ANALISIS PRIMARIO.(DISPARADOR)
Cómo protegerte contra los deepfakes

Las tecnologías de deepfake pueden usarse para robar tu identidad incluso si no utilizas plataformas de IA generativa.

Probablemente has oído hablar de la IA generativa (inteligencia artificial), pero quizás no estés al tanto de que estas tecnologías han traído consigo nuevas preocupaciones sobre privacidad, robo de identidad y desinformación. Una forma perniciosa de estafa de IA se llama tecnología "deepfake".

Los deepfakes son videos o clips de audio generados por inteligencia artificial que hacen parecer que alguien está diciendo o haciendo algo que nunca hizo. Solo con esta definición, las posibilidades de robo de identidad y desinformación pueden volverse obvias para ti. Los deepfakes pueden usarse para difamar a las personas y cometer fraudes. Por ejemplo, si tu identidad vocal e información sensible llegaran a las manos equivocadas, un ciberdelincuente podría usar audio deepfake para contactar a tu banco.

Puedes pensar que como no usas ningún producto de IA nunca podrías ser una víctima. La verdad es que estas tecnologías pueden recolectar datos (como videos, fotografías y grabaciones de voz) de millones de personas de sitios web, como plataformas de redes sociales.

Puedes tomar algunas medidas para reducir las posibilidades de que un criminal cree un deepfake tuyo. Principalmente, deberías pensar detenidamente sobre lo que compartes públicamente. Aquí hay algunas estrategias para protegerte, y algunos consejos sobre qué hacer si sospechas que eres víctima de un deepfake.

Comparte con cuidado: El primer paso para evitar los deepfakes es ser extremadamente cauteloso con la información personal que compartes en línea. Limita la cantidad de datos disponibles sobre ti, especialmente fotos y videos de alta calidad, que podrían usarse para crear un deepfake. Puedes ajustar las configuraciones de las plataformas de redes sociales para que solo personas de confianza puedan ver lo que compartes. Por supuesto, también debes asegurarte de confiar en cualquiera que solicite seguirte o agregarte como amigo.

Habilita configuraciones de privacidad fuertes: Aprovecha al máximo las configuraciones de privacidad de los sitios web para controlar quién puede acceder a tu información personal y contenido. Restringe quién puede ver tus fotos, videos y otros datos sensibles. Esto incluye sitios web donde almacenas archivos de fotos. Reduce la cantidad de material disponible públicamente y minimizas los recursos que pueden tener los creadores de deepfakes potenciales.

Marca de agua en fotos: Al compartir imágenes o videos en línea, considera usar una marca de agua digital en ellos. Esto puede desalentar a los creadores de deepfakes de usar tu contenido, ya que hace que sus esfuerzos sean más rastreables.

Infórmate sobre los deepfakes y la IA: El ámbito de la IA está cambiando rápidamente. Mantenerse al tanto de los últimos desarrollos puede ayudarte a estar vigilante. No necesitas convertirte en un experto, pero seguir las noticias sobre estas tecnologías es importante para todos. Este conocimiento puede ayudarte a reconocer posibles señales de alerta al encontrar contenido sospechoso.

Utiliza la autenticación multifactor: Hoy en día, realmente deberías duplicar tu seguridad implementando autenticación multifactor para todas tus cuentas. Esto es cuando necesitas un paso

extra para iniciar sesión en una cuenta, como un escaneo facial, ingresar un código enviado por mensaje de texto a tu teléfono, o usar una aplicación independiente en tu dispositivo. Esta capa extra de seguridad ayuda a prevenir el acceso no autorizado a tus cuentas, reduciendo las posibilidades de que alguien obtenga tus datos personales.

Usa contraseñas largas, fuertes y únicas: Cada contraseña debe tener al menos 16 caracteres de longitud, ser única para la cuenta, y contener una mezcla aleatoria de letras mayúsculas, minúsculas, números y caracteres especiales. La mejor manera de recordar todas estas contraseñas únicas es almacenándolas en un gestor de contraseñas con MFA activado.

Mantén tu software actualizado: Mantén tus dispositivos y software actualizados con los últimos parches de seguridad y actualizaciones. El software desactualizado puede tener vulnerabilidades que los hackers pueden explotar para acceder a tus datos. Recomendamos activar las actualizaciones automáticas para no tener que estar revisando constantemente por nuevas actualizaciones.

No caigas en el cebo del phishing: Ten mucho cuidado al recibir correos electrónicos, mensajes directos, mensajes de texto, llamadas telefónicas u otras comunicaciones digitales si la fuente es desconocida. Esto es especialmente cierto si el mensaje exige que actúes rápidamente, como afirmando que tu computadora ha sido hackeada o que has ganado un premio. Los creadores de deepfakes intentan manipular tus emociones para que descargues malware o compartas información personal. Verifica la identidad del remitente y evita hacer clic en enlaces sospechosos. Siempre decimos: piensa antes de hacer clic.

Informa sobre contenido deepfake: Si encuentras contenido deepfake que te involucra a ti o a alguien que conoces, infórmalo a la plataforma que aloja el contenido. Esto puede ayudar a que sea eliminado o investigado, limitando su alcance potencial. También debes informarlo a las autoridades federales.

Consulta asesoría legal: Si eres víctima de un deepfake que ha dañado tu reputación, consulta con expertos legales en ciberseguridad y privacidad de datos. Las leyes están evolucionando rápidamente para abordar el problema de los deepfakes, pero con la tecnología cambiando tan rápido, el sistema legal tarda en ponerse al día. Puedes tomar medidas: contacta a tus representantes electos y diles que quieres ver más acciones para prevenir los deepfakes.

Mientras los deepfakes presentan un nuevo terreno en la batalla contra la desinformación y la difamación, puedes tomar medidas proactivas para proteger tu identidad digital. De hecho, este consejo es bueno para protegerte de otras amenazas cibernéticas comunes. Mantente informado, adopta estos hábitos de ciberseguridad y piensa detenidamente sobre lo que publicas en línea, así como sobre quién tiene acceso a ello.