**Artificial Intelligence and cybercrime: implications for individuals and the healthcare sector – Scott Monteith et al.**

Supplemental References

Akhtar N, Mian A, Kardan N, Shah M. Advances in adversarial attacks and defenses in computer vision: A survey. IEEE Access. 2021 Nov 12;9:155161-96.

Aminifar A. Universal adversarial perturbations in epileptic seizure detection. In2020 International Joint Conference on Neural Networks (IJCNN) 2020 Jul 19 (pp. 1-6). IEEE.

Brooks C, Lemieux F. Three Key Artificial Intelligence Applications For Cybersecurity by Chuck Brooks and Dr. Frederic Lemieux. Forbes. 2021 <https://www.forbes.com/sites/chuckbrooks/2021/09/24/three-key-artificial-intelligence-applications-for-cybersecurity/?sh=7897aa6e7b7e>

CA (state of California). AI Investment Scams are Here, and You’re the Target! 2023 <https://dfpi.ca.gov/2023/04/18/ai-investment-scams/>

Chamorro-Premuzic T. Human Error Drives Most Cyber Incidents. Could AI Help? Harvard Business Review. 2023. <https://hbr.org/2023/05/human-error-drives-most-cyber-incidents-could-ai-help>

Cheng C, Chan L, Chau CL. Individual differences in susceptibility to cybercrime victimization and its psychological aftermath. Computers in Human Behavior. 2020 Jul 1;108:106311.

FBI. Malicious Actors Manipulating Photos and Videos to Create Explicit Content and Sextortion Schemes. 2023. <https://www.ic3.gov/Media/Y2023/PSA230605>

Geluvaraj B, Satwik PM, Ashok Kumar TA. The future of cybersecurity: Major role of artificial intelligence, machine learning, and deep learning in cyberspace. InInternational Conference on Computer Networks and Communication Technologies: ICCNCT 2018 2019 (pp. 739-747). Springer Singapore.

Greitzer FL, Li W, Laskey KB, Lee J, Purl J. Experimental investigation of technical and human factors related to phishing susceptibility. ACM Transactions on Social Computing. 2021 Jun 28;4(2):1-48.

Gupta M, Akiri C, Aryal K, Parker E, Praharaj L. From ChatGPT to ThreatGPT: Impact of generative AI in cybersecurity and privacy. IEEE Access. 2023 Aug 1.

Han X, Hu Y, Foschini L, Chinitz L, Jankelson L, Ranganath R. Deep learning models for electrocardiograms are susceptible to adversarial attack. Nature medicine. 2020 Mar;26(3):360-3.

Hern A, Milmo D. AI chatbots making it harder to spot phishing emails, say experts. The Guardian. 2023. <https://www.theguardian.com/technology/2023/mar/29/ai-chatbots-making-it-harder-to-spot-phishing-emails-say-experts>

Inskit Group. I, Chatbot. 2023. <https://www.recordedfuture.com/i-chatbot>

Liu N. The dark side of ChatGPT: Hackers tap WormGPT and FraudGPT for sophisticated attacks. Sdxcentral. 2023 <https://www.sdxcentral.com/articles/analysis/the-dark-side-of-chatgpt-hackers-tap-wormgpt-and-fraudgpt-for-sophisticated-attacks/2023/08/>

Ma X, Niu Y, Gu L, Wang Y, Zhao Y, Bailey J, Lu F. Understanding adversarial attacks on deep learning based medical image analysis systems. Pattern Recognition. 2021 Feb 1;110:107332.

Modic D, Anderson R. It's all over but the crying: The emotional and financial impact of internet fraud. IEEE Security & Privacy. 2015 Oct 28;13(5):99-103.

Monteith S, Bauer M, Alda M, Geddes J, Whybrow PC, Glenn T. Increasing Cybercrime Since the Pandemic: Concerns for Psychiatry. Curr Psychiatry Rep. 2021 Mar 3;23(4):18.

Monteith S, Glenn T. Automated Decision-Making and Big Data: Concerns for People With Mental Illness. Curr Psychiatry Rep. 2016 Dec;18(12):112.

Morel B. Artificial intelligence and the future of cybersecurity. InProceedings of the 4th ACM workshop on Security and artificial intelligence 2011 Oct 21 (pp. 93-98).

Newaz AI, Haque NI, Sikder AK, Rahman MA, Uluagac AS. Adversarial attacks to machine learning-based smart healthcare systems. InGLOBECOM 2020-2020 IEEE Global Communications Conference 2020 Dec 7 (pp. 1-6). IEEE.

Paoletti N, Jiang Z, Islam MA, Abbas H, Mangharam R, Lin S, Gruber Z, Smolka SA. Synthesizing stealthy reprogramming attacks on cardiac devices. InProceedings of the 10th ACM/IEEE International Conference on Cyber-Physical Systems 2019 Apr 16 (pp. 13-22).

Qadri YA, Nauman A, Zikria YB, Vasilakos AV, Kim SW. The future of healthcare internet of things: a survey of emerging technologies. IEEE Communications Surveys & Tutorials. 2020 Feb 11;22(2):1121-67.

Ravichandran H. How AI Is Disrupting And Transforming The Cybersecurity Landscape. Forbes 2023. <https://www.forbes.com/sites/forbestechcouncil/2023/03/15/how-ai-is-disrupting-and-transforming-the-cybersecurity-landscape/?sh=25397daf4683>

Ren Z, Baird A, Han J, Zhang Z, Schuller B. Generating and protecting against adversarial attacks for deep speech-based emotion recognition models. InICASSP 2020-2020 IEEE International conference on acoustics, speech and signal processing (ICASSP) 2020 May 4 (pp. 7184-7188). IEEE.

Sun M, Tang F, Yi J, Wang F, Zhou J. Identify susceptible locations in medical records via adversarial attacks on deep predictive models. InProceedings of the 24th ACM SIGKDD international conference on knowledge discovery & data mining 2018 Jul 19 (pp. 793-801).

WEF (World Economic Forum). 3 ways AI will change the nature of cyber attacks. 2019. <https://www.weforum.org/agenda/2019/06/ai-is-powering-a-new-generation-of-cyberattack-its-also-our-best-defence/>

Whitney L. How an AI tool could crack your passwords in seconds. ZDNET. 2023. <https://www.zdnet.com/article/how-an-ai-tool-could-crack-your-passwords-in-seconds/>

Wolff J. How to improve cybersecurity for artificial intelligence. Brookings. 2020. <https://www.brookings.edu/articles/how-to-improve-cybersecurity-for-artificial-intelligence/>

Wu D, Xu J, Fang W, Zhang Y, Yang L, Xu X, Luo H, Yu X. Adversarial attacks and defenses in physiological computing: a systematic review. National Science Open. 2023 Jan 1;2(1):20220023.

Zbrzezny AM, Grzybowski AE. Deceptive Tricks in Artificial Intelligence: Adversarial Attacks in Ophthalmology. J Clin Med. 2023 May 4;12(9):3266.

Zhang X, Wu D. On the vulnerability of CNN classifiers in EEG-based BCIs. IEEE transactions on neural systems and rehabilitation engineering. 2019 Apr 2;27(5):814-25.