

# FINANCIAL & LEGAL SCAMS

COVID-19 Cybersecurity Scams & The Impact on Small Business





# Pikes Peak Small Business Development Center

FREE CONSULTING | PRACTICAL TRAINING | BUSINESS RESOURCES

[www.pikespeaksbdc.org](http://www.pikespeaksbdc.org)





The Pikes Peak SBDC's Cyber: CYA program is built to assist small and medium sized businesses by focusing on topics for all levels of business and their needs from cloud computing, security measures using social media, to securing technology to meet compliance standards in government contracting.

Free and confidential consulting and low cost workshops are available! Browse our resources and workshops at [www.pikespeaksbdc.org/cyber](http://www.pikespeaksbdc.org/cyber)

## Free Consulting | Practical Training | Cyber Resources

# Event Overview

COVID19 has had significant impacts on the community and especially for small businesses. Unfortunately, while business owners develop strategies to stay afloat, they are becoming vulnerable targets for many of the scams aimed at stealing what valuable resources they have left. In this session we will cover important information for business owners and consumers on how to protect yourself from scams and cyberattacks.



## FINANCIAL AND LEGAL SCAMS

COVID-19 CYBERSECURITY SCAMS  
& THE IMPACT ON SMALL  
BUSINESS

IN PARTNERSHIP WITH





# Dr. Shawn Murray

## SBDC LEAD Cybersecurity Consultant

### President

### Murray Security Services & Consulting

Shawn Murray is a Principal Scientist and the President/CEO at Murray Security Services. He is assigned to the U.S. Missile Defense Agency as a Senior Cyber Security Professional and is an officer in the U.S. Civil Air Patrol. Dr. Murray has worked with the NSA, FBI, CIA and the U.S. Defense and State Departments on various cyber initiatives and has over 20 years of IT, Communications, and Cyber Security experience.

#### Consulting Expertise Includes:

- Cybersecurity
- Risk & Information Systems Control
- Vulnerability Assessment
- Federal Information Technology
- Program Management
- CISSP

[View Consultant Bio or Schedule Consulting](#)



## Jonathan A. Liebert

CEO & Executive Director  
Better Business Bureau of Southern Co.

Jonathan is CEO and Executive Director of the Better Business Bureau of Southern Colorado and the Colorado Institute for Social Impact, BBB's recently restructured Foundation. Jonathan is a Colorado Springs native, a recognized Leader in Colorado by the Beanstalk Foundation, and a 2016 Rising Star Award recipient by the Colorado Springs Business Journal. In his current position since June 2015, Jonathan has increased awareness of the importance of integrity and trust in business, and has revitalized the BBB brand that has played a crucial role in our community for more than 35 years.

# Agenda

- SBA Loan Scams (PPP & EIDL)
- Stimulus Check Scam
- IT Impersonation Scams
- Phishing & Vishing Coronavirus Scams
- Fake Medical Supplies for Business Scams
- Top 5 Things You Can Do

# Top 5 Things You Can Do

- Report scams to [BBB.org/scamtracker](https://www.bbb.org/scamtracker)
- Think twice before you click!
- Do your homework
- Don't accept calls from strangers
- Be alert to scams that are out there



# Trusted Resources

- Report your scam to BBB: bbb.org/scamtracker
  - <https://www.bbb.org/scamtracker/>
  - Call your local BBB at 636-1155 and we will help give you more resources
- Helpful websites
  - <https://www.bbb.org/council/coronavirus/>
  - <https://www.fcc.gov/covid-scams>
  - <https://www.justice.gov/coronavirus>
  - <https://home.treasury.gov/services/report-fraud-waste-and-abuse/covid-19-scams>
  - <https://www.us-cert.gov/ncas/current-activity/2020/03/06/defending-against-covid-19-cyber-scams>
  - <https://www.fbi.gov/news/stories/protect-yourself-from-covid-19-scams-040620>
  - <https://us.norton.com/internetsecurity-online-scams-coronavirus-phishing-scams.html>



# Pikes Peak Small Business Development Center

FREE CONSULTING | PRACTICAL TRAINING | BUSINESS RESOURCES

[www.pikespeaksbdc.org](http://www.pikespeaksbdc.org)





# New Risks and Emerging Technologies

**2019**

**BBB Scam Tracker<sup>SM</sup>  
Risk Report**





# Table of Contents

4	Introduction
5	About BBB Scam Tracker <sup>SM</sup>
6	Snapshot of 2019
10	BBB Risk Index: A Three-Dimensional Approach to Measuring Scam Risk
11	10 Riskiest Scams of 2019
12	- Employment Scams Utilize a “High-Touch” Approach
13	- Cryptocurrency Scams Are on the Rise
14	- Top Product Categories of Online Purchase Scams
15	Demographics
15	- Age
17	- Gender
18	- Loneliness and Lacking Companionship Contribute to Financial Loss
20	- Geographic Area
21	Scam Delivery and Payment Methods
23	Spotlight on Military Families and Veterans
25	Spotlight on Students
26	Spotlight on Impersonated Organizations: Scammers Co-opt Household Brands to Deceive Their Targets
28	- Intervention by Front-Line Employees
29	Working Together to Stop Scammers
30	Conclusion
30	- About BBB Institute for Marketplace Trust
31	BBB Institute Research: Consumer Insights Shed Light on Victimization and Scammer Trends
32	Acknowledgments
33	Appendix A: Glossary of Scam Type Definitions
36	Appendix B: Scam Type Data Table
37	Appendix C: Top 10 Scam Types by Overall Risk, Exposure, Susceptibility, and Monetary Loss
38	Authors and Contributors



# Introduction

The BBB Institute for Marketplace Trust (BBB Institute), the educational foundation of the Better Business Bureau® (BBB), presents the *2019 BBB Scam Tracker Risk Report: New Risks and Emerging Technologies*. This annual report uses data submitted by consumers to BBB Scam Tracker<sup>SM</sup> ([BBB.org/ScamTracker](https://www.bbb.org/ScamTracker)). It sheds light on how scams are being perpetrated, who is being targeted, which scams have the greatest impact, and much more. Highlights of the 2019 report are provided in Figure 1.

BBB has been building trust between consumers and businesses for more than 100 years. The *BBB Scam Tracker Risk Report* is a critical component in our fight to create consumer awareness and reduce scams. Along with our ongoing research and educational programs, the BBB Institute aims to empower consumers and businesses to take action against fraud. Our efforts seek to limit the financial and emotional damage inflicted upon victims, and to create a level playing field where ethical businesses prosper. The very existence of BBB Scam Tracker empowers consumers to avoid scams and fraud; 21.8 percent of those who visited the crowd-sourced tool said BBB Scam Tracker helped them avoid a scam, with 60.4 percent saying they visited the site to see if a situation they were experiencing could be a scam.

The data and insights provided via BBB Scam Tracker tell the full story about the impact of scams. BBB Scam Tracker data enables us to explore differences in risk borne by particular subsets of the population and provide useful insights for creating effective messaging on how to avoid falling prey to scams. The BBB Risk Index (Figure 2) is a multidimensional approach to evaluating scam risk that considers three dimensions: exposure, susceptibility, and monetary loss. This information enables us to provide a more meaningful measure of the relative risk of a given scam type.

---

This report would not be possible without the consumers and business leaders who shared their stories via BBB Scam Tracker. Thanks to their willingness to come forward, we are able to provide valuable insights about how to stop fraudsters and prevent others from becoming scam victims. We extend our thanks to the more than 185,000 citizen heroes who chose to speak out by reporting scams.

---





## About BBB Scam Tracker<sup>SM</sup>

Data in the *2019 BBB Scam Tracker Risk Report* is provided via BBB Scam Tracker, an online tool that enables consumers and businesses to report scams and suspicious activities to BBB and warn others about similar cons. By using technology to collect information from consumers and businesses, and utilizing the power of our network of Better Business Bureaus working in communities across the United States and Canada, BBB Scam Tracker maximizes our efforts to educate consumers and stop fraudsters.

The scam reports submitted to BBB Scam Tracker are made available to the general public via an interactive website. The website features a searchable “heat map” that allows users to view the number and types of scams reported in their communities. This enables consumers and businesses to take action by sharing their knowledge and reporting fraudulent behavior they’ve encountered.

---

By working together, we can  
all fight back against scammers  
who steal billions of dollars and  
erode marketplace trust.

---



## Snapshot of 2019

In 2019, more than 37,000 scam reports were published on BBB Scam Tracker. Businesses and individuals across North America, representing a cross section of the population, filed these reports. We classified scam reports into 30 scam types (Appendix A) and an “other” category, which represented 5 percent of all reports. The data collected included a description of the scam, the dollar value of any loss, and information about the means of contact and method of payment.<sup>1</sup> The BBB Scam Tracker tool also collected optional demographic data—age, gender, and postal code—about the victim or target, along with military and/or student status. See Appendix B for more detailed data by scam type. The total number of scams reported to BBB Scam Tracker in 2019 declined to 37,283 from the 50,559 scams reported in 2018.

About 1.2 million people visited BBB Scam Tracker in 2019, and a January 2020 survey helped us understand how these individuals used the tool: 60.4 percent used BBB Scam Tracker to verify whether they were dealing with a potential scam. In addition, 20.4 percent wanted to protect themselves and their loved ones by proactively learning about scams happening in their area. **BBB Scam Tracker was able to save, per our initial estimates, \$42 Million in 2019 by helping 21.8 percent of unique visitors avoid being scammed.**

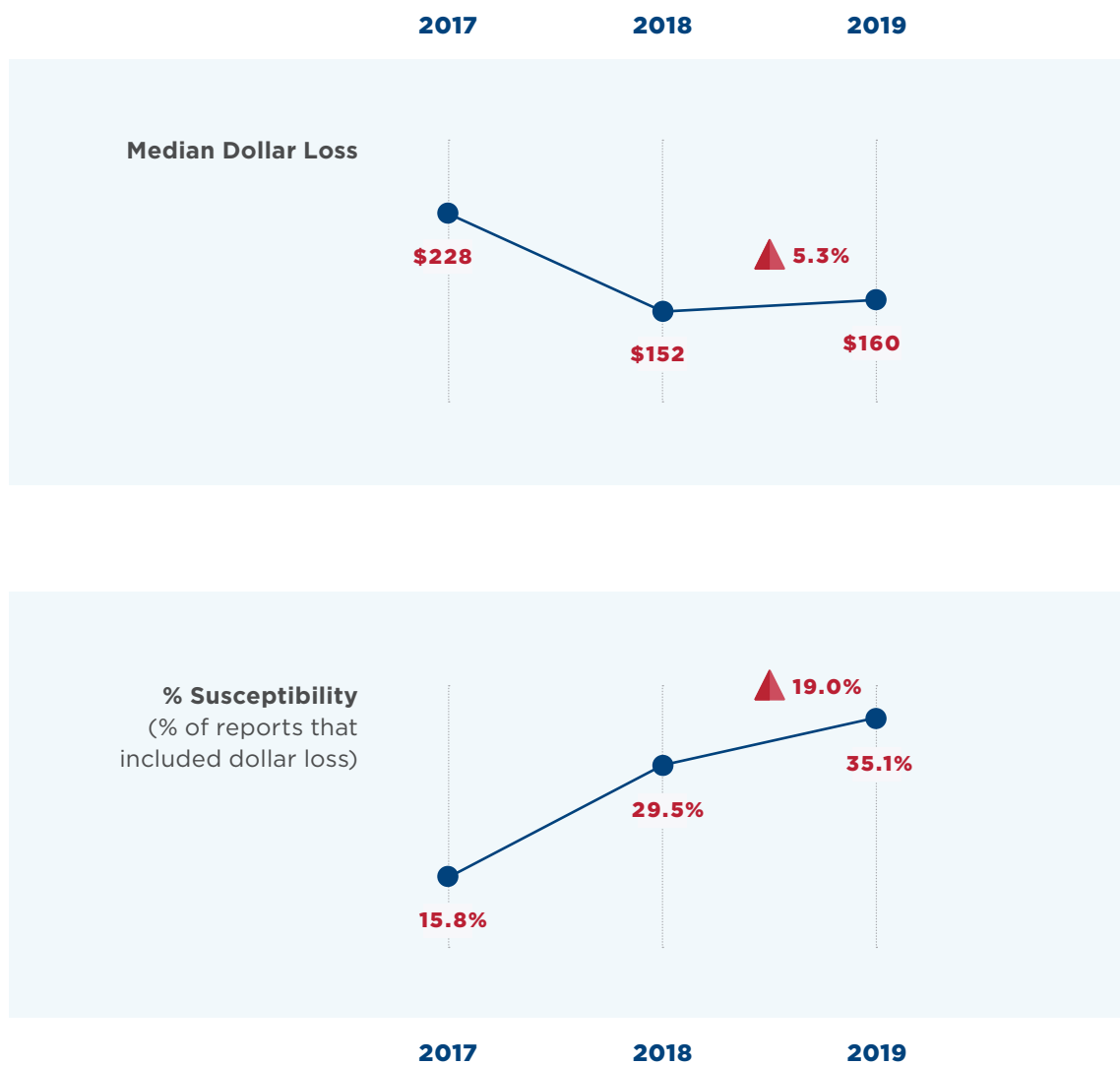
The impact of BBB Scam Tracker and the Better Business Bureau goes far beyond the tool itself. Our partnerships with local and national media resulted in 4,700 media mentions of BBB Scam Tracker in 2019 alone. In addition, local BBBs present workshops across the United States and Canada that reach vulnerable populations with limited or no access to online resources.

Both the overall reported median dollar loss and the susceptibility (the percentage of consumers who lost money when exposed to a scam) increased from 2018 to 2019, as shown in Table 1.

---

<sup>1</sup> All dollar values in this report have been converted to USD.




**TABLE 1****Snapshot of 2019  
Compared with 2017/2018**

The median dollar loss rose 5.3 percent, up from \$152 in 2018 to \$160 in 2019, but remained lower than in 2017, when it was \$228. More alarming is that consumers seem to be more likely to lose money when exposed to a scam. Susceptibility continues to climb, from 15.8 percent in 2017, to 29.5 percent in 2018, to 35.1 percent in 2019. This rise of 19.0 percent over last year, as well as the 122.2 percent increase since 2017, may be related to the rise in online purchase scams, which made up 24.3 percent of all scams reported to BBB Scam Tracker (up from 20.6 percent in 2018 and 9.7 percent in 2017). In 2019, a staggering 81.2 percent of consumers reported losing money to online purchase scams. This is extremely high when compared to the overall susceptibility of 35.1 percent.

A new scam category was added to BBB Scam Tracker in mid-2018 to account for reports involving cryptocurrencies. In 2019, these scams jumped from a small subsection of investment scams to the second riskiest scam for consumers overall. Cryptocurrency scams also tied romance scams for the highest median dollars lost, at \$3,000, up from \$900 in 2018. The reported scams were a combination of situations: 32.0 percent involved the purchase of cryptocurrencies as a form of payment for goods, services, or cash, and 23.4 percent involved the purchase of digital assets as an investment opportunity. The sites used to complete these exchanges varied, but 31.0 percent of cryptocurrency scams with a financial loss involved a company called C2CX, which is based in China (outside of BBB's North American purview).

The full report offers greater detail about specific scam types as well as the demographic groups that are most vulnerable to certain types of scams. We encourage readers to dig deeper into the data and insights provided here. More must be done to ensure consumers do not fall for the tactics and persuasions commonly used by scammers. The *2019 BBB Scam Tracker Risk Report* is one piece of a larger, multifaceted consumer education effort.



More must be  
done to ensure  
consumers do not  
fall for the tactics  
and persuasions  
commonly used  
by scammers.

FIGURE 1

## 2019 RISK REPORT HIGHLIGHTS

# 37,283 Scams

## REPORTED IN 2019

### RISKIEST SCAM BY AGE

18-54

EMPLOYMENT

55-64

ROMANCE

65+

TRAVEL/  
VACATION/  
TIMESHARE



#### EMPLOYMENT

was the **RISKIEST SCAM** for both men and women, as well as for students and military spouses



#### ONLINE PURCHASE

was both the **MOST COMMON SCAM** (largest exposure) and **SCAM TYPE WITH THE MOST VICTIMS** (highest susceptibility)



#### CREDIT CARD

##### TOP PAYMENT METHOD

used to pay scammers (2016-2019)



#### PHONE

##### TOP MEANS OF CONTACT

used to approach victims (2016-2019)

## THE 5 RISKIEST SCAMS

1

#### EMPLOYMENT



A job offer comes with high pay, options to work remotely, and flexible hours. To get the job, a candidate must complete forms that require personal and/or sensitive information and may be required to “purchase equipment” with part of the proceeds of what turns out to be a fake check.

2

#### CRYPTOCURRENCY



Cryptocurrency is purchased from, traded by, or stored with a person or exchange site that turns out to be fraudulent. Sometimes these digital assets are purchased as part of a fraudulent Initial Coin Offering (ICO), in which investors are scammed into paying money or trading digital assets for a company or product that never materializes.

3

#### ONLINE PURCHASE



A buyer makes a purchase online from an individual seller or company, but the item never arrives. Or, in other scenarios, a person sells an item online, but the check received for payment is fake.

4

#### FAKE CHECK/ MONEY ORDER



A check is sent to a consumer that contains an “accidental overpayment” or some other overage. The consumer is asked to wire back the excess money. The check appears real and “clears,” so the consumer thinks it is okay to withdraw funds, but weeks later the bank discovers the check is phony. The consumer now owes the withdrawn funds to the bank plus penalties and fees.

5

#### ADVANCE FEE LOAN



A loan is “guaranteed,” but comes with upfront charges, including taxes or “processing fees.” When the charges are paid, the loan never materializes and the applicant is left with larger debts.

# BBB Risk Index

## A Three-Dimensional Approach to Measuring Scam Risk

To better understand which scam types pose the highest risk, we assess scams on the basis of three factors: exposure, susceptibility, and monetary loss. By combining these three factors, we gain a more meaningful picture of scam risk that goes beyond merely the volume of reports received. This helps us better target our scam prevention outreach. We call this unique formula the BBB Risk Index (Figure 2).

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

The BBB Risk Index does not factor in the emotional and psychological harm scams can inflict or the damage done in diminishing trust between consumers and businesses. It does, however, provide a more accurate way to assess which scams have the largest effect on those reporting to BBB Scam Tracker—and helps track changes in risk from year to year.<sup>2</sup>

**FIGURE 2**

### BBB Risk Index

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

**Exposure x Susceptibility x (Median Loss / Overall Median Loss) x 1,000.**

The 2019 overall median loss was \$160.

### BBB RISK INDEX



#### 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 reported 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.

<sup>2</sup> It is important to acknowledge that no measure of risk is without limitations. The BBB Risk Index is calculated using data collected through BBB Scam Tracker, which is limited by the very nature of self-reporting as an imperfect measure of the extent of the problem. Because of the embarrassment associated with being a scam victim, it is likely that there is significant underreporting of scams. Moreover, although local BBBs review reports to determine whether they describe what a reasonable person would believe to be a scam, these reviews do not validate consumer allegations.

# 10 Riskiest Scams of 2019

Table 2 lists the 10 riskiest scam types based on all reports submitted to BBB Scam Tracker in 2019. The biggest change from 2018 to 2019 in the top 10 riskiest scams is the appearance of cryptocurrency scams for the first time as the second riskiest scam type. Cryptocurrency scams resulted in a median dollar loss of \$3,000 in 2019, up from \$900 in 2018; this is significantly higher than the overall median dollar loss of \$160. Employment scams are again the top riskiest scam type, with exposure, susceptibility, and median dollar loss up from 2018; the median dollar loss for these scams increased from \$1,204 in 2018 to \$1,500 in 2019. Online purchase scams dropped one place to the third riskiest, also with an increase in exposure, susceptibility, and median dollar loss. Investment, tech support, and romance scams all had notable increases in median dollar loss from data reported in 2018.

**TABLE 2**

## Riskiest Scams in 2019

RANK		SCAM TYPE	BBB RISK INDEX	EXPOSURE		SUSCEPTIBILITY		MEDIAN \$ LOSS	
2019	2018			2019	2018	2019	2018	2019	2018
1	1	Employment	153.6	9.3% ↑	9.1%	17.7% ↑	13.7%	\$1,500 ↑	\$1,204
2	NA	Cryptocurrency	93.8	0.7% ↑	0.3%	68.5% ↑	63.6%	\$3,000 ↑	\$900
3 ↓	2	Online Purchase	93.6	24.3% ↑	20.6%	81.2% ↑	75.2%	\$76 ↑	\$75
4 ↓	3	Fake Check/ Money Order	72.7	4.7% ↑	4.0%	16.6% ↑	14.6%	\$1,490 ↓	\$1,500
5	5	Advance Fee Loan	64.5	3.1% ↑	3.0%	41.8% ↓	42.8%	\$794 ↑	\$675
6	6	Romance	64.3	0.6% ↓	0.8%	53.6% ↑	44.4%	\$3,000 ↑	\$2,500
7 ↓	4	Home Improvement	64.2	1.0%	1.0%	60.1% ↑	52.8%	\$1,800 ↑	\$1,745
8	8	Investment	58.7	0.6% ↑	0.5%	61.4% ↓	62.4%	\$2,550 ↑	\$1,965
9 ↓	7	Tech Support	40.2	4.2% ↓	5.3%	30.7% ↓	31.7%	\$500 ↑	\$403
10 ↓	9	Travel/Vacation/ Timeshare	34.1	1.0%	1.0%	49.2% ↑	32.7%	\$1,097 ↓	\$1,875



## Employment Scams Utilize “High-Touch” Approach

Employment scams are a good example of a high-touch approach, where scammers take the time to prepare elaborate setups. Scammers conduct in-depth interviews via Google Hangouts and other online technologies, provide employment forms, and ask their targets to perform job duties before the scam is discovered. What makes these scams particularly risky is the fact that they made up 9.3 percent of all scams reported to BBB Scam Tracker in 2019. These scams often offer part-time, flexible jobs that fit within the growing gig economy.<sup>3, 4</sup> Employment scams result in a high median dollar loss, which has been increasing year over year: \$1,500 in 2019, up 24.6 percent from 2018 (\$1,204) and 87.5 percent from 2017 (\$800). Employment scams often involve other types of scams as well, especially fake check scams.

*Melissa, a college student from Wisconsin, shared her story with us. See page 25 for more about scams and students:*

“I received an email from Job Placement and Student Services at my school. The email was from a student account and stated that there was a job that was recruiting, looking for people who wanted a part-time job. They said how they had tried it and made \$300 and that you could make up to \$300 a week.... I figured since it was from my school it wouldn't be a scam (I had no idea the email system had actually been compromised). I went on the website and filled out an application and a few days later I was contacted via email and text from Jerome Harris, that they would be mailing information to my house. I received details in the mail...I would be a secret survey shopper for Best Buy and I also received a check for \$1,700. I was told to deposit the check and to buy Best Buy gift cards with it. They said if I did the survey within 48 hours of receiving it, I would make \$300, if I waited longer than that, I would make \$200. I went to Best Buy [the next day] and bought the \$1,400 of gift cards like they said. The clerk tried to warn me about these kinds of scams, but the letter said specifically not to tell anyone what the gift cards were for, or I would forfeit the secret shop—so I made up a different reason. They then told me to take a picture of the cards and the filled-out survey and text it to them. I did this and was told that they would be sending out my next assignment. I looked at my bank account today and saw the \$1,700 check had bounced, due to it being a fake. I had never heard of this scam before. **I would tell other students to double-check employment opportunities in-person with their schools and make sure it was actually sent from their office.**”

<sup>3</sup> Nearly one-third (32%) of employed Americans earned money from work outside of their main employment in 2018, with 17 percent taking on a work assignment through a gig economy website or app, according to the latest U.S. Financial Capability Survey. (FINRA Investor Education Foundation, 2019. [USFinancialCapability.org](https://www.finra.org/investor/education/survey))

<sup>4</sup> In 2016, participation in the gig economy was 8.2 percent of Canadian workers ages 15 and older—up from 5.5 percent in 2005, according to a 2019 study by Statistics Canada. <https://www150.statcan.gc.ca/n1/daily-quotidien/191216/dq191216d-eng.htm>

*Jose from Arizona shared his experience with a cryptocurrency scam:*

“I was scrolling my Instagram when a person named Elizabeth sent me a private message about cryptocurrency trading. I was desperate at that time and she got me interested because of the earnings. She [said she would] manage my account [and] do all the trading. She sent me the wallet address through WhatsApp, and from there I would go to a bitcoin ATM. To do the deposit initially I started at \$100, then later boosted it to \$150, and created a password and username on Fastcoinbitsoptions.com. I would deposit money to her bitcoin account and watch the money increase. The problem is I trusted her and that’s the lesson I’ve learned. They always say to “trust me.” After about two months I asked to withdraw the funds, and was shown a bank site, which looked fake. They told me I needed to pay \$500 to the bank for a code to withdraw the \$25,000 I had in my account. In total I lost about \$1,200 – I was so frustrated. **My advice is to talk to someone or a friend before making any [financial] decisions, especially during a desperate time. It was my mistake to keep this to myself.**”



## Cryptocurrency Scams Are on the Rise

Cryptocurrency scams rose to the second riskiest scam in 2019. With a median dollar loss of \$3,000, these scams are having a devastating impact on consumers. In some cases, consumers don’t quite understand these digital assets, enabling scammers to take advantage of them by convincing consumers they’ll make significant returns on an “investment.” Conversely, some scams occurred because consumers purchased, stored, or traded cryptocurrencies on an exchange site that was vulnerable to hackers. Unlike money stored in a traditional bank account, which is insured against theft, digital assets such as cryptocurrency cannot be retrieved and transactions cannot be reversed in the case of theft or cyber hacking.

With a median dollar loss of \$3,000, cryptocurrency scams are having a devastating impact on consumers.



## Top Product Categories of Online Purchase Scams

Online purchase scams, the third riskiest scam type in 2019, made up 24.3 percent of all scams reported to BBB Scam Tracker. The majority of online purchase scams occur when a payment is made online in exchange for goods and services, but the item ordered is never delivered. We applied the BBB Risk Index to rank these online purchase categories from most to least risky (Table 3).

The most common products promised but not delivered once payment was made included clothing/jewelry, home/furniture, and medical/nutrition. The highest median loss was for medical/nutrition at \$177 and pets (including pet supplies) at \$153, and was lowest for hobbies/sports.

**TABLE 3**

**Top Product Categories  
of Online Purchase Scams**

RANK	PRODUCT	DETAILS	EXPOSURE	SUSCEPTIBILITY	MEDIAN \$ LOSS
1	Clothing/ Jewelry	Clothing, jerseys, jewelry, shoes	31.2%	91.3%	\$50
2	Home/ Furniture	Lamps, rugs, clocks, blankets, candles	20.5%	92.2%	\$68
3	Medical/ Nutrition	Supplements/extracts for health, weight loss	7.2%	88.9%	\$177
4	Pets	Puppies, kittens, birds, exotic animals	7.1%	85.2%	\$153
5	Electronics/ Appliances	Cell phones, laptops, cases, headphones	9.8%	89.9%	\$60
6	Cosmetics	Skin creams, lotions, makeup, perfumes, soaps	8.9%	91.0%	\$60
7	Automobiles	Car, car parts, motorcycles	4.9%	69.6%	\$100
8	Tickets/ Events	Concert/event tickets	1.8%	93.1%	\$100
9	Hobbies/ Sports	Guns, bicycles, toys, collectibles	6.8%	85.5%	\$15
10	Food/ Beverage	Food and drink items	1.1%	100.0%	\$44
11	Information/ Media	Subscriptions or downloads of content	0.6%	90.0%	\$60



## Demographics

The collection of self-reported demographic data such as age, gender, and geographic location enhances our ability to identify individuals most at risk and helps us better understand how the nature of risk varies across different subgroups of the population. This information is utilized to enhance how we develop outreach and educational strategies. From there, we're able to create content, resources, and programming to empower consumers and businesses alike to identify and avoid scams.

### Age

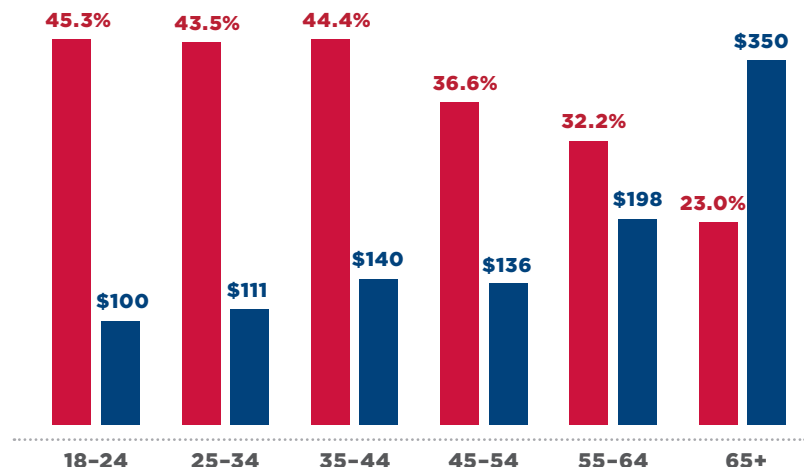
The data show a significant difference between older adults and younger adults, both in median dollar loss and susceptibility (Figure 3). An inverse relationship exists, where the median dollar loss increases with age (\$100 for ages 18-24 compared to \$350 for ages 65+) and susceptibility decreases with age (45.3% for ages 18-24 compared to 23.0% for ages 65+). This finding may be related to the types of scams different age groups are most susceptible to or are targeted by, or it may be related to differences in access to financial resources with increasing age. Table 4 highlights the three riskiest scams by age. Employment scams were the riskiest for ages 18 through 54. Cryptocurrency scams were the second riskiest scams for ages 25 through 44, whereas investment scams were the second riskiest for ages 45 through 64. Romance scams continued to be the riskiest scams for ages 55 through 64. Travel/vacation/timeshare scams rose to be the top riskiest for ages 65+.

**FIGURE 3**

### Susceptibility and Median Loss by Age

 **SUSCEPTIBILITY**

 **MEDIAN \$ LOSS**



**TABLE 4****3 Riskiest Scam Types  
by Age Range**

	1	2	3
<b>AGES 18-24</b>	Employment	Fake Check/ Money Order	Online Purchase
<b>AGES 25-34</b>	Employment	Cryptocurrency	Online Purchase
<b>AGES 35-44</b>	Employment	Cryptocurrency	Advance Fee Loan
<b>AGES 45-54</b>	Employment	Investment	Online Purchase
<b>AGES 55-64</b>	Romance	Investment	Home Improvement
<b>AGES 65+</b>	Travel/Vacation/ Timeshare	Home Improvement	Romance

## Gender

In 2019, 65.4 percent of reports to BBB Scam Tracker were submitted by women; 34.6 percent of reports were submitted by men. Overall, susceptibility to losing money when exposed to a scam was similar for both men and women at 35.5 and 35.7 percent, respectively. However, median dollar loss for women (\$130) remained substantially lower than that for men (\$239) (Figure 4). Similar to the differences in losses seen by age group, this may reflect gender differences in access to financial resources or differences in the types of scams that tend to impact women versus men. The three riskiest scams for men and women are listed in Table 5. Cryptocurrency scams appeared as the second most risky scam type for men, a change from 2018.

**FIGURE 4**

### Susceptibility and Median Loss by Gender

MEDIAN DOLLAR LOSS	GENDER	% SUSCEPTIBILITY
\$239	MEN	35.5%
\$130	WOMEN	35.7%

**TABLE 5**

### Riskiest Scam Types by Gender

	MEN	WOMEN
1	Employment	Employment
2	Cryptocurrency	Romance
3	Investment	Online Purchase



## Loneliness and Lacking Companionship Contribute to Financial Loss

Research conducted by BBB Institute, FINRA Investor Education Foundation, and the Stanford Center on Longevity found that feelings of loneliness were associated with being more likely to engage with and lose money to scammers—especially when the individual felt he or she lacked companionship and was isolated from loved ones.<sup>5</sup> In addition, the likelihood of losing money to a scammer is higher for individuals who are single, divorced, or widowed—as many felt they did not have anyone with whom to discuss their experiences and hesitations.

This contributes to romance scams being the riskiest for consumers ages 55 through 64 and the second riskiest scam type for women overall. Romance scams are also tied with cryptocurrency scams for the highest median dollar loss of all scam types in 2019 at \$3,000. **For individuals feeling isolated or alone who suspect a potential romantic partner is suspicious, we recommend they reach out to a friend, neighbor, or their local BBB. Never send money to a person you have never met.**

### *Rosemary from Illinois wanted to warn other women of romance scams by sharing her story:*

“This started over a dating website called OurTime.com back in March 2018. A man named Frederick Boyd contacted me through their website, and a few weeks later asked if we [could] exchange phone numbers and take our profiles off of the site, as he told me that I was the one he was interested in and was attracted to me. He seemed sincere to me, and we started communicating via email, and eventually he contacted me via phone. In April 2018 he informed me that he was going to South Africa, and taking his daughter (who was 17 then, as he told me he got divorced in 2011 and that his wife died in 2013 [from] drugs and alcohol) to do a construction project worth over \$2 million to redesign an art museum. He said he would be gone for a few months, and that we would meet when he returned. Well, during his trip things came up. He first started asking me to buy him iTunes cards worth \$600 for his equipment. I hesitated, but sent copies of the numbers to him. I didn’t pay attention to the red flags. The next story was that his daughter ended up in the hospital while they were in South Africa due to drinking contaminated water. He needed money to help her get released from the hospital. After that, back in May 2018, his daughter contacted me stating that he sent her back home, and that he had to stay on in South Africa. He [then] stated that he was being sued by family members of an employee who got hurt on the job. He kept asking for money to be sent via wire transfers for help in legal fees. He told me he had to find a good lawyer in South Africa. I sent money via the wire transfers but got angry with him several times as

<sup>5</sup> *Exposed to Scams: What Separates Victims from Non-Victims?*  
[BBB.org/ExposedToScams](https://www.bbb.org/ExposedToScams)

I was waiting to be paid back [and] I was going into debt. A few coworkers even informed me that this man was suspicious by his emails and that he wanted me to transfer money from an account. He kept promising me that he would pay me back every cent if I would help him as he had to get back home. When he [supposedly] got back to Houston, TX, where he said he lives, he then stated that he was held up in customs due to his Swiss passport not being renewed, and that he needed \$8,200 to renew it plus \$10,000 allowance money to get through customs. He told me they transferred him to Dallas to be detained until he could be stamped to get released. I sent some money, and he told me his mom helped him also...Well I found out (too late) that his Swiss passport was fake. The Swiss Embassy in Atlanta, GA, confirmed to me that it was a fake passport, and a bad one at that. The total loss from Frederick Boyd was about \$80,000 and it cost me plenty as I still have outstanding debts from this scammer. I cannot reach him as he blocked me on his phone, and I have not received any more text messages or messages from his [email]. The last time I spoke to him was in August 2019. I have reported him to OurTime.com and they are having their security team check on this person. I have also reported this to the FBI Crime Bureau, and the Federal Trade Commission...I wish I could retrieve some of my money back. **I would suggest to women to listen to their gut feelings, and be careful. Don't give out any money even if you think it is sincere."**

► Women and Consumers Ages 55-64 Need to Be Especially Vigilant About Romance Scams

## Geographic Area

As shown in Figure 5, scams show some variability by region. In Canada, for example, the riskiest scam was travel/vacation/timeshare scams, with advance fee loan scams the second riskiest. These scams are on the top 10 list overall, but they had a more pronounced impact on Canadian consumers.<sup>6</sup> This may be an indication that scammers are more active in certain areas and may also reflect demographic and socioeconomic differences by regions that in turn correlate with different types of scams and levels of susceptibility and loss. It is important to note that the data points refer to the location of the person reporting the scam, not the location of the perpetrator of the scam. Although location information about perpetrators is provided in some cases, the accuracy of this information varies because most victims and targets are uncertain about the location of the perpetrator and are often given false information with respect to the scammer's location.

**FIGURE 5**

### Riskiest Scam Types by Geographic Area

#### UNITED STATES

##### West

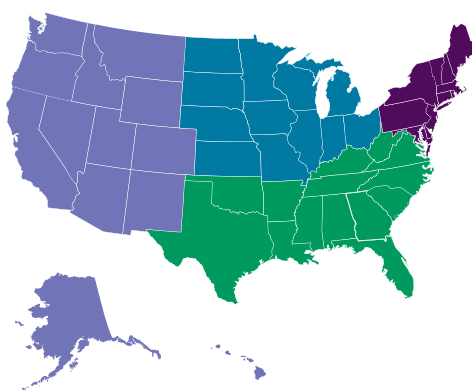
Median \$ Loss: **\$175**

Riskiest Scam:  
**Employment**

##### Midwest

Median \$ Loss: **\$115**

Riskiest Scam:  
**Romance**



##### Northeast

Median \$ Loss: **\$218**

Riskiest Scam:  
**Cryptocurrency**

##### South

Median \$ Loss: **\$170**

Riskiest Scam:  
**Employment**

#### CANADA\*

##### Western & Northern

Median \$ Loss: **\$377**

Riskiest Scam:  
**Travel/Vacation/Timeshare**



##### Northeast

Median \$ Loss: **\$603**

Riskiest Scam:  
**Advance Fee Loan**

*\* All dollar amounts have been converted to USD.*

<sup>6</sup> Visit [BBB.org/RiskReport](https://www.bbb.org/RiskReport) to view the 2019 Canadian Risk Report, which contains additional scam data specifically relevant to Canadian consumers.

## Scam Delivery and Payment Methods

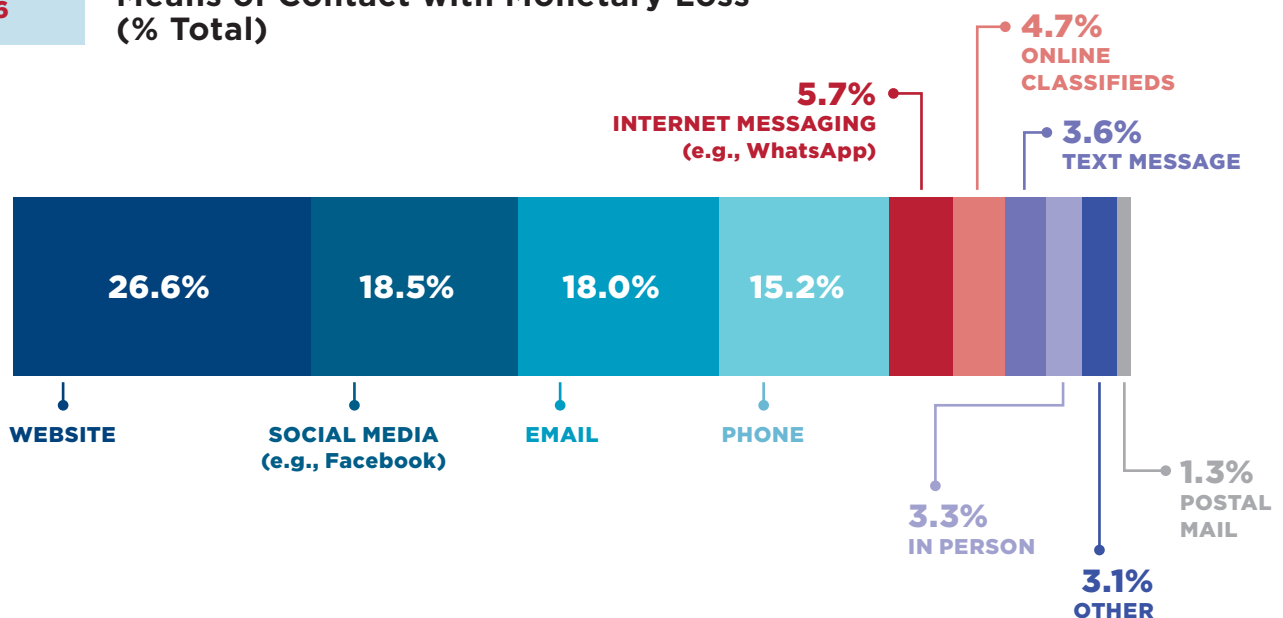
Scammers continued to use the latest technologies to perpetrate scams in 2019. Delivery methods that resulted in a monetary loss are listed in Figure 6. The top three delivery methods used online tactics (website, social media, and email), make up 63.1 percent of scams in which the victim lost money. Once again, email (18.0 percent) eclipsed phone (15.2 percent) as a scam delivery tactic resulting in a monetary loss. Website was again the top delivery method resulting in a monetary loss, at 26.6 percent.

Credit cards (37.8%) remained the top payment method requested by scammers in 2019 (Figure 7). Online payment systems were the second most requested payment type—up from 13 percent in 2018 to 19.7 percent in 2019. Payments by prepaid card, wire transfer, check, cash, and money order decreased by approximately 1 percent each from 2018 to 2019.

Data reported in 2019 (Figure 8) again shows that consumers who are approached online (email, website, social media, internet messaging, and online classifieds) are significantly more likely to report losing money. If approached by phone or in person, they are less likely to report losing money.

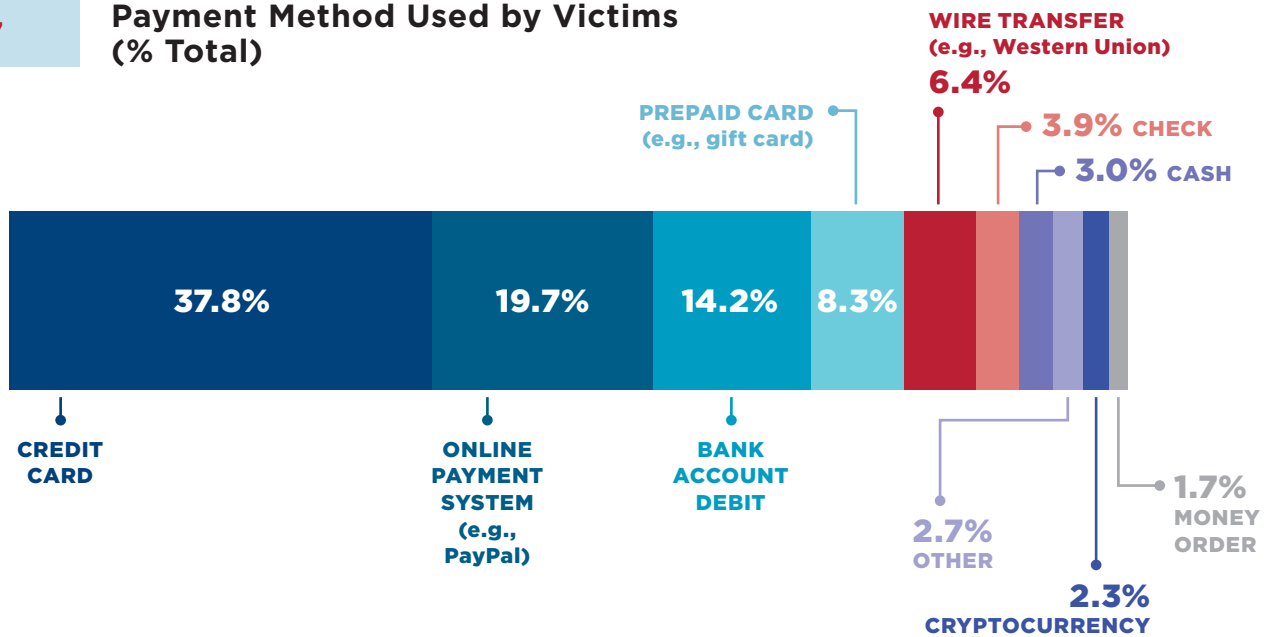
**FIGURE 6**

### Means of Contact with Monetary Loss (% Total)



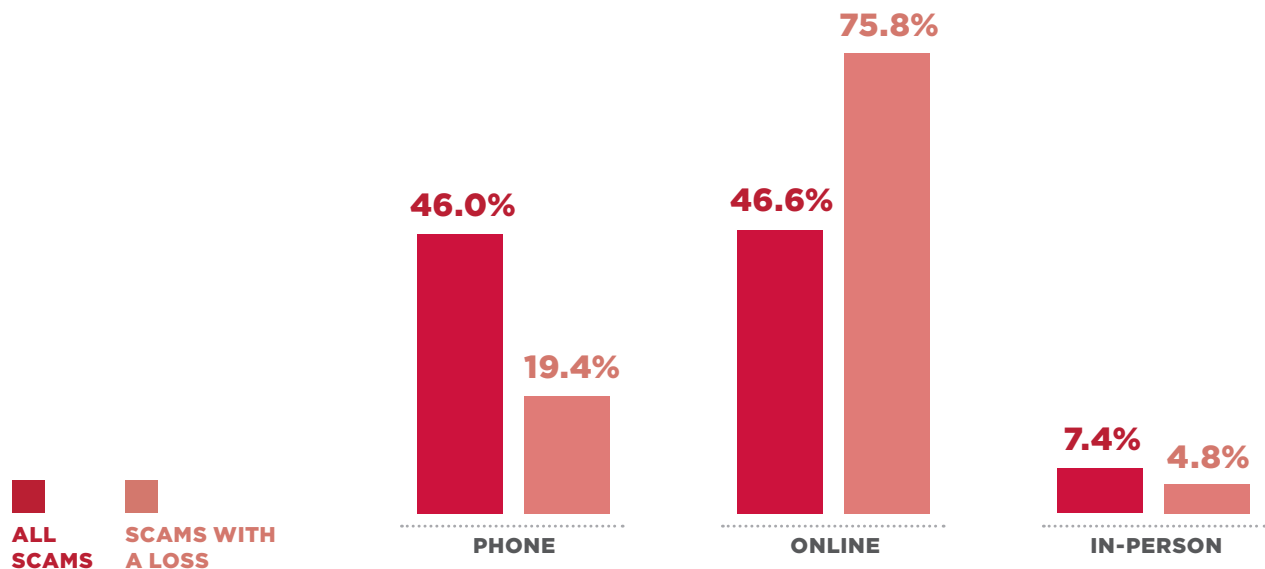
**FIGURE 7**

**Payment Method Used by Victims  
(% Total)**



**FIGURE 8**

**All Scams Compared with Scams with a Loss (% Total)  
by Means of Contact**



*Note: Categories include Phone (phone + text messaging), Online (email + website + social media + internet messaging + online classifieds), and In Person (in person + postal mail + fax).*





## Spotlight on Military Families and Veterans

Members of the military community, including veterans, are at an increased risk of becoming a target for scammers. Service members are often young and have a steady paycheck. Military families may be required to put faith in others while juggling deployment and frequent moves, which leaves them particularly vulnerable. Individuals who self-identified as being active-duty military personnel, spouses, or veterans represent 10.1 percent of reports submitted to BBB Scam Tracker in 2019. Although the susceptibility of the military community was slightly less than the susceptibility of non-military, the median dollar loss was 32.5 percent higher at \$200 (Figure 9).

**FIGURE 9**

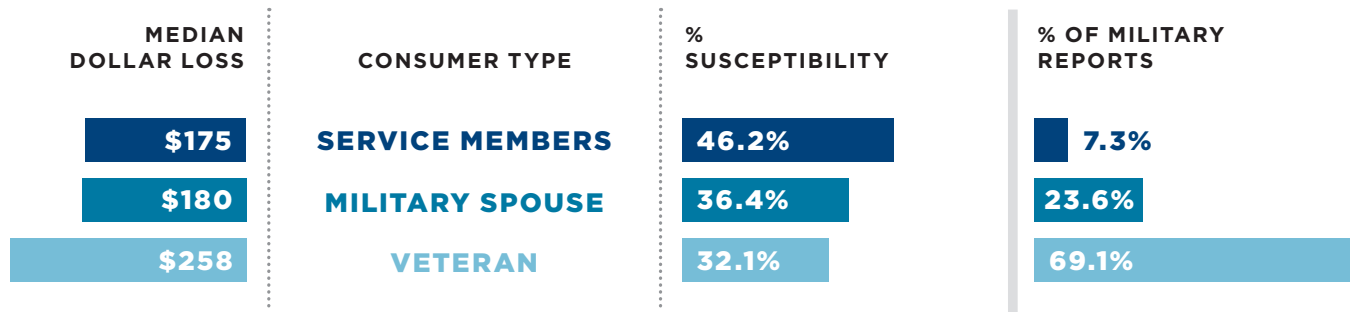
### Median \$ Loss and Susceptibility of Military Families and Veterans versus Non-Military

MEDIAN DOLLAR LOSS	CATEGORY	% SUSCEPTIBILITY
<b>\$200</b>	<b>MILITARY</b>	<b>34.2%</b>
<b>\$151</b>	<b>NON-MILITARY</b>	<b>35.2%</b>

We added an additional question to BBB Scam Tracker in August 2018 to segment the data between service members, military spouses, and veterans; this allowed us to get a better understanding of the impact of scams on the military community in 2019. As noted in Figure 10, service members reported an increased frequency of losing money to scammers at 46.2 percent—31.3 percent higher than non-military consumers. Conversely, veterans reported losing significantly more money to scammers, with a median dollar loss of \$258—over \$100 higher than the loss by non-military consumers. This could be attributed to the age of these individuals: younger consumers are more susceptible to scams but lose less money than older consumers (see page 15).

**FIGURE 10**

### Median \$ Loss and Susceptibility of Military Consumers



The BBB Risk Index was then applied to identify the three riskiest scams for military spouses and veterans (Table 6). Reports by service members were spread out among the 30 scam types, with only online purchase scams having a significant quantity of scam records (35.7%). Not surprisingly, employment scams remained high on the list for both military spouses and veterans. What is interesting, however, is that for military spouses, government grants were the second riskiest scam—a scam type that did not make the top 10 list overall in 2019. With military consumers reporting higher financial losses to scams, we must ensure that scam prevention education and resources are available to those who bravely serve or have served in the U.S. and Canada.

**TABLE 6**

### 3 Riskiest Scams: Military Spouses and Veterans versus Non-Military

	MILITARY SPOUSES	VETERANS	NON-MILITARY
1 .....	Employment	Travel/Vacation/ Timeshare	Employment
2 .....	Government Grant	Employment	Cryptocurrency
3 .....	Online Purchase	Online Purchase	Online Purchase

## Spotlight on Students

Individuals who self-identified as students represented 9.1 percent of reports submitted to BBB Scam Tracker in 2019. As reported in past reports, students continue to be more vulnerable when exposed to a scam: 44.7 percent of students reported a loss when exposed to a scam as compared to 34.2 percent of non-students (Figure 11). However, the median dollar loss of \$100 for students is significantly lower than the median dollar loss for non-students of \$173. This trend is similar to findings in the past few reports and may reflect differences in the scam types to which students are most vulnerable as well as differences in access to funds. It should be noted that the susceptibility rate and median dollar losses for students are similar to those of the overall 18-24 age category into which most students fall. Table 7 includes the riskiest scams for students, which remained the same as reported in the 2018 report.

**FIGURE 11**

### Median \$ Loss and Susceptibility of Students versus Non-students

MEDIAN DOLLAR LOSS	CATEGORY	% SUSCEPTIBILITY
\$100	STUDENT	44.7%
\$173	NON-STUDENT	34.2%

**TABLE 7**

### 3 Riskiest Scams: Students versus Non-students

	STUDENT	NON-STUDENT
1	Employment	Employment
2	Fake Check/Money Order	Online Purchase
3	Online Purchase	Cryptocurrency



# Spotlight on Impersonated Organizations

## Scammers Co-opt Household Brands to Deceive Their Targets

“Impersonation” is one of the most common tactics fraudsters use to perpetrate scams. By pretending to be well-known and trusted companies, government agencies, and organizations, scammers can better manipulate their targets. Scams impersonating the Social Security Administration rose sharply in 2019, overtaking the Internal Revenue Service as the top impersonated organization in 2018. Table 8 includes the most impersonated organizations in 2019.



### Social Security Scams

The fraudster pretends to represent the Social Security Administration, misleading victims into making cash or gift card payments to avoid arrest for problems with their Social Security number.



### Sweepstakes, Lottery, Prize Scams

The scammer pretends to represent a well-known company that distributes sweepstakes or lottery winnings, such as Publishers Clearing House.



### IRS Scams

The scammer pretends to represent the Internal Revenue Service or Canada Revenue Agency.



### Travel/Vacation Scams

The scammer pretends to represent a well-known travel brand.



### Phishing and Government Grant Scams

The scammer pretends to represent a government agency.



### Credit Card Scams

The scammer pretends to represent a well-known bank or credit card company.



### Tech Support Scams

The scammer pretends to represent a well-known technology company such as Microsoft or Apple.

**TABLE 8****Top 15 Legitimate Organizations/Brands  
Used for Impersonation**

<b>1</b>	<b>Social Security Administration</b>	<b>1,963</b>
<b>2</b>	<b>Publishers Clearing House</b>	<b>444</b>
<b>3</b>	<b>Microsoft</b>	<b>367</b>
<b>4</b>	<b>U.S. Internal Revenue Service</b>	<b>251</b>
<b>5</b>	<b>Apple</b>	<b>244</b>
<b>6</b>	<b>Amazon</b>	<b>194</b>
<b>7</b>	<b>Medicare</b>	<b>193</b>
<b>8</b>	<b>Walmart</b>	<b>156</b>
<b>9</b>	<b>Cash Advance/Advance America</b>	<b>125</b>
<b>10</b>	<b>Better Business Bureau</b>	<b>111</b>
<b>11</b>	<b>Facebook</b>	<b>107</b>
<b>12</b>	<b>U.S. Treasury</b>	<b>60</b>
<b>13</b>	<b>PayPal</b>	<b>56</b>
<b>14</b>	<b>Dominion Energy</b>	<b>54</b>
<b>15</b>	<b>Capital One</b>	<b>33</b>



***Deborah from Virginia was able to spot and avoid losing money to a Microsoft imposter scam:***

“I was sitting at home when my newly purchased computer started making a noise louder than a smoke alarm. It was so frightening! The screen indicated for me to call Microsoft Technical Support and provided a phone number. At the time, I wasn’t thinking clearly and thought I didn’t do something correctly since I had just purchased it, so I gave them a call. I let them gain control of my computer, and he said he would apply the necessary virus protection. Then, he said it was going to cost \$199, told me to get in the car, keep him on the phone, and go to the nearest Walmart to buy a gift card to cover the purchase price. When he asked where I lived, every hair on my neck stood up. I was so uncomfortable. I immediately shut down my computer and hung up. I later found out the software he installed was to track my online purchases and see everything I typed on the screen! I had my IT person at work help me remove the software. **Now, I’m always telling my friends and family: if that alarm sounds, just shut it down! Go report it to the BBB!**”

▶ 51% of people who reported a third-party intervention were able to avoid losing money.<sup>7</sup>

### **Intervention by Front-Line Employees**

Research published by BBB Institute, FINRA Investor Education Foundation, and Stanford University in the fall of 2019 found that among people who engaged with a scammer, 20 percent reported that an employee or representative from a company tried to intervene to stop the scam. Often, these are bank tellers or front-line employees who have been trained to recognize indicators of fraud. The report found that 51 percent of people who reported a third-party intervention were able to avoid losing money. This is a promising finding—and we encourage cashiers, bank tellers, and other vigilant employees to alert consumers who might otherwise become fraud victims.

<sup>7</sup> *Exposed to Scams: What Separates Victims from Non-Victims?*  
[BBB.org/ExposedToScams](https://www.bbb.org/ExposedToScams)



## Working Together to Stop Scammers

Although scams and scammers continue to plague the marketplace, consumers can learn key strategies that will enable them to avoid falling prey to scams. In fact, 64.9 percent of reports to BBB Scam Tracker in 2019 were from non-victims.

One of the top tips to avoid becoming a victim is to never rush to take action: go online and do a quick search to see if the situation could be fraudulent. A January 2020 survey of BBB Scam Tracker viewers revealed 60.4 percent said the primary reason they visited the site was to verify whether they were dealing with a potential scam. In addition, 20.4 percent wanted to protect themselves and their loved ones by proactively learning about scams happening in their area.

Together, we can empower all consumers to pause, assess, and report scams. BBB Scam Tracker and BBBs serving communities across North America will continue to educate consumers to avoid scams 24/7/365. By partnering with companies and like-minded organizations to distribute research and important fraud prevention tactics, responding to inquiries from consumers and businesses, and presenting workshops across the United States and Canada we can protect vulnerable populations who do not have access to online resources.

---

Thank you to the tens of  
thousands of citizen heroes  
who took the time to help  
us in the fight to stop  
scammers.

---



## Conclusion

Scams undermine trust in the marketplace, distort the level playing field, and siphon money from legitimate transactions that benefit both businesses and consumers, thus impeding economic growth. A person who has been scammed not only has less money to spend in the market but also may shy away from engaging with new businesses in the future. In addition, a business whose trustworthy brand has been impersonated by scammers may find its customers have a reduced trust in its brand. A healthy marketplace requires empowered and aware consumers and principled businesses that are proactively working to stop scammers.

The *2019 BBB Scam Tracker Risk Report* is a critical part of our ongoing work to contribute new, useful data and analysis to further the efforts of all who are engaged in combating marketplace scams. We are working with top officials in business, law enforcement, and government to determine the best ways to stop scammers, and we partner with corporate partners and like-minded organizations to better allocate resources to tackle the problem and determine which prevention tactics are working and improve upon the tactics that are not. BBB Institute will continue its work to reduce the impact of scams to help consumers and legitimate businesses prosper in a trustworthy marketplace.

### ABOUT BBB INSTITUTE



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 by BBBs serving communities across North America. You can find more information about BBB Institute and its programs at [BBBMarketplaceTrust.org](https://BBBMarketplaceTrust.org).



## Consumer Insights Shed Light on Victimization and Scammer Trends

The 2019 *BBB Scam Tracker Risk Report* is the fourth annual report published by BBB Institute that highlights the year's riskiest scams. We are committed to delivering new and timely research that enables us to continue creating and delivering programs that empower both consumers and businesses to avoid falling prey to scams.

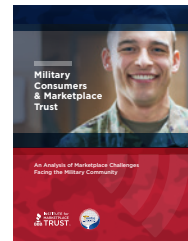


### *Exposed to Scams: What Separates Victims from Non-Victims?*

To better understand the fraud victimization process and craft better interventions to reduce fraud, BBB Institute

collaborated with the FINRA Foundation, Stanford Center on Longevity, and Federal Trade Commission to explore the cognitive, behavioral, and attitudinal differences between victims and non-victims.

**Download at:** [BBB.org/ExposedToScams](https://www.bbb.org/exposedtoscams)



### *Military Consumers & Marketplace Trust: An Analysis of Marketplace Challenges Facing the Military Community*

This report examines the tens of thousands of business

complaints and scams reported to the BBB in 2018 by military consumers to analyze the unique pain points of service members, veterans, and military families when engaging with businesses.

**Download at:** [BBB.org/MilitaryReport](https://www.bbb.org/militaryreport)

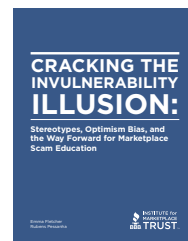


### *Scams and Your Small Business*

The Council of Better Business Bureaus teamed up with BBB Institute in 2018 to analyze both BBB Scam Tracker

data and insights from an outside panel of small business owners to shed light on the scams targeting small businesses.

**Download at:**  
[BBB.org/SmallBizScams](https://www.bbb.org/smallbizscams)



### *Cracking the Invulnerability Illusion: Stereotypes, Optimism Bias, and the Way Forward for Marketplace Scam Education*

Our first research report surveyed consumers in

the United States and Canada to identify the stereotypes and misperceptions around scam victimization that are a barrier to effective outreach to at-risk populations.

**Download at:**  
[BBBMarketplaceTrust.org/Resources#research](https://www.bbbmarketplacetrust.org/resources#research)



# Acknowledgments

The BBB Scam Tracker tool utilizes the strength of the 100-year-old BBB brand to collect data from people who have been targeted by fraudsters. The BBB Scam Tracker program and our research are possible thanks to the dedicated, collaborative work of BBBs. We harness the power of BBBs across North America to review these consumer reports to eliminate those that do not appear to be actual scams, thus ensuring the best data possible. Our system collects data as well as real-life narratives told in the words of the victims themselves.

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 of the BBB Serving Western Pennsylvania; Jane Rupp, president and CEO of the BBB Serving Northern Nevada and Utah; Craig Turner, director of information systems of the BBB Serving Eastern & Southwest Missouri & Southern Illinois; Dené Joubert, investigations manager of the BBB Serving Northwest + Pacific; Jon Bell, the director of business relations of the BBB Serving Delaware; David Wheeler, vice president of innovation and development of the BBB Serving Central Florida; and Yolanda Moore, investigations director of the BBB Serving Western Pennsylvania.

We would also like to thank the International Association of Better Business Bureaus for its support of BBB Institute and the *2019 BBB Scam Tracker Risk Report*. Special thanks to Dr. Rubens Pessanha, MBA, PMP, SPHR, GPHR, SHRM-SCP, senior director, research & development, International Association of Better Business Bureaus (IABBB); Matt Scandale, IABBB senior data analyst; and Sean Xiangwen Lai, IABBB research and development specialist, for analyzing the data from BBB Scam Tracker for this report. We'd also like to thank Katherine Hutt, IABBB chief communications officer, as well as Sandra Guile, IABBB director of communications, for their efforts to get the word out about our most recent findings, and Jody Thomas, IABBB director of brand management, for her insights and input.

## APPENDIX A: Glossary of Scam Type Definitions

Scams reported to BBB Scam Tracker this year were classified into 30 scam types, plus an “other” category; in December 2019, the categories were split into scams targeting consumers (27) and scams targeting businesses (13), which will be reflected in the 2020 report. These classifications represent common scams seen by BBB over time 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 percent of all scams reported to BBB Scam Tracker can be classified into one of these general types.

<b>ADVANCE FEE LOAN</b>	A loan is guaranteed, but once the victim pays up-front charges such as taxes or a “processing fee,” the loan never materializes.
<b>BUSINESS EMAIL COMPROMISE</b>	This financial fraud targets businesses engaged in international commerce. Scammers gain access to company email and trick employees into sending money to a “supplier” or “business partner” overseas.
<b>CHARITY</b>	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.
<b>COUNTERFEIT PRODUCT</b>	Counterfeit products 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.
<b>CREDIT CARD</b>	This con typically involves impersonation of a bank or other credit card issuer. By verifying account information, con artists try to fool their targets into sharing credit card or banking information.
<b>CREDIT REPAIR/ DEBT RELIEF</b>	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.
<b>CRYPTO-CURRENCY</b>	These scams involve the purchase, trade, or storage of digital assets known as cryptocurrencies. The situation will often involve fraudulent Initial Coin Offerings (ICOs), a type of fundraising mechanism in which a company issues its own cryptocurrency to raise capital. Investors are scammed into paying money or trading their own digital assets when the scammer has no intention of building a company. Cryptocurrency scams also involve scenarios in which investors store their cryptocurrencies with fraudulent exchanges.
<b>DEBT COLLECTION</b>	Phony debt collectors harass their targets to get them to pay debts they don’t owe.
<b>EMPLOYMENT</b>	Job applicants are led to believe they are applying or have just been hired for a promising new job when instead they have given personal information 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.

## APPENDIX A: Glossary of Scam Type Definitions

<b>FAKE CHECK/ MONEY ORDER</b>	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.
<b>FAKE INVOICE</b>	This scam targets businesses. Employees are conned into paying for products that the business did not order and that may not even exist. Fake invoices are often submitted for office supplies, website or domain hosting services, and directory listings.
<b>FAMILY/FRIEND EMERGENCY</b>	This scheme involves the impersonation of a friend or family member in 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.
<b>FOREIGN MONEY EXCHANGE</b>	The target receives an email from a foreign government official, member of royalty, or a business owner offering a huge sum of money to help get money out of the scammer’s country. The victim fronts costs for the transfer, believing that they will be repaid.
<b>GOVERNMENT GRANT</b>	Individuals are enticed by promises of free, guaranteed government grants. The only catch is a “processing fee.” Other fees follow, but the promised grant never materializes.
<b>HEALTH CARE, MEDICAID, AND MEDICARE</b>	These schemes vary, with many attempting to defraud private or government health care programs. The con artist is often after the insured’s health insurance, Medicaid, or Medicare information to submit fraudulent medical charges or for purposes of identity theft.
<b>HOME IMPROVEMENT</b>	Door-to-door solicitors offer quick, low-cost repairs and then either take payments 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.
<b>IDENTITY THEFT</b>	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.
<b>INVESTMENT</b>	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.
<b>MOVING</b>	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.
<b>ONLINE PURCHASE</b>	These cons often involve purchases and sales on eBay, Craigslist, or other direct seller-to-buyer sites. Scammers may pretend to purchase an item only to send a bogus check and ask for a refund of the “accidental” overpayment. In other cases, if the scammer is the seller, they never deliver the goods.

## APPENDIX A: Glossary of Scam Type Definitions

<b>PHISHING</b>	These schemes employ communications impersonating a trustworthy entity, such as a bank or mortgage company, intended to mislead the recipient into providing personal information with which the scammer can gain access to bank accounts or can steal the recipient's identity. This type of scheme can also happen within the workplace as an email coming from the CEO, accounting, or other member of management seeking personal information.
<b>RENTAL</b>	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.
<b>ROMANCE</b>	An individual believing he/she is in a romantic relationship is tricked into sending money, personal and financial information, or items of value to the perpetrator.
<b>SCHOLARSHIP</b>	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.
<b>SWEEPSTAKES, LOTTERY, AND PRIZE</b>	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.
<b>TAX COLLECTION</b>	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 up or sharing personal information.
<b>TECH SUPPORT</b>	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 of well-known tech companies hassle victims into paying for "support." If the victim allows remote access, malware may be installed.
<b>TRAVEL/ VACATION/ TIMESHARE</b>	Con artists post listings for properties that are not for rent, that do not exist, or that 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.
<b>UTILITY</b>	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.
<b>YELLOW PAGES/ DIRECTORY</b>	Businesses are fooled into paying for a listing or ad space in a nonexistent directory or "Yellow Pages." In some cases, the directory technically exists but is not widely distributed and a listing is of little or no value; these directories are essentially props in the scammer's ploy.

## APPENDIX B: Scam Type Data Table

SCAM TYPE	# OF REPORTS	% EXPOSURE	% SUSCEPTIBILITY	MEDIAN \$ LOSS	RISK INDEX	TOP MEANS OF CONTACT	TOP PAYMENT METHOD
Advance Fee Loan	1,160	3.1%	41.8%	\$794	64.5	Phone	Prepaid Card
Business Email Compromise	179	0.5%	31.8%	\$300	2.9	Email	Credit Card
Charity	200	0.5%	32.5%	\$150	1.6	Phone	Credit Card
Counterfeit Product	942	2.5%	65.6%	\$100	10.4	Website	Credit Card
Credit Card	815	2.2%	33.0%	\$100	4.5	Phone	Credit Card
Credit Repair/Debt Relief	543	1.5%	30.2%	\$800	22.0	Phone	Bank Account Debit
Cryptocurrency	273	0.7%	68.5%	\$3,000	93.8	Email	Cryptocurrency
Debt Collection	1,698	4.5%	11.9%	\$450	15.2	Phone	Credit Card
Employment	3,461	9.3%	17.7%	\$1,500	153.6	Email	Other
Fake Check/Money Order	1,758	4.7%	16.6%	\$1,490	72.7	Email	Prepaid Card
Fake Invoice/Supplier Bill	848	2.3%	20.4%	\$269	7.8	Postal Mail	Credit Card
Family/Friend Emergency	177	0.5%	14.1%	\$2,000	8.3	Phone	Prepaid Card
Foreign Money Exchange	135	0.4%	5.2%	\$500	0.6	Postal Mail	Prepaid Card
Government Grant	1,278	3.4%	14.1%	\$900	27.2	Social Media	Prepaid Card
Health Care, Medicaid, Medicare	859	2.3%	6.4%	\$250	2.3	Phone	Credit Card
Home Improvement	356	1.0%	60.1%	\$1,800	64.2	In Person	Check
Identity Theft	1,199	3.2%	9.9%	\$400	8.0	Phone	Credit Card
Investment	223	0.6%	61.4%	\$2,550	58.7	Phone	Online Payment System
Moving	127	0.3%	78.0%	\$100	1.7	Website	Credit Card
Online Purchase	9,050	24.3%	81.2%	\$76	93.6	Website	Credit Card
Phishing	5,188	13.9%	4.8%	\$350	14.7	Phone	Credit Card
Rental	303	0.8%	41.3%	\$1,000	20.9	Email	Online Payment System
Romance	237	0.6%	53.6%	\$3,000	64.3	Social Media	Wire Transfer
Scholarship	18	0.0%	33.3%	\$775	0.8	Phone	Prepaid Card
Sweepstakes, Lottery, Prize	1,540	4.1%	9.2%	\$900	21.3	Phone	Prepaid Card
Tax Collection	433	1.2%	3.2%	\$363	0.8	Phone	Credit Card
Tech Support	1,558	4.2%	30.7%	\$500	40.2	Phone	Credit Card
Travel/Vacation/Timeshare	378	1.0%	49.2%	\$1,097	34.1	Phone	Credit Card
Utility	433	1.2%	6.7%	\$506	2.5	Phone	Prepaid Card
Yellow Pages/Directories	59	0.2%	22.0%	\$395	0.9	Phone	Credit Card
Other	1,855	5.0%	22.7%	\$345	24.2	Phone	Credit Card
<b>TOTAL REPORTS</b>	<b>37,283</b>	<b>100%</b>	<b>35.1%</b>	<b>\$160</b>	<b>NA</b>	<b>Phone</b>	<b>Credit Card</b>

## APPENDIX C: Top 10 Scam Types by Overall Risk, Exposure, Susceptibility, and Monetary Loss

	<b>RISK</b>	<b>EXPOSURE</b>	<b>SUSCEPTIBILITY</b>	<b>MEDIAN \$ LOSS</b>
<b>1</b>	Employment	Online Purchase	Online Purchase	Romance & Cryptocurrency
<b>2</b>	Cryptocurrency	Phishing	Moving	Investment
<b>3</b>	Online Purchase	Employment	Cryptocurrency	Family/Friend Emergency
<b>4</b>	Fake Check/ Money Order	Fake Check/ Money Order	Counterfeit Product	Home Improvement
<b>5</b>	Advance Fee Loan	Debt Collection	Investment	Employment
<b>6</b>	Romance	Tech Support	Home Improvement	Fake Check/ Money Order
<b>7</b>	Home Improvement	Sweepstakes/ Lottery/Prize	Romance	Travel/Vacation/ Timeshare
<b>8</b>	Investment	Government Grant	Travel/Vacation/ Timeshare	Rental
<b>9</b>	Tech Support	Identity Theft	Advance Fee Loan	Government Grant & Sweepstakes/ Lottery/Prizes
<b>10</b>	Travel/Vacation/ Timeshare	Advance Fee Loan	Rental	Credit Repair/ Debt Relief



# Authors and Contributors

## AUTHORS

**Melissa “Mel” Trumpower** is the executive director of 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 overseeing BBB Institute, Mel manages the BBB Scam Tracker program and is co-author of *Exposed to Scams* (2019), the *BBB Scam Tracker Risk Report* (2017 and 2018), and *Scams and Your Small Business* (2018). Mel has a bachelor’s degree from Cornell University and a master’s degree from Johns Hopkins University.

**Melissa Bittner** is the curriculum development and training manager for BBB Institute for Marketplace Trust. Her role includes managing fraud-prevention programs facilitated throughout North America, including Fighting Financial Fraud and the Military & Veterans Initiative. Melissa is the author of *Military Consumers and Marketplace Trust* (2019) and is co-author of the *BBB Scam Tracker Risk Report* (2018). She has a master’s degree in public administration with a concentration in ethical leadership from Marist College.



## CONTRIBUTORS

**Sean Xiangwen Lai** is a research and development specialist at the International Association of Better Business Bureaus. Sean has experience in data gathering, processing, and data analysis and visualization and is currently finishing his Ph.D. in physics at Georgetown University. He has passed two levels of Charter Financial Analyst (CFA) exams and is pursuing a CFA charter holder. He has a great passion for implementing statistics, programming, data analysis, finance, and marketing to come up with decisions and innovations that have a positive impact on society. Sean can speak English, Mandarin, and Hokkien fluently, as well as some Japanese and Korean. His hobbies include all kinds of outdoor activities.

**Matt Scandale** has worked for the Better Business Bureau since 1991, serving in a variety of hands-on managerial and consulting roles in the areas of technology and data analysis, particularly in relation to operations. He specializes in development of custom database applications for internal business processes, including reporting. He hails from Buffalo, New York, and has a degree from Cornell University in consumer economics.

**Dr. Rubens Pessanha, MBA, PMP, GPHR, SPHR, SHRM-SCP**, is the senior director of research & 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* (2016 and 2017), *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). As a hobby, Dr. Pessanha teaches project management, business ethics, strategy, and marketing for graduate and undergraduate students.



4250 North Fairfax Drive, Suite 600  
Arlington VA 22203

[Institute@IABBB.org](mailto:Institute@IABBB.org)

**[BBB.org/RiskReport](https://www.BBB.org/RiskReport)**







[Home](#) » [Tips & Advice](#) » [Business Center](#) » [Business Blog](#) » Seven Coronavirus scams targeting your business

## Seven Coronavirus scams targeting your business

By: Lesley Fair | Mar 25, 2020 1:33PM

1. PUBLIC HEALTH SCAMS
2. GOVERNMENT CHECK SCAMS
3. BUSINESS EMAIL SCAMS
4. I.T. SCAMS
5. SUPPLY SCAMS
6. ROBOCALL SCAMS
7. DATA SCAMS



Re: COVID-19 Adjustment !  Spam 



**Admin Department**

to me 

1:20 PM (3 hours ago)



### This message seems dangerous

Similar messages were used to steal people's personal information. Avoid clicking links, downloading attachments, or replying with personal information.

Looks safe



Dear Staff

New notification ,Please due to COVID-19, all staff & Employee are expected to kindly Click **PROCEED** and complete the required directive to be added to March and April benefit payroll directory as compilation is ongoing and will last within 48hours.

Thank you,  
Admin Department



# Federal Bureau of Investigation Internet Crime Complaint Center(IC3)





Federal Bureau of Investigation  
Internet Crime Complaint Center(IC3)

[Home](#) [File a Complaint](#) [Press Room](#) [News](#) [About IC3](#)

### Filing a Complaint with the IC3

The IC3 accepts online Internet crime complaints from either the actual victim or from a third party to the complainant. We can best process your complaint if we receive accurate and complete information from you. Therefore, we request you provide the following information when filing a complaint:

- Victim's name, address, telephone, and email
- Financial transaction information (e.g., account information, transaction date and amount, who received the money)
- Subject's name, address, telephone, email, website, and IP address
- Specific details on how you were victimized
- Email header(s)
- Any other relevant information you believe is necessary to support your complaint

[File a Complaint](#)

### Welcome to the IC3



### Site Navigation

[Alert Archive](#)  
[FAQs](#)  
[Disclaimer](#)  
[Privacy Notice](#)  
[Internet Crime Prevention Tips](#)  
[Internet Crime Schemes](#)

### Annual Report



2019 IC3 Annual Report

### Flyer/Poster

[IC3 Brochure](#)   
[IC3 Fraud Alert](#)   
[Ransomware Brochure](#) 

[Contact the FBI's IC3 to file a complaint:](https://www.ic3.gov/default.aspx)  
<https://www.ic3.gov/default.aspx>



# U.S. DEPARTMENT OF THE TREASURY

[ABOUT TREASURY](#)

[SECRETARY MNUCHIN](#)

[POLICY ISSUES](#)

[DATA](#)

[SERVICES](#)

[NEWS](#)

[SEARCH](#)

[For small businesses seeking direct relief from COVID-19, CLICK HERE to learn more about Paycheck Protection Loans.](#)

[HOME](#) > [SERVICES](#) > [REPORT FRAUD WASTE AND ABUSE](#) > [COVID-19 SCAMS](#)

## SERVICES

### Report Fraud Waste and Abuse

#### COVID-19 Scams

[Report Scam Attempts](#)

[Report Fraud or Misconduct  
Related to Government Contracts  
or Grants](#)

## COVID-19 Scams

If you receive calls, emails, or other communications claiming to be from the Treasury Department and offering COVID-19 related grants or stimulus payments in exchange for personal financial information, or an advance fee, or charge of any kind, including the purchase of gift cards, please do not respond. These are scams. Please contact the FBI at [www.ic3.gov](http://www.ic3.gov) so that the scammers can be tracked and stopped.

Fraud involving payment of **Federal taxes** should be reported to the [Treasury Inspector General for Tax Administration](#).

<https://home.treasury.gov/services/report-fraud-waste-and-abuse/covid-19-scams>





[Home](#) / [Consumer](#) /

# COVID-19 Consumer Warnings and Safety Tips

As the novel coronavirus (COVID-19) pandemic continues to impact the United States, phone scammers have seized the opportunity to prey on consumers.

The FCC has received reports of scam and hoax text message campaigns and scam robocalls offering free home testing kits, promoting bogus cures, [selling health insurance](#), and preying on virus-related fears.

A text message scam may falsely advertise a cure or an offer to be tested for coronavirus. Do not click on links in texts related to the virus, and check [cdc.gov/coronavirus](https://www.cdc.gov/coronavirus) for the most current information.

Some text scams are impersonating government agencies. The FCC recently learned of a text scam claiming to be from the "FCC Financial Care Center" and offering \$30,000 in COVID-19 relief. There is no FCC program to provide relief funds to consumers. The text is likely a [phishing](#) attempt to get banking or other personal information from victims. The [BBB is also warning](#) of a text message scam impersonating the U.S. Department of Health and Human Services informs recipients that they must take a "mandatory online COVID-19 test" using the included link.

<https://www.fcc.gov/covid-scams>

# COVID-19 Consumer Warnings and Safety Tips

## Sample Hoax Text

From my next door neighbor

Just received this...from good friend of mine who works for the CDC

Please be advised, within 48 to 72 hours the president will evoke what is called the Stafford Act. Just got off the phone with some of my military friends up in DC who just got out of a two hour briefing. The president will order a two week mandatory quarantine for the nation. Stock up o whatever you guys need to make sure you have a two week supply of everything. Please forward to your network.

## Coronavirus Scam Audio Samples

### Test Kit Phone Scam

▶ 0:06 / 0:15 🔊 ⋮

Audio transcript: ...[The Coronavirus] Response Act has made coronavirus testing more accessible immediately. If you want to receive a free testing kit delivered overnight to your home, press 1. If you do not want your free testing, press 2. (Audio source: YouMail)

### Student Loan Callback Scam

▶ 0:03 / 0:36 🔊 ⋮

Audio transcript: Hello this is Brad ... with an important message regarding the effects of the coronavirus outbreak on your student loans. As you may have already heard, President Trump invoked his power as commander-in-chief by declaring a national emergency due to the widespread impact of COVID-19. New measures will include waiving interest on your federal student loans until further notice. During this time our offices have continued to maintain full staffing levels and will continue to do so until further notice. For more information on how these new measures will impact your future payment obligations, call us back today at 855-264-XXXX before 6:00 PM Pacific Standard Time. Thanks, and have a great day (Audio source: Nomorobo)



# Hackers are selling two serious Zoom zero-day vulnerabilities for \$500,000



By [Mark Wyciślik-Wilson](#)

Published 23 hours ago

Both the Windows and macOS versions of Zoom have critical, unpatched security vulnerabilities that could be exploited by hackers to target users and spy on calls and meetings.

Security experts say -- despite not having seen the actual code for the exploits -- that the Windows version of Zoom is affected by an RCE (Remote Code Execution) described as being "perfect for industrial espionage". The zero-days have been offered for sale for \$500,000.

## See also:

1. [Hundreds of thousands of stolen Zoom accounts for sale on hacker forums for next to nothing](#)
2. [Zoom will soon let some users choose which countries their data is routed through](#)
3. [Zoom is taking steps to improve privacy and security, and to prevent Zoombombing](#)

As reported by Vice's [Motherboard](#), three separate sources have confirmed that the vulnerabilities are available to buy in hacking circles, and have been offered to these individual directly. News of the zero-days comes just days after it was reported that hacker forums are being used to [offer Zoom user credentials for sale](#) at incredibly low prices.

# Zoom apologises for major security vulnerabilities, promises fixes

By [Mike Moore](#) 14 days ago

[Questions raised around Zoom security and safety](#)



# Seven Coronavirus scams targeting your business

By: Lesley Fair | Mar 25, 2020 1:33PM from the [ftc.gov](https://www.ftc.gov) website

We've warned consumers about [Coronavirus-related scams](#), but businesses are at risk, too. Keep your guard up against these seven B2B scams that try to exploit companies' concerns about COVID-19. In addition to sharing this information with your employees and social networks, read on for how you can report Coronavirus scams to the FTC.

## "PUBLIC HEALTH" SCAMS

---

Fraudsters are sending messages that claim to be from the Centers for Disease Control and Prevention (CDC), World Health Organization (WHO), or other public health offices. They may ask for Social Security numbers, tax IDs, etc. Other variations direct you to click on a link or download a document. Remind your staff not to respond to messages like this – and definitely don't download anything or click on links in unsolicited email. It's the latest form of phishing aimed at stealing confidential data or installing malware on your network.

## GOVERNMENT CHECK SCAMS

---

You've seen news stories about whether financial help for businesses might be available in the future. But remember that criminals read those headlines, too, and use them to make their phony pitches sound more credible. If someone calls or emails you out of the blue claiming there's money available from a government agency if you just make an up-front payment or provide some personal information, it's a phony. Our [Checks from the government](#) blog post offers tips on spotting those scams.

## BUSINESS EMAIL SCAMS

---

We've warned companies about frauds perpetrated via business email. For example, in a [CEO scam](#), an employee gets a message that appears to come from a company higher-up directing the person to wire money, transfer funds, send gift card codes, etc. In reality, a con artist has spoofed the boss' email address or phone number. Why are we renewing the call for vigilance? The economic upheaval caused by the Coronavirus has led to a flurry of unusual financial transactions – expedited orders, cancelled deals, refunds, etc. That's why an emergency request that would have raised eyebrows in the past might not set off the same alarms now. Compounding the problem is that teleworking employees can't walk down the hall to investigate a questionable directive. Warn your staff about these scams and give them a central in-house contact where they can verify requests they may receive.

## I.T. SCAMS

---

It works like a CEO scam, but this time the call or message claims to come from a member of your technology staff asking for a password or directing the recipient to download software. These scams pose a particular problem now due to what cybercrime experts call social engineering: the dark art of manipulating human behavior to facilitate fraud. Your employees already may be distracted by changes to their routine and your tech support team is swamped. Taking advantage of this temporary "upside down-ness," con artists may do a quick online search to glean a tidbit to really sell their story – for example, "I spoke with Fred, who said you were having a computer problem" or "The meeting has been shifted to our new teleconferencing platform. Here's the link." Your best defense is a workforce warned against this form of fraud. Again, an in-house source for accurate information can help protect your company.

## SUPPLY SCAMS

---

With many businesses scrambling for supplies, it's wise to heed warnings about websites that mimic the look of well-known online retailers. They claim to have the essentials you need, but in reality, they're fakes that take your "order," grab your credit card number, and run. The safer strategy is to type in URLs you know to be genuine. And before taking a chance on an unfamiliar supplier, check them out with trusted industry colleagues.

## ROBOCALL SCAMS

---

While working from home, your employees are hearing a new crop of annoying – and illegal – robocalls. It's no surprise that fraudsters who already flout the law would try to exploit people's COVID concerns to make a buck. Some of these tele-phonies pitch bogus test kits and sanitation supplies. Others have businesses in their sights. Curious what these calls sound like? [This recording](#) targets "small business who may be affected by the Coronavirus," warning them to "ensure your Google listing is correctly displaying. Otherwise customers may not find you online during this time." We've seen scams like this before and the call definitely isn't from Google. Remind your staff that the only right response to an illegal robocall trying to sell something is to hang up.

## DATA SCAMS

---

The rest of us may be adjusting to new ways of working, but it's business as usual for hackers. With more people telecommuting, hackers are hoping companies will drop their online defenses, making it easier to infiltrate data-rich networks. We have tips to help your staff [maintain security when working from home](#). Also, the National Institute of Standards and Technology (NIST) has resources on making a safer transition to a remote workplace. A good place to start: NIST's updated [Telework Cybersecurity](#) page. Check out NIST's infographic, [Telework Security Overview & Tip Guide](#). Read their recent bulletin on [Security for Enterprise Telework, Remote Access, and Bring Your Own Device \(BYOD\) Solutions](#). And review their advice on [Navigating the Conference Call Security Highway](#).

If you spot a bogus pitch, [report it to the FTC](#). There's a [special link](#) where you can report possible COVID-19 frauds.

## Americans have lost \$13.4 million to fraud linked to COVID-19

PUBLISHED WED, APR 15 2020 12:17 PM EDT UPDATED WED, APR 15 2020 2:52 PM EDT BY GREG IACURCI FOR CNBC

Americans have lost \$13.4 million to coronavirus-related fraud since the beginning of the year, according to the Federal Trade Commission.

The figure is based on 18,235 reports related to Covid-19 that the agency has received from consumers since Jan. 1, according to a blog post published Wednesday by Paul Witt, lead data analyst in the FTC's Division of Consumer Response and Operations.

Because not all consumers may have reported fraud to the agency, the true dollar figure could be much higher.

The top complaint categories for Covid-19 scams are related to travel and vacations, online shopping, bogus text messages and imposter scams, whereby the con artist pretends to be someone they're not, according to Witt.

The IRS recently [warned of scammers trying to steal](#) the stimulus checks it's sending Americans to help them weather the economic repercussions of Covid-19.

The agency started depositing those one-time payments — up to \$1,200 per individual, \$2,400 per couple and \$500 extra per eligible dependent, depending on income levels — into people's bank accounts [over the past several days](#). Paper checks will [arrive in May](#).

"We've spotted plenty of bogus cures and treatments, but many of you have told the FTC about straight-up scams, like texts/emails/calls from a 'government agency' promising to get your relief money for you," Witt wrote.

Other reported frauds include scams like websites promising scarce cleaning products or masks, which then never arrive after being ordered, or problems related to being reimbursed for canceled travel plans.

The \$13.4 million lost to these scams is around 3% of the [total \\$432.4 million](#) in fraud reported to the FTC through the end of March.

The typical American lost \$270 among the nearly 310,000 cases of fraud reported to the agency over that time period.

If you're getting calls, emails or texts related to the coronavirus, or seeing related ads or offers online, here are some things to remember, according to Witt:

- The government will never call to ask for money or your personal information like Social Security, bank account or credit card numbers.
- Anyone who tells you to pay by Western Union or Money Gram, or by putting money on a gift card, is a scammer. The government and legitimate businesses will never tell you to pay with those methods.

# Google saw more than 18 million daily malware and phishing emails related to COVID-19 last week

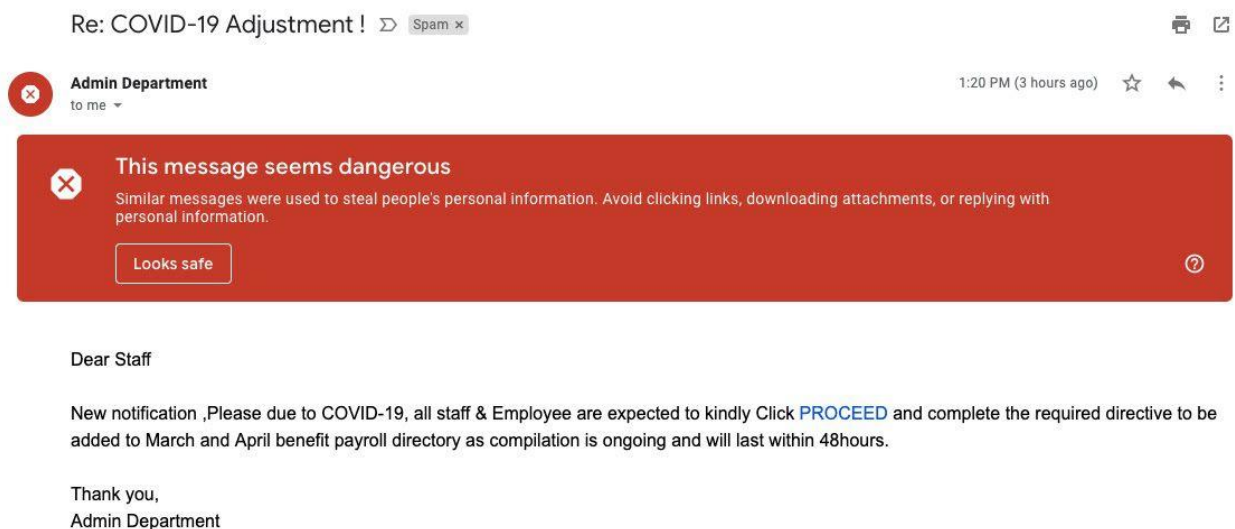
*Existing phishing scams have been updated to exploit COVID-19 concerns*

**By Kim Lyons, Apr 16, 2020 from the Verge**

Google says it saw more than 18 million daily malware and phishing emails related to COVID-19 scams just in the past week. That's on top of the more than 240 million daily spam messages it sees related to the novel coronavirus, the company says.

The phishing attacks and scams "use both fear and financial incentives to create urgency to try to prompt users to respond," Google says. In other words, same email scam, different subject line.

These scams include impersonating government organizations like the World Health Organization to try to solicit donations or trick users into downloading malware; pretending to have information about government stimulus payments; and phishing attempts aimed at workers who are working remotely. This scammer pretends to be affiliated with the recipient's employer:



Google say its artificial intelligence-powered protections filter such threats, and that it blocks "more than 99.9 percent of spam, phishing, and malware from reaching our users" using AI and other techniques. The company also says it worked with WHO on implementing DMARC (Domain-based Message Authentication, Reporting, and Conformance) to make it more difficult for scammers to impersonate the who.int domain and prevent legitimate emails from the WHO from being caught in spam filters.

The company says in many cases the malware and phishing threats aren't new but just existing malware campaigns updated to exploit fear and confusion around COVID-19. The usual cautions apply: don't click links in emails you weren't expecting, report phishing emails, and make sure a URL is legitimate before providing any information, since most scammers try to closely approximate real URLs.

# Don't Fall for These 7 Coronavirus Scams - COVID-19 swindles are costing Americans millions. Here's what you need to know to protect yourself.

April 14, 2020, By Kailey Hagen of fool.com.

While many Americans are struggling financially during the COVID-19 pandemic, a few are flourishing -- including scammers. The Federal Trade Commission (FTC) reports that Americans have lost almost \$13 million in COVID-19-related scams so far. That's probably not going to slow down until the crisis is over, so in the meantime, you need to be wise to scammers' tricks.

Here's a look at seven common COVID-19 scams going around right now. If you encounter any of these, do not give out your personal information. Make note of whatever information the scammer gave you, including names, websites, and phone numbers, and report it to the FTC and your local police.

## 1. Stimulus check scams

The government will be sending out stimulus checks to millions of Americans in the coming weeks, and scammers are capitalizing upon the confusion around this new process to trick people into handing over their bank account information. They may call pretending to be from the government or your bank, asking you to verify your bank account for swift delivery of your check, or they might claim to have early access to the checks and offer to deposit the money into your account if you hand over your financial information.

Don't fall for any of it. If you submitted a tax return for 2018 or 2019, there's a good chance the government already knows where to send the money. For those it doesn't have bank account information for, the IRS is working on a form you can use to indicate where you want the funds deposited. And if the government can't get a bank account number for you, it will mail the check to your last known address. It will never contact you by phone, email, or mail asking you to verify your information.

## 2. COVID-19 product and treatment scams

The pandemic has made some supplies, like hand sanitizer and face masks, hard to find. An enterprising scammer may create a fake website pretending to offer these elusive products in the hope that you will "buy" them. Some are also claiming to have access to home COVID-19 test kits or an experimental treatment, but there are no treatments or test kits approved by the Food and Drug Administration for home use at this time.

Be careful about where you shop. Avoid making purchases from unfamiliar websites, but if you want to, do some research online first to investigate its legitimacy and look for a lock icon near the URL bar. This tells you the website encrypts your personal information so hackers cannot steal it.

## 3. Work-from-home scams

Millions of Americans are out of work until the crisis passes. While many are on unemployment, they may still be under financial strain and looking for ways to earn more money to make ends meet. Scammers may reach out offering a job that promises a large amount of income for a small amount of work. If you respond, they may request you to provide them with a small amount of money for training or special equipment. Or they may request your bank account information so they can directly deposit your funds. In reality, there is no job. They will just take the money or the information you give them and use it to steal whatever money you have left.

That's not to say there aren't legitimate work-from-home opportunities out there. You just have to do your research to make sure you're dealing with a real company. Do some research on the company and don't be afraid to contact it and ask questions before accepting a position, especially if it's asking for sensitive information. If you get a bad feeling, explore some other options instead.

## 4. Debt reduction scams

Thieves know some people are really struggling financially and may have trouble keeping up with their debt payments. They capitalize on people's desire to be rid of their debt by promising debt reduction techniques that

probably sound too good to be true (because they are). They'll ask for some money for their services and then take it and run.

Many banks, credit card companies, and other service providers are offering hardship assistance to customers affected by COVID-19. They may enable you to defer payments without hurting your credit score or incurring late fees. These programs are better options if you're struggling to keep up with your payments right now.

#### **5. A sick family member**

Have you ever heard of the scam where a thief contacts you pretending to be a friend or relative who is stranded in a foreign country and desperately needs money to get back? The latest version of that is, "I'm in the hospital with COVID-19 and I really need money for treatment." It's a little easier to pull off than normal right now because everyone is so isolated at home and may not be in close contact with relatives who live far away.

Before you hand over any money, you should double check the person's claims. Reach out to the friend or relative using the phone number you usually contact them at, or contact another friend or relative who knows that person to see if they know what's going on. You could also try asking the alleged family member or friend a personal question. If they cannot answer it, it's a good sign you're not dealing with someone you know.

#### **6. Fake websites with exclusive COVID-19 information**

COVID-19 has rapidly become one of the most searched topics on the internet, and all sorts of companies have created dedicated COVID-19 pages on their websites to address the crisis. There are also websites that track the progress of the pandemic. Scammers may make COVID-19 websites of their own, possibly claiming to have exclusive information from the Centers for Disease Control and Prevention (CDC) or a similar organization. When you visit the site, it may download malicious software to your computer that steals your personal information.

Be wary of where you get your information right now to make sure it's accurate and not part of a scam. You should be especially careful of websites that have "coronavirus" or "COVID-19" in the site name itself, as these have probably just been created recently and could be fake. Rely on legitimate sources, like the CDC, World Health Organization (WHO), and government websites, for accurate information.

#### **7. Charity scams**

Tough times bring out the good in a lot of people, and many companies and individuals are donating money to charities to help those affected by COVID-19. Scammers may reach out claiming to work for one of these charities to request a donation, but the money lines their pockets instead of going to the intended recipients.

If you're going to donate, make sure it's to a legitimate charity. Do some research online to see what you can find. You can also search the company in the [IRS Tax-Exempt Organization Search Tool](#). If you can't find it there, it's probably not legitimate. Follow the instructions to donate on the company's website, not information you got from a random phone call or email.

It would be nice if you could count on everyone to have compassion for others during these challenging times. But in every crisis, there are selfish individuals hoping to turn others' misfortune into their own personal gain. You may not be able to stop all of them, but you can stop yourself from becoming another one of their victims by watching out for the above scams and spreading the word to others.



## **U.S. Attorney's Office » Western District of Pennsylvania**

### **COVID-19 Fraud Hotline: 1-888-C19-WDPA**

In the face of the COVID-19 virus, your health and safety are the Department of Justice's top priority. The U.S. Attorney's Office for the Western District of Pennsylvania is on-duty to protect the citizens of western Pennsylvania from fraudsters and criminals who seek to exploit this crisis for their profit. We have heard reports of scammers using email phishing schemes that claim to be from legitimate health organizations, advertising counterfeit virus test kits, and seeking donations fraudulently for illegitimate or non-existent charitable organizations, all in an effort to exploit people's anxiety and uncertainty.

Please don't fall victim to these frauds and crimes. If you see these frauds being attempted or if you are victimized by these frauds, please report them to:

FBI at: <https://www.ic3.gov/default.aspx> or **412-432-4000**,

COVID-19 Fraud Coordinator, Senior Litigation Counsel **Shaun Sweeney** at [USAPAW.COVID19@usdoj.gov](mailto:USAPAW.COVID19@usdoj.gov) or **1-888-C19-WDPA**, or

Federal Trade Commission at [ftc.gov/complaint](https://ftc.gov/complaint).

For continuing information on the COVID-19 virus and the federal response, check <https://www.cdc.gov/coronavirus/2019-ncov/index.html>

#### **Avoid Coronavirus Scams**

Scammers are taking advantage of fears surrounding the Coronavirus. They're setting up websites to sell bogus products, and using fake emails, texts, and social media posts as a ruse to take your money and get your personal information. The emails and posts may be promoting awareness and prevention tips, and fake information about cases in your neighborhood. They also may be asking you to donate to victims, offering advice on unproven treatments, or contain malicious email attachments. Some examples of COVID-19 scams include:

- **Treatment scams:** Scammers are offering to sell fake cures, vaccines, and advice on unproven treatments for COVID-19.
- **Supply scams:** Scammers are creating fake shops, websites, social media accounts, and email addresses claiming to sell medical supplies currently in high demand, such as surgical masks. When consumers attempt to purchase supplies through these channels, fraudsters pocket the money and never provide the promised supplies.
- **Provider scams:** Scammers are also contacting people by phone and email, pretending to be doctors and hospitals that have treated a friend or relative for COVID-19, and demanding payment for that treatment.
- **Charity scams:** Scammers are soliciting donations for individuals, groups, and areas affected by COVID-19.
- **Phishing scams:** Scammers posing as national and global health authorities, including the World Health Organization (WHO) and the Centers for Disease Control and Prevention (CDC), are sending phishing emails



designed to trick recipients into downloading malware or providing personal identifying and financial information.

- **App scams:** Scammers are also creating and manipulating mobile apps designed to track the spread of COVID-19 to insert malware that will compromise users' devices and personal information.
- **Investment scams:** Scammers are offering online promotions on various platforms, including social media, claiming that the products or services of publicly traded companies can prevent, detect, or cure COVID-19, and that the stock of these companies will dramatically increase in value as a result. These promotions are often styled as "research reports," make predictions of a specific "target price," and relate to microcap stocks, or low-priced stocks issued by the smallest of companies with limited publicly available information.

**U.S. Attorney Brady urges everyone, especially those most at risk of serious illness, to avoid these and similar scams by taking the following steps:**

- Independently verify the identity of any company, charity, or individual that contacts you regarding COVID-19.
- Check the websites and email addresses offering information, products, or services related to COVID-19. Be aware that scammers often employ addresses that differ only slightly from those belonging to the entities they are impersonating. For example, they might use "cdc.com" or "cdc.org" instead of "cdc.gov."
- Be wary of unsolicited emails offering information, supplies, or treatment for COVID-19 or requesting your personal information for medical purposes. Legitimate health authorities will not contact the general public this way.
- Do not click on links or open email attachments from unknown or unverified sources. Doing so could download a virus onto your computer or device.
- Make sure the anti-malware and anti-virus software on your computer is operating and up to date.
- Ignore offers for a COVID-19 vaccine, cure, or treatment. Remember, if there is a medical breakthrough, you won't hear about it for the first time through an email, online ad, or unsolicited sales pitch.
- Check online reviews of any company offering COVID-19 products or supplies. Avoid companies whose customers have complained about not receiving items.
- Research any charities or crowdfunding sites soliciting donations in connection with COVID-19 before giving. Remember, an organization may not be legitimate even if it uses words like "CDC" or "government" in its name or has reputable looking seals or logos on its materials. For online resources on donating wisely, visit the **Federal Trade Commission** (FTC) website.

- Be wary of any business, charity, or individual requesting payments or donations in cash, by wire transfer, gift card, or through the mail. Don't send money through any of these channels.
- Be cautious of "investment opportunities" tied to COVID-19, especially those based on claims that a small company's products or services can help stop the virus. If you decide to invest, carefully research the investment beforehand. For information on how to avoid investment fraud, visit the **U.S. Securities and Exchange Commission** (SEC) website.
- For the most up-to-date information on COVID-19, visit the **Centers for Disease Control and Prevention** (CDC) and **World Health Organization** (WHO) websites.
- If anyone believes they have been the victim of a COVID-19 fraud scheme, please contact the U.S. Attorney's Office and the COVID19 Fraud Coordinator (as listed above), or your state or local authorities.