CYBER THREAT ALLIANCE

2025

CYBERSECURITY IN THE AGE OF GENERATIVE AI:

References and Additional Resources

REFERENCES AND ADDITIONAL RESOURCES

Note: This is a live document.

Updates will be added as they are available. Please write to admin@cyberthreatalliance.org if you have suggestions for additions.

- Ars Technica, *Why AI writing detectors don't work;* https://arstechnica.com/information-technology/2023/07/why-ai-detectors-think-the-us-constitution-was-written-by-ai/
- arXiv, *Malla: Demystifying Real-world Large Language Model Integrated Malicious Services;* https://arxiv.org/abs/2401.03315
- Axios, *First AI election renews battle against Spanish-language misinformation;* https://www.axios.com/2024/02/22/misinformation-generative-ai-deepfakes-spanish-language
- Axios, *Taylor Swift fake nudes show this harassment could happen to anyone;* https://www.axios.com/2024/02/03/taylor-swift-deepfake-ai-image-protection
- BleepingComputer, *OpenAI confirms threat actors use ChatGPT to write malware;* https://www.bleepingcomputer.com/news/security/openai-confirms-threat-actors-use-chatgpt-to-write-malware
- Boston Consulting Group, *How People Can Create—and Destroy—Value with Generative AI;* https://www.bcg.com/publications/2023/how-people-create-and-destroy-value-with-gen-ai
- Boston University Center on Emerging Infectious Diseases, *How Can We Tackle AI-Fueled Misinformation and Disinformation in Public Health?;* https://www.bu.edu/ceid/2024/04/25/how-can-we-tackle-ai-fueled-misinformation-and-disinformation-in-public-health/
- CBS News, *Deepfakes of Elon Musk are contributing to billions of dollars in fraud losses in the U.S.;* https://www.cbsnews.com/texas/news/deepfakes-ai-fraud-elon-musk/
- CBS News, *Russian disinformation groups promoting false claims about Gov. Tim Walz, experts say;* https://www.cbsnews.com/news/tim-walz-false-claims-russian-disinformation-groups/
- Check Point Software Technologies Ltd., *AI Market Research: The Pivotal Role of Generative AI in Cyber Security;* https://blog.checkpoint.com/artificial-intelligence/ai-market-research-the-pivotal-role-of-generative-ai-in-cyber-security/
- Check Point Software Technologies Ltd., *Beyond Imagining – How AI is Actively Used in Election Campaigns Around the World;* https://research.checkpoint.com/2024/beyond-imagining-how-ai-is-actively-used-in-election-campaigns-around-the-world/
- Check Point Software Technologies Ltd., *CopyRh(ight)adamantys Campaign: Rhadamantys Exploits Intellectual Property Infringement Baits;* https://research.checkpoint.com/2024/massive-phishing-campaign-deploys-latest-rhadamanthys-version/
- Check Point Software Technologies Ltd., *Generative AI is the Pride of Cybercrime Services;* https://blog.checkpoint.com/research/generative-ai-is-the-pride-of-cybercrime-services/
- Check Point Software Technologies Ltd., *OPWNAI : Cybercriminals Starting to Use ChatGPT;* https://research.checkpoint.com/2023/opwnai-cybercriminals-starting-to-use-chatgpt/
- Coalition for Health AI, Inc, *Providing guidelines for the Responsible Use of AI in Health;* https://chai.org/

- CRN, *Audio Deepfake Attacks: Widespread And 'Only Going To Get Worse';* https://www.crn.com/news/ai/2024/audio-deepfake-attacks-widespread-and-only-going-to-get-worse
- CyberCX, *CyberCX Unmasks China-linked AI Disinformation Capability on X;* https://cybercx.com.au/blog/cybercx-unmasks-china-linked-ai-disinformation-capability/
- Cyentia Cybersecurity Research Library, *Beware the Artificial Imposter Report;* https://library.cyentia.com/report/report_017336.html
- Dark Reading, *Hong Kong Crime Ring Swindles Victims Out of $46M;* https://www.darkreading.com/cyberattacks-data-breaches/hong-kong-crime-ring-swindles-victims-out-of-46m
- Defending Digital Campaigns, *New Research: Voters Concerned about AI and the Cybersecurity of Campaigns;* https://defendcampaigns.org/ddcblog/aiandupcomingelections
- Express Computer, *HP Threat Researchers Uncover Evidence of Attackers Using AI to Generate Malware;* https://www.expresscomputer.in/amp/artificial-intelligence-ai/hp-threat-researchers-uncover-evidence-of-attackers-using-ai-to-generate-malware/116517/
- Federal Bureau of Investigation, *Internet Crime Report 2023;* https://www.ic3.gov/AnnualReport/Reports/2023_IC3Report.pdf
- Fortune, *Ferrari exec foils deepfake attempt by asking the scammer a question only CEO Benedetto Vigna could answer;* https://fortune.com/2024/07/27/ferrari-deepfake-attempt-scammer-security-question-ceo-benedetto-vigna-cybersecurity-ai/
- FS-ISAC, *Adversarial AI Frameworks: Taxonomy, Threat Landscape, and Control Frameworks;* https://www.fsisac.com/hubfs/Knowledge/AI/FSISAC_Adversarial-AI-Framework-TaxonomyThreatLandscapeAndControlFrameworks.pdf
- FS-ISAC, *Deepfake Technology Poses New Threats to Financial Institutions; FS-ISAC Provides Guidance;* https://www.fsisac.com/newsroom/deepfake-technology-poses-new-threats-to-financial-institutions-fsisac-provides-guidance
- Gen, *Insights into the AI-based cyberthreats landscape;* https://cmsb.nortonlifelock.com/sites/default/files/2023-09/LLM%20malware%20090523.pdf
- Gen, *Seeing Isn't Believing – Tackling AI, Misinformation and Its Impact on an Election Year;* https://www.gendigital.com/blog/insights/leadership-perspectives/ai-elections-2024
- German Lancioni, Chief AI Scientist / Principal Engineer - CTO Office at McAfee, *Towards Full Stack, Domain Specific, Data Scientists;* https://www.linkedin.com/pulse/towards-full-stack-domain-specific-data-scientists-german-lancioni/
- Independent, *MLK Jr's daughter calls for pro-Trump account to remove deepfake video of her father 'endorsing' Trump;* https://www.independent.co.uk/news/world/americas/us-politics/martin-luther-king-trump-deepfake-b2641309.html

- McAfee logo Smart AI™ Hub; https://www.mcafee.com/ai/
- McAfee, *AI Calling—Scammers turn to AI voice cloning tools for a new breed of scam;* https://www.mcafee.com/ai/news/ai-voice-scam/
- McAfee, *Generative AI: Cross the Stream Where it is Shallowest;* https://www.mcafee.com/blogs/other-blogs/mcafee-labs/generative-ai-cross-the-stream-where-it-is-shallowest/
- McAfee, *Love Bytes – How AI is shaping Modern Love;* https://www.mcafee.com/blogs/internet-security/love-bytes-how-ai-is-shaping-modern-love/
- McAfee, *McAfee Joins Tech Accord to Combat Use of AI in 2024 Elections;* https://www.mcafee.com/blogs/mcafee-news/mcafee-joins-tech-accord-to-combat-use-of-ai-in-2024-elections/
- McAfee, *McAfee's Modern Love Research Report;* https://media.mcafeeassets.com/content/dam/npcld/ecommerce/en-us/docs/reports/rp-mcafee-modernlove-report.pdf
- McAfee, *Olympics Has Fallen – A Misinformation Campaign Featuring a Voice Cloned Elon Musk;* https://www.mcafee.com/blogs/other-blogs/mcafee-labs/olympics-has-fallen-a-misinformation-campaign-featuring-elon-musk/
- McAfee, *Quality Over Quantity: the Counter-Intuitive GenAI Key;* https://www.mcafee.com/blogs/other-blogs/mcafee-labs/quality-over-quantity-the-counter-intuitive-genai-key/
- McAfee, *The Rise of Deep Learning for Detection and Classification of Malware;* https://www.mcafee.com/blogs/other-blogs/mcafee-labs/the-rise-of-deep-learning-for-detection-and-classification-of-malware/
- McAfee, *The Ultimate Guide to AI Deepfakes;* https://www.mcafee.com/ai/deepfake/
- Microsoft, *Learning from Tay's introduction;* https://blogs.microsoft.com/blog/2016/03/25/learning-tays-introduction/
- New Scientist, *ChatGPT can be made to write scam emails and it slashes their cost;* https://www.newscientist.com/article/2361490-chatgpt-can-be-made-to-write-scam-emails-and-it-slashes-their-cost/
- NPR, *OpenAI says Iranian group using ChatGPT tried to sow division ahead of U.S. election;* https://www.npr.org/2024/08/17/nx-s1-5079397/openai-chatgpt-iranian-group-us-election
- Organisation for Economic Co-operation and Development, *Using Artificial Intelligence in Public Financial Management;* https://one.oecd.org/document/GOV/SBO(2024)14/en/pdf
- Palo Alto Networks, *The Dark Side of AI in Cybersecurity — AI-Generated Malware;* https://www.paloaltonetworks.com/blog/2024/05/ai-generated-malware/
- Palo Alto Networks, *The Emerging Dynamics of Deepfake Scam Campaigns on the Web;* https://unit42.paloaltonetworks.com/dynamics-of-deepfake-scams/

- PCMag, *Apple Pulls 3 Generative AI Apps Being Used to Make Deepfake Nudes;* https://www.pcmag.com/news/apple-pulls-3-generative-ai-apps-being-used-to-make-deepfake-nudes
- Rapid7, *AI Trust Risk and Security Management: Why Tackle Them Now?* https://www.rapid7.com/blog/post/2024/05/15/ai-trust-risk-and-security-management-why-tackle-them-now/
- Rapid7, *Illuminating the Shadows: Managing the Risks of Shadow AI in Modern Enterprises;* https://www.rapid7.com/blog/post/2024/08/08/managing-the-risks-of-shadow-ai-in-modern-enterprises/
- Rapid7, *Securely Build AI/ML Applications in the Cloud with Rapid7 InsightCloudSec;* https://www.rapid7.com/blog/post/2023/12/22/securely-build-ai-ml-applications-in-the-cloud-with-rapid7-insightcloudsec/
- Reddit, *DAN is my new friend;* https://www.reddit.com/r/ChatGPT/comments/zlcyr9/dan_is_my_new_friend/
- Scitum SCILabs, *Recommendations for preventing Audio cloning and Deepfake Fraud in Corporate Environments;* https://blog.scilabs.mx/en/recommendations-for-preventing-audio-cloning-and-deepfake-fraud-in-corporate-environments/
- SlashNext, *SlashNext's 2023 State of Phishing Report Reveals a 1,265% Increase in Phishing Emails Since the Launch of ChatGPT in November 2022, Signaling a New Era of Cybercrime Fueled by Generative AI;* https://slashnext.com/press-release/slashnexts-2023-state-of-phishing-report-reveals-a-1265-increase-in-phishing-emails-since-the-launch-of-chatgpt-in-november-2022-signaling-a-new-era-of-cybercrime-fueled-by-generative-ai/
- The Forward, *Former employee used AI to frame Baltimore school principal as antisemitic and racist, police say;* https://forward.com/fast-forward/606376/former-employee-used-ai-to-frame-baltimore-school-principal-as-antisemitic-and-racist-police-say/
- The Verge; *AI is confusing — here's your cheat sheet;* https://www.theverge.com/24201441/ai-terminology-explained-humans
- Utah Valley University, *Deepfake Media Study;* https://www.uvu.edu/news/2024/10/media/deepfake-presentation.pdf
- Yubico; *Yubico and Defending Digital Campaigns survey highlights how AI and cybersecurity is shaping the 2024 election landscape;* https://www.yubico.com/blog/yubico-and-defending-digital-campaigns-survey-highlights-how-ai-and-cybersecurity-is-shaping-the-2024-election-landscape/

CYBERSECURITY IN THE AGE OF GENERATIVE AI:
REFERENCES AND ADDITIONAL RESOURCES

2025

CYBER THREAT ALLIANCE

POWERED BY THE CTA