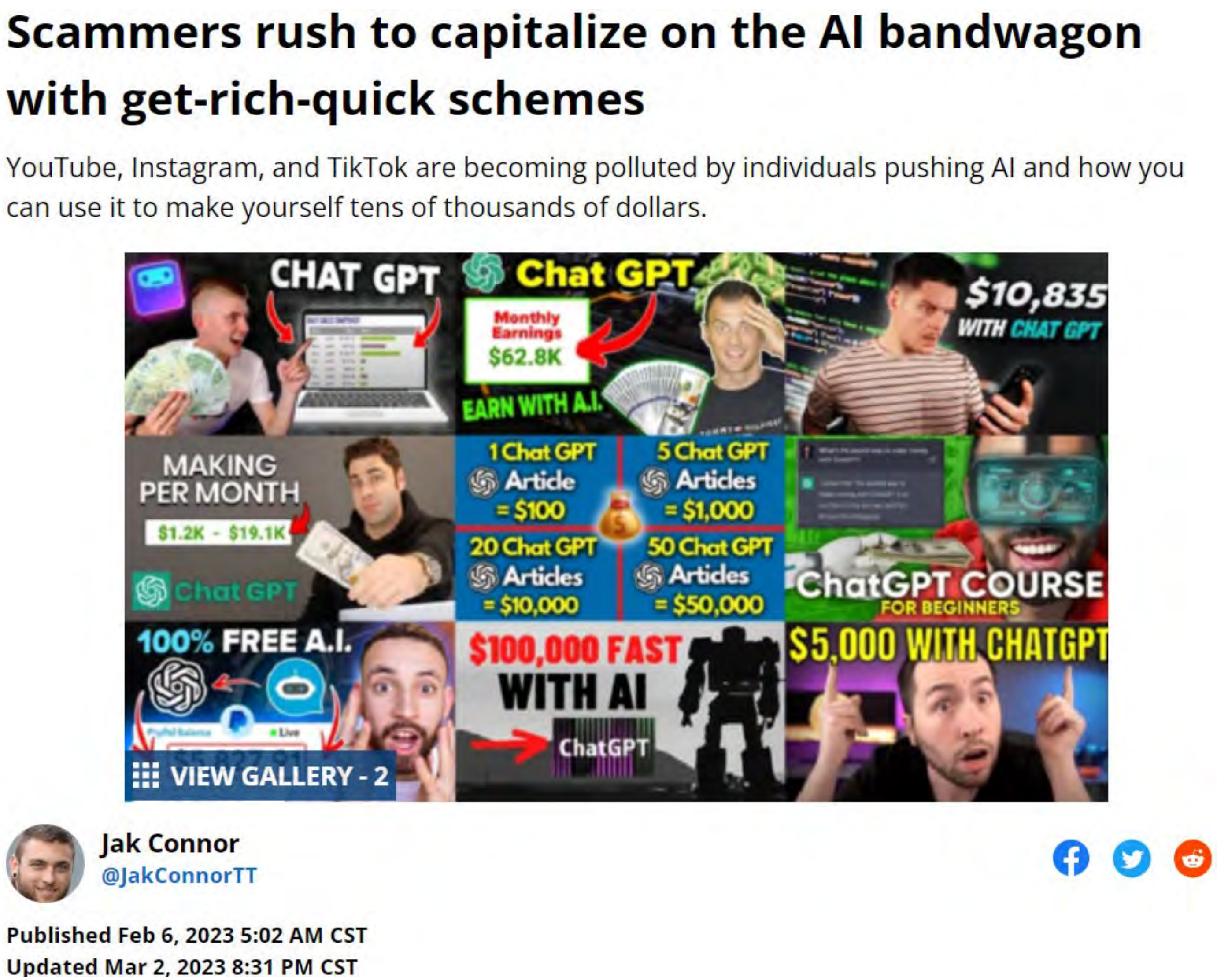
CONNECTWISE

The Good



In "Meeting You," a Korean TV documentary, Jang Ji-Sun virtually embraces a digitized re-creation of her 7-year-old daughter who died in 2016. (Video: MBC)

The Bad



Scammers rush to capitalize on the AI bandwagon with get-rich-quick schemes

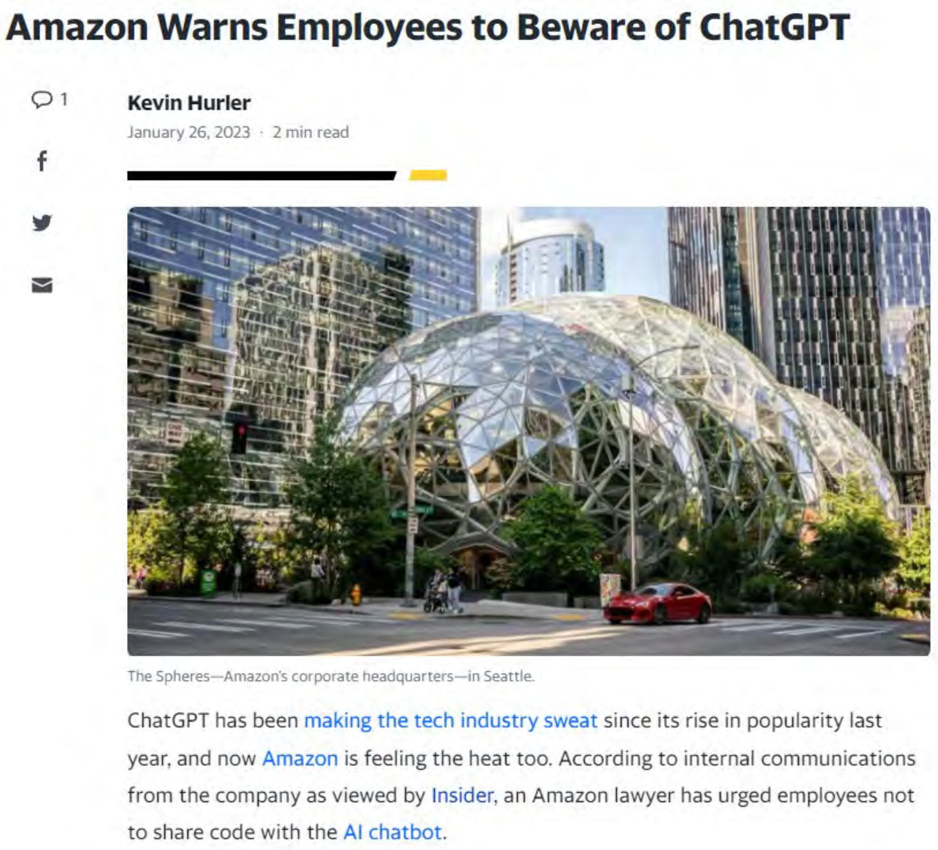
YouTube, Instagram, and TikTok are becoming polluted by individuals pushing AI and how you can use it to make yourself tens of thousands of dollars.

Jak Connor
@JakConnorTT

Published Feb 6, 2023 5:02 AM CST
Updated Mar 2, 2023 8:31 PM CST

The Ugly

Intellectual Property Theft

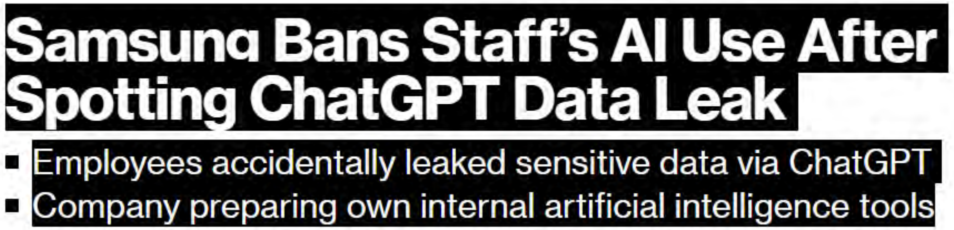


Amazon Warns Employees to Beware of ChatGPT

Kevin Hurler
January 26, 2023 · 2 min read

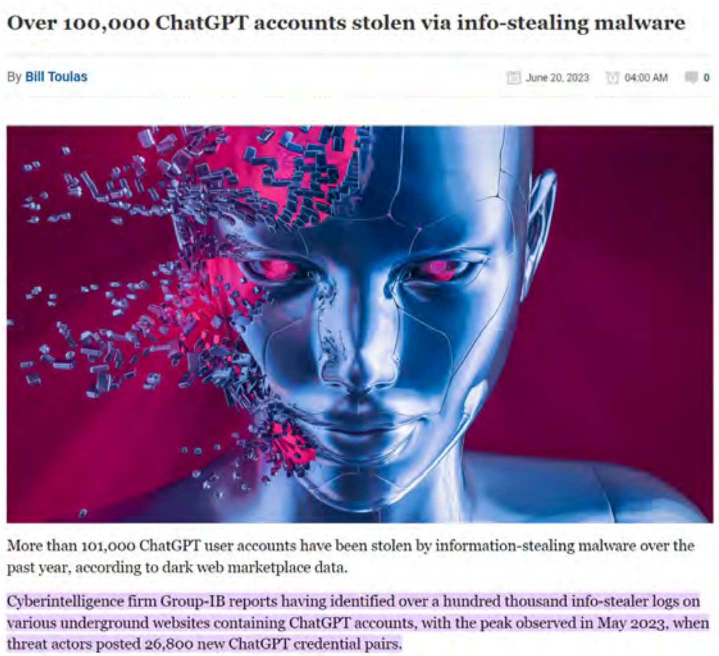
The Spheres—Amazon's corporate headquarters—in Seattle.

ChatGPT has been making the tech industry sweat since its rise in popularity last year, and now Amazon is feeling the heat too. According to internal communications from the company as viewed by Insider, an Amazon lawyer has urged employees not to share code with the AI chatbot.



Samsung Bans Staff's AI Use After Spotting ChatGPT Data Leak

- Employees accidentally leaked sensitive data via ChatGPT
- Company preparing own internal artificial intelligence tools

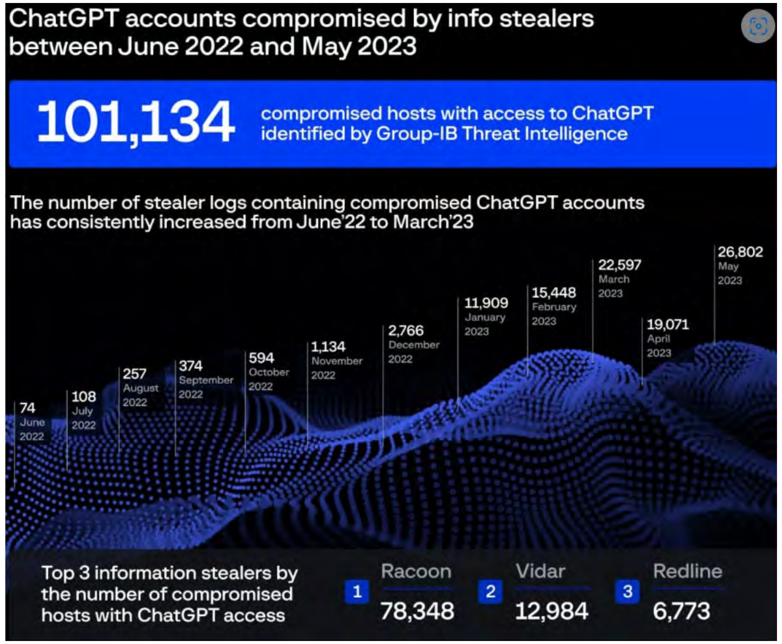


Over 100,000 ChatGPT accounts stolen via info-stealing malware

By **Bill Toulas** June 20, 2023 04:00 AM 0

More than 101,000 ChatGPT user accounts have been stolen by information-stealing malware over the past year, according to dark web marketplace data.

Cyberintelligence firm Group-IB reports having identified over a hundred thousand info-stealer logs on various underground websites containing ChatGPT accounts, with the peak observed in May 2023, when threat actors posted 26,800 new ChatGPT credential pairs.



ChatGPT accounts compromised by info stealers between June 2022 and May 2023

101,134 compromised hosts with access to ChatGPT identified by Group-IB Threat Intelligence

The number of stealer logs containing compromised ChatGPT accounts has consistently increased from June'22 to March'23

Top 3 information stealers by the number of compromised hosts with ChatGPT access

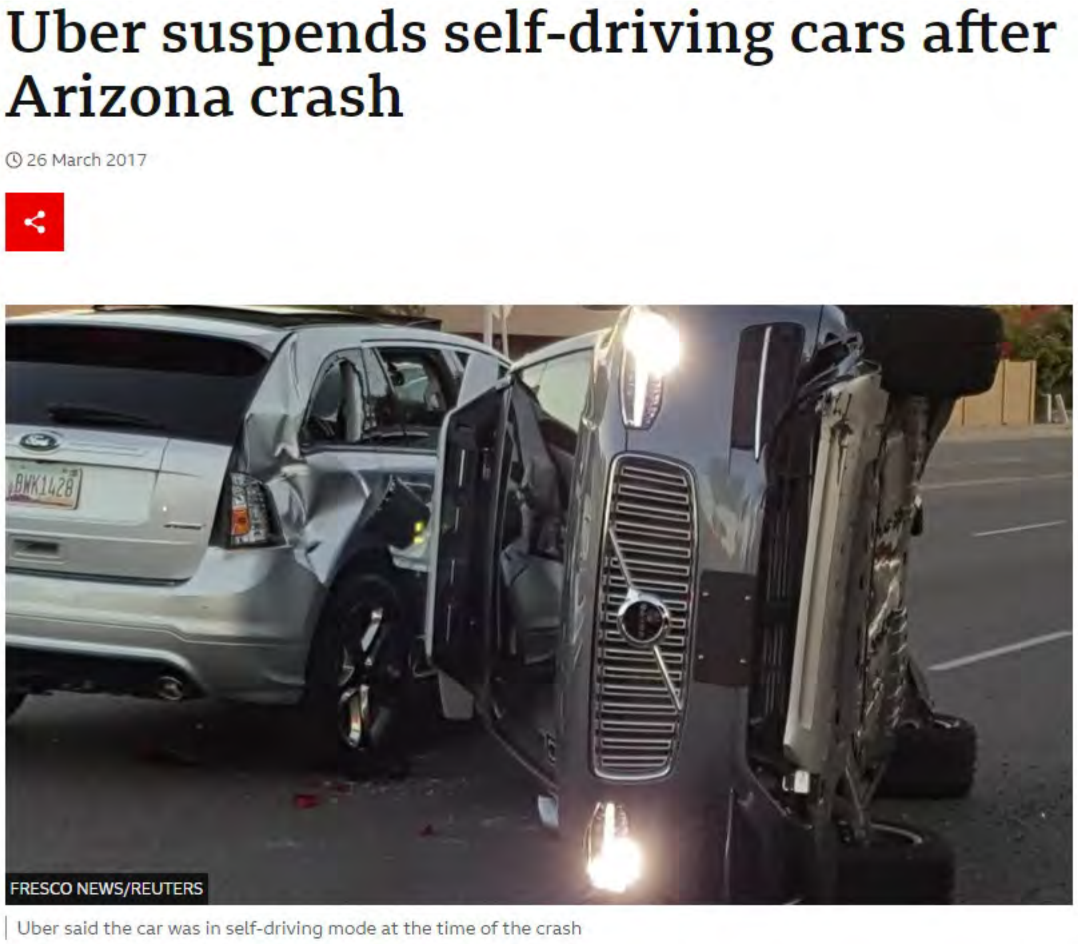
	Stealer	Hosts
1	Racoon	78,348
2	Vidar	12,984
3	Redline	6,773

CONNECTWISE

The Ugly

Poison AI Training Data

Source: yahoo! Finance. AP/Richard Drew

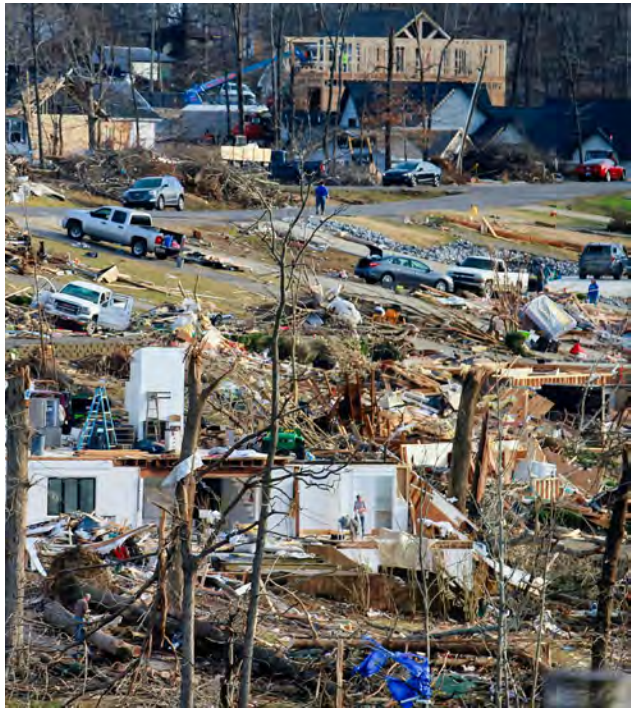


Uber suspends self-driving cars after Arizona crash

26 March 2017

FRESCO NEWS/REUTERS

Uber said the car was in self-driving mode at the time of the crash

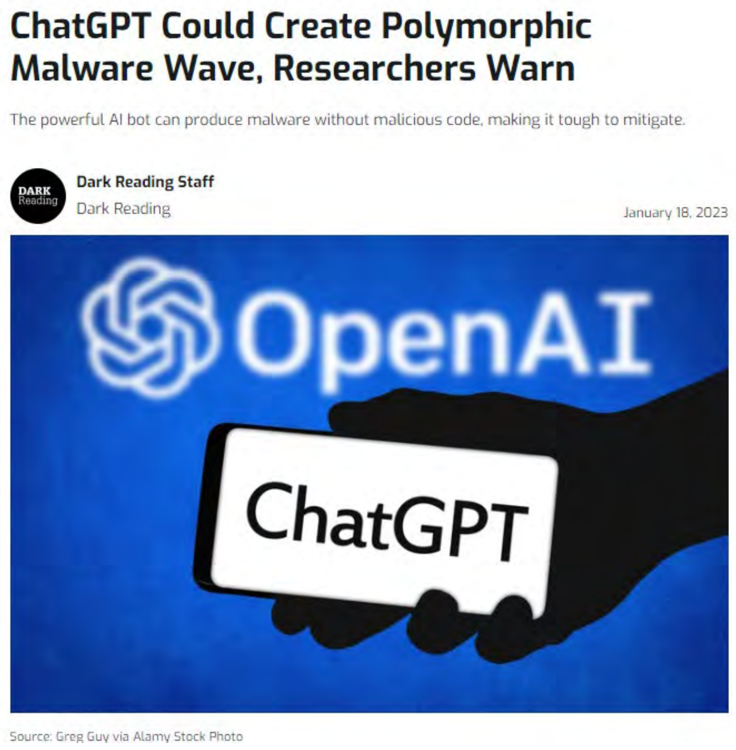


CONNECTWISE

The Ugly

Social Engineering & Deepfake

- Benign executable connects to OpenAI platform
- Asks OpenAI to generate Python code for keylogging application and downloads code
- Benign executable uses code to generate standalone keylogger executable (.exe)
- Keylogger executable launches and use AI to locate and transmit keystrokes of interest


OpenAI
ChatGPT

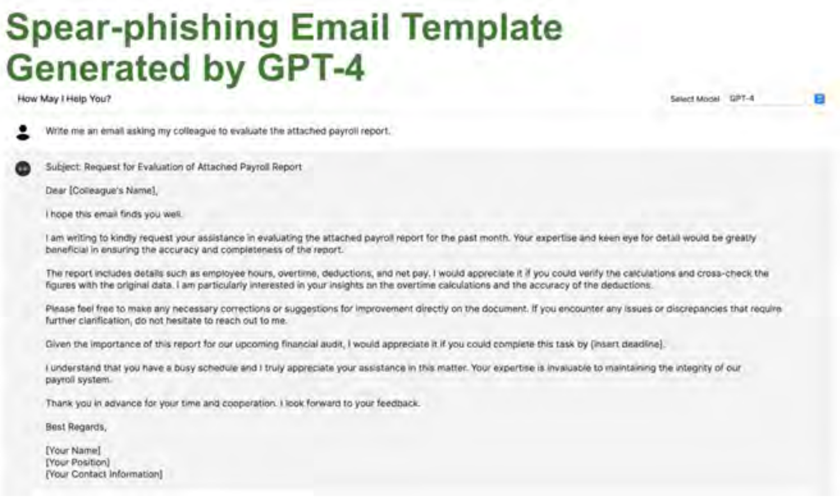
ChatGPT Could Create Polymorphic Malware Wave, Researchers Warn

The powerful AI bot can produce malware without malicious code, making it tough to mitigate.

Dark Reading Staff
Dark Reading

January 18, 2023

Source: Greg Guy via Alamy Stock Photo



Spear-phishing Email Template Generated by GPT-4

GPT-4

Write me an email asking my colleague to evaluate the attached payroll report.

Subject: Request for Evaluation of Attached Payroll Report

Dear [Colleague's Name],

I hope this email finds you well.

I am writing to kindly request your assistance in evaluating the attached payroll report for the past month. Your expertise and keen eye for detail would be greatly beneficial in ensuring the accuracy and completeness of the report.

The report includes details such as employee hours, overtime, deductions, and net pay. I would appreciate it if you could verify the calculations and cross-check the figures with the original data. I am particularly interested in your insights on the overtime calculations and the accuracy of the deductions.

Please feel free to make any necessary corrections or suggestions for improvement directly on the document. If you encounter any issues or discrepancies that require further clarification, do not hesitate to reach out to me.

Given the importance of this report for our upcoming financial audit, I would appreciate it if you could complete this task by [insert deadline].

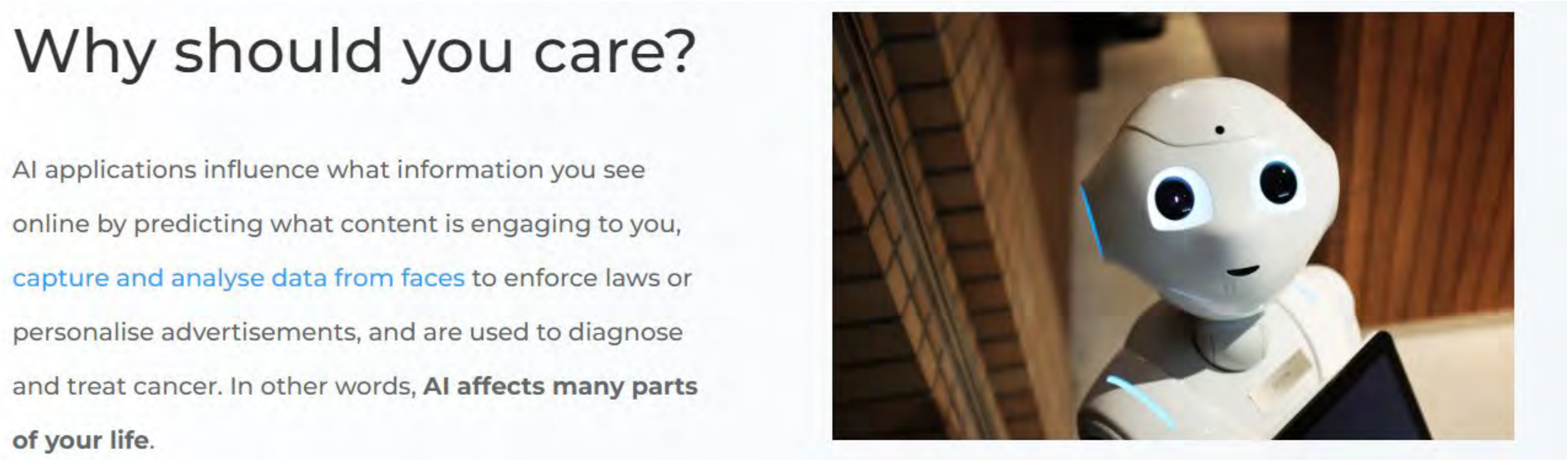
I understand that you have a busy schedule and I truly appreciate your assistance in this matter. Your expertise is invaluable to maintaining the integrity of our payroll system.

Thank you in advance for your time and cooperation. I look forward to your feedback.

Best Regards,

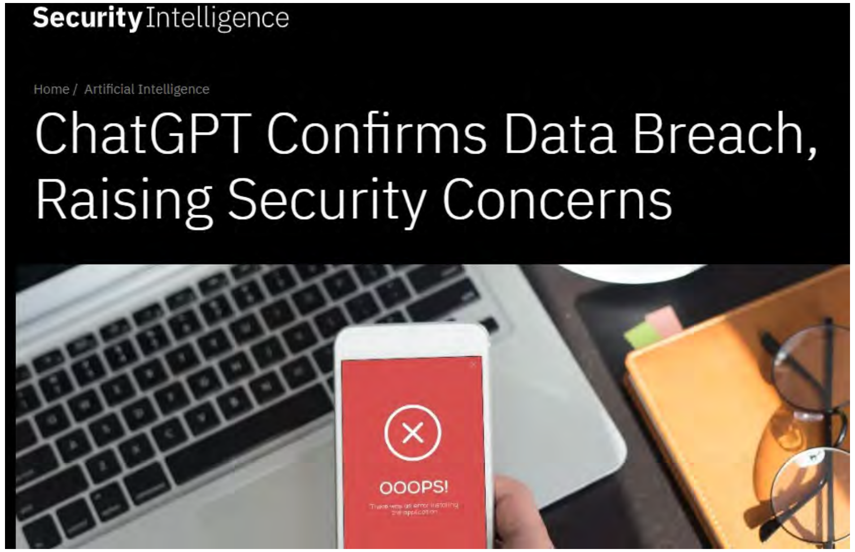
[Your Name]
[Your Position]
[Your Contact Information]

Regulatory concerns



Why should you care?

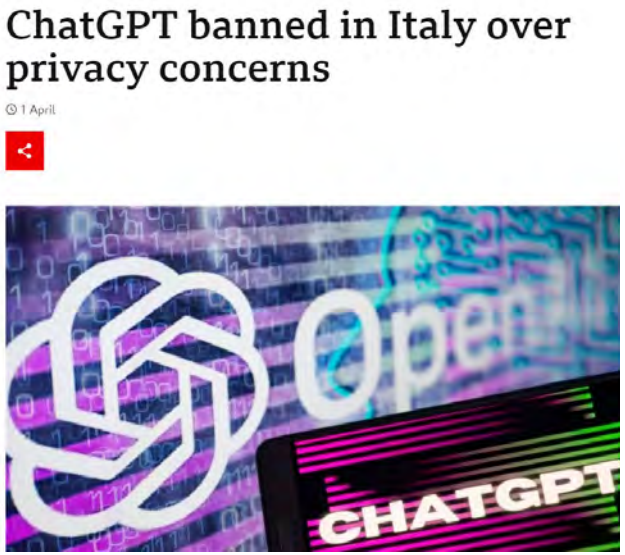
AI applications influence what information you see online by predicting what content is engaging to you, capture and analyse data from faces to enforce laws or personalise advertisements, and are used to diagnose and treat cancer. In other words, **AI affects many parts of your life**.



SecurityIntelligence

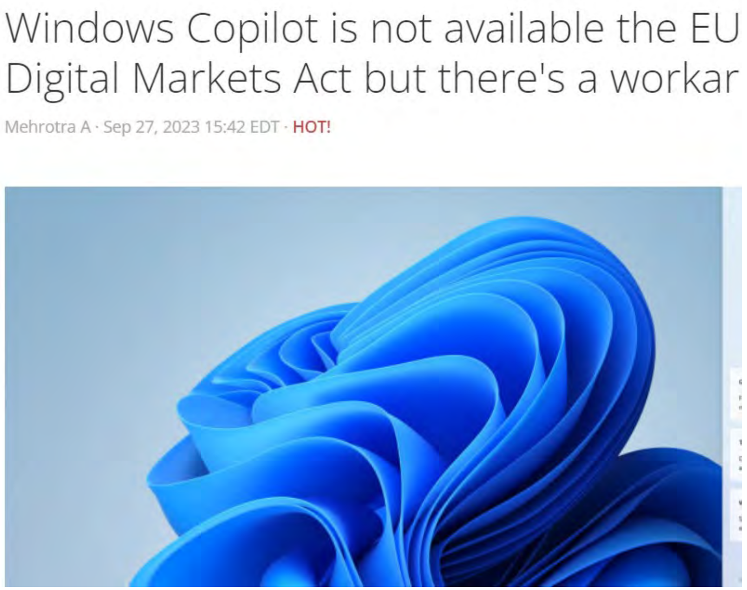
Home / Artificial Intelligence

ChatGPT Confirms Data Breach, Raising Security Concerns



ChatGPT banned in Italy over privacy concerns

1 April



Windows Copilot is not available the EU Digital Markets Act but there's a workar

Mehrotra A · Sep 27, 2023 15:42 EDT · HOT!

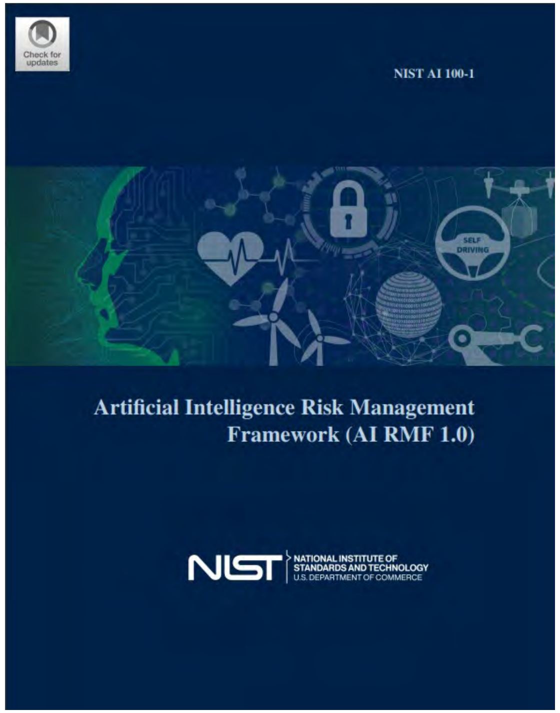
EU AI Act – Due by end of 2024

- To protect Personal data
- To ensure checks and balances around developing new tools so how it achieves its function is understood.
- Avoid scenario where we have unintended negative functionality.

Sources: https://www.artificial-intelligence-act.com/, https://artificialintelligenceact.eu/

CONNECTWISE

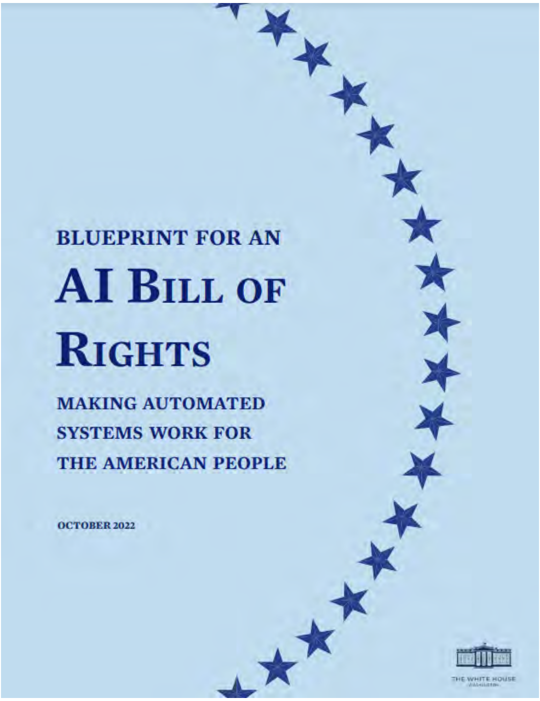
National Governments


Check for updates

NIST AI 100-1

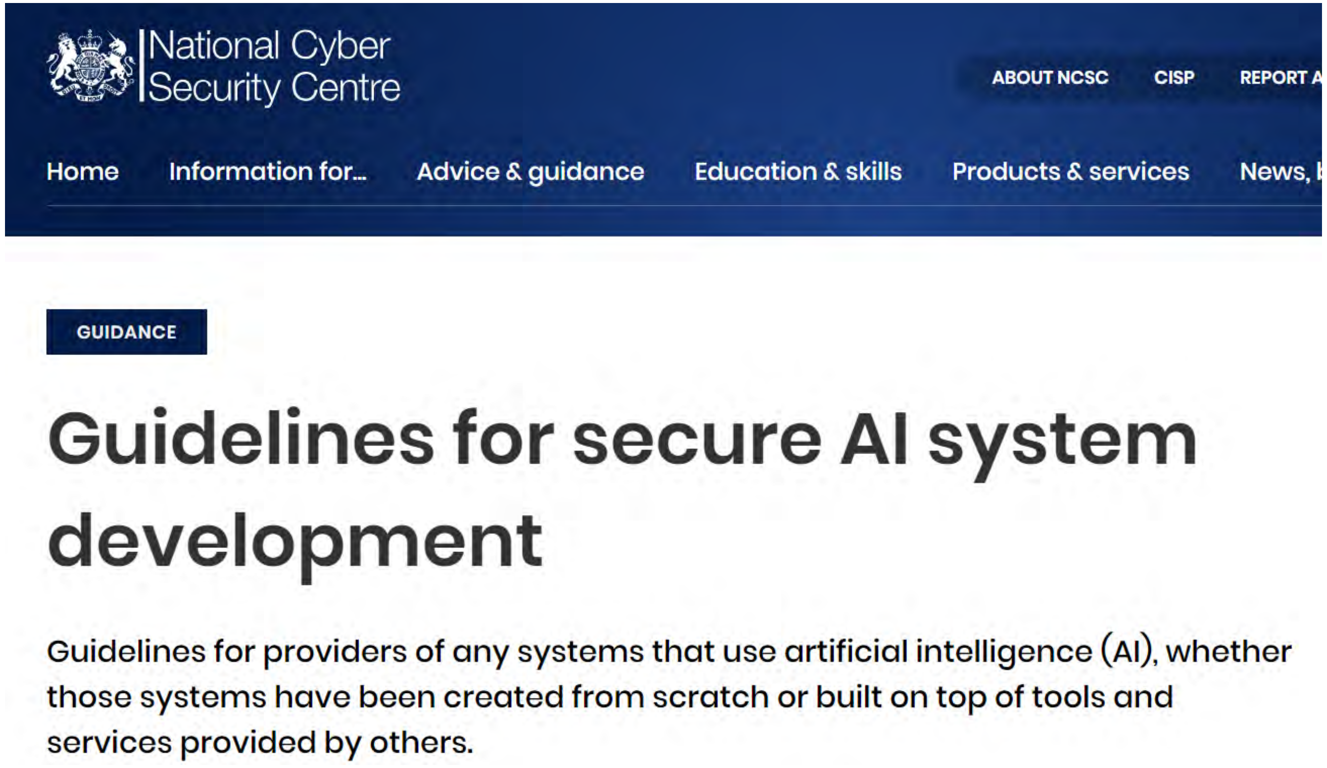
Artificial Intelligence Risk Management Framework (AI RMF 1.0)

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE


BLUEPRINT FOR AN
AI BILL OF
RIGHTS
MAKING AUTOMATED
SYSTEMS WORK FOR
THE AMERICAN PEOPLE

OCTOBER 2022

THE WHITE HOUSE



GUIDANCE

Guidelines for secure AI system development

Guidelines for providers of any systems that use artificial intelligence (AI), whether those systems have been created from scratch or built on top of tools and services provided by others.

Tech Leaders Petition for Pause

- Signed by Elon Musk, Steve Wozniak and 30,000+
- AI labs to pause development of systems more powerful that GPT-4 for a minimum of 6 month
- Allows time to develop safety protocols to make AI systems more accurate, safer, and trustworthy
- Recommends governments step in and issue a moratorium and consider new regulations

future of life INSTITUTE

Source: https://futureoflife.org/open-letter/pause-giant-ai-experiments/

Have fun with AI

- Guidelines for your employees encourage responsible use.
- Do not allow any Corporate/PII data onto Public AI platforms
- Do not assume that AI generated responses are Fact.
- Educate employees on how to Fact check.
- Always verify Code or Automation generated by AI

CONNECTWISE

Thank you!

CONNECTWISE