Article

Oct 2024

The dangers of deepfakes

With the rise in use of Artificial Intelligence across all areas of life, there has also been a rise in its malicious usage.

Callum Lake
Information Security Consultant

Email callum.lake@waterstons.com

Online communication plays an important role in our lives and, when combined with AI, has led to the growth of deepfakes; realistic yet completely fabricated videos or images. Deepfakes can make it appear as though someone is saying or doing something they never actually did.

The AI technology behind deepfakes can analyse then produce content that mimics the facial expressions, voice, and movements of a person. The result being entirely fake images, voice recordings and videos, which can then be used for an array of malicious activity.

Why are deepfakes dangerous?

Deepfakes can have a massive benefit to those carrying out social engineering attacks.

In April 2024, Bleeping Computer reported LastPass was targeted by a voice phishing attack in which the CEO's voice was run through an AI generator, and a voice recording sent to an employee via WhatsApp with a request to send a large sum of money to an account. Luckily, it was unsuccessful.

Attacks like these are very common and their usage falls broadly into the below categories:

1. **Misinformation**: False information can be spread via deepfake videos, images and voice recording, and is prominent critical times like elections. A deepfake video of a politician making controversial statements could sway voters or incite unrest.
2. **Personal attacks**: Deepfakes can be weaponized to damage the reputation of individuals, for example showing someone in a compromising situation that never happened, leading to personal and professional reputational damage, or even bullying, harassment, or worse.
3. **Financial scams**: Criminals can use deepfakes to impersonate company executives or public figures in order to carry out financial scams, similar to the LastPass April attack.
4. **Erosion of trust**: As deepfake technology becomes more advanced and accessible, it becomes increasingly difficult to trust what we see online, causing serious implications for society, as people may start to question the authenticity of legitimate videos and images.

How to protect yourself

While deepfakes are a serious threat, there are steps you can take to protect yourself and others:

- **Verify sources**: Always check the source of a video or image before believing or sharing it. Trusted news outlets and official sources are more likely to provide accurate information.
- **Be sceptical**: If a video or image seems too outrageous or unlikely, it might be a deepfake; approach such content with caution.
- **Educate others**: Spread awareness about the dangers of deepfakes; the more people know about this technology, the less likely they are to be deceived.

This article and other fantastic insights are shared in our monthly cyber threat report. You can join the mailing list to receive it here.

Waterstons has 25+ years' experience across the UK and Australia preparing and protection organisations from cyber threats. We are committed to assisting all organisations to stay agile and prepared in today's cyber conscious economy.

Empower your organisation today, get in touch with one of our team members.

info@waterstons.com.au | 02 9160 8430