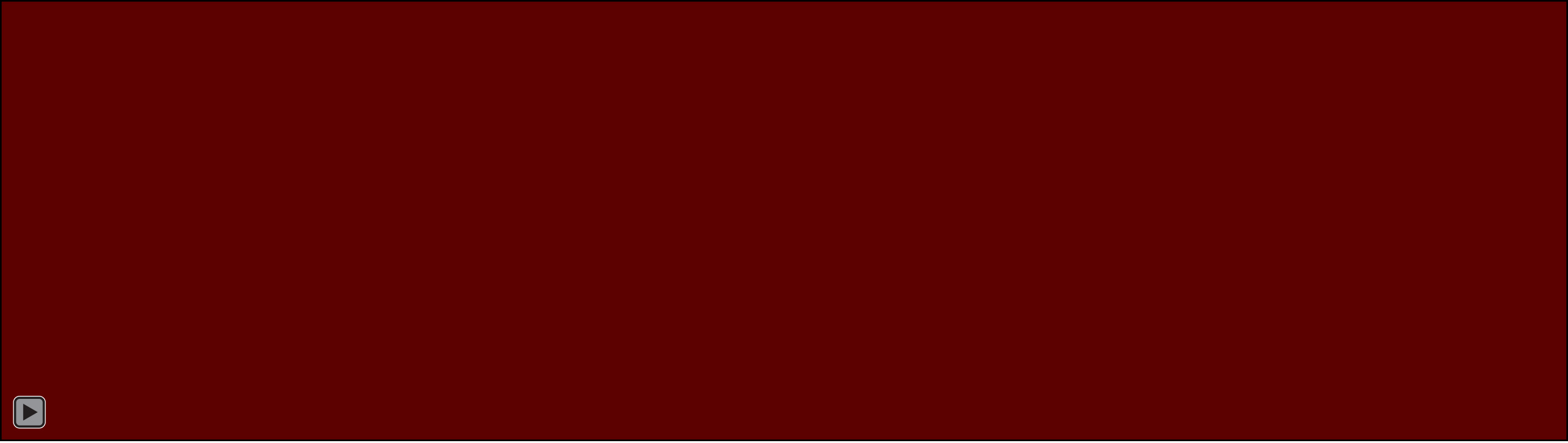


James Moore Technology Services

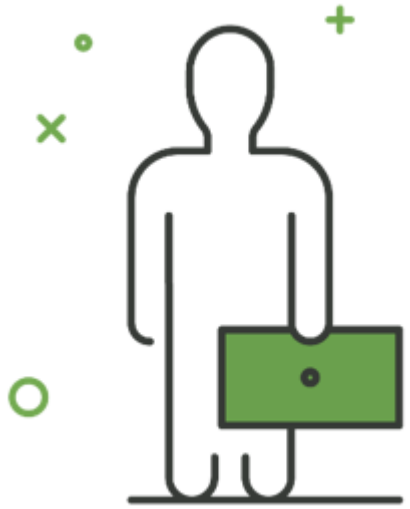
Cybersecurity in Finance: Hack-Proof your business

JAMESMOORE
TECHNOLOGY SERVICES

It is an early Saturday morning..

- I get a phone call from a New York finance institution
- Several user accounts were locked out, and one of their admin accounts was not accessible anymore
- Their cloud environment was fully breached
- The cause of the breach were several accounts with weak passwords, combined with human error allowing for MFA bypass
- The threat actors attempted to change the account number for an existing partner and pay themselves a large amount

I've seen a thing or two...

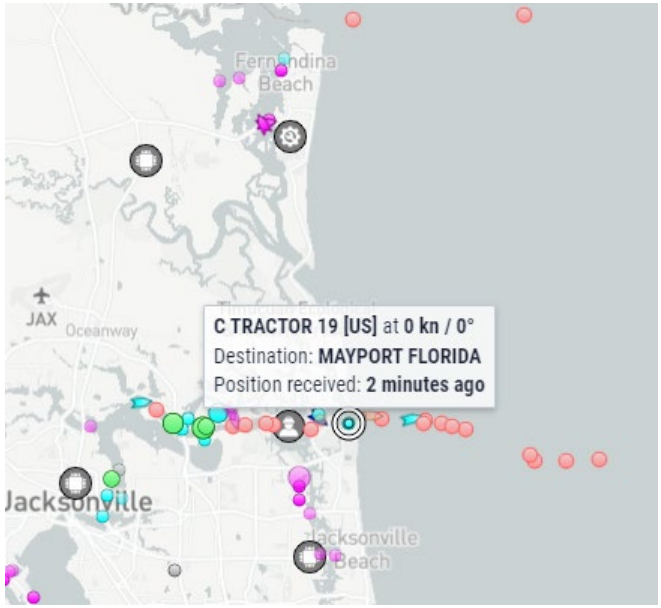


WIRED NEWS REPORT SCIENCE APR 30, 1998 1:15 PM

Ericsson Manages Net Telephony

Ericsson says its new IP telephony system will make it easier for telcos to get into voice on the Net.

ERICSSON SAYS IT has the system to give phone companies and corporate network administrators easier entry into shuttling their voice traffic over data networks.



Agenda

1

Introduction

2

Key takeaways

- The internet is a scary place
- Cybersecurity can be complicated
- But you only need to outrun your competition!

3

Finance Departments – Prime Targets

- Budget challenges for cybersecurity
- Source of valuable data
- Supported causes

4

Cyber attacks are evolving

- Ease of entry
- Speed
- Anyone is a target

5

Case Study:

- Finance Breach

6

AI and Cybersecurity

- AI defined
- Types of AI
- AI in Cybersecurity

7

How do you outrun your competition?

- Everyone plays a part
- Education and training
- Zero trust mentality

Key takeaways

Cybersecurity **attacks occurred every 39 seconds** in **2023**.

In **2024**, the total amount of **money received by ransomware** actors amounted to **$814 million.**

Organization	Impact of the Breach	Estimated Cost
Yahoo	Data of all 3 billion user accounts compromised (2013–2014)	$350 million (valuation drop)
Equifax	Personal data of 147 million people breached (2017)	$575 million+ (settlement)
Marriott International	Data of 500 million guests exposed (2014–2018)	$300+ million (fines & costs)
Sony Pictures	Sensitive data & unreleased films leaked, major business disruption (2014)	$100 million+
Target	Payment and personal data of 110 million customers stolen (2013)	$162 million+
Capital One	Data of 106 million customers exposed (2019)	$190 million+ (settlement)
Facebook (Meta)	533 million user records leaked (2021, from earlier scraping)	$276 million (fine by EU)
Uber	Data of 57 million users and drivers stolen (2016, disclosed 2017)	$148 million (settlement)
TJX Companies	94 million credit cards stolen (2007)	$162 million
eBay	145 million user records stolen (2014)	~$200 million (recovery est.)

The threat is real...

The internet is a scary place...

Cybersecurity Can Be Complicated

But you only need to outrun your competition!

Finance Departments Are Prime Targets!

JAMESMOORE
TECHNOLOGY SERVICES

Sector Challenges

Finance departments handle:

- **High-value** financial transactions
- **Sensitive** vendor and payroll data
- Access to **internal banking systems and credentials**
- **Invoices**, **tax IDs**, and **W-2** information

This makes the sector a very lucrative entry point for attackers aiming for direct financial gain or extortion leverag

Key Cyber Threats

Key Cyber Threats Targeting Finance Departments:

- **Business Email Compromise (BEC)**
  - **Tactic:** Impersonation of CFOs or vendors to redirect wire transfers
  - **Example:** According to the FBI IC3 Report 2023, BEC scams cost businesses $2.9 billion in the U.S. alone in 2023.
  - **Target:** Often begins with finance staff being socially engineered via spoofed or compromised emails.
- **Ransomware**
  - **Tactic:** Encrypt finance records or systems (like QuickBooks, SAP, or Oracle Financials), then demand ransom.
  - **Example:** In the 2021 Accellion breach, financial documents were stolen from dozens of companies. Victims received ransom threats demanding payment to prevent public leaks.
  - **Validation:** The Verizon DBIR 2023 shows ransomware is involved in 24% of all breaches, with finance-related departments being disproportionally affected.
- **Invoice Fraud**
  - **Tactic:** Manipulate legitimate invoices or spoof them to reroute payments.
  - **Example:** The Scoular Co. breach (2014) saw the company lose $17 million to a fake email appearing to be from the CEO, requesting wire transfers for an acquisition.
  - **Trend:** Financial teams are often targeted due to routine handling of large vendor payments.
- **Credential Harvesting / Phishing**
  - **Tactic:** Fake finance software login pages (like Xero, NetSuite, SAP).
  - **Data:** Proofpoint's 2023 report shows finance staff are 2x more likely to be phished than other departments.

Impact of finance breaches

- **Financial Losses**: Direct theft or ransom payments
- **Operational Disruption**: Payroll halted; accounting systems disabled
- **Reputation Damage**: Breached trust with vendors, clients, regulators
- **Compliance Fines**: Violations of SOX, PCI-DSS, GDPR, etc.

Company	Incident	Finance Dept. Targeted?	Cost
Scoular (2014)	CEO impersonation led to $17M transferred fraudulently	✅ Yes	$17 million
Toyota Boshoku (2019)	Executive spoofed, finance staff wired $37M to attackers	✅ Yes	$37 million
Maersk (NotPetya)	Financial systems (SAP) encrypted; operations disrupted	✅ Yes	$200–300 million
Colonial Pipeline (2021)	Ransomware encrypted finance + billing systems	✅ Yes	$4.4 million ransom paid

Defense Recommend-ations

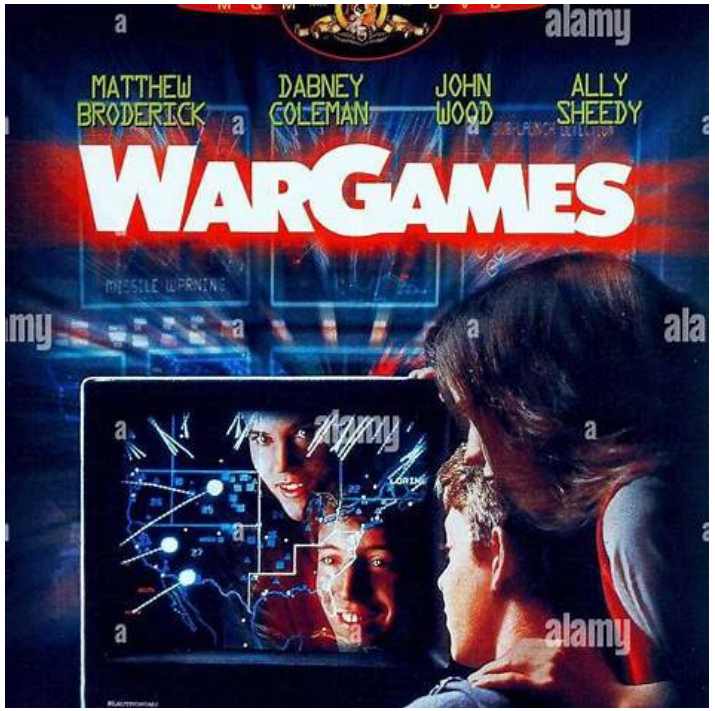
Defense Recommendations (For CISOs and CFOs)

- **Multi-Factor Authentication (MFA)** for finance software and email accounts.
- **Segregation of Duties** – no single person should approve & execute payments.
- **Out-of-Band Verification** – always confirm wire changes via phone/video.
- **AI-powered Email Filtering** – detect BEC and invoice spoofing patterns.
- **Security Awareness Training** – simulate phishing against finance roles.
- **Incident Response Plan** tailored for finance-related ransomware/extortion.

Be Alert, not alarmed

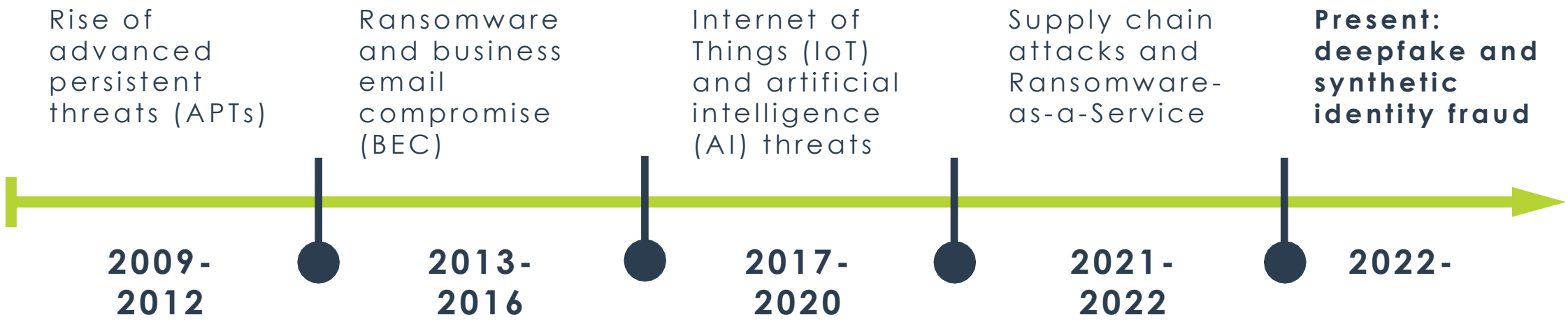
January 2020:
Criminals used deep voice technology to simulate the voice of the director of a transnational company. Through various calls with the branch manager of a bank based in the United Arab Emirates, criminals were able to steal $35 million that were deposited into several bank accounts, making the branch manager of the bank believe that the funds will be used for the acquisition of another company.[Footnote23]

Cyberattacks are evolving



Anyone remember these times?

JAMESMOORE
TECHNOLOGY SERVICES



Cyberattacks are evolving

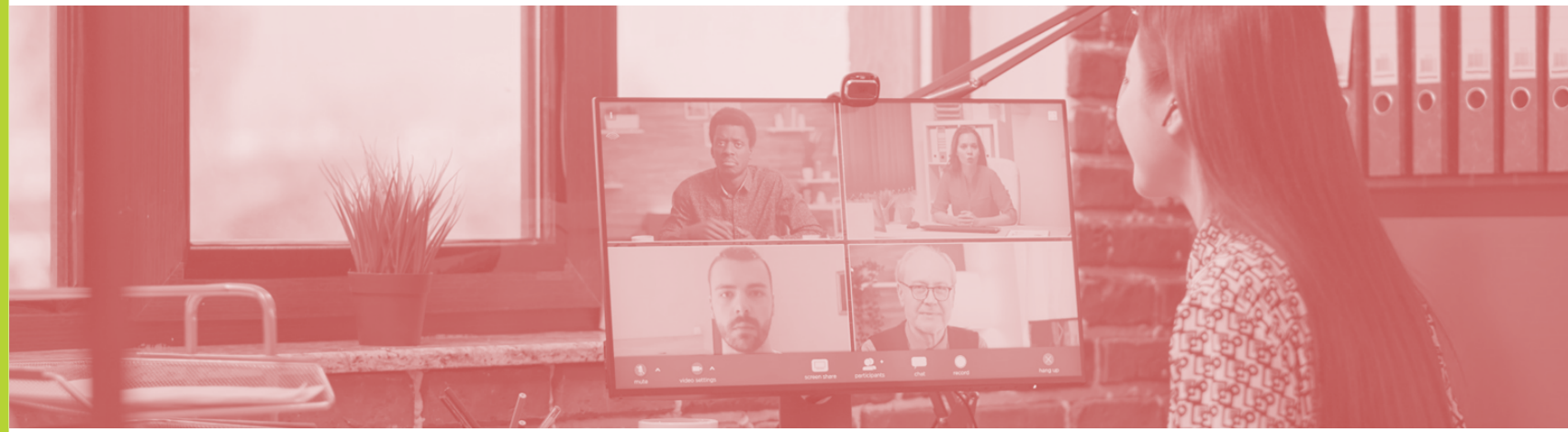
- Ease of entry
- Speed
- Anyone is a target

Case Study 2023
Ransomware Attack
City of Dallas

JAMESMOORE
TECHNOLOGY SERVICES

Incident Summary

- **Date of Attack:** May 2023
- **Attack Type:** Ransomware (Royal Ransomware Group)
- **Targeted Systems:** Police, courts, and **financial operations**, including payroll and payment processing



Sequence of Events

- **Entry Point:** Likely via phishing or exploitation of a known vulnerability (exact vector undisclosed).
- **Lateral Movement:** Attackers moved laterally through city networks, reaching **financial databases and systems**.
- **Finance Dept. systems were encrypted**
- **Payroll was delayed** for hundreds of city employees
  - Vendor payments and budget systems were disrupted
  - Sensitive financial records (e.g., W-2s, invoices, PII) were **exfiltrated and leaked**
- **Extortion Strategy:**
  - Royal Ransomware threatened to **leak stolen data** unless a ransom was paid.
  - Sample data included **tax documents**, vendor banking details, and internal finance emails

Recovery and Impact

- **Estimated Recovery Cost:** $8–10 million (as of late 2023)
- **Downtime:** Weeks of disrupted services, including financial disbursements.
- **Public Disclosure:** Widespread media coverage and damage to public trust

Lessons Learned

Lessons Learned for Government Finance Teams

- **Legacy Risk:** Many public finance systems (e.g., Oracle, SAP, PeopleSoft) are **under-patched and poorly segmented.**
- **Data Classification:** Governments need to **label and** isolate financial PII and tax data.
- **Ransomware Resilience: Regular backups** and **simulated recovery** processes are essential.
- **Cyber Insurance Complexity:** The City struggled with **policy limits** and **coverage debates**—highlighting the need for **tailored public-sector policies**.

AI and Cybersecurity

JAMESMOORE
TECHNOLOGY SERVICES

About James Moore

January 2020:
Criminals used **deep voice technology** to simulate the **voice of the director** of a transnational company. Through various calls with the branch manager of a bank based in the United Arab Emirates, criminals were able to **steal $35 million** that were deposited into several bank accounts, making the branch manager of the bank believe that the funds will be used for the acquisition of another company.Footnote23

What is Artificial Intelligence (AI)

Artificial Intelligence (AI) refers to the ability of computer systems to perform tasks that typically require human intelligence, such as learning, problem-solving and decision-making.

- **Key Concepts:**
- **Learning:** AI systems can learn from data and improve their performance over time.
- **Problem-solving:** AI can be used to develop solutions to complex problems by analyzing data and identifying patterns.
- **Decision-making:** AI can make decisions based on available information and can be programmed to make predictions or recommendations.

What is AI (continued)?

Examples of AI applications:

- **Machine learning:** Using algorithms to allow computers to learn from data without being explicitly programmed.
- **Natural language processing:** Enabling computers to understand and generate human language.
- **Computer vision:** Allowing computers to "see" and interpret images.
- **Robotics:** Creating robots that can perform tasks autonomously.

Types of AI:

- **Reactive Machines**
  - **Behavior:** Responds to specific inputs with programmed responses; no memory.
  - **Example:** IBM's Deep Blue chess computer.
- **Limited Memory**
  - **Behavior:** Can use past data for a short period to make decisions.
  - **Example**: Most modern AI like self-driving cars.
- **Theory of Mind**
  - **Behavior:** Hypothetical AI that can understand emotions, beliefs, and intentions.
  - **Goal:** Improved human-AI interaction. Still under research.
- **Self-Aware AI**
  - **Behavior:** AI with consciousness, self-awareness, and understanding of its own existence.
  - **Status:** Purely theoretical for now.

AI solutions and tools

AI Assistants (Chatbots)

- **ChatGPT:** A versatile language model for various tasks, including writing, coding, and answering questions.
- **Claude:** Another powerful language model, known for its ability to generate human-like text.
- **Gemini:** Google's AI model, capable of handling complex tasks and generating different content formats.
- **DeepSeek:** A language model focused on research and development.
- **Grok**: An AI assistant that can access and process real-time information.

Video Generation and Editing

- **Synthesia:** A platform for creating AI-generated videos.
- **Runway:** An AI-powered video editing tool with creative capabilities.
- **Filmora:** A popular video editing software with AI-assisted features.
- **OpusClip:** An AI tool for creating short-form videos.

Image Generation

- **GPT-4o:** A multimodal AI model that can process text and images.
- **Midjourney:** A popular AI tool for generating images from text prompts.

Other Notable AI Tools:

- Iguazio: A platform for accelerating MLOps.
- DataRobot: A platform for automated machine learning.
- OpenAI: A research-driven AI company known for its models.
- Keras: A deep learning model flexibility platform.
- TensorFlow: A free and open-source software library designed for machine learning and artificial intelligence applications.
- PyTorch: A popular open-source machine learning framework.
- scikit-learn: A library for machine learning tasks.
- Google AI Studio: A platform for integrating Gemini models into apps.
- NotebookLM: A personalized AI assistant that surfaces insights and provides Audio Overviews on data you upload.
- Translation Basic: Translate and localize text in real time with support for 100+ language pairs.
- Translation Advanced: Translation support for batch text and formatted documents, custom models, and romanized text.
- Perplexity: A search engine that provides high-quality answers and quotes sources.
- Jasper: An AI content creation platform for enterprise marketing teams.
- Bardeen: An AI-powered automation tool that enhances productivity by streamlining workflows.
- Notion AI: An AI tool for note-taking and knowledge management.
- Mem: An AI tool for organized notes.

AI used in Cybercrime

AI is increasingly used by cybercriminals to enhance their attacks, automating processes, creating more sophisticated phishing campaigns, and even enabling new types of attacks like deepfakes and voice cloning, while also being used by cybersecurity professionals to detect and defend against these threats. [1, 2, 3, 4]

Automation and Efficiency:

- AI algorithms can automate various stages of cyberattacks, including reconnaissance, phishing campaigns, malware development, and credential stuffing, allowing criminals to operate faster and with less manual effort. [2, 5, 6, 7]

Sophisticated Phishing and Social Engineering:

- AI can be used to create highly personalized and convincing phishing emails and messages, making it harder for victims to identify them as malicious. [3, 5, 8]

Deepfakes and Voice Cloning:

- AI-powered deepfake technology can be used to create realistic fake videos and audio recordings, enabling cybercriminals to impersonate trusted individuals or organizations and manipulate victims. [1, 3, 9, 10]

Malware Development:

- AI can be used to develop new and sophisticated malware, including adaptive malware that can change its code to evade detection. [11, 12]

Exploiting Vulnerabilities:

- AI can be used to identify and exploit vulnerabilities in systems and networks, allowing criminals to gain unauthorized access. [2, 13]

Data Poisoning

- AI can also be used to poison data sets used for training AI models, leading to the models making incorrect predictions and decisions. [3]

Credential Stuffing

- AI can automate credential stuffing attacks by systematically testing stolen username-password pairs across multiple online accounts. [5]

Language Translation

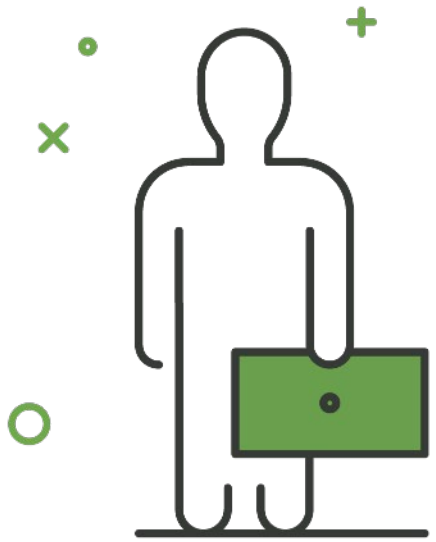
- AI can be used to translate phishing emails and other malicious content into multiple languages, enabling criminals to target a wider audience. [6]

AI Used in Cybersecurity

AI is increasingly used by cybercriminals to enhance their attacks, automating processes, creating more sophisticated phishing campaigns, and even enabling new types of attacks like deepfakes and voice cloning, while also being used by cybersecurity professionals to detect and defend against these threats. [1, 2, 3, 4]

- **Threat Detection and Prevention:**
  - AI can be used to analyze vast amounts of data and identify suspicious patterns and anomalies, helping cybersecurity professionals detect and prevent cyberattacks. [4, 14, 15]
- **Vulnerability Scanning:**
  - AI can automate vulnerability scanning and identification, helping organizations identify and remediate potential weaknesses in their systems and networks. [13]
- **Fraud Detection:**
  - AI can be used to detect and prevent fraudulent activities, such as identity theft and financial fraud. [15, 16, 17]
- **Intrusion Detection:**
  - AI can be used to detect and respond to real-time cyberattacks, helping organizations protect their systems and data. [4, 14]
- **Incident Response:**
  - AI can be used to analyze and respond to cyber incidents, helping organizations contain damage and prevent future attacks. [4]
- **AI-powered security tools**
  - Cybersecurity organizations are increasingly relying on AI to help flag suspicious data and detect or thwart attacks [2] [3]

Sources



[1] https://www.fbi.gov/contact-us/field-offices/sanfrancisco/news/fbi-warns-of-increasing-threat-of-cyber-criminals-utilizing-artificial-intelligence

[2] https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/ai-powered-cyberattacks/

[3] https://www.morganstanley.com/articles/ai-cybersecurity-new-era

[4] https://www.balbix.com/insights/artificial-intelligence-in-cybersecurity/

[5] https://www.nyu.edu/life/information-technology/safe-computing/protect-against-cybercrime/ai-assisted-cyberattacks-and-scams.html

[6] https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/back-to-the-hype-an-update-on-how-cybercriminals-are-using-genai

[7] https://cltc.berkeley.edu/2025/01/16/beyond-phishing-exploring-the-rise-of-ai-enabled-cybercrime/

[8] https://www.criticalstart.com/ai-evolution-in-cybercrime-threats-and-deceptive-tactics/

[9] https://cpl.thalesgroup.com/blog/data-security/scary-cyber-creatures

[10] https://blog.barracuda.com/2024/04/19/5-ways-cybercriminals-are-using-ai--deepfakes

[11] https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat

[12] https://blog.coursera.org/how-ai-is-changing-cybercrime-and-cybersecurity/

[13] https://www.snowflake.com/guides/ai-cybersecurity/

[14] https://onlinedegrees.uwf.edu/articles/cybersecurity-and-ai/

[15] https://datadome.co/learning-center/ai-fraud-detection/

[16] https://www.signicat.com/blog/ai-identity-fraud-real-time-detection-and-prevention-strategies

[17] https://www.okta.com/identity-101/fraud-detection/

[-] https://www.nyu.edu/life/information-technology/safe-computing/protect-against-cybercrime/ai-assisted-cyberattacks-and-scams.html

So how do you outrun the competition?

JAMESMOORE
TECHNOLOGY SERVICES

Back to Key Takeaways

Assume breach

- Plan out what to do **WHEN** it happens
- Build your solutions with the assumption that **you will be breached**

Engage your workforce

- **Continuous** training
- Recurring **phishing training** campaigns

Get eyes on the prize

- Make sure you **log events**
- Have someone **monitoring logs and events**

Basics in place

- Timely **patching**
- Secure **backups**
- **Endpoint Security**

Zero trust

- **MFA**
- **Tiering**
- **ZeroTrust** Endpoint Security

Robert H Morris

(Cryptographer at Bell Labs and NSA)

"The three golden rules to ensure computer security are:

- *do not own a computer*
- *do not power it on*
- *do not use it."*

QUESTIONS