



# The Dangers of AI Art and Deepfakes

## What are AI Art and Deepfakes?

AI art is generated using billions of images and examples of art. When you enter a prompt, the AI art generator builds an image for you by combining many of these examples into a single image. Deepfake technology is similar, but it involves manipulating real photographs and videos of people and places. This technology can make it look like a person did or said something that they never did. Both of these technologies can be used in a harmless way, but cybercriminals have learned to use them maliciously.

## Deepfake Scams

Scammers can use deepfake technology to impersonate celebrities or other public figures. This type of scam can make it seem like a celebrity has endorsed a product even though they have not. Scammers use this technique to trick people into purchasing a fake product, and they will steal consumers' personal or financial information. Deepfakes can be used for political figures as well. A deepfake video can make it appear that a government official said or did something that they didn't say or do. These types of videos can be used to lure people into visiting fake websites or clicking on fake news articles.

## AI-Generated Art and Photograph Scams

Cybercriminals commonly use AI in online romance scams. They can generate fake photographs to use in dating profiles to try and steal money or information from their victims. The cybercriminals will also use current events as the subject of their scams. They use AI to create realistic photographs of tragedies and other events. They post the photographs on fake websites to coerce people into donating money to a charity organisation. The organisation is fake, of course, and the cybercriminals will keep any donated money.

## What Can I Do to Stay Safe?

Follow the tips below to keep yourself safe from AI art scams:

- AI-generated images often have subtle differences or mistakes. Keep an eye out for anything in the photograph that appears to be unusual. A hand with more than five fingers or a photograph with strange lighting or shadows are common signs that an image was created with AI.
- Always stop and think before clicking or taking action. If a photograph or image seems bizarre or too good to be true, it could be a scam.
- When possible, verify the claim in a different location. For example, if you see a video with a celebrity endorsement, check that person's official website for proof that they are actually involved with the product.

