Deepfakes

Introduction

1 min

With the advent of generative AIs, the limits of technological creation are continually being pushed. While AI-generated text, images, and videos may have seemed like a far-a-way pipe dream only recently, continued innovation has made these concepts a reality. As with any generative algorithm, creating these things becomes possible given enough time, data, and training.

That said, we have created a new concerning output of AI. This output is referred to as “DeepFakes”. Deepfakes is a sizeable encompassing term that describes content created by various AI systems designed to mimic legitimate content.

These deepfakes include fake images designed to look real, fake videos designed to appear legitimate, and fake audio content designed to mimic that of a real person/persons. While this content has a great deal of legitimate use, malicious actors have quickly adopted this new technology.

Since their recent adoption, threat actors have begun to use deepfakes for various scams, including fake endorsements, MFA bypass, and other attacks.

In the following exercises, we’ll explore how these deepfakes are created and how exactly threat actors use them.

Image courtesy of Wikimedia Commons