**Columna del Seguro Social**

# CÓMO DETECTAR UNA ESTAFA

Por <Name>

<Título> del Seguro Social en <Place>



Ahora es el momento perfecto para protegerse de estafas que pueden dañar sus finanzas y su reputación. ¡Podemos trabajar juntos para mantener segura su información personal!

Manténgase informado de las últimas tendencias en estafas

Los estafadores siguen cambiando de táctica. Asegúrese de comprender las últimas tendencias de estafas en [www.ssa.gov/espanol/estafas](https://www.ssa.gov/espanol/estafas/). Manténgase informado:

* Siguiendo fuentes de noticias confiables.
* Suscribiéndose a boletines informativos de alerta de estafas.
* Manteniéndose conectado con las agencias locales de orden público.

Cuanto más sepa, mejor preparado estará para identificar y evitar estafas.

Piense con cuidado antes de compartir información personal

El fraude electrónico (también conocido como *phishing*) es una de las formas principales en que los estafadores intentan engañar a las personas para que proporcionen información personal. Preste mucha atención a los correos electrónicos o mensajes que le soliciten su nombre de usuario, contraseña u otra información personal.

Los estafadores fingen pertenecer a organizaciones conocidas para ganarse su confianza. Manténgase alerta cuando reciba llamadas que no solicitó y afirman ser de bancos, agencias gubernamentales u otras empresas conocidas.

En caso de duda, contacte la organización directamente a través de los canales oficiales para verificar que la solicitud es real antes de compartir cualquier información personal o hacer un pago.

Utilice contraseñas seguras

Cree contraseñas seguras y únicas, como una frase con letras mayúsculas y minúsculas, números y caracteres especiales. No utilice contraseñas que sean fáciles de adivinar, como cumpleaños o nombres.

Considere utilizar un administrador de contraseñas para generar contraseñas únicas y almacenarlas de forma segura para cada una de sus cuentas por internet.

Sea inteligente con los códigos QR

Los códigos QR están ganando popularidad. Están en restaurantes, parquímetros, correos electrónicos y redes sociales.

¡Los estafadores se han dado cuenta! Están colocando físicamente códigos QR falsos encima de los oficiales o creando códigos QR falsos en anuncios de redes sociales para obtener acceso a su información personal.

Nunca escanee códigos QR casualmente. Si el código QR parece extraño o está alterado, no lo escanee.

Protege sus perfiles de redes sociales

Tómese un momento para revisar la configuración de privacidad en sus plataformas de redes sociales y limite la cantidad de información personal que comparte públicamente.

Los estafadores pueden usar sus publicaciones en las redes sociales para personalizar estafas u obtener acceso a sus cuentas sin su permiso. Revisa periódicamente su lista de amigos y elimina cualquier cuenta desconocida o sospechosa.

Este mes, hagamos una máxima prioridad protegernos contra las estafas. Podemos reducir significativamente el riesgo de ser estafados si se mantienen informados, están alertas y son cuidadosos, y salvaguardar sus cuentas.

Lo invitamos a ver nuestro video en [www.youtube.com/watch?v=cyaUWTFLw3c%20](https://www.youtube.com/watch?v=cyaUWTFLw3c%20) (solo disponible en inglés) para aprender a identificar las señales de alerta. Comparta esta información con quienes puedan necesitarla y publíquela en las redes sociales.

# # #