



2022 BBB SCAM TRACKERSM RISK REPORT

Employment scams make a resurgence

2022 BBB SCAM TRACKERSM RISK REPORT

Employment scams make a resurgence

All third party trademarks referenced by BBB Institute for Marketplace Trust remain the intellectual property of their respective owners. Use of the third party trademarks does not indicate any relationship, sponsorship, or endorsement between BBB Institute for Marketplace Trust and the owners of these trademarks. Any references by BBB Institute for Marketplace Trust to third party trademarks is to identify the corresponding third party.

Table of Contents

4	Introduction
6	Snapshot of 2022
8	– Infographic: BBB Scam Tracker Risk Report Highlights
9	BBB Risk Index: A three-dimensional approach to measuring scam risk
11	10 riskiest consumer scams
13	Spotlight on employment scams
15	Spotlight on home improvement scams
16	Demographics
16	– Age
19	– Gender
20	Scam contact and payment methods
28	Impact on specific audiences
28	– Canadian consumers
29	– Military families and veterans
31	– Students
32	– Impersonated organizations and individuals
33	Carrot versus stick: Analyzing the impact of scam tactics
35	Self-reported cues and behaviors that helped people avoid losing money
37	10 tips for avoiding a scam
38	About BBB Institute for Marketplace Trust
39	BBB launches new and improved BBB Scam Tracker
41	Appendix A: Glossary of scam types targeting consumers
44	Appendix B: Scam type data table, consumer scams
45	Appendix C: Top 10 consumer scam types by overall risk, exposure, susceptibility, and median dollar loss
46	Acknowledgements
47	Project Team



Introduction

The BBB Institute for Marketplace Trust (BBB Institute), the educational foundation of the Better Business Bureau® (BBB®), is pleased to present the *2022 BBB Scam Tracker Risk Report*. The annual report analyzes the data that individuals and businesses submit to BBB Scam TrackerSM ([BBB.org/ScamTracker](https://www.bbb.org/ScamTracker)) as a way to shed light on how scams are perpetrated, who is being targeted, which scams have the greatest impact, and behaviors and factors that may impact a person's susceptibility. Highlights of the 2022 report are provided in Figure 3.

This report is a critical part of our ongoing work to share timely data and analysis that support the efforts of all who are engaged in combating marketplace fraud. Scams undermine trust in the marketplace, distort the level playing field, and siphon money from legitimate transactions that could benefit both consumers and businesses, thus impeding economic growth. A healthy marketplace requires empowered and knowledgeable consumers and principled businesses that are proactively working to stop scammers and foster trustworthy relationships.

Prevention is critical in BBB Institute's effort to reduce the impact of scams on consumers and businesses. Our risk report findings enable us to develop timely and effective consumer education programs. BBB Institute delivers these programs digitally and in person, leveraging the expansive network of BBBs serving communities throughout the United States and Canada.

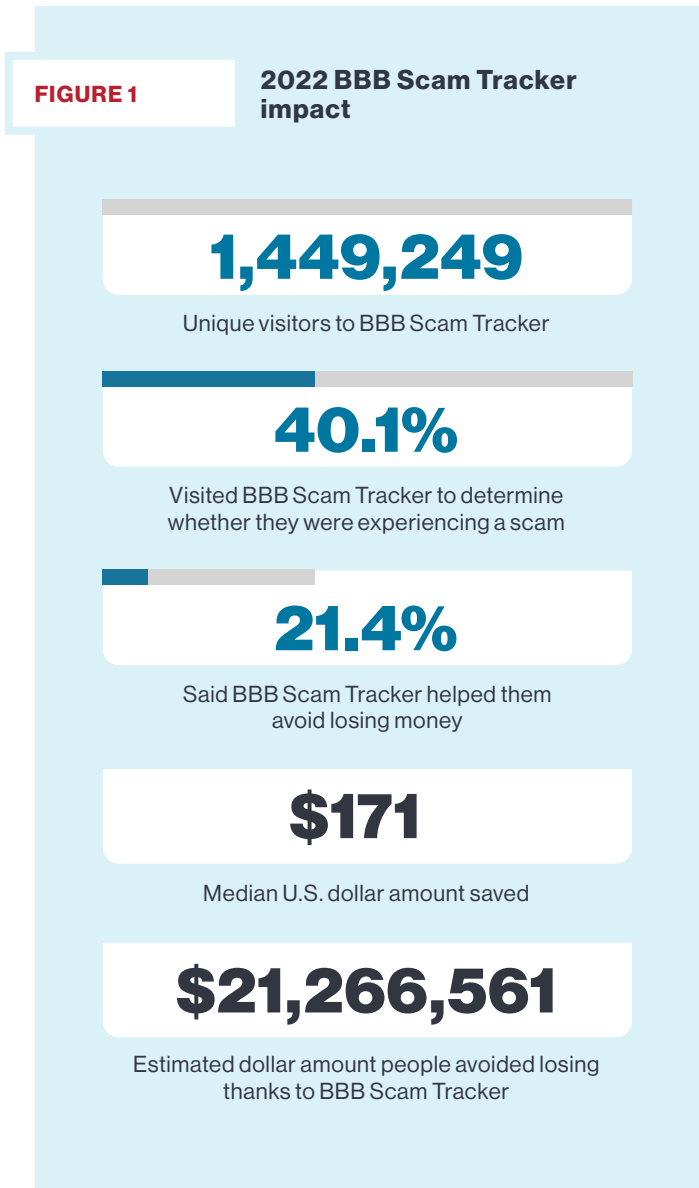
Stopping scammers requires a multisector effort by government agencies and law enforcement, not-for-profits, the media, and the business community. BBB shares its data with partners who are also combating fraud in the marketplace. We work with leaders in business, law enforcement, and government to strategize about the best ways to stop scammers, and we team with corporate partners and like-minded organizations to expand our programming and consumer education activities, evaluate which efforts are working, and continually update them based on internal and external research and data.

BBB Scam Tracker

The *BBB Scam Tracker Risk Report* is made possible with data collected by BBB Scam Tracker, an online platform that enables consumers and businesses to report fraud and fraud attempts. BBBs review and post these reported instances of fraud, enabling the public to search published scams, determine whether they're being targeted, and avoid losing money. In 2022, BBB Institute launched a newly designed BBB Scam Tracker platform in partnership with Amazon and Capital One (more detail about the project is included on [page 39](#)).

According to a survey of BBB Scam Tracker visitors,¹ 40.1% said they visited the BBB Scam Tracker site to determine whether a situation they were experiencing could be a scam, and 21.4% of those said the scam-tracking tool helped them avoid losing money when targeted by a scam. With more than 1.4 million people visiting the platform in 2022,² we estimate BBB Scam Tracker saved people \$21.2 million in 2022 alone (Figure 1).

Our survey research found that 49.7% of visitors to BBB Scam Tracker sought to warn others about a scam, 28.5% sought to help law enforcement stop the scammer, and 21.8% wanted to avoid losing money to a scam attempt.³ We extend our thanks to the more than 300,000 people who reported to BBB Scam Tracker to help others avoid losing money to scams.



¹ Web-intercept survey with 1,125 unique respondents who visited BBB Scam Tracker in January 2023. Respondents could choose multiple reasons for visiting BBB Scam Tracker.

² Adobe Analytics.

³ A survey was distributed to those who submitted a scam report to BBB Scam Tracker in 2022; 4,100 respondents completed the survey.



Snapshot of 2022

The data and insights gleaned from BBB Scam Tracker reports enable us to better understand the impact of scams being perpetrated in the marketplace. This report explores differences in risk borne by specific subsets of the population. In 2022, more than 40,000 scams were published via BBB Scam Tracker, a 12.2% decrease from 2021. We classified scam reports submitted by businesses and individuals in the United States and Canada into 28 consumer scam types, 13 business scam types, and an “other” category that represented 6.2% of all reports. See Appendix A ([page 41](#)) for a full glossary of consumer scam types. Data collected include a description of the scam, the dollar value of any loss, and information about the means of contact and method of payment. Optional demographic data (age, gender, and postal code) about the person targeted by the scam, along with military and/or student status, were also reported via the BBB Scam Tracker platform. See Appendix B and Appendix C for detailed data by scam type.

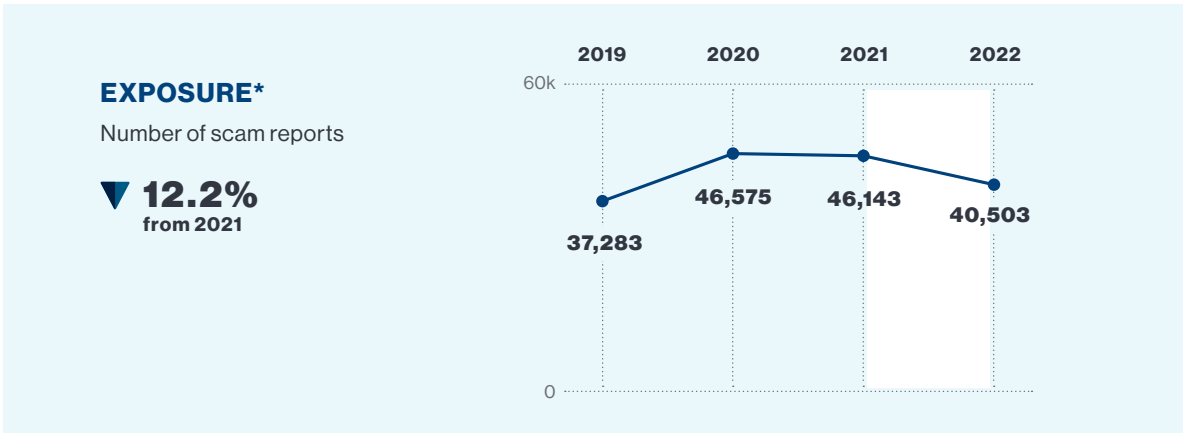
Susceptibility (the percentage of consumers who reported losing money when exposed to a scam) decreased again this year, dropping 4.9% from 42.8% in 2021 to 40.7% in 2022 (Figure 2). Reported median dollar loss rose slightly (1.2%) from \$169 in 2021 to \$171 in 2022.

Online purchase scams remained the riskiest scam type for the third year in a row, despite a drop in exposure, susceptibility, and median dollar loss. Online purchase scams comprised the highest number of reports to BBB Scam Tracker (31.9%) and the highest reported susceptibility (74.0%) in 2022. Employment scams traded places with cryptocurrency scams as the second riskiest, because of an increased number of reported scams and a higher median dollar loss. In 2022, employment scams tied home improvement scams with the highest median dollar loss (\$1,500).

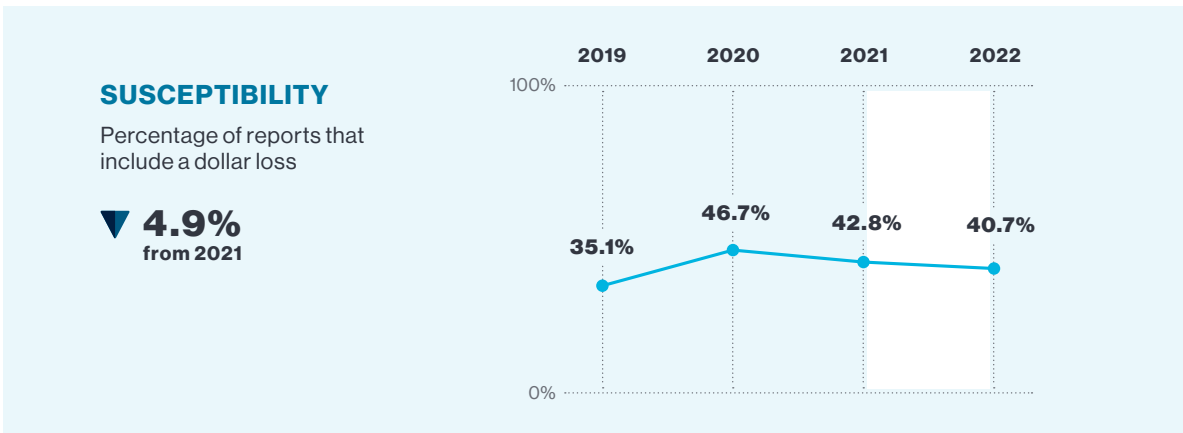
Similar to 2020 and 2021, the top three contact methods in 2022 resulting in a reported monetary loss were website, social media, and email. Credit cards remained the top payment method for scams with a monetary loss, followed by online payment systems.

FIGURE 2

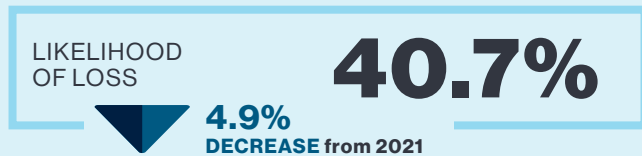
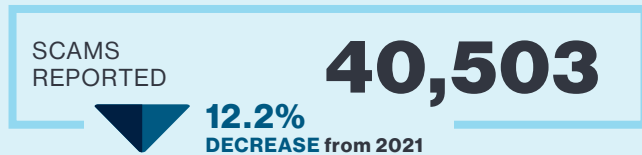
Snapshot of risk (2019–2022)





* Exposure is limited by the nature of self-reporting; the percentage of those who reported to BBB Scam Tracker does not necessarily match the percentage of people in the full population who were targeted by scams.




2022 BBB Scam Tracker Risk Report HIGHLIGHTS




 **Employment scams**, the #2 riskiest scam type, has ranked in the top three riskiest scam types since we began publishing the *BBB Scam Tracker Risk Report* in 2016.

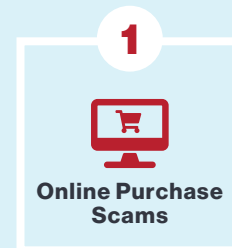
 **Scams perpetrated online** were more likely to result in a reported monetary loss than those perpetrated in person or via phone (see [page 22](#)).

 **18-24** People ages 18 to 24 reported a higher median dollar loss than all other age groups.

 **Amazon was the most reported organization impersonated by scammers again this year**, followed by Geek Squad, Publishers Clearing House, and the U.S. Postal Service.

 Employment scams (#2 riskiest) and home improvement scams (#4 riskiest) had the **highest reported median dollar loss**.

TOP 3 RISKIEST SCAMS REPORTED BY CONSUMERS

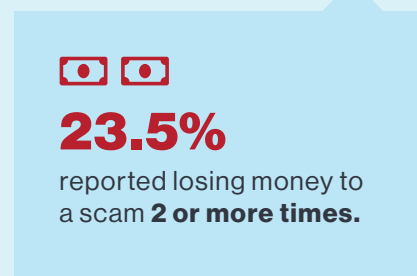


Online purchase scams ranked as the riskiest scam for the third year in a row.

Nearly a third (31.9%) of all scams reported in 2022 **were online purchase scams.**

Almost 3 out of 4 people (74.0%) targeted by online purchase scams **reported losing money.**

SURVEY RESEARCH HIGHLIGHTS





BBB Risk Index: A three-dimensional approach to measuring scam risk

To better understand which scam types pose the highest risk, we assessed scams on the basis of three factors: exposure, susceptibility, and monetary loss. This unique formula makes up the BBB Risk Index (Figure 4). By combining these three factors, we gain a meaningful understanding of scam risk that goes beyond the volume of reports received, enabling BBB and its partners to better target scam prevention outreach.

Risk cannot be determined by viewing just one of these factors in isolation. For example, scams that occur in high volumes typically target as many people as possible but yield a lower likelihood of monetary loss. In comparison, scams with a “high-touch” approach often reach fewer individuals, but those exposed individuals are often more likely to lose money and to lose more money.

The BBB Risk Index does not factor in the emotional and psychological harm scams can inflict on those who are targeted. Our survey research explored the non-financial impacts of scams, with 47.5% of survey respondents reporting they lost confidence or peace of mind because of the emotional impact of being targeted by a scam (Figure 5).⁴ More people reported losing time (57.4%) than reported losing money (54.4%) after being targeted by a scam.

FIGURE 4

BBB Risk Index

The formula for calculating the BBB Risk Index for a given scam in a given population is:

$$\text{Exposure} \times \text{Susceptibility} \times (\text{Median Loss} / \text{Overall Median Loss}) \times 1,000.$$



EXPOSURE*

is a measure of the prevalence of a scam type, calculated as the percentage of a particular scam type as part of the total scams reported.



SUSCEPTIBILITY

is a measure of the likelihood of losing money when exposed to a scam type, calculated as the percentage of all reports that included a monetary loss.



MONETARY LOSS

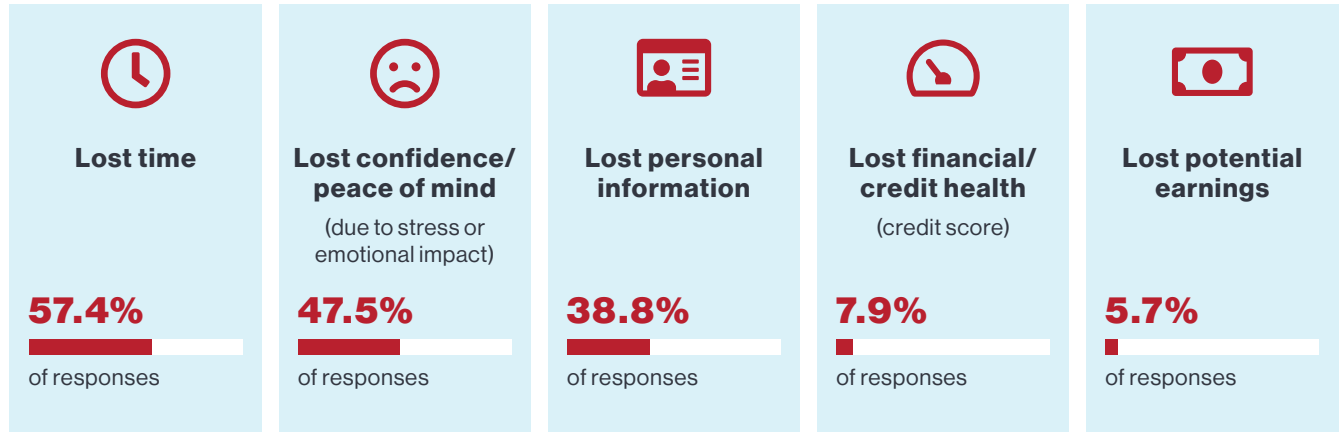
is calculated as the median dollar amount of losses reported for a particular scam type, excluding reports where no loss occurred.

* Exposure is limited by the nature of self-reporting; the percentage of those who reported to BBB Scam Tracker does not necessarily match the percentage of people in the full population who were targeted by scams.

⁴ A survey was distributed to those who submitted a scam to BBB Scam Tracker in 2022; 4,100 respondents completed the survey.

FIGURE 5

Non-financial impacts of being targeted by a scam



47.5% reported losing confidence or peace of mind after being targeted by a scam.



10 riskiest scams reported by consumers in 2022

Each year, BBB publishes our list of the 10 riskiest scam types (Table 1), based on the BBB Risk Index and reports submitted to BBB Scam Tracker. This year's list, which highlights the scam types that pose the most significant risks to consumers, changed slightly from the 2021 list.

In 2022, online purchase scams⁵ remained at the top of our list of riskiest scam types for the third year in a row, making up about one-third of all scams reported to BBB Scam Tracker, with almost three-quarters of people reporting they lost money. The products most used to perpetrate online purchase scams are pets/pet supplies, digital devices, and motor vehicles.⁶

Employment scams have ranked in the top three riskiest scams on our list since we first published the BBB Scam Tracker Risk Report in 2016.

Employment scams have ranked in the top three riskiest scams on our list since we first published the *BBB Scam Tracker Risk Report* in 2016. This scam type rose to the second riskiest in 2022, up from third riskiest in 2021. Though the susceptibility of employment scams remained the same, the number of employment scams reported to BBB Scam Tracker increased 23.1%, from 7.8% of all reported scams in 2021 to 9.6% in 2022. The median dollar loss for employment scams rose 66.7%, from \$900 in 2021 to \$1,500 in 2022.

Cryptocurrency scams fell to the third riskiest scam type in 2022, with exposure, susceptibility, and median dollar loss dropping slightly from 2021. Home improvement scams remained fourth riskiest on the list; the median dollar loss for home improvement scams increased 57.1%, from \$955 in 2021 to \$1,500 in 2022.

Another notable change to the top 10 list is the inclusion of romance scams, which rose from fourteenth riskiest in 2021 to seventh riskiest in 2022; the median dollar loss for this scam type rose 56.8%, from \$900 in 2021 to \$1,411 in 2022. Though investment scams dropped from number five to number six on the list, the median dollar loss for this scam type rose 24.5% from 2021. Fake check/money order scams fell off the list to #14 riskiest.

⁵ Additional information about online purchase scams can be found in [Start With Trust® Online: 2022 BBB Online Scams Report](#).

⁶ Learn more about products used to perpetrate scams on page 21 of our report [Start With Trust® Online: 2022 BBB Online Scams Report](#), published in October 2022.

TABLE 1

10 riskiest consumer scams in 2022

RANK		SCAM TYPE	BBB RISK INDEX	EXPOSURE*		SUSCEPTIBILITY		MEDIAN \$ LOSS	
2022	2021			2022	2021	2022	2021	2022	2021
1	1	Online purchase	137.9	31.9%	37.4%	74.0%	74.9%	\$100	\$101
2	3	Employment	127.6	9.6%	7.8%	15.1%	15.1%	\$1,500	\$900
3	2	Cryptocurrency	67.3	1.7%	1.9%	60.5%	66.2%	\$1,100	\$1,200
4	4	Home improvement	67.1	1.4%	1.4%	55.3%	59.1%	\$1,500	\$955
5	7	Advance fee loan	32.8	1.9%	1.8%	36.7%	40.6%	\$800	\$609
6	5	Investment	28.3	0.7%	0.8%	49.0%	56.9%	\$1,369	\$1,100
7	14	Romance	21.6	1.6%	0.6%	16.1%	36.6%	\$1,411	\$900
8	8	Government grant	20.8	1.6%	2.2%	22.3%	19.5%	\$1,000	\$1,000
9	11	Phishing/social engineering	19.3	11.7%	11.9%	10.6%	9.3%	\$267	\$270
10	9	Tech support	18.6	2.6%	3.1%	25.2%	24.3%	\$490	\$500

* Exposure is limited by the nature of self-reporting; the percentage of those who reported to BBB Scam Tracker does not necessarily match the percentage of people in the full population who were targeted by scams.



SPOTLIGHT ON

Employment scams

Employment scams rose to number two on the list of the riskiest scams in 2022, with reports increasing 23.1% from 2021 to 2022 and a reported median dollar loss of \$1,500.⁷

Scammers promise work-from-home jobs, high wages, and flexible opportunities. Job offers often require only general skills most people could have, enabling the scammer to target a greater number of people.

A few typical scenarios include the following:

- You are hired for a work-from-home opportunity and receive a check for home office equipment. After it arrives, your new employer asks you to wire funds to an account to cover the costs or to transfer funds via an online payment system. Once you've sent the employer the funds, you learn their check is bad, and you must now cover the money you transferred.
- Somebody reaches out to say you are a great fit for a specific position and asks you to fill out an application. You fill it out, providing your birth date, SSN/SIN, driver's license, and other personally identifiable information. They then tell you they are no longer hiring, but now they have your information and can use it for identity theft or another type of fraud.
- You receive an opportunity to work for an "offshore" company that requires funds for a work permit, visa, or international training. Once you pay for the training, your contact stops responding to you.

The following scam report⁸ was submitted by a woman in Alabama:

"I was told I was hired for a data entry position making \$35 an hour. They sent me a check for \$4,860 to purchase equipment. They had me send some money through Zelle, then take \$2,500 of the cash and deposit it into Bitcoin. I am unemployed, and in need of a job, so I was desperate. Now I owe PNC all this money. They took all my funds that I had and left me broke to cover this fraudulent check."

⁷ For more information about employment scams, you can read BBB Institute's [Employment Scams Report](#), the [2020 BBB Job Programs Study](#), or read our [employment scams prevention tips](#).

⁸ This scam report was edited for brevity and clarity.



Employment scam prevention tips

Be wary of offers that seem too good to be true. If you are paying for the promise of a job, it's probably a scam.

Always do background research on the job offer (find the job listing on the company's website).

Be wary of work-from-home offers, shipping/warehouse opportunities, and secret shopper positions. Our research found many fake job offers related to becoming a "warehouse redistribution coordinator" or similar jobs involving reshipping packages.

On-the-spot job offers are a red flag. Beware of offers made too quickly or without an interview.

Don't fall for a fake check scam. Be wary if the "employer" asks you to deposit a check and transfer funds to another account for training or equipment or for any other reason.

Be wary of vague job descriptions. To reach as many people as possible, scammers list job requirements that are broad enough to enable anyone to qualify.



SPOTLIGHT ON

Home improvement scams

Home improvement scams were the fourth riskiest scam type for the second year in a row. People reported losing a median dollar amount of \$1,500 to this scam type, which was tied with employment scams for the highest median dollar loss for any scam type.

Home improvement scams are often perpetrated by door-to-door solicitors who:

- offer quick, low-cost repairs and take payment without returning,
- do shoddy work or don't finish the job, or
- find issues that dramatically raise the price.

These scams can also be perpetrated via online advertisements that offer great deals. Home improvement scams often take place following a major storm or natural disaster, when scammers know people have a strong need for help.

The following scam report⁹ was submitted by a man in Missouri:

"I went on Facebook Marketplace and found an ad for this company for storage buildings. It said they build buildings; the ad included photos. I contacted them and they told me it would be \$1,200. They said they could come by and pick up the check. I dealt with Heather through email. They sent me an invoice with no address. Someone named Bryce showed up to my home and took my check. They cashed the check. The Facebook ad is gone. The last time I had correspondence with them is 11/15/2022. They were supposed to start, and no one showed up. I called and a man answered the phone and said they were coming and never showed up. They will not answer my calls."

⁹ This scam report was edited for brevity and clarity.



Home improvement scam prevention tips

Watch out for red flags.

Say no to cash-only deals, high-pressure sales tactics, high up-front payments, handshake deals without a contract, and on-site inspections. Not all "storm chasers" are con artists, but enough are that you should be cautious anytime a home contractor contacts you first—especially after a natural disaster.

Ask for references and check them out.

Bad contractors will be reluctant to share this information, and scammers won't wait for you to do your homework. Get references from past customers, both older references to check on the quality of the work and newer references to make sure current employees are up to the task. Check them out at BBB.org to see what other customers have experienced. And always be sure to get a written contract with the price, materials, and timeline. The more detail, the better.

Know the law.

Work with local businesses that have proper identification, licensing, and insurance. Confirm that your vendor will get related permits, make sure you know who is responsible for what according to your local laws, and check that your vendor is ready to comply.



Demographics

Self-reported demographic data provided through BBB Scam Tracker combined with survey research enable us to better understand how risk varies across different subgroups of the population. BBB uses this information to enhance how we target outreach and educational strategies aimed at empowering consumers and businesses to identify and avoid scams.

Age

In 2022, a higher percentage of people ages 35–54 years reported losing money when targeted by a scam (susceptibility) than other age groups; people ages 65+ reported the lowest susceptibility (31.8%) again this year. People ages 18–24 reported the highest median dollar loss (\$220) of all age groups, up 29.4% from \$170 in 2021. See Figure 6.

Table 2 highlights the three riskiest scam types by age. Online purchase scams were the riskiest scam types for ages 35–64 again this year, whereas employment scams became the riskiest scam type for people ages 18–34. Home improvement scams rose to become the riskiest scam type for ages 65+.

***In 2022,
ages 18–24
reported the
highest median
dollar loss
(\$220) of all
age groups,
up 29.4% from
\$170 in 2021.***

FIGURE 6

Exposure, susceptibility, and median dollar loss by age (all scam types)

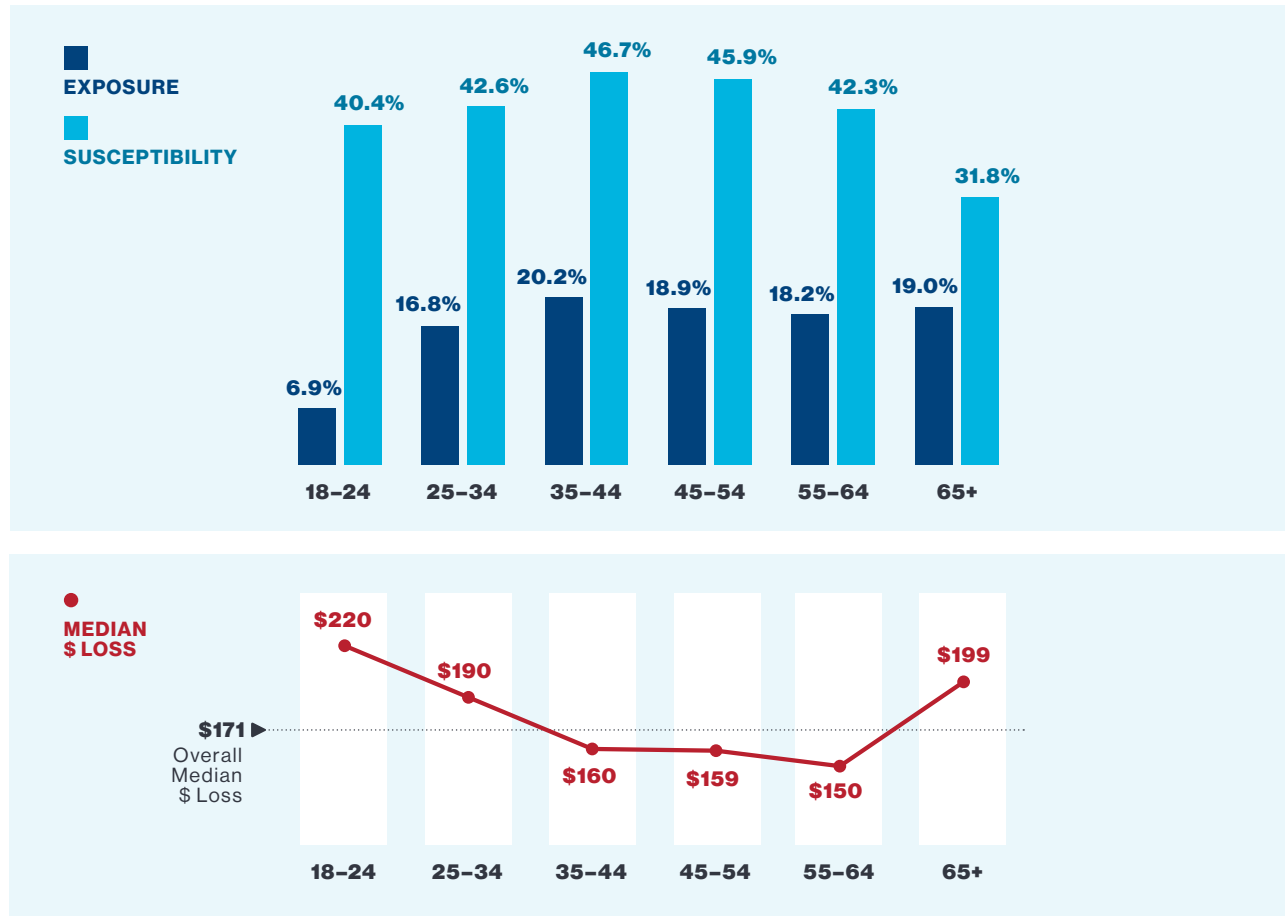


TABLE 2

Three riskiest scam types by age

	18-24	25-34	35-44	45-54	55-64	65+
1	Employment scams	Online purchase scams	Online purchase scams	Online purchase scams	Online purchase scams	Home improvement scams
2	Online purchase scams	Online purchase scams	Employment scams	Employment scams	Employment scams	Online purchase scams
3	Rental scams	Cryptocurrency scams	Cryptocurrency scams	Home improvement scams	Sweepstakes/lottery/prizes scams	Cryptocurrency scams

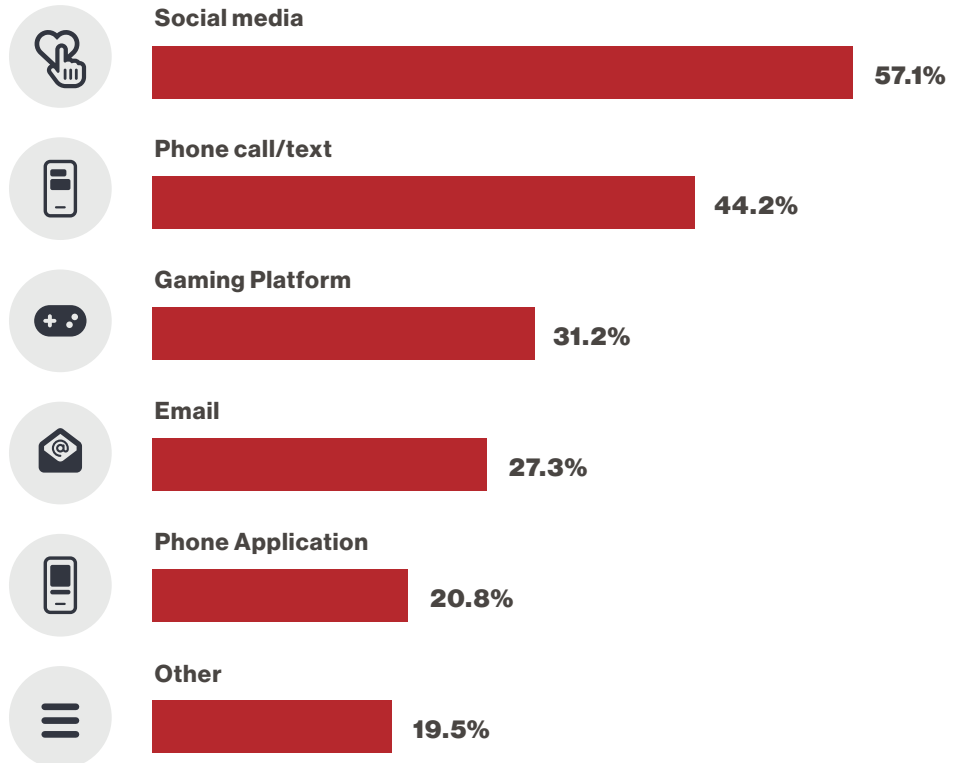
Scams Targeting Youth

BBB Scam Tracker does not collect information from people under the age of 18. However, we know younger people are being targeted. Of the 21.7% of survey respondents¹⁰ who reported having children between the ages of seven and 18 years, 11.1% said their children were targeted by scams. Respondents reported that their children were targeted via social media, phone call/text message, gaming platforms, email, and phone application (Figure 7). More research is needed to better understand how and where children are being targeted and how parents can protect them.

FIGURE 7

Reported method of contact for youth

Where were they targeted by a scam?



The totals do not add up to 100% because respondents were encouraged to choose all that applied.

¹⁰ A survey was distributed to those who submitted a scam report to BBB Scam Tracker in 2022; 4,100 respondents completed the survey.

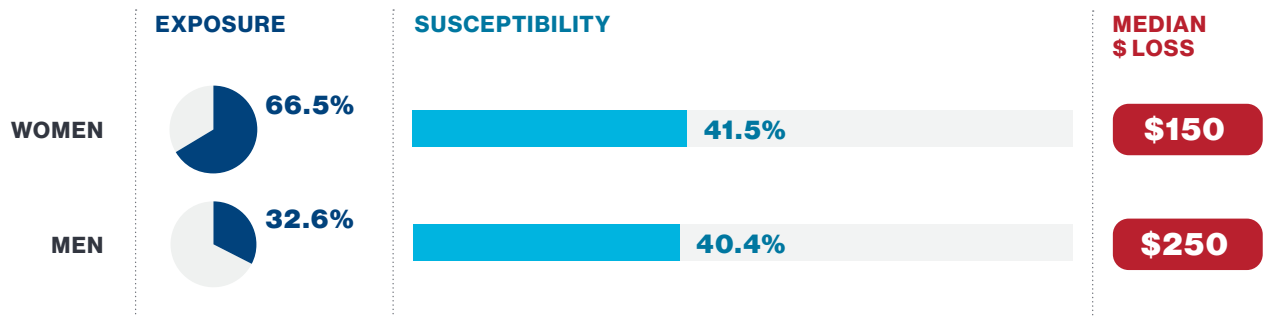
Gender

Similar to previous years, more than two-thirds of reports to BBB Scam Tracker in 2022 were submitted by women. Women reported being slightly more susceptible to losing money when exposed to a scam (41.5%) compared to men (40.4%) (Figure 8). The reported median dollar loss for women (\$150) was significantly lower than that of men (\$250). The reported median dollar loss for men rose 13.6% from \$220 in 2021 to \$250 in 2022.

Online purchase scams were the riskiest scam type reported by men and women (Table 3). This year, employment scams were the second riskiest scam type for men and women, with home improvement scams third riskiest for women, and cryptocurrency scams third riskiest for men.

FIGURE 8

Exposure, susceptibility, and median dollar loss by gender



The figures do not add up to 100% because some reported as non-binary; we don't have enough data to provide insights about susceptibility, median dollar loss, or the riskiest scams for non-binary people.

TABLE 3

Three riskiest scam types by gender

	WOMEN	MEN
1	Online purchase scams	
2	Employment scams	
3	Home improvement scams	Cryptocurrency scams

Scam contact and payment methods



The top three contact methods in 2022 that resulted in a reported monetary loss were website (31.5%), social media (18.7%), and email (17.3%) (Figure 9). Reports of scams being perpetrated via text message increased 39.6%, with 12.7% being targeted in 2022 compared to 9.1% being targeted in 2021. Those who reported losing money to scams perpetrated via text message also increased from 4.6% in 2021 to 4.9% in 2022.

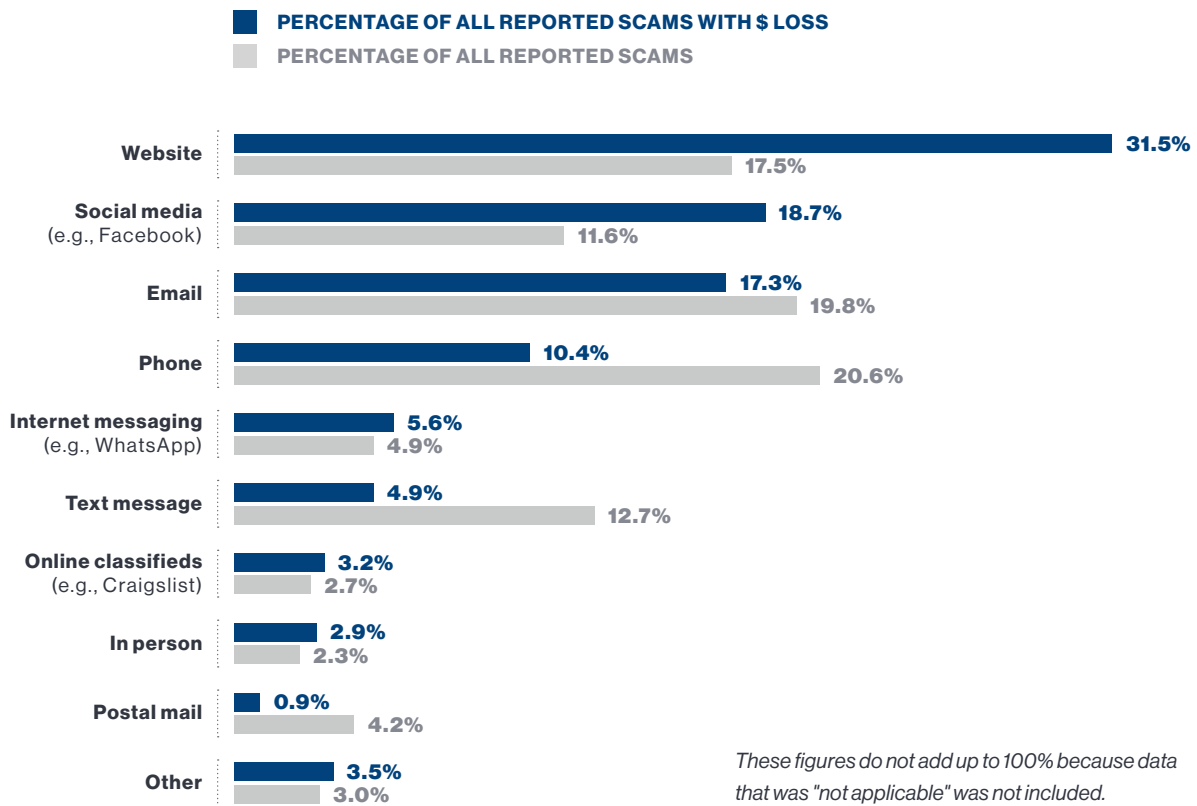
Scams perpetrated online were more likely to result in a reported median dollar loss than those perpetrated in person or via phone (Figure 10).

Figure 11 breaks out age range and contact method with a monetary loss. Those ages 65+ were more likely to report losing money than other age groups when contacted by phone or postal mail. People ages 35–54 were more likely to report losing money when targeted via website or social media. Those ages 25–44 were more likely to report losing money when contacted by text message.

Reports of scams being perpetrated via text message increased 39.6%, with 12.7% being targeted in 2022 compared to 9.1% being targeted in 2021.

FIGURE 9

Means of contact with a monetary loss compared to all reported scams

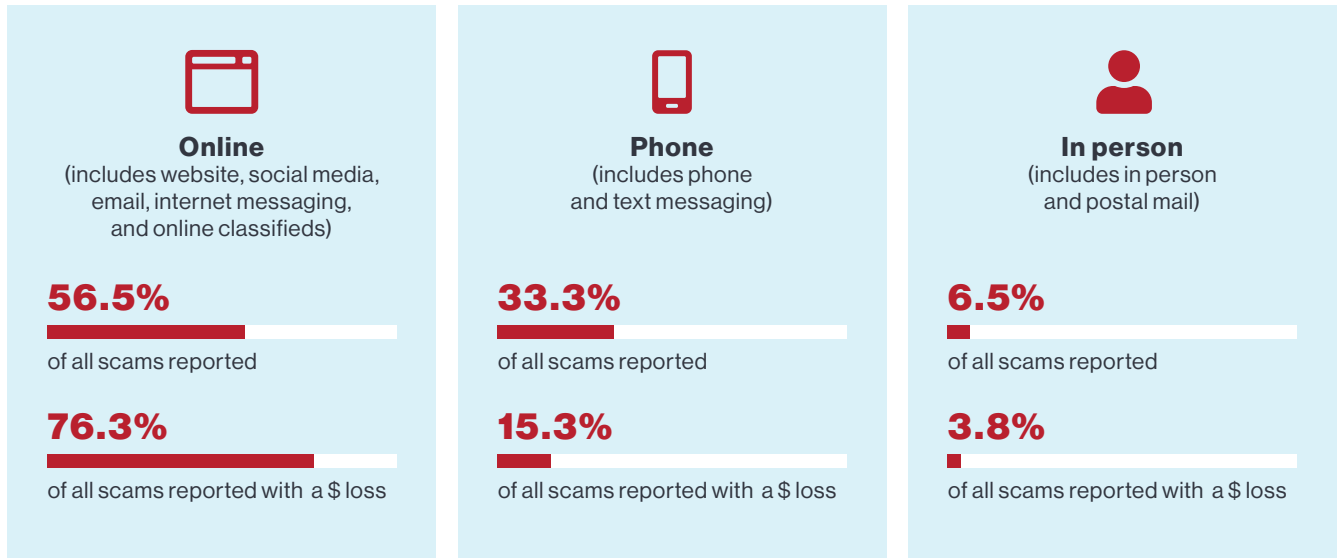


Susceptibility and monetary loss by means of contact

MEANS OF CONTACT	SUSCEPTIBILITY	MEDIAN \$ LOSS
Website	72.1%	\$100
Social media (e.g., Facebook)	64.8%	\$100
Email	35.0%	\$189
Phone	20.3%	\$550
Internet messaging (e.g., WhatsApp)	46.1%	\$500
Text message	15.5%	\$579
Online classifieds (e.g., Craigslist)	47.4%	\$200
In person	52.0%	\$715
Postal mail	8.5%	\$190
Other	47.2%	\$157

FIGURE 10

**All scams compared to scams with a reported monetary loss
by means of contact**



Note: Percentage of all scams and scams with a \$ loss do not add up to 100% because the "other" category was not included.

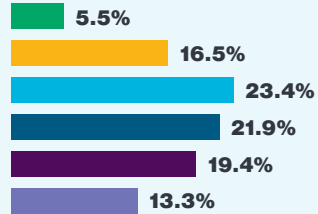
**Scams
perpetrated
online
were more
likely to
result in a
reported
median
dollar loss.**

FIGURE 11

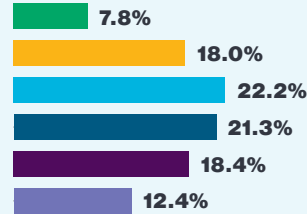
Means of contact that resulted in a monetary loss, by age

- 18-24
- 25-34
- 35-44
- 45-54
- 55-64
- 65+

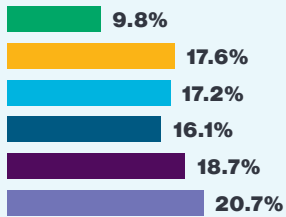
WEBSITE



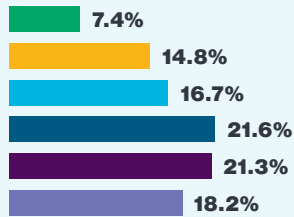
SOCIAL MEDIA



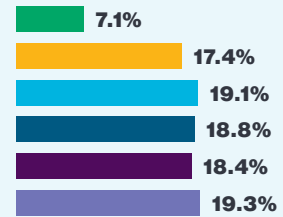
INTERNET MESSAGING
(e.g., WhatsApp)



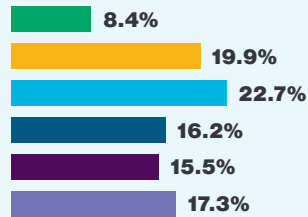
ONLINE CLASSIFIEDS
(e.g., Craigslist)



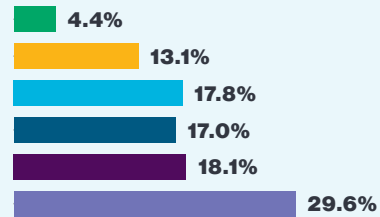
EMAIL



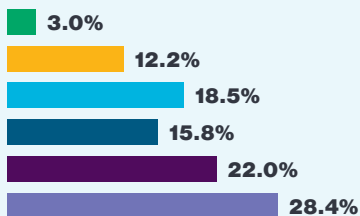
IN PERSON



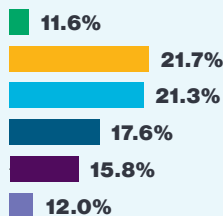
PHONE



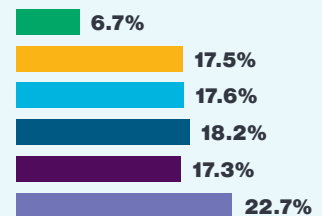
POSTAL MAIL



TEXT MESSAGE



OTHER



These figures do not add up to 100% due to rounding.

In 2022, credit cards (37.3%) remained the top reported payment method with a monetary loss (Figure 12), followed by online payment systems (25.3%) and bank account debit (13.1%) (Figure 12). The payment methods with the highest median dollar loss were wire transfer (\$2,700), check (\$1,277), and cryptocurrency (\$1,135).

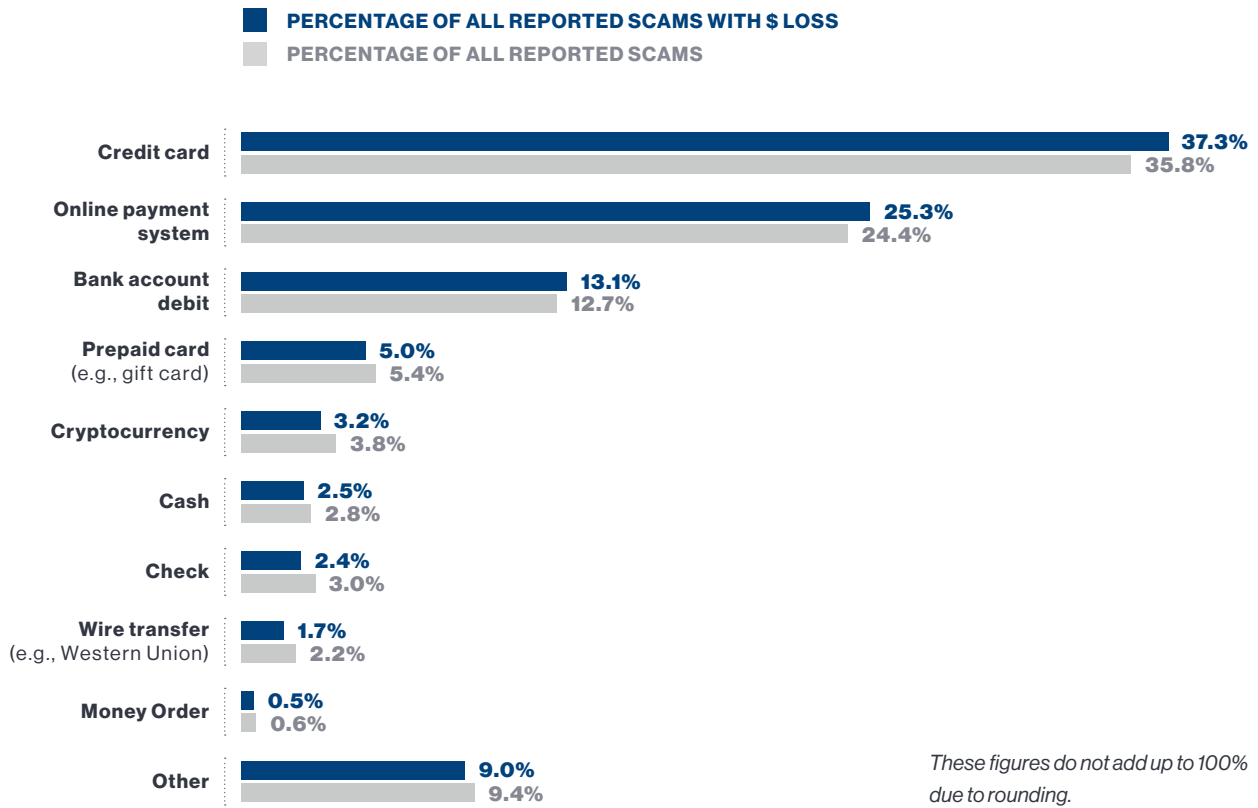
When broken out by age and payment method with a monetary loss (Figure 13), individuals ages 65+ were more likely to report paying via check and money order than other age groups. People ages 55+ were more likely to report paying via prepaid cards than other age groups. Those ages 35–44 were more likely to report paying by online payment system. And people ages 25–44 were more likely to report paying via cryptocurrency than other age groups.

This year, the *BBB Scam Tracker Risk Report* breaks out the most reported scam types by payment method (Table 4). Online purchase scams were the most reported scam type for several payment methods (credit card, online payment system, bank account debit, prepaid card, and wire transfer). Counterfeit product scams were the second most reported scam type for credit card, online payment system, and bank account debit. Home improvement scams were the most reported scam type associated with cash and check payment methods.

Credit cards remained the top reported payment method with a monetary loss while the payment method with the highest median dollar loss was wire transfer.

FIGURE 12

Payment method with a monetary loss compared to all reported scams



Monetary loss by payment method

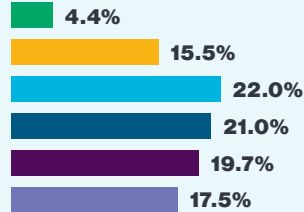
PAYMENT METHOD	MEDIAN \$ LOSS
Credit card	\$89
Online payment system	\$239
Bank account debit	\$108
Prepaid card (e.g., gift card)	\$650
Cryptocurrency	\$1,135
Cash	\$723
Check	\$1,277
Wire transfer (e.g., Western Union)	\$2,700
Money order	\$1,045
Other	\$532

FIGURE 13

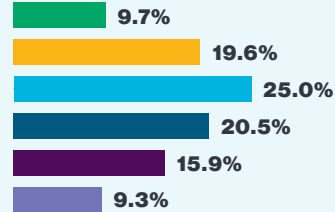
Payment method that resulted in a monetary loss, by age

- 18-24
- 25-34
- 35-44
- 45-54
- 55-64
- 65+

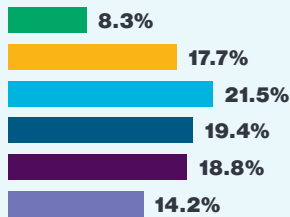
CREDIT CARD



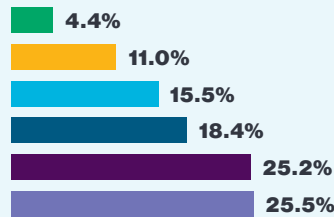
ONLINE PAYMENT SYSTEM



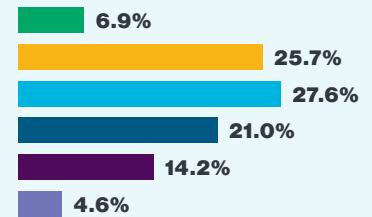
BANK ACCOUNT DEBIT



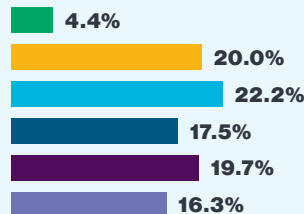
PREPAID CARD



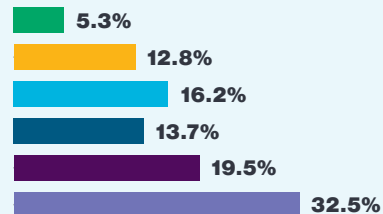
CRYPTOCURRENCY



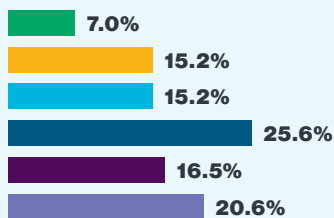
CASH



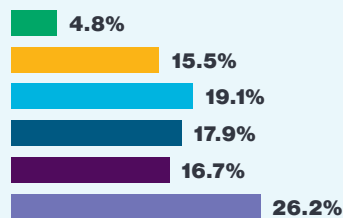
CHECK



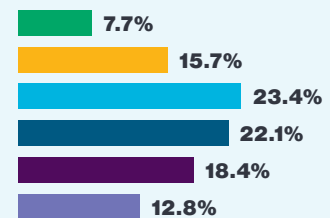
**WIRE TRANSFER
(e.g. Western Union)**



MONEY ORDER



OTHER



These figures do not add up to 100% due to rounding.

TABLE 4

Most reported scam type by payment method

CREDIT CARD	ONLINE PAYMENT SYSTEM	BANK ACCOUNT DEBIT
#1 Online purchase	#1 Online purchase	#1 Online purchase
#2 Counterfeit product	#2 Counterfeit product	#2 Counterfeit product
#3 Credit card	#3 Employment	#3 Phishing
PREPAID CARD	CRYPTOCURRENCY	CHECK
#1 Online purchase	#1 Cryptocurrency	#1 Home improvement
#2 Government grant	#2 Investment	#2 Employment
#3 Sweepstakes/lottery/prizes	#3 Online purchase	#3 Tech support
WIRE TRANSFER	MONEY ORDER	CASH
#1 Online purchase	#1 Advance fee loan	#1 Home improvement
#2 Travel/vacation/timeshare	#2 Online purchase	#2 Online purchase
#3 Advance fee loan	#3 Sweepstakes/lottery/prizes	#3 Counterfeit product

Impact on specific audiences



Canadian consumers

In 2022, Canadian consumers submitted 1,297 scam reports to BBB Scam Tracker (3.2% of total reports). Overall reported median dollar loss in 2022 was \$300 CAD, a 20% increase from \$250 CAD in 2021. The percentage of those who reported losing money after being targeted by a scam (susceptibility) increased 4.0%, from 45.1% in 2021 to 46.9% in 2022.

The top three riskiest scams reported in Canada shifted slightly in 2022, with home improvement scams rising to the number one riskiest scam type from fourth riskiest in 2021 (Table 5). Reports of home improvement scams increased 51.2%, from 4.1% of all scams reported in Canada in 2021 to 6.2% in 2022; reported median dollar loss for home improvement scams rose 187.4%, from \$661 CAD in 2021 to \$1,900 CAD. Susceptibility to home improvement scams also increased 25.3%, up from 62.9% in 2021 to 78.8% in 2022.

Cryptocurrency scams, the riskiest scam type in Canada in 2021, fell to number two on the list in 2022. The number of reported cryptocurrency scams (exposure) dropped slightly from 4.7% in 2021 to 4.6% in 2022; susceptibility to this scam type dropped from 69.6% in 2021 to 62.7% in 2022. Advance fee loan scams, the second riskiest scam in 2021, dropped to the third riskiest in 2022. More information about scams reported by Canadians can be found in the [2022 BBB Scam Tracker Canadian Risk Report](#).

TABLE 5

Top 3 riskiest scams reported in Canada

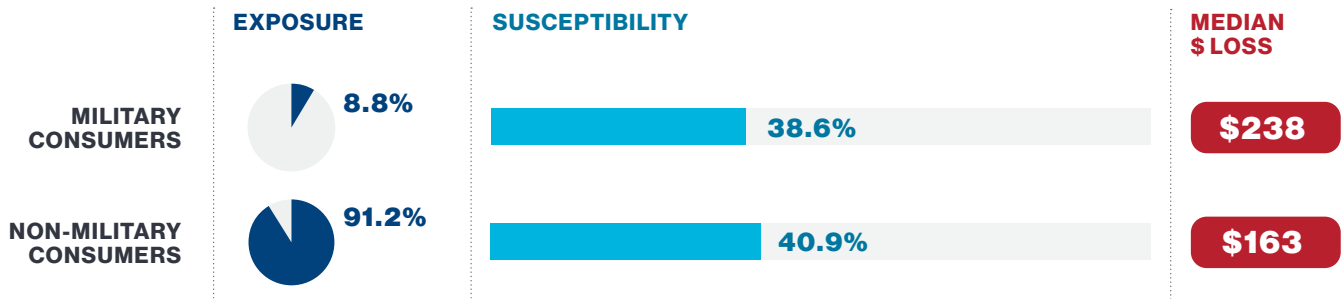
RANK	SCAM TYPE	BBB RISK INDEX	EXPOSURE	SUSCEPTIBILITY	MEDIAN \$ LOSS
1	Home improvement	307.6	6.2%	78.8%	\$1,900 CAD
2	Cryptocurrency	190.2	4.6%	62.7%	\$2,000 CAD
3	Advance fee loan	185.6	6.8%	59.1%	\$1,388 CAD

Military families and veterans

Individuals who self-identified as being active-duty military personnel, military spouses, or veterans submitted 8.8% of reports to BBB Scam Tracker in 2022. Military consumers reported significantly higher median financial losses (\$238) than non-military consumers (\$163) (Figure 14). The percentage of military consumers who reported losing money when targeted by scams (susceptibility) dropped from 44.1% in 2021 to 38.6% in 2022.

FIGURE 14

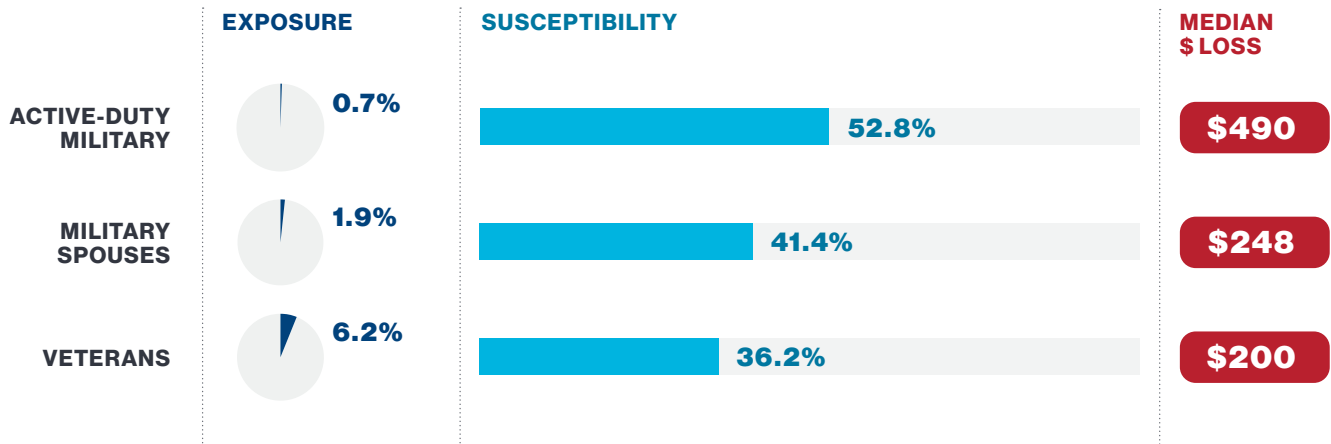
Exposure, susceptibility, and median \$ loss reported by military consumers compared with non-military consumers



In 2022, the percentage of those who reported losing money when targeted by a scam (susceptibility) dropped for active-duty military, military spouses, and veterans. Active-duty military reported losing significantly more money (\$490) than did military spouses (\$248) and veterans (\$200) (Figure 15). The median dollar loss for active-duty military rose 63.3%, from \$300 in 2021 to \$490 in 2022. The median dollar loss for military spouses also rose 45.9%, from \$170 in 2021 to \$248 in 2022. The median dollar loss for veterans, on the other hand, dropped from \$220 in 2021 to \$200 in 2022.

FIGURE 15

Exposure, susceptibility, and median \$ loss reported by military families and veterans



The BBB Risk Index was applied to identify the three riskiest scams for military spouses and veterans (Table 6).¹¹ Online purchase scams were again the riskiest for both military spouses and veterans in 2022. Employment scams remained second riskiest for military spouses but dropped to third riskiest for veterans. Home improvement scams were second riskiest for veterans.

TABLE 6

Three riskiest scam types for military spouses and veterans compared with non-military consumers

	MILITARY SPOUSES	VETERANS	NON-MILITARY
1	Online purchase scams		
2	Employment scams	Home improvement scams	Employment scams
3	Tech support scams	Employment scams	Cryptocurrency scams

¹¹ Reports submitted by active-duty service members were spread out among the 30 scam types, with only online purchase scams having a significant number of scam records.

Students

Individuals who self-identified as students submitted 6.3% of reports to BBB Scam Tracker in 2022. Students were slightly more likely to lose money when targeted by a scam than were non-students (Figure 16). In 2022, students reported a significantly higher median dollar loss (\$205) than did non-students (\$166). Table 7 includes the riskiest scams for students. Employment scams rose to the riskiest scam type reported by students in 2022, with online purchase and cryptocurrency scams ranking second and third, respectively.

FIGURE 16

Susceptibility and median \$ loss reported by students versus non-students

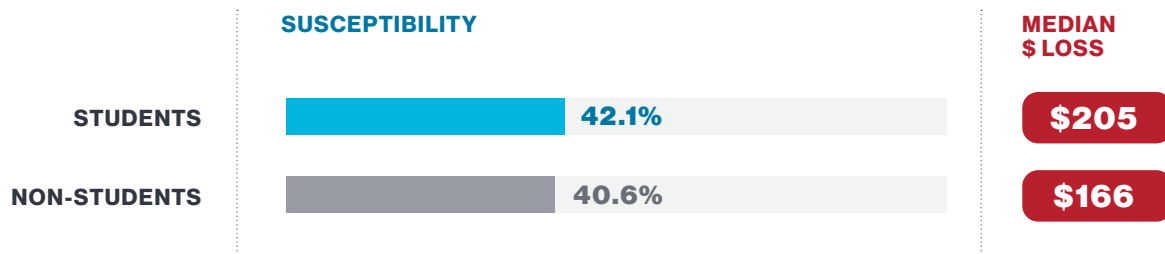


TABLE 7

Three riskiest scam types reported by students compared with non-students

	STUDENTS	NON-STUDENTS
1	Employment scams	Online purchase scams
2	Online purchase scams	Employment scams
3	Cryptocurrency scams	Home improvement scams

Impersonated organizations and individuals

According to survey research by BBB Institute, “impersonation” was reported as the most common tactic used to perpetrate scams.¹² By pretending to be well-known companies, government agencies, and organizations, scammers seek to co-opt the trust and authority of these organizations. In some cases, scammers impersonate real-life individuals.

For the second year in a row, Amazon appeared at the top of the list of most-impersonated organizations reported to BBB Scam Tracker (Table 8). Geek Squad broke onto the list this year, becoming the second most-impersonated organization. Publishers Clearing House remained the third most-impersonated organization. A significant shift is the addition of the U.S. Postal Service as the fourth most-impersonated organization, with the Social Security Administration falling from the second-most impersonated organization in 2021 to number 17 this year.

According to reports submitted to BBB Scam Tracker, scammers continued to impersonate sweepstakes winners Manuel Franco (308 reports) and Scott Godfrey (47 reports); people also reported scams in which the perpetrator impersonated Mega Millions (47 reports). The Indiana Department of Workforce Development appeared on the list in 2022 because of a scam that claimed the target was owed unclaimed money from the state.¹³ Other impersonated organizations farther down on the list include Center Point Energy (utility industry), Better Business Bureau, Spectrum (cable/internet provider), Lending Club (financial services), eBay, and Bank of America.

TABLE 8

Top 15 organizations, individuals used for impersonation

Rank	Organization/individual name	No. of reports
1	Amazon	763
2	Geek Squad	492
3	Publishers Clearing House	430
4	U.S. Postal Service	413
5	Norton	384
6	PayPal	378
7	Manuel Franco	308
8	Medicare	273
9	Walmart	139
10	Microsoft	126
11	Indiana Department of Workforce Development	123
12	McAfee	121
13	Facebook	102
14	Advance America	97
15	Cash App	88

¹² *Start With Trust® Online: 2022 Online Scams Report.*

¹³ *BBB Scam Alert: Indiana Department of Workforce Development fake text scam.*



Carrot versus stick: Analyzing the impact of scam tactics

Scammers use a wide variety of tactics to perpetrate their scams, and some are more effective than others. Some tactics use the promise of some sort of opportunity (“carrot”) to encourage the target to continue the engagement. Examples of the carrot approach include the opportunity to make quick money through low-risk investments or too-good-to-be-true job offers. Other tactics utilize some sort of threat (“stick”) or negative situation to manipulate the targets, such as jail time for back taxes or news that a loved one is in trouble and needs help. This year’s report breaks out the various scam types into three categories: carrot method, stick method, and other (scam types that do not easily fit into a category).

Using the BBB Risk Index, we found that people were much more likely to lose money to scams perpetrated via a carrot method (51.1%) compared to a stick method (17.6%) (Figure 17). However, when people reported losing money to scams that were perpetrated with a stick method, they reported losing more than twice the amount of money (\$349) than those who reported losing money to carrot-type scams (\$150).

Carrot-type tactics were more likely to use social media or websites to target people. Stick-type tactics were more likely to use phone or postal mail as the contact method (Figure 18).

FIGURE 17 "Carrot" versus "stick" tactics by median dollar loss and susceptibility

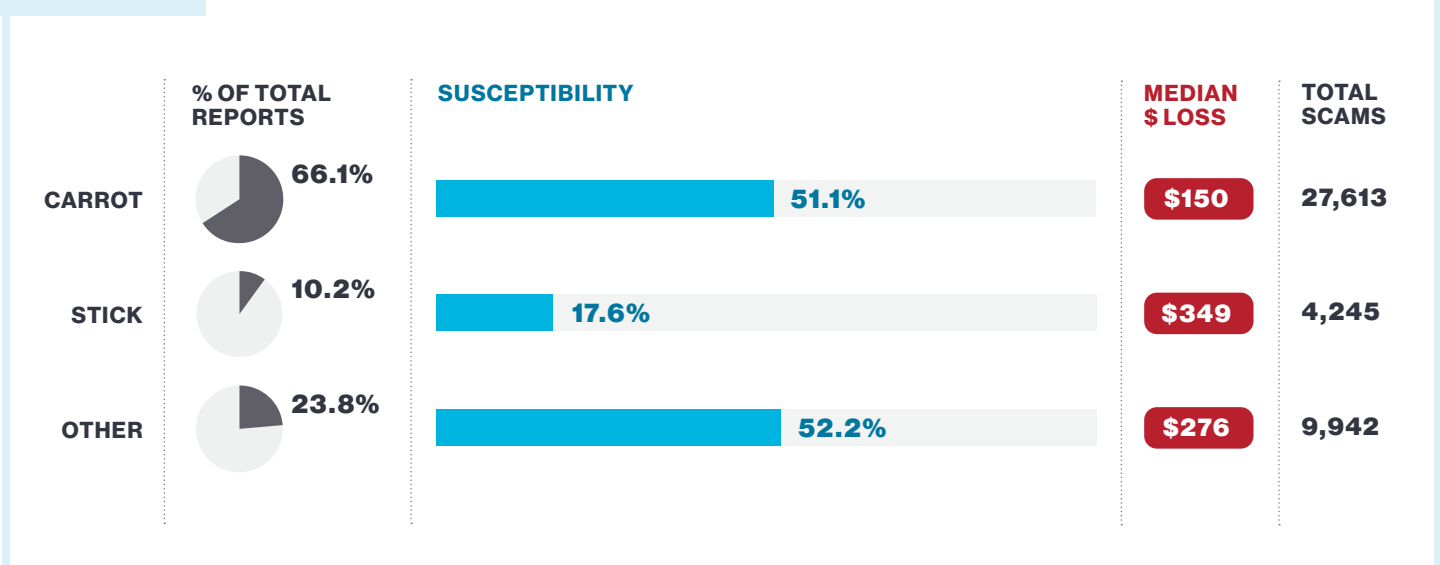
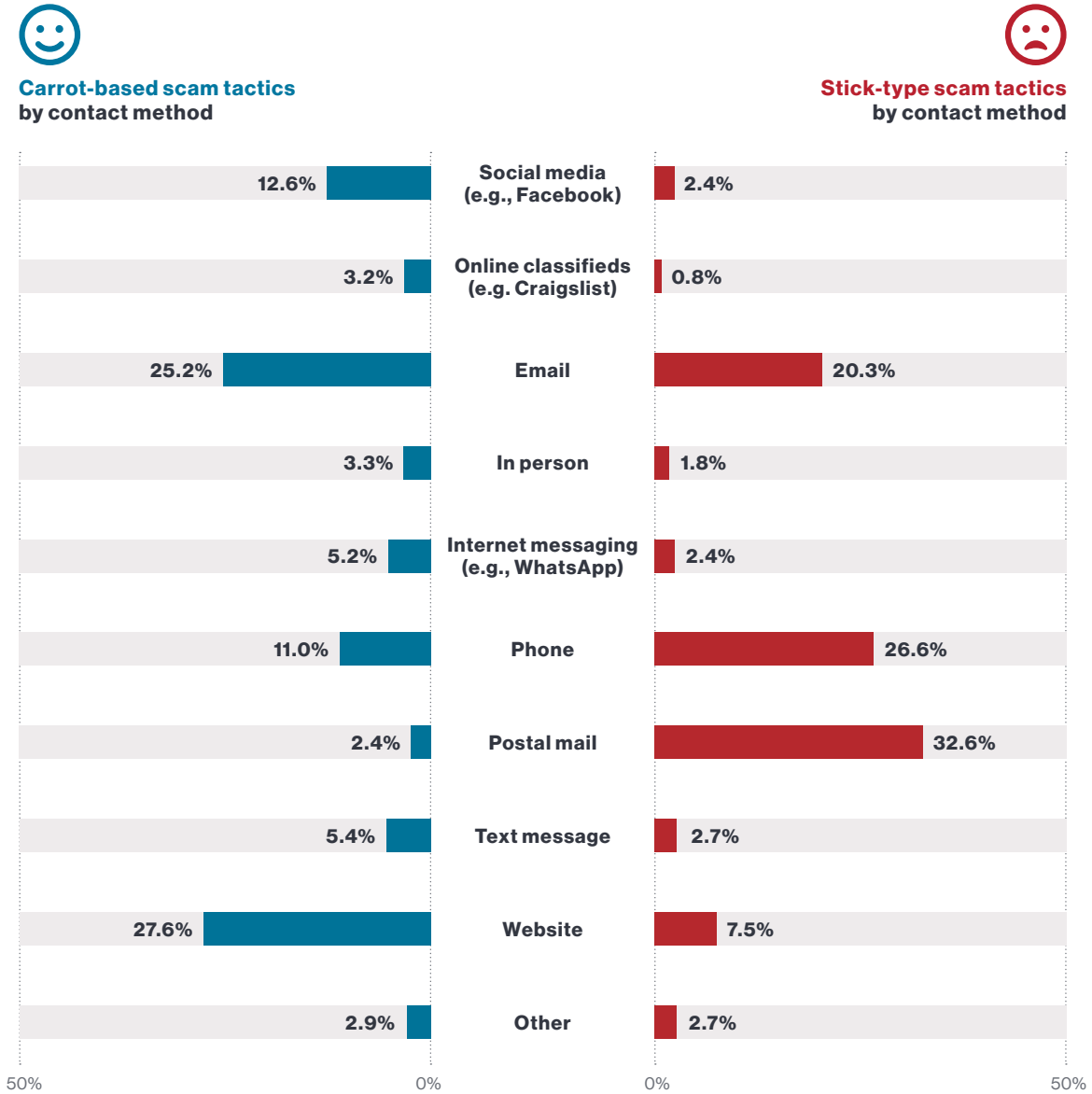


FIGURE 18

Contact method broken out by carrot or stick method



These figures do not add up to 100% because data that was "not applicable" was not included.



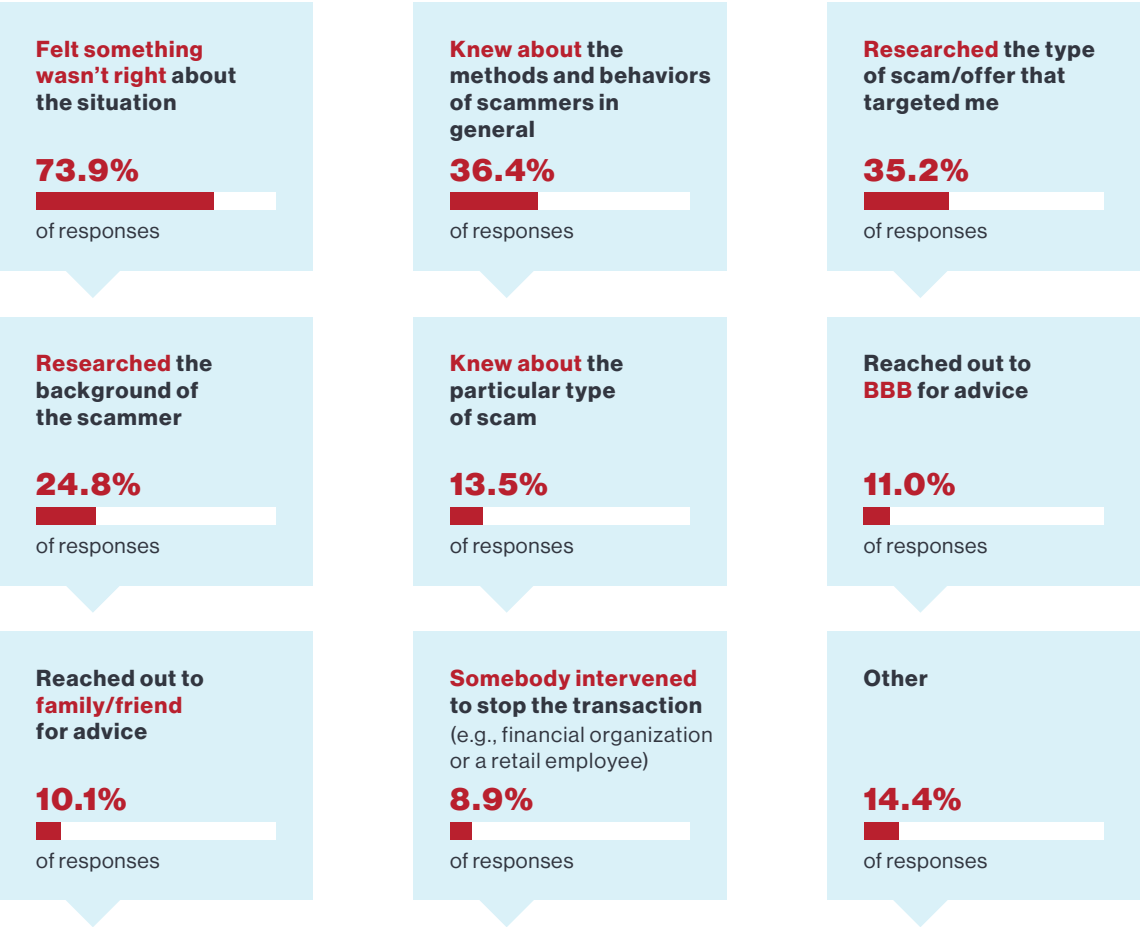
Self-reported cues and behaviors that helped people avoid losing money

Factors people say helped them avoid losing money

Our team asked survey respondents again this year what they believe helped them avoid losing money when targeted by a scam (Figure 19). The same percentage of respondents in 2021 and 2022 (73.9%) said they avoided losing money to a scam because they “felt something wasn’t right about the situation.” Prior knowledge about scams appears to be protective, with 36.4% of survey respondents reporting they avoided losing money because they knew about the methods/behaviors of scammers in general and 35.2% reporting that they researched the type of scam/offer for which they were targeted.

FIGURE 19

Cues/behaviors survey respondents said helped them avoid losing money to a scam



Respondents were encouraged to choose multiple options.

Behaviors, actions that may impact susceptibility

When survey respondents were asked to self-report how they handle certain situations, those who reported being less likely to panic during a stressful situation were less likely to report losing money to scams than those who said they were more likely to panic. Similarly, those who reported being more cynical about new situations or persuasive offers were less likely to report losing money than those who said they were less likely to be cynical. Those who reported experiencing significant financial distress during the past year were more likely to report losing money to scams compared to those who reported not experiencing financial distress.

Repeat victims

We asked survey respondents to tell us how many times they have lost money to a scam. According to our findings, 39.7% reported losing money to fraud once, 15.1% reported losing money twice, 4.9% reported losing money three times, 1.6% lost money four times, and 1.9% lost money five or more times (Figure 20).

People who reported losing money three or more times were more likely to say they (1) panic during stressful situations; (2) felt financial stress during the past year; and (3) are more isolated (live alone or have few friends) than those who reported losing money zero to two times.

People who reported losing money three or more times were more likely to say they:

panic during stressful situations;

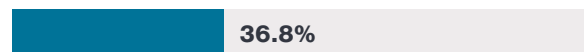
felt financial stress during the past year; and

are more isolated (live alone or have few friends) than those who reported losing money zero to two times.

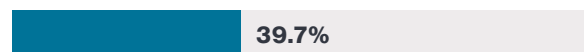
FIGURE 20

Number of times a person reported losing money to a scam

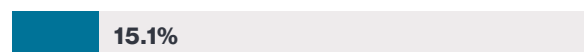
I have not lost money to a scam



One time



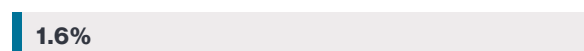
Two times



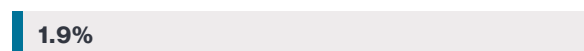
Three times



Four times



Five or more times



10 GENERAL TIPS for avoiding a scam

1

Never send money to someone you have never met face-to-face.



2

Don't click on links or open attachments in unsolicited email or text messages.

3

Don't believe everything you see or read. Scammers are great at mimicking official seals, fonts, and other details. Just because a website or email looks official does not mean it is. Even Caller ID can be faked.

4

Take precautions when making online purchases.

Don't shop on price alone. Scammers offer hard-to-find products at great prices.

Don't buy online unless the transaction is secure. Make sure the website has "https" in the URL (the extra "s" is for "secure") and a small lock icon on the address bar. Even then, the site could be shady. Research the company first at BBB.org.

Avoid making quick purchases while browsing social media. Scammers advertise websites that offer great deals, but either don't deliver the product at all or deliver counterfeit products.

Do more research on those products you found via online search.

5

Be extremely cautious when dealing with anyone you've met online.



6

Never share personally identifiable information with someone who has contacted you unsolicited.

7

Don't be pressured to act immediately.



8

Use secure, traceable transactions when making payments for goods, services, taxes, and debts. (Gift cards can't be traced!)

9

Whenever possible, work with businesses that have proper identification, licensing, and insurance.

10

Be cautious about what you share on social media.



Learn more at [BBB.org/AvoidScams](https://www.bbb.org/avoidscams)

BBB Institute for Marketplace Trust



The *BBB Scam Tracker Risk Report* is published each year by the BBB Institute for Marketplace Trust (BBB Institute), the charitable arm of the Better Business Bureau. Our mission is to educate and protect consumers, establish best practices for businesses, and solve complex marketplace problems. Our consumer educational programs, which include a wide array of resources on fraud prevention and education, are delivered digitally and in person through the network of BBBs serving communities across the United States and Canada. Research is an integral component of our work, enabling us to incorporate the latest scammer trends in our consumer education resources and initiatives. You can find more information about BBB Institute and its programs at [BBBMarketplaceTrust.org](https://www.BBBMarketplaceTrust.org).



BBB Institute research

BBB® 2022 Online Scams Report: Start With Trust® Online

This report spotlights all scam types that are perpetrated online to provide new information about which tactics have the biggest impact on consumers and to identify tips that can help consumers protect themselves from online fraud. The report also spotlights impersonation scams and online purchase (shopping) scams.

Download at [BBBMarketplaceTrust.org/OnlineScams](https://www.BBBMarketplaceTrust.org/OnlineScams).

All BBB Institute research can be found on our website at [BBBMarketplaceTrust.org](https://www.BBBMarketplaceTrust.org).

Thank you to our sponsors

BBB Institute would like to recognize our funding partners for making BBB Institute's research and programs possible.



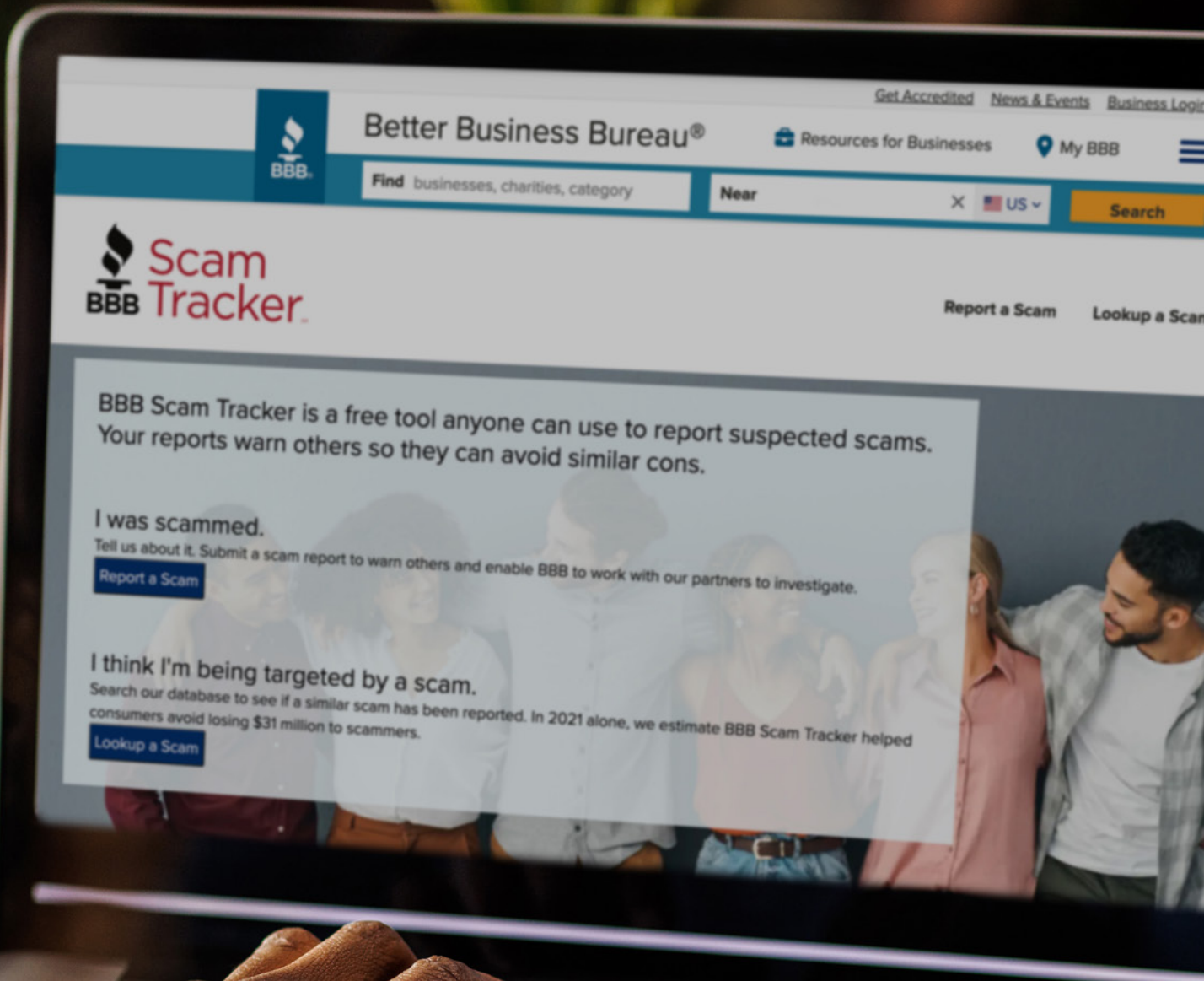


BBB launches new and improved BBB Scam Tracker

In 2022, the BBB Institute for Marketplace Trust partnered with Amazon and Capital One to build a new and improved BBB Scam Tracker platform ([BBB.org/ScamTracker](https://www.bbb.org/ScamTracker)) with the goal of helping people learn about scams, report them, and avoid losing money and/or personal information. The updated website makes it easier for people to identify scams and report them while arming partners with more robust data for their fraud-fighting efforts.

Improved features of the new BBB Scam Tracker include:

- **A new guided questionnaire** that makes it quick and easy to report a scam
- **An upgraded mobile experience**, enabling people to report scams from anywhere at any time
- **An upgraded search function** that enables consumers to determine whether they're being targeted by searching reported scams (by URL, email address, phone number, and more)
- **Expanded search engine optimization (SEO)** abilities to enable those searching for specific scams on other platforms to find BBB Scam Tracker reports
- **The ability to review and edit reports** before final submission
- **The ability to share scam reports** via social media, email, and direct links
- Application programming interface (API) and system-generated report functionality that enables **scam data sharing with fraud-fighting partners**
- **Updated back-end technology** to improve the speed of the tool and allow for future enhancements



Check out the new
BBB Scam Tracker platform today.

BBB.org/ScamTracker

APPENDIX A: Glossary of scam types targeting consumers

Scams reported to BBB Scam Tracker this year are classified into 28 consumer scams. These classifications represent common scams reported to BBB and are informed by type classifications used by the Federal Trade Commission and the Internet Crime Complaint Center of the Federal Bureau of Investigation. Although scams vary widely, about 95% of all scams reported to BBB Scam Tracker can be classified into one of these general types. You can find more information about some of these scam types at <https://www.bbb.org/all/scamtips>.

ADVANCE FEE LOAN	A loan is guaranteed, but once the victim pays up-front charges such as taxes or a "processing fee," the loan never materializes. Read our advance fee loan scam prevention tips.
CHARITY	Charity scams use deception to get money from individuals who believe they are making donations to legitimate charities. This is particularly common in the wake of a natural disaster or other tragedy. Read our charity scam prevention tips.
COUNTERFEIT PRODUCT	Counterfeit goods mimic original merchandise, right down to the trademarked logo; however, they are typically of inferior quality. This can result in a life-threatening health or safety hazard when the counterfeit item is medication, a supplement, or an auto part. Read our counterfeit product scam prevention tips.
COVID-19	Scammers seek to make money off the COVID-19 pandemic in some manner, such as by offering nonexistent or inferior products such as masks or cleaning supplies, or any other scam type that uses the COVID-19 situation to steal money or personal information.
CREDIT CARD	Scammers impersonate a bank or other credit card issuer, pretending to verify account details to get a target's credit card or banking information. Read our credit card scam prevention tips.
CREDIT REPAIR/DEBT RELIEF	Scammers posing as legitimate service providers collect payment in advance, with promises of debt relief and repaired credit, but provide little or nothing in return. Read our credit repair/debt relief scam prevention tips.
CRYPTOCURRENCY	These scams involve the purchase, trade, or storage of digital assets known as cryptocurrencies. The situations often involve fraudulent Initial Coin Offerings (ICOs), a type of fundraising mechanism in which a company issues its own cryptocurrency to raise capital. Investors pay money or trade their own digital assets even though the scammer has no intention of building a company. Cryptocurrency scams also involve scenarios in which investors store their cryptocurrencies with fraudulent exchanges. Read the BBB study on crypto scams.
DEBT COLLECTION	Phony debt collectors harass their targets to get them to pay debts they don't owe. Read our debt collection scam prevention tips.
EMPLOYMENT	Job applicants are led to believe they are applying for or have just been hired for a promising new job when, instead, they have given personal information via a fake application or money to scammers for "training" or "equipment." In another variation, the victim may be "overpaid" with a fake check and asked to wire back the difference. Read our employment scam prevention tips.
FAKE CHECK/MONEY ORDER	The victim deposits a phony check and then returns a portion by wire transfer to the scammer. The stories vary, but the victim is often told they are refunding an "accidental" overpayment. Scammers count on the fact that banks make funds available within days of a deposit but can take weeks to detect a fake check. Read BBB's Fake Check study.

APPENDIX A: Glossary of scam types targeting consumers

FAMILY/FRIEND EMERGENCY	This scheme involves the impersonation of a friend or family member experiencing a fabricated urgent or dire situation. The "loved one" invariably pleads for money to be sent immediately. Aided by personal details typically found on social media, imposters can offer very plausible stories to convince their targets. <u>Read our family/friend emergency scam prevention tips.</u>
FOREIGN MONEY EXCHANGE	The target receives an email from a scammer pretending to be a foreign government official, member of royalty, or a business owner offering a huge sum of money to help get funds out of the scammer's country. The victim fronts costs for the transfer, believing they will be repaid. <u>Read our foreign money exchange scam prevention tips.</u>
GOVERNMENT GRANT	Individuals are enticed by promises of free, guaranteed government grants requiring an up-front "processing fee." Other fees follow, but the promised grant never materializes. <u>Read our government grant scam prevention tips.</u>
HEALTHCARE, MEDICAID, AND MEDICARE	The scammer seeks to obtain the insured's health insurance, Medicaid, or Medicare information to submit fraudulent medical charges or for purposes of identity theft. <u>Read our healthcare scam prevention tips.</u>
HOME IMPROVEMENT	Door-to-door solicitors offer quick, low-cost repairs and then either take payment without returning, do shoddy work, or "find" issues that dramatically raise the price. These types of schemes also often occur after a major storm or natural disaster. <u>Read our home improvement scam prevention tips.</u>
IDENTITY THEFT	Identity thieves use a victim's personal information (e.g., Social Security number, bank account information, and credit card numbers) to pose as that individual for their own gain. Using the target's identity, the thief may open a credit account, drain an existing account, file tax returns, or obtain medical coverage. <u>Read our identity theft prevention tips.</u>
INVESTMENT	These scams take many forms, but all prey on the desire to make money without much risk or initial funding. "Investors" are lured with false information and promises of large returns with little or no risk. <u>Read our investment scam prevention tips.</u>
MOVING	These schemes involve rogue moving services offering discounted pricing to move household items. The alleged movers may steal the items or hold them hostage from the customer, demanding additional funds to deliver them to the new location. <u>Read our moving scam prevention tips.</u>
ONLINE PURCHASE	These scams typically involve the purchase of products and/or services where the transaction occurs via a website or other online means. Scammers use technology to offer attractive deals, but once the payment is made, no product or service is delivered. In some cases, fraudsters send low-quality or counterfeit products. <u>Read our online purchase scam prevention tips.</u>
PHISHING/SOCIAL ENGINEERING	In these schemes, scammers impersonating a trustworthy entity, such as a bank or mortgage company, employ communications to mislead recipients into providing personal information that the scammer will use to gain access to bank accounts or steal a recipient's identity. This type of scheme can also happen within the workplace as an email coming from the CEO, accounting department, or other member of management seeking personal information. <u>Read our phishing scam prevention tips.</u>
RENTAL	Phony ads are placed for rental properties that ask for up-front payments. Victims later discover the property doesn't exist or is owned by someone else. <u>Read our rental scam prevention tips.</u>
ROMANCE	An individual believing he/she is in a romantic relationship agrees to send money, personal and financial information, or items of value to the perpetrator. <u>Read our romance scam prevention tips.</u>

APPENDIX A: Glossary of scam types targeting consumers

SCHOLARSHIP	Victims, often students struggling with tuition costs, are promised government scholarship money, but the up-front “fees” never produce those much-needed funds. Sometimes a fake check does arrive, and the student is asked to wire back a portion for taxes or other charges. Read our scholarship scam prevention tips.
SWEEPSTAKES, LOTTERY, AND PRIZES	Victims are tricked into thinking they have won a prize or lottery jackpot but must pay up-front fees to receive the winnings, which never materialize. Sometimes this con involves a fake check and a request to return a portion of the funds to cover fees. Read our sweepstakes/lottery/prize scam prevention tips.
TAX COLLECTION	Imposters pose as Internal Revenue Service representatives in the United States or Canada Revenue Agency representatives in Canada to coerce the target into either paying back taxes or sharing personal information. Read our tax collection scam prevention tips.
TECH SUPPORT	Tech support scams start with a call or pop-up warning that alerts the target of a computer bug or other problem. Scammers posing as tech support employees from well-known tech companies hassle victims into paying for “support.” If the victim allows remote access to their device, malware may be installed. Read our tech support scam prevention tips.
TRAVEL/VACATION/ TIMESHARE	Con artists post listings for properties that are not for rent, do not exist, or are significantly different from what’s pictured. In another variation, scammers claim to specialize in timeshare resales and promise they have buyers ready to purchase. Read our travel scam prevention tips.
UTILITY	Imposters act as water, electric, and gas company representatives to take money or personal information. They frequently threaten residents and business owners with deactivation of service unless they pay immediately. In another form, a “representative” may come to the door to perform “repairs” or an “energy audit” with the intent of stealing valuables. Read our utility scam prevention tips.

APPENDIX B: Scam type data table, consumer scams

SCAM TYPE	RISK INDEX	EXPOSURE	SUSCEPTIBILITY	MEDIAN \$ LOSS
Advance fee loan	32.8	1.9%	36.7%	\$ 800
Charity	1.0	0.6%	20.9%	\$ 150
Counterfeit product	11.2	2.9%	65.1%	\$ 100
COVID-19	0.5	0.4%	17.7%	\$ 134
Credit card	4.2	1.8%	36.2%	\$ 112
Credit repair/debt relief	18.5	1.1%	33.9%	\$ 870
Cryptocurrency	67.3	1.7%	60.5%	\$ 1,100
Debt collection	4.6	2.6%	7.6%	\$ 400
Employment	127.6	9.6%	15.1%	\$ 1,500
Fake check/money order	16.5	1.8%	16.4%	\$ 970
Family/friend emergency	2.7	0.3%	34.9%	\$ 494
Foreign money exchange	1.1	0.2%	21.7%	\$ 560
Government grant	20.8	1.6%	22.3%	\$ 1,000
Healthcare/Medicaid/Medicare	3.0	1.6%	9.7%	\$ 334
Home improvement	67.1	1.4%	55.3%	\$ 1,500
Identity theft	4.2	1.4%	24.1%	\$ 205
Investment	28.3	0.7%	49.0%	\$ 1,369
Moving	10.9	0.4%	66.9%	\$ 750
Online purchase	137.9	31.9%	74.0%	\$ 100
Phishing/social engineering	19.3	11.7%	10.6%	\$ 267
Rental	18.4	0.9%	52.8%	\$ 642
Romance	21.6	1.6%	16.1%	\$ 1,411
Scholarship	.03	.03%	9.1%	\$ 191
Sweepstakes/lottery/prizes	5.4	5.4%	14.4%	\$ 120
Tax collection	2.0	0.2%	13.0%	\$ 1,375
Tech support	18.6	2.6%	25.2%	\$ 490
Travel/vacation/timeshare	17.2	1.0%	49.3%	\$ 602
Utility	3.8	1.3%	15.8%	\$ 327
Other	42.3	6.2%	40.3%	\$ 290

APPENDIX C: Top 10 consumer scam types by overall risk, exposure, susceptibility, and median dollar loss

	BY RISK INDEX	BY EXPOSURE	BY SUSCEPTIBILITY	BY MEDIAN \$ LOSS
1	Online purchase	Online purchase	Online purchase	Employment and Home improvement
2	Employment	Phishing/social engineering	Moving	Romance
3	Cryptocurrency	Employment	Counterfeit product	Tax collection
4	Home improvement	Sweepstakes/lottery/prizes	Cryptocurrency	Investment
5	Advance fee loan	Counterfeit product	Home improvement	Cryptocurrency
6	Investment	Tech support	Rental	Government grant
7	Romance	Debt collection	Travel/vacation/timeshare	Fake check/money order
8	Government grant	Advance fee loan	Investment	Credit repair/debt relief
9	Phishing/social engineering	Fake check/money order	Advance fee loan	Advance fee loan
10	Tech support	Credit card	Credit card	Moving

Acknowledgements

BBB Scam Tracker utilizes the trust of the 110-year-old BBB brand to collect data from people who have been targeted by fraudsters. The program is made possible thanks to the dedicated, collaborative work of BBBs across the United States and Canada; BBBs review consumer reports to eliminate those that do not appear to be actual scams, thus ensuring the best data possible.

We'd like to thank a team of BBB experts who provide guidance and input to BBB Institute regarding the BBB Scam Tracker program, including Warren King, president and CEO, BBB Serving Western Pennsylvania; Jane Rupp, president and CEO, BBB Serving Northern Nevada and Utah; Craig Turner, director of information systems, BBB Serving Eastern & Southwest Missouri & Southern Illinois; Dené Joubert, investigations manager, BBB Great West + Pacific; David Wheeler, vice president of innovation and development, BBB Serving Central Florida; and Tammy Ward, communications director, BBB Serving Northwest Florida.

We would also like to thank the International Association of Better Business Bureaus for its support of BBB Institute and the *2022 BBB Scam Tracker Risk Report*. We extend a special thank you to IABBB senior research director Dr. Rubens Pessanha, MBA, PMP, SPHR, GPHR, SHRM-SCP; IABBB data quality analyst Ryan Hessling; and IABBB data quality analyst Logan Haskew, for analyzing the BBB Scam Tracker and survey research data for this report. We'd also like to thank IABBB director of public relations and social media Melanie McGovern, IABBB director of content and SEO Sara Grube, IABBB director of brand policy Jody Thomas, and IABBB deputy general counsel Angela Isabell Taylor for providing their insights and input and helping us share these findings with the public.

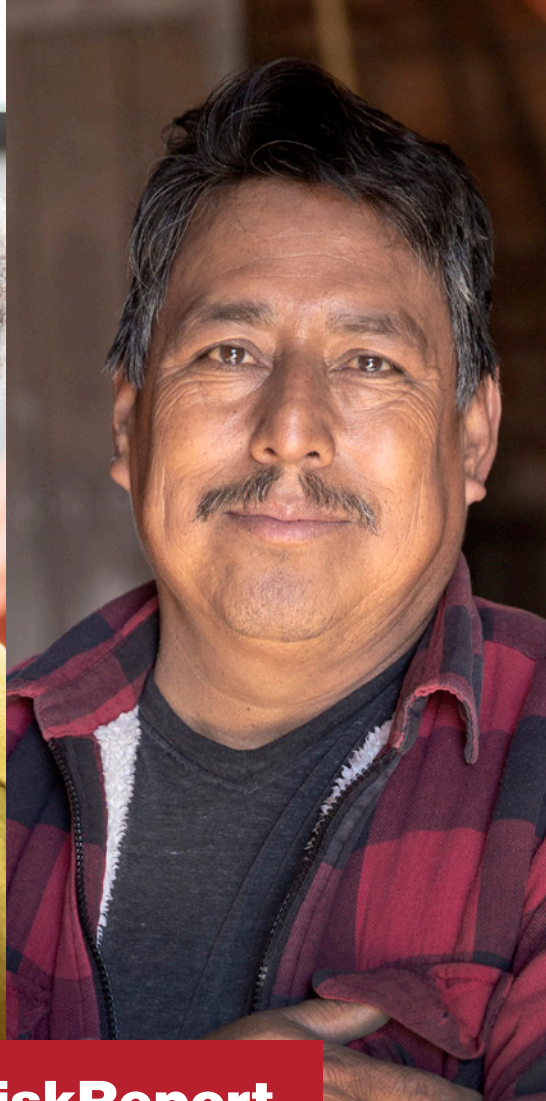
Project team

Logan Haskew is a data quality analyst for the International Association of Better Business Bureaus. With a background in engineering and data science, he is an advocate for data-driven decision-making for both consumers and enterprises alike. When not working, he can be found traveling to some far corner of the United States with his wife and three dogs.

Ryan Hessling is a data quality analyst for the International Association of Better Business Bureaus. Coming from a career in the environmental sciences, Ryan has experience in data gathering, processing, and analysis. He enjoys how much can be learned and inferred by diving into data sets from around the world. A native of southeastern Connecticut, he has two degrees from Three Rivers Community College and a bachelor's from the University of Connecticut. During his downtime, when he is not taking a new course or working on projects, you can find him by the ocean reading a book or walking his dog.

Dr. Rubens Pessanha, MBA, PMP, GPHR, SPHR, SHRM-SCP, is the senior director of research and development at the International Association of Better Business Bureaus. Rubens has more than 20 years of global experience in marketing, strategic organizational development, project management, and market research. He has presented at conferences in North America, Asia, Europe, Africa, and South America. A production engineer with an MBA, he completed his doctorate at George Washington University. He is the co-author of the *BBB Scam Tracker Risk Report (2017–2022)*, *Scams and Your Small Business (2018)*, *Cracking the Invulnerability Illusion (2016)*, *The State of Cybersecurity (2017 and 2018)*, the *BBB Trust Sentiment Index (2017)*, *5 Gestures of Trust (2018)*, and the *BBB Industry Research Series—Airlines (2018)*, among other titles. As a hobby, Rubens teaches project management, business ethics, strategy, and marketing for graduate and undergraduate students.

Melissa "Mel" Lanning Trumpower is the executive director of the BBB Institute for Marketplace Trust. Mel has more than 25 years of nonprofit leadership experience working with a wide range of nonprofit organizations and trade associations. In addition to leading BBB Institute, Mel manages the BBB Scam Tracker program and is the co-author of *Start With Trust Online: Online Scams (2022)*, the *Online Purchase Scams Report (2020 and 2021)*, the *BBB Scam Tracker Risk Report (2017–2022)*, *Scams and Your Small Business (2018)*, *Exposed to Scams (2019 and 2021)*, the *Employment Scams Report (2020)*, and *Building Better Together: The BBB Impact Report (2021)*. Mel has a bachelor's degree from Cornell University and a master's degree from Johns Hopkins University.



BBBMarketplaceTrust.org/RiskReport



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

Institute@IABBB.org