

HOW AI IS REWRITING THE RULES OF CYBER WARFARE

Bobby Spooner, Principal Security Consultant
- Attack Manager, LRQA



**LEADERSHIP
SERIES**

WHO ARE WE?

Artificial Intelligence Driven Attacks

Key Facts	 Security Testing LRQA Nettitude's security testers hold the highest technical qualifications available to provide real world, human led testing services • Penetration testing • Red teaming • Cloud testing • Bug bounty • Application testing	 Managed Security Services 24x7 managed security services delivered by LRQA Nettitude's dedicated Security Operations Center (SOC) and Cyber Incident Response Team (N-CIRT) • SOC-as-a-Service • Vulnerability scanning • Sentinel XDR • SIEM • Detection & response
	 Risk & Compliance Strategic guidance & certification around compliance mandates (such as HIPAA, PCI, GDPR, ISO 27002) • VCISO • Security Strategy Creation • Cyber Security Planning • Cyber essentials • Security awareness • Policy and process creation & review • Due diligence	 Advisory Services Bespoke services ensuring clients' cybersecurity maturity & resiliency is in line with their risk tolerance • Threat intelligence • Incident response • Cloud assessments • Purple teaming • Cyber training

1,000+
clients globally

240+
cyber experts

20 Years
cyber heritage

#1
The only organisation with a full suite of CREST accreditations

Bobby Spooner



- Risk managing simulated cyber-attacks across geographies
- CREST Certified Simulated Attack Manager
- Hold active CISSP and CCSP Certifications.
- Built and managed Operational Security Assurance in a large UK Government Department.
- Managed Red & Purple Teaming across UK Critical National Infrastructure (CNI), programme managing associated remediation.
- Designated Covid-19 InfoSec Lead for UK government Department
 - Managed urgent risk assessments to facilitate secure working in the post-covid world.

HOW AI IS REWRITING THE RULES OF CYBER WARFARE

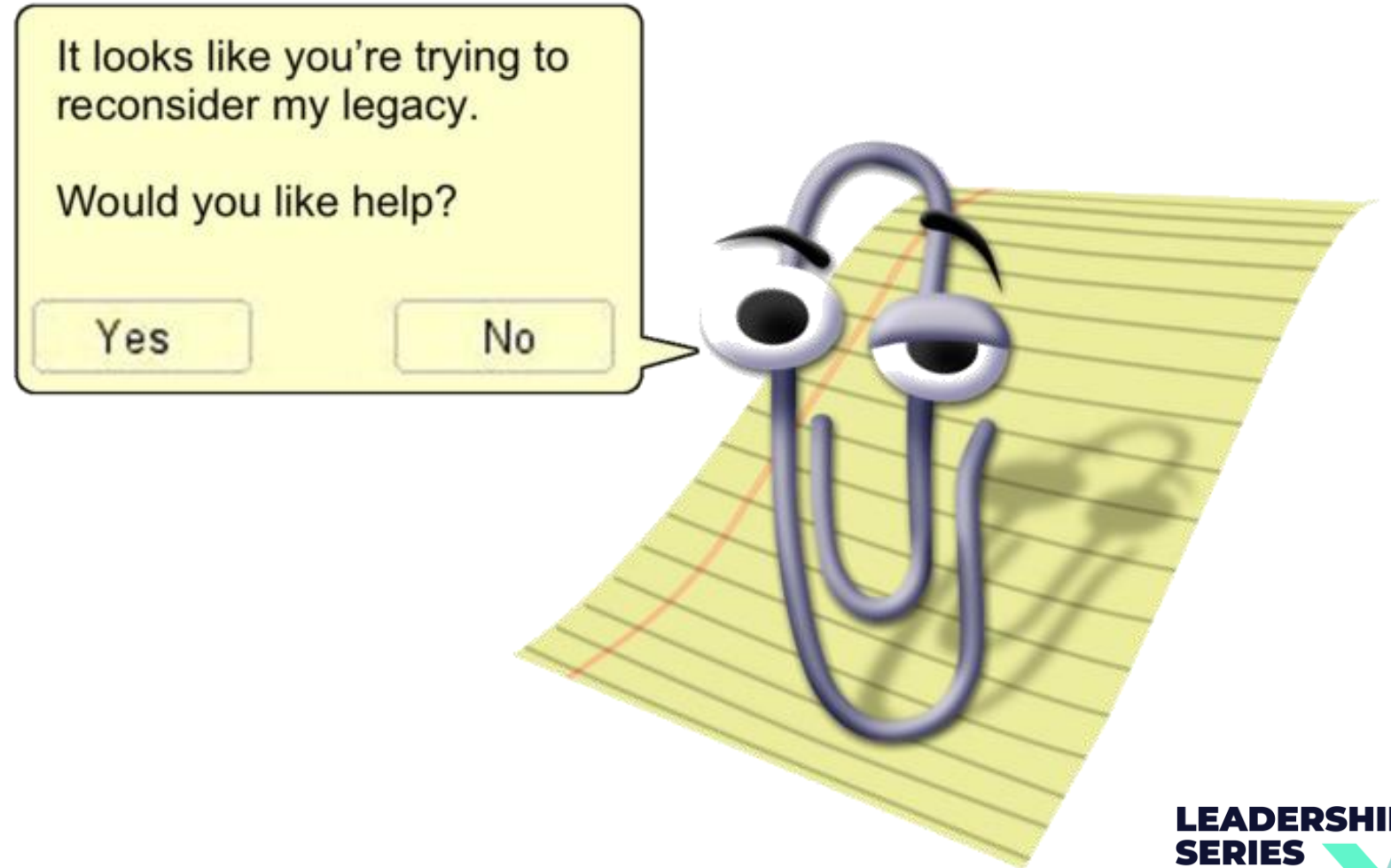
A TRIP DOWN MEMORY LANE

oasis



IN THE BEGINNING

Artificial Intelligence Driven Attacks



DESKTOP DANGER

Artificial Intelligence Driven Attacks

Desktop Buddy Driven Attacks



HOW AI IS REWRITING THE RULES OF CYBER WARFARE

AI TODAY



LRQA

LEADERSHIP
SERIES



TOOLS WE CAN ALL EMBRACE

Artificial Intelligence Driven Attacks

Write a poem reevaluating Clippy's legacy for presentation at LRQA's leadership series.

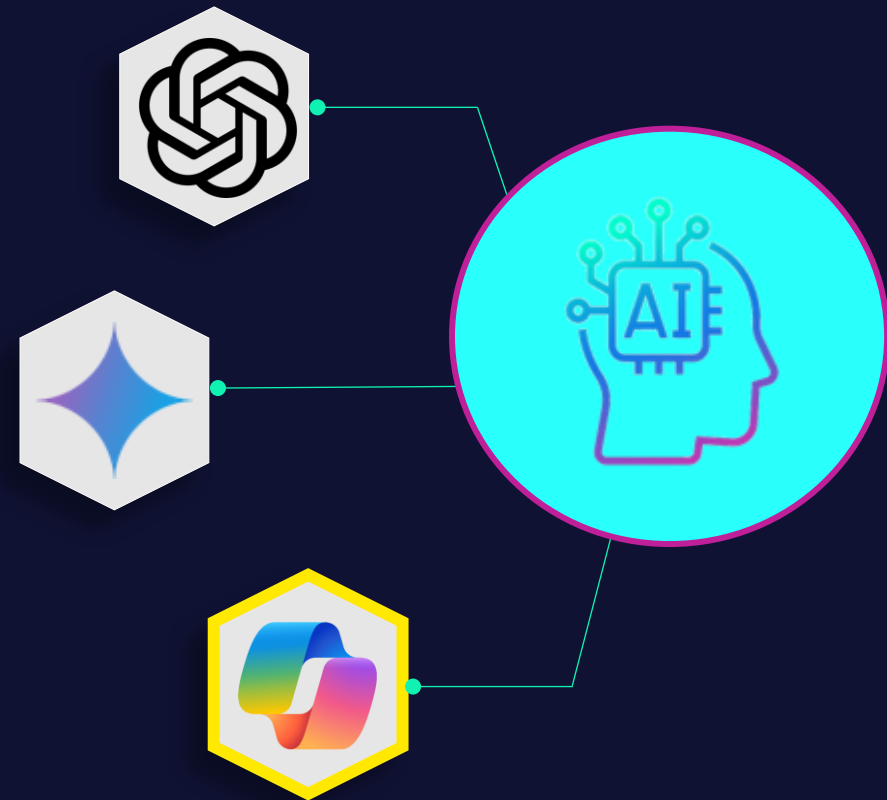
Absolutely—here's a thoughtful and slightly cheeky poem that reimagines Clippy's legacy through a leadership lens, perfect for LRQA's series:

🗣️ "Clippy: A Legacy Reconsidered"

He popped up unbidden, a pixel-bound sage,
With eyes full of hope on a blank Word page.
"Looks like you're writing," he'd chirp with delight—
A helper, a herald, a well-meaning sprite.

Dismissed as annoying, a relic, a joke,
He bore every meme and sarcastic poke.
Yet beneath the cartoon and comic disdain,
Was a vision of service—though clumsy, humane.

Clippy believed in the power of aid,
That guidance, though simple, should never degrade.
He taught us that presence—however maligned—
Can spark innovation when purpose is aligned.



WIDE RRANGING BENEFITS

Artificial Intelligence Driven Attacks

Automates repetitive tasks, improving operational efficiency.

- **Reduced** human error, faster turnaround times

Analyses large datasets to support better decision-making.

- **Improved** accuracy, strategic insights

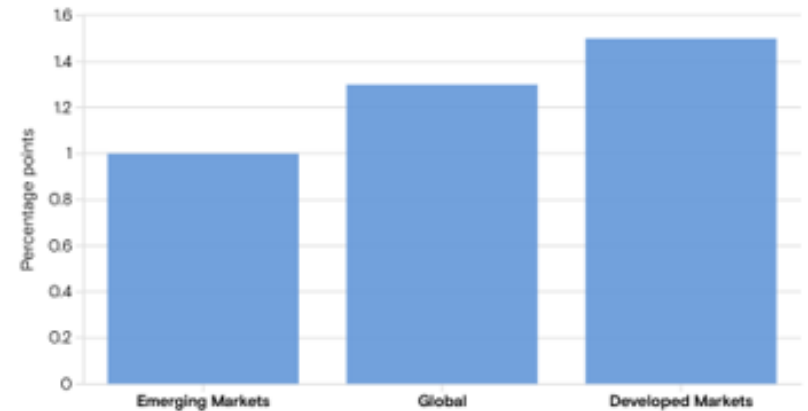
Aids in diagnosing and treating patients, enhancing healthcare.

- **Early** detection, tailored treatments

Contributes to economic growth by driving innovation.

- **Increased** productivity, competitive advantage

AI has the potential to be a major driver of labor productivity growth
Estimated effect of widespread AI adoption on annual productivity growth



Source: Goldman Sachs Research
Composites based on market FX GDP country weights. Estimates are not forecasts and represent stylized scenarios in which AI productivity gains are realized over a 10-year period following widespread adoption.

Goldman Sachs

naturemed

Explore content ▾ About the journal ▾ Publish with us ▾

[nature](#) > [nature medicine](#) > [articles](#) > article

Article | [Open access](#) | Published: 07 January 2025

Nationwide real-world implementation of AI for cancer detection in population-based mammography screening

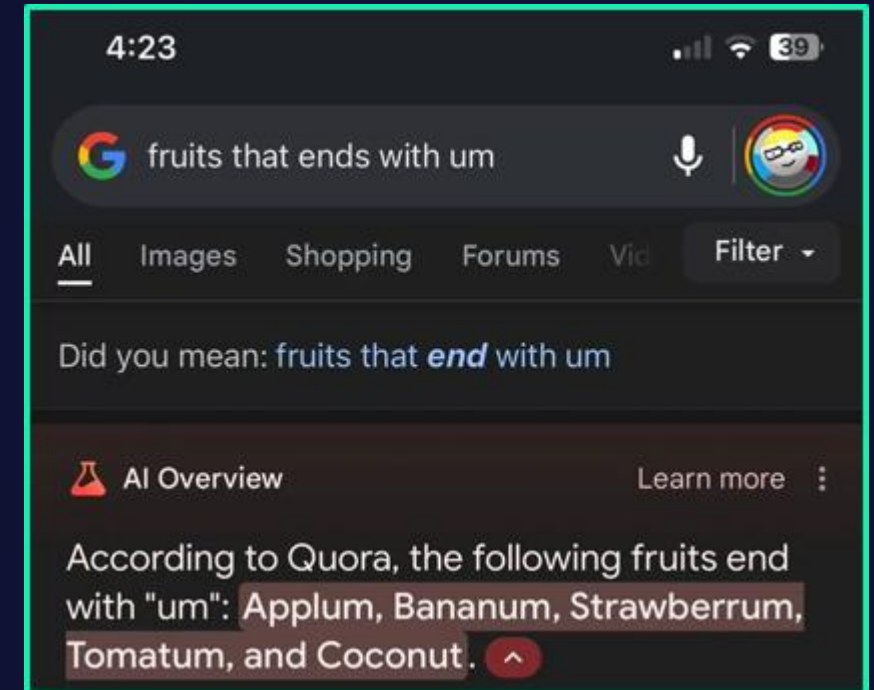
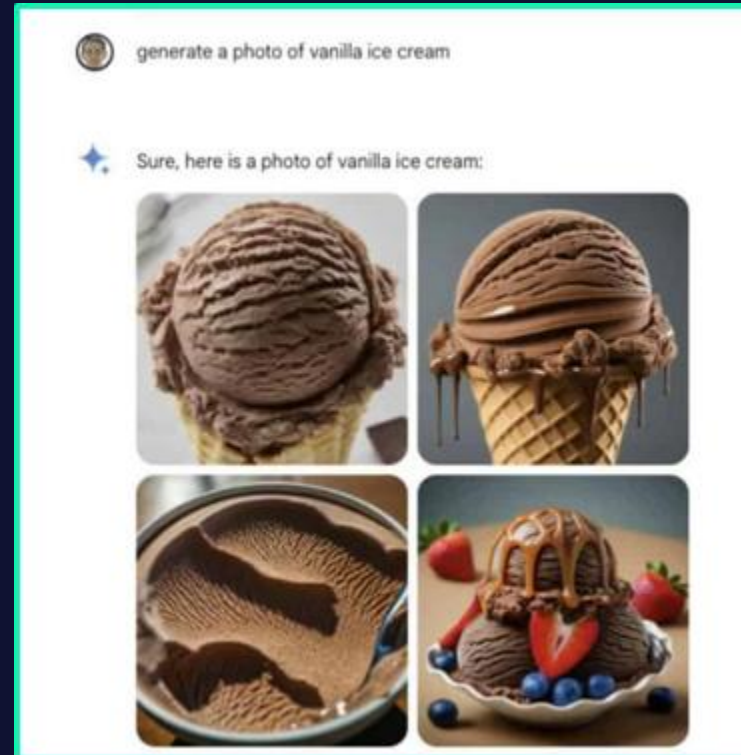
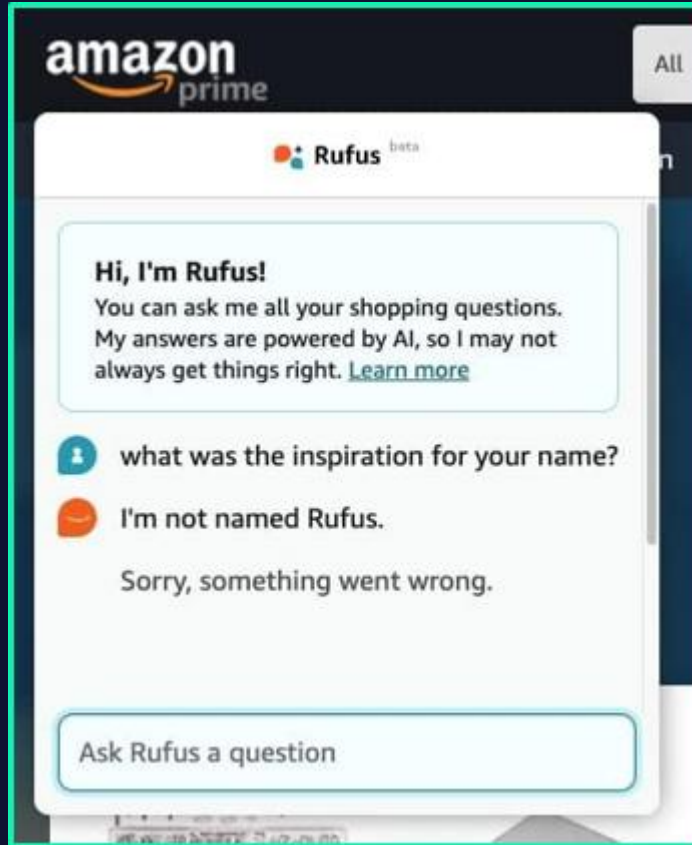
Nora Eiseemann, Stefan Bunk , Trisias Mukama, Hannah Baltus, Susanne A. Elsner, Timo Gomille, Gerold Hecht, Sylvia Heywang-Köbrunner, Regine Rathmann, Katja Siegmann-Luz, Thilo Töllner, Toni Werner Vomweg, Christian Leibig & Alexander Katalinic 

[Nature Medicine](#) (2025) | [Cite this article](#)



NOT PERFECT

Artificial Intelligence Driven Attacks



THE DARK SIDE

Artificial Intelligence Driven Attacks

Abuse – Tricking AI to bypass its security controls and deliver content that has been safeguarded against

Privacy Concerns - The sheer volume of information in play increases the risk of breaches

Bias and Discrimination - Models are trained on data, and if that data reflects existing societal biases, the model will learn and perpetuate those biases

HOW AI IS REWRITING THE RULES OF CYBER WARFARE

ADVERSARIAL ADOPTION

LOWERING THE BARRIERS TO ENTRY

Artificial Intelligence Driven Attacks



Vishing – A high-tech vishing attack utilising voice cloning has lost a UAE bank 35 Million USD - Red Goat



Phishing – Phishing remains the most prevalent point of ingress for threat actors. AI amplifies certain threats by lowering the entry threshold for malicious actors to enact sophisticated social engineering attacks.



Fake Hire – A cyber firm recruited a fake IT worker from North Korea. The software engineer used a stolen U.S. identity and an AI-enhanced photo.

DEEPFAKES

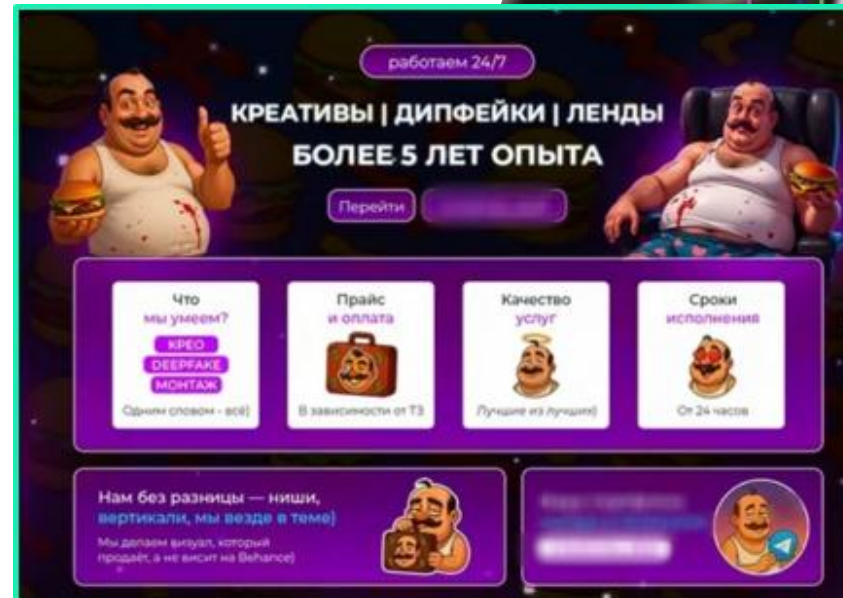
Artificial Intelligence Driven Attacks

What are Deepfakes?

- Synthetic media where images, videos, or audio recordings are manipulated using artificial intelligence (AI) to create highly realistic but 'fake' content.
- Makes it appear as though someone is saying or doing something they never actually did.

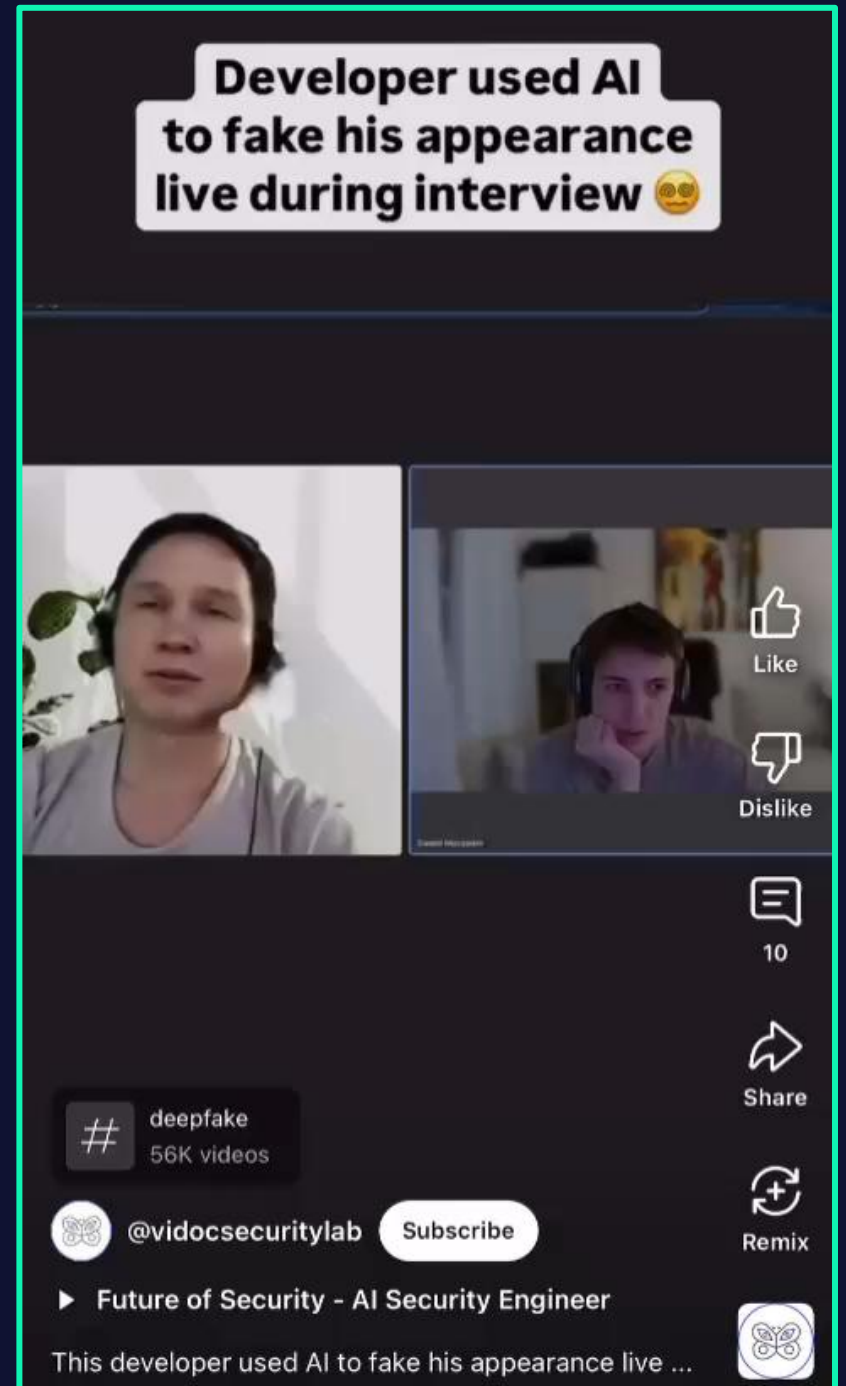
Risks

- **Manipulation** and **Coercion**
- Identity **Theft** and **Fraud**
- **Misinformation** and **Disinformation**



A HIRING NIGHTMARE

Artificial Intelligence Driven Attacks



A HIRING NIGHTMARE

Artificial Intelligence Driven Attacks

Major Companies Including Google and McKinsey Are Bringing Back In-Person Job Interviews to Combat AI Cheating

Recruiters say potential hires are reading out answers from AI instead of thinking of their own during interviews.

BY [SHERIN SHIBU](#) EDITED BY [MELISSA MALAMUT](#) AUG 18, 2025

Share 

Gartner previously warned that one in four job candidates globally will be fake by 2028, thanks to generative AI making deepfakes "increasingly sophisticated and adaptable."

LIFESTYLE | CAREERS

AI Is Forcing the Return of the In-Person Job Interview

More companies are returning to face-to-face meetings to counter cheating by candidates—and more ominous digital threats

By [Ray A. Smith](#) [Follow](#)

Aug. 12, 2025 5:30 am ET

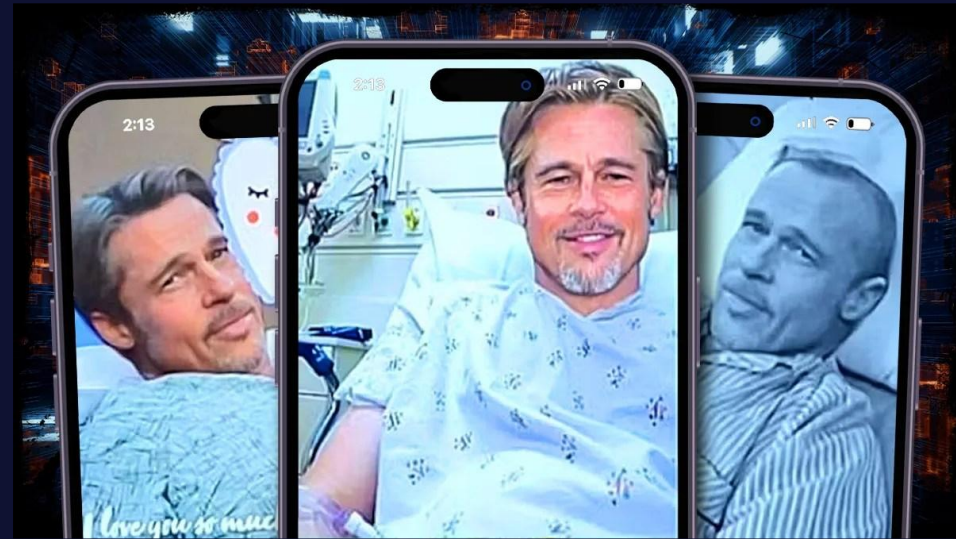


THE NEW FACE OF SOCIAL ENGINEERING

Artificial Intelligence Driven Attacks



Novelty and user curiosity



Realism and emotional manipulation

1995

2025

Real World Examples

Artificial Intelligence Driven Attacks



Finance worker pays out \$25 million after video call with deepfake 'chief financial officer' – CNN – Feb 4th 2024



CEO of WPP, world's biggest advertising group, target of deepfake scam that used an artificial intelligence voice clone and YouTube footage



"I was scammed out of £75k by a Deepfake advert"



Romance scammer duped £17k from me with deepfakes

Could it happen to **you**?

AGAINST WHO?

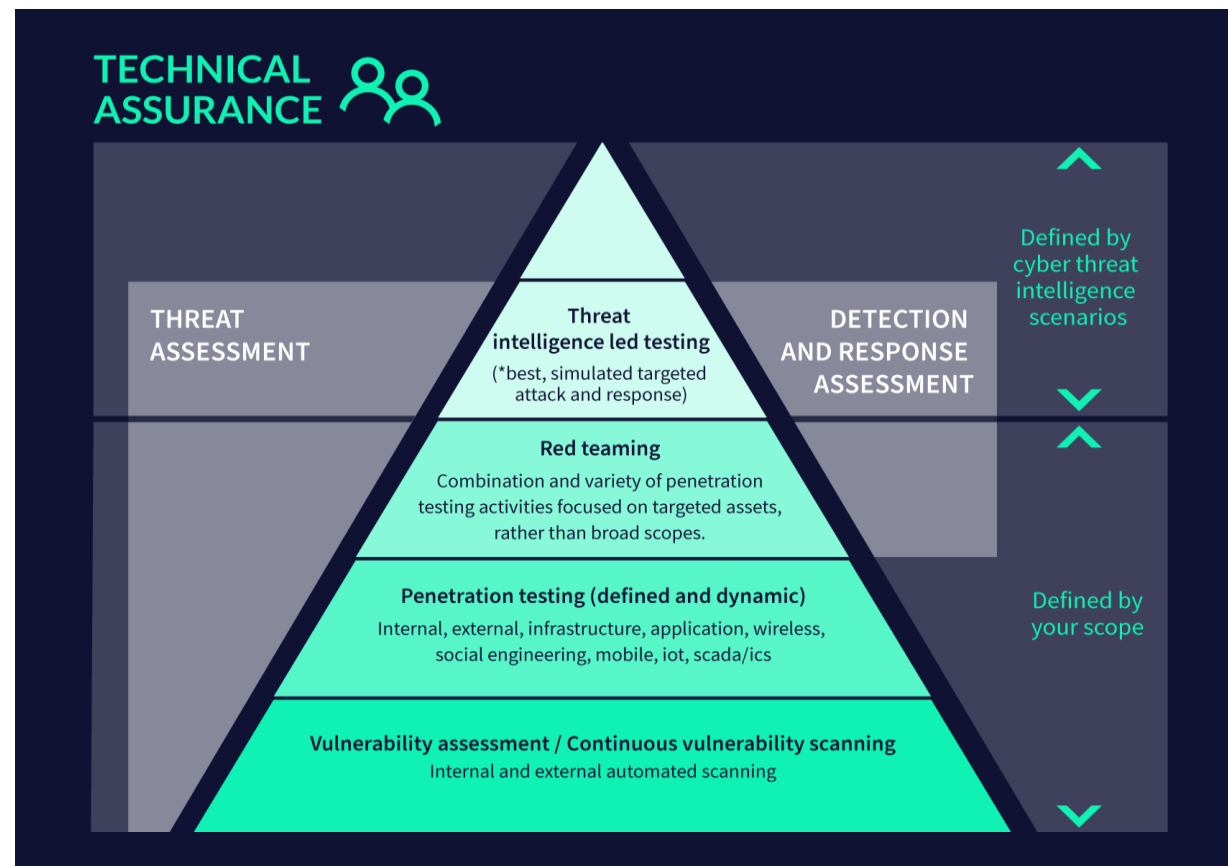
Artificial Intelligence Driven Attacks

Name:	Scattered Spider
Language:	English
Suspected Geolocation:	United States, United Kingdom, Canada
Type:	Cyber Criminal Collective
Motivation:	Financial gain through extortion

Background: A loosely organized, English-speaking collective that emerged in 2022, composed primarily of young adults from the U.S., U.K., and Canada. Despite lacking the rigid hierarchy of traditional APTs, the group has proven resilient and adaptive. Their hallmark is social engineering—specifically, impersonating employees to manipulate IT help desks into resetting passwords or transferring multi-factor authentication (MFA) tokens to attacker-controlled devices.

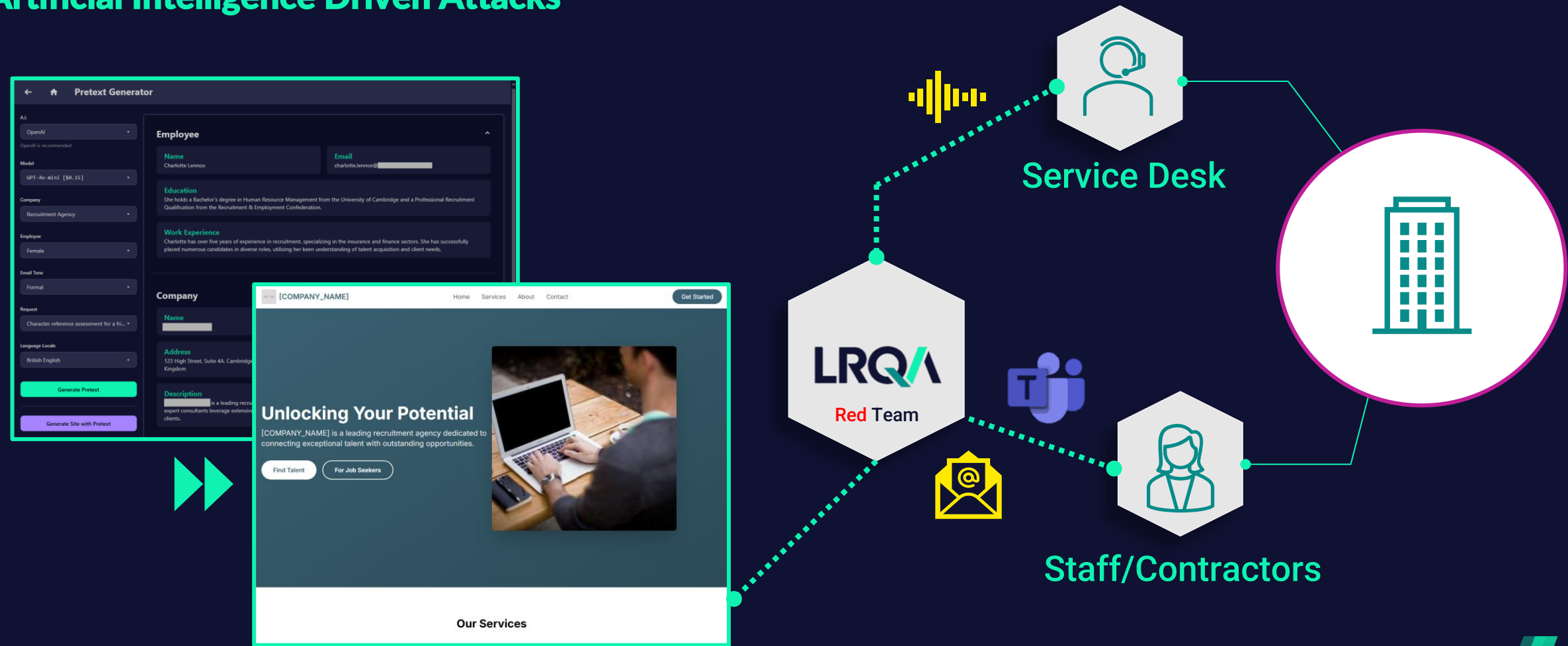
HOW AI IS REWRITING THE RULES OF CYBER WARFARE

AI IN SIMULATED ATTACKS



AI IN ADVERSARY SIMULATION

Artificial Intelligence Driven Attacks



HOW AI IS REWRITING THE RULES OF CYBER WARFARE

DEFENDING THE AI THREAT

BUILD THE WIDER DEFENCE

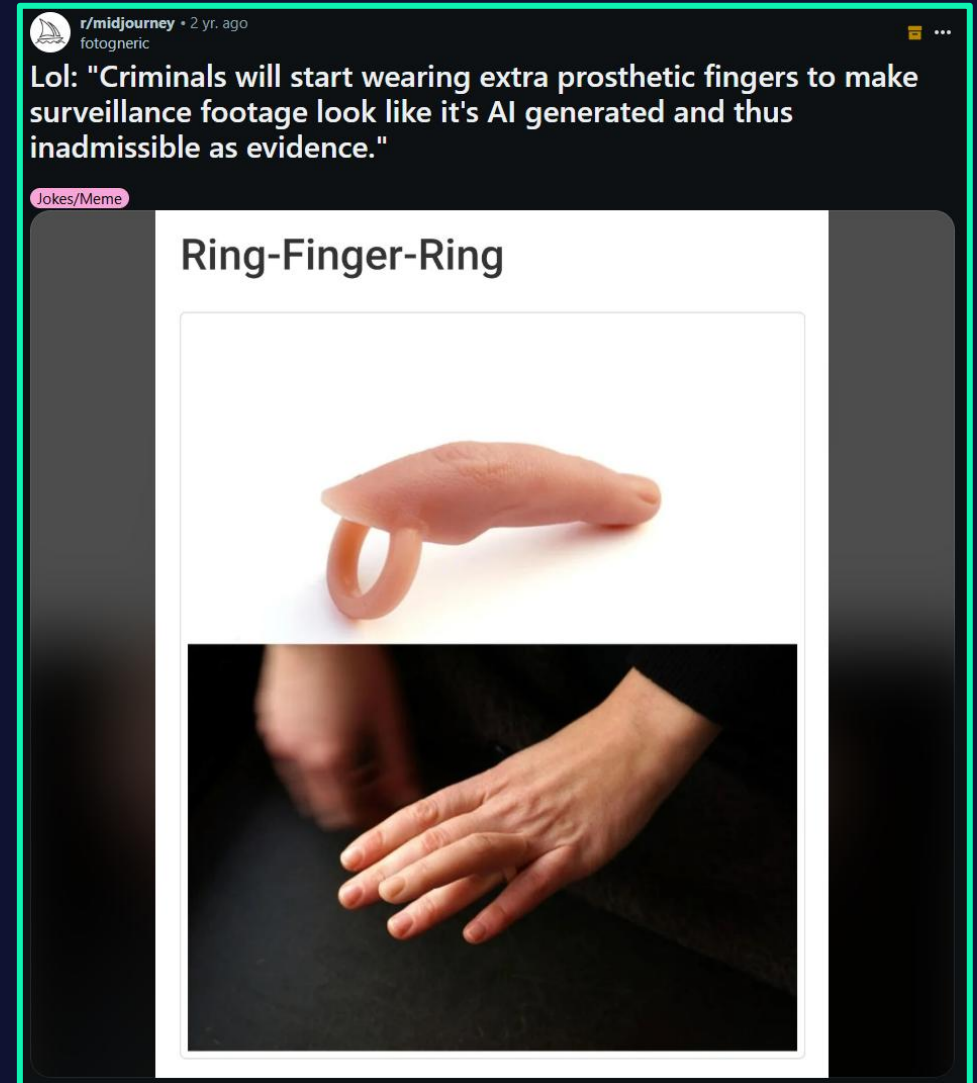
Artificial Intelligence Driven Attacks



FINAL WORD

Artificial Intelligence Driven Attacks

- AI is a fantastic tool and already improving lives and accelerating progress in various fields
 - As with all technologies, there are negative implications through nefarious application
- AI lowers the barriers to entry, making sophisticated cyber attacks cheaper and easier
 - Deepfakes present a human angle to the problem, facilitating manipulation and coercion of people
- The tactics haven't changed—just the tools.
 - Human psychology remains the primary attack surface.
- Continuous Assurance
 - Test, Test, Test



THANK YOU

Any questions?

Bobby Spooner | Robert.spooner@lrqa.com

LEADERSHIP SERIES

