



Seguridad Cibernetica para personas mayores

Presentado por:

Shriyanka Hiremagalur

Senior, Notre Dame High School, San Jose

Aarini Naskar

Senior, Notre Dame High School, San Jose

Sahana Shyam

Junior, Notre Dame High School, San Jose

FBI RELEASE INFOGRAPHIC ON DEEPFAKE SCAMS

DEEPFAKE MEDIA SCAMS

Scams targeting Americans are surging.



Since 2020, the FBI has received
4.2 million+ reports of fraud.
That's **\$50.5 billion in losses.**



Imposter scams in particular are on the rise in the age of artificial intelligence (AI). Criminals are using deepfakes, or media that is generated or manipulated by AI, to gain your trust and scam you out of your hard-earned money.

Deepfakes can be altered images, videos or audio. They may depict people you know — including friends and family — or public figures including celebrities, government officials and law enforcement.

FBI RELEASE INFOGRAPHIC ON DEEPFAKE SCAMS

HOW TO DETECT A DEEPFAKE



LOOK FOR INCONSISTENCIES:

- Are any of the facial features blurry or distorted?
- Does the person blink too much or too little?
- Do the hair and teeth look real?
- Are the audio and video out of sync?
- Is the voice tone flat or unnatural?
- Does the visual show odd or unnatural shadows or lighting?

RED FLAGS OF A DEEPFAKE SCAM



Unexpected requests for money, passwords, personal information or secrecy.



Emotional manipulation involving fear or urgency.



Uncharacteristic communication from someone you know, especially over text, phone or video.

REPORT SCAMS



To **your**
local police



To the **FBI** at
IC3.Gov



To **your bank** if
you sent money

FBI ALERT: SCAMMERS IMPERSONATING AGENCY'S CYBER-CRIMES WEBSITE

- Los estafadores suplantán el sitio web del Centro de Denuncias de Delitos en Internet (IC3) de la agencia para engañar a los consumidores y conseguir que proporcionen información financiera.
- Un sitio web suplantado está diseñado para suplantar la identidad de un sitio web legítimo y puede utilizarse para robar información personal y facilitar estafas monetarias.



TIPOS:

- El FBI recomendó a los consumidores que ingresaran la dirección web del IC3 (www.ic3.gov) directamente en la barra de direcciones de su navegador para asegurarse de acceder a la dirección correcta.
- La agencia recomendó no hacer clic en resultados "patrocinados" en las búsquedas web del IC3, ya que podrían ser sitios falsificados. En su lugar, se recomendó verificar que la dirección termine en ".gov" y coincida con la del IC3.
- Las posibles víctimas deben reportar cualquier interacción con sitios web o personas que se hagan pasar por el IC3 a su oficina local del FBI o al IC3 a través de su dirección web oficial, indicó la agencia.



FEDERAL TRADE COMMISSION (FTC) WARNS CONSUMERS ABOUT SOCIAL MEDIA CHECK FRAUD SCAM

Las publicaciones en redes sociales que comparten un supuesto "hackeo" de una cuenta corriente son en realidad una estafa que podría ocasionar problemas financieros y legales.

Cómo funciona:

- El supuesto hackeo consiste en emitir un cheque por una cantidad mayor a la que tienes, depositarlo en una cuenta diferente y luego retirar el dinero antes de que el cheque (sin fondos) se procese por completo.
- Lo que el video o la publicación podrían no decirte es que podrías tener que pagar todo el dinero, ser expulsado de tu banco y enfrentarte a serios problemas legales por fraude bancario.



TIPOS:

Antes de sumarte a una tendencia viral:

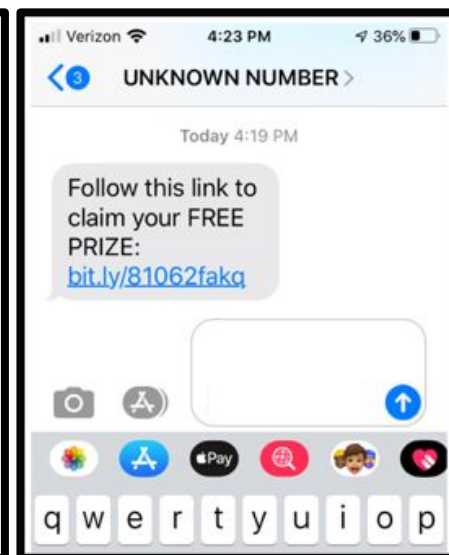
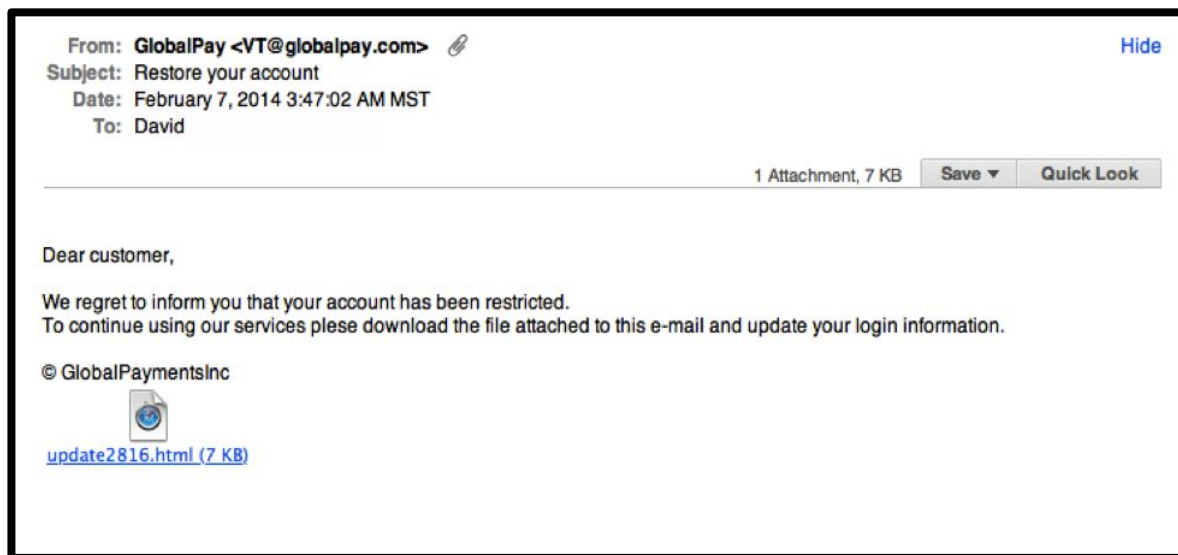
- ❑ Investiga. Busca la tendencia junto con términos como "estafa" o "fraude" para ver qué opinan otros al respecto. Habla con amigos y familiares para saber qué opinan.
- ❑ Piensa en la fuente. ¿Qué sabes de la persona o cuenta que la hace confiable?
- ❑ Compara los consejos de diversas fuentes reconocidas. No te fíes solo de lo que dice una persona o cuenta.

¿Qué es la ciberseguridad?



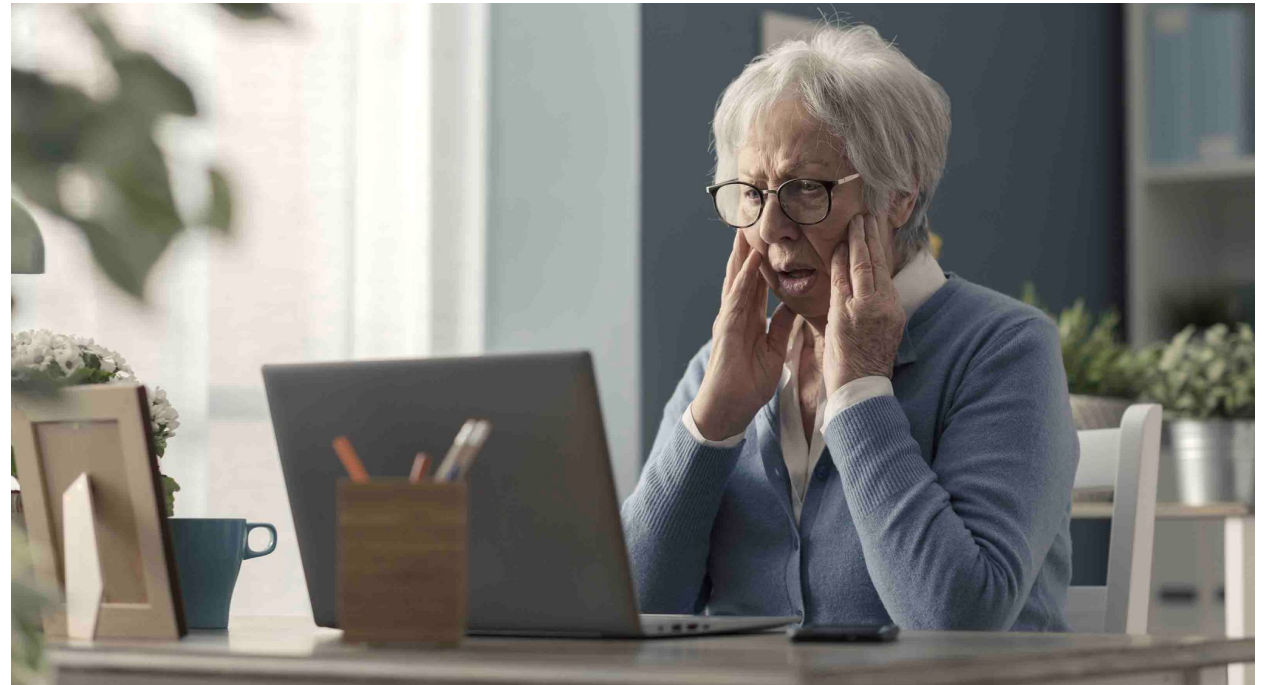
La ciberseguridad es la práctica de proteger los sistemas conectados a Internet, incluidos el hardware, el software y los datos, de ataques digitales y accesos no autorizados..

Pregunta: ¿Cuántos de ustedes aquí han recibido una llamada telefónica, un correo electrónico o un mensaje de texto sospechoso?



¿Por qué las personas mayores son el blanco de ataques?

- Es más probable que tengan más dinero.
- Pueden dudar en reportar estafas por miedo a perder su independencia.
- A menudo se los percibe como personas que no saben usar la tecnología, lo que los convierte en blancos fáciles para estafas telefónicas y en las redes sociales.
- Pueden tener discapacidades cognitivas o físicas que dificulten su juicio.





Pérdidas de personas mayores por delitos cibernéticos en 2023



TDM	729.89	915.51	185.62	▲25.43%	FLR	660.27	745.28	85.01	▲12.88%
HUM	749.73	924.29	174.56	▲23.28%	UVD	155.59	181.57	25.98	▲16.70%
DMW	833.72	1004.01	170.29	▲20.43%	QUV	440.55	540.21	99.66	▲22.62%
YZJ	903.49	1127.46	223.97	▲24.79%	HZT	285.51	344.98	59.47	▲20.83%
GLY	982.07	1219.39	237.32	▲24.17%	PCW	811.44	1029.66	218.22	▲26.89%
VDA	113.74	143.41	29.67	▲26.09%	AIK	361.77	451.39	89.62	▲24.77%
UVV	468.08	535.41	67.33	▲14.38%	ZJJ	858.36	994.57	136.21	▲15.87%
HJS	545.49	659.05	113.56	▲20.82%	RHJ	894.79	1046.68	151.89	▲16.97%
EQC	556.96	664.69	97.73	▲17.24%	VGV	425.08	509.95	84.87	▲19.97%

PPJ	912.63	1038.36	125.73	▲13.78%	ZGK	391.59	491.48	99.89	▲25.51%
UAQ	1309.55	1655.62	346.07	▲26.43%	BNY	969.21	1130.65	161.44	▲16.66%
DAQ	1295.17	1641.66	346.49	▲26.75%	SDM	735.44	913.39	177.95	▲24.20%
PNR	654.33	775.84	121.51	▲18.57%	TQQ	1323.91	1646.42	322.51	▲24.36%
ZTM	151.11	183.11	32.00	▲21.18%	OIS	543.42	667.21	123.82	▲22.79%

¿Qué estado creen ustedes que tiene el mayor número de quejas/pérdidas reportadas por personas mayores de 60 años?

Perdidas Mayores Estado:

2023 OVERALL STATE STATISTICS, COM

COMPLAINTS FILED BY INDIVIDUALS OVER 60			
Rank	State	Loss	Rate
1	California	\$643,230,534	3.1%
2	Florida	\$293,817,911	3.1%
3	Texas	\$278,320,107	3.1%
4	New York	\$203,437,635	3.1%
5	Illinois	\$137,940,620	3.1%
6	Arizona	\$127,977,700	3.1%
7	Pennsylvania	\$117,427,238	3.1%
8	New Jersey	\$104,087,085	3.1%
9	Virginia	\$94,037,054	3.1%
10	Georgia	\$92,422,609	3.1%

Mayores Quejas Estado:

2023 OVERALL STATE STATISTICS

COMPLAINTS FILED BY INDIVIDUALS OVER 60		
Rank	State	Count
1	California	11,622
2	Florida	8,138
3	Texas	7,035
4	Arizona	5,003
5	New York	4,328
6	Ohio	3,299
7	Pennsylvania	3,020
8	Colorado	2,905
9	Illinois	2,887
10	Washington	2,873

¿Cuáles son algunas
de las estafas de
fraude más
frecuentes que
afectan a las personas
mayores?



ESTAFA DE IMPOSTORES DE MEDICARE

Los estafadores llaman, envían correos electrónicos, mensajes de texto o mensajes en las redes sociales afirmando que:

- ❑ “avisarle” que su nueva tarjeta de beneficios de Medicare está lista.
- ❑ Ofreciéndole ayuda para registrarse o cambiar su plan.
- ❑ que es elegible para un dispositivo médico que no sabía que necesitaba.



ESTAFAS DE IMPOSTORES EN LA ADMINISTRACIÓN DEL SEGURO SOCIAL

Recibe una llamada, un correo electrónico, un mensaje de texto o un mensaje en las redes sociales advirtiéndole que:

- ❑ Sus beneficios del Seguro Social están a punto de expirar.
- o
- ❑ que serán suspendidos porque debes dinero por una razón que previamente no conocías.





Por Favor Recuerda:

“Si alguien que no conoces comienza a presionarte de inmediato (por teléfono, por mensaje de texto o de otra manera), eso es una **GRAN SEÑAL DE ALERTA**”.

Tácticas comunes que indican una estafa:

Estableciendo credibilidad.

Construyendo una buena relación.

Amenazándote.

Exigen pago.

Nunca confíes en el número que aparece en tu identificador de llamadas ni en la dirección de correo electrónico que aparece en tu bandeja de entrada.

¿Cómo puedo evitar las estafas de impostores del gobierno??

Cuelgue

Ya sea que reconozca el número en el identificador de llamadas o no, finalice inmediatamente cualquier llamada de alguien que no conozca.

Borre

Incluso si la dirección del remitente parece ser de una agencia gubernamental, no la abras. Envíala directamente a la carpeta de Papelera (basura).

Ignore

Si recibe un mensaje de texto o un mensaje directo en las redes sociales del IRS, SSA, Medicare, FTC u otra cuenta gubernamental, no responda.

RECUERDA....

Se Proactivo

Si le preocupa que una agencia gubernamental esté intentando comunicarse con usted legítimamente, sea proactivo.

Busca

Busque usted mismo la información de contacto de la agencia (vaya a su sitio web oficial)

No confíes en

No confíe en su identificador de llamadas o en un correo electrónico que haya recibido) y póngase en contacto de esa manera.

¿Qué debo hacer si me ha estafado un impostor del gobierno?

- Reporte lo que paso. Puede llamar a **National Elder Fraud Hotline** at 833-FRAUD-11 (833-372-831)
- Alerta a la Comisión Federal de Comercio (FTC) **online** or by phone at 877-FTC-HELP (877-382-4357).
- Finalmente, si los delincuentes consiguieron accesar su información personal, su dinero o ambos., el **FTC ofrece consejos paso-a-paso** que hacer.



Tenga en cuenta:

Si el IRS, la Administración del Seguro Social, Medicare u otra agencia gubernamental lo necesitan,
le enviarán una carta.

Estafas de Sorteos y Loterías



Debes pagar para reclamar tu premio.



Los estafadores afirman que pagar aumentará las probabilidades de ganar.



Solicitar información financiera.



Los estafadores le enviarán un cheque falso y le pedirán que devuelva parte del dinero.



Los estafadores te presionan para que “actúes ahora” para reclamar el premio.

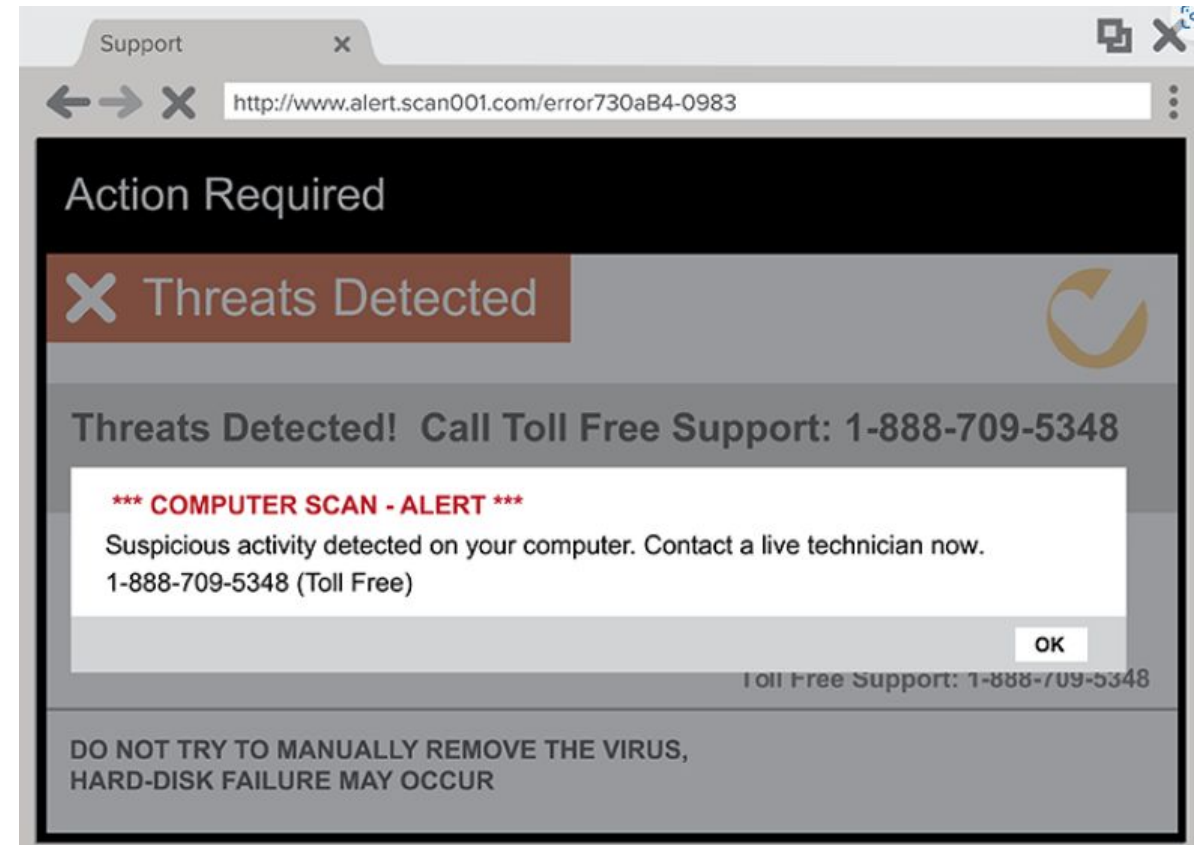


Consejos de Prevención

Aborda	Aborda los reclamos de premios inesperados con escepticismo.
Verificar	Verifica la legitimidad de la organización de lotería o sorteo de forma independiente.
Consultar	Consulte el sitio web de la organización o la información publicada, no el mensaje del remitente.
No compartir	No comparta información personal/financiera con contactos no solicitados.
No enviar	No envíe dinero ni realice pagos para reclamar un premio

Estafas de Soporte Técnico

- Los estafadores de soporte técnico utilizan muchas tácticas de miedo diferentes para engañarlo y hacer que utilice servicios de soporte técnico innecesarios para supuestamente solucionar problemas de dispositivos o software que no existen, como se detalla a continuación:
- Llamadas
- Advertencias emergentes en la computadora
- Anuncios y listados en línea en las páginas de resultados de búsqueda



Cómo Reconocer Una Estafa de Soporte Técnico

mensajes emergentes de seguridad falsos que solicitan llamar a un número

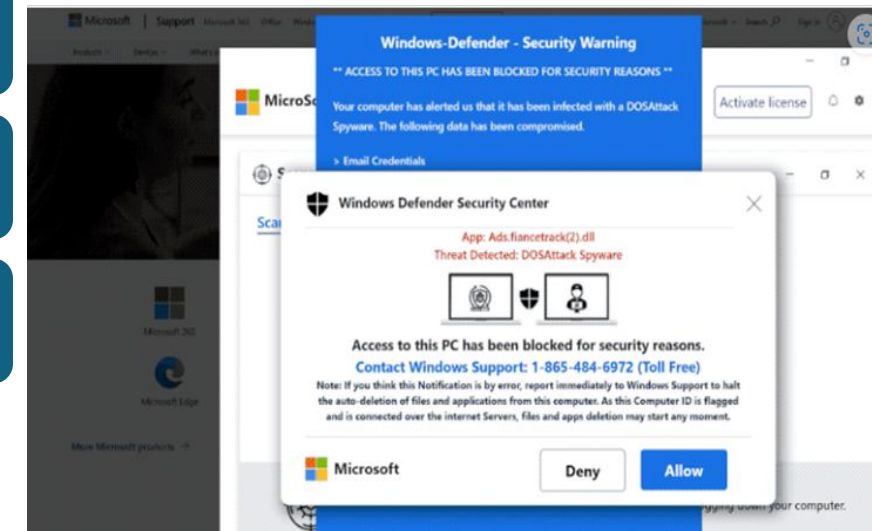
Llamadas telefónicas no solicitadas

Correos electrónicos o mensajes de texto sospechosos con enlaces maliciosos

Solicitando acceso remoto

Creando un sentido de urgencia

Solicitar pagos inmediatos



Consejos de Prevención

no hagas clic

- No haga clic en ningún enlace ni llame a ningún número que aparezca en su pantalla advirtiéndole de un problema informático..

Cuelgue

- Cuelgue las llamadas inesperadas de cualquiera que diga ser soporte técnico.

No Creas

- No confíe en su identificador de llamadas: puede ser falsificado fácilmente.

No Ceda

- Nunca ceda el control de su computadora ni comparta contraseñas/información financiera con nadie que se comuniquen con usted.

Mantenga

- Mantenga su software de seguridad actualizado

Contacte

- Si necesita ayuda, póngase en contacto con un técnico informático de confianza. No se limite a confiar en una búsqueda en Internet.





NUEVA: Estafa de Hackers Fantasmas Con Inteligencia Artificial

ESTAFA DE HACKERS CON AI

Las estafas se producen de tres maneras:

1. Uso de inteligencia social con AI.
2. Suplantación del identificador de llamadas.
3. **Voces deepfake** para suplantación de identidad.

Cómo interviene la AI: Las voces deepfake se recrean a partir de breves muestras de audio para suplantar a funcionarios reales. También existen guiones generados por IA para crear correos electrónicos, mensajes, etc. realistas.



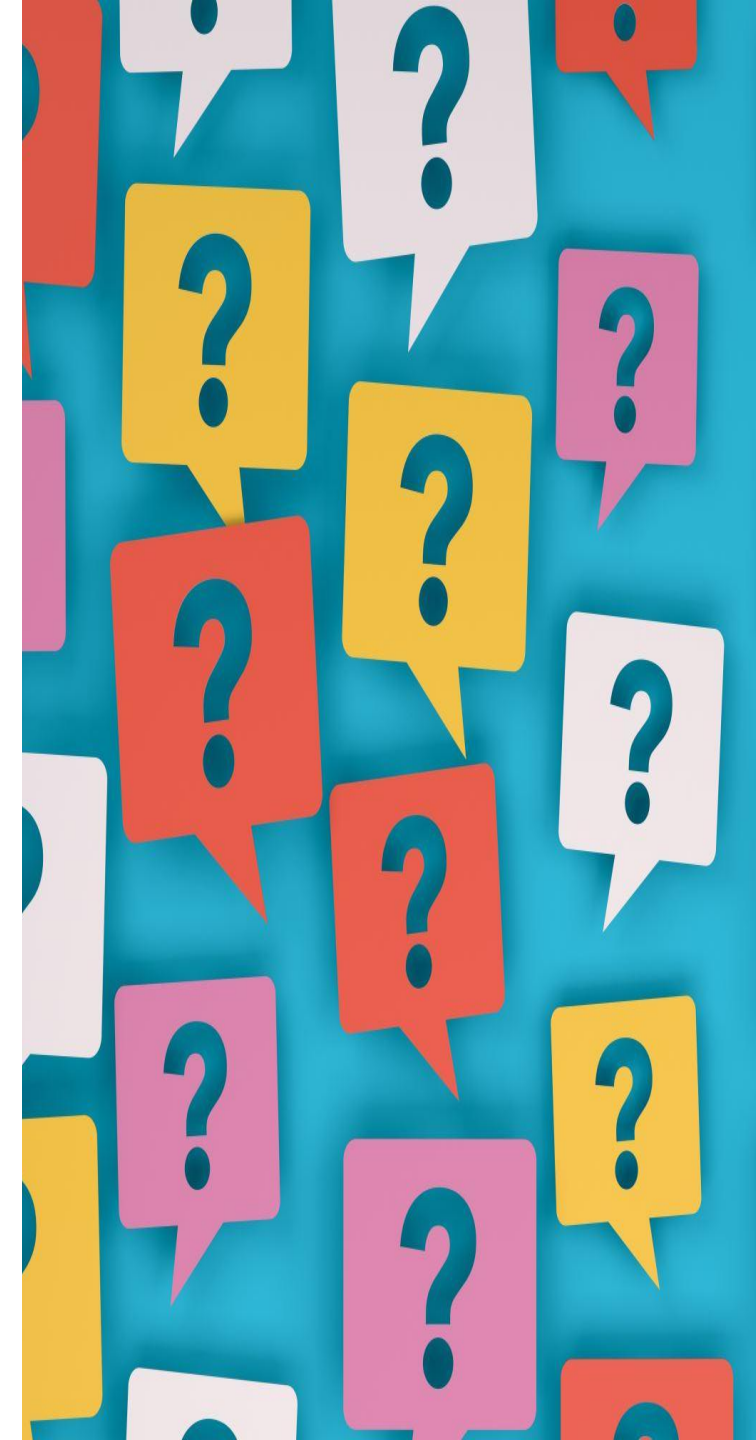
Consejos de prevención

Pregunte	*Haga preguntas, detecte inconsistencias que puedan revelar un impostor.
Converse	*Hable sobre su nuevo interés amoroso con familiares y amigos; preste atención a sus inquietudes.
Ten Cuidado	*Desconfíe de los correos electrónicos coquetos y excesivamente elogiosos.
Corte Contacto	*Si sospecha de un estafador, corte el contacto inmediatamente.
Reporte	*Denuncie al estafador en la plataforma de citas.
Informese	*Tenga cuidado incluso si inicia el contacto: los estafadores acechan en todas partes.
Comparte	*Comparte información personal mínima en tu perfil de citas o chats en línea.
Nunca Envíe	Nunca envíe dinero ni tarjetas de regalo a contactos que solo estén en línea.



Pregunta: Si cree que es víctima de una estafa en línea o un ciberataque, ¿qué debe hacer?

- se vocal.
- No te sientas avergonzado por lo que pasó.
- Reporte incidente a [Internet Crime Center \(IC3\) at the “Internet Crime Complaint \(IC3\)” Home Page](#), the Federal Bureau of Investigation (FBI) nearest field office using the [Electronic Tip Form](#), and [Federal Trade Commission \(FTC\)](#).
- Comuníquese con su agencia policial local para presentar un informe y notificar a sus instituciones financieras.
- Instale un software antivirus confiable en su computadora y actualícelo periódicamente.



Gracias!

