Joshua Martin

AI uses fake profiles to lure targets to scam and other crimes.

How to Spot a Bot

Remember that old internet theory that most of the people online were fakes? It sounded silly then, but we're nearing that reality. AI (artificial intelligence) exploded on cyberspace in recent years, infesting every social platform with bots built for deception. And they get smarter by the day. Cybercriminals and creeps beyond our screens send these automated proxies into the digital wild in search of prey— you.

What are bots?

Profiles exist online that look like people but are not people. You've probably dealt with automated phone calls and chat assistants or scams with scripted answers. These are bots. If you've come across them, then you probably believe you're immune. However, in the wise words of Frank Abagnale, technology breeds crime. They've evolved.

How convincing are these bots?

There's an incomprehensible number of personalized bots out there masquerading as humans, which we estimate nearly outnumber authentic users. With so many bots lurking about the internet, you can guess most of them are up to no good. They send sophisticated phishing attacks and attempt to trap their prey in a web of lies. But how smart are they? Disturbingly smart. The rise of advanced language models, such as *ChatGPT*, has spawned lifelike bots that can converse with humans.

AI can scan your online profile for behavioral patterns and clues of your interests, allowing it to tailor its responses perfectly to your personality and native language. Bots could even mask themselves with convincing profiles constructed by their creators, dawning deepfakes of people that might not exist. These techniques make it harder to discern bots from people, and it make it easier for criminals to hit more targets.

The dangers of falling for a bot

Losing your savings to a clever phishing bot disguised as your grandma sounds like the worst thing in the world. However, there are untold horrors these bots could lead to. An AI-generated profile could lure you out of your home. Whether it's a date or a friendly meetup, you can't know for sure who you're going to meet is who you saw and heard on their profiles. You could be in a trap for:

- Robbery (they follow you back home or rob you on the spot)
- Human trafficking (forced labor or prostitution)
- Organ harvesting (enough said)
- Murder (simply put, there are some weirdos out there)

Any age or gender could fall victim to kidnapping, and it mostly starts on social media. AI can analyze patterns to determine who's the most vulnerable and talk to victims for weeks and months. This could make other rare but serious crimes easier to commit, such as with digital kidnapping, AI can scan social media contacts for a victim's parents' account, obtain child photos from years ago, and use that to "prove" they know the victim's family to gain trust. Creeps could also use deepfake technology to appear related to the target. This would also make it difficult for law enforcement to track them using image-search software. Impressionable children and young teens, who tend to accept more friend requests on the internet, are the most likely targets.

Detect the threat

Today, asking for your Tinder match to send photos of specific poses to prove their likeness won't cut it, nor will be asking for a voice clip. Although every scam bot or user on the internet may not be equipped with these tricks, you can never be too careful with your information and your life.

As for photographs and videos, it's hard for humans to detect subtle manipulation, but the clues are there.

- Details that look too smooth
- Repetitive details and patterns, something too symmetrical
- Abnormalities in the background

As for chatbots and AI-operated emails, comb through their texts and look for formulaic speech. If their responses always feel like the "right answer" for you, it's probably too good to be true. Chatbots are also designed to respond to predictable answers. Say something random and you could expose their wired conversation pattern.

AI Detection Services

With the influx of fraudulent content on the web, AI detection has become a growing industry. There are many, many AI detection tools out there designed to tackle different problems for different people.

- Illuminarty (free image and text detection, browser extension coming soon, currently struggles with deepfakes)
- HuggingFace (image only, but decent with deepfakes, free but not perfect)
- GPTZero (specializes in AI text detection, targeted toward professors and students)
- Reality Defender (specializes in deepfakes, tier-one bank and government trusted, requires a demo request)

Learn from research, not from a mistake

The arms race between AI-generated content and AI detection has started, and both sides are neck-in-neck for advancement. Hopefully, soon, we'll have built-in software that sniffs out the bots and AI-generated content. Until then, we only have our wits and intuition. Only the future will tell if that'll be enough.