PHISHX

Como reconhecer e se proteger de Deepfake

Introdução

Separar o que é verdade ou mentira enquanto navega na internet tem sido cada vez mais difícil nos últimos tempos. O crescimento da confiança nos meios de comunicação eletrônicos fez com que as pessoas se tornassem menos propensas a não questionar informações que estão sendo consumidas.

Dentro desse contexto, começaram a surgir ferramentas que possibilitam produzir vídeos adulterados e realistas, colocando pessoas em situações constrangedoras e até mesmo aplicando golpes com a imagem e vozes de outras pessoas.

O que é deepfake

O deepfake é uma técnica que pode ser usada na criação de conteúdos falsos, que podem ser áudios e imagens, produzidos com ajuda de uma inteligência artificial. Esses conteúdos buscam enganar as pessoas e são gerados a partir de arquivos verdadeiros. Em seguida, são manipulados através de tecnologias criadas para editar os materiais.

De forma detalhada, a intenção dessa tecnologia é criar vídeos, imagens e áudios realistas, fazendo parecer que pessoas reais disseram ou fizeram coisas que nunca foram ditas ou feitas, de fato. Dessa forma, vídeos e imagens são misturados para criar um conteúdo sintético que aparenta ser verdadeiro.

Assim, mesmo que o foco do deepfakes seja a criação de vídeos falsificados, criados a partir de computadores e softwares, a prática não se restringe a isso. A técnica também é utilizada para simular vozes de pessoas, assim como criar textos e até mesmo alterar rostos e transmissões ao vivo.

Como os deepfakes funcionam

Criar esse tipo de falsificação requer a utilização de uma inteligência artificial. Dessa forma, é utilizado um processo de aprendizado de máquinas, em que um sistema é abastecido com quantidades enormes de referência.

A prática costuma utilizar arquivos de referência para que essa inteligência artificial possa aprender como uma pessoa fala, além de como como seu rosto e seu corpo se movimentam. Assim ela pode desenvolver maneiras para reproduzir de forma virtual aquilo que aprendeu.

Quando falamos de falsificações de áudio, todo o material passa pelo algoritmo de uma inteligência artificial que clona a voz das pessoas, incluindo os traços que podem ser únicos da sua fala.

Qual a função dos deepfakes?

O termo fake em inglês significa falso. Dessa forma, como o próprio termo sugere, deepfakes são feitos para enganar. Embora o objetivo do uso seja variado, podendo servir para diversos fins, a técnica vem se popularizando pelo uso para a produção de conteúdos que buscam levar à desinformação.

Dessa forma, os deepfakes representam uma ameaça para as pessoas e organizações. Para as pessoas, o deepfake pode ser utilizado para roubar a identidade de alguém, aplicando fraudes financeiras ou até realizando compras.

Já para as organizações, um deepfake pode ser utilizado para que um criminoso se passe por funcionários, fornecedores e executivos durante ligações. Tudo depende da criatividade e da disponibilidade de arquivos que podem ser utilizados. Assim, esse tipo de técnica também pode ser utilizado para impactar diretamente a imagem ou reputação de uma marca.

Como se proteger

Proteger suas informações pode ser uma forma de prevenir que suas fotos e vídeos sejam utilizados para deepfakes. Por isso, é importante configurar suas redes sociais como privadas, uma vez que fotos, áudios e vídeos podem ser utilizados para alimentar inteligências artificiais.

Ainda assim, também é fundamental aprender a reconhecer uma manipulação com deepfake, o que pode ser uma tarefa que exige observação. Para fazer isso, observe se o rosto e os lábios se movem em conjunto com o que a pessoa diz. Além disso, preste atenção se a fala parece contínua, robótica ou se em algum momento apresenta cortes entre palavras.

Não se esqueça de considerar o contexto. Ainda que o vídeo esteja muito bem manipulado, avalie se faz sentido o que aquela pessoa está dizendo. Desconfie de tudo e evite compartilhar informações sem antes pesquisar e conferir se são verdadeiras.