NATIONAL CYBERSECURITY ALLIANCE

How to protect yourself against deepfakes

December 22, 2023 | 7 min read

Deepfake technologies can be used to steal your identity even if you don't use generative AI platforms.

You've probably heard about generative AI (artificial intelligence), but you might not be aware that these technologies have brought with them new concerns about privacy, identity theft, and misinformation. One pernicious form of AI scam is called "deepfake" technology.

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.

1) **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.

2) **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.

3) **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.

4) **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.

5) **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.

6) **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.

7) **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.

8) **Don't take the phishing bait:** Be extremely cautious when receiving emails, direct messages, texts, phone calls, or other digital communications if the source is unknown. This is especially true if the message is demanding that you act fast, such as claiming your computer has been hacked or that you won a prize. Deepfake creators attempt to manipulate your emotions so you download malware or share personal information. Verify the identity of the sender and avoid clicking on suspicious links. We always say: think before you click.

9) **Report deepfake content:** If you come across deepfake content that involves you or someone you know, report it to the platform hosting the content. This can help in having it removed or investigated, limiting its potential reach. You should also report it to federal law enforcement.

10) **Consult legal advice:** If you are the victim of a deepfake that has damaged your reputation, consult with cybersecurity and data privacy legal experts. Laws are quickly evolving to address the issue of deepfakes, but with technology changing so fast, the legal system takes time to catch up. You can take action – contact your elected representatives and tell them you want to see more action around preventing deepfakes!

While deepfakes provide a new terrain in the battle against misinformation and defamation, you can take proactive measures to protect your digital identity. In fact, this advice is good for protecting yourself from other common cyber threats. Stay informed, adopt these cybersecurity habits, and think hard about what you post online, as well as who has access to it.