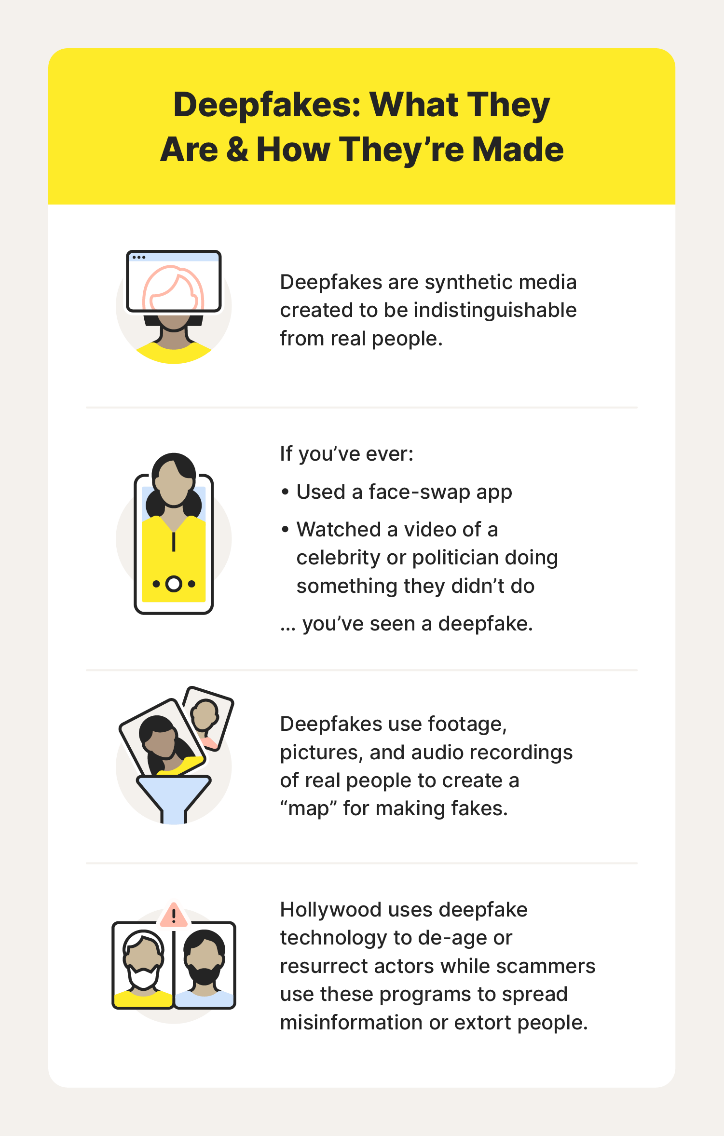
**Deepfakes: Navigating the New Frontier of Digital Deception**

Today's advanced digital age means that reality and fiction are more difficult to distinguish than ever before. One of the most striking expressions of this trend is deepfakes—overwhelmingly realistic yet entirely fabricated media material created by means of an artificial intelligence (AI).

**What Are Deepfakes?**



Deepfakes are artificially produced media—video, photos, or audio recordings—manipulated or created by means of AI algorithms, most notably by applying techniques of deep learning. "Deepfake" is a blend of "deep learning" and "fake" that signifies the basis and application of the technology.

These computer tools can put pre-recorded images and videos on top of source material, making them appear realistic looking with people seemingly saying or doing something they didn't. Deepfakes are created utilizing computer programs that make them nearly impossible to distinguish from original materials.

**How Are Deepfakes Made?**

Deepfakes are produced with the use of artificial intelligence, in this case by a method referred to as deep learning. Two neural networks, one which generates images (the generator) and one that examines them (the discriminator), compete against one another in a Generative Adversarial Network (GAN). The system gets better at making very realistic videos, audio recordings, or photos that are copies of real individuals over a long period.

**Why Are Deepfakes Concerning?**



Deepfakes pose serious risks because they can realistically impersonate actual individuals. Some of the key concerns are:

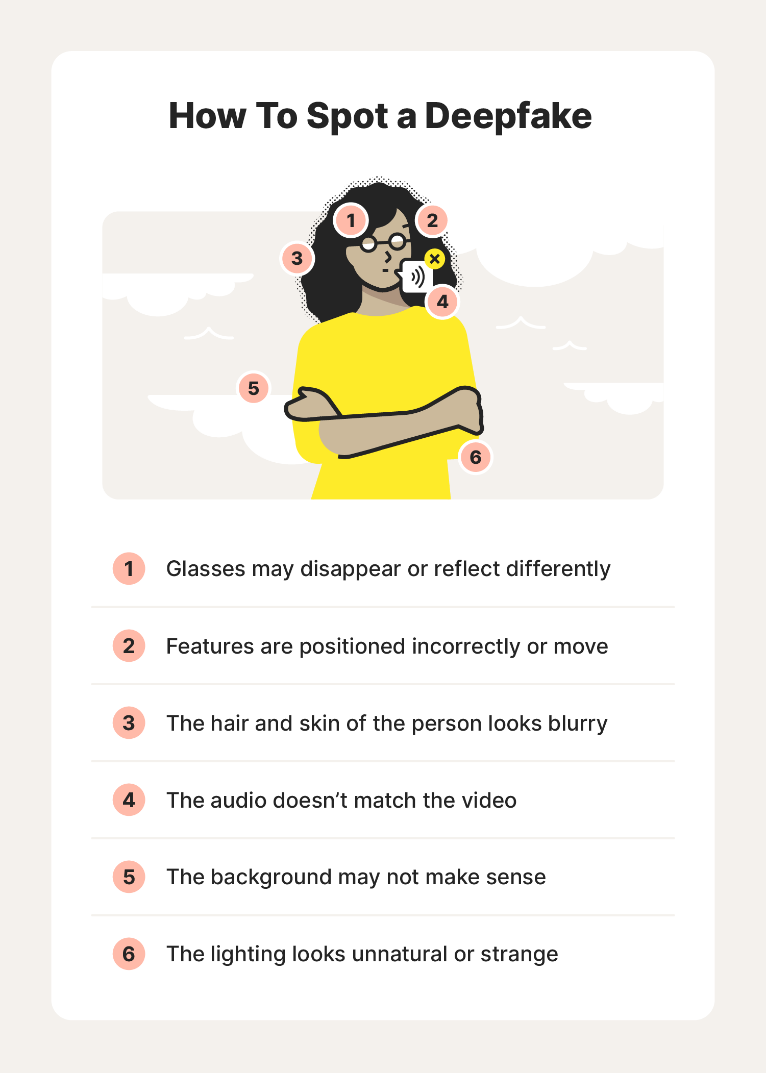
* **Scams and Hoaxes**: Cybercriminals can create fake videos of executives confessing to crimes, potentially damaging reputations and stock prices.
* **Nonconsensual Content**: Most deepfakes online are used in explicit content targeting celebrities without consent.
* **Election Manipulation**: Fake political statements from leaders can mislead voters and influence public opinion.
* **Social Engineering**: Audio deepfakes have been used to trick people into transferring money, believing they were talking to a trusted superior.
* **Disinformation**: Deepfakes can spread false narratives, like conspiracy theories, that undermine trust in media.
* **Identity Theft**: Fake voices and visuals can be used to impersonate individuals and commit fraud.

**Acceptable Uses of Deepfake Technology**

Though deepfakes tend to evoke ethical and security concerns, there are a variety of permissible and positive applications for the technology with proper disclosure. These include:

* **Parody and Satire**: Creators have used deepfakes to produce humorous or satirical content, especially in political or entertainment settings.
* **Tech Demonstrations**: Developers and news outlets employ deepfakes to showcase advancements in AI and video manipulation.
* **Historical Recreation**: Enthusiasts and educators use deepfakes to animate historical figures or simulate historical events for educational purposes.
* **Creative Simulations**: Artists leverage deepfakes to reimagine modern media in older styles or fictional settings, creating engaging visual narratives.

**Spotting a Deepfake: Tips for the Public**



While deepfakes can be highly convincing, there are several telltale signs:

* **Unnatural Movements**: Look for awkward facial expressions, jerky motions, or inconsistent blinking.
* **Mismatched Features**: Misaligned facial features or poor lip-syncing are major clues.
* **Visual Errors**: Watch out for odd lighting, blurry edges, unrealistic hair, and skin discoloration.
* **Audio Issues**: Robotic voices or misaligned audio with the lips can signal a deepfake.
* **Zoom In**: Slowing down the video or viewing it on a larger screen may help reveal subtle inconsistencies.​

**Protecting Yourself Against Deepfakes**



To guard against the misuse of your identity through deepfakes:

* Limit how many personal photos and videos you share online.
* Set your social media accounts to private.
* Use a VPN for safer internet browsing.
* Install and maintain antivirus or malware protection.
* Set up a family “code word” for verification during emergencies.
* Conduct sensitive or financial transactions in person when possible.

**References**

<https://us.norton.com/blog/emerging-threats/what-are-deepfakes>

<https://www.fortinet.com/resources/cyberglossary/deepfake>