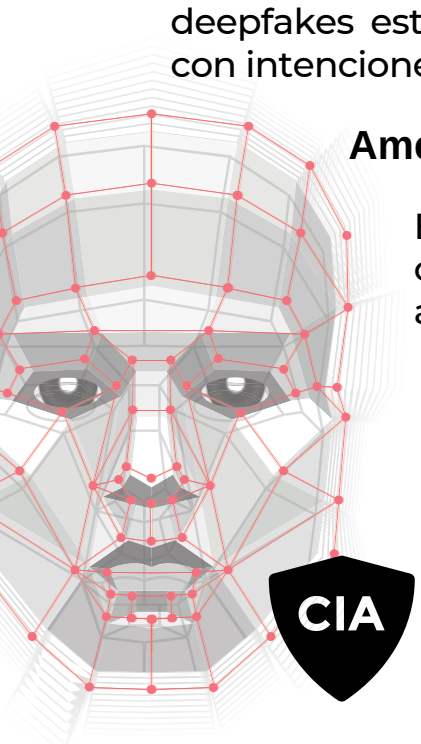
SEPTIEMBRE 2024

NEWSLETTER

1 LA CIA PUBLICA UN INFORME SOBRE DEEPFAKES Y ESTRATEGIAS PARA MANEJAR ESTA AMENAZA

Los deepfakes son técnicas de manipulación de contenido que utilizan inteligencia artificial y aprendizaje automático para crear vídeos, audios, imágenes o textos sintéticos que parecen reales, pero son falsos. Esta tecnología ha avanzado rápidamente, haciendo que la creación de deepfakes esté al alcance de casi cualquier persona, incluyendo aquellos con intenciones maliciosas.



Amenazas Asociadas a los Deepfakes

El informe de la CIA, junto con otras agencias de seguridad como la NSA, FBI y CISA, destaca varios peligros significativos asociados a los deepfakes:

- Daño a la imagen de las organizaciones: Los deepfakes pueden ser utilizados para desprestigiar a empresas y personas.
- Imitación de ejecutivos y personal de finanzas: Suplantar la identidad de altos cargos para cometer fraudes.
- Falsificación de comunicaciones: Acceso no autorizado a redes privadas mediante la manipulación de comunicaciones.

Técnicas de Protección

El informe clasifica las técnicas de protección en dos grandes grupos: detección y autenticación.

Detección

Técnicas forenses: Buscan rastros estadísticamente significativos de manipulación en el contenido para identificar posibles deepfakes.

Autenticación

Marcas de agua: Incorporación de señales que legitimen el origen del contenido.

Demostración de vida: Verificación de que el contenido es generado por un ser humano real.

Hashing del dispositivo: Inclusión de información del dispositivo que crea o edita el contenido para su posterior validación.

Sabias que...

SOPHOS

En Grupo BeIT brindamos las mejores soluciones en colaboración con nuestro socio Sophos y su solución Extended Detection and Response (XDR), aplicamos capacidades avanzadas de detección, respuesta y análisis. Esta herramienta es esencial para mitigar los riesgos asociados con la tecnología emergente. Esta plataforma nos permite obtener una visión completa del entorno, identificar amenazas y actuar de manera proactiva para proteger nuestros sistemas contra ataques sofisticados. **¡Mantenerte seguro en el mundo digital es nuestra prioridad!.**

Fuente: CSI-DEEPFAKE-THREATS.PDF (defense.gov)

admmarketing@buromc.com

SEPTIEMBRE 2024

NEWSLETTER

2 “VISHING” SOFÍA NIÑO DE RIVERA VÍCTIMA DE CIBERDELINCUENTES.

La comediante mexicana tendencia en redes sociales tras ser víctima de ciberdelincuentes.

El vishing, es una estrategia de los ciberdelincuentes, que se presenta como una forma de ingeniería social similar al phishing y al smishing, tiene como objetivo obtener información personal y bancaria de los usuarios.

El fraude se lleva a cabo mediante llamadas telefónicas, en las cuales el delincuente se hace pasar por una entidad de confianza.

Sofía Niño le contó al diario El Universal ¿Cómo sucedió todo?

Recibí una llamada por la tarde. “Hablamos de tal banco, ¿es usted Sofía Niño de Rivera con terminación de tarjeta tal?” Tenían varios de mis datos personales. Me dijeron: “Estamos viendo que alguien está haciendo un cargo en una página de autopartes de Mercado Libre. ¿Es usted?” Respondí que no.

El individuo, con un discurso aparentemente profesional, me instruyó para seguir una serie de pasos que, según él, eran necesarios para prevenir un cargo no reconocido en mi cuenta.

“Vamos a tener que hacer una investigación porque alguien está tratando de robarte la identidad y usar tu tarjeta. Tenemos que rastrear el IP de la computadora donde lo están haciendo para poder atraparlos. Toda esta investigación va por cuenta del banco, nosotros nunca te vamos a pedir ningún dato”, me aseguró. Irónicamente, el que me estaba haciendo fraude, me decía qué hacer para evitar ser víctima de fraude.

Para iniciar la supuesta investigación sobre la dirección IP del comprador, el estafador me sugirió que no accediera a mi banca electrónica ni utilizara la aplicación del banco. Siguiendo sus instrucciones, desactivé el reconocimiento facial que tenía configurado para acceder a mi cuenta bancaria.

“Debes ir al cajero y presionar un botón que permitirá bloquear la tarjeta”, me dijeron. Fui al banco, retiré dinero y verifiqué la cantidad que tenía, sin preocuparme porque ahí estaba mi dinero.

Tras varios días, exigí que terminaran la presunta investigación. Fue entonces cuando me informaron que mi cuenta de fondo de inversión había sido completamente despojada. “Nos dimos cuenta de que te quitaron todo el fondo de inversión”, me dijeron. Les colgué, entré a la app y ya no tenía dinero. Todo lo del fondo de inversión se lo robaron".

admmarketing@buromc.com