Barracuda

Click Thinking Extra

Deepfakes and phishing

How this emerging digital threat is impacting one of online's oldest dangers.

This is Not Your Parent's Phish

Phishing has long been a prevalent cyber threat. However, the integration of deepfakes into phishing tactics has elevated the sophistication and effectiveness of these attacks.

By creating realistic videos or audio recordings featuring prominent individuals such as corporate executives, government officials, or celebrities, malicious actors can deceive targets into believing they are interacting with a legitimate source. This deception not only increases the likelihood of victims falling for phishing schemes but also undermines trust in institutions and public figures.

Moreover, deepfake technology allows attackers to customize phishing attempts based on the preferences and vulnerabilities of individual targets. By analyzing extensive data collected from social media profiles and online activity, cybercriminals can craft highly personalized and convincing messages tailored to exploit specific interests, relationships, or concerns of their targets. This targeted approach significantly enhances the success rate of phishing attacks by evading traditional detection methods and leveraging the psychological vulnerabilities of victims.

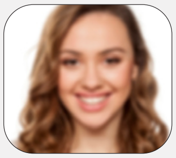
Deepfake technology lets attackers customize phishing attempts based on the vulnerabilities of individual targets.

The integration of deepfakes into phishing tactics represents a concerning evolution in cyber threats, presenting significant challenges for cybersecurity professionals and individuals alike.

To mitigate the risks associated with deepfake-enabled phishing, it is important to remain vigilant, adopt proactive security measures, and foster greater awareness of the potential dangers posed by synthetic media manipulation.

Identifying Deepfake Content

Although deepfake content can be difficult to spot, there are several things you can look and listen for that can help you identify whether content is authentic or artificial. Here are some:



a

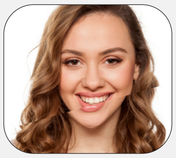
Pay attention to areas where the face might be blurred or distorted, indicating manipulation. (a)

Eyes that don't blink naturally or seem to lack focus can be a sign of manipulation.

b

Look for unnatural movements or expressions that don't align with the context or emotions of the video. (b)

Pay attention to speech patterns that sound robotic or unnatural, indicating the voice may have been synthesized.



c

Check for unusual artifacts or glitches in the video, especially around the face or background. (c)

d

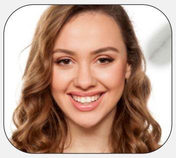
Check if the lips don't sync with the audio, which may suggest the video has been altered. (d)

Listen for discrepancies in audio quality, such as sudden changes in background noise or tone.

Look for inconsistencies in lighting and shadows that don't match the environment or other objects in the scene. (e)

e

Watch for inconsistencies or distortions in backgrounds, such as strange reflections or movement. (f)



f

Whenever possible, verify the authenticity of the video or voice message with trusted sources or additional context.