

## Think That's a Celebrity Endorsement? It Might Be a Deepfake Scam.

Have you ever seen a video of a celebrity endorsing a new investment or giving away free tickets that seemed too good to be true? You might be witnessing a deepfake AI scam. These scams are becoming more and more convincing, leveraging advanced technology to deceive unsuspecting people.

In this article, we're going to look at how these scams work, what deepfakes are, and, most importantly, how you can protect yourself.

### Celebrities endorsing shady products? It could be a scam

Hackers have been creating videos featuring famous celebrities promoting shady products or giveaways. Maybe it's an actor offering "exclusive cryptocurrency opportunities" or a pop star announcing "free concert tickets" if you click a link. These scenarios can look and sound incredibly real, but they are often scams designed to trick you.

Hackers are banking on the fact that you trust your favorite celebrities. They use that trust to get you to act against your best interest, such as like entering personal details or making payments.

It's incredibly easy to fall for it, but with a little awareness, you can stay one step ahead.

### What are deepfakes?

You might be wondering, "What exactly is a deepfake?" A deepfake is a video or audio clip where artificial intelligence (AI) is used to convincingly replicate a person. In the context of scams, this often means creating a realistic version of a celebrity's face or voice to deceive viewers.

### Why are deepfakes so convincing?

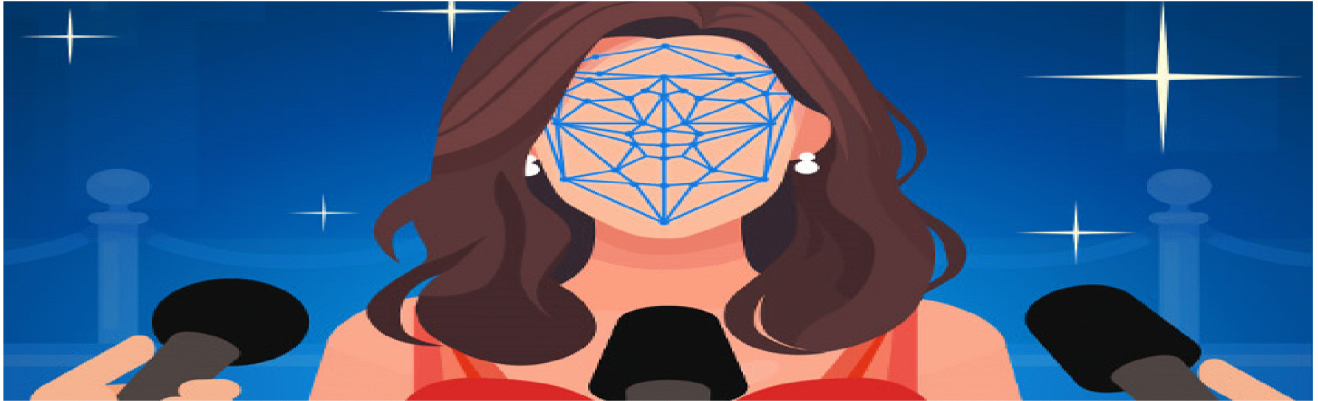
The key reason deepfakes of celebrities are so convincing is the sheer amount of source material available. Celebrities are everywhere - movies, talk shows, podcasts, social media - and all of that is fuel for deepfake AI. The AI studies their facial expressions, voice tone, and movements, and then recreates them nearly perfectly. This level of accuracy makes it extremely difficult to determine whether a video is real or fake just by watching it.

### How to spot a deepfake scam

Spotting a deepfake isn't always easy, but there are signs you can look for to protect yourself.

- **Check the account.** Does the account posting the video look legitimate? Often, scammers will use usernames that are very close to the real celebrity's name but with subtle variations, such as an extra letter or number.
- **Verify on official channels.** Head over to the celebrity's known real social media accounts. Are they promoting this product or giveaway on their official platforms? If a deepfake video claims that Taylor Swift is endorsing a new product, yet there's no mention on her verified pages, it's a red flag, and it's worth taking a moment to check.

**CONTINUED ON NEXT PAGE**



## Think That's a Celebrity Endorsement? It Might Be a Deepfake Scam. >>>Continued from prior page<<<

- **Look closely at the video.** Deepfake technology is very advanced, but it's not perfect. You might notice odd glitches, such as like unnatural blinking, awkward body movements, hands that seem to disappear, or slightly off voice patterns. These can be tell-tale signs that the video is fake.

Does it fit the celebrity's usual behavior? Ask yourself if the promotion makes sense for that celebrity. Would this person usually promote something such as a cryptocurrency or a random giveaway? If it feels off-brand, it probably is.

### **Deepfakes are getting better, so stay vigilant**

The truth is that deepfakes are getting more convincing by the day. It's becoming increasingly difficult to distinguish between what's real and what's fake. That's why it's essential not to trust videos of celebrities blindly, even if they appear authentic. Scammers thrive on impulse reactions, so if something seems too good to be true, take a step back and think it through.

Awareness is your biggest weapon against these scams, so please share this information with friends and family who might need to be made aware of how far this technology has come.

### **Think you might have been scammed?**

If you think you might have fallen victim to a deepfake scam, especially if you've been asked to install software or allow access to your computer, don't panic. Give us a call.

We're here to help assess the situation and take steps to keep you secure. Scams such as these are becoming more common, but with the right support, you can minimize the impact and avoid falling victim again.

### **Conclusion**

Deepfake AI celebrity scams are a modern threat, using the faces and voices we know and trust to pull us into traps. But remember, staying alert and questioning anything that feels out of place can go a long way to keeping you safe.

**If you have any questions OR believe you have been hacked/compromised, feel free to reach out anytime to see how we can help you.**

**Call us at 940-282-0290.**



## “You Have Been Hacked!” Don’t Fall for This Common Scam Email.

Have you ever received a terrifying email claiming someone has hacked your computer, watched you through your webcam, and gathered your personal files? If so, you're not alone. These types of scam emails are becoming more common and are designed to frighten you into paying up. Let's take a closer look at how this scam works and why you shouldn't worry.

### **"Your computer has been hacked!" – what the email says**

The first thing you need to know is that this email is designed to scare you. It will often claim that your computer has been hacked, and that someone has gained access to all your files, messages, and even emails. To make things even more chilling, it might say that they've been watching you through your webcam.

This message is all about creating panic. The scammers want you to feel vulnerable and out of control, which makes you more likely to meet their demands. But before you react, remember that this is all just a tactic, a very common trick to prey on fear.

### **The cryptocurrency demand**

These scam emails often end with a demand for cryptocurrency, such as Bitcoin, in exchange for not releasing your so-called "private" information. They'll give you a short deadline to pay up, making it sound urgent and dire. They know that if they can pressure you

into acting quickly, you might not have time to think logically or seek advice.

### **The scary part: mentioning your real password**

One thing that makes these emails particularly unsettling is that they sometimes mention a password you recognize, perhaps even a password you still use! This can make the threat seem very real, but here's what's really going on.

Your email address and passwords may have been part of a public data leak at some point. Large-scale data breaches have affected platforms such as LinkedIn, Facebook, and many others. When these breaches happen, hackers often get hold of millions of usernames and passwords. They then use this information to craft convincing emails to make their scam look legitimate.

It's a good reminder of why using a unique password for every account is so important. Using a password manager can help with that, and adding two-factor authentication (2FA) adds another layer of security.

### **The good news: it's just a scam**

The good news is that this email is just a scam. No one has access to your computer, files, or webcam. These scammers are relying on scare tactics to pressure you into paying. The best thing

you can do is not respond and delete the email.

The scammer has no control over your computer. They just hope you'll be frightened enough to believe them and send money. By ignoring them, you take away all their power.

### **We're here to help**

We understand how stressful it can be to receive an email like this, especially when it mentions something as personal as your password. If you ever feel unsure or need help figuring out what's real and what's not, feel free to reach out to us. The only real concern here is that your password may have been leaked, and anything using that password should be changed.

**We can help you set up a password manager and two-factor authentication to keep your accounts safe. Don't be afraid to give us a call; we're here to help you feel safer and more confident with your computer.**

**Call us today at 940-282-0290.**