¡Alto a la trata de personas!

SensibilizarAbogarActuar

Boletín de lucha contra la trata de personas • Octubre 2025 • Vol. 23 • No. 10

ENFOQUE: El boletín de este mes se centra en el uso creciente de deepfakes y su papel en la explotación.

Los sistemas de Inteligencia Artificial (IA) han permitido a las personas trabajar de forma más eficiente. Sin embargo, los ciberdelincuentes abusan de esta misma tecnología para producir desnudos deepfake y crear audios, vídeos e imágenes falsos, pero con una apariencia y un sonido realistas.

Los **deepfakes** son fotos o vídeos manipulados para mostrar a una persona haciendo algo que no ha hecho. Para crear un deepfake, se combinan datos antiguos y nuevos para producir algo falso. El software de reconocimiento facial es tan avanzado que cualquier persona puede aparecer en una imagen deepfake. Por ejemplo, se puede colocar el rostro de un niño en el cuerpo de otra persona para crear imágenes de abuso sexual.

La tecnología deepfake, que antes se asociaba principalmente con la desinformación política y el entretenimiento, ahora se está utilizando indebidamente en escuelas y otros lugares como una forma insidiosa de ciberacoso. A diferencia del acoso tradicional, los deepfakes permiten la creación de contenido sexual realista pero falso, que muestra a estudiantes en situaciones inventadas, dañinas y comprometedoras.

Los deepfakes también pueden ser creados por las llamadas "apps de desnudez", en las que una persona sube una foto de otra persona y la app genera una foto falsa de desnudo. Han surgido casos relacionados con el uso de estas apps en escuelas secundarias y preparatorias de todo el mundo, donde las adolescentes son frecuentemente víctimas de sus compañeros varones. Recientemente, el **FBI emitió una advertencia** a los padres y a cualquiera que publique fotos en redes sociales después de que una foto de "regreso a clases" se haya convertido en un deepfake. El FBI también advirtió que compartir este tipo de imágenes de menores es ilegal.

La producción de deepfakes no consensuados y sexualmente explícitos ha aumentado significativamente en los últimos dos años. Estos se utilizan a menudo como herramientas de chantaje, acoso o humillación pública, causando trauma, ansiedad, pérdida de confianza personal, daño a la reputación e incluso el retiro de la vida social o profesional de las víctimas. El uso indebido de los deepfakes puede adoptar muchas formas dañinas, como fraude financiero, manipulación emocional y abuso sexual facilitado por la tecnología. La naturaleza engañosa de los deepfakes no solo viola la privacidad y la seguridad personal, sino que también subraya la urgente necesidad de fuertes protecciones legales y salvaguardas tecnológicas.

Trata de Personas y Deepfakes

El rápido avance de las tecnologías de Inteligencia Artificial (IA), en particular los Deepfakes, plantea desafíos alarmantes en la lucha contra la trata de personas al facilitar la explotación, el abuso y el reclutamiento. Según el Law Journal for Social Justice, los traficantes pueden utilizar la tecnología Deepfake para crear imágenes o vídeos falsos convincentes de víctimas para la explotación sexual comercial en línea. Los Deepfakes también contribuyen a la producción y difusión de material de abuso sexual infantil (CSAM).

Reconocer los desafíos que plantean estas tecnologías es esencial para desarrollar sistemas de apoyo eficaces para las víctimas. El realismo de los Deepfakes dificulta enormemente que las víctimas

(continúa en la página siguiente

Sensibilizar

Trata de Personas y Deepfakes

demuestren que las imágenes o los vídeos no son auténticos, lo que puede agravar su trauma y dificultar su capacidad para buscar ayuda. Al comprender cómo los traficantes manipulan estas tecnologías, podemos prepararnos mejor para reconocer y contrarrestar sus tácticas.

El auge de la inteligencia artificial también ha tenido un profundo impacto en la lucha contra la trata sexual, ofreciendo nuevas herramientas a las fuerzas del orden. Sin embargo, a día de hoy, el rápido desarrollo de la IA ha superado los marcos legales que la rigen.

Los deepfakes también se utilizan en el porno de venganza, a menudo motivado por el deseo de vengarse de una expareja. El porno de venganza se utiliza para buscar poder sobre el sujeto de las imágenes o intimidarle.

El papel de los deepfakes en la sextorsión

Tras el suicidio de Elijah Heacock, un adolescente de Kentucky de 16 años descrito como "un adolescente vibrante que hacía sonreír a la gente", sus padres descubrieron que había recibido mensajes de texto amenazantes exigiendo $3,000 dólares para eliminar una imagen suya desnuda generada por IA. Era sólo uno de los miles de adolescentes y preadolescentes estadounidenses víctimas de chantaje digital.

La muerte de Elijah también puso de relieve cómo los avances en inteligencia artificial, como los deepfakes, las aplicaciones de "desnudez" y la pornografía generada por IA, agravan el delito de sextorsión, en el que se chantajea a personas tras enviar fotos, mensajes de texto o información comprometedora a alguien que resulta ser un estafador. Quienes usan deepfakes en la sextorsión toman fotos comunes de redes sociales y las manipulan para crear imágenes falsas y explícitas.

El agresor exige dinero para evitar la distribución de contenido deepfake que muestra su imagen en posiciones sexuales. El impacto de estas estafas va mucho más allá de las pérdidas económicas. Los ciberdelincuentes crean material deepfake que mancha la reputación de la víctima. Se aprovechan del miedo a la humillación pública. Este miedo suele impulsar a las víctimas a actuar con rapidez para evitar un escándalo. La mayoría de las víctimas de sextorsión son hombres de entre 10 y 17 años, aunque ha habido víctimas de tan solo siete años, y también se ha atacado a niñas. La sextorsión es un delito federal con una pena de hasta dos años en casos de víctimas adultas y de hasta tres años en casos de víctimas menores de edad.

Generadores de imágenes con IA: Los delincuentes emplean software avanzado diseñado para alterar imágenes. Dos tipos comunes de estas herramientas son los autocodificadores y las redes generativas antagónicas (GAN). Estos programas pueden analizar conjuntos de datos de rostros y crear nuevas imágenes que parecen reales.

Scraping de redes sociales: Plataformas como Instagram y Facebook están repletas de fotos personales. Estas imágenes, a menudo compartidas públicamente, se convierten en blancos fáciles para quienes buscan crear desnudos deepfakes. Al recopilar imágenes de estos sitios, los estafadores cuentan con una rica fuente de material para sus proyectos.

Servicios de alojamiento anónimo: Una vez creado el deepfake de desnudo, necesita un lugar seguro donde almacenarse. Aquí es donde entran en juego los servicios de alojamiento anónimo. Estas plataformas permiten a los creadores subir su contenido ocultando su identidad y, a menudo, no cumplen con las prácticas de la Ley de Derechos de Autor del Milenio Digital (DMCA) para gestionar las infracciones de derechos de autor en internet.

Digital Forensics Corporation

*El 17 de julio de 2025, el **FBI advirtió** sobre un "número alarmante de suicidios" asociados con el chantaje mediante aplicaciones "nudify" impulsadas por inteligencia artificial.*

Pornografía Sintética

Otro tipo de contenido multimedia que puede conducir al abuso sexual basado en imágenes virtuales es la pornografía sintética (PS). Esta se diferencia de los deepfakes en que estos últimos incluyen rostros reales de personas y características identificativas en cuerpos ajenos a los suyos, mientras que la pornografía sintética implica cuerpos ficticios generados por IA que participan en actividades sexuales. Aunque la PS no muestra rostros reales de niños, es importante saber que este tipo de contenido multimedia puede contener cuerpos infantiles y ser potencialmente dañino.

El 41 % de las mujeres de entre 18 y 29 años se autocensuran para evitar el acoso en línea.

Acoso en línea, abuso digital y ciberacoso en Estados Unidos

El Congreso y los deepfakes

En diciembre pasado, más de dos docenas de mujeres congresistas y un congresista, representando a diversas afiliaciones partidarias y zonas geográficamente dispersas, fueron víctimas de deepfakes sexualmente explícitos. Las víctimas no estaban afiliadas a ningún partido ni tenían conexión geográfica.

El American Sunlight Project (ASP), un grupo de expertos que investiga la desinformación y promueve políticas que apoyan la democracia, publicó la semana pasada hallazgos que identifican más de 35,000 menciones de imágenes íntimas no consensuadas (NCII) relacionadas con miembros del Congreso. El ASP no divulgó los nombres de los legisladores para evitar fomentar la búsqueda de las imágenes. Se contactó con las oficinas de todas las personas afectadas por las imágenes para alertarlas y ofrecerles recursos sobre daños en línea y apoyo para la salud mental.

El ASP señaló que las imágenes se eliminaron con relativa rapidez, algo que, según afirmaron, no suele ocurrir con las mujeres afectadas por deepfakes que no son congresistas. También indicó que las eliminaciones no impiden que el material se comparta o se vuelva a publicar. La ASP también señaló que los daños de la IA y los deepfakes afectan desproporcionadamente a las mujeres y a las comunidades marginadas.

Casi el 16 % de las mujeres que actualmente sirven en el Congreso —o aproximadamente 1 de cada 6 congresistas— son víctimas de imágenes íntimas no consensuadas generadas por IA. La ASP también advierte que el abuso sexual basado en imágenes puede tener efectos devastadores en la salud mental de las víctimas, entre las que se incluyen personas comunes que no participan en la política, incluidos los niños.

"Más del 90% de todos los videos Deepfake que se hacen son imágenes sexualmente explícitas no consensuadas, y las mujeres son el objetivo 9 de cada 10 veces," dijo Alexandria Ocasio-Cortez, quien también ha sido blanco de este tipo de Deepfakes.

Abogar

¿Son ilegales los deepfakes?

Es ilegal usar voces deepfake en llamadas automáticas, según una resolución de la FCC de 2024. En general, las leyes de suplantación de identidad que prohíben hacerse pasar, por ejemplo, por un médico o un funcionario del gobierno, pueden aplicarse a los deepfakes. Por otro lado, incluso en la industria del entretenimiento, que lleva mucho tiempo lidiando con los problemas de deepfake, las leyes están desfasadas.

La Oficina de Derechos de Autor de EE. UU. examina las obras generadas por IA caso por caso y agradece las aportaciones del público sobre estos temas, ya que las protecciones de la libertad de expresión suelen aplicarse a los deepfakes, siempre que no incurran en difamación, obscenidad ni fraude. Para más información, visite la Conferencia Nacional de Legisladores Estatales.

*Estadísticas de Deepfake de 2024 de **Security.org***

- *Según una encuesta de McAfee, el 70% de las personas afirmó no tener confianza en su capacidad para distinguir entre una voz real y una clonada. Sin embargo, el 40 % de los participantes en el mismo estudio afirmó que ayudaría si recibiera un mensaje de voz de su cónyuge que necesitara ayuda.*
- *Los delincuentes pueden usar un pequeño fragmento de la voz de una persona para atacar a sus seres queridos con fines monetarios, quizá simulando una situación en la que parecen necesitar ayuda en una situación difícil. Una de cada diez personas afirma haber recibido un mensaje clonado de este tipo, y el 77% de estas personas perdió dinero debido a estafas.*
- *Según Google Trends, las búsquedas de "software gratuito de clonación de voz" aumentaron un 120% entre julio de 2023 y 2024. Los usuarios no necesitan grandes conocimientos técnicos para generar audio manipulado con estas aplicaciones gratuitas.*
- *A veces, bastan tres segundos de audio para producir una coincidencia de voz del 85% entre la voz original y la clonada.*
- *Las noticias falsas, las mentiras o los rumores pueden propagarse más rápido que las noticias veraces, lo que explica la eficacia de los deepfakes. Provocan reacciones emocionales y ofrecen nuevas perspectivas. En un estudio, el 1% de los rumores más comunes en Twitter (ahora X) llegó a entre 1,000 y 100,000 personas, mientras que las noticias veraces rara vez superaban las 1,000.*

Ley DEFIANCE

La Ley para Interrumpir las Imágenes Falsificadas Explícitas y las Ediciones No Consensuales (Ley DEFIANCE) de 2025 es una propuesta de ley federal estadounidense destinada a combatir las falsificaciones digitales íntimas no consensuadas, a menudo conocidas como "Deepfakes". La Ley Defiance define un "Deepfake" sexualmente explícito no consensuado como una "representación visual creada mediante el uso de software, aprendizaje automático, inteligencia artificial o cualquier otro medio informático o tecnológico para aparentar ser auténtica" que "muestra a la víctima desnuda o participando en conductas o escenas sexuales explícitas".

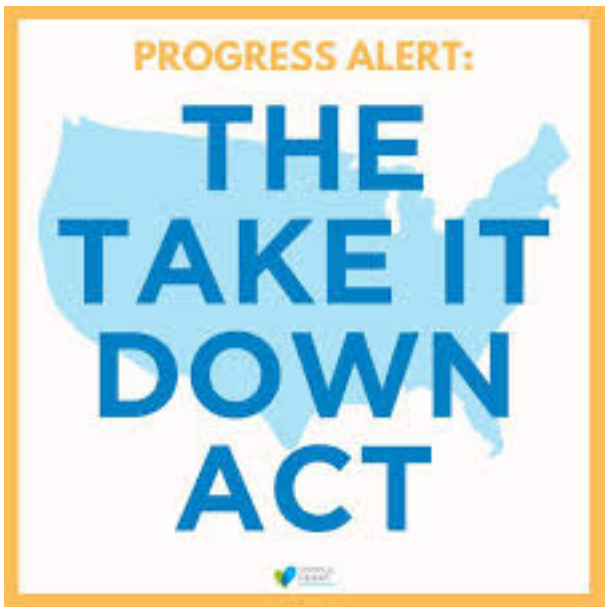
El proyecto de ley otorgaría a las víctimas el derecho a emprender acciones civiles contra quienes, a sabiendas, produzcan, distribuyan, soliciten, reciban o posean falsificaciones digitales sexualmente explícitas no consensuadas con la intención de distribuirlas. El plazo de prescripción para este recurso es de 10 años. El texto del proyecto de ley está disponible aquí.

"El contenido sexualmente explícito 'Deepfake' se utiliza a menudo para explotar y acosar a mujeres y niñas, y nadie debería ver violada su privacidad ni su autonomía por alguien que genere contenido explícito generado por IA. Aunque las imágenes puedan ser falsas, el daño a las víctimas es muy real. Las víctimas han perdido sus trabajos, su reputación y muchas han sufrido depresión o ansiedad que les ha alterado la vida. Con la *Ley DEFIANCE*, devolvemos el poder a las víctimas; tomamos medidas enérgicas contra la producción, recepción, distribución y posesión de imágenes 'Deepfake'; y exigimos responsabilidades a los responsables de las imágenes."

-Senador Durbin al reintroducir la Ley DEFIANCE

La Ley Take It Down

La Ley TAKE IT DOWN fue firmada por el presidente el 19 de mayo de 2025, tras ser aprobada tanto por la Cámara de Representantes como por el Senado. La ley penaliza la difusión no consentida de imágenes íntimas en línea, incluyendo las creadas mediante IA (deepfakes), y exige que las plataformas cuenten con un proceso de "notificación y eliminación". Cabe destacar que la ley establece explícitamente que el consentimiento para crear una imagen no implica el consentimiento para su distribución. Esto significa que, incluso si una persona ha compartido voluntariamente una imagen o un vídeo íntimo con alguien, publicarlo sin su consentimiento explícito ahora constituye un delito. La plataforma debe eliminar las imágenes cuando la persona representada lo solicite



Abogar

Cómo los deepfakes pueden ayudar a las fuerzas del orden

Las fuerzas del orden utilizan inteligencia artificial para detectar y desmantelar las redes de trata de personas. Analizan datos en línea en busca de patrones e identifican actividades sospechosas. Herramientas como IDentify y Track de Veritone pueden cruzar imágenes y rastrear a personas a través de múltiples grabaciones de cámaras, lo que desempeña un papel crucial en esta lucha. Sin embargo, es importante tener en cuenta que estas herramientas tienen sus limitaciones y no son una solución para todos los problemas relacionados con la trata.

Thorn desarrolló Spotlight, que utiliza IA para analizar una gran cantidad de datos en línea en busca de indicios de trata infantil. El rápido desarrollo de la IA puede superar la capacidad de los marcos legales para abordar el uso indebido de deepfakes en la trata de personas.

Abordar este desafío requiere un enfoque multifacético que incluya no únicamente soluciones tecnológicas y una legislación sólida, sino también la colaboración entre gobiernos, organizaciones no gubernamentales, y la industria tecnológica, considerando cuidadosamente las implicaciones éticas del uso de la IA en esta lucha.

A raíz de un incidente de alto perfil en el que imágenes sexualmente sugerentes de la cantante Taylor Swift generadas por inteligencia artificial se volvieron virales en X, anteriormente Twitter, varios legisladores presentaron una legislación estatal y federal para combatir el problema

La Ley de Gavin, oficialmente la Ley 54 de 2023 en Carolina del Sur, tipifica la extorsión sexual como delito grave. Aborda específicamente el chantaje mediante imágenes o vídeos sexualmente explícitos, con penas agravadas si la víctima es menor de edad, un adulto vulnerable o si sufre daños a causa del delito. La ley también exige que las escuelas eduquen a los estudiantes sobre los peligros y las consecuencias de la extorsión sexual. Recibe su nombre en memoria de Gavin Guffey, un adolescente de Carolina del Sur que se suicidó tras ser extorsionado sexualmente.

Desafíos legales y éticos

La tecnología deepfake se ha convertido en un desafío importante para quienes trabajan en ciberseguridad y gobernanza. Muchas leyes existentes no fueron diseñadas para abordar situaciones donde el contenido no es real, lo que dificulta la aplicación de los marcos legales tradicionales.

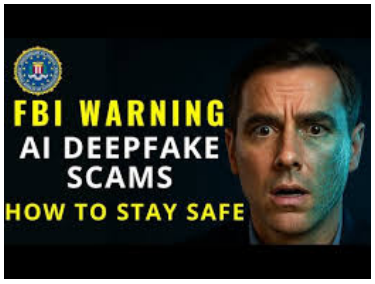
Dado que el contenido utilizado en la sextorsión deepfake es inventado, a menudo crea una zona gris que los delincuentes pueden explotar. Cuando alguien es perjudicado por información falsa, sus opciones de recurso son limitadas, dejando a las víctimas con una sensación de indefensión y desprotección. Por favor haga clic aquí para obtener más información.

Digital Forensics Corp

Digital Forensics Corp ayuda a empresas y particulares a recuperarse de ataques digitales, como chantajes en línea, desnudos falsos y estafas de sextorsión.

Con el auge del chantaje en línea y la sextorsión, han creado un sistema que permite descubrir la identidad de los chantajistas y detener sus actividades maliciosas. Mediante tecnologías avanzadas, como el rastreo de IP a ubicación, pueden obtener la ubicación y los datos de los autores e interceder en nombre del cliente. También garantizan la rápida eliminación del contenido explícito y, en caso de filtraciones, trabajan para minimizar la exposición.

FBI



En junio de 2023, el FBI advirtió que los avances tecnológicos en IA llevarían las estafas a un nivel alarmante a través de deepfakes y programas de generación de rostros. El FBI insta a las víctimas a denunciar la explotación llamando a la oficina local del FBI, al 1-800-CALL-FBI o en línea en tips.fbi.gov.

Aquí hay algunas recomendaciones que los padres pueden tomar para proteger a sus hijos adolescentes de ser víctimas de una amenaza creciente.

- Configuración de privacidad al máximo

Es fundamental utilizar una configuración de privacidad eficaz. Asegurarse de usar configuraciones extremadamente restrictivas para que la información sólo sea visible para las personas dentro de su red de contactos.

- Lea la letra pequeña de los términos y condiciones de las redes sociales.

Es fundamental revisar la configuración de sus redes sociales para asegurarse de que el contenido no sea visible fuera de su red. Es común que las aplicaciones sociales compartan una parte significativa de los datos de uso, la información personal y, a veces, la biometría de una persona con terceros, lo cual suele indicarse en sus términos y condiciones. Leer estos acuerdos a fondo es la mejor práctica para garantizar que sus datos, fotos y otra información confidencial no caigan en manos de personas maliciosas.

- Tenga una conversación honesta.

La mejor manera de evitar que los adolescentes se pongan en peligro en línea es informarles de los riesgos que pueden cambiar sus vidas. También es fundamental que los padres informen a sus hijos que pueden y deben acudir a ellos si son víctimas de sextorsión, enfatizó Frank Ahearn, experto en privacidad que asesora a personas que sufren chantaje.

#CCRI Cyber Civil Rights Initiative

Si ha sido víctima de abuso sexual basado en imágenes, la Iniciativa de Derechos Civiles Cibernéticos mantiene una lista de recursos legales

Actuar

Cómo identificar deepfakes

Puede identificar un deepfake combinando varios métodos. Security.org sugiere los siguientes consejos:

- Revise el contenido en cuestión para detectar si hay alguna etiqueta o anuncio que indique que se ha generado artificialmente o que es un deepfake. Muchos creadores de contenido, artistas y otros etiquetan su contenido generado por IA como tal.
- Busque movimientos bruscos, distorsiones y movimientos poco naturales, como parpadeos excesivos (o ausencia de parpadeo).
- Preste atención a las inconsistencias en los rasgos faciales. Preste especial atención a las mejillas y la frente. También, busque vello facial o lunares que parezcan inusuales. Si la persona usa gafas, ¿reflejan el funcionamiento natural de la luz? Si la persona se mueve, ¿también cambia el ángulo del reflejo en las gafas?
- Analice los patrones de habla para detectar diferencias en la tonalidad y el tono en comparación con el habla humana cotidiana.
- Verifique que los movimientos de los labios coincidan con las palabras habladas.
- Considere si la persona en cuestión estaría en realidad en esta situación, diciendo o haciendo tales cosas.
- Revise la foto o el video para detectar marcas de agua digitales. Estas marcas de agua pueden ser visibles (como un logotipo), pero es posible eliminarlas o alterarlas. A pesar de ser visibles, son útiles para la protección de derechos de autor y pueden ser combinadas con otros tipos.

Puede usar software de detección de deepfakes. Los deepfakes de audio son más difíciles de identificar que los de imagen y video. Además, son más fáciles y económicos de crear. Identificar deepfakes de audio requiere un alto nivel de experiencia, y sólo unos pocos laboratorios en todo el mundo pueden hacerlo de forma fiable.

security.org

Centro Nacional para Niños Desaparecidos y Explotados

El año pasado, el Centro Nacional para Niños Desaparecidos y Explotados recibió más de 10,000 denuncias relacionadas con sextorsión. El NCMEC (por sus siglas en inglés) cuenta con recursos gratuitos para ayudar a los niños a afrontar una situación abrumadora y aterradora. El NCMEC también ofrece un servicio gratuito llamado "Take It Down," que ayuda a las víctimas a eliminar o detener la publicación en línea de imágenes o videos sexualmente explícitos.

American Academy of Pediatrics

DEDICATED TO THE HEALTH OF ALL CHILDREN™

Para obtener más información sobre los posibles impactos de las imágenes alteradas por IA, consulte la respuesta del portal de la Academia Americana de Pediatría: El impacto de los deepfakes, la pornografía sintética y el material virtual de abuso sexual infantil.

Si usted es padre, madre o cuidador de un niño víctima de abuso sexual generado por IA y basado en imágenes, aquí encontrará consejos sobre cómo proceder y recursos de la Academia Americana de Pediatría que pueden ser útiles.

El impacto de los deepfakes

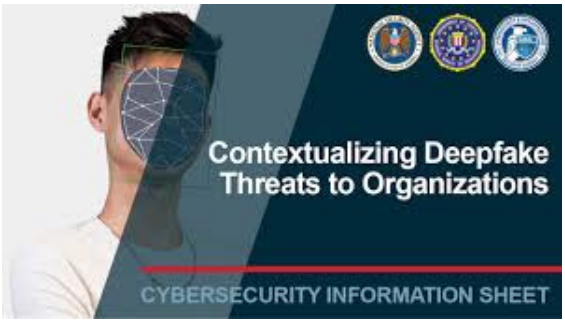
'Crianza digital: Criando a la generación de la IA'

Valerie Castro, de NBC News, destaca a una adolescente víctima de deepfakes en línea. Los expertos, la Dra. Jennifer Hartstein y Adam Dodge, participan en directo para hablar sobre cómo afrontar los peligros de los deepfakes y cómo proteger a sus hijos. Haga clic **aquí** para ver este video de 12 minutos.

La Fundación Ra

La Fundación Ra es una organización sin fines de lucro 501(c)3, liderada por sobrevivientes, que apoya a niños, mujeres y hombres víctimas de abuso sexual basado en imágenes en línea. También trabaja incansablemente para proteger y prevenir a cualquier tipo de víctima de abuso sexual basado en imágenes, independientemente de sus antecedentes, creencias, preferencias, decisiones personales o circunstancias. Creemos que todas las personas merecen ser tratadas con dignidad y respeto

FOUNDATION RA
#PROTECTMYIMAGE



La NSA y las agencias federales de EE. UU. asesoran sobre las amenazas de deepfakes

La Agencia de Seguridad Nacional (NSA por sus siglas en inglés) y sus socios, agencias federales de EE. UU., han emitido un aviso sobre una amenaza mediática conocida como deepfakes. Esta amenaza emergente podría representar un desafío para la ciberseguridad de los Sistemas de Seguridad Nacional (NSS), el Departamento de Defensa (DoD) y las organizaciones del DIB. Publicaron la Hoja de Información de Ciberseguridad (CSI) conjunta, "Contextualizando las amenazas de deepfakes para las organizaciones", para ayudar a las organizaciones a identificar, defenderse y responder a las amenazas de deepfakes. La NSA elaboró la Hoja de Información de Ciberseguridad con contribuciones del Buró Federal de Investigaciones (FBI) y la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA).

Las imágenes íntimas no consensuadas generadas por IA plantean amenazas a la seguridad nacional al propiciar el chantaje y las concesiones geopolíticas. Esto podría tener un impacto en los responsables políticos, independientemente de si son el objetivo directo de las imágenes.

Actuar

Thorn, en colaboración con el Centro Nacional para Niños Desaparecidos y Explotados (NCMEC por sus siglas en inglés), descubrió que alrededor del 10% de los reportes de sextorsión monetaria en 2023 involucraban imágenes que no eran auténticas. Esta cifra no ha hecho más que crecer a nivel mundial. Además, la investigación de Thorn con jóvenes reveló que 1 de cada 6 menores que experimentan interacción sexual en línea nunca lo revelan a nadie.

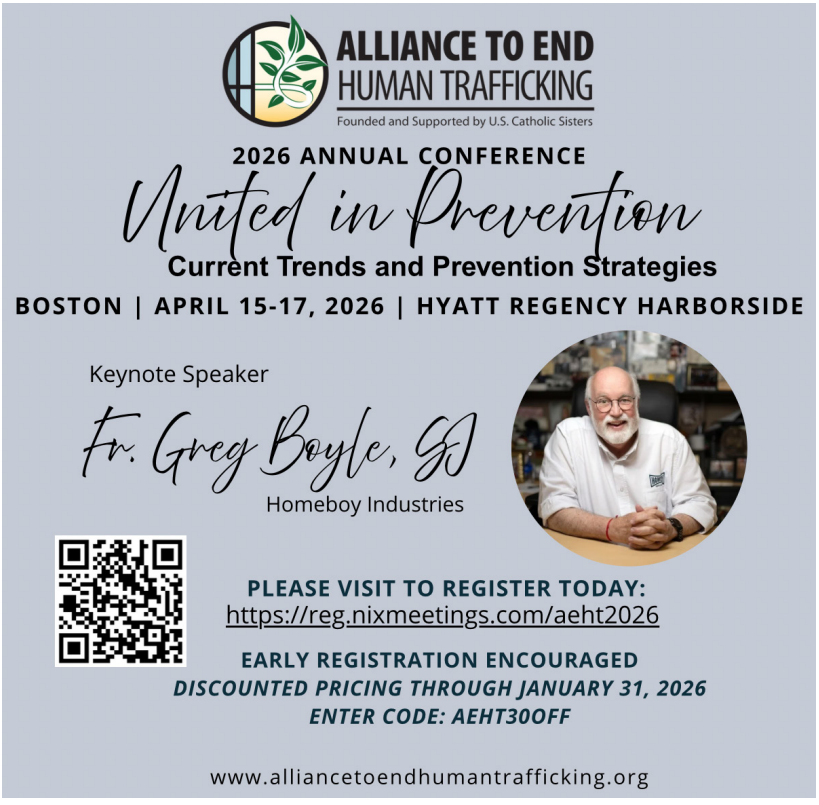
Los niños pueden ser menos propensos a revelar que son víctimas de delitos sexuales, a menudo debido a las expectativas sociales y las normas de género que los disuaden de hablar.

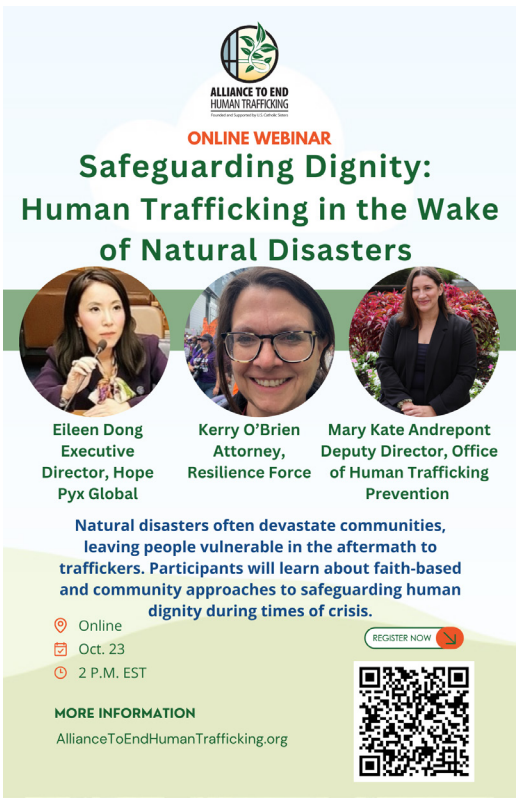
Cuando se trata de deepfakes, el miedo a no ser creído puede intensificarse, creando una barrera aún mayor para buscar ayuda. Las conversaciones abiertas y continuas sobre seguridad en línea son esenciales, pero también debemos reconocer que los niños no siempre recurren primero a sus padres y cuidadores.

El programa de prevención juvenil NoFiltr de Thorn permite a los adolescentes interactuar con sus compañeros sobre temas importantes relacionados con la seguridad en línea.

El consejo para los adolescentes de "No compartas desnudos" puede ser insuficiente. Los deepfakes sólo magnifican las deficiencias de este mensaje. Los niños que nunca han tomado ni compartido una imagen explícita de sí mismos ahora pueden ser fácilmente blanco de sextorsionistas mediante la creación de imágenes con IA generativa.

La sextorsión financiera ocurre en línea a diario. Sus efectos han tenido graves consecuencias entre las víctimas jóvenes, incluyendo autolesiones. Comprender por qué un menor puede ser reacio a buscar apoyo y tomar medidas para reducir esas barreras puede salvar vidas.





¿Qué puede hacer si usted o su hijo/a son víctimas?

La siguiente información proviene de la Academia Estadounidense de Pediatría. Recuerde que publicar o compartir imágenes íntimas sin su permiso es un delito.

Si usted es padre/madre o cuidador/a de un/a menor víctima de abuso sexual basado en imágenes generadas por IA, es fundamental hacerle saber que está ahí para él/ella y que no es su culpa. Tome medidas para garantizar la seguridad de su hijo/a.

Bloquee y denuncie al agresor o agresora. Solicite la eliminación de las imágenes. Utilice la herramienta "Take It Down" del Centro Nacional para Niños Desaparecidos y Explotados para ayudar a eliminar imágenes o videos explícitos si la víctima es menor de 18 años y no participa en plataformas en línea. Si la víctima tiene 18 años o más, puede utilizar la herramienta StopNCII.org. En el sitio web de Cyber Rights Initiative, puede encontrar una guía detallada de eliminación en línea para ayudarle a eliminar imágenes de Facebook, Instagram, Twitter, Reddit, Tumblr, Yahoo, Google y Microsoft.

También puedes informar a la Comisión Federal de Comercio si una empresa publica su imagen sin su consentimiento y no la retira.

Si es víctima, mantenga la calma y denuncie la estafa inmediatamente al FBI o a su agencia local de seguridad. Puede contactar con la policía o la oficina del Fiscal de Distrito si prefiere que el asunto se resuelva en un tribunal penal. Supongamos que la persona que comparte las imágenes es su pareja actual o anterior, o un familiar. En ese caso, puede acudir al Tribunal de lo Familiar para obtener una Orden de Protección en su contra y evitar que comparta las imágenes. Denuncie la cuenta del depredador a través de la función de seguridad de la plataforma. La mayoría de las plataformas y aplicaciones en línea ofrecen una forma de denunciar a usuarios abusivos. Las víctimas de deepfakes pueden reclamar una indemnización por daños y perjuicios.

Puede encontrar enlaces a abogados de bajo costo o pro bono (voluntarios gratuitos) en el sitio web de Cyber Rights Initiative.

Si es víctima de explotación sexual de imágenes, llame a la Línea de Ayuda para Crisis de Cyber Civil Rights Initiative Crisis Helpline al 844-878-2274 para obtener apoyo y asesoramiento.

No borre ninguna comunicación ni amenaza del chantajista. Tome capturas de pantalla o grabaciones de los mensajes, fotos, videos y cualquier información del perfil del agresor. Esta evidencia será valiosa para que las fuerzas del orden investiguen el delito y posiblemente identifiquen al chantajista.

Vigile los síntomas de salud mental y el bienestar general de su hijo/a: Esté atento a cambios inusuales en el estado de ánimo, los patrones de sueño, el apetito, los niveles de energía, el deseo de socializar con amigos y familiares, y la asistencia regular a la escuela y a las actividades extracurriculares. Consulte con su pediatra o profesional de la salud si nota algún cambio preocupante.

Un revelador segmento de 60 Minutos destaca el alarmante aumento de imágenes de desnudos generadas por IA y su devastador impacto, especialmente en niños. Vea el segmento completo de 60 Minutos aquí.

ALLIANCE TO END HUMAN TRAFFICKING

Founded and Supported by U.S. Catholic Sisters

Haga clic en el enlace abajo para visitar las páginas web de nuestras patrocinadoras

- Adorers of the Blood of Christ
- Adrian Dominicans
- Benedictine Sisters of Chicago
- Benedictine Sisters of Mount St. Scholastica, Atchison, KS
- Benet Hill Monastery
- Congregation of Notre Dame
- Congregation of Sisters of St. Agnes
- Congregation of S. Joseph
- Daughters of Charity, Province of the West
- Daughters of Charity, Province of St. Louise
- Daughters of the Holy Spirit
- Dominican Sisters of Houston, TX
- Dominican Sisters of Mission San Jose, CA
- Dominican Sisters of Peace
- Dominican Sisters of San Rafael, CA
- Dominican Sisters of Sinsinawa, WI
- Dominican Sisters of Sparkill
- Dominican Sisters of Springfield, IL
- Felician Sisters of North America
- Franciscan Sisters of Peace
- Franciscan Sisters of Perpetual Adoration
- Franciscan Sisters of the Sacred Heart
- Holy Spirit Missionary Sisters
- Institute of the Blessed Virgin Mary
- Marianites of Holy Cross
- Maryknoll Sisters
- Medical Mission Sisters
- Medical Missionaries of Mary
- Missionary Sisters of the Society of Mary
- Northern California Catholic Sisters Against Human Trafficking
- Our Lady of Victory Missionary Sisters
- Presentation Sisters, Aberdeen
- Presentation Sisters, San Francisco
- Racine Dominicans
- Religious of the Sacred Heart of Mary
- Religious Sisters of Charity
- School Sisters of Notre Dame, North America
- School Sisters of St. Francis of Christ the King
- Sisters of Bon Secours
- Sisters of Charity of Cincinnati
- Sisters of Charity of Halifax
- Sisters of Charity of Leavenworth
- Sisters of Charity of New York
- Sisters of Charity of St. Joan Antida
- Sisters of Charity of the Blessed Virgin Mary
- Sisters of Charity of the Incarnate Word - Houston
- Sisters of Charity of Nazareth
- Sisters of Charity of Seton Hill
- Sisters of Christian Charity Mendham, NJ & Wilmette, IL
- Sisters of Mercy Catherine's Residence
- Sisters of Mercy of the Americas
- Sisters of Notre Dame of the United States
- Sisters of Notre Dame de Namur, USA
- Sisters of Providence, Mother Joseph Province
- Sisters of St. Chretienne
- Sisters of St. Dominic - Racine, WI
- Sisters of St. Francis of Clinton
- Sisters of St. Francis of Colorado Springs
- Sisters of St. Francis of Dubuque
- Sisters of St. Francis of Mary Immaculate
- Sisters of St. Francis of Philadelphia
- Sisters of St. Francis of Redwood City
- Sisters of St. Francis of the Providence of God
- Sisters of St. Francis Rochester, MN
- Sisters of St. Joseph of Baden
- Sisters of St. Joseph of Carondelet
- Sisters of St. Joseph of Chestnut Hill Philadelphia
- Sisters of St. Joseph of Cluny, USA & Canada Provinces
- Sisters of St. Joseph of Concordia, KS
- Sisters of St. Joseph of Orange
- Sisters of the Blessed Sacrament
- Sisters of the Divine Savior
- Sisters of the Good Shepherd
- Sisters of the Holy Cross
- Sisters of the Holy Family
- Sisters of the Holy Names of Jesus and Mary
- Sisters of the Humility of Mary
- Sisters of the Precious Blood
- Sisters of the Presentation of the Blessed Virgin Mary
- Sisters of the Sacred Hearts
- Sisters of the Sorrowful Mother
- Society of the Divine Savior
- Society of the Holy Child Jesus
- Society of the Sacred Heart
- Southern CA Partners for Global Justice
- St. Mary's Institute of O'Fallon
- Tri-State Coalition Against Human Trafficking & Slavery
- U.S. Ursuline Sisters of the Roman Union

*El Boletín de Lucha contra la Trata de Personas está dedicado exclusivamente a promover un intercambio de información entre los miembros de la alianza, organizaciones y personas interesadas que colaboran para eliminar todas las formas de la trata de personas. Pulse **aquí** para acceder a los boletines previos de ¡Alto a la Trata de Personas! Para contribuir información, favor de contactar: stoptrafficking@feliciansisters.org. Editor: Maryann Agnes Mueller, CSSF. Diseño y presentación: Mary Francis Lewandowski, CSSF. Traducción al español: Teresa Lefranc.*