AI and Identity Theft - The Genie is Out of the Bottle

July 24, 2023 - Artificial intelligence, or AI as it has become known, is tool. And like any tool, it can be used for good or for bad. Of late, there has been a great deal of talk about regulating AI. In fact, there was a meeting held at the White House just last week on this topic. At the end of that meeting, a number of companies like Google, Microsoft and Open.ai agreed to implement a water marking scheme for things that are produced using AI. But there is one little problem with that scheme. It isn't just big and well-known companies that have access to this technology. A lot of it is now "open source", and no amount of regulation is going to stop its use by criminal elements. That's especially true when it comes to identity theft.

In fact, AI is opening new doors for criminals. It can be used to scrape websites for information, and the person doing the programming can get very specific for the type of information it is looking for. Social security numbers for instance. But AI can also do a lot more than that.

It is being used now to create pictures. It's fairly easy for some AI platforms to transform a picture by replacing the faces of the people being photographed. These are known as "deep fakes" and they can be quite convincing. You don't need to have a vivid imagination to understand the kinds of problems this will create.

AI is also now being used to alter voices. The most convincing of these platforms that we've seen is run by ElevenLabs. They can synthesize voice in a way that makes it sound totally real. But you will have to subscribe and kick in a few bucks. On the other hand Voice.ai has released a totally free voice changer app that allows anyone to mimic someone else. And that's a real issue.

Just think about the following scenario. Someone is targeting you for fraud. They know that you have a grandchild and that you are close to that grandchild. So they contact your grandchild by phone and record the call. The get a few minutes of solid audio when they are on the phone and then run that audio through an AI platform to train it. They then write a statement that says that someone is in trouble, or has been kidnapped and then have the AI made an audio recording with your grandchild's synthesized voice reading the statement. The next thing you know, you get a call from what sounds like your grandchild who is in desperate need of money. What are you going to do?

That's just one example and itâ€™s a scam that has already worked without the use of AI. And to be perfectly clear, we don't

have reason to believe that any of the AI platforms named herein have been used in this manner. The point here is that this is coming, and it is coming very fast. And the problems that are going to be created probably can't be stopped at this point. That means that consumers are going to have to get very smart, very quickly.

Consumers really need to start thinking about the calls that they receive and ask themselves the question, was that a real person on the other end of the call or a computer? And then, before they send any money to anyone, they need to do some legwork just to make sure their conclusion what correct? Just any every scam artist out there knows how to spoof a phone number so just because the call came from a number you know, doesn't really mean much anymore. You need to call the person back yourself.

As previously mentioned, a lot of AI models are now open source. That means that anyone with a little computer knowledge can download the code, train the model to do what they want, and then run it. The fact that larger companies are going to start watermarking some AI generated data won't impact anyone doing this. It's very similar to the argument that people make about guns. On the one side you have people calling for more regulation. On the other, you have people saying that criminals don't care about the regulations and that only law-abiding citizens will be negatively impacted. Just substitute the term "AI" for "gun" and you'll see the dilemma. It is now the very same argument.

AI is going to mean that we are entering a new era of scams. We can guess at what some of those scams will look like but if there is one thing that we can count on it is the ingenuity of crooks. There are likely to be a lot of new scams that we have never even thought of, so it is up to consumers to be vigilant. And it is most unlikely that any form of regulation will stop this.
by Jim Malmberg
Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.

Follow ACCESS