

Les dangers de l'art généré par IA et de l'hypertrucage

En quoi consistent l'art généré par IA et les hypertrucages?

L'art généré par IA utilise des milliards d'images et d'exemples d'œuvres d'art. Lorsque vous le lui demandez, le générateur d'art par IA construit une image en combinant plusieurs de ces exemples en une seule image. La technologie de l'hypertrucage est semblable, sauf qu'elle comprend la manipulation de véritables photographies et vidéos de vraies personnes et de vrais endroits. Cette technologie peut donner l'impression qu'une personne a dit ou fait quelque chose, alors que ce n'est pas le cas. L'utilisation de ces deux technologies peut être inoffensive, mais les cybercriminels ont appris comment les utiliser de manière malveillante.

Escroqueries utilisant l'hypertrucage

Les escrocs peuvent utiliser des technologies d'hypertrucage pour se faire passer pour des célébrités ou autres personnalités publiques. Ce type d'escroquerie peut donner l'impression qu'une célébrité cautionne un produit, alors que ce n'est pas le cas. Les escrocs utilisent cette technique pour tromper les gens et les amener à acheter un faux produit. Ils en profitent pour voler les renseignements personnels et financiers du consommateur. Les hypertrucages peuvent également exploiter des personnalités politiques. L'hypertrucage d'une vidéo peut donner l'impression qu'un représentant du gouvernement a dit ou fait quelque chose qu'il n'a ni fait ni dit. Ce type de vidéo peut être utilisé pour tromper les gens et les inciter à visiter un faux site Web ou à cliquer sur un faux article de nouvelles.

Art généré par IA et escroquerie photographique

Cyberkriminelle setzen KI häufig für Onlinebetrug in Zusammenhang mit einer angeblichen Partnersuche („Love Scamming“ oder „Romance Scamming“) ein. Sie nutzen gefälschte Fotos in Dating-Profilen, um Geld oder Informationen von ihren Opfern zu entwenden. Cyberkriminelle nutzen auch aktuelle Ereignisse für Betrug. Beispielsweise erstellen sie mithilfe von KI realistische Fotos von Katastrophen und anderen Ereignissen. Sie veröffentlichen die Fotos auf gefälschten Websites, um ihre Opfer dazu zu bewegen, Geld an eine Wohltätigkeitsorganisation zu spenden. Die Organisation gibt es in Wirklichkeit selbstverständlich gar nicht und die Cyberkriminellen greifen die Spenden ab.

Que puis-je faire pour me protéger?

Mettez en pratique les conseils suivants pour vous protéger des escroqueries liées à l'art généré par IA :

- Les images générées par IA présentent de subtiles variations ou erreurs. Soyez à l'affût de tout ce qui peut sembler inhabituel dans une photo. Par exemple, une main ayant plus de cinq doigts ou un éclairage ou des ombres inhabituels sont des signes courants qu'une image a été créée à l'aide de l'IA.
- Prenez toujours un temps d'arrêt et réfléchissez avant de cliquer ou d'entreprendre une action. Si une photo ou une image vous paraît bizarre ou trop belle pour être vraie, il pourrait s'agir d'une escroquerie.
- Lorsqu'il est possible de le faire, vérifiez l'information auprès d'une autre source. Par exemple, si vous voyez une vidéo d'une célébrité cautionnant un produit, vérifiez le site Web officiel de cette personne pour avoir la preuve qu'elle est réellement impliquée avec ce produit.

