Deepfakes

Deepfakes are artificial intelligence-generated videos or audio clips that make it appear as though someone is saying or doing something they never did. Just by this definition, the possibilities for identity theft and misinformation might become obvious to you. Deepfakes can be used to defame individuals and commit fraud. For example, if your vocal identity and sensitive information got into the wrong hands, a cybercriminal could use deepfaked audio to contact your bank.

You might think that because you don't use any AI product you could never be a victim. The truth is that these technologies can scrub data (such as video, photographs, and voice recordings) of millions of people from websites, like social media platforms.

You can take some steps to reduce the chances that a criminal creates a deepfake of you. Mostly, you should think hard about what you share publicly. Here are some strategies to protect yourself, and some tips about what to do if you suspect you're the victim of a deepfake.

Share with care

The first step in avoiding deepfakes is to be extremely cautious about what personal information you share online. Limit the amount of data available about yourself, especially high-quality photos and videos, that could be used to create a deepfake. You can adjust the settings of social media platforms so that only trusted people can see what you share. Of course, you should also make sure that you trust anyone who requests to follow or friend you.

Enable strong privacy settings

Take full advantage of websites' privacy settings to control who can access your personal information and content. Restrict who can see your photos, videos, and other sensitive data. This includes websites where you store photo files. Reduce the amount of publicly available material, and you minimize the resources potential deepfake creators have.

Watermark photos

When sharing images or videos online, consider using a digital watermark on them. This can discourage deepfake creators from using your content since it makes their efforts more traceable.

Learn about deepfakes and AI

The realm of AI is changing rapidly. Staying abreast of the latest developments can help you stay vigilant. You don't need to become an expert, but following the news about these technologies is important for everybody. This knowledge can help you recognize potential red flags when encountering suspicious content.

Use multi-factor authentication

These days, you really should double your security by implementing multi-factor authentication for all of your accounts. This is when you need an extra step to log into an account, such as a facial scan, entering a code texted to your phone, or using a standalone app on your device. This extra layer of security helps prevent unauthorized access to your accounts, reducing the chances of someone obtaining your personal data.

Use long, strong, and unique passwords

Every password should be at least 16 characters long, unique to the account, and contain a random mix of upper case letters, lower case letters, numbers, and special characters. The best way to remember all these unique passwords is by storing them in a password manager with MFA turned on.

Keep your software up to date

Keep your devices and software up to date with the latest security patches and updates. Outdated software can have vulnerabilities that hackers may exploit to access your data. We recommend turning on automatic updates so you don't have to constantly check for new updates.