Píldora Informativa

GPIT

DEEPFAKES

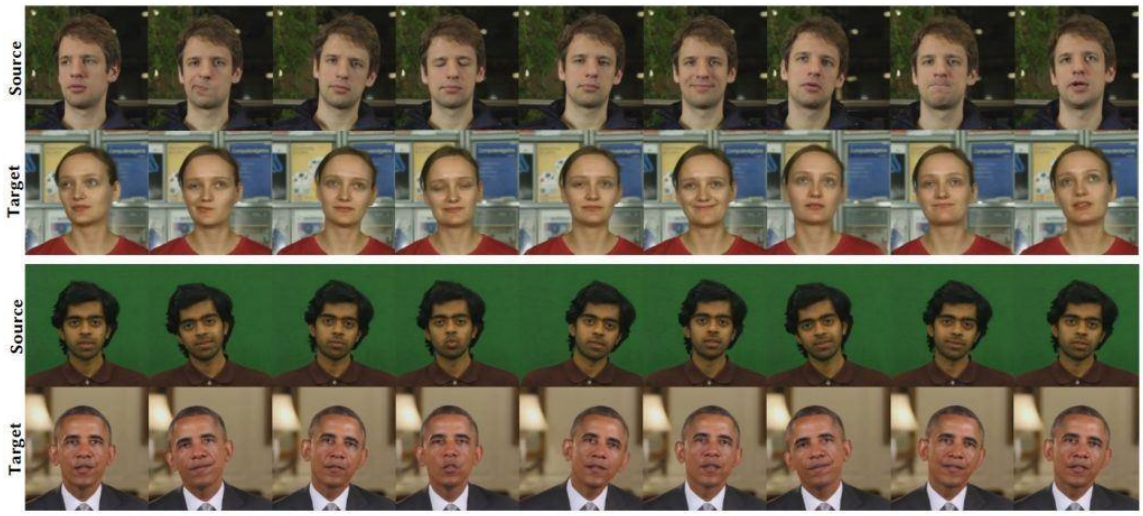
No. 005

UNAD
GRUPO FUNCIONAL DE SEGURIDAD
IFORMATICA - GFSI
28/11/2022

¿Qué es deepfake?

El nombre de deepfake viene de Deep Learning, lo que traduce como "*aprendizaje profundo*", que viene de la Inteligencia Artificial. Para seguridad de la información, es lo aprendido con inteligencia artificial para usarse con la intención de crear contenido falso.

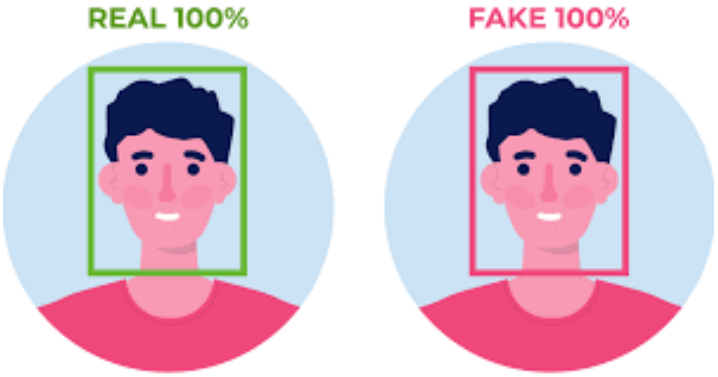
Se basa en la manipulación de videos, en donde el software analiza el material de origen y extrae parte de él y luego lo adapta en un nuevo video. Los ejemplos más comunes son el intercambio de la cara de las personas conocidos como *deep video portraits*.



Tomado de https://www.iebschool.com/blog/wp-content/uploads/2019/05/deepfakes-que-son-1024x472.jpg

Esto da para que sea difícil la detección de que es real y que no lo es, aunque no es imposible de validar, ya que se trabaja con técnicas de style transfer (transferencia de estilo).

Los ataques deepfake se realizan muy similar a un ataque de phishng, la única diferencia es que utiliza elementos tecnológicos que realizan la simulación de que un individuo entra en contacto directo con la víctima (posiblemente haciéndose pasar por un conocido) con el fin de realizar un ataque o acción ilícita. Teniendo en cuenta lo anterior, el ataque deepfake es la falsificación de la identidad de un individuo.



Tomado de https://www.sivsa.com/site/wp-content/uploads/2022/01/deep_fake-SIVSA.jpg

Tipos de ataque

Estos pueden ser no sólo por video, sino también por audio.

- Grabación de un audio

El ataque se realiza cuando el delincuente se hace pasar por otra persona, usa rasgos de una persona concreta para engañar a la víctima que recibe este contacto.

Tomado de https://liukin.es/wp-content/uploads/2022/09/Deepfake-audio-tiene-un-indicador-y-los-investigadores-pueden-detectarlo.jpg

- Grabación de vídeo

El ataque se realiza por medio de vídeos en donde el delincuente tiene el conocimiento de evitar las tecnologías para la seguridad.

Tomado de: https://www.rrhhdigital.com/userfiles/ciberataques_fuera.jpg

Formas de prevención de los ataques

En primera instancia debe considerarse que no existe un sistema que garantice el 100% de la seguridad, por lo que por más seguros que sean, pueden ser susceptibles a los ataques. A continuación, se mencionan algunos puntos para la prevención de ataques deepfake.

- Fortalecimiento de la identidad del usuario

Es importante crear y tener medios o accesos para que un usuario pueda identificarse siempre de manera segura a través de los respectivos servicios de la empresa. Por esto se puede tener en cuenta el MFA (Multi-factor authentication). Para que un usuario acceda al sistema, se necesita que sea aprobado a través de un segundo acceso.

- Mapeo del tráfico de la red

Los ataques deepfake generan un tráfico considerable en la red debido al uso de redes sociales, es esencial que se tenga un mapeo total sobre lo que realmente está transitando en la red. Es importante que se consiga visualizar la gestión que realizan las aplicaciones que se están usando (el tráfico que utiliza).

- Uso de herramientas adicionales de seguridad

Es importante el uso de herramientas adicionales de seguridad que dificulten los ataques (provenientes de la falsificación de la identidad de usuarios). Se deben evaluar y valdar los canales de comunicación que se utilizan, así como las herramientas de comunicación internas. Es importante que se utilice solo las aplicaciones que están validadas por el equipo de TI y en conformidad con la política de seguridad que se tenga.

BIBLIOGRAFÍA

Vídeos falsos y deepfake: ¿cómo pueden protegerse los usuarios? Tomado de: https://latam.kaspersky.com/resource-center/threats/protect-yourself-from-deep-fake

¿EN QUÉ CONSISTEN LOS ATAQUES «DEEPFAKES» Y CÓMO PROTEGER A TU EMPRESA? Tomado de: https://www.telcomanager.com/es/blog/en-que-consisten-los-ataques-deepfakes-y-como-proteger-a-tu-empresa/

Cómo prevenir y detectar ataques deepfakes, según los expertos. Tomado de: https://www.muyinteresante.es/tecnologia/articulo/como-prevenir-ataques-deepfakes-segun-los-expertos-351622047607

Deepfakes: Qué es, tipos, riesgos y amenazas. Tomado de: https://www.lisainstitute.com/blogs/blog/deepfakes-tipos-consejos-riesgos-amenazas

¿Qué son los Deepfakes y cómo detectarlos? Tomado de: https://www.iebschool.com/blog/deepfakes-como-detectarlas-business-tech/

Que es un Deep fakes, cómo se crean, cuáles fueron los primeros y su futuro. Tomado de: https://www.esic.edu/rethink/tecnologia/deep-fakes-que-es-como-se-crean-primeros-y-futuros

GPIT - Gerencia de plataformas e infraestructura tecnológica
VIEM – Vicerrectoría de Innovación y Emprendimiento
Seguridad Informática
Tel: 601-3443700 Ext 1687
UNAD