

Impersonation is at the heart of insurance fraud – for example, fake physicians submitting fake medical records to support fake claims. Someone – or something – needs to supply the fake content, and generative artificial intelligence (AI) is more than available to fill the role. AI is fast becoming a criminal's best friend.

Fraudsters once needed extensive technical skills to set up and execute their schemes. Today, the average criminal only needs to apply one of many easy-to-use and accessible AI tools. These provide sophisticated capabilities in writing, coding, and image generation and manipulation. Taken together, they create the perfect storm of criminal innovation and criminal opportunity.

The intelligence is artificial, but the crimes are real

Because they are trained on large language models, generative AI tools like ChatGPT are skilled at mimicking human speech and writing. Users feel like they are talking to real people, but AI-based chatbots also make all-too-human mistakes. Attorneys have learned the hard way never to rely on chatbots for legal research. In one recent episode, ChatGPT “hallucinated” cases with realistic-seeming, but false case citations, resulting in disciplinary action for one less-than-careful attorney. In another instance, a New Zealand grocery store created a bot to generate tasty recipes from submitted lists of ingredients. The same bot made news when it recommended an “aromatic water mix” based on a list of deadly household chemicals.

AI may occasionally produce nonsensical results, but in the hands of a skilled criminal, chatbots can create vivid, immersive simulations of people and even manufacture false medical evidence.

f Voice cloning: One method people can use to verify the source of a suspicious email or document is to call a listed phone number and speak directly to the sender. If the voice on the other end of the line sounds familiar and makes sense, it's a
