Publicado en Madrid el 26/06/2023

Claves para protegerse de ‘deepfakes' en periodo electoral

Uno de los principales objetivos de la tecnología deepfake es el engaño mediante difusión de información falsa, práctica que cada vez es más habitual entre la ciberdelincuencia principalmente en periodos electorales. Según ha advertido S2 Grupo, los ciberdelincuentes pueden difundir noticias falsas que cambien la percepción de la opinión pública, lo que puede tener un impacto tremendo en unas elecciones, por ejemplo

Según ha informado la compañía de ciberseguridad en un comunicado, todo lo que se necesita para el uso de esta tecnología, está accesible desde los mercados clandestinos, pero también en foros abiertos como GitHub. "Cada vez resulta más sencillo conseguirlos y esto ha hecho que se haya incrementado el caso de ciberestafas de phishing. Normalmente, haciéndose pasar por un político, un líder empresarial u otras personalidades famosas", ha declarado Miguel A. Juan, socio-director de S2 Grupo.

En este sentido, la compañía advierte de que los peligros y objetivos de los ciberdelincuentes con el uso de las deepfakes son principalmente: la desestabilización de organizaciones a través de afirmaciones falsas y engaños, la pornografía de personajes famosos (se calcula que representan hasta el 96% de los deepfakes que circulan por Internet), la manipulación electoral, la ingeniería social a través de audios haciendo creer que una persona de confianza ha dicho algo, ataques de desinformación automatizados como teorías de conspiración o robos de identidad de personas reales en los que se crean documentos falsos o se falsifica la voz de las víctimas.

Ante la relevancia de este tipo de tecnología con fines engañosos, el equipo de expertos de S2 Grupo ha desarrollado un decálogo con claves sobre las deepfake, con el fin de conocerlas mejor para evitar caer en su trampa:

Hay 3 tipos de deepfakes:
Lo primero de todo es saber identificar las campañas de deepfakes. Por un lado, están las campañas de desinformación en las que se edita el contenido legítimo para cambiar el significado original de una noticia o vídeo. Se incluyen el uso de imágenes de una persona que no se encontraba en el lugar como, por ejemplo, pornografía de venganza. Pero también se encuentran los deepfakes con cambios en logotipos o imágenes. En tercer lugar están los deepfakes sintéticos que derivan de una colección de originales para crear una nueva versión.

Según advierte S2 Grupo, aunque es difícil reconocer una deepfake, se pueden detectar al observar movimientos forzados o actividades inusuales, como el movimiento ocular antinatural; la falta de parpadeo; las expresiones faciales, forma del cuerpo o cabello antinaturales. Además, las deepfakes no pueden replicar los colores de la piel. "La posición facial es otro posible indicativo de que lo que se está viendo no se corresponde con la realidad". Hay veces en las que a través de la iluminación es posible detectar sombras fuera de lugar. En otras ocasiones, es evidente la mala sincronización de las

palabras con la boca de la persona que está hablando.

Las ciberestafas más comunes relacionadas con las deepfakes:

Estafas de mensajería.
Business E-Mail Compromise (BEC). Aunque esta estafa ya es muy común sin la tecnología deepfake, los estafadores también pueden usar videollamadas para hacerse pasar por alguien de la empresa y pedir dinero.
Confección y secuestro de cuentas. Evadiendo la verificación de identidad, los delincuentes pueden crear cuentas en bancos con documentos de identidad robados y retirar o transferir dinero.
Chantaje. Los ciberdelincuentes pueden crear tecnologías deepfake para usarlos como método de extorsión.
Campañas de desinformación para manipular a la opinión pública, lo que puede conllevar consecuencias financiera, políticas y reputacionales.
Estafas de soporte técnico. Por ejemplo, pueden usar identidades falsas para crear ingeniería social con el fin de que los usuarios compartan credenciales de pago.
Ataques de ingeniería social que manipulen a familiares y conocidos de la persona suplantada.
Secuestros de dispositivos IoT. Como los deepfakes pueden suplantar la voz o la apariencia física de una persona, pueden usarse para desbloquear dispositivos.

Recomendaciones para evitarlos:

Activar el doble factor de autenticación. Desde S2 Grupo se recomienda a las organizaciones autenticar a un usuario con tres factores básicos: algo que el usuario tiene, algo que el usuario sabe y algo que el usuario es.
La concienciación del personal de la empresa y el principio de conocer a su cliente (KYC) son fundamentales.
Los usuarios de las redes sociales deben minimizar la exposición de imágenes personales de alta calidad.
Priorizar el uso de patrones biométricos como el iris o las huellas dactilares para verificar cuentas sensibles como las del banco.

Datos de contacto:
Luis Núñez Canal
667574131

Nota de prensa publicada en: Madrid

Categorías: Nacional Sociedad Ciberseguridad