



2022

BBB® Online Scams Report

Start With Trust® Online



2022

BBB® Online Scams Report

Start With Trust® Online

Table of contents

3	Introduction
5	Scams perpetrated online (all types)
11	How and where people engaged with an online scam
12	Impersonation scams
16	Online purchase scams
22	Factors impacting engagement and susceptibility
24	Consumer trust and confidence
26	How to protect yourself from online scams
28	Acknowledgements



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.



Introduction

The manner in which scams are perpetrated in the marketplace shifts continually thanks to new technologies such as social media, changes in consumer behavior patterns, world events, and other factors. Scams perpetrated online continue to make a significant impact. So far in 2022, they are more prevalent overall (55%) than other delivery methods, with a higher percentage of people losing money when targeted (75%) (Figure 1).

FIGURE 1

Percentage of scams reported with monetary loss compared with total reported scams by means of contact, 2022.



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

For the past two years, the BBB Institute for Marketplace Trust (BBB Institute), BBB's educational foundation, has published the **BBB Online Purchase Scams Report** to better understand how online purchase scams were being perpetrated in the marketplace. This year, we've expanded the focus of our report to spotlight all scam types that are perpetrated online to provide new information about which tactics have the biggest impact on consumers and to identify new information that can help consumers protect themselves from online fraud.

In addition to analyzing all scams perpetrated online, this report spotlights some of the most common

scam tactics used to target consumers online. Pretending to be a well-known and respected organization (one type of impersonation) was the most common tactic reported by survey respondents.¹ BBB Scam Tracker does not identify “impersonation” as a specific scam type because this tactic is used across all scam types. However, survey research enabled us to take a closer look at this tactic to help us better understand factors that could help consumers spot the fraud.

The report also highlights online purchase scams, which continue to be the most reported scam type reported to BBB Scam Tracker so far in 2022, making up 30.0% of all scams reported, with 71.6% reporting a monetary loss when targeted by an online purchase scam² (Figure 14).

How did we define an online scam?

For the purposes of this report, online scams are defined as scams that started either via an online means of contact (e.g., website, social media, email, internet messaging, online classifieds) or ended up online after starting offline (e.g., phone, in-person, postal mail).

BBB Scam TrackerSM

This report is possible thanks to data provided through **BBB Scam Tracker**, an online platform that enables consumers and businesses to report attempted or successful acts of fraud they’ve experienced. These instances of fraud are reviewed and posted for the public, empowering others to identify scams and avoid losing money. In 2021 alone, BBB Scam Tracker helped people avoid losing an estimated \$31.4 million. BBB Institute will launch a newly designed BBB Scam Tracker platform in 2022 with support from our partners, Amazon and Capital One.

*In 2021 alone,
BBB Scam Tracker
helped people avoid
losing an estimated
\$31.4
million.*

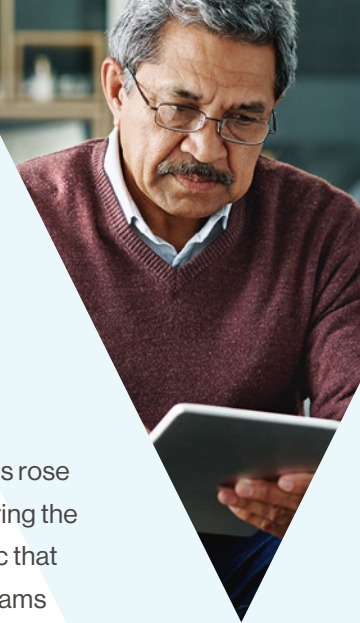
BBB Risk Index

BBB Institute utilized a multidimensional approach (BBB Risk Index) to evaluate scam risk. This approach considers three dimensions: exposure (prevalence of a scam type), susceptibility (the likelihood of losing money when exposed to a scam type), and monetary loss (the median dollar loss reported for a scam type).

This research paper is based on two sets of data: 1) An analysis of more than 300,000 reports submitted to BBB Scam TrackerSM between 2015 and 2022, and 2) survey research conducted in 2022.³ Our analysis included more than 130,000 records that were classified with a means of contact that fell within our definition of an online scam.

^{1,3} BBB Institute conducted survey research in July 2022 with almost 3,000 people who reported a scam to BBB Scam Tracker in the last 12 months.

² [2021 BBB Scam Tracker Risk Report](#).



Scams perpetrated online (all types)

The percentage of scams reported to BBB Scam Tracker that were perpetrated via online means rose 87% between 2015/2016 (30%) and 2021/2022 (56%) (Figure 2). This is not surprising considering the increased amount of time consumers spend online today, especially following a global pandemic that forced many consumers to work, shop, and socialize via the internet. During the same period, scams perpetrated via phone dropped 42% from 59% in 2015/2016 to 34% in 2021/2022.

Scams perpetrated via phone with a monetary loss dropped from 26% in 2015 to 17% in 2022 (Figure 3). In 2020, reported online scams with a monetary loss hit a high of 81%. Though the percentage of reported online scams with a monetary loss dropped slightly since then, they continue to be higher than pre-2020 percentages at 77% in 2021 and 75% in 2022.

When we break out phone as a means of contact with a monetary loss, we see that phone calls dropped from 86% in 2015 to 70% in 2022 (Figure 4). However, text message climbed significantly (from 11% in 2015 to 30% in 2022).

FIGURE 2

Change in reported means of contact (2015/2016 and 2021/2022)

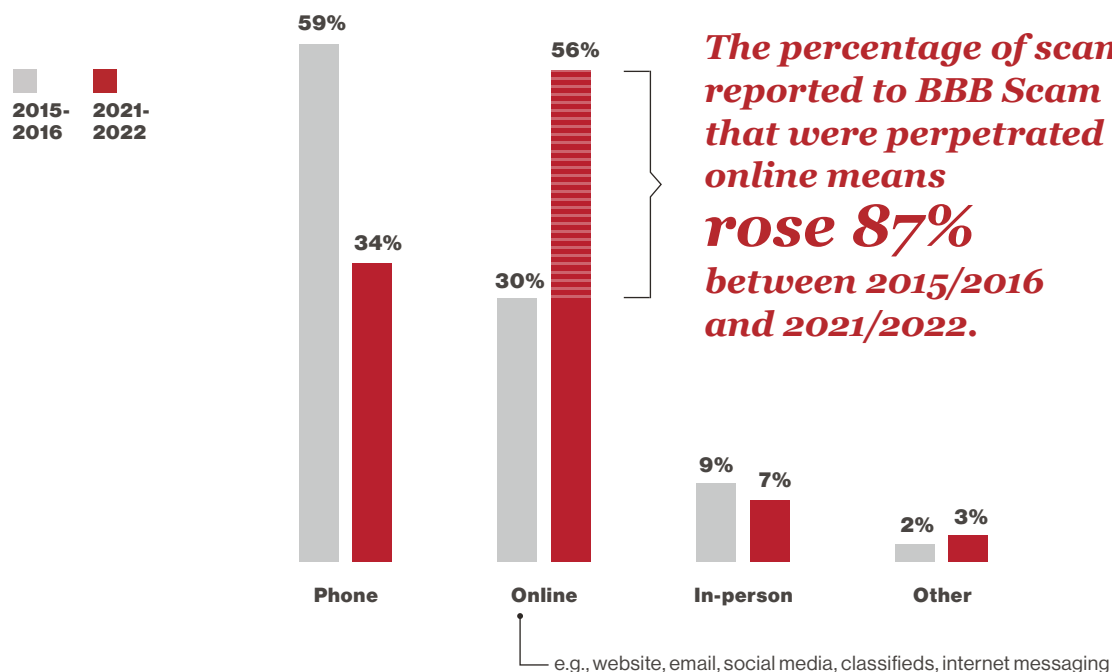
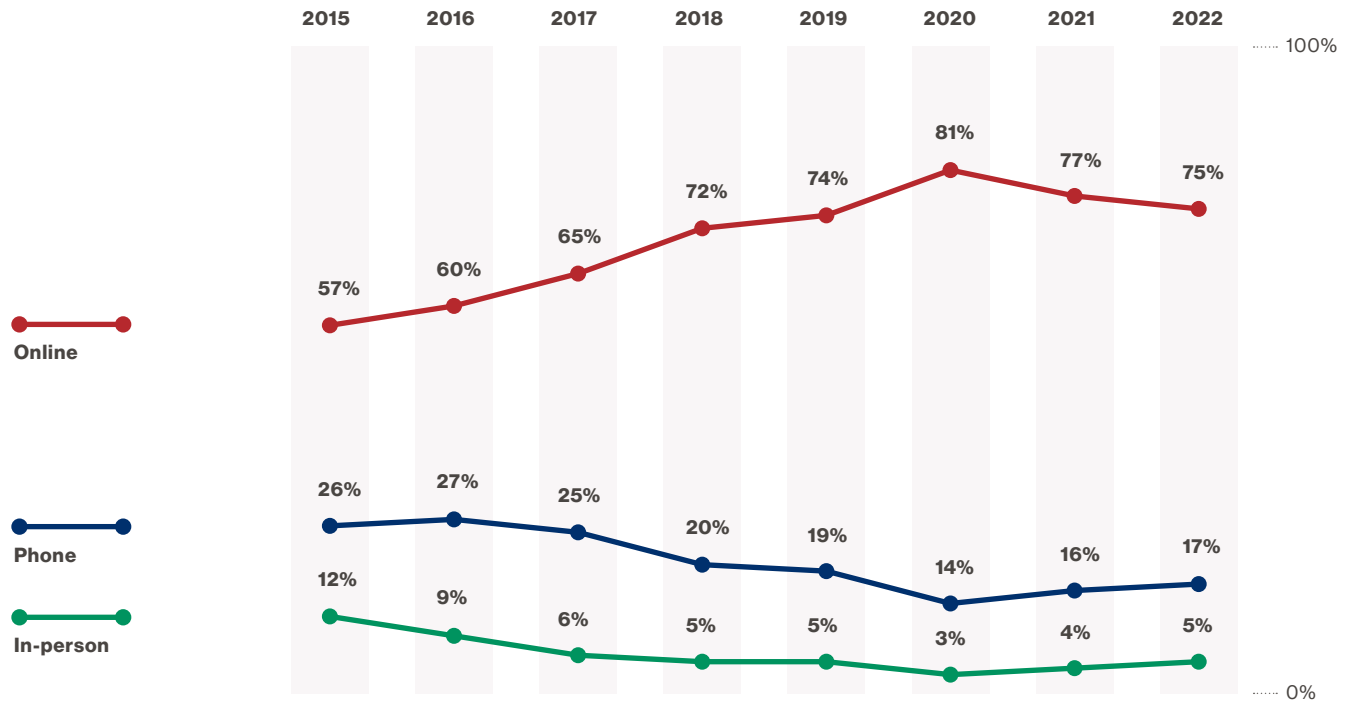
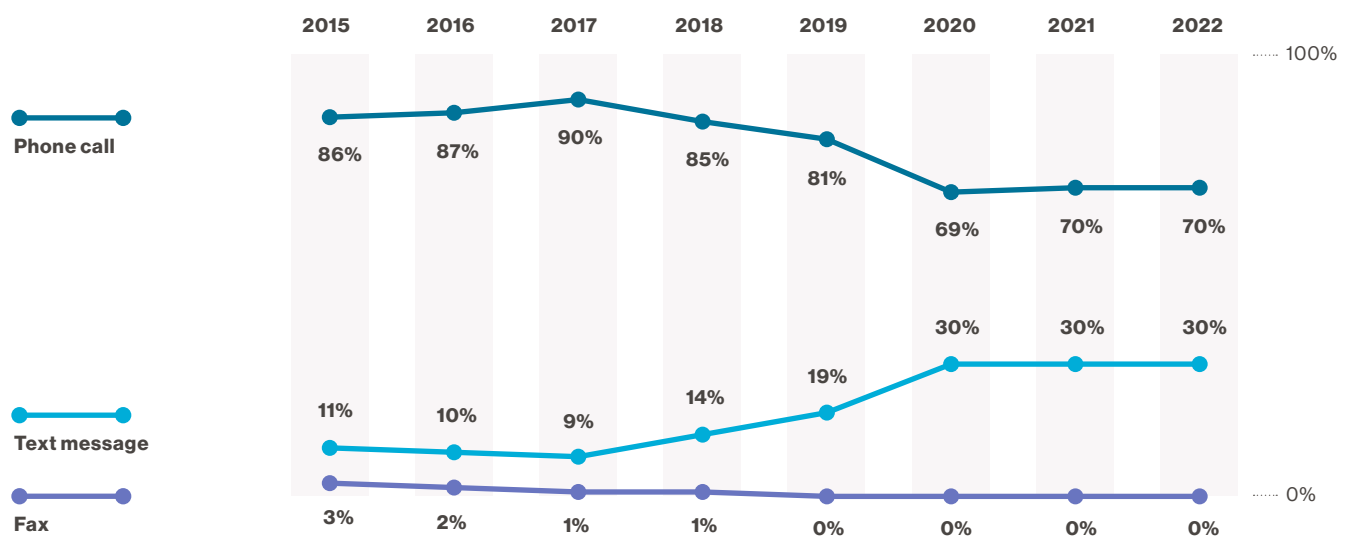


FIGURE 3**Change in reported means of contact with a monetary loss (2015 to 2022)**

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

FIGURE 4**Phone as a means of contact with a monetary loss (2015 to 2022)**

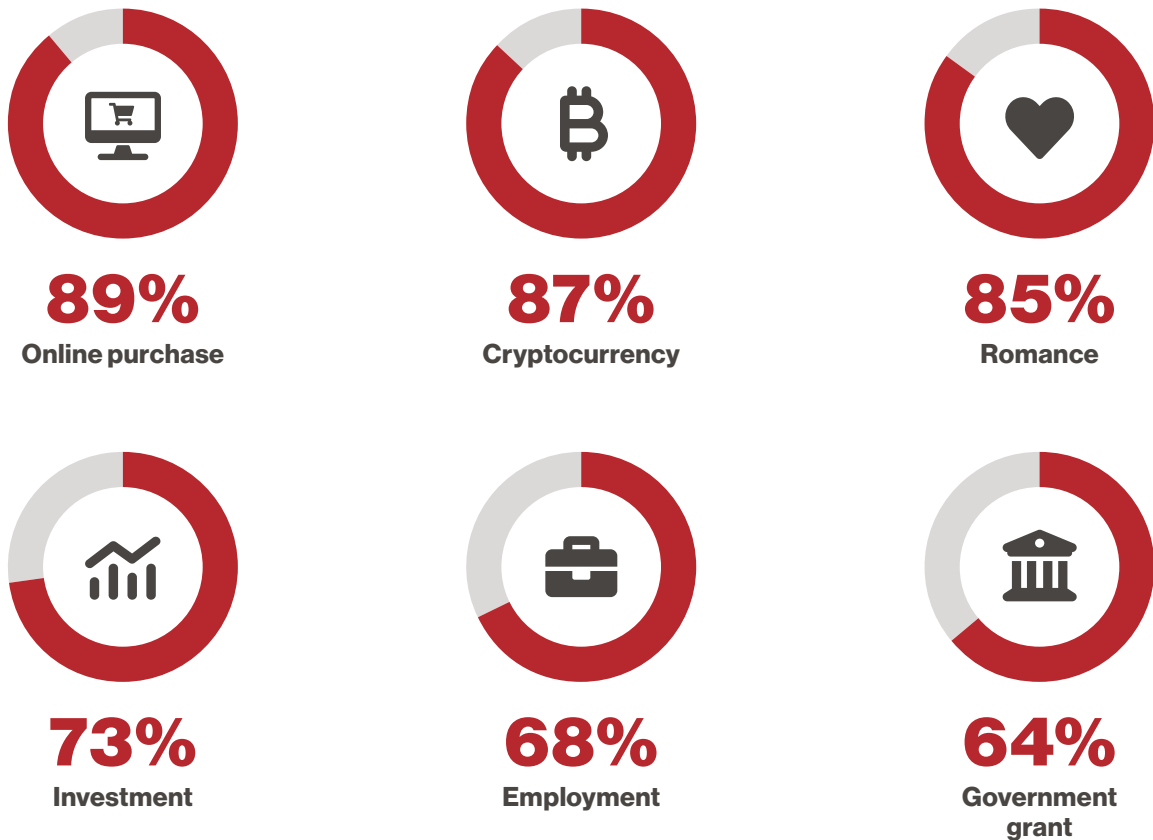
Percentages with a monetary loss do not add up to 100% because of rounding.

Scam types more likely to be perpetrated online.

Every type of scam can be perpetrated online. However, some scam types are more likely to begin with an online means of contact. According to BBB Scam Tracker data reported between January 2021 and August 2022, the scam type with a monetary loss most often reported beginning online was online purchase scams (89%). The other scam types that were more likely to begin via online means include cryptocurrency scams (87%), romance scams (85%), investment scams (73%), employment scams (68%), and government grant scams (64%).

FIGURE 5

Scam types with a monetary loss most often reported as beginning with an online engagement.



The scam type with a monetary loss most often reported beginning online was online purchase scams.

Payment method.

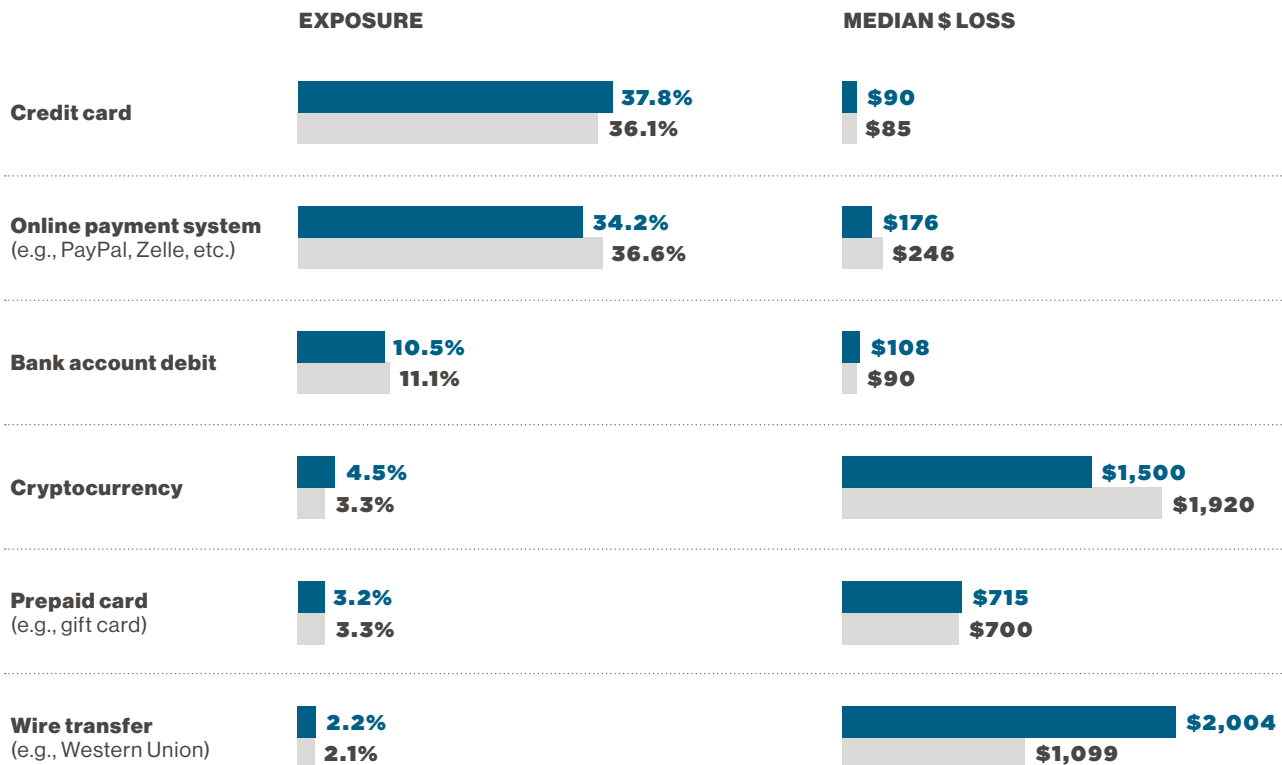
The most reported payment methods with a monetary loss for scams perpetrated online in 2022 so far are credit card (37.8%), online payment system (34.2%), and bank account debit (10.5%). Cryptocurrency as a payment method with a monetary loss rose from 3.3% in 2021 to 4.5% in 2022. The payment methods with the highest median dollar loss in 2022 were wire transfer (\$2,004) and cryptocurrency (\$1,500).

Almost 83% of those targeted online reported paying via credit card, online payment system or bank account debit.

FIGURE 6

Payment methods with a monetary loss for all scam types perpetrated online

■ 2022*
■ 2021



*Data for 2022 includes scams reported to BBB Scam Tracker between January 1, 2022 and June 20, 2022.

Percentage of exposure for payment methods with a \$ loss do not add up to 100% because the "other" category was not included.

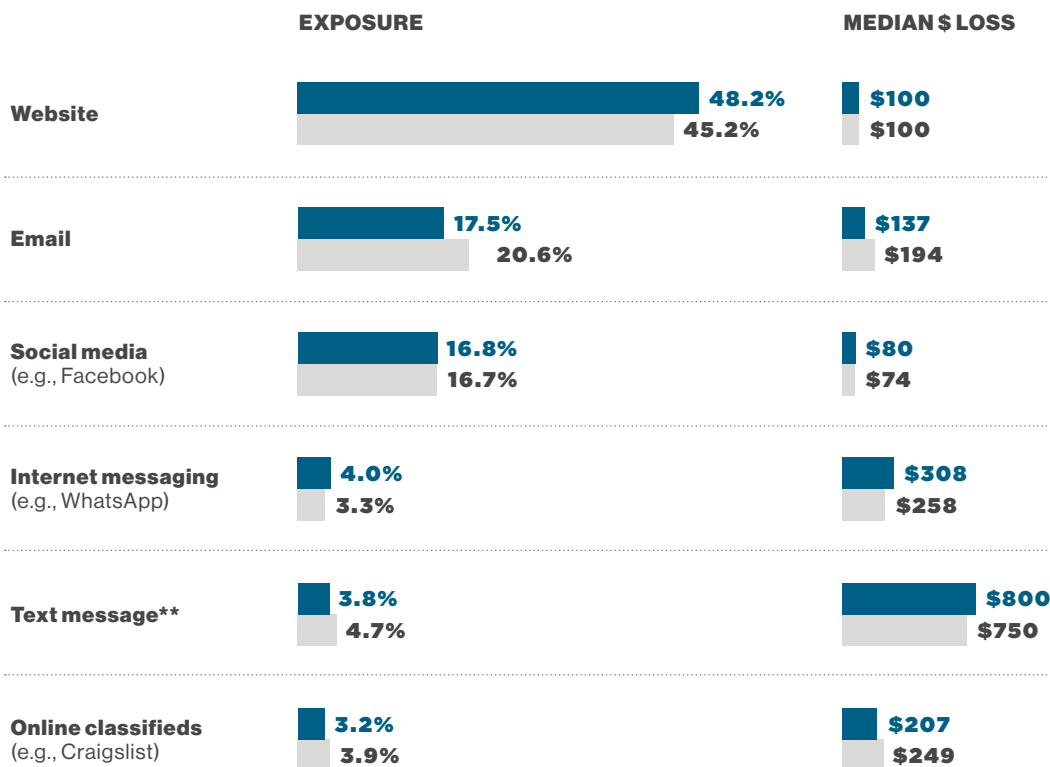
Means of contact.

The most reported means of contact with a monetary loss for scams perpetrated online included website (48.2%), email (17.5%), and social media (16.8%). The means of contact with the highest median loss included text message (\$800), internet messaging (\$308), and online classifieds (\$207).

FIGURE 7

Means of contact with a monetary loss for all scam types perpetrated online

■ 2022*
■ 2021



*Data for 2022 includes scams reported to BBB Scam Tracker between January 1, 2022 and June 20, 2022.
Percentage of exposure for payment methods with a \$ loss do not add up to 100% because the "other" category was not included.

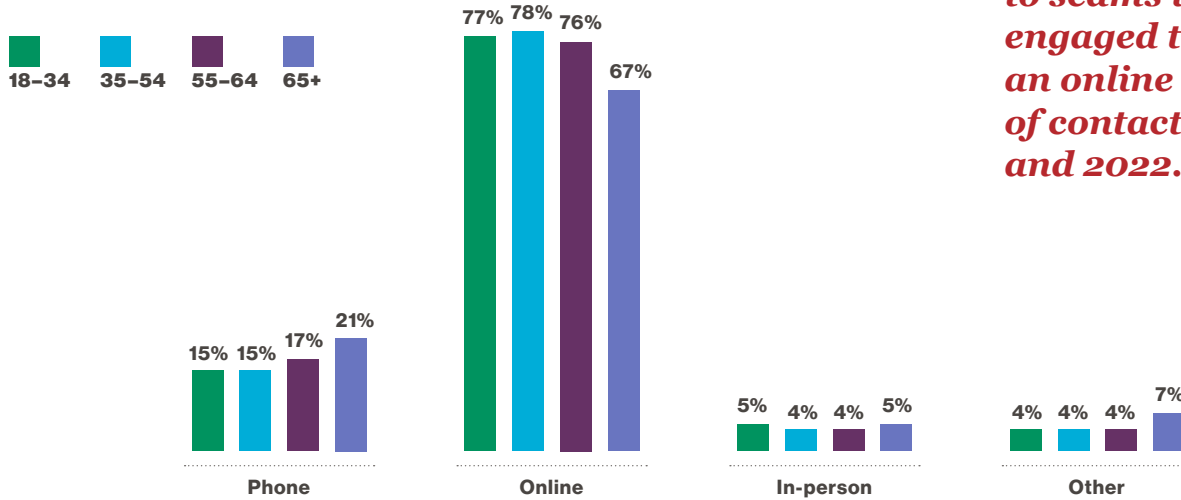
Impact by age.

For all age groups, scams perpetrated via an online means of contact with a monetary loss were reported more than all other contact methods to BBB Scam Tracker (Figure 8). In fact, an online engagement was reported by almost eight out of ten people who lost money in 2021 and 2022.

*Almost
8 out of 10
people reported
losing money
to scams that
engaged them via
an online means
of contact in 2021
and 2022.*

FIGURE 8

Online means of contact with a monetary loss, by age group



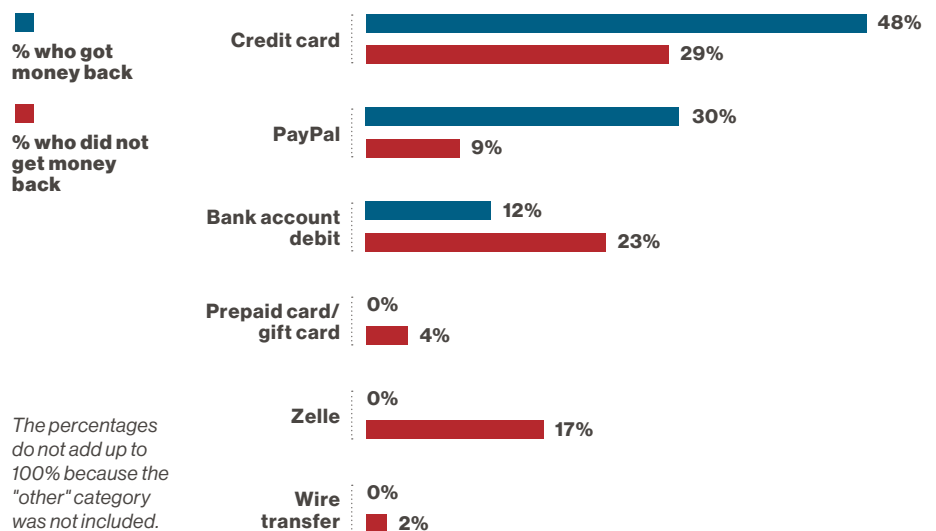
The percentages do not add up to 100% due to the rounding of numbers.

Getting funds reimbursed.

The two payment methods most reported by those who were able to get their money back following the scam were credit cards and PayPal.

FIGURE 9

Reported reimbursements following scam by payment method



The percentages do not add up to 100% because the "other" category was not included.

How and where people engaged with an online scam

The nature of a person's online activity appears to have an impact on their chances of being targeted by a scam. Twenty-five percent of survey respondents reported they were browsing social media when they were targeted (Figure 10). Respondents also reported being targeted while shopping online (24%), checking email (14%), using search engines (10%), and searching for a job (7%). Other reported activities included playing online games, checking internet messaging, and selling items online.

Scammers use offline tactics to get people online

Not all online scams begin when you're browsing the internet. Scammers use offline tactics to draw their targets online where they can perpetrate the scam. The most common offline method reported was a link sent via text to push the person online (Figure 11). Text messages continue to be risky with an \$800 median dollar loss across all scam types so far in 2022. Respondents also reported phone calls and postal mail as offline methods used by scammers to draw them online.

FIGURE 10



25% reported being targeted by a scam while browsing social media.

FIGURE 11

If you started the engagement offline, how did the scammer instruct you to get online?

Text messages continue to be risky with an \$800 median dollar loss across all scam types so far in 2022.



#1

Texted me a link that took me online



#2

Called me and told me to go online



#3

Sent me postal mail with instructions to go online

Impersonation scams

Scammers use a variety of tactics to perpetrate their fraudulent schemes. By pretending to be well-known and trusted companies, government agencies, and organizations, scammers aim to co-opt the trust people feel toward these organizations. Claiming to be from a legitimate organization (one type of impersonation) was by far the most reported tactic used by scammers (54%), according to our survey research. Other top reported tactics included offering a great price (24%), pressuring the target to act quickly (21%), and offering a great job opportunity (10%).

54% of survey respondents said the scammer claimed to be from a legitimate organization.



FIGURE 12

Most reported tactics used by scammers to perpetuate online scams.



Claimed to be from a legitimate organization.

54%

of reports

Offered me a great price.

24%

of reports

Told me I needed to act quickly.

21%

of reports

Offered a great job opportunity.

10%

of reports

Sent me a photo.

9%

of reports

The percentages do not add up to 100% because respondents were able to select multiple options.

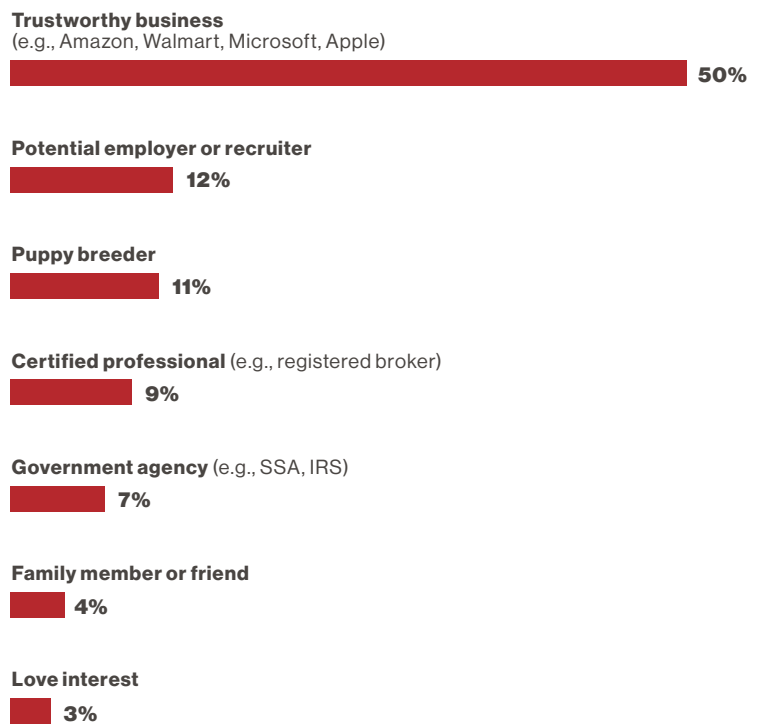
People who lost money to a scam were almost twice as likely as those who avoided losing money to say the scammer used impersonation as a tactic. According to our survey research, the types of organizations most impersonated by scammers were trustworthy business (50%), employer/recruiter (12%), puppy breeder (11%), certified professional (9%), and government agency (7%) (Figure 13).

People who lost money to a scam were almost twice as likely as those who avoided losing money to say the scammer used impersonation as a tactic.

FIGURE 13



Types of organizations impersonated to perpetrate scams.



Other (4%) includes potential client; charitable organization; work colleague or supervisor; police officer.

Factors that helped people spot the impersonation

43%



Forty-three percent of survey respondents **suspected the scammer was impersonating an organization or a person.**

Respondents said they became suspicious for the following reasons.

- They **knew real businesses do not contact people the way they did** or ask for the information they requested.
- The **offer seemed too good to be true** (e.g., price).
- The **website seemed suspicious** (e.g., a few months old, contradicting information, bad grammar, typos, confusing).
- The scammer put **too much pressure** on them to purchase or do something.
- The scammer got **aggressive or threatened** the target when questioned.
- The target was able to identify/verify that **the photos shared by the scammer were fake.**
- The scammer provided **inconsistent information.**
- The target was **unable to connect with the scammer by phone.**

Reasons some did not detect the impersonation scam

57%



Fifty-seven percent **did not suspect the scammer was impersonating** an organization or a person and listed the following reasons.

- They were **friendly and knowledgeable.**
- They **provided a name and address** information.
- They **sent me tracking** (or other type of shipping) information.
- They **sent me pictures** that seemed legitimate.
- They **promised significant gains** or benefits.
- They were a **top result on Google** search.
- They offered a **money-back guarantee.**
- They offered **consistent communication.**
- They **assured me they were a legitimate business** and urged me to check.
- They had a **professional website** and marketing.
- I was **under the impression that Facebook sold advertisement space only to reputable businesses.**
- They had **positive reviews/testimonials** on their website.

Verifying a person or organization's credentials

68%

Sixty-eight percent of those surveyed **did not ask the person to provide verification** that they were a legitimate representative of the organization. Respondents provided the following reasons for why they did not ask for verification.

- They were **concerned about losing out** on the opportunity.
- They **wanted to believe** it was true.
- They really **needed or wanted** what the scammer was offering.
- The scammer included a **phone number that seemed legitimate** (800 number).
- The **website looked professional** and had favorable reviews.
- The scammer presented themselves as a legitimate company and **seemed legitimate**.
- They **trusted the person** or trusted that the person worked for the company they said they did.
- The scammer **seemed to know them** (e.g., knew the person's name).
- The scammer **seemed to have information** about the person's situation.
- The target trusted the ad and **thought any business advertising on Facebook had to be legitimate**.

How scammers pretend to offer verification



When respondents **requested the scammer to provide verification**, they reported being provided with the following.

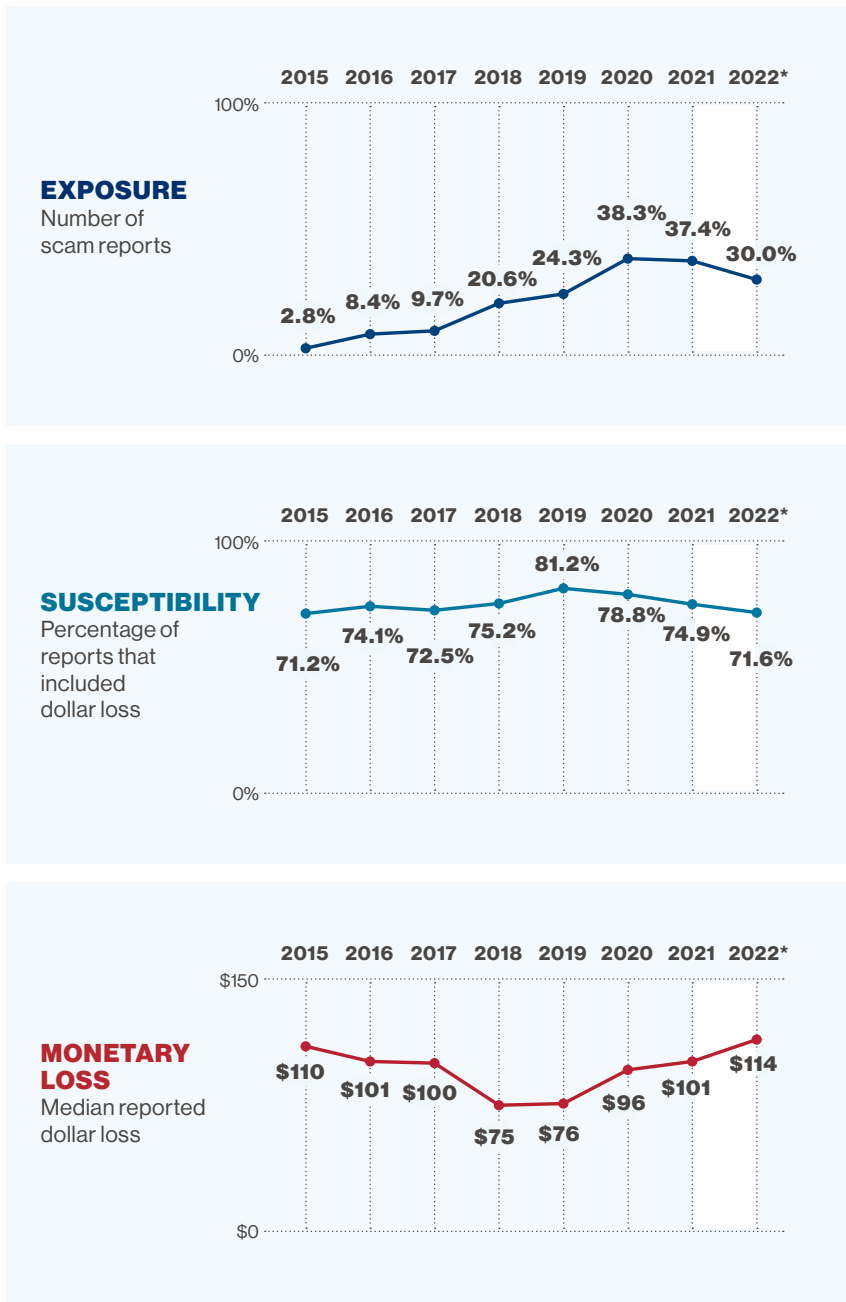
- They showed or sent a **business card**.
- They sent me to their **professional website**.
- They **told me to look them up** online.
- They showed **paperwork/certificate/certification/documentation**.
- They gave me an **address** and told me to come and check.
- They shared an **original order form** or a link to a shipping company.
- They sent me **pictures or photos** as proof of other customers receiving their products.
- They gave me a **phone number** to contact them if needed.
- They had a **video call with me**.
- They said I could **call their boss to confirm** they were legitimate.
- They **told me they had an A rating with the BBB**.

Online Purchase Scams

Online purchase scams (also known as online shopping scams) ranked as the #1 riskiest scam type in 2021, according to the **BBB Scam Tracker Risk Report**. Online purchase scams continue to be the most prevalent of all scam types reported to BBB Scam Tracker, making up 30.0% of all reported scams so far in 2022 with 71.6% losing money (Figure 14). Though susceptibility for this scam type appears to be dropping, median dollar loss has risen in recent years.

FIGURE 14

Exposure, susceptibility, and median dollar loss by year for online purchase scams.



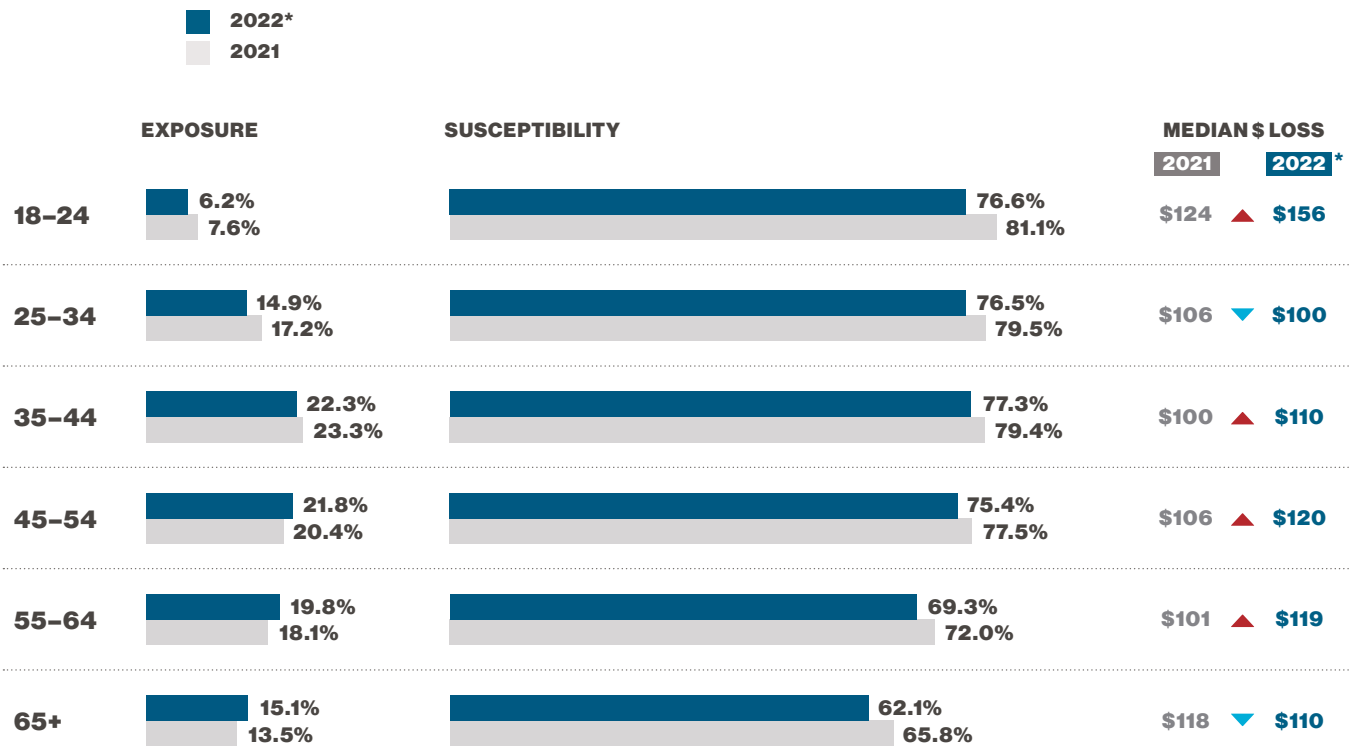
*Data for 2022 includes reports submitted between January 1, 2022 and June 20, 2022.

Age, online purchase scams

Those between the ages of 35 and 64 reported a higher exposure to online purchase scams in 2022 than other age groups. Susceptibility has dropped for all age groups so far in 2022. However, the reported median dollar loss for ages 18-24 increased 25.8% from \$124 in 2021 to \$156 in 2022; this age group reported the highest median dollar loss. Ages 35-64 also reported an increase in median dollar loss from 2021 to 2022.

FIGURE 15

Exposure, susceptibility, and monetary loss by age for online purchase scams, 2022* versus 2021



*Data for 2022 includes reports submitted between January 1, 2022 and June 20, 2022.
The percentages do not add up to 100% due to the rounding of numbers.

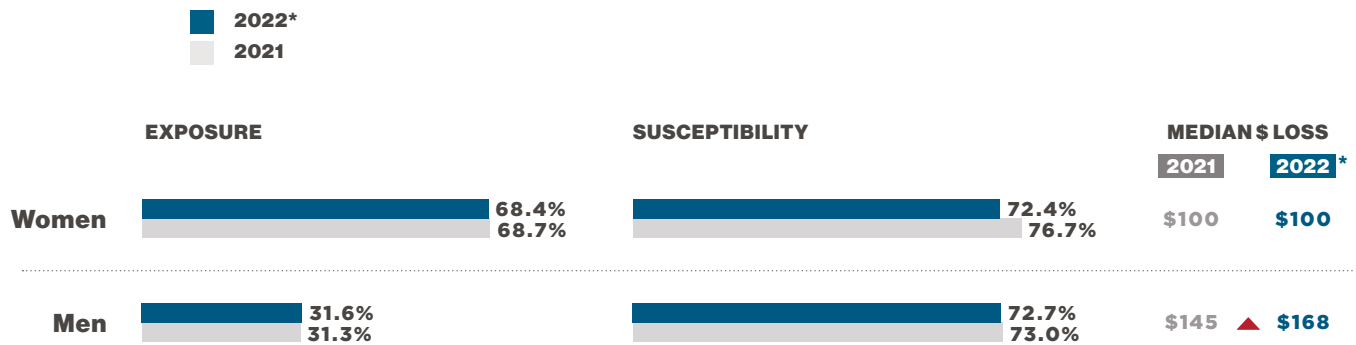
Ages 18-24 reported the highest median dollar loss in both 2021 and 2022.

Gender, online purchase scams

Similar to reports from previous years, women reported 68.4% of all online purchase scams, compared to 31.6% reported by men (Figure 16). Men reported losing significantly more money (\$168) than women (\$100). The reported median dollar loss for men rose 15.9% from \$145 in 2021 to \$168 in 2022.

FIGURE 16

Exposure, susceptibility, and monetary loss by gender for online purchase scams, 2022* versus 2021



*Represents scams reported between January 1, 2022, and June 20, 2022.

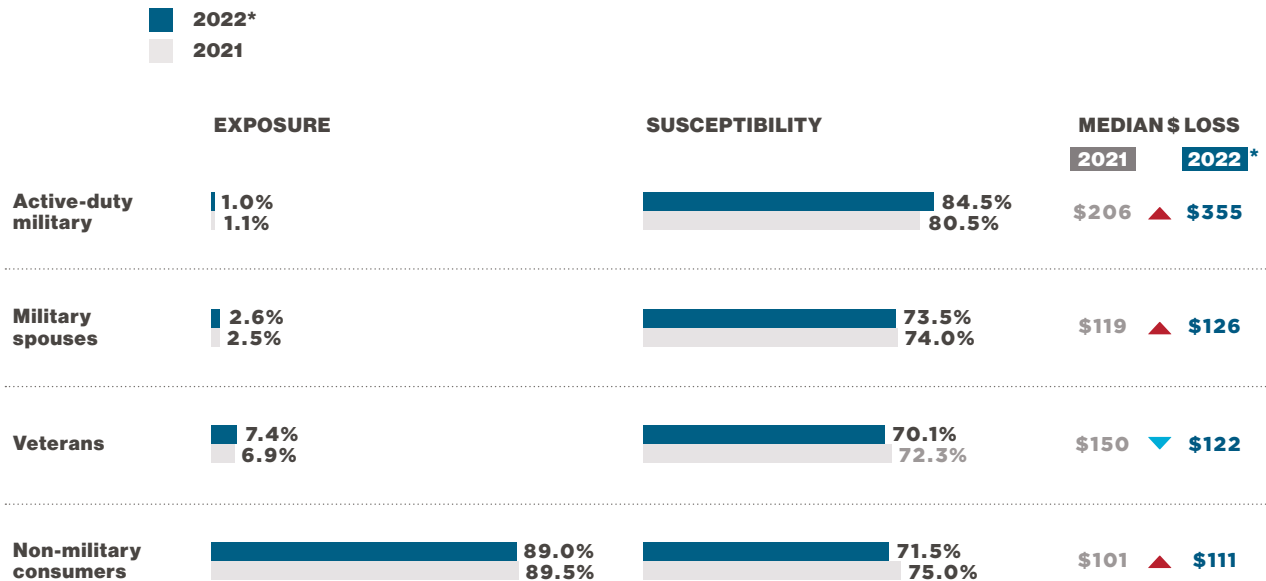
Women reported 68.4% of all online purchase scams, compared to 31.6% reported by men, but men reported losing significantly more money than women again in 2022.

Military status, online purchase scams

About 11% of online purchase scams reported to BBB Scam Tracker so far in 2022 came from the military community (active duty, spouses, and veterans). Active-duty military were more likely to report losing money to this type of scam, with 84.5% reporting a monetary loss; this was an increase from a susceptibility of 80.5% in 2021. Active-duty military also reported losing significantly more money (\$355) than veterans (\$122) and spouses (\$126). The reported monetary loss for active-duty military rose 72.3% from a reported median dollar loss of \$206 in 2021.

FIGURE 17

Exposure, susceptibility, and monetary loss by military status for online purchase scams, 2022* versus 2021



*Represents scams reported between January 1, 2022, and June 20, 2022.

Active-duty military were more likely to report losing money to online purchase scams, with 84.5% reporting a monetary loss so far in 2022.

Payment methods, online purchase scams

The top payment method used by those who reported losing money to online purchase scams in 2022 was credit cards (41.0%) followed by online payment systems (33.0%). The median dollar loss reported by those who paid with cryptocurrency rose 21.8% from \$550 in 2021 to \$670 in 2022. The median dollar loss for those who reported paying with bank account debit rose 21% from \$81 in 2021 to \$98 in 2022.

Means of contact, online purchase scams

The top three reported means of contact for online purchase scams were website (36.7%), social media (20.3%), and email (19.8%). While the reported median dollar loss for email dropped from \$156 in 2021 to \$128 in 2022, it rose for those who engaged with the scammer via social media (from \$75 in 2021 to \$92 in 2022). Text messages continue to be the means of contact with the highest reported median dollar loss for online purchase scams at \$638.

Text messages continue to be the means of contact with the highest reported median dollar loss for online purchase scams at \$638.

FIGURE 18

Top 3 payment methods reported by those who lost money to online purchase scams



FIGURE 19

Top 3 means of contact reported by those who lost money to online purchase scams



Top reported product types and motivating factors

The top reported product types used to perpetrate online purchase scams were pets and pet supplies, similar to reporting from previous years. Other top reported products used to target people for online purchase scams were digital devices, motor vehicles, and medical/nutritional products.

The top three factors people said motivated them to make the online purchase were sales prices, nice photos, and availability of the product.

Passive vs. active searching/shopping

Fifty-five percent of those who reported losing money to online purchase scams were actively searching/shopping for a product/service, while 31% were not searching/shopping, and 14% were passively searching/shopping.

55% of those who reported losing money to online purchase scams were actively searching/shopping for a product/service.


FIGURE 20


Top reported product types used to perpetrate online purchase scams


1	Pets/pet supplies
2	Digital devices
3	Motor vehicles
4	Medical/nutritional
5	Information/media
6	Footwear
7	Clothing/accessories
8	Home decorations
9	Musical instruments
10	Furniture

FIGURE 21

Top motivating factors for making an online purchase

- 

#1
Sales price/lower price/discount
- 

#2
Photos on the website
- 

#3
Availability (e.g., hard-to-find item)



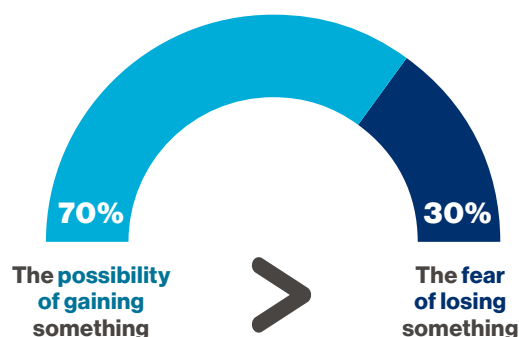
Factors impacting engagement and susceptibility

There are a variety of factors and behaviors that appear to influence why people continue to engage with scammers. Offering something that is too good to be true, for example, appears to be more effective than a threat. About 70% of survey respondents said they continued the online engagement because they hoped to gain something, sell something, or were curious to learn more (Figure 22). The other 30% said they continued the engagement because they feared they'd lose something, were threatened, or there was an urgent situation they needed to address.

About 70% of respondents said they continued the online engagement because they hoped to gain something, sell something, or were curious to learn more.

FIGURE 22

What was your biggest motivating factor for continuing the engagement?



Doing research on the business

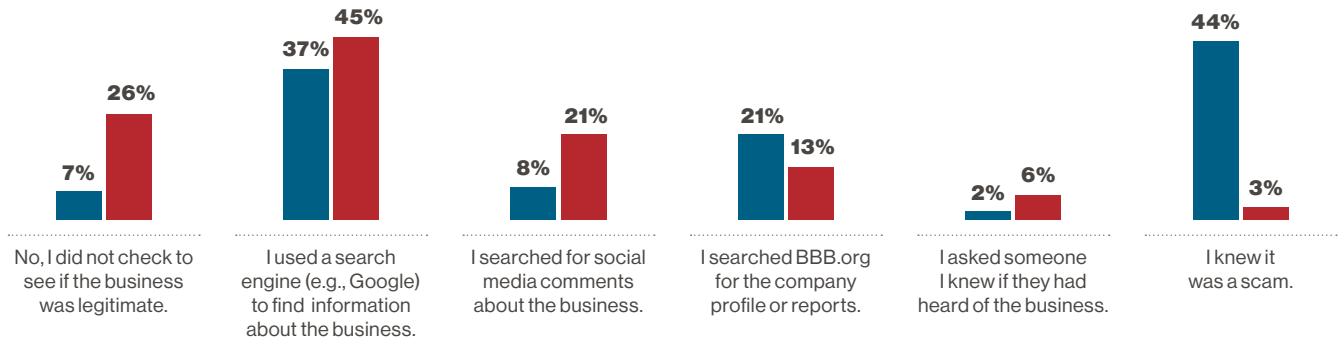
Of those who reported that they avoided losing money, 7% did not do any form of research, 37% searched for information via a search engine, 8% searched social media comments, 21% searched BBB.org, and 2% reached out to friends and/or family. Of those who reported losing money, 26% did not do any form of research, 45% searched for information via a search engine, 21% searched social media comments, 13% searched BBB.org, and 6% reached out to friends and/or family.

Those who reported that they avoided losing money were more likely than those who reported losing money to say they searched BBB.org to determine if the business was legitimate.

FIGURE 23

Did you take time to determine if the business was legitimate? If so, what did you do?

DID NOT LOSE \$
LOST \$



Respondents were allowed to choose more than one response, which is why these results do not add up to 100%.

Prevention factors

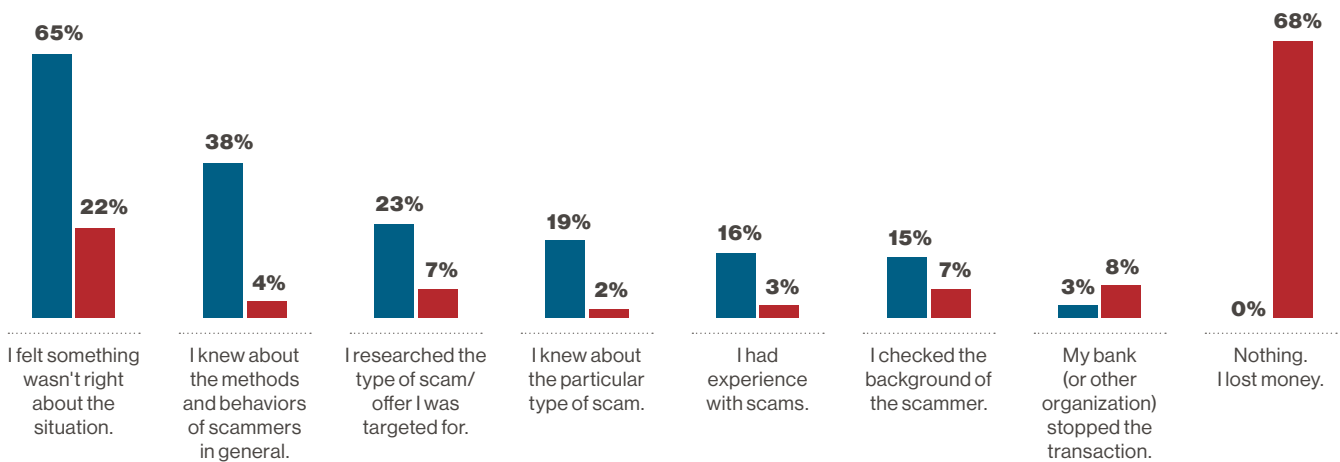
We asked respondents if something helped them avoid the scam. Of those who reported that they avoided losing money, 65% felt something wasn't right about the situation, 38% knew about the methods and behaviors of scammers in general, 23% researched the specific type of scam, 19% had knowledge about the scam type, 16% had general experience with scams, and 15% checked the background of the scammer.

It's important to note that 22% of survey respondents felt something wasn't right about the situation but still continued the engagement and lost money. For this reason, it's most protective to combine following your gut with other activities such as learning about the methods/behaviors of scammers in general and/or researching the offer/scammer with trusted sources.

FIGURE 24

Did something help you avoid being scammed?

DID NOT LOSE \$
LOST \$



Respondents were allowed to choose more than one response, which is why these results do not add up to 100%.

Consumer trust and confidence

The impact of being targeted by a scam goes beyond losing money. According to our survey research, 56% of those who reported being targeted by online scams lost money, followed by time (46%), confidence/emotional well-being (31%), personal information (30%), and credit health (5%) (Figure 25).

31% said they lost confidence/emotional well-being after being targeted by an online scam.

FIGURE 25

Did you lose any of the following?



Impact on trust

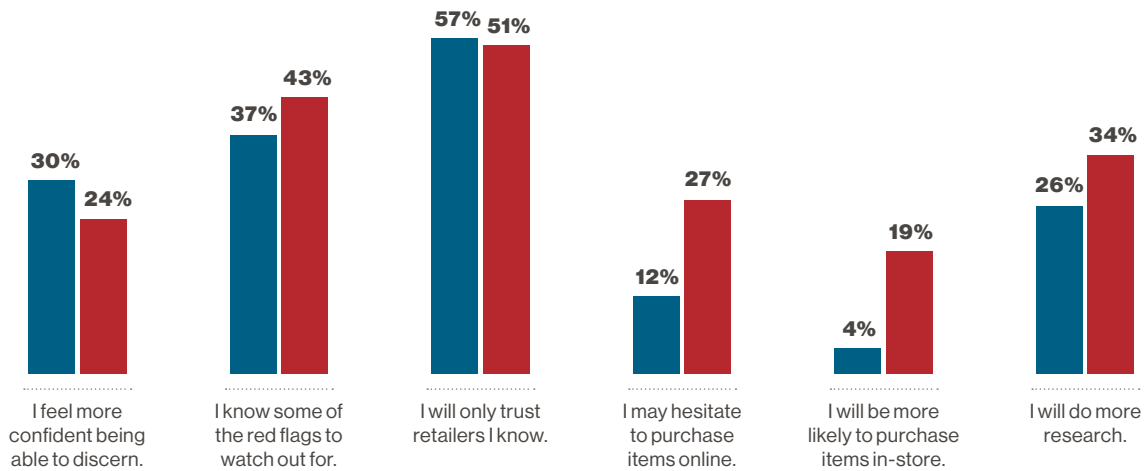
Following their scam experience, 57% of those who avoided losing money and 51% of those who lost money said they will only trust retailers they know (Figure 26). Nineteen percent of those who lost money said they'd be more likely to purchase items in person. Similarly, 27% of those who lost money said they will hesitate to purchase products online.

Thirty percent of those who avoided losing money to the scam said they were more confident about detecting future scam attempts compared to 24% of those who reported losing money. Twenty-six percent of those who avoided losing money and 34% of those who lost money said they will do more research before making another purchase.

FIGURE 26

As you prepare for the holiday season this year, how do you feel now about purchasing items online?

DID NOT LOSE \$
LOST \$



Respondents were allowed to choose more than one response, which is why these results do not add up to 100%.

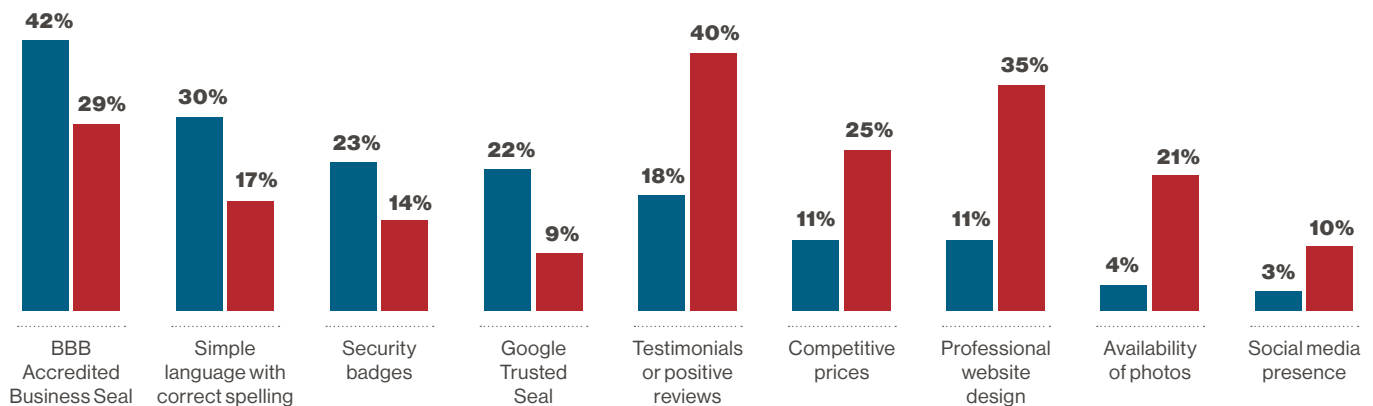
Building trust

Survey respondents who avoided losing money said the top factors that help them trust a business included the BBB Accredited Business Seal (42%), simple language/correct spelling (30%), security badges (23%), and the Google Trusted Seal (22%). Those who reported losing money said the top factors that help them trust a business included testimonials/positive reviews (40%), professional website design (35%), competitive prices (25%), availability of photos (21%), and social media presence (10%).

FIGURE 27

Select the three most important factors you consider when deciding to trust a company.

DID NOT LOSE \$
LOST \$



Respondents were allowed to choose more than one response, which is why these results do not add up to 100%.

How to protect yourself from online scams

General tips

If the deal looks too good to be true, it probably is. Price was the top reported factor to motivate people to make the purchase. Seventy percent of respondents reported continuing their engagement with a scammer who offered a reward or some sort of gain.

Be careful purchasing sought-after products. Scammers offer hard-to-find items and highly sought-after products at great prices.

That shipping information you received might be fake. Look closely to make sure you are dealing with a legitimate business. Go to the shipper's website and type in the code they've provided to see if it's real.

Before you buy, do your research. One of the best ways to avoid scams is to do research with trustworthy sources and avoid making snap buying decisions.

But remember, the source of your research is important. For example, those who reported that they avoided losing money were more likely than those who reported losing money to say they searched BBB.org to determine if the business was legitimate.



Impersonation scams

Ask for verification and take time to do research with a trusted source. People who lost money to a scam were almost twice as likely as those who avoided losing money to say the scammer used impersonation as a tactic.

Be skeptical about anyone who reaches out to you unsolicited. Survey respondents told us scammers produced fake business cards, websites, credentials, ratings and more to convince them they were legitimate.

Don't believe everything you see. Scammers are great at mimicking official seals, fonts, and other details. Just because a website or email looks official does not mean it is. For example, if a business displays a BBB Accredited Business seal, you can verify its legitimacy by going to BBB.org and looking up the company yourself.

Websites



Take a few moments to research a new website:

Check the URL. Scammers will create fake URLs that mimic well-known brand names. If you look closely, you can usually detect one character or something else that is incorrect.

Watch for bad grammar. Read the content carefully—you may detect typos and bad grammar, indicating the website was put together quickly.

Research age of domain. Scammers create professional looking sites quickly to attract targets before the sites are taken down. Online tools can help you find out how long the domain has been active. If it's a newer website, proceed with caution.

Search for contact information. Is there a way to contact the business (phone, email address, address, online chat)? If the only contact information you can find is an online form, that's a red flag. Do more research.

Make sure it's secure. Look for the "https" in the URL (the extra s is for "secure") and a small lock icon on the address bar. Never enter payment or personal information into a website with only "http" (it is not secure).

Text messages

NEVER click on links in unsolicited text messages.

Text message was the means of contact with the highest reported median loss (\$800) for all reported online scams. Of all scams perpetrated by phone with a monetary loss, text message rose from 11% in 2015 to 30% in 2022.



Online search, social media, and comments/reviews

Avoid making quick purchases while browsing social media. Social media was the third most reported means of contact for online scams with a monetary loss behind websites and email in 2022. Some survey respondents said they continued engaging with a scammer because they thought ads on Facebook had to be legitimate.

Do more research on those products you found via online search. Ten percent of survey respondents told us they were targeted while doing an online search.

Do not make a buying decision solely based on comments/reviews. Twenty-one percent of those who lost money reported searching the social media comments.



Payment methods

Use secure and traceable transactions.

Those who paid with a credit card or PayPal were more likely to recover their funds. Avoid paying by wire transfer, prepaid money card, gift card, or other non-traceable payment methods.

Be cautious when paying with cryptocurrency.

According to BBB Scam Tracker data, the percentage of those losing money when paying with crypto rose from 3.3% in 2021 to 4.5% in 2022; the reported median dollar loss was \$1,500 in 2022.

Choose your online payment system carefully.

Those who reported paying with PayPal were more likely to get their money back than other online payment systems. Take the time to understand the rules around your online payment system; not all will reimburse money if you get scammed.

Detect. Protect. Report.
BBB.org/ScamTracker





Acknowledgements

This research report was a joint project of the BBB Institute for Marketplace Trust and the International Association of Better Business Bureaus (IABBB). Contributors include Dr. Rubens Pessanha, MBA, PMP, GPHR, SPHR, SPHR-i, IABBB senior director of research, Sean Xiangwen Lai, PhD, IABBB research and development specialist, Melissa Trumpower, BBB Institute executive director, and Mark Batchelor, BBB Institute manager of programs and outreach.

About BBB Institute

The BBB Institute for Marketplace Trust (BBB Institute) is the educational foundation of the International Association of Better Business Bureaus. Our mission is to educate and protect consumers, promote 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 by Better Business Bureaus serving communities across North America. You can find more information about BBB Institute and its programs at [BBBMarketplaceTrust.org](https://www.BBBMarketplaceTrust.org).

About BBB Scam TrackerSM

BBB Scam Tracker ([BBB.org/ScamTracker](https://www.BBB.org/ScamTracker)) is an online tool that enables consumers to learn about the latest scams being perpetrated in their communities, report scam activity, and prevent others from losing money to similar cons. This year, BBB Institute will launch a new-and-improved BBB Scam Tracker platform with support from our partners, Amazon and Capital One.

BBBMarketplaceTrust.org/OnlineScams

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

Institute@IABBB.org