Consejos para protegerse

No proporcione información confidencial por teléfono, correo electrónico, mensajes de texto ni redes sociales.

No transfiera ni envíe dinero a lugares desconocidos.

Considere designar una "palabra de seguridad" para su familia que solo se comparta con los miembros de la misma y los contactos cercanos.

No proporcione ninguna información personal ni confidencial a un chatbot en línea.

Denuncie posibles estafas a las autoridades y a las empresas involucradas.

Para obtener más información sobre cómo protegerse a sí mismo y a los demás visite:

Comisión Federal de Comercio (FTC, por sus siglas en inglés):
https://www.consumer.ftc.gov/scams

Comité Especial del Senado de los EE.UU. para Asuntos de la Vejez

Línea de ayuda contra el fraude

El Comité para la Vejez opera una línea directa gratuita contra el fraude, que sirve como un recurso para que los adultos mayores estadounidenses y sus familiares denuncien actividades sospechosas, y proporciona información sobre cómo denunciar fraudes y estafas a los funcionarios correspondientes, incluidas las fuerzas del orden.

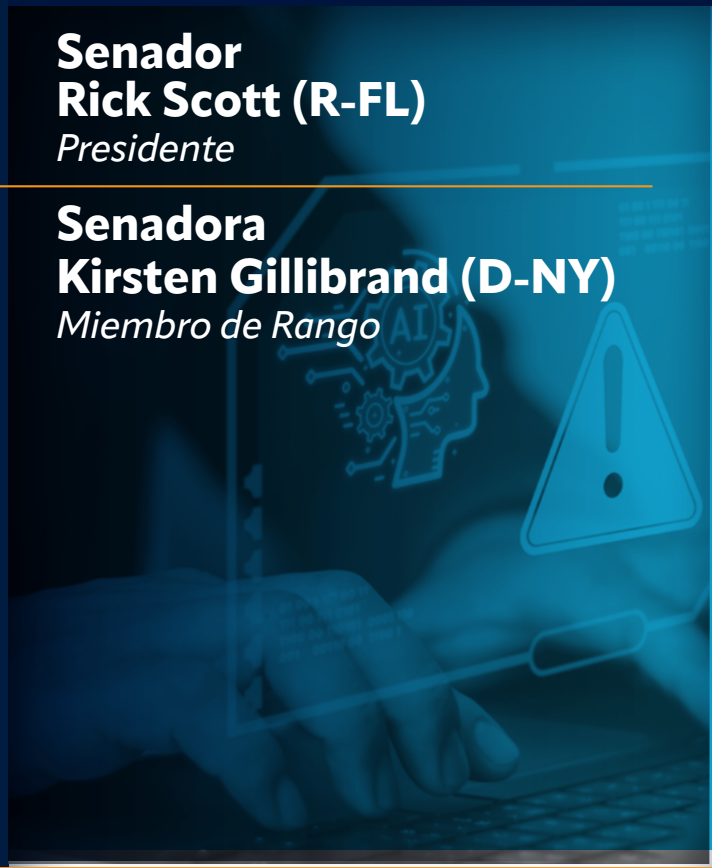
1-855-303-9470

Lunes a viernes 9AM a 5PM
Hora del Este (ET)

El Comité publica anualmente la Guía contra el Fraude para informar a los consumidores sobre las estafas comunes, las señales de alerta a las que deben estar atentos y los consejos para protegerse contra estafadores. Puede encontrarla aquí: www.aging.senate.gov.

Inteligencia Artificial:

Una amenaza emergente



Senador
Rick Scott (R-FL)
Presidente

Senadora
Kirsten Gillibrand (D-NY)
Miembro de Rango

Comité Especial del Senado de los EE.UU. para Asuntos de la Vejez

Comité Especial del Senado de los EE.UU. para Asuntos de la Vejez

¿Qué es la Inteligencia Artificial?

La Inteligencia Artificial (IA) es una tecnología que permite a las computadoras imitar ciertos comportamientos similares a los humanos, como el habla o la escritura. La IA, aunque es una herramienta útil en algunas circunstancias, puede ser explotada por los delincuentes para lograr que las estafas sean más convincentes.

Tres términos que debe conocer

1. Chatbots:

Un chatbot es un programa informático que utiliza la IA para simular una conversación humana, y podría usarse de forma maliciosa para obtener, almacenar o manipular sus datos personales.

2. Tecnología de clonación de voz:

La clonación de voz utiliza la IA para imitar la voz de alguien que quizás conozcas.

3. Deepfakes:

El deepfake (o ultrafalso) es un video o una imagen de apariencia auténtica generado por la IA.

Estafas con IA a las que debemos prestar atención

Ataques de phishing

Con el uso de la IA, los estafadores pueden personalizar rápidamente los correos electrónicos de *phishing* (suplantación de identidad), imitar el diálogo y eludir los filtros de correos no deseados o spam, lo que obstaculiza la distinción entre comunicaciones genuinas y fraudulentas.

Estafas de "emergencia familiar"

Los estafadores pueden utilizar la clonación de voz y los deepfakes para hacerse pasar por un ser querido que afirma estar en peligro y necesita dinero.

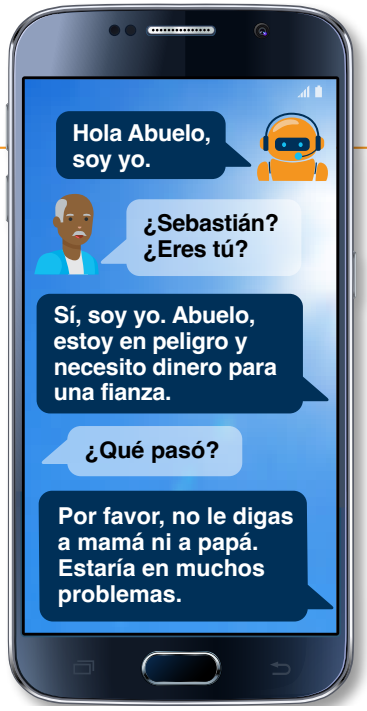
Estafas "románticas"

Los estafadores pueden utilizar la tecnología de IA para operar perfiles falsos en sitios web de citas y plataformas de redes sociales. Luego, los chatbots impulsados por IA simulan una conversación real para generar confianza, con el objetivo de engañar a la víctima para que le envíe dinero.

Ejemplos de IA en fraudes y estafas

Puede ser difícil saber si alguien está utilizando la tecnología de IA para realizar una estafa. Lo cierto es que la IA hace que los fraudes y estafas tradicionales resulten más fáciles de implementar a gran escala y son aún más convincentes.

Estafa de emergencia familiar falsa



Mensaje de texto falso

Actualización de Transacción:
Tu cuenta está siendo debitada por iPhone 13 USD $599.97.
¿No ha sido tu? Comunícate con Amazon al (888) ***-****