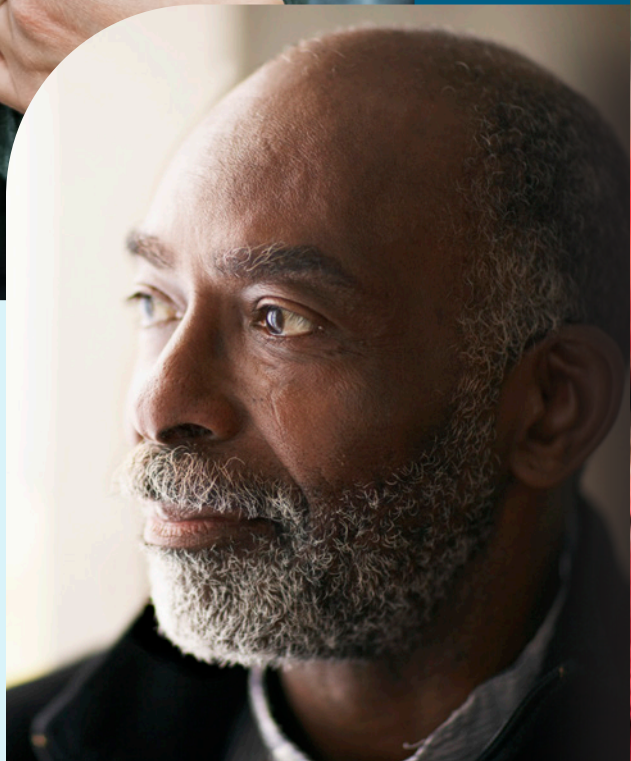




2023

BBB Scam TrackerSM
**INFORME
DE RIESGO**



2023

BBB Scam TrackerSM INFORME DE RIESGO

Todas las marcas comerciales de terceros a las que hace referencia BBB Institute for Marketplace TrustSM son propiedad intelectual de sus respectivos propietarios. El uso de las marcas comerciales de terceros no indica ningún tipo de relación, patrocinio o respaldo entre BBB Institute for Marketplace Trust y los propietarios de estas marcas comerciales. Cualquier referencia de BBB Institute for Marketplace Trust a marcas comerciales de terceros es para identificar al tercero correspondiente.



Índice de contenidos

4	Introducción
4	Acerca del BBB Scam Tracker SM
6	Resumen de 2023
8	– Destacados del Informe de Riesgo 2023
9	Índice de riesgo de BBB: un enfoque tridimensional para medir el riesgo de estafa
12	Las estafas de mayor riesgo denunciadas por los consumidores en 2023
13	– Las 10 estafas más riesgosas a consumidores
14	Este año aumentó el número de personas que perdieron dinero por estafas relacionadas con romances
16	Las estafas relacionadas con reparación del crédito y alivio de deuda entran por primera vez en la lista de las 10 primeras
18	Datos demográficos
18	– Edad
19	– Estafas que apuntan a los jóvenes
20	– Género
21	Métodos de pago y de contacto
29	Impacto en públicos específicos
29	– Consumidores de Canadá
30	– Organizaciones con suplantación de identidad
31	El palo y la zanahoria: análisis del impacto de las tácticas de estafas
33	Indicios y comportamientos que observaron los afectados y ayudaron a evitar la pérdida de dinero
34	Otros factores que pueden influir en la victimización
38	Estafas dirigidas a empresas
39	10 consejos generales para evitar que lo estafen
40	BBB Institute for Marketplace Trust
42	Apéndice A: Glosario de tipos de estafas
46	Apéndice B: Tabla de datos con tipo de estafa, estafas al consumidor
47	Apéndice C: Los 10 principales tipos de estafas al consumidor por riesgo general, exposición, susceptibilidad y pérdida mediana en dólares
48	Agradecimientos
49	Equipo del proyecto



Introducción



BBB Institute for Marketplace Trust (BBB Institute), la fundación educativa de la International Association of Better Business Bureaus, se complace en presentar el *Informe de Riesgo de BBB Scam Tracker 2023*. El informe anual analiza los datos que los consumidores y las empresas enviaron a BBB Scam TrackerSM ([BBB.org/ScamTracker](https://www.bbb.org/ScamTracker)) en 2023. Las conclusiones arrojan luz sobre la manera en que se cometen las estafas, a quiénes apuntan, qué estafas tienen el mayor impacto y los comportamientos y factores que pueden afectar la susceptibilidad de una persona. En la Figura 3 se presentan los aspectos más destacados del informe de 2023.

Las estafas erosionan la confianza en el mercado, distorsionan la igualdad de condiciones y desvían dinero de transacciones legítimas que podrían beneficiar tanto a consumidores como a empresas, impidiendo así el crecimiento económico. Un mercado próspero requiere consumidores empoderados y bien informados y empresas con principios que trabajen de forma proactiva para detener a los estafadores y fomentar relaciones de confianza.

Combatir a los estafadores requiere un esfuerzo multisectorial. BBB comparte sus datos con socios que también luchan contra el fraude en el mercado, como las agencias del gobierno y las fuerzas policiales, las organizaciones sin fines de lucro, los medios de comunicación y la comunidad empresarial. Trabajamos con líderes para elaborar las mejores estrategias para detener a los estafadores y formamos equipos con socios corporativos y organizaciones afines para ampliar nuestra programación y nuestras actividades educativas para los consumidores, evaluar qué iniciativas están funcionando y actualizarlas constantemente en función de estudios de investigación y datos internos y externos.

El BBB Institute utiliza las conclusiones de este informe para crear recursos de educación del consumidor que empoderen a las personas para protegerse a sí mismas y a los demás. El BBB Institute ofrece estos programas para los consumidores en forma digital y presencial, aprovechando la amplia red de BBB que presta servicios a comunidades de todo Estados Unidos y Canadá.

Acerca del BBB Scam Tracker

El *Informe de Riesgo de BBB Scam Tracker* es posible gracias a los datos recopilados por BBB Scam Tracker, una plataforma en línea que permite tanto a los consumidores como a las empresas denunciar fraudes e intentos de fraude. La red de BBB miembro revisa y publica estos casos de fraude denunciados para que el público pueda buscar entre las estafas publicadas, determinar si están en la mira de los estafadores y evitar perder dinero.

Según una encuesta realizada entre los que presentaron denuncias en BBB Scam Tracker,¹ 37.8 % dijo que visitó la página web del BBB Scam Tracker para determinar si una experiencia que estaban teniendo podría ser una estafa y el 36.6 % de ellos dijo que la herramienta de seguimiento de estafas les ayudó a evitar perder dinero cuando fueron blanco de una estafa. Con más de 1.7 millones de visitas a la plataforma en 2023,² estimamos que BBB Scam Tracker logró un ahorro de \$24.3 millones solo en 2023 (Figura 1).

Los que presentaron denuncias en la página web de BBB Scam Tracker buscaban advertir a otros sobre una estafa (44.3 %), ayudar a las fuerzas policiales a detener al estafador (25.2 %) y evitar perder dinero por un intento de estafa (30.5 %).³ Extendemos nuestro agradecimiento a los cientos de miles de personas que decidieron hacerse oír y ayudar a otros a evitar perder dinero por estafas al hacer denuncias en BBB Scam Tracker.

FIGURA 1

Impacto del BBB Scam Tracker en 2023

1 753 544

Visitantes únicos a BBB Scam Tracker

37.8 %

Visitaron BBB Scam Tracker para determinar si estaban siendo víctimas de una estafa

36.6 %

Indicaron que BBB Scam Tracker les ayudó a evitar perder dinero

\$100

Monto mediano ahorrado, en dólares estadounidenses

\$24 259 931

Monto mediano en dólares que las personas evitaron perder gracias a BBB Scam Tracker

¹ Encuesta por interceptación con 1027 participantes únicos que visitaron BBB Scam Tracker en enero de 2024. Los encuestados podían elegir varias razones para visitar BBB Scam Tracker.

² Adobe Analytics.

³ Se distribuyó una encuesta a quienes presentaron una denuncia de estafa a BBB Scam Tracker en 2023; 6947 encuestados completaron la encuesta.

Resumen de 2023



Los datos y la información que se desprenden de los informes de BBB Scam Tracker permiten al BBB Institute comprender mejor el impacto de las estafas que se cometen en el mercado. En 2023, BBB Scam Tracker publicó más de 67 000 denuncias de estafas. Clasificamos las denuncias de estafas presentadas por empresas e individuos de Estados Unidos y Canadá en 28 tipos de estafas a consumidores, cinco tipos de estafas a empresas y una categoría “otros” que representaba el 7.7 % de todas las denuncias. Consulte en el Apéndice A un glosario completo de los tipos de estafas. Los datos recogidos de las denuncias de estafas incluyen una descripción de la estafa, el valor en dólares de la pérdida e información sobre los medios de contacto y el método de pago. Al presentar una denuncia a través de la plataforma BBB Scam Tracker, los datos demográficos (edad, género y código postal) sobre la persona que fue blanco de la estafa es opcional para empresas o consumidores. Consulte los datos detallados por tipo de estafa en los Apéndices B y C.

La susceptibilidad general aumentó, mientras que la pérdida mediana en dólares disminuyó.

En 2023, la susceptibilidad (el porcentaje de personas que declararon haber perdido dinero al verse expuestos a una estafa) aumentó por primera vez desde 2020. El incremento fue del 27.8 % en comparación con el año anterior (Figura 2). La pérdida mediana en dólares que se denunció disminuyó un 41.5 % de \$171 en 2022 a \$100 en 2023.⁴

Las estafas de inversión/criptomonedas fueron las más riesgosas.

En 2023, hubo un cambio en nuestra lista de las 10 principales estafas más riesgosas. Con frecuencia, las estafas de inversión se han clasificado entre las 10 principales estafas más riesgosas desde que comenzamos a publicar el Informe de Riesgo. En 2019, agregamos una categoría para las estafas de criptomonedas, que han aparecido de forma constante entre las tres principales estafas más riesgosas desde entonces. Este año, combinamos las estafas de inversión y de criptomonedas en una categoría, ya que la mayoría de las estafas de criptomonedas implicaron oportunidades de inversión. Como resultado, las estafas de inversión/criptomonedas llegaron a la cima de nuestra lista de estafas más riesgosas con un porcentaje alto de personas que denunciaron una pérdida monetaria (80.4 %) y una pérdida mediana en dólares alta (\$3800).

Las estafas laborales continuaron siendo el segundo tipo de estafa más riesgoso con una pérdida mediana en dólares alta, de \$1995. Las denuncias de estafas laborales aumentaron un 54.2 % de 2022 a 2023.

⁴ La mediana de las pérdidas en dólares se calculó solamente para las estafas con pérdidas declaradas.

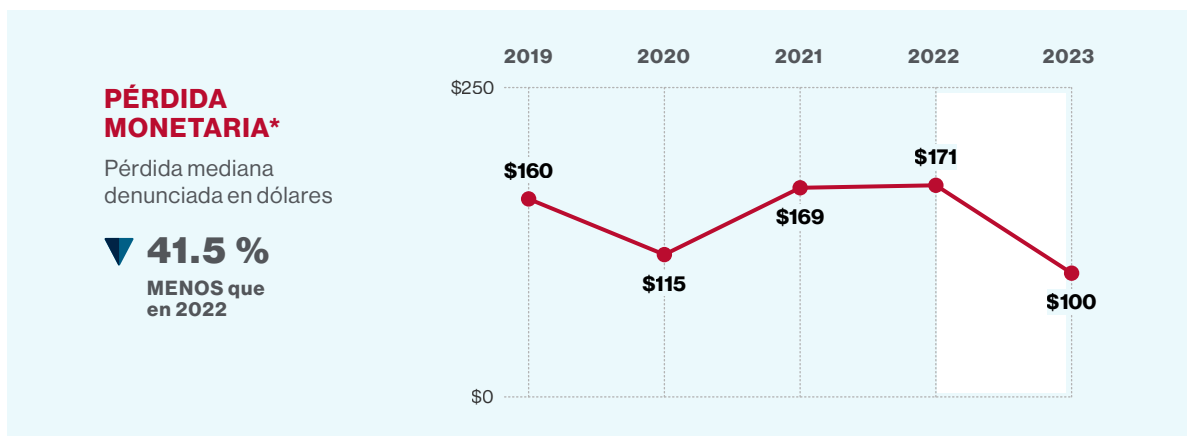
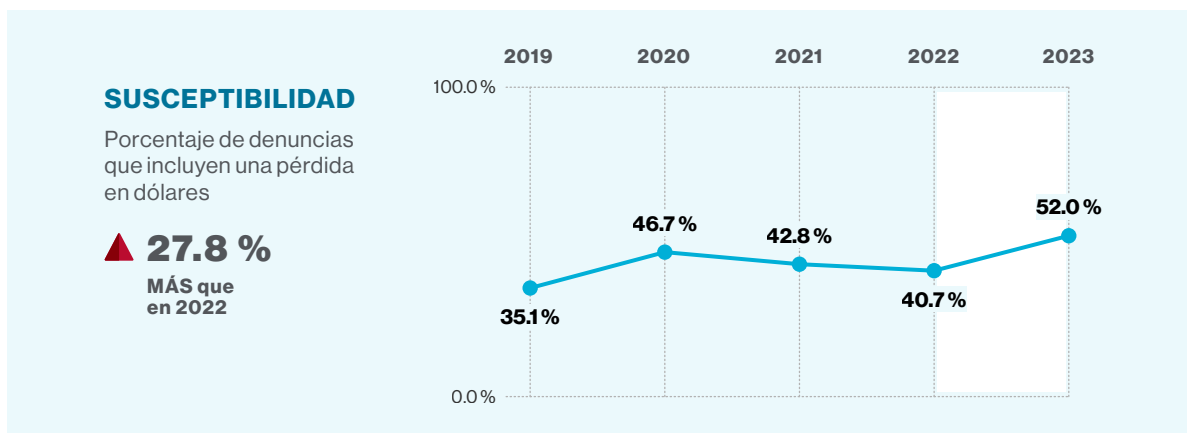
Aunque las estafas por compras en línea volvieron a tener la mayor cantidad de denuncias en BBB Scam Tracker este año y la segunda mayor susceptibilidad, este tipo de estafa pasó a ser el número tres de nuestra lista después de tres años como el principal tipo de estafa más riesgoso. Puede encontrar más información sobre nuestra lista de los 10 tipos principales en la página 13.

Cómo se contactaron los estafadores con sus víctimas

En 2023, los tres principales métodos de contacto que dieron lugar a una pérdida monetaria declarada continuaron siendo los mismos que en 2022, pero con un cambio en el orden. Por primera vez, las redes sociales superaron a las páginas web como el método de contacto principal que implicó una pérdida monetaria. Las tarjetas de crédito continuaron siendo el principal método de pago de las estafas con pérdidas monetarias, seguidas de los débitos de cuentas bancarias y los sistemas de pago en línea. La susceptibilidad a las estafas cometidas a través de redes sociales aumentó un 23.8 % en comparación con el año anterior. Puede encontrar más información en las páginas 21-28.

FIGURA 2

Resumen de riesgo (2019-2023)

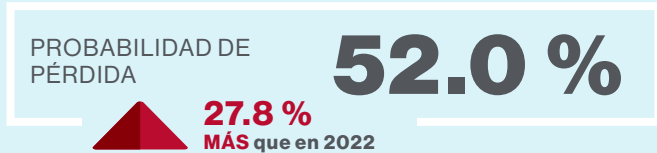


* La mediana de las pérdidas en dólares se calculó solamente para las estafas con pérdidas declaradas.

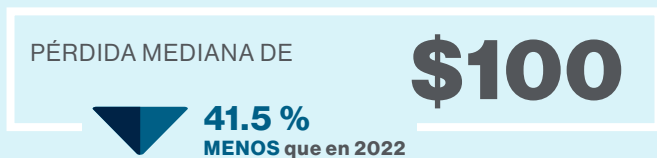
Informe de Riesgo de BBB Scam Tracker 2023

DESTACADOS

SUSCEPTIBILIDAD GENERAL



PÉRDIDA MONETARIA GENERAL



ASPECTOS DESTACADOS DE LA INVESTIGACIÓN MEDIANTE ENCUESTAS

El 92.5 %

de las personas encuestadas expresaron que **serán capaces de identificar las señales de alarma** de estafas similares en el futuro.

Las personas de **18 a 54 años de edad** prefieren **obtener información sobre estafas en historias de redes sociales**, mientras que las personas de más de 55 años de edad prefieren recibir alertas de fraude.

La principal emoción que denunciaron **las personas de 18 a 44 años de edad** después de ser blanco de una estafa fue **la ansiedad/el estrés**.

La principal emoción que denunciaron **las personas de más de 45 años de edad** fue **el enojo**.

El 10.3 %

de las personas encuestadas indicó **haber perdido dinero en una estafa al menos tres veces**, un aumento en comparación con el 8.4 % de 2022.

LAS 3 ESTAFAS MÁS RIESGOSAS DENUNCIADAS POR LOS CONSUMIDORES

1

Estafas de inversión/criptomoneda

Las estafas de inversión/criptomonedas aumentaron y se convirtieron en el principal tipo de estafa más riesgoso con la tercera mayor susceptibilidad y la segunda mayor pérdida mediana en dólares.

2

Estafas laborales

Las estafas laborales continuaron siendo el segundo tipo de estafa más riesgoso con una pérdida mediana en dólares alta, de \$1995. Las denuncias de estafas laborales aumentaron un 54.2 % de 2022 a 2023.

3

Estafas por compras en línea

Más del 40 % de las estafas denunciadas en BBB Scam Tracker fueron estafas por compras en línea, que, por primera vez desde 2019, pasaron al tercer lugar de la lista de estafas más riesgosas.

Las estafas cometidas en línea siguen creciendo y representan el 68.4 % de todas las denuncias. Lo más preocupante es que **las estafas en línea tuvieron más probabilidades de dar como resultado una pérdida monetaria** que las que se llevaron a cabo en persona o por teléfono.

Por segundo año consecutivo, **las personas de 18 a 24 años de edad fueron las que más pérdidas mediana en dólares** tuvieron de todos los grupos etarios.

El porcentaje de personas **contactadas a través de redes sociales aumentó un 63.8 %** de 2022 a 2023.

Según las denuncias, **el Servicio Postal de EE. UU.** fue la organización **suplantada con más frecuencia** por estafadores en 2023.

Las estafas relacionadas con romances subieron del séptimo al quinto puesto de la lista debido a un aumento significativo de la susceptibilidad y a una pérdida mediana en dólares alta.

Índice de riesgo de BBB: un enfoque tridimensional para medir el riesgo de estafa



Para comprender mejor qué tipos de estafa representan un mayor riesgo, evaluamos las estafas en función de tres factores: exposición, susceptibilidad y pérdida monetaria. Esta fórmula única conforma el Índice de Riesgo de BBB (Figura 4). Al combinar estos tres factores, obtenemos información importante del riesgo de estafa que va más allá del volumen de denuncias recibidas, lo que permite a BBB y a sus socios orientar mejor las actividades para prevenir las estafas.

El riesgo no puede determinarse considerando aisladamente uno solo de estos factores. Por ejemplo, las estafas en grandes volúmenes suelen dirigirse a la mayor cantidad posible de personas, pero con una menor probabilidad de pérdidas monetarias. En comparación, las estafas con un enfoque de “alto contacto” suelen llegar a menos personas, pero esas personas expuestas suelen tener más probabilidades de perder dinero y de perder grandes cantidades de dinero.

El Índice de Riesgo de BBB no tiene en cuenta los impactos no financieros de las estafas. Según nuestra encuesta, los encuestados también declararon haber perdido tiempo (55.8 %) e información personal (37.7 %) (Figura 5).⁵

También encuestamos a la gente sobre el impacto emocional de ser blanco de una estafa (Figura 6). La principal emoción que declararon fue el enojo (69.0 %), seguido de la ansiedad y el estrés (66.7 %). La pérdida de confianza fue la tercera respuesta más común (58.0 %).

⁵ Se distribuyó una encuesta a quienes presentaron una denuncia de estafa a BBB Scam Tracker en 2023; 6947 encuestados completaron la encuesta.

FIGURA 4

Índice de riesgo de BBB

La fórmula para calcular el Índice de Riesgo de BBB para una estafa cualquiera en una población determinada es la siguiente:

$$\text{Exposición} \times \text{Susceptibilidad} \times (\text{Pérdida mediana} / \text{Pérdida mediana general}) \times 1,000.$$



EXPOSICIÓN*

es una medida de la prevalencia de un tipo de estafa, calculada como el porcentaje de un tipo de estafa en particular como parte del total de estafas denunciadas.



SUSCEPTIBILIDAD

es una medida de la probabilidad de perder dinero cuando se expone a un tipo de estafa, calculada como el porcentaje de todas las denuncias que incluyeron una pérdida monetaria.



PÉRDIDA MONETARIA

se calcula como la cantidad mediana en dólares de las pérdidas denunciadas para un tipo de estafa en particular, excluyendo las denuncias en las que no hubo pérdidas.

* La exposición está limitada por la naturaleza de la auto-denuncia; el porcentaje de quienes reportaron a BBB Scam Tracker ser víctimas de estafas no necesariamente coincide con el porcentaje de personas en la población total que fueron blanco de estafas.

El desglose por grupos etarios destaca algunas diferencias interesantes (Figura 7). Las personas de 18 a 44 años de edad mencionaron la ansiedad/el estrés como el principal impacto emocional, mientras que las personas de más de 45 años de edad expresaron que el enojo fue el principal impacto emocional. Las personas más jóvenes denunciaron porcentajes más altos de vergüenza, pérdida de confianza en sí mismo y culpa.

FIGURA 5

Impactos no financieros de ser víctima de una estafa

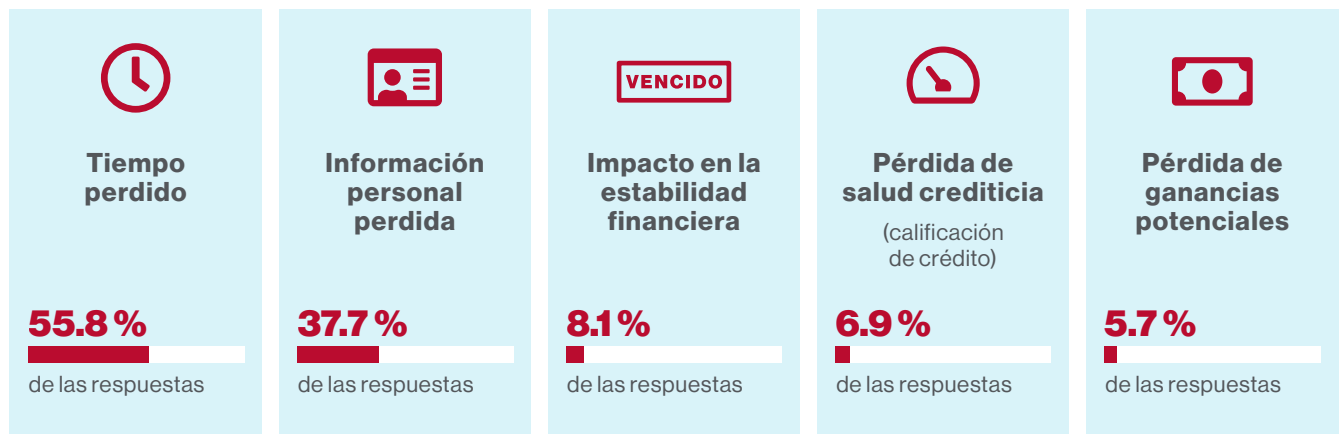
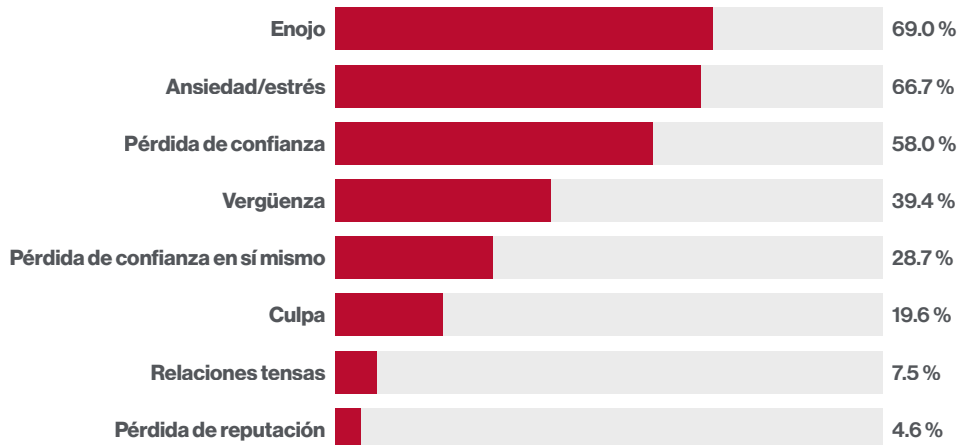


FIGURA 6

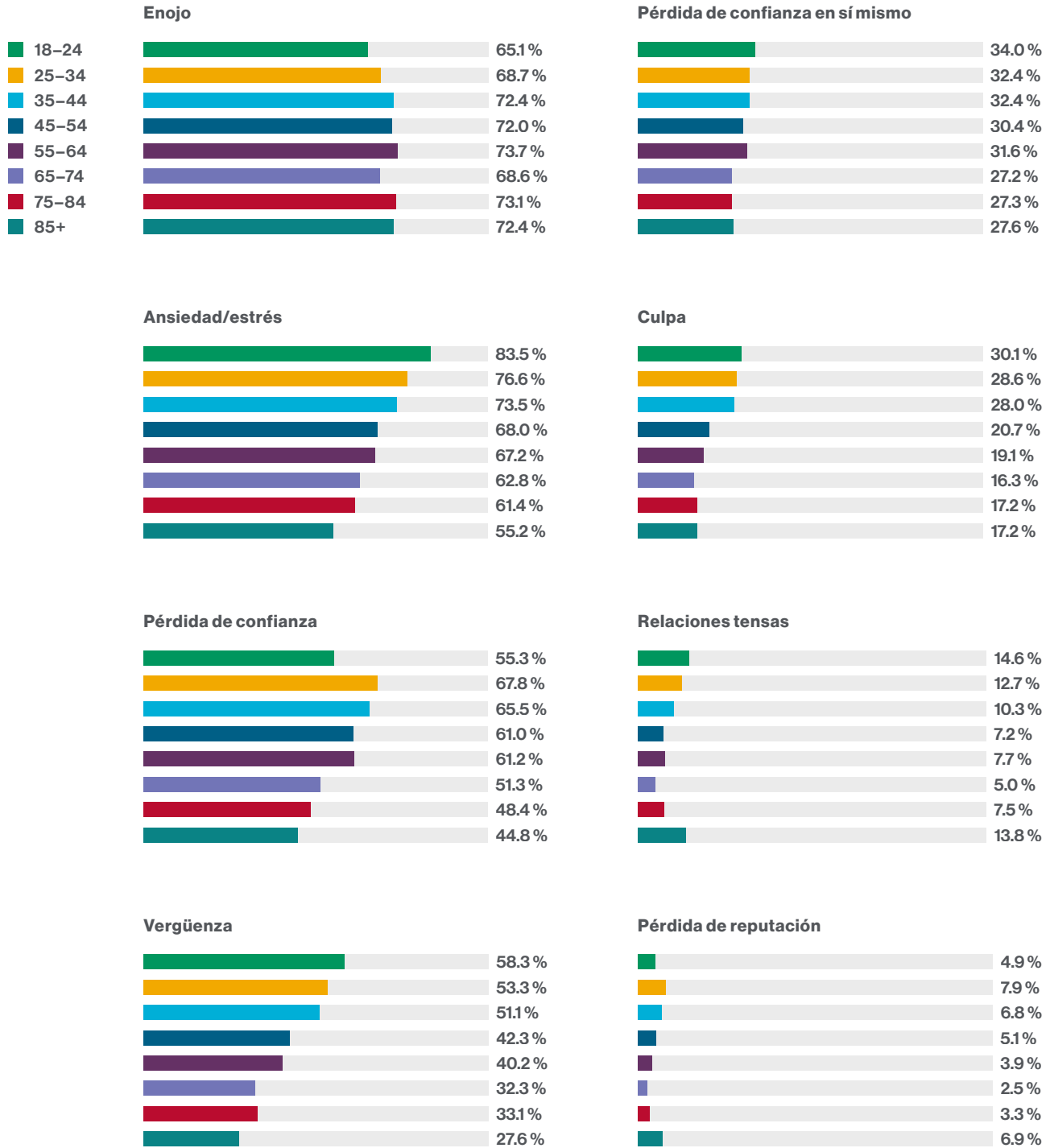
Principales emociones/impacto de ser víctima de una estafa



Quando se les preguntó sobre el impacto emocional de ser blanco de una estafa, **las personas denunciaron que el enojo fue la principal emoción, seguido de la ansiedad y el estrés.**

FIGURA 7

Impacto emocional de ser blanco de una estafa (por edad)



Las 10 estafas de mayor riesgo denunciadas por los consumidores en 2023



Cada año, BBB publica nuestra lista de los 10 tipos de estafa de mayor riesgo (Tabla 1), que se calcula en función del Índice de Riesgo de BBB y de las denuncias presentadas a BBB Scam Tracker. En 2023, hubo algunos cambios significativos en cuanto a las posiciones en la lista.

Este año, **las estafas de inversión/criptomonedas** se convirtieron en el principal tipo de estafa más riesgoso, y el 80.4 % de las víctimas denunciaron una pérdida monetaria. La pérdida mediana en dólares denunciada (\$3800) fue la segunda más alta de todos los tipos de estafa.⁶

En 2023, **las estafas laborales** continuaron siendo la segunda estafa más riesgosa. El porcentaje de denuncias sobre este tipo de estafa aumentó un 54.2 %, de 9.6 % en 2022 a 14.8 % en 2023. La pérdida mediana en dólares declarada en relación con estafas laborales aumentó un 33 %, de \$1500 en 2022 a \$1995 en 2023.

Aunque **las estafas por compras en línea** pasaron a ser las terceras más riesgosas de nuestra lista, estas estafas continuaron teniendo un impacto enorme, ya que representaron el porcentaje más alto de denuncias en BBB Scam Tracker (41.9 %) y el segundo porcentaje más alto de denuncias con pérdidas monetarias (susceptibilidad). Más del 82 % de las personas que denunciaron haber sido blanco de estafas por compras en línea perdieron dinero. La pérdida mediana en dólares por este tipo de estafa se redujo de \$100 en 2022 a \$71 en 2023.

Las estafas relacionadas con romances subieron del séptimo al quinta puesto de mayor riesgo de la lista. La pérdida mediana en dólares declarada aumentó de \$1411 en 2022 a \$3600 en 2023. En 2023, el 65.7 % de las denuncias de estafas relacionadas con romances implicaron una pérdida monetaria en comparación con solo el 16.1 % de 2022.

Por primera vez desde que comenzamos a publicar el *Informe de Riesgo de BBB Scam Tracker* en 2016, **las estafas de reparación de crédito/alivio de deudas** aparecieron en la lista de las 10 estafas más riesgosas. El porcentaje de denuncias con pérdidas monetarias (susceptibilidad) sobre este tipo de estafa aumentó un 64.3 % de 2022 a 2023. La pérdida mediana en dólares aumentó de \$870 a \$1000.

Por primera vez desde que comenzamos a publicar el *Informe de Riesgo de BBB Scam Tracker* en 2016, **las estafas de reparación de crédito/alivio de deudas** aparecieron en la lista de las 10 estafas más riesgosas.

⁶ Este año, combinamos las estafas de criptomonedas y de inversión en una categoría, ya que la mayoría de las estafas de criptomonedas implican situaciones de inversión.

Susceptibilidad en alta, en general

La susceptibilidad general aumentó significativamente en 2023, ya que más personas denunciaron pérdidas monetarias. Además de las cinco estafas principales que se mencionaron previamente, los siguientes tipos de estafa también tuvieron un aumento significativo en cuanto a la susceptibilidad en comparación con el año anterior: producto falsificado (83.3 %), alquiler (64.1 %), viaje/vacaciones/tiempo compartido (59.6 %) y reparación de crédito/alivio de deudas (55.7 %). Puede encontrar un desglose completo de los tipos de estafa con mayor susceptibilidad en la página 46.

Reducción de la pérdida mediana general en dólares

Aunque la pérdida mediana general en dólares disminuyó en 2023, varios tipos de estafa, además de los cinco principales más riesgosos, tuvieron una pérdida mediana en dólares declarada alta, incluyendo el intercambio de moneda extranjera (\$7400), el cobro de impuestos (\$2306), los cheques/giros postales falsos (\$1165), la reparación de crédito/el alivio de deudas (\$1000), las emergencias de familiares/amigos (\$900) y las subvenciones del gobierno (\$948). Puede encontrar un desglose completo de los tipos de estafa con mayor pérdida mediana en dólares en la página 46.

TABLA 1

Las 10 estafas más riesgosas a consumidores

PUESTO	TIPO DE ESTAFA	ÍNDICE DE RIESGO DE BBB	EXPOSICIÓN*		SUSCEPTIBILIDAD		PÉRDIDA MEDIANA EN \$	
			2023	2022	2023	2022	2023	2022
1	6/3 Inversión/criptomoneda**	520.9	1.7 %	0.7 %/ 1.7 %	80.4 %	49.0 %/ 60.5 %	\$3800	\$1369/ \$1100
2	2 Laboral	445.9	14.8 %	9.6 %	15.1 %	15.1 %	\$1995	\$1500
3	1 Compras en línea	244.9	41.9 %	31.9 %	82.6 %	74.0 %	\$71	\$100
4	4 Mejoras en el hogar	201.2	1.3 %	1.4 %	74.7 %	55.3 %	\$2073	\$1500
5	7 Romance	151.4	0.6 %	1.6 %	65.7 %	16.1 %	\$3600	\$1411
6	5 Tarifa por anticipo de préstamo garantizado	57.2	1.4 %	1.9 %	45.3 %	36.7 %	\$900	\$800
7	9 Phishing/ingeniería social	56.5	12.6 %	11.7 %	15.0 %	10.6 %	\$300	\$267
8	11 Reparación de crédito/alivio de deuda	29.4	0.5 %	1.1 %	55.7 %	33.9 %	\$1000	\$870
9	10 Soporte técnico	25.5	1.9 %	2.6 %	26.6 %	25.2 %	\$500	\$490
10	13 Viajes/vacaciones/tiempo compartido	23.6	0.7 %	1.0 %	59.6 %	49.3 %	\$543	\$602

* La exposición está limitada por la naturaleza de la auto-denuncia; el porcentaje de quienes reportaron a BBB Scam Tracker ser víctimas de estafas no necesariamente coincide con el porcentaje de personas en la población total que fueron blanco de estafas.

** Para el informe de este año, combinamos las estafas de criptomonedas con las estafas de inversión. Nuestro motivo es que la mayoría de las estafas de criptomonedas implican situaciones de inversión.

Este año aumentó el número de personas que perdieron dinero por estafas relacionadas con romances

Este año, las estafas relacionadas con romances subieron del séptimo al quinto puesto de la lista de estafas más riesgosas por varios motivos. En primer lugar, la pérdida mediana en dólares declarada aumentó un 155.1% de 2022 a 2023. En segundo lugar, el porcentaje de personas que denunciaron haber perdido dinero en estafas relacionadas con romances aumentó un 308.1%. En 2023, el 65.7% de las denuncias de estafas relacionadas con romances implicaron una pérdida monetaria en comparación con solo el 16.1% de 2022.

Cómo funciona la estafa

La mayoría de las estafas relacionadas con romances comienzan con perfiles falsos en sitios de citas en línea que los estafadores crean a partir de fotografías y textos robados de cuentas reales o de otros lugares. Los estafadores suelen afirmar que están en el ejército o trabajando en el exterior para explicar por qué no pueden reunirse en persona. En un período de tiempo corto, los estafadores construyen una relación falsa con la persona que es blanco de la estafa mediante el intercambio de fotografías y mensajes románticos, e incluso llamadas telefónicas o videollamadas. En el momento en el que la relación parece estar volviéndose seria, el nuevo interés romántico de la persona tiene un problema de salud o una emergencia familiar, o quiere planificar una visita. Independientemente de la historia, el pedido es el mismo: necesita dinero. Sin embargo, después de que la persona envía dinero, hay otro pedido y después otro. O el estafador deja de comunicarse por completo.

Estafas relacionadas con romances y criptomonedas

Los estafadores han comenzado a formar relaciones con el fin de presentarles las criptomonedas a sus víctimas. Al principio, el tema de las criptomonedas surge de forma casual a través de insinuaciones que hace el estafador sobre su éxito financiero. Con el tiempo, el estafador incentiva a la persona a que intente invertir en criptomonedas. Siempre comienza de a poco y, con el tiempo, el estafador comienza a forjar confianza. La víctima comienza a notar que su inversión inicial crece y el estafador la incentiva a invertir más dinero. Sin embargo, luego, la víctima descubre demasiado tarde, una vez que ya ha invertido un monto significativo, que la plataforma es falsa y no puede recuperar el dinero.



El porcentaje de personas que denunciaron haber perdido dinero en estafas relacionadas con romances **aumentó más del 300% desde 2022.**



La siguiente denuncia de estafa fue enviada por una persona de Dakota del Norte.⁷

Conocí a una mujer que me envió un mensaje de texto accidentalmente. Comencé a hablar con ella y pensé que quería tener una relación conmigo. Hablábamos por Telegram. Me presentó a su tía, que supuestamente es la encargada del mercado de valores. Después de hablar con ella durante semanas, me dijo que vendría y tendría una relación conmigo, y comencé a creerle. Luego, me pidió que invirtiera en Tiger Trades, y lo hice. Después, cambió de parecer sobre venir a estar conmigo. Me conecté e intenté retirar mi dinero, pero no puedo. Investigué a Tiger Trades en Internet y hablé con alguien que me dijo que era una aplicación falsa que no estaba relacionada con la empresa real de Tiger Trades. ¡Perdí \$587!



⁷ Esta denuncia de estafa se editó en aras de la brevedad y la claridad.

ESTAFAS RELACIONADAS CON ROMANCES

Señales de alarma para tener en cuenta:

Demasiado atractivo para ser cierto. Los estafadores brindan fotografías atractivas e historias de éxito financiero. Si parece "demasiado perfecto", es una señal de alarma.

Con prisa por salir del sitio. Los estafadores intentarán trasladar la comunicación a otro medio, como correo electrónico, Messenger o teléfono, muy rápido.

Avanzar deprisa. Los estafadores comienzan a hablar de un futuro juntos y expresan que lo aman en poco tiempo. Con frecuencia, dicen que nunca se habían sentido así.

Hablar de confianza. Los estafadores comenzarán a manipularlo hablando sobre la confianza y su importancia. Este suele ser el primer paso para pedirle dinero.

No querer reunirse. Tenga cuidado con las personas que siempre tienen una excusa para posponer un encuentro, como decir que están viajando, que viven en el exterior o que están en el ejército.

Usar un lenguaje sospechoso. Si la persona con la que se comunica dice ser de su ciudad, pero tiene errores ortográficos o gramaticales, usa lenguaje demasiado florido o utiliza frases que no tienen sentido, es una señal de alarma.

Historias de infortunio. Antes de proceder a pedirle dinero, el estafador puede insinuar que tiene problemas financieros, como que le cortaron la calefacción, le robaron el automóvil o tiene un familiar enfermo, o puede compartir una historia triste sobre su pasado (la muerte de sus padres o su pareja, etcétera).

Oportunidad financiera. Si la persona lo incentiva a aprovechar una oportunidad de inversión, como comprar criptomonedas, es una señal de alarma muy grande.

Las estafas relacionadas con reparación del crédito y alivio de deuda entran por primera vez en la lista de las 10 primeras

Por primera vez desde que comenzamos a publicar el *Informe de Riesgo de BBB Scam Tracker* en 2016, las estafas de reparación de crédito/alivio de deudas aparecieron en la lista de las 10 estafas más riesgosas. El porcentaje de denuncias con pérdidas monetarias (susceptibilidad) sobre este tipo de estafa aumentó un 64.3 % de 2022 a 2023. La pérdida mediana en dólares aumentó de \$870 en 2022 a \$1000 en 2023.

Cómo funciona la estafa

Se ofrecen servicios a las personas que tienen deudas grandes o mal crédito mediante publicidades en línea, mensajes emergentes en redes sociales o llamadas telefónicas espontáneas. Es posible que estas ofertas “garanticen” una mejor calificación de crédito, aseguren el alivio de deudas o prometan una mejor situación financiera. Las personas que son blanco de estas estafas pueden verse tentadas a pagar la tarifa por adelantado para ayudar a aliviar su estrés. Las empresas que llaman o se publicitan en línea suelen prometer, y cobrar, servicios imposibles. Esto incluye eliminar errores previos en relación con el crédito, como pagos tardíos o una insolvencia, de su informe de crédito. Ofrecen brindar una “identidad crediticia” nueva o negociar con los prestamistas o las empresas de las tarjetas de crédito para eliminar la deuda por completo. Cuando los servicios no se brindan, la persona pierde las tarifas que pagó.

La pérdida mediana en dólares por estafas de reparación de crédito/alivio de deudas aumentó de \$870 en 2022 a **\$1000 en 2023.**



El siguiente informe de estafa fue enviado por una persona en Kentucky.⁸

Me contactaron por teléfono hace un poco más de un año en relación con la resolución de deudas. Acepté y pagué \$369 mensuales por el servicio. No resolvieron ninguna de mis deudas. Vengo intentando comunicarme con ellos desde hace más de un mes sin suerte. Necesito saber qué está sucediendo. La dirección de correo electrónico me devuelve los correos con un mensaje que dice que la dirección no existe. Los teléfonos me dirigen a una lista de espera y después cortan. Intenté con cinco números diferentes. Recibí una llamada de Mallory, que me dijo que los pagos dejarían de salir. Hoy, mi cuenta bancaria está en descubierto debido a ellos. También me dijo que podía llamarla si tenía preguntas. Sin embargo, no responde. Su buzón de voz está lleno. Necesito respuestas.

⁸ Esta denuncia de estafa se editó en aras de la brevedad y la claridad.



REPARACIÓN DE CRÉDITO/ALIVIO DE DEUDA Señales de alarma para tener en cuenta:

Tarifas anticipadas. No todas las empresas que prometen ayudarlo a reparar su mal crédito son estafas, pero, si le solicitan que pague por adelantado, es una señal de alarma muy grande. Tanto en EE. UU. como en Canadá, las empresas de reparación de crédito y alivio de deudas solo pueden cobrar la tarifa después de realizar los servicios prometidos.

Demasiadas promesas. Otras señales de alarma son las grandes promesas, como eliminar la información negativa de su informe de crédito o instarlo a obtener una identidad nueva o a solicitar un Número de Identificación del Empleador para usar en lugar de su SSN/SIN (a propósito, eso es un delito). No recibir un contrato o recibir uno que es impreciso es otra señal de alarma.

Garantías. Nadie puede garantizar hacer desaparecer las deudas ni mejorar su calificación de crédito. De hecho, no pueden prometerle nada antes de haber revisado su situación financiera personal.

Datos demográficos



Los datos demográficos aportados a través de BBB Scam Tracker, combinados con la investigación mediante encuestas, nos permiten comprender mejor cómo varía el riesgo en los distintos subgrupos de población. BBB utiliza esta información para mejorar sus estrategias educativas y de divulgación para ayudar a los consumidores y a las empresas a identificar y evitar las estafas.

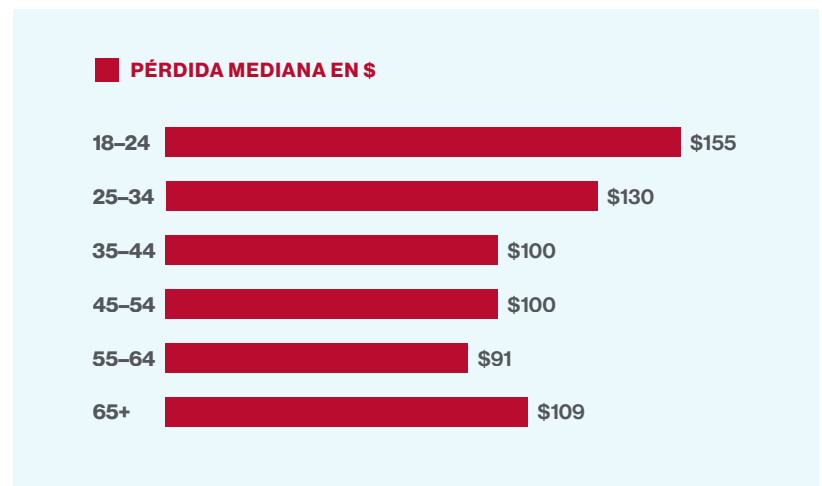
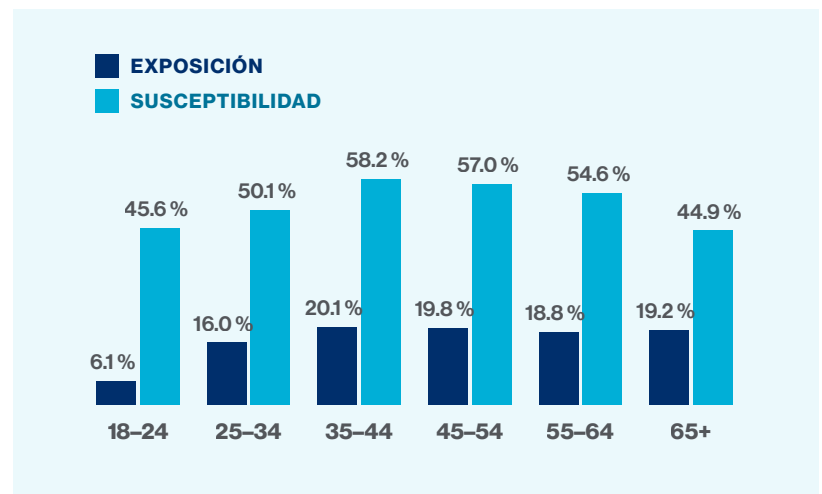
Edad

Por segundo año consecutivo, el grupo de 18 a 24 años de edad indicó una pérdida mediana en dólares más alta (\$155) que todos los demás grupos etarios (Figura 8). Un mayor porcentaje de personas entre 35 y 54 años denunció haber perdido dinero cuando fueron blanco de una estafa (susceptibilidad) que otros grupos etarios; las personas mayores de 65 volvieron a ser el grupo de menor susceptibilidad (44.9%).

La tabla 2 destaca los tres tipos de estafas más riesgosas por edad. Las estafas laborales fueron el tipo de estafa más riesgosa para el grupo etario de 18 a 44 años. Las estafas de inversión/criptomoneda fueron las más riesgosas para el grupo etario de más de 45 años.

FIGURA 8

Exposición, susceptibilidad y pérdida mediana en dólares por edad (todos los tipos de estafas)



Por segundo año consecutivo, el grupo de **18 a 24 años de edad** indicó una **pérdida mediana en dólares más alta (\$155)** que todos los demás grupos etarios.

TABLA 2

Los tres tipos de estafas más riesgosas por edad

	18-24	25-34	35-44	45-54	55-64	65+
1	Laboral	Laboral	Laboral	Inversión/criptomoneda	Inversión/criptomoneda	Inversión/criptomoneda
2	Compras en línea	Inversión/criptomoneda	Inversión/criptomoneda	Laboral	Compras en línea	Romance
3	Inversión/criptomoneda	Compras en línea	Compras en línea	Compras en línea	Mejoras en el hogar	Mejoras en el hogar

Estafas que apuntan a los jóvenes

BBB Scam Tracker no recopila información de personas menores de 18 años. Sin embargo, sabemos que los jóvenes son blanco de estafas. Del 20.1% de los encuestados que informaron tener hijos de entre 7 y 18 años, el 16.4% afirmó que sus hijos fueron blanco de estafas. Esta cifra representa un aumento con respecto al 11.1% que afirmó que sus hijos habían sido blanco de estafas en 2022. Los encuestados informaron que sus hijos fueron blanco a través de redes sociales, llamadas telefónicas, mensajes de texto, plataformas de gaming, correo electrónico y aplicaciones móviles (Figura 9).

FIGURA 9

Método de contacto con los jóvenes, de acuerdo a las denuncias

A la pregunta de dónde fueron blanco de una estafa, los encuestados respondieron:



Los totales no suman 100% porque se sugirió a los encuestados que eligieran todas las respuestas que correspondieran.

Género

Al igual que en años anteriores, más de dos tercios de las denuncias a BBB Scam Tracker en 2023 fueron de mujeres (Figura 10). Las mujeres fueron más susceptibles a perder dinero cuando estuvieron expuestas a una estafa (53.2 %) que los hombres (49.8 %) y que las personas que se identifican como no binarias (36.3 %). La pérdida mediana en dólares denunciada fue significativamente inferior para las mujeres (\$95) que para los hombres (\$178) y las personas no binarias (\$187).

Este año, hubo cambios en los tres tipos de estafas más riesgosas por género. En 2023, las estafas laborales fueron más riesgosas para las mujeres, las estafas de inversión/criptomoneda fueron más riesgosas para los hombres y las estafas de compras en línea fueron más riesgosas para las personas que se identifican como no binarias (Tabla 3).

FIGURA 10

Exposición, susceptibilidad y pérdida promedio en dólares por género

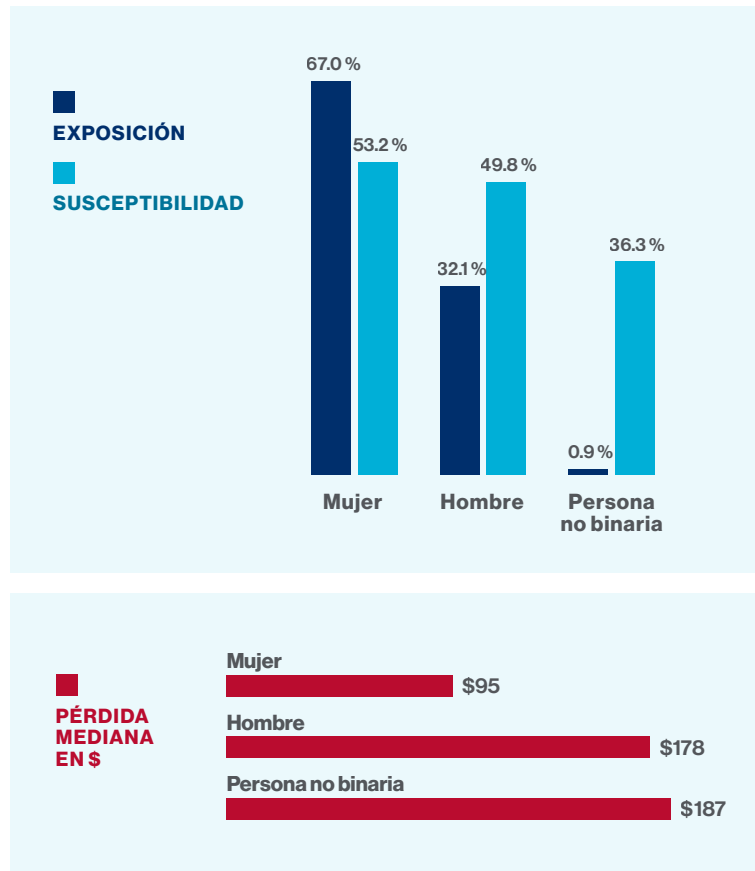


TABLA 3

Los tres tipos de estafas más riesgosas por género

	MUJER	HOMBRE	PERSONA NO BINARIA
1	Laboral	Inversión/ criptomoneda	Compras en línea
2	Inversión/ criptomoneda	Laboral	Laboral
3	Compras en línea	Mejoras en el hogar	Phishing/ ingeniería social

Métodos de pago y de contacto



Métodos de contacto

Los tres principales métodos de contacto en 2023 que dieron lugar a una denuncia con pérdida monetaria fueron las redes sociales (29.3 %), las páginas web (28.9 %) y los correos electrónicos (18.5 %) (Figura 11). El porcentaje de personas que dijeron haber sido contactadas a través de correos electrónicos aumentó un 31.8 % de 2022 a 2023.

El impacto de las redes sociales aumenta

El porcentaje de personas que denunciaron haber sido contactadas a través de redes sociales aumentó un 63.8 % de 2022 a 2023. La pérdida mediana en dólares por estafas en redes sociales disminuyó con respecto al año anterior, pero la susceptibilidad aumentó de 64.8 % en 2022 a 80.2 % en 2023.

Las estafas en línea continúan aumentando

Las estafas cometidas en línea aumentaron de 56.5 % en 2022 a 68.4 % en 2023. Al igual que en años anteriores, las estafas cometidas en línea tuvieron una mayor probabilidad de dar como resultado una pérdida monetaria que las que se llevaron a cabo en persona o por teléfono (Figura 12).

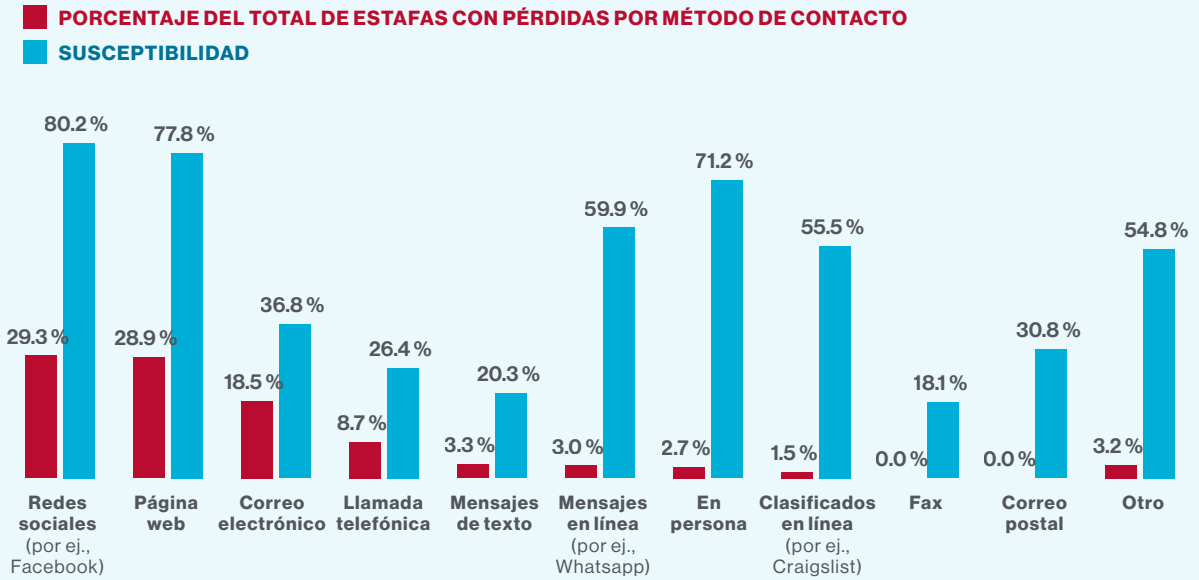
La Figura 13 desglosa los niveles de edad y el método de contacto. Las personas mayores fueron más propensas a denunciar la pérdida de dinero cuando se las contactó por teléfono o clasificados en línea. Las personas más jóvenes fueron más propensas a denunciar la pérdida de dinero cuando se las contactó por mensaje de texto o mensajes en línea.

Las estafas por compras en línea fueron el tipo de estafa más denunciado en el que la persona informó haberse comunicado con un estafador a través de una página web, redes sociales, correos electrónicos, mensajes en línea o clasificados en línea (Tabla 4).

El porcentaje de personas que denunciaron haber sido contactadas a través de redes sociales aumentó un **63.8 %** de 2022 a 2023.

FIGURA 11

Forma de contacto que implicó una pérdida monetaria

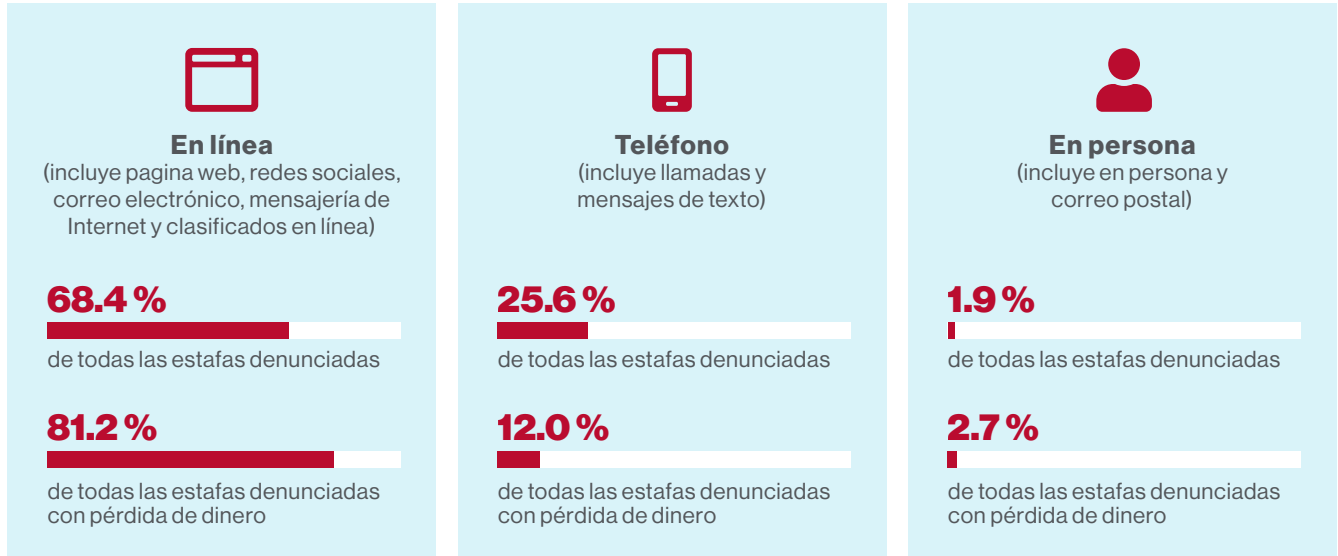


Estas cifras no suman 100 % porque no se incluyeron los datos que "no correspondían".



FIGURA 12

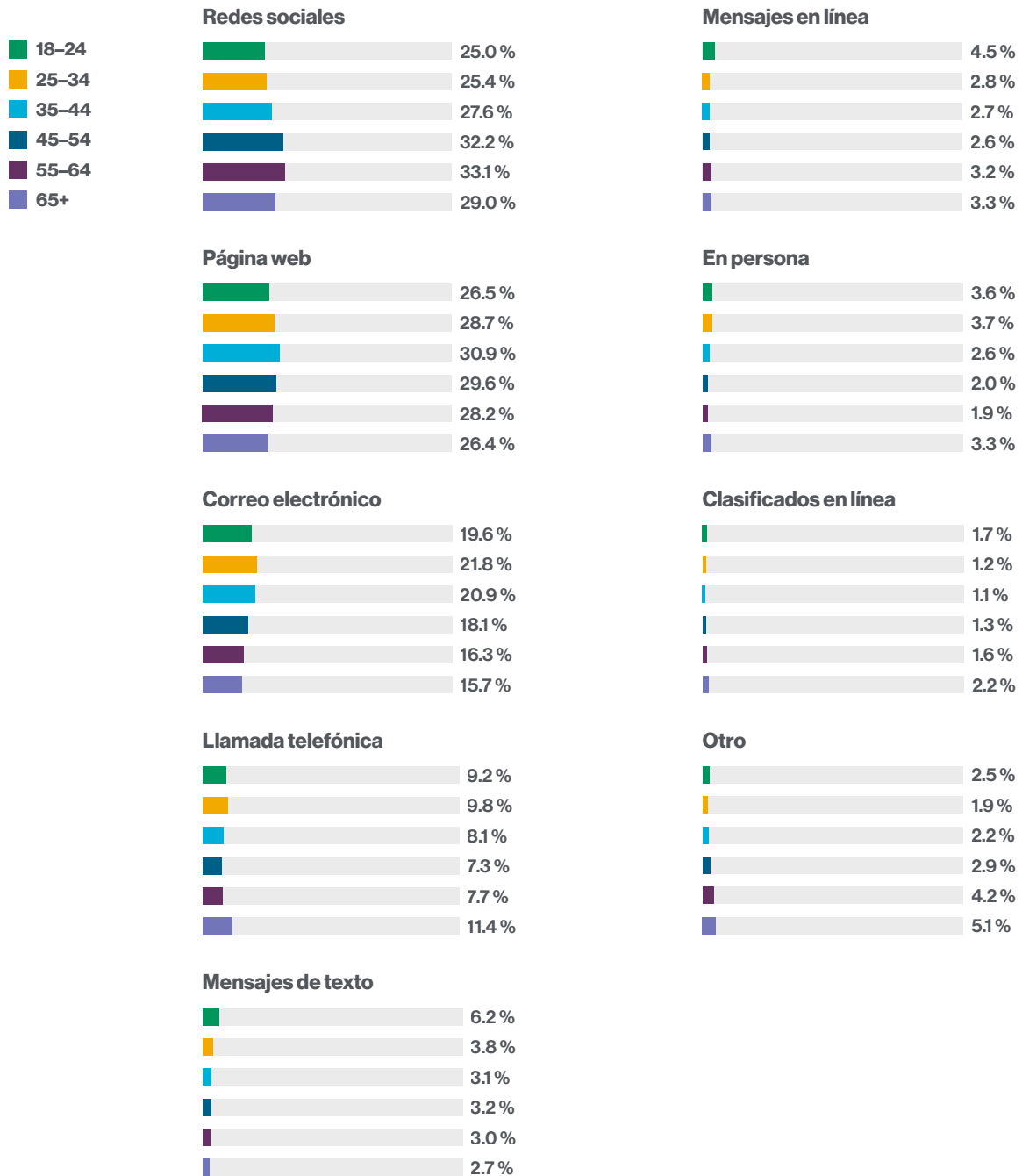
Todas las estafas en comparación con las estafas con una pérdida monetaria denunciada por medio de contacto



Los porcentajes de todas las estafas y de las estafas con pérdidas monetarias no suman 100 % porque no se incluyó la categoría "otros".

FIGURA 13

Forma de contacto por edad (con pérdida monetaria)



No se muestran los métodos de contacto con respuestas insignificativas.

TABLA 4
Tipos de estafa más denunciados por método de contacto

MÉTODO DE CONTACTO	Nº1	Nº2	Nº3
Página web	Compras en línea	Laboral	Producto falsificado
Mensajes en línea (por ej., Whatsapp)			Inversión/criptomoneda
Redes sociales			Phishing/ ingeniería social
Clasificados en línea (por ej., Craigslist)			
Correo electrónico			
Fax			Laboral
Mensajes de texto	Phishing/ ingeniería social		
En persona	Mejoras en el hogar		
Llamada telefónica	Phishing/ ingeniería social	Compras en línea	Cobranza de deudas
Correo postal		Sorteos/lotería/ premios	Cheque/ giro postal falso

Método de pago

En 2023, las tarjetas de crédito (41.9 %) continuaron siendo el principal método de pago con pérdidas monetarias (Figura 14), seguido por los débitos de cuentas bancarias (21.8 %) y los sistemas de pago en línea (17.5 %). Resulta interesante que las denuncias de débitos de cuentas bancarias con pérdidas aumentaron un 66.4 %, mientras que las denuncias de sistemas de pagos en línea con pérdidas disminuyeron un 30.8 % de 2022 a 2023. Las estafas de tarjetas prepagas (de regalo) con pérdidas se redujeron de 5.0 % en 2022 a 3.2 % en 2023.

Los métodos de pago con la mayor mediana de pérdidas en dólares fueron las transferencias bancarias (\$8000), las criptomonedas (\$3300) y los cheques (\$2625). La pérdida mediana en dólares declarada en relación con estos métodos de pago aumentó significativamente con respecto al año anterior.

Al desglosar la pérdida monetaria por edad y método de pago (Figura 15), las personas mayores fueron más propensas a denunciar pérdidas monetarias mediante tarjetas de crédito, tarjetas prepagas/de regalo y cheques. Las personas más jóvenes fueron más propensas a denunciar pérdidas monetarias mediante sistemas de pago en línea y débitos de cuentas bancarias.

Las estafas por compras en línea fueron el tipo de estafa que más se denunció con varios métodos de pago (tarjeta de crédito, sistema de pago en línea, débito en cuenta bancaria, tarjeta prepaga, transferencia electrónica y giro postal) (Tabla 5).

FIGURA 14

Método de pago con denuncia de pérdida monetaria

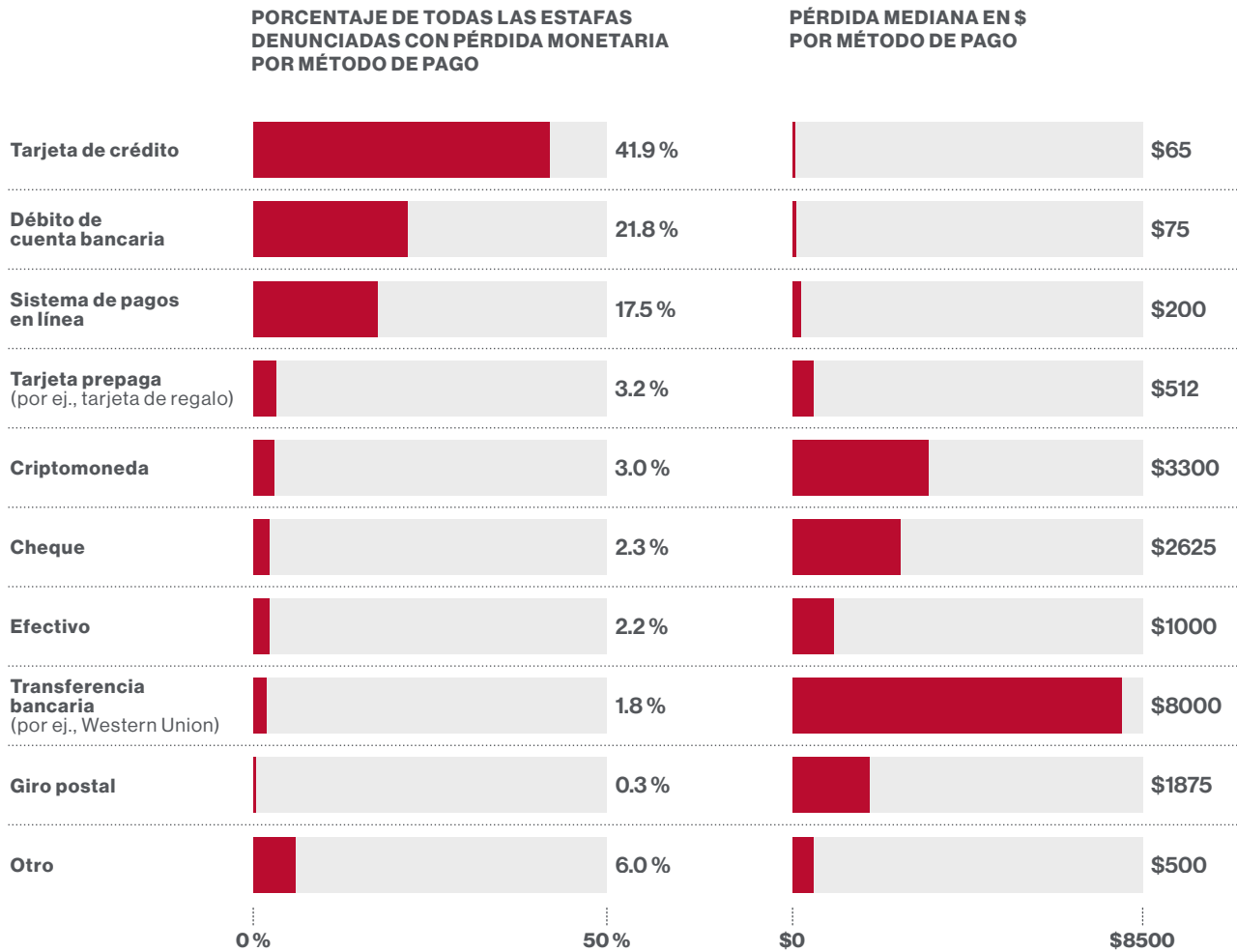


FIGURA 15

Forma de contacto por edad (con denuncia de pérdida monetaria)

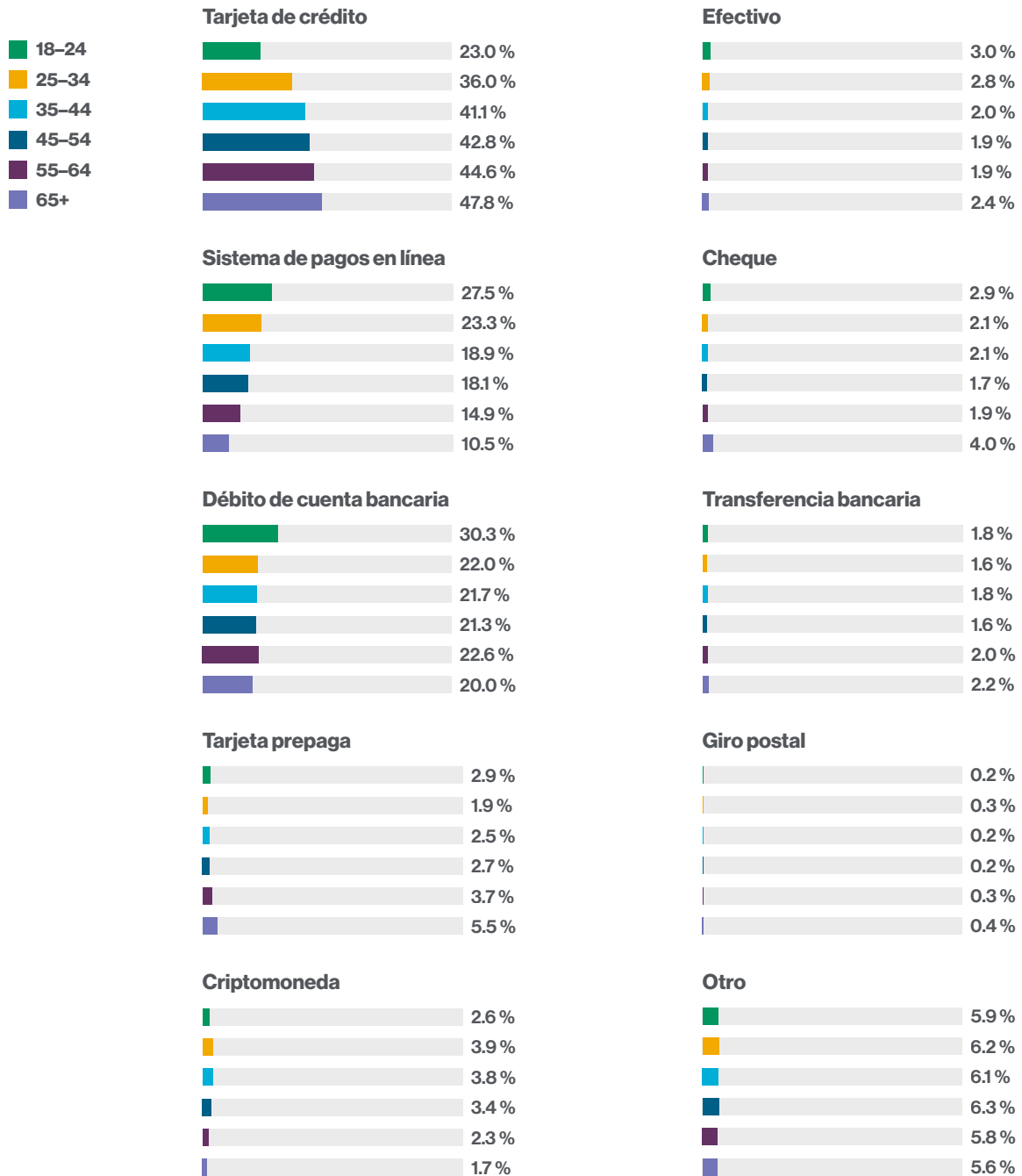


TABLA 5
Tipos de estafa más denunciados por método de pago

MÉTODO DE CONTACTO	Nº1	Nº2	Nº3
Tarjeta de crédito	Compras en línea	Producto falsificado	Phishing/ ingeniería social
Sistema de pagos en línea		Phishing/ ingeniería social	Laboral
Débito de cuenta bancaria			Tarifa por anticipo de préstamo garantizado
Tarjeta prepaga		Inversión/ criptomoneda	Compras en línea
Criptomoneda	Laboral	Mejoras en el hogar	Compras en línea
Cheque	Compras en línea	Inversión/ criptomoneda	Tarifa por anticipo de préstamo garantizado
Transferencia bancaria		Laboral	
Giro postal	Mejoras en el hogar	Compras en línea	Laboral
Efectivo			

Impacto en públicos específicos



Consumidores de Canadá

En 2023, los consumidores de Canadá denunciaron 2104 estafas a BBB Scam Tracker (3.2 % de las denuncias totales presentadas tanto en los Estados Unidos como en Canadá). La pérdida mediana general en dólares declarada en 2023 fue de 300 dólares canadienses, la misma pérdida mediana general en dólares declarada en 2022. El porcentaje de personas que denunciaron haber perdido dinero al ser blanco de una estafa (susceptibilidad) aumentó de 46.9 % en 2022 a 61.1% en 2023.

Las tres principales estafas más riesgosas que se denunciaron en Canadá cambiaron en 2023. Este año, combinamos dos tipos de estafa (criptomonedas e inversión) en una categoría, ya que la mayoría de las estafas de criptomonedas implican situaciones de inversión. Las estafas de inversión/criptomonedas pasaron a ser la principal estafa más riesgosa con una pérdida mediana en dólares alta (9365 dólares canadienses). Más del 82 % de las personas que denunciaron haber sido blanco de estafas de inversión/criptomonedas perdieron dinero (Tabla 6).

Las estafas laborales pasaron de ser la quinta estafa más riesgosa a ser la segunda con una pérdida mediana en dólares de 3600 dólares canadienses. Las estafas de mejoras para el hogar, la tercera estafa más riesgosa, tuvo una pérdida mediana en dólares de 2000 dólares canadienses y un porcentaje alto de denuncias con pérdidas en dólares (84.1%). Puede acceder al Informe de Riesgo de Canadá completo en BBBMarketplaceTrust.org/CanadaRiskReport.

TABLA 6 Las tres estafas más riesgosas de Canadá

PUESTO	TIPO DE ESTAFA	ÍNDICE DE RIESGO DE BBB	EXPOSICIÓN*	SUSCEPTIBILIDAD	PÉRDIDA MEDIANA EN \$
1	Inversión/ criptomoneda	1127.6	4.4 %	82.6 %	\$9365 CAD
2	Laboral	484.8	15.6 %	25.8 %	\$3600 CAD
3	Mejoras en el hogar	469.0	8.4 %	84.1 %	\$2000 CAD

* La exposición está limitada por la naturaleza de la auto-denuncia; el porcentaje de quienes reportaron a BBB Scam Tracker ser víctimas de estafas no necesariamente coincide con el porcentaje de personas en la población total que fueron blanco de estafas.

Organizaciones con suplantación de identidad

Los estafadores, haciéndose pasar por compañías reconocidas, agencias de gobierno y organizaciones buscan apropiarse de la confianza y la autoridad de estas marcas. En algunos casos, los estafadores suplantan la identidad de personas reales.

En 2023, el Servicio Postal de EE. UU. pasó a ocupar el primer puesto de la lista de organizaciones con más suplantación de identidad que se denunciaron a BBB Scam Tracker (Tabla 7). La agencia intercambió posiciones con Amazon, que descendió al segundo puesto de la lista. Aproximadamente el 58 % de las denuncias de suplantación de identidad del Servicio Postal de EE. UU. se trató de estafas de phishing. En cuanto a Amazon, el 43 % de las denuncias de suplantación de identidad se trató de estafas de phishing, el 17 % de estafas por compras en línea y el 10 % de estafas laborales.

Varias de las mismas organizaciones de 2022 continúan estando en la lista de este año. Este año, Better Business Bureau apareció entre las 15 principales organizaciones con suplantación de identidad. También se denunciaron alusiones al “Departamento de Garantías” y al “Departamento de Regulación Comercial de EE. UU”, pero no se incluyeron en la lista porque las referencias no pudieron vincularse a una organización específica.

TABLA 7

Las 20 principales organizaciones, personas utilizadas para la suplantación de identidad

Puesto	Organización/ Nombre de persona	Cantidad de denuncias de estafa
1	Servicio Postal de EE. UU.	804
2	Amazon	606
3	Publishers Clearing House	536
4	Geek Squad	430
5	Norton	387
6	PayPal	384
7	Microsoft	206
8	Walmart	198
9	Facebook	189
10	McAfee	188
11	Better Business Bureau	184
12	Bed Bath & Beyond	178
13	Servicio de Rentas Internas (IRS)	162
14	Medicare	154
15	Advance America	136
16	Macy's	134
17	Spectrum	114
18	Best Buy	104
19	Capital One	98
20	Lending Club	95

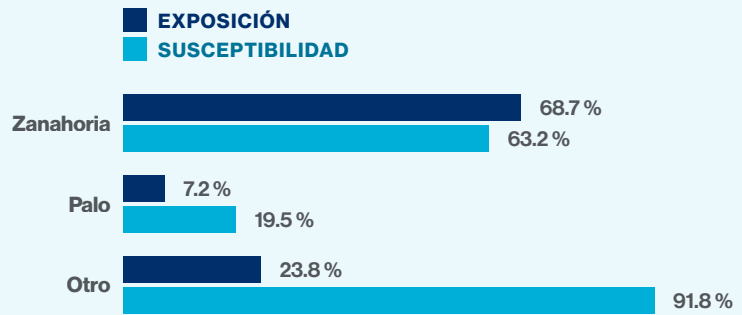
El palo y la zanahoria: análisis del impacto de las tácticas de estafas



Los estafadores utilizan una amplia variedad de tácticas para llevar a cabo sus estafas, algunas de las cuales resultan más efectivas que otras. Algunas tácticas utilizan la promesa de una oportunidad (“zanahoria”) para alentar al blanco a que no interrumpa la comunicación con los estafadores. Algunos ejemplos del enfoque de la zanahoria incluyen la posibilidad de ganar dinero de manera rápida con inversiones de bajo riesgo o con ofertas laborales demasiado buenas para ser ciertas. Otras tácticas utilizan una amenaza (“palo”) o una situación negativa para manipular a las víctimas de fraude, como por ejemplo, la cárcel por impuestos atrasados o noticias de que un ser querido está en problemas y necesita ayuda. El informe de este año desglosa los diferentes tipos de estafas en tres categorías: método de la zanahoria, método del palo y otros (tipos de estafa que no se pueden clasificar fácilmente en una categoría).

FIGURA 16

Tácticas “el palo y la zanahoria” por exposición, susceptibilidad y pérdida mediana de dólares



Estas cifras no suman 100 % porque no se incluyeron los datos que “no correspondían”.



En este análisis, se incluyeron las estafas dirigidas tanto a consumidores como a empresas. El desglose de los tipos de estafa incluye los siguientes:

Estafas con el método de la zanahoria:

tarifa por anticipo de préstamo garantizado, inversión/criptomonedas, cheques/giros postales falsos, reparación de crédito/alivio de deudas, estafas laborales, productos falsificados, subvenciones del gobierno, mejoras en el hogar, sorteos/loterías/premios, beneficencia, intercambio de moneda extranjera, alquiler, estafas relacionadas con romances, premios relacionados con la vanidad, viajes/vacaciones/tiempos compartidos, compras en línea, COVID-19, Páginas Amarillas/directorios y servicios inútiles de resolución de problemas.

Estafas con el método del palo:

cobranza de deudas, cobro de impuestos, vulneración de correos electrónicos empresariales, emergencias de familiares/amigos, impostores de agencias de gobierno, facturas falsas de proveedores o de otras personas, soporte técnico y servicios públicos.

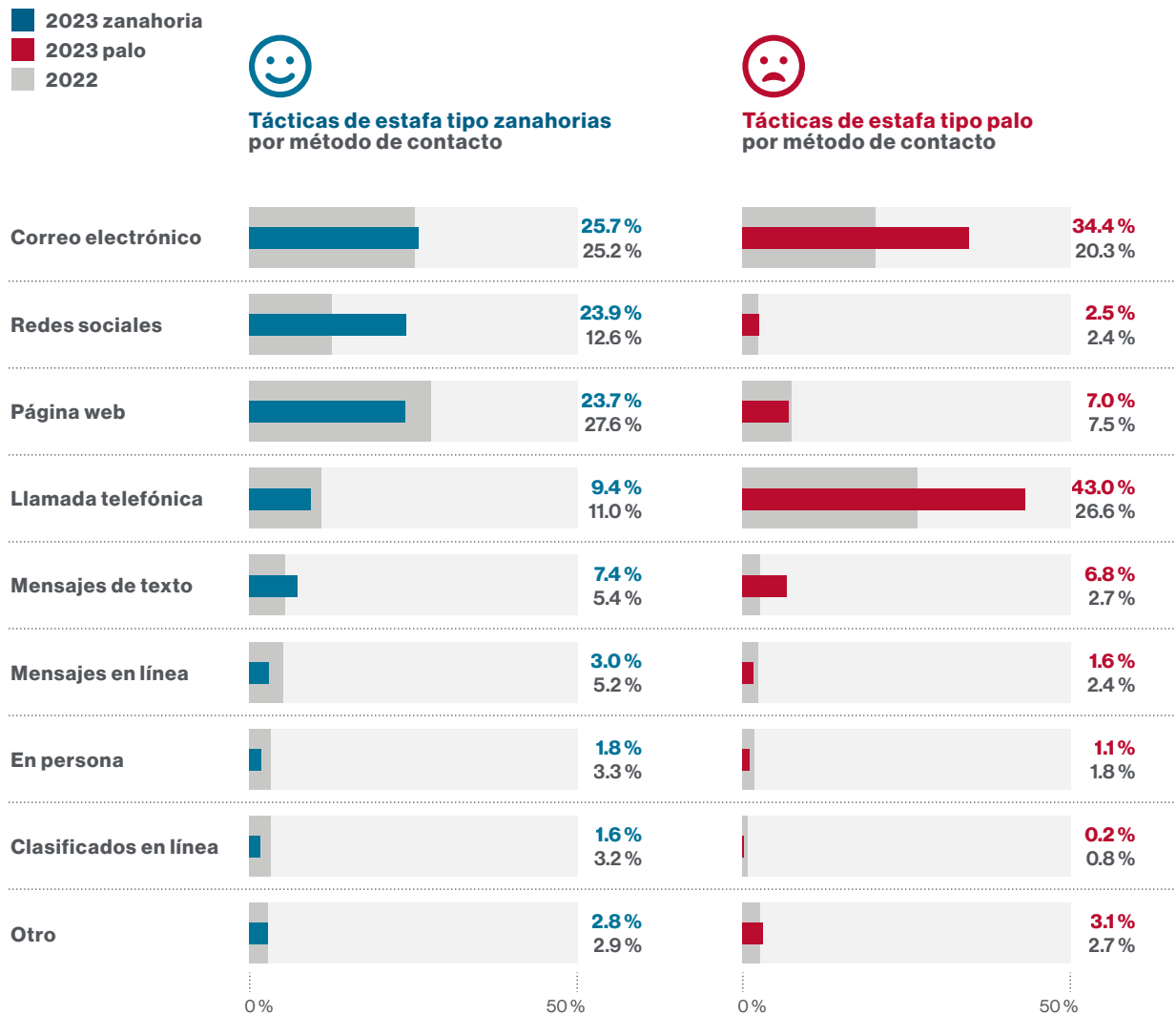
Otras estafas que no se pueden clasificar fácilmente como método de la zanahoria o del palo: phishing, impostores de empresas bancarias/de tarjetas de crédito, robo de identidad, tarjetas de crédito, mudanzas y atención médica/Medicaid/Medicare.

Usando el Índice de Riesgo de BBB, descubrimos que las personas son más propensas a denunciar la pérdida de dinero en estafas que se llevan a cabo mediante el método de la zanahoria (63.2 %) que con el método del palo (19.5 %) (Figura 16). Sin embargo, cuando las personas denunciaron pérdidas de dinero en estafas que se llevaron a cabo con el método del palo, denunciaron haber perdido mucho más dinero (\$400) que en las estafas con el método de la zanahoria (\$96).

Las tácticas del método de la zanahoria utilizaron más redes sociales o páginas web para atraer a las víctimas. Es más probable que las tácticas del método del palo intentaran llegar a sus víctimas por teléfono (Figura 17). Es interesante destacar que las tácticas del método de la zanahoria mediante redes sociales aumentó de un 12.6 % en 2022 a un 23.9 % en 2023.

FIGURA 17

Método de contacto por método de zanahoria o palo



Estas cifras no suman 100 % porque no se incluyeron los datos que "no correspondían".

Indicios y comportamientos que observaron los afectados y ayudaron a evitar la pérdida de dinero



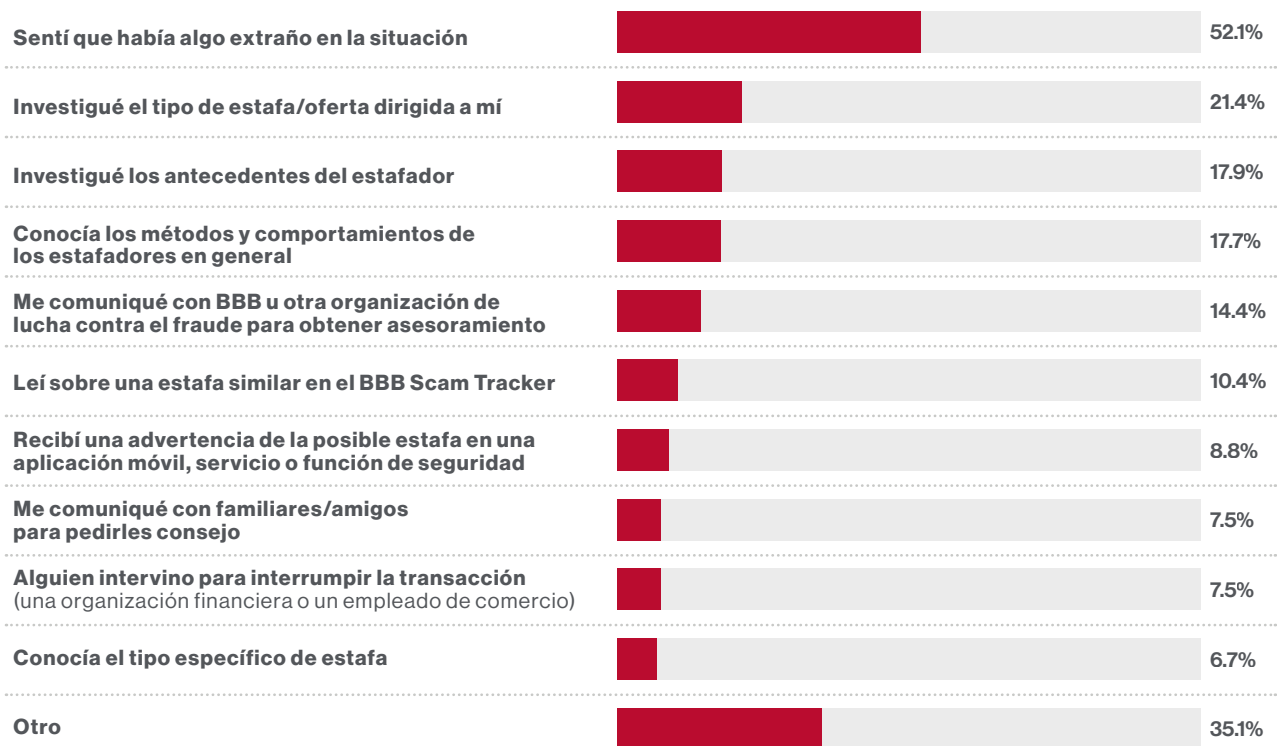
Factores que según las personas les ayudaron a evitar pérdidas de dinero

Nuestro equipo preguntó a los encuestados nuevamente este año qué creían que les ayudó a evitar la pérdida de dinero cuando los contactaba un estafador (Figura 18). De los encuestados que presentaron una denuncia por estafa en 2023, el 52.1 % dijo que evitó perder dinero en una estafa porque “advirtió que había algo extraño en la situación”.

Otros de los indicios/comportamientos principales incluyeron investigar el tipo de estafa/oferta (21.4 %), investigar los antecedentes del estafador (17.9 %) y conocer los métodos y los comportamientos generales de los estafadores (17.7 %).

FIGURA 18

Factores/Pistas que según las personas les ayudaron a evitar pérdidas de dinero



Los totales no suman 100 % porque se sugirió a los encuestados que eligieran todas las respuestas que correspondieran.

Otros factores que pueden influir en la victimización

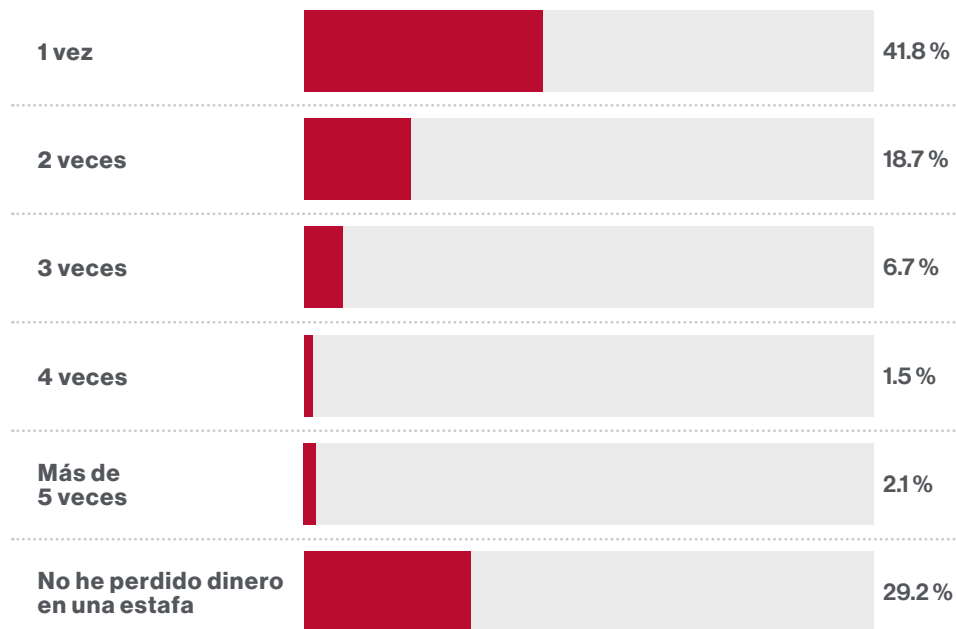


Víctimas repetidas

Cuando pedimos a los encuestados que indicaran cuántas veces habían perdido dinero a causa de una estafa, el 10.3 % declaró haber perdido dinero al menos tres veces, en comparación con 8.4 % en 2022 (Figura 19). El 29 % declaró haber perdido dinero más de dos veces (frente al 23.5 % en 2022).

FIGURA 19

Cantidad de veces que la persona denunció haber perdido dinero en una estafa

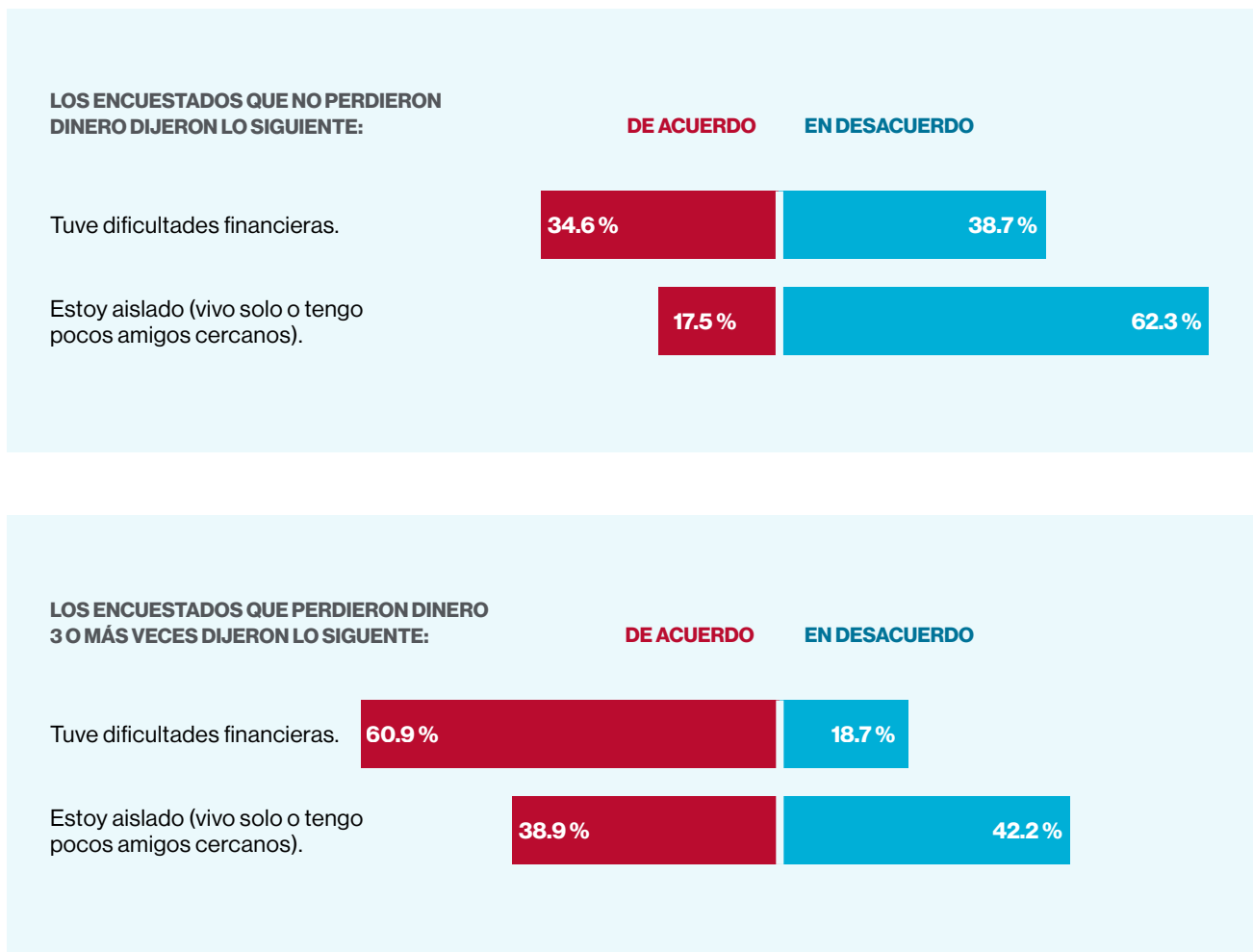


Las personas encuestadas que declararon haber perdido dinero en una estafa tres o más veces fueron más propensas a denunciar que tuvieron dificultades financieras significativas en el último año. Las personas que denunciaron haber perdido dinero tres o más veces también fueron más propensas a indicar que están aisladas (viven solas o tienen pocos amigos) (Figura 20).

FIGURA 20

Factores que pueden tener un impacto en la victimización repetida

Cuando se les preguntó si estaban de acuerdo o en desacuerdo con los factores que describen su experiencia al ser blanco de una estafa:



Recursos preferidos de educación para el consumidor

Pedimos a las personas encuestadas que nos indicaran cómo prefieren recibir información sobre la prevención de estafas (Figura 21). Las personas de 18 a 54 años de edad eligieron las redes sociales como fuente principal de información de educación sobre estafas. Las personas de más de 55 años de edad dijeron que preferían las alertas de fraude.

FIGURA 21

Recursos preferidos de educación sobre estafas por edad



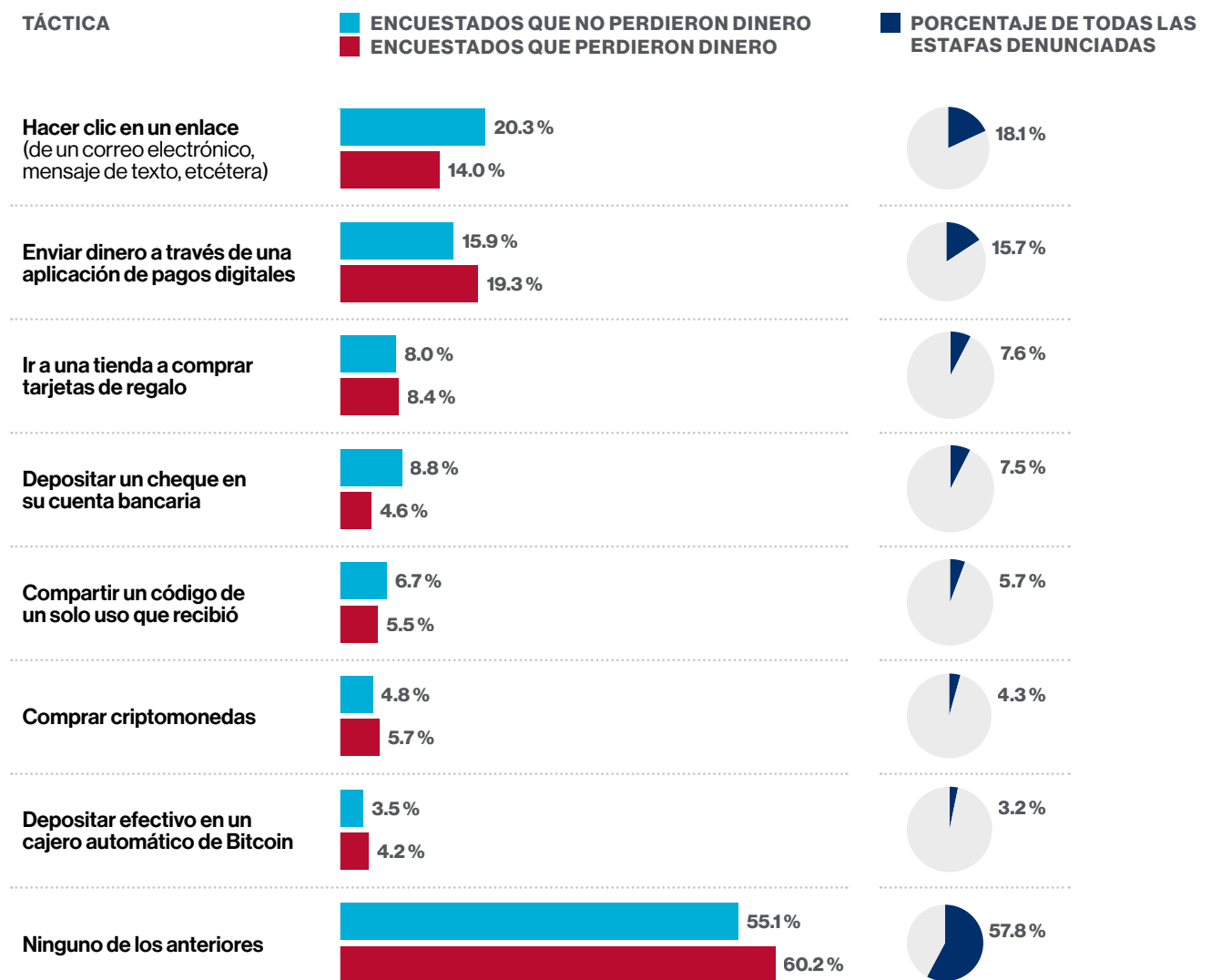
Otras tácticas de estafa

Pedimos a las personas que hicieron denuncias en BBB Scam Tracker que nos contaran sobre otras tácticas que los estafadores utilizaron para comunicarse con ellas (Figura 22). La principal táctica denunciada fue hacer clic en un enlace de un correo electrónico o mensaje de texto, seguida de enviar dinero a través de un sistema de pago en línea (aplicación de pagos digitales).

FIGURA 22

Tácticas de los estafadores

Cuando se les preguntó “En algún momento de la interacción con los estafadores, ¿le pidieron que hiciera alguna de las siguientes cosas?”, las personas encuestadas seleccionaron todas las tácticas de los estafadores que correspondían.



Los totales no suman 100 % porque se sugirió a los encuestados que eligieran todas las respuestas que correspondieran.

Estafas dirigidas a empresas



BBB Scam Tracker también recopila información sobre estafas dirigidas a empresas. Las empresas declararon haber perdido dinero el 29.5 % de las veces, una susceptibilidad significativamente más baja que la declarada por los consumidores (52.0 %). Sin embargo, la pérdida mediana general en dólares que declararon las empresas (\$523) fue significativamente más alta que la declarada por los consumidores (\$100) (Figura 23).

Las tres estafas más riesgosas dirigidas a empresas según el Índice de Riesgo de BBB fueron las estafas de servicios inútiles de resolución de problemas⁹, las estafas de impostores de empresas bancarias/de tarjetas de crédito y las estafas de facturas falsas de proveedores o de otras personas (Tabla 8).

FIGURA 23

Susceptibilidad general y pérdida monetaria (estafas a empresas frente a estafas a consumidores)

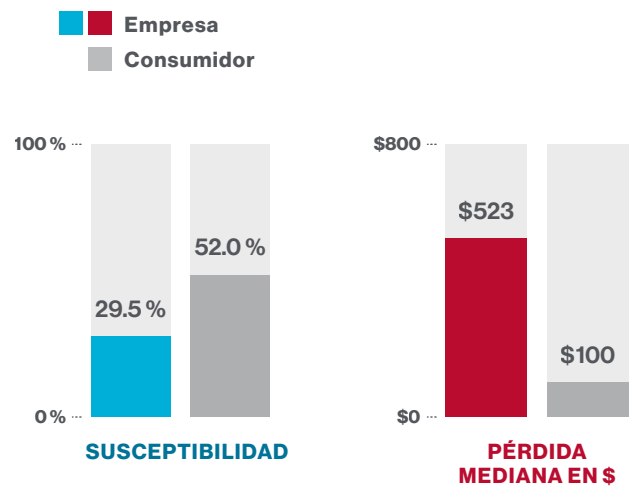


TABLA 8

Estafas más riesgosas denunciadas por empresas

PUESTO	TIPO DE ESTAFA	ÍNDICE DE RIESGO DE BBB	SUSCEPTIBILIDAD	PÉRDIDA MEDIANA EN \$
1	Servicio inútil de resolución de problemas	175.1	59.8 %	\$500
2	Impostores de empresas bancarias/ de tarjetas de crédito	111.6	28.0 %	\$983
3	Factura falsa/Factura de proveedor	36.7	11.9 %	\$413

⁹ A veces, los estafadores afirman poder ofrecer soluciones de bajo costo a problemas que saben que tienen muchas empresas. Por ejemplo, pueden afirmar que pueden reparar la reputación online de la empresa o proporcionar alivio rápido si tiene problemas de deudas o impuestos atrasados, por supuesto, pagando una tarifa por adelantado.

10 consejos generales para evitar que lo estafen

Estos consejos pueden ayudarlo a evitar la mayoría de las estafas y a protegerse y proteger a su familia.

1 Evite hacer compras rápidas mientras navega por las redes sociales.

Las denuncias de estafas llevadas a cabo en redes sociales aumentaron un 63.8 % de 2022 a 2023. Tómese un momento para investigar la página web que tiene esa oferta increíble para asegurarse de que no sea falsa.

2 Sea muy prudente al comunicarse con alguien que conoció en línea.

Asegúrese de no compartir información personal con alguien que no conoce en persona. Si la persona comienza a pedir dinero o le ofrece una oportunidad de inversión sin riesgos, es una señal de alarma.

3 No haga clic en enlaces ni abra archivos adjuntos en correos electrónicos o mensajes de texto no solicitados.

Si la persona afirma ser alguien que conoce o una organización conocida, comuníquese con la persona directamente o diríjase a su cuenta directamente para confirmar la información. Se informó que la suplantación de identidad fue la táctica más común que se utilizó para cometer estafas.

4 No crea todo lo que ve o lee.

Los estafadores son excelentes para imitar sellos oficiales, fuentes de letras y otros detalles. El hecho de que una página web o correo electrónico parezca oficial no significa que lo sea. Incluso hasta se puede falsificar el identificador de llamadas en el teléfono.

5 Tome precauciones al hacer compras en línea.

No compre solo por el precio. Los estafadores ofrecen productos difíciles de encontrar a excelentes precios.

No compre en línea a menos que la transacción sea segura. Asegúrese de que la página web tenga "https" en la URL (la "s" es para "seguro") y un pequeño icono de candado en la barra de direcciones. Sin embargo, incluso las páginas web seguras pueden ser fraudulentas.

Investigue más sobre los productos y la empresa antes de hacer la compra.

6 Conozca las señales de alarma generales de las estafas:

La oferta suena demasiado buena para ser real.

La persona insiste en que debe actuar de inmediato o la oferta terminará pronto.

Alguien le pide que deposite dinero en un cajero automático de Bitcoin o le envía un cheque y le pide que lo deposite y luego transfiera los fondos.

Le exigen un pago por adelantado antes de brindar un servicio.

7 Nunca divulgue información de identificación personal a un contacto no solicitado.

Si alguien le pide que comparta su número de seguro social (SSN)/número de la seguridad social (SIN) o su número de licencia de conducir, considere que es una señal de alarma y proceda con precaución.

8 Tómese su tiempo. No se deje presionar para actuar de inmediato.

En cambio, investigue o discuta la situación con un tercero.

9 Utilice transacciones seguras y rastreables

cuando haga pagos de bienes, servicios, impuestos y deudas. Las tarjetas prepagas/de regalo, por ejemplo, no se pueden rastrear. Su fin es usarlas como regalo, no como pago.

10 Siempre que sea posible, trabaje con empresas que tengan la identificación, la licencia y el seguro adecuados.

Investigue la compañía primero en BBB.org.

Obtenga más información sobre estas estafas.

BBB.org/AvoidScams

BBB.org/ScamTips

Más información sobre estafas a empresas:
BBB.org/all/business-scams

BBB Institute for Marketplace Trust

El BBB Institute for Marketplace Trust (BBB Institute), el sector de beneficencia de Better Business Bureau, publica el *Informe de Riesgo BBB Scam Tracker* todos los años. Nuestra misión es educar y proteger a los consumidores, establecer prácticas recomendadas para los negocios y resolver problemas complejos del mercado. Nuestros programas de educación para el consumidor, que incluyen una amplia variedad de recursos educativos y preventivos con respecto al fraude, se ofrecen en formato digital y en forma presencial a través de la red de comunidades que brindan servicios de BBB en Estados Unidos y Canadá. La investigación es un componente integral de nuestro trabajo y nos permite incorporar las tendencias más recientes sobre fraude en nuestros recursos e iniciativas de educación para el consumidor. Puede encontrar más información sobre el BBB Institute y sus programas en BBBMarketplaceTrust.org.

Guía de prevención de estafas

En 2023, BBB Institute presentó un micrositio nuevo que tiene como objetivo ayudar a las personas a obtener el conocimiento que necesitan para identificar y evitar las estafas. La guía incluye cuestionarios, videos, una biblioteca de materiales y una calculadora de riesgo que ayuda a los usuarios a entender los tipos de estafa que representan el mayor riesgo para su perfil demográfico (edad, género, país, situación militar). Puede encontrar la guía en BBB.org/scam-prevention.

Scam Survival Toolkit

(Kit de herramientas para recuperarse de estafas)

También presentamos una versión de prueba de un recurso en línea nuevo para las víctimas de estafa. Desarrollado con el apoyo de Amazon y Capital One, el Kit de herramientas para recuperarse de estafas conecta a las víctimas de estafa con los recursos que necesitan para restaurar su bienestar financiero, mental y emocional. La versión final se publicará este año en BBB.org/ScamSurvivalKit.

Gracias a nuestros patrocinadores.

BBB Institute desea reconocer a nuestros socios financieros por posibilitar la investigación y los programas de BBB Institute.





Investigación del BBB Institute

Targeting Our Youth: How Scams Are Impacting Ages 18-24 (Los jóvenes en la mira: cómo afectan las estafas a los jóvenes de 18 a 24 años)

Sabemos por estudios de investigación anteriores que las estafas se dirigen a personas de todas las edades. Sin embargo, las formas en las que las personas se comunican con los estafadores y en las que se ven afectadas pueden variar entre los diversos grupos demográficos. El informe *Targeting Our Youth*, publicado en octubre de 2023, analiza en más detalle cómo se apunta al grupo etario de los jóvenes y cómo se ven afectados por las estafas.

Todos los estudios de investigación de BBB Institute se pueden encontrar en nuestra página web: BBBMarketplaceTrust.org/research



Elegida como la mejor herramienta para combatir estafas

por la Alianza Mundial contra la Estafa y ScamAdviser.com

Más información sobre el BBB Scam Tracker en:
BBB.org/ScamTracker



APÉNDICE A: Glosario de tipos de estafas

Las estafas denunciadas a BBB Scam Tracker este año se clasifican en 28 estafas al consumidor y cinco estafas a empresas. Estas clasificaciones representan estafas comunes denunciadas a BBB y se basan en clasificaciones de tipos utilizadas por la Comisión Federal de Comercio y el Centro contra Delitos Cibernéticos de la Oficina Federal de Investigaciones. Puede encontrar consejos útiles para prevenir estos tipos de estafa en <https://www.bbb.org/all/scamtips>.

Los tipos de estafa **resaltados en azul** son estafas denunciadas por empresas.

Tarifa por anticipo de préstamo garantizado	Un préstamo está garantizado, pero una vez que la víctima paga cargos por adelantado, como impuestos o una "tarifa de procesamiento", el préstamo nunca se concreta. Lea nuestros consejos para la prevención de estafas relacionadas con tarifas por anticipo de préstamo garantizado.
Impostores de empresas bancarias/ de tarjetas de crédito	Esta estafa suele implicar la suplantación de identidad de un banco o de otro emisor de tarjetas de crédito. Con el pretexto de verificar información de la cuenta, convencen a sus víctimas de compartir información bancaria o de tarjetas de crédito
Vulneración de correos electrónicos empresariales	Un estafador suplanta la identidad de un ejecutivo de alto rango a través de un correo electrónico u otro medio de comunicación para convencer a un empleado de que transfiera el pago de bienes a otra cuenta bancaria. Lea nuestros consejos sobre vulneración de correos electrónicos empresariales.
Beneficencia	Las organizaciones benéficas falsas o impostoras se utilizan para obtener dinero de personas que creen que están haciendo donaciones a organizaciones benéficas legítimas. Esto es particularmente común después de un desastre natural u otra tragedia. Lea nuestros consejos de prevención de estafas de beneficencia.
Producto falsificado	Los productos falsificados imitan la mercadería original, hasta el logotipo de la marca registrada; sin embargo, por lo general son de inferior calidad. Este tipo de estafa puede resultar en un peligro para la salud o la seguridad de riesgo mortal cuando el artículo falsificado es un medicamento, un suplemento de nutrición o una repuesto de un automóvil. Lea nuestros consejos para la prevención de estafas con productos falsificados.
Tarjeta de crédito	Los estafadores se hacen pasar por un banco u otro emisor de tarjetas de crédito, pretendiendo verificar los detalles de la cuenta para obtener la tarjeta de crédito o la información bancaria de la víctima. Lea nuestros consejos para la prevención de estafas con tarjetas de crédito.
Reparación de crédito/ alivio de deuda	Los estafadores que se hacen pasar por proveedores de servicios legítimos cobran el pago por adelantado, con promesas de alivio de la deuda y reparación del crédito, pero dan poco o nada a cambio. Lea nuestros consejos para la prevención de estafas de reparación de crédito/alivio de deudas.
Cobranza de deudas	Los cobradores de deudas falsos acosan a sus víctimas para que paguen deudas que no deben. Lea nuestros consejos para la prevención de estafas relacionadas con las cobranzas.
Laborales	A los candidatos que buscan empleo se les hace creer que están solicitando o que acaban de ser contratados para un trabajo nuevo y prometedor cuando, en realidad, divulgaron información personal mediante una solicitud falsa o enviaron dinero a estafadores para "capacitación" o "equipo". En otra variante de esta estafa, es posible que a una persona se le "pague de más" con un cheque falso y se le pide que devuelva la diferencia. Lean nuestros consejos para evitar las estafas laborales.

APÉNDICE A: Glosario de tipos de estafas

Cheque/giro postal falso	<p>La víctima deposita un cheque falso y luego devuelve una parte por transferencia bancaria o aplicación digital de pago al estafador. Las historias varían, pero a menudo se le dice a la víctima que está reembolsando un sobrepago “accidental”. Los estafadores cuentan con el hecho de que los bancos ponen a disposición los fondos a los pocos días de un depósito, pero pueden tardar semanas en detectar un cheque falso.</p> <p><u>Lea el estudio de cheques falsos de BBB.</u></p>
Facturas falsas de proveedores o de otras personas	<p>Los estafadores eligen a los propietarios de empresas como víctimas y esperan que no noten una factura, que suele ser de suministros de oficina que la empresa nunca pidió. Incluso pueden entregar mercadería que no se pidió y, luego, intentar hacer que la empresa pague. En otros casos, los estafadores envían avisos urgentes de renovación del hosting del dominio de una página web o de otros servicios fundamentales, y esperan que las empresas paguen sin hacer la debida diligencia. <u>Lea nuestros consejos sobre facturas falsas de proveedores o de otras personas.</u></p>
Emergencias de familiares/amigos	<p>Esta estafa implica la suplantación de identidad de un amigo o de un familiar que aparentemente está atravesando una situación urgente o grave. El “ser querido” siempre pide que le envíen dinero de inmediato. Con la ayuda de detalles personales que, por lo general se encuentran en las redes sociales, los impostores cuentan historias muy creíbles para convencer a las víctimas de la estafa. <u>Lea nuestros consejos para prevenir estafas relacionadas con emergencias de familiares/amigos.</u></p>
Intercambio de moneda extranjera	<p>El blanco recibe un correo electrónico de un funcionario de gobierno extranjero, miembro de la realeza o propietario de una empresa que ofrece una enorme suma de dinero para que le ayuden a sacar dinero del país del estafador. La víctima se hace cargo de los costos de la transferencia, ya que cree que se los devolverán. <u>Lea nuestros consejos para prevenir estafas relacionadas con intercambio de moneda extranjera.</u></p>
Agencia de gobierno impostora	<p>Los estafadores fingen ser representantes de una agencia gubernamental estadounidense o canadiense, como el Servicio de Rentas Internas (IRS), la Agencia de Rentas de Canadá, la Administración del Seguro Social o una amplia selección de otras agencias. En 2023, los estafadores fingieron ser del Servicio Postal de EE. UU.</p>
Subvenciones del gobierno	<p>Se engaña a las personas con promesas de subvenciones gratuitas garantizadas por el gobierno que requieren el pago por adelantado de un “cargo por procesamiento”. Luego se le agregan otros cargos, pero la subvención prometida nunca se concreta. <u>Lea nuestros consejos para prevenir estafas relacionadas con subvenciones del gobierno.</u></p>
Atención médica, Medicaid y Medicare	<p>El estafador busca obtener información del seguro médico, de Medicaid o de Medicare del asegurado para enviar cargos médicos fraudulentos o para robarle la identidad. <u>Lea nuestros consejos para prevenir estafas relacionadas con la atención médica.</u></p>
Mejoras en el hogar	<p>Los que ofrecen trabajo de puerta en puerta dicen que hacen reparaciones rápidas y de bajo costo para luego tomar el pago y no regresar; hacen trabajos pésimos o “descubren” problemas que aumentan de manera significativa el precio del trabajo. Estos tipos de estafas suelen ocurrir después de fuertes tormentas o desastres naturales. <u>Lea nuestros consejos para la prevención de estafas relacionadas con mejoras en el hogar.</u></p>
Robo de identidad	<p>Los ladrones de identidad usan información personal de la víctima (p. ej., números de seguro social, información de cuenta bancaria y números de tarjetas de crédito) para hacerse pasar por esa persona en beneficio propio. Al usar la identidad de los blancos de las estafas, el ladrón puede abrir una cuenta de crédito, sacar todo el dinero de una cuenta existente, presentar declaraciones impositivas u obtener cobertura médica. <u>Lea nuestros consejos para la prevención de estafas por robo de identidad.</u></p>

APÉNDICE A: Glosario de tipos de estafas

Inversión/criptomoneda	Estas estafas adoptan muchas formas, pero todas se aprovechan del deseo de las víctimas de hacer dinero sin asumir muchos riesgos o inversión inicial. Los "inversionistas" son engañados con información falsa y con promesas de una gran rentabilidad con poco o nada de riesgo. Lea nuestros consejos para la prevención de estafas relacionadas con inversiones. Las estafas de criptomoneda implican la compra, el intercambio o el almacenamiento de activos digitales conocidos como criptomonedas. Las situaciones a menudo involucran ofertas iniciales de monedas (ICO) fraudulentas, un tipo de mecanismo de recaudación de fondos en el que una empresa emite su propia criptomoneda para recaudar capital. Los inversionistas son estafados para que paguen dinero o intercambien sus propios activos digitales, aunque el estafador no tenga intención de desarrollar una empresa. Las estafas de criptomonedas también implican escenarios en los que los inversionistas guardan sus criptomonedas con intercambios fraudulentos. Lea el estudio de BBB sobre estafas con criptomoneda.
Mudanzas	Estas estafas implican servicios de mudanzas fraudulentos que ofrecen precios con descuentos para trasladar objetos domésticos. Los supuestos encargados de la empresa de mudanzas roban los objetos o los retienen y exigen al cliente pagos adicionales para entregarlos en el nuevo lugar. Lea nuestros consejos para la prevención de estafas relacionadas con mudanzas.
Compras en línea	Estas estafas, por lo general, implican la compra de productos o servicios donde las transacciones se hacen a través de una página web o por otros medios en línea. Los estafadores utilizan tecnología para mostrar ofertas atractivas, pero una vez que se hace el pago, no se entrega ningún producto ni servicio. En algunos casos, los estafadores envían productos de baja calidad o falsificados. Lea nuestros consejos para la prevención de estafas relacionadas con las compras en línea.
Phishing/ingeniería social	Con estos mecanismos de engaño, los estafadores suplantan la identidad de una entidad confiable, como un banco o una compañía de hipotecas, y utilizan comunicaciones para engañar a los destinatarios para que brinden información personal que el estafador luego utilizará para obtener acceso a cuentas bancarias o para robar la identidad del destinatario. Este tipo de estafa también puede suceder en el lugar de trabajo, como un correo electrónico proveniente del director ejecutivo, del departamento de contabilidad o de otro miembro de la gerencia que necesita información personal. Lea nuestros consejos para la prevención de estafas relacionadas con el phishing.
Alquiler	Se suelen colocar anuncios falsos para alquilar propiedades en donde se piden pagos anticipados. Las víctimas luego descubren que la propiedad no existe o que otra persona es el propietario. Lea nuestros consejos para prevenir estafas relacionadas con alquileres.
Comercio impostor	Los estafadores se hacen pasar por conocidos comercios minoristas. A menudo, el estafador envía un mensaje de texto o un correo electrónico no solicitado en el que pide al destinatario que haga clic en un enlace para verificar los datos de la cuenta o responder a una duda sobre su cuenta. El objetivo es obtener acceso a la cuenta de la persona.
Romance	Una persona que cree estar en una relación romántica acepta enviar dinero, información personal y financiera u objetos de valor al estafador. A veces ofrecerán oportunidades de inversión, como criptomonedas. Lea nuestros consejos para la prevención de estafas relacionadas con romances.
Becas	A las víctimas, que suelen ser estudiantes que luchan con los costos de educación, se les promete dinero del gobierno para becas, pero luego de pagar los "cargos" anticipados, los fondos tan necesarios nunca llegan. A veces, los estudiantes reciben un cheque falso y se les pide que envíen una parte para impuestos u otros cargos. Lea nuestros consejos para la prevención de estafas relacionadas con becas.

APÉNDICE A: Glosario de tipos de estafas

Sorteos, loterías y premios	Se hace creer a las víctimas que han ganado un premio o la lotería, pero deben pagar cargos anticipados para recibir los premios, que nunca se concretan. A veces, esto implica un cheque falso y se le solicita al supuesto ganador que envíe una parte de los fondos como cargos de cobertura. <u>Lea nuestros consejos para la prevención de estafas relacionadas con sorteos/loterías/premios.</u>
Cobro de impuestos	Los impostores se hacen pasar por representantes del Servicio de Rentas Internas de Estados Unidos o de la Agencia de Rentas de Canadá para obligar al blanco a pagar los impuestos o compartir información personal. <u>Lea nuestros consejos para la prevención de estafas relacionadas con el cobro de impuestos.</u>
Soporte técnico	Las estafas de soporte técnico comienzan con una llamada o con una ventana de advertencia emergente que alerta a la víctima de que la computadora tiene un virus u otro problema. Los estafadores, que se hacen pasar por empleados de soporte técnicos de reconocidas empresas de tecnología, hacen que las víctimas paguen por el "soporte". Si la víctima permite el acceso remoto al dispositivo, se instalará un malware. <u>Lea nuestros consejos para la prevención de estafas relacionadas con soporte técnico.</u>
Viajes/vacaciones/ tiempo compartido	Los estafadores publican anuncios de propiedades que no se alquilan, que no existen o que son muy distintas de las que aparecen en la foto. En otra variante, los estafadores afirman estar especializados en reventas de unidades de tiempo compartido y aseguran que tienen compradores dispuestos a comprar. <u>Lea nuestros consejos para la prevención de estafas relacionadas con viajes.</u>
Servicios públicos	Los estafadores se hacen pasar por representantes de empresas públicas de agua, electricidad y gas para obtener dinero o información personal. Suelen amenazar a los residentes y propietarios de negocios con la desconexión del servicio si no pagan de inmediato. En otra modalidad, un "representante" puede acudir a un domicilio para hacer "reparaciones" o una "auditoría de energía" con la intención de robar objetos de valor. <u>Lea nuestros consejos para la prevención de estafas relacionadas con los servicios públicos.</u>
Servicio inútil de resolución de problemas	A veces, los estafadores afirman poder ofrecer soluciones de bajo costo a problemas que saben que tienen muchas empresas. Por ejemplo, pueden afirmar que pueden reparar la reputación online de la empresa o proporcionar alivio rápido si tiene problemas de deudas o impuestos atrasados, por supuesto, pagando una tarifa por adelantado.
Páginas amarillas/ directorios	Los estafadores convencen a una empresa para que pague por publicidad inexistente o por un anuncio en un directorio o "Páginas amarillas" que no existen. En algunos casos, el directorio existirá técnicamente, pero no se distribuirá ampliamente y un listado en dicho directorio tendrá poco o ningún valor para la empresa.

APÉNDICE B: Tabla de datos con tipo de estafa, estafas al consumidor

TIPO DE ESTAFA	ÍNDICE DE RIESGO	EXPOSICIÓN	SUSCEPTIBILIDAD	PÉRDIDA MEDIANA EN \$
Tarifa por anticipo de préstamo garantizado	57.2	1.4 %	45.3 %	\$ 900
Beneficencia	0.5	0.3 %	28.0 %	\$ 70
Producto falsificado	14.4	2.2 %	83.3 %	\$ 80
COVID-19*	0.03	0.06 %	5.1 %	\$ 86
Tarjeta de crédito	13.3	1.1 %	33.5 %	\$ 380
Reparación de crédito/alivio de deuda	29.4	0.5 %	55.7 %	\$ 1000
Cobranza de deudas	9.8	2.2 %	9.2 %	\$ 500
Laboral	445.9	14.8 %	15.1 %	\$ 1995
Cheque/giro postal falso	8.6	0.3 %	26.7 %	\$ 1165
Emergencia familiar/de un amigo	7.8	0.3 %	32.1 %	\$ 900
Cambio de moneda extranjera	1.1	0.1 %	1.4 %	\$ 7400
Agencia de gobierno impostora	5.7	1.5 %	26.2 %	\$ 149
Subvención del gobierno	21.0	0.7 %	33.8 %	\$ 948
Atención médica/Medicaid/Medicare	6.4	0.7 %	19.1 %	\$ 477
Mejoras en el hogar	201.2	1.3 %	74.7 %	\$ 2073
Robo de identidad	8.9	1.0 %	28.9 %	\$ 300
Inversión/criptomoneda**	520.9	1.7 %	80.4 %	\$ 3800
Mudanza	6.3	0.2 %	78.1 %	\$ 350
Compras en línea	244.9	41.9 %	82.6 %	\$ 71
Phishing/ingeniería social	56.5	12.6 %	15.0 %	\$ 300
Alquiler	17.8	0.6 %	64.1 %	\$ 504
Comercio impostor	4.4	0.7 %	48.1 %	\$ 129
Romance	151.4	0.6 %	65.7 %	\$ 3600
Sorteos/lotería/premios	10.4	2.5 %	21.3 %	\$ 200
Recaudación de impuestos	4.4	0.1 %	18.3 %	\$ 2306
Soporte técnico	25.5	1.9 %	26.6 %	\$ 500
Viaje/vacaciones/tiempo compartido	23.6	0.7 %	59.6 %	\$ 543
Servicios públicos	5.7	0.5 %	24.1 %	\$ 463
Otro	71.7	7.7 %	44.5 %	\$ 210

* El tipo de estafa de COVID-19 se eliminó de BBB Scam Tracker el 25 de mayo de 2023.

** Este año, combinamos las estafas de criptomonedas y de inversión en una categoría, ya que la mayoría de las estafas de criptomonedas implican situaciones de inversión.

APÉNDICE C: Los 10 principales tipos de estafas al consumidor por riesgo general, exposición, susceptibilidad y pérdida mediana en dólares

	ÍNDICE DE RIESGO	EXPOSICIÓN	SUSCEPTIBILIDAD	PÉRDIDA MEDIANA EN \$
1	Inversión/ criptomoneda	Compras en línea	Producto falsificado	Cambio de moneda extranjera
2	Laboral	Laboral	Compras en línea	Inversión/ criptomoneda
3	Compras en línea	Phishing/ ingeniería social	Inversión/ criptomoneda	Romance
4	Mejoras en el hogar	Sorteos/lotería/ premios	Mudanza	Recaudación de impuestos
5	Romance	Producto falsificado	Mejoras en el hogar	Mejoras en el hogar
6	Tarifa por anticipo de préstamo garantizado	Cobranza de deudas	Romance	Laboral
7	Phishing/ ingeniería social	Soporte técnico	Alquiler	Cheque/ giro postal falso
8	Reparación de crédito/ alivio de deuda	Inversión/ criptomoneda	Viajes/vacaciones/ tiempo compartido	Reparación de crédito/ alivio de deuda
9	Soporte técnico	Agencia de gobierno impostora	Reparación de crédito/ alivio de deuda	Subvención del gobierno
10	Viajes/vacaciones/ tiempo compartido	Tarifa por anticipo de préstamo garantizado	Comercio impostor	Emergencia familiar/ de un amigo y tarifa por anticipo de préstamo garantizado

Agradecimientos

BBB Scam Tracker utiliza la reputación de la marca BBB, de 110 años, para recopilar datos de personas que han sido blanco de estafadores. El programa es posible gracias a la dedicada colaboración de las BBB que trabajan en comunidades de todo Estados Unidos y Canadá; BBB revisa los informes de los consumidores para eliminar los que no parecen ser verdaderas estafas, garantizando así los mejores datos posibles.

Queremos agradecer al equipo de expertos de BBB que ofrecen orientación y aportes al BBB Institute en relación con el programa BBB Scam Tracker, que incluye a Warren King, Presidente y Director Ejecutivo, BBB Serving Western Pennsylvania; Jane Rupp, Presidenta y Directora Ejecutiva, BBB Serving Northern Nevada y Utah; Craig Turner, Director de Sistemas de Información, BBB Serving Eastern & Southwest Missouri & Southern Illinois; Dene Joubert, Gerenta de Investigaciones, BBB Great West + Pacific; y Lindsay Walsh, Asistente de Operaciones, BBB Serving Vancouver Island, The Gulf Islands, Haida Gwaii and Powell River.

También queremos agradecer a la Asociación Internacional de Better Business Bureaus por su apoyo al BBB Institute y al INFORME DE RIESGO 2023 de BBB SCAM TRACKER. Extendemos un agradecimiento especial al Director Sénior de Investigación de IABBB, Dr. Rubens Pessanha, MBA, PMP, SPHR, GPHR, SHRM-SCP; al Analista de Calidad de Datos de IABBB, Ryan Hessling; y al Analista de Calidad de Datos de IABBB, Logan Haskew, por analizar los datos de BBB Scam Tracker y los datos de la investigación de la encuesta para este informe. También queremos agradecer a Melanie McGovern, Directora de Relaciones Públicas y Redes Sociales de IABBB, Sara Grube, Directora de Contenidos y SEO de IABBB, Jody Thomas, Directora de Gestión de la Marca de IABBB y Angela Isabell, Consejera General Adjunta de IABBB por sus aportes y por ayudarnos a compartir estos resultados con el público.

Equipo del proyecto

Logan Haskew es Analista de Calidad de Datos de la Asociación Internacional de Better Business Bureaus. Con capacitación en ingeniería y ciencia de datos, cree fervientemente en la toma de decisiones en función de los datos, tanto para consumidores como para empresas. Cuando no trabaja, se dedica a viajar a lugares lejanos de los Estados Unidos con su mujer y sus tres perros. Logan es coautor del *Informe de Riesgos 2022 de BBB Scam Tracker* y de *Los jóvenes en la mira: cómo afectan las estafas a los jóvenes de 18 a 24 años (Targeting Our Youth: How Scams Are Impacting Ages 18-24)*.

Ryan Hessling es Analista de Calidad de Datos de la Asociación Internacional de Better Business Bureaus. Como especialista en ciencias ambientales, Ryan tiene experiencia en recopilación, procesamiento y análisis de datos. Disfruta de lo mucho que se puede aprender e inferir analizando exhaustivamente conjuntos de datos de todo el mundo. Es oriundo del sureste de Connecticut, tiene dos títulos de Three Rivers Community College y una licenciatura de la Universidad de Connecticut. En su tiempo libre, cuando no está haciendo un nuevo curso o trabajando en proyectos, se lo puede ver junto al mar leyendo un libro o paseando a su perro.

Dr. Rubens Pessanha, MBA, PMP, GPHR, SPHR, SHRM-SCP, es el Director Sénior de Investigación y Desarrollo de la Asociación Internacional de Better Business Bureaus. Rubens tiene más de 20 años de experiencia a nivel global en marketing, desarrollo organizativo estratégico, gestión de proyectos e investigación de mercados. Participó en conferencias en América del Norte, Asia, Europa, África y América del Sur. Ingeniero de producción con un MBA, completó su doctorado en la Universidad George Washington. Es coautor de *BBB Scam Tracker Risk Report (2017-2022)*, *Scams and Your Small Business (2018)*, *Cracking the Invulnerability Illusion (2016)*, *The State of Cybersecurity (2017 y 2018)*, *the BBB Trust Sentiment Index (2017)*, *5 Gestures of Trust (2018)*, *Targeting Our Youth: How Scams Are Impacting Ages 18-24*, y *BBB Industry Research Series—Airlines (2018)*, entre otros títulos. Como hobby, Rubens imparte clases de gestión de proyectos, ética empresarial, estrategia y marketing para estudiantes de grado y posgrado.

Melissa "Mel" Lanning Trumpower es directora ejecutiva del BBB Institute para Marketplace Trust. Mel cuenta con más de 25 años de experiencia en liderazgo de organizaciones sin fines de lucro y trabaja con una amplia variedad de organizaciones benéficas y asociaciones comerciales. Además de dirigir el BBB Institute, Mel dirige el programa BBB Scam Tracker y es coautora de *Targeting Our Youth: How Scams Are Impacting Ages 18-24*, *Start With Trust Online: Online Scams (2022)*, *Online Purchase Scams Report (2020 y 2021)*, *BBB Scam Tracker Risk Report (2017-2022)*, *Scams and Your Small Business (2018)*, *Employment Scams Report (2020)* y *Building Better Together: The BBB Impact Report (2021)*. Mel es licenciada de la Cornell University y tiene una maestría de la Johns Hopkins University.



BBBMarketplaceTrust.org/RiskReport



BBB Institute for Marketplace TrustSM
4250 North Fairfax Drive, Suite 600
Arlington VA 22203

Institute@IABBB.org

