TechXplore

Four ways criminals could use AI to target more victims

June 23 2023, by Daniel Prince

Credit: AI-generated image (disclaimer)

Warnings about artificial intelligence (AI) are ubiquitous right now. They have included fearful messages about AI's potential to cause the extinction of humans, invoking images of the Terminator movies. The UK Prime Minister Rishi Sunak has even set up a summit to discuss AI safety.

However, we have been using AI tools for a long time—from the algorithms used to recommend relevant products on shopping websites, to cars with technology that recognizes traffic signs and provides lane positioning. AI is a tool to increase efficiency, process and sort large volumes of data, and offload decision making.

Nevertheless, these tools are open to everyone, including criminals. And we're already seeing the early stage adoption of AI by criminals. Deepfake technology has been used to generate revenge pornography, for example.

Technology enhances the efficiency of criminal activity. It allows lawbreakers to target a greater number of people and helps them be more plausible. Observing how criminals have adapted to, and adopted, technological advances in the past, can provide some clues as to how they might use AI.

1. A better phishing hook

AI tools like ChatGPT and Google's Bard provide writing support, allowing inexperienced writers to craft effective marketing messages, for example. However, this technology could also help criminals sound more believable when contacting potential victims.

Think about all those spam phishing emails and texts that are badly written and easily detected. Being plausible is key to being able to elicit information from a victim.

Phishing is a numbers game: an estimated 3.4 billion spam emails are sent every day. My own calculations show that if criminals were able to improve their messages so that as little as 0.000005% of them now convinced someone to reveal information, it would result in 6.2 million more phishing victims each year.

2. Automated interactions

One of the early uses for AI tools was to automate interactions between customers and services over text, chat messages and the phone. This enabled a faster response to customers and optimized business efficiency. Your first contact with an organization is likely to be with an AI system, before you get to speak to a human.

Criminals can use the same tools to create automated interactions with large numbers of potential victims, at a scale not possible if it were just carried out by humans. They can impersonate legitimate services like banks over the phone and on email, in an attempt to elicit information that would allow them to steal your money.

3. Deepfakes

AI is really good at generating mathematical models that can be "trained" on large amounts of real-world data, making those models better at a given task. Deepfake technology in video and audio is an example of this. A deepfake act called Metaphysic, recently demonstrated the technology's potential when they unveiled a video of Simon Cowell singing opera on the television show America's Got Talent.

This technology is beyond the reach of most criminals, but the ability to use AI to mimic the way a person would respond to texts, write emails, leave voice notes or make phone calls is freely available using AI. So is the data to train it, which can be gathered from videos on social media, for example.

Social media has always been a rich seam for criminals mining information on potential targets. There is now the potential for AI to be used to create a deepfake version of you. This deepfake can be exploited to interact with friends and family, convincing them to hand criminals information on you. Gaining a better insight into your life makes it easier to guess passwords or pins.

4. Brute forcing

Another technique used by criminals called "brute forcing" could also benefit from AI. This is where many combinations of characters and symbols are tried in turn to see if they match your passwords.

That's why long, complex passwords are safer; they are harder to guess by this method. Brute forcing is resource intensive, but it's easier if you know something about the person. For example, this allows lists of potential passwords to be ordered according to priority—increasing the efficiency of the process. For instance, they could start off with combinations that relate to the names of family members or pets.

Algorithms trained on your data could be used to help build these prioritized lists more accurately and target many people at once—so fewer resources are needed. Specific AI tools could be developed that harvest your online data, then analyze it all to build a profile of you.

If, for example, you frequently posted on social media about Taylor Swift, manually going through your posts for password clues would be hard work. Automated tools do this quickly and efficiently. All of this information would go into making the profile, making it easier to guess passwords and pins.

Healthy skepticism

We should not be frightened of AI, as it could bring real benefits to society. But as with any new technology, society needs to adapt to and understand it. Although we take smart phones for granted now, society had to adjust to having them in our lives. They have largely been beneficial, but uncertainties remain, such as a good amount of screen time for children.

As individuals, we should be proactive in our attempts to understand AI, not complacent. We should develop our own approaches to it, maintaining a healthy sense of skepticism. We will need to consider how we verify the validity of what we are reading, hearing or seeing.

These simple acts will help society reap the benefits of AI while ensuring we can protect ourselves from potential harms.

This article is republished from The Conversation under a Creative Commons license. Read the original article.

Provided by The Conversation

Citation: Four ways criminals could use AI to target more victims (2023, June 23) retrieved 15 May 2024 from https://techxplore.com/news/2023-06-ways-criminals-ai-victims.html