AI will make scam emails look genuine, UK cybersecurity agency warns

Publication Date: 2024-01-24

Author: Dan Milmo

Section: Technology

Tags: Artificial intelligence (AI), GCHQ, Cybercrime, ChatGPT, Internet, Computing, UK security and counter-terrorism, news

Article URL: https://www.theguardian.com/technology/2024/jan/24/ai-scam-emails-uk-cybersecurity-agency-phishing

Artificial intelligence will make it difficult to spot whether emails are genuine or sent by scammers and malicious actors, including messages that ask computer users to reset their passwords, the UK's cybersecurity agency has warned. The National Cyber Security Centre (NCSC) said people would struggle to identify phishing messages – where users are tricked into handing over passwords or personal details – due to the sophistication of AI tools. Generative AI, the term for technology that can produce convincing text, voice and images from simple hand-typed prompts, has become widely available to the public through chatbots such as ChatGPT and free-to-use versions known as open source models. The NCSC, part of the GCHQ spy agency, said in its latest assessment of AI's impact on the cyber threats facing the UK that AI would "almost certainly" increase the volume of cyber-attacks and heighten their impact over the next two years. It said generative AI and large language models – the technology that underpins chatbots – will complicate efforts to identify different types of attack such as spoof messages and social engineering, the term for manipulating people to hand over confidential material. "To 2025, generative AI and large language models will make it difficult for everyone, regardless of their level of cybersecurity understanding, to assess whether an email or password reset request is genuine, or to identify phishing, spoofing or social engineering attempts." Ransomware attacks, which had hit institutions such as the British Library and Royal Mail over the past year, were also expected to increase, the NCSC said. It warned that the sophistication of AI "lowers the barrier" for amateur cybercriminals and hackers to access systems and gather information on targets, enabling them to paralyse a victim's computer systems, extract sensitive data and demand a cryptocurrency ransom. The NCSC said generative AI tools already helped make approaches to potential victims more convincing by creating fake "lure documents" that did not contain the translation, spelling or grammatical errors that tended to give away phishing attacks – their contents having been crafted or corrected by chatbots. However, it said generative AI – which emerged as a competent coding tool – would not enhance the effectiveness of ransomware code but would help sift through and identify targets. According to the Information Commissioner's Office, the UK's data watchdog, 706 ransomware incidents were reported in the UK in 2022, compared with 694 in 2021. The agency warned that state actors probably have enough malware – short for malicious software – to train a specially created AI model that would create new code capable of avoiding security measures. The NCSC said such a model would have to be trained on data extracted from its target. "Highly capable state actors are almost certainly best placed among cyber threat actors to harness the potential of AI in advanced cyber operations," the NCSC report says. The NCSC added that AI would also work as a defensive tool, with the technology able to detect attacks and design more secure systems. The report came as the UK government set out new guidelines encouraging businesses to better equip themselves to recover from ransomware attacks. The “Cyber Governance Code of Practice” aims to place information security on the same tier as financial and legal management, the NCSC said. But cybersecurity experts have called for stronger action. Ciaran Martin, the former head of the NCSC, says that unless public and private bodies fundamentally change how they approach the threat of ransomware, “an incident of the severity of the British Library attack is likely in each of the next five years.” In a newsletter, Martin wrote that the UK needs to reassess its approach to ransomware, including by creating stronger rules around the payment of ransoms and giving up on “fantasies” of “striking back” against criminals based in hostile nations.