



SCAMS AND YOUR SMALL BUSINESS RESEARCH REPORT

LEARN → PROTECT → REPORT

WELCOME

WE ARE

OPEN

PLEASE COME IN

Executive Summary

There is considerable overlap between scams targeting individual consumers and those targeting small businesses (with or without employees). This may explain why research and outreach efforts targeted at both audiences has generally been one and the same.

However, our research suggests that the scam activity directed at small businesses is growing, that these scams pose a significant risk, and that they generally result in a higher monetary loss per incident than those targeting individuals. Scams can reach and impact every business, regardless of location, size, industry, or length of time in business. And while scams vary in sophistication, businesses lose money to all types of scams every year. Thus, in order to better educate businesses and effectively combat small business scams in general, we believe we must customize our research, reporting, and educational outreach based on the target audience.

Researching the types, susceptibility and impact of small business scams is a complex exercise; therefore, our main intention with this report is to begin a conversation. We invite others to join us in this ongoing exploration to help build awareness around the need to treat individual and business audiences differently. That way, we can more effectively communicate our message, improve our understanding of the nature and scope of the problem, and enhance research and education approaches and methodologies.

We hope that by publishing this research and collaborating with the Federal Trade Commission (FTC) to educate and empower small businesses, we can contribute new insights and encourage others to join us. We hope small businesses will feel empowered to speak up and report fraud, enabling us to expand our knowledge of how they are uniquely impacted.

We urge business owners of all sizes to share this report with their colleagues and staff, and to consider sharing the educational materials that accompany this initiative. Spreading the word about the risks, approaches, and methods of scammers — and the most common types of scams — can help us create a safer and more trusted marketplace for all.

We encourage the media to consider expanding coverage of small business scams, in addition to continuing their great work informing the public at-large about scams that target individuals and families. With almost 30 million small businesses in the United States¹ — employing nearly half of the private workforce and representing a significant part of our economy — it is important that we focus as much time and resources on small businesses as we do on consumers. We hope this report will serve as an initial step in that direction.

¹ https://www.sba.gov/sites/default/files/advocacy/All_States.pdf

Introduction

Beginning in 2016, the Better Business Bureau (BBB) and the Better Business Bureau Institute for Marketplace Trust (BBB Institute) began publishing timely research regarding scams targeted at consumers, thanks to data reported through BBB Scam TrackerSM — an online crowdsourcing tool that empowers consumers and businesses to report and learn about scams in real time. This research has enabled BBB to provide significant insights about scammers and to publicize the many ways they perpetrate their schemes. More importantly, the research has allowed the organization to educate consumers and share important and detailed information about how to avoid falling prey to scams.

Small businesses, like individuals, are susceptible to scams. Con artists rely on gaps in knowledge, awareness, and preparedness among small business owners and their employees to successfully perpetrate scams. The limited research available on the topic — mostly from outside of the United States — suggests that small businesses are particularly vulnerable to scams, are less inclined to report scams, are likely to be subject to repeat attacks, and are particularly susceptible to online scams.²

Additionally, small business owners themselves believe that the risk of business scams is greater today than it was three years ago (Figure 1). We believe targeted research is needed. By learning about scammers' methods and how common scams work, by proactively educating business owners/employees and by raising awareness, we can potentially minimize the impact of scams on small business.

FIGURE 1
Do you believe today there is more risk, about the same risk, or less risk of business scams than there was 3 years ago?



² Schaper, M. T., & Weber, P. (2012). Understanding Small Business Scams. *Journal of Enterprising Culture*, 20(3), 333-356.

³ Select businesses earn BBB Accreditation by undergoing a thorough evaluation and upholding the BBB Code of Business Practices.

⁴ We expect to expand and launch a Canada-specific study during Canada's Small Business Week.

This year, to address this need for research on scams specifically targeting small businesses, BBB developed a Small Business Scams Survey, which is the primary source of data used to create this report. (Additional data included in this report is based on business scams reported to BBB Scam Tracker and information gathered through secondary research.)

The survey was distributed in March 2018 through six local BBBs to BBB Accredited Businesses³ and to non-Accredited Businesses through an external panel provider. We listened to about 1,200 small businesses in the United States,⁴ which were recruited via the internet using a custom email invitation with a live link to a survey (see Table 1 for a profile of respondents). The margin of error was approximately 3 percent, with a 95 percent confidence interval.

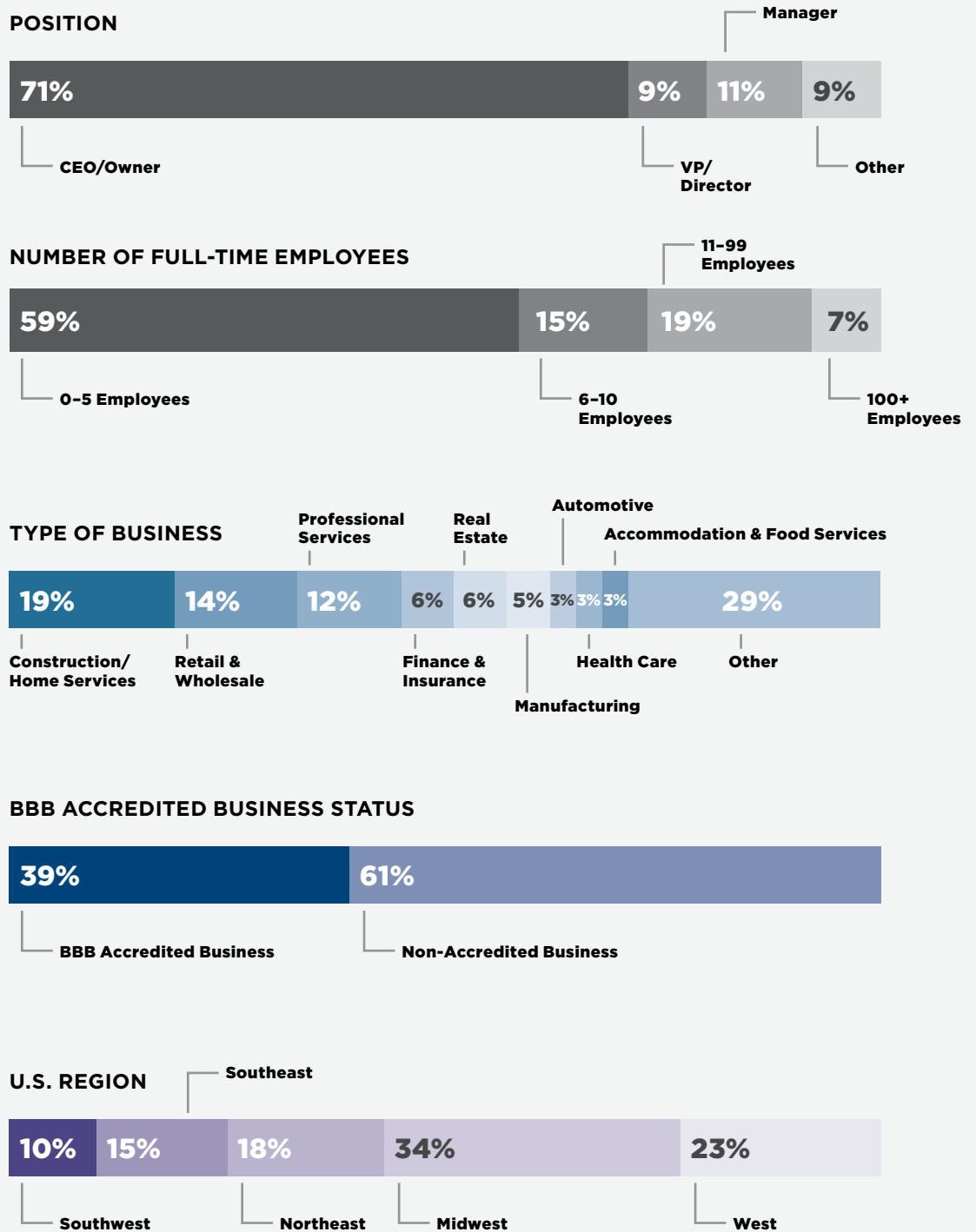
The Small Business Scams Survey asked small business owners questions about experiences they had with scams in the marketplace. For the purpose of the study, a scam was defined as “a dishonest way to make money by deceiving people through misrepresenting, concealing or omitting facts.”

Among the questions we set about to answer were:

- What do we really know about small business scams?
- How aware (or concerned) are small business owners of the risks?
- What are small businesses doing to protect themselves?
- How common are scams against small businesses?
- What are the most prevalent scams that target small businesses?
- What hinders small businesses from doing more to protect themselves?
- How can we get educational information to the small business community?

It is important to note the limitations of this research. By combining data from BBB Scam Tracker with data from the Small Business Scams Survey, we are able to present important insights into small business scams and how they are perpetrated. However, our research is limited by the very nature of self-reporting as an imperfect measure, by sampling challenges, and by the complex nature of this problem. We look forward to working with others to continue to expand on the research that is available in this area.

TABLE 1
Profile of Survey Respondents



Awareness of Business Scams

Scams come in a variety of forms, and classifying them is an ongoing challenge. For the purpose of this study, small business scams were organized into 12 different types of scams (including “Other”) known to target small businesses (Table 2).

TABLE 2
Types of Business Scams



Bank/Credit Card Company Imposter

This scam typically involves impersonation of a bank or other credit card issuer. Under the guise of verifying account information, con artists try to fool their targets into sharing credit card or banking information.



Charity

These scammers typically choose a name that sounds similar to a reputable charity. They may ask the business to donate or show its support by buying space in a calendar or publication. Then they disappear.



Directory Listing and Advertising

This scam fools businesses into paying for non-existent advertising or a listing in a non-existent directory or “Yellow Pages.” In some cases, the directory will technically exist, but will not be widely distributed, and a listing will be of little or no value.



Fake Check

These scammers ask the business to deposit a check and wire some of the money to a third-party. The scammers always have a good story to explain the overpayment – they need the business to cover taxes or fees, purchase supplies or something else. By the time the bank discovers the business has deposited a bad check, the scammer already has the money.



Fake Invoice/Supplier Bill

Scammers prey on business owners and hope they won't notice a bill, often for office supplies that the company never ordered. They may even deliver unordered merchandise and then try to make the business pay. In other cases, scammers send urgent notices for renewal of website domain hosting or other critical services, hoping businesses will pay without proper due diligence.



Government Agency Imposter

Scammers impersonating government agents threaten to suspend business licenses, impose fines, or even take legal action if the business doesn't pay taxes, renew government licenses or registrations, or pay other fees. Sometimes they trick businesses into buying workplace compliance posters that are available for free, or they may pressure them to pay upfront fees for a non-existent business grant.



Social Engineering and Phishing

Cyber scammers trick employees into giving up confidential or sensitive information such as passwords or bank information. It often starts with a phishing email, a social media contact, or a call that seems to come from a trusted source such as a supervisor or other senior employee, but creates urgency or fear.



Tech Support

Tech support scams start with a call or an alarming pop-up message. Scammers pretend to be from a well-known company. The goal is to collect money, gain access to the computer, or both. They may ask the employee to pay them to fix a problem they don't really have or enroll the business in a non-existent or useless computer maintenance program.



Utility Company Imposter

Scammers pretend to call from a gas, electric, or water company saying the service is about to be interrupted. Scammers want to scare the employee into believing a late bill must be paid immediately.



Vanity Award

The business receives a notice indicating that an employee or the business itself has won recognition for achievement such as a "Best of Local Business Award." The "winner" may be asked to link to the group's website to obtain a plaque commemorating the award.



Worthless Problem-Solving Service

Sometimes scammers claim to be able to provide low-cost solutions to problems they know many businesses have. For example, they might claim they can repair the business's online reputation or provide quick relief if it's struggling with debt or back taxes — for an up-front fee, of course.



Other⁵

⁵ The most common other scams cited by respondents were "Other Imposter Scams" and "Fake Customer Scams" (i.e., customers with no intention of paying).

Survey respondents reported a high level of awareness about scams, with only 2 percent of BBB Accredited Businesses (see right) and 10 percent of Non-Accredited Businesses indicating they had never heard of any type of business scam.



Select businesses earn BBB Accreditation by undergoing a thorough evaluation and upholding the BBB Code of Business Practices.

The five best-known business scams (Figure 2) are:

- Tech support scams;
- Government agency imposter scams;
- Directory listing and advertising scams;
- Fake check scams; and
- Bank/credit card company imposter scams.

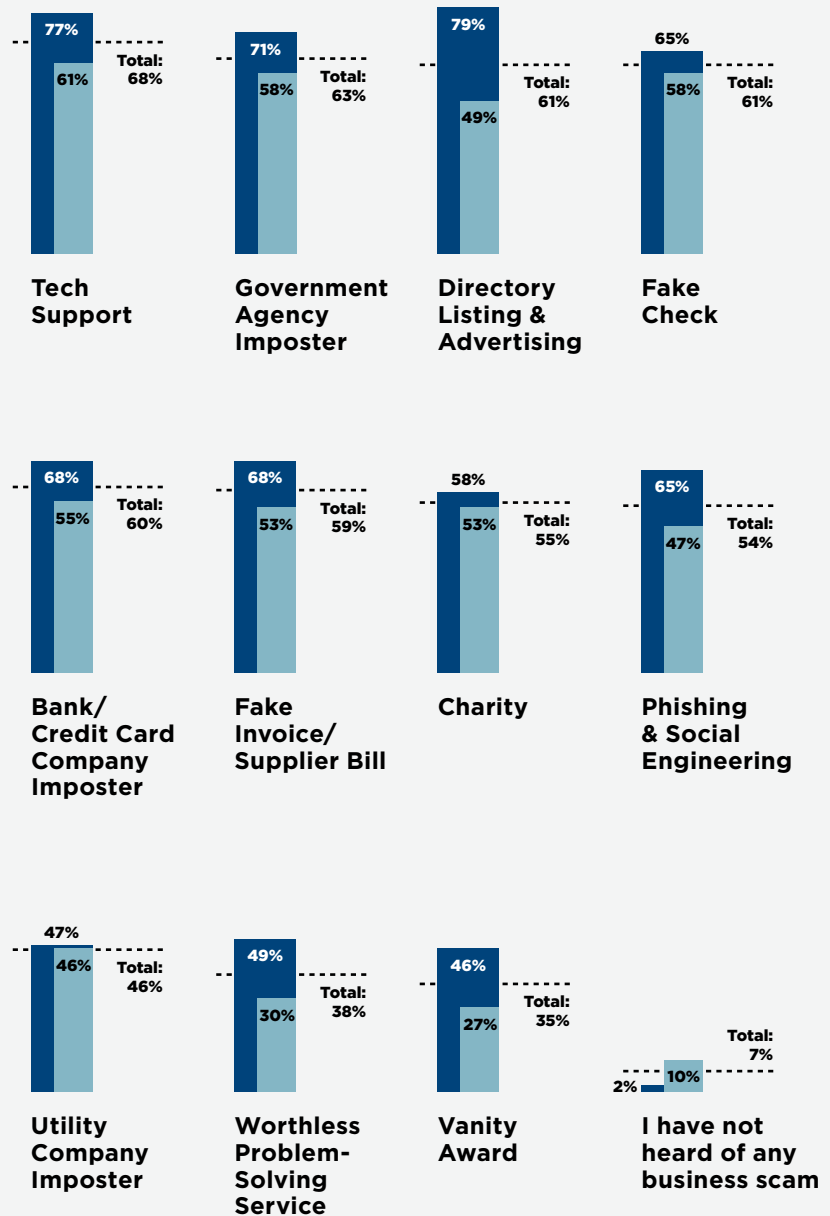
Vanity award scams were the least known among our list of business scams. Respondents identified other types of imposter scams that were not among those listed in the survey, as well as the risk of customers who do not pay, some of whom may be scammers who pretend to be potential customers but have no intention of paying.

In many cases, scams that target small businesses are similar to the types of scams that focus on the general public (e.g., tech support, fake checks, charity). But that is not always the case, and there are certain types of scams that are specifically focused on businesses (e.g., fake invoice/supplier bill, directory listing and advertising, fake customers).

FIGURE 2 - BBB Accredited vs. Non-Accredited Businesses

Have you ever HEARD of any of the following scams?

% YES



BBB ACCREDITED ■
NON-ACCREDITED ■

Means of Contact and Method of Payment

Fraudsters exploit the full range of communication channels to make contact with their targets, and readily adapt new communication methods or popular media. Phone is the top means of contact for business scams. While consumers are routinely advised not to answer calls from unknown numbers, businesses likely answer their phones whether they recognize the number or not, as these callers could be clients or new customers. Figure 3 provides a comparison of all contact methods used where a business was harmed.

The range of payment methods used by scammers (Figure 4) is consistent with the variability and adaptability generally seen in the marketplace. However, criminals have an obvious interest in trying to reduce or eliminate the likelihood that their transactions will be traced or charges reversed, which drives their use of wire transfers and prepaid cards.

FIGURE 3
Which of the following methods of contact were used by the scammer? Select all that apply.

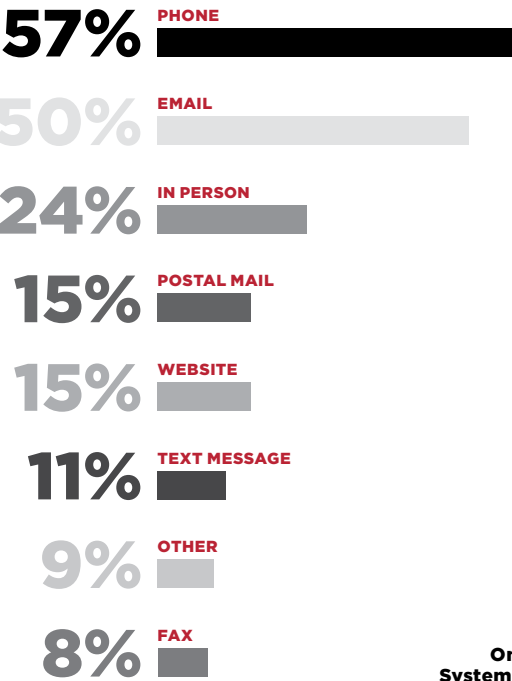
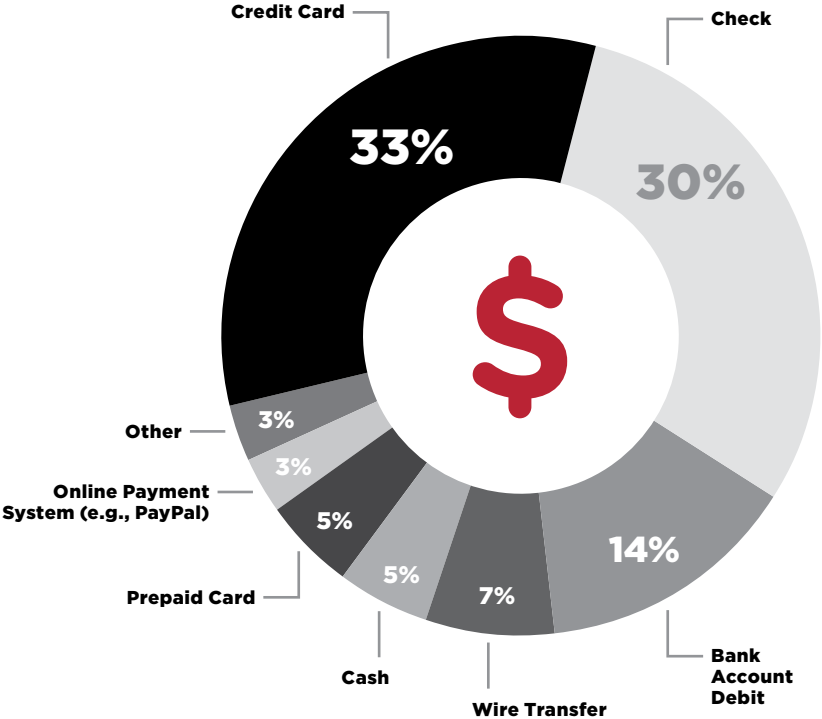


FIGURE 4
When your business lost money to a scam, what was the payment method used?



Businesses of All Sizes are at Risk of Scams

Even though the majority of small businesses (58 percent) agree or strongly agree that their company's risk of being scammed is low, approximately six out of 10 also agree or strongly agree that they are concerned about business scams. The key reasons businesses cited for being concerned (Table 3) are related to the potential impact of scams on the business (e.g., reputation, costs, time and lost customers), the proliferation and sophistication of scams, and the need to put more emphasis on preventive measures.

Those not concerned about business scams claim to have protections in place, believe businesses like theirs are not typical targets of scammers or think that having few or no employees puts them at lower risk. Furthermore, eight out of 10 small business owners also believe that other businesses are more at risk of scams than their own business (Figure 5). This mirrors results from an earlier consumer-focused study, *Cracking the Invulnerability Illusion*,⁶ which found that individuals overwhelmingly believe others are at greater risk than themselves. It is important for businesses to understand that scammers can target businesses of any size and in any industry with a multitude of high-tech or low-tech schemes that are ever evolving and adapting.

Why is your company concerned about business scams?

Selected Verbatim

“It can IMPACT OUR REPUTATION and harm our customers.”

“It can be COSTLY.”

“Don’t want to LOSE MONEY.”

“LOSS OF MONEY and employee safety.”

“Because of the POTENTIAL HARM it can do to a business.”

“It could JEOPARDIZE OUR CLIENTS’ PRIVILEGED INFO and create major issues for them and us.”

“We are WORRIED because of the PROLIFERATION AND SOPHISTICATION OF THE SCAMS TODAY.”

“It’s a PROBLEM AFFECTING ALL BUSINESSES.”

“Cost, waste of time, waste of resources.”

“We constantly are getting scam phone calls and emails, non-stop every day. We are always afraid we will think someone is a business we deal with and then it won’t be.”

“Loss of man hours and potential THREAT TO OUR REPUTATION AND BOTTOM LINE.”

“Nuisance, potential work stoppage, inconvenience, annoyance.”

“They are changing every day, and are becoming more professional. So the ABILITY TO SPOT THEM IS MORE DIFFICULT.”

⁶ Emma Fletcher and Rubens Pessanha. *Cracking the Invulnerability Illusion: Stereotypes, Optimism Bias, and the Way Forward for Marketplace Scam Education*. BBB Institute for Marketplace Trust, 2016. www.bbb.org/truthaboutscams.

Why is your company not concerned about business scams?

Selected Verbatim

“We have **PROCEDURES SET IN PLACE** to spot scams.”

“We **HAVE A PROCESS** for all spending involving the company.”

“**Nature of the business.**”

“**RISK is pretty LOW IN MY MARKET.**”

“We’re a **SMALL BUSINESS**. We live in a **SMALL TOWN**. If something sounded or looked out of the ordinary, it would stick out like a sore thumb.”

“**Because I have no employees.**”

“**SMALL SIZE, few employees.**”

“We go thru a national **VERIFICATION PROCESS** for all new clients.”

“I am a **BUSINESS OF 1**. Have antivirus software and Carbonite backing up my data.”

“Our employees are **EDUCATED** and we have **NOT YET FACED A BUSINESS SCAM.**”

“We have been **TRAINED** and have things in place **TO PREVENT IT.**”

“As a law office we are **NOT A TYPICAL TARGET.**”

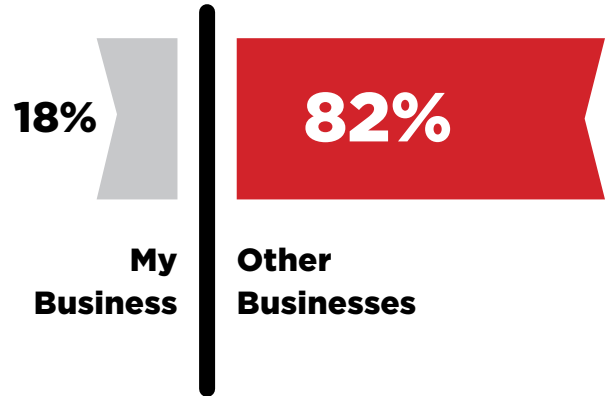
“We are experienced professionals that **CAN TELL THE DIFFERENCE** between real business and scams that would try and steal info or cheat services.”

“We **HAVE A STRONG IT TEAM** that keep in front of this...we also block certain sites, emails etc., and we have strong virus/malware protection.”

“As a contractor, we always require a deposit and we **HAVE LEGAL ACTIONS AVAILABLE TO US**, such as liens.”

FIGURE 5

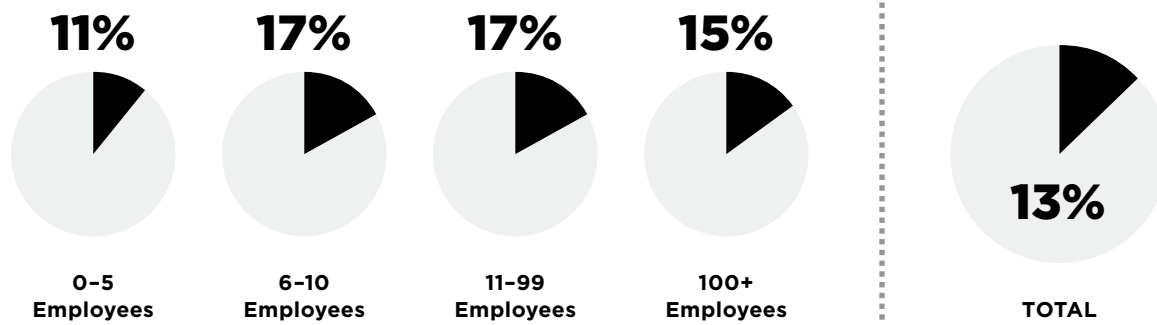
From the options below, which one do you think is most likely to be scammed?



Despite many businesses feeling they are at reduced risk of being scammed, about 63 percent of small businesses were aware of being exposed to (i.e., targeted by a scammer) at least one type of scam in the past three years. Small businesses of all sizes were targeted. **Overall, 13 percent of businesses responding to the survey indicated they had been harmed (i.e., lost money or information) by a scam (Figure 6).** Of those harmed, 80 percent lost money. In addition, 19 percent of those reporting they were scammed lost information, 11 percent indicated their reputation was compromised and 5 percent indicated their business experienced a decrease in customer trust as a result of being scammed.

FIGURE 6

To your knowledge, has your business ever been scammed? (% answering Yes)

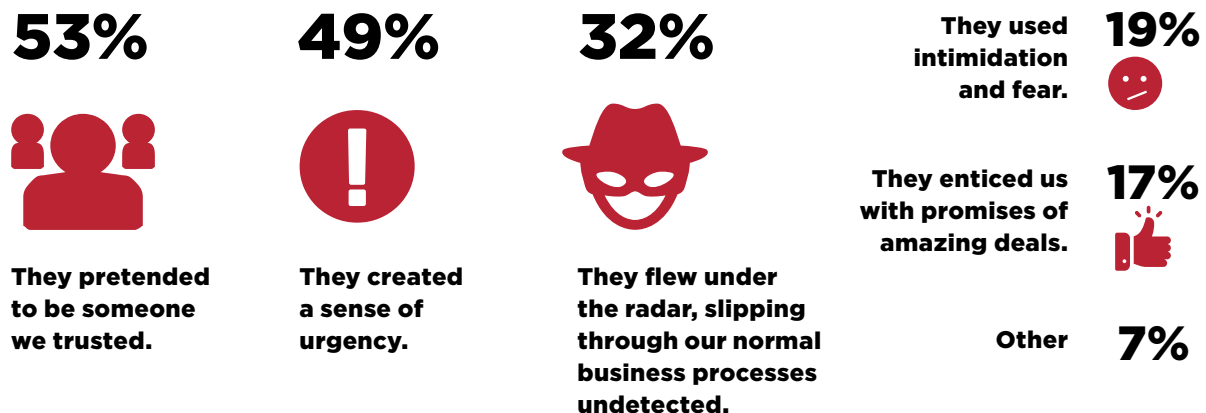


Scammers use a wide range of tactics — both high and low-tech — to harm businesses and, as shown in Figure 7 below, the most common are:

1. Pretending to be someone the business trusts to appear credible and gain their trust;
2. Creating a sense of urgency to force businesses into making quick decisions before they have time to look into it; and
3. Flying under the radar, slipping through normal business processes undetected.

FIGURE 7

Which of the following tactics were used by the scammer(s) that harmed your business? Select all that apply.



Impersonation – pretending to be a trusted individual or entity – is a common tactic used by scammers to target small businesses. From our analysis of a random sample of business scams reported to BBB Scam Tracker, we learned that scammers pretend to be:











- a) Potential providers of services or suppliers, such as advertising directories or publishers, printer toner suppliers, or utility companies;
- b) Lenders (e.g., banks);
- c) Potential customers; and
- d) Government officials (e.g., IRS, OSHA).

Exposure, Susceptibility, and Monetary Loss

For each of the scam categories included in the survey, respondents were asked to indicate if their business had been targeted by a scammer for a particular scam or had been harmed by a scam (i.e., lost money or information) in the past three years. Businesses that were impacted by a scam were asked to indicate the dollar loss for each scam category. For each of these questions, respondents were also able to write in scam categories not specifically listed (i.e., “Other”).

We used a slightly modified⁷ version of the BBB Risk Index algorithm,⁸ which considers **exposure** (i.e., how likely is your business to be targeted by a particular scam?), **susceptibility** (i.e., what are the odds of being harmed by a scam when exposed to it?), and **estimated median dollars lost**, to calculate the most risky business scams. Table 4 below showcases the 10 riskiest business scams.

TABLE 4
Top 10 Riskiest Business Scams (ref. past three years)

	Risk Order	Business Scam Type	% Exposure	% Susceptibility	Median \$ Loss
	1	Bank/Credit Card Company Imposter	18%	8%	\$1400
	2	Directory Listing and Advertising	32%	9%	\$500
	3	Fake Invoice/Supplier Bill	21%	10%	\$500
	4	Fake Check	15%	10%	\$675
	5	Tech Support	30%	7%	\$400
	6	Social Engineering/Phishing	16%	5%	\$500
	7	Charity	13%	8%	\$300
	8	Worthless Problem-Solving Service	13%	6%	\$300
	9	Government Agency Imposter	20%	3%	\$275
	10	Vanity Award	14%	4%	\$50

⁷ Exposure was modified since we considered that a business can be exposed to more than one scam type and thus respondents were asked to select all that applied. Susceptibility was modified to include the concept of harm, which encompasses both money loss and/or information loss.

⁸ Read more at [BBB.org/RiskReport](https://www.bbb.org/RiskReport).



CAUTION

In order to triangulate our findings from the survey research, we extracted a random sample of approximately 281 business scams reported to BBB Scam Tracker that were identified via text mining. We found that the top reported scams in terms of volume (i.e., % exposure) were consistent with our survey findings.

We also found from our sample of business scams reported to BBB Scam Tracker that the median dollar loss for scams that harmed businesses was higher than the median dollar loss for scams that target consumers.

Based on our survey data, we estimate that approximately 6 percent of small businesses lose money to scams every year and that the median loss per year is \$800 per harmed business, with an average of \$4,373 per harmed business, and a total loss estimated to be more than \$7 billion per year, not including intangible costs such as time, impact on reputation, and loss of consumer trust.

Lessons Learned from Targeted Businesses

In preparing this report, we heard stories from a number of businesses. Through these stories, we were able to learn more about the tactics scammers use to deceive small businesses. Sometimes, warning bells went off and the scammers were unsuccessful. Other times, the scammers succeeded. But in either case, these stories reveal a great deal about the manipulative tactics scammers use.

We thank the people whose stories are recounted here.

SELECTED STORIES

Describe a time when your business was harmed by a scam. Why do you think the scam WAS NOT detected or avoided?

“Advertising in local telephone book.

Everything looked good, even checked them out. But after taking money for an order that was supposed to take about 6-8 weeks for delivery, they disappeared.”

“It was a company calling stating that I owed them money

for internet research that they did over the last year. I was very busy at the time and didn't have time to look up the paper work so I paid them over the phone. I later found out the company never did anything for me.”

“A business helped me start a business, and I had to pay

\$10K for their help. They started helping at first, but after a short time, they disappeared. At the time, I was not really aware of all the scammers out there and their abilities. But after that one, I learned real quick... You cannot trust everyone's word.”

“Seven counterfeit checks totaling about \$4000 using our payroll account numbers cleared our bank and were not detected until we reconciled our checking account.”

“Caller would say they were ordering parts for a large reputable customer

and issue a PO [purchase order]. Then they would send a driver to pick up parts. We would then send an invoice to a customer. We later found out it was a scam.”

“Fake computer repair for non-existent problem. They harvested data from our customer database.”

“We were approached by a ‘business person’ who said they could help us with our social media exposure and updates. They said they would do it all and our exposure would create lots of jobs since social media is where it's at! We paid. They did not do ANYTHING AT ALL.”

SELECTED STORIES

Describe a time when your business was able to avoid a scam.

Why do you think the scam WAS detected or avoided?

“Basic awareness prevented a funds transfer for an executive out on vacation when the email address was not correct.”

“Noticed an email didn’t look correct so didn’t open the attachment that was with it. Found out later it was a virus.”

“We recently got targeted by the ‘tech support’ scam in which someone said they needed access to our computer to detect a virus that came across. What was funny was I had just listened to a podcast that week about this scam. As we do have virus protection/tech support that sometimes DOES need access to our computer, I can see where this scam would work. However, I asked for the company name and a phone number to call back after I ‘checked on it.’ They hung up.”

“Contacted via text for a free estimate on exterior painting. Person wanted desperately to pay with credit card. When we refused, they offered to send a check (which was for twice the amount of the bid); looked legitimate but **I contacted the bank and the title company that issued it and found out it was bogus.**”

“I am on high alert for watching for scams at all times, as are my key employees. A typical situation would be a blind email which supposedly comes from one of our clients but is actually from a scammer.”

“Our company, myself in particular, does diligent research on every potential client/agency. I listen carefully and take lots of notes. Many advertising agencies that have contacted us, we usually contact other local small businesses we partner with or know and ask them about credibility.”

“A phone call came in from ‘our’ gas company stating that they were going to turn off the gas to our building if we didn’t pay within 24 hours. This call was forwarded to me directly. I questioned the caller, knew that we paid our bills timely and told them that I would ‘call them back.’ After hanging up, I called our gas company myself, verified all was fine with our account. The rep from the gas company said that they were receiving calls from clients in regards to this scam. Added us to the list.”

“Just a couple of days ago ‘our Utility Department’ called and said he was heading out to shut off our power due to delinquent account status. The employee who answered the phone said ‘oh no; let me guess you just need a credit card and/or my date of birth and Social Security number to take care of it.’ The person immediately hung up.”

“I received several email appeals for long-term training or boarding, written in poor English, offering compensation in excess of what I charge, asking if I accept credit cards. These are giant red flags of con artists.”



Businesses Tell Their Stories

DIRECTORY LISTINGS / ADVERTISING SCAMMERS TAKE ADVANTAGE OF BUSY BUSINESSES

Gina owns a boarding and grooming service for pets located in Union Grove, Wisconsin. She received a call from Brian Mays, a representative from All Listings YP (Yellow Pages), who informed her that she had a number of past due invoices for advertising she purchased to promote her company. Gina remembered placing listings years before, but nothing in recent years. She thought it sounded fishy—she had been receiving phony invoices for years from a variety of sources—but Brian was pleasant to speak with and had such an even-keel voice that Gina thought twice. She told him she'd look into it and hung up the phone.

But Brian kept calling back and left Gina multiple voicemails.

“He'd say, ‘please give me a call.’” Gina wasn't sure what to do. She thought perhaps it was real after all, so the next time he called, she decided to answer.

“He [told] me if I pay now, I will only owe \$1,701.06. But if I don't pay within one week, I will owe for all of 2017, all of 2018, plus late fees [and] lawyer fees.”

His tone had shifted—at first he seemed like a pleasant man just trying to settle an old account, but now he was demanding. Gina was frightened, so she hung up. Brian

called back several times, tying up her phone line.

“It made me feel anxious. I lost sleep over it... I thought how long is this going to go on?”

The calls continue today, but Gina has learned not to believe random callers telling her she owes money.

“I don't trust anybody anymore.”

She keeps diligent records of those she does business with, and asks anyone who calls about or emails her invoices for proof that they're real. When they say they have her verbal agreement, she challenges them to prove it and supply the recording.

“With today's technology they should have proof, right then and there or they should be able to get it quickly and easily.”

And when in doubt, she gives her local BBB a call to get their advice. Often the same scammers hit multiple businesses in an area, so she finds it reassuring to check with the BBB when she receives invoices that may be phony.

“He [told] me if I pay now, I will only owe \$1701.06. But if I don't pay within one week, I will owe for all of 2017, all of 2018, plus late fees [and] lawyer fees.”



What Gina wants other businesses to know:

- ➔ **Keep accurate records of your accounts payable. If you get an invoice you were not anticipating, always investigate before paying it.**
- ➔ **Scammers often appear to be nice, professional people. Even if they are polite, do not assume they are legitimate.**
- ➔ **Do not let the scammer make you feel isolated. When in doubt, ask for another opinion.**

SCAMMERS TARGET NEW BUSINESSES

Katie owns a painting company in Oklahoma City, Oklahoma. About a year after opening her business, she updated her business profile on a known online directory, excited at the prospect of new clients. Katie knew lots of people used online review sites and was pleased to join one that was referral-only. That same day, she received text messages from two different clients wanting to find out more about her exterior home painting service. She texted them both, eager to get started on a couple of new jobs.

The first client was very insistent that he pay by credit card. While Katie hadn't been set up to accept credit card payments, she was reluctant to turn down his business. Instead, she asked for the property address and drove to the house to give him an estimate. When she pulled up, the house was small and not in the best neighborhood. She walked to the back of the house to begin assessing the cost of the project, and noticed the back door had been kicked in and someone had been in the house. Worried, she immediately called the prospective client's number to tell him.

"He didn't seem to care," she remembered. "That was a red flag."

She decided to concentrate on the second new client—hoping that would yield a less-alarming result. The client said he was "out of town for a medical procedure," and wouldn't be able to join her for the estimate, but told her the address. She asked for payment prior to starting the job, and after explaining that she did not take credit card

payments, he offered to mail her a check. The check arrived a few weeks later, but the amount was double the cost of her estimate.

"I thought, OK—I'm not sure how this works," Katie said.

The check arrived and looked valid, even though it was from a title company. Upon further reflection though, her instincts told her not to cash the check, but to investigate first and call the title company.

"They told me it was not a valid check."

Frustrated, she did not reach out to the second client and never heard from him again, but she did contact her local district attorney's office to report the incident.

In the weeks and months after signing up for this online directory, Katie received a number of inquiries by text message for exterior work. Each time, the outcome was similar to one of the first two situations. She now checks county records to verify the owner's name against the property record prior to providing estimates. In nearly all instances of scams, the names do not match and the property is listed for sale or rent online; sometimes she even calls the listing agent to see if the seller had requested the service. She spends countless hours researching requests for service because of the high incidence of credit card and check fraud, and it's made her wary.

But what worries her most is a pattern of scammers using these sites to con new small business owners.

"They are going after the newbies who may not be able to spot the scam, while we're out there, trying so hard to build good business and be an ethical business." She hopes that by sharing her story, new small business owners may become more aware of scams and red flags, so that they may "focus on the real customers."

"He didn't seem to care," she remembered. "That was a red flag."

What Katie wants other businesses to know:

- ➔ **Meet your clients in person when possible. Scammers always have a story about why they aren't there.**
- ➔ **Investigate the client to make sure they own the property prior to performing services or traveling for an estimate.**
- ➔ **If accepting credit card payment, make sure the name matches the client's ID.**
- ➔ **Do not cash checks if the amount does not match the estimate or contract amount.**

CREDIT CARD CONS TARGET SMALL BUSINESSES

John owns a used car lot in Crystal, Minnesota. He is dedicated to serving his customers and helping them go home with the perfect vehicle. John and his employees believe in going the extra mile to assist customers, so when one of those customers took advantage, John felt the need to warn others.

John and his team found themselves victims of a payment scam perpetrated by an alleged out-of-state student who needed a vehicle fast. The customer told them he had tried to purchase a vehicle elsewhere, but had to return the vehicle because the title wasn't clean. The customer explained that his funding was being held up because the return of the other vehicle had to clear.

John took the necessary personal information from the customer and even called his credit service provider to verify available funds on the customer's credit card. The paperwork was completed, payment was made via credit card, and the customer drove off the lot. John and his team didn't think about it until a month and a half later when their credit card provider called to tell them the funds didn't clear and he was out a vehicle and the payment. John

called his insurance company and was told that because the vehicle had been sold, the company would only be able to recoup a portion of the funds. His insurance company verified that there was a pattern with this customer and that they had indeed fallen victim to fraud.

The weeks that followed were stressful as John and his team waited to learn if the insurance company would renew their policy. If the policy didn't get renewed, he didn't know what would happen to his company. They were able to renew, but the cost was more than double what they had been paying because they are now considered a high risk.

John and his team spent numerous hours in meetings talking about how to protect the company from another incident such as this one. They decided they wouldn't take credit card payments for more than \$1000, they will ask more questions, and be more careful with whom they do business. Now his company is feeling distressed due to the higher insurance rates, the stress and the distrust toward new customers.

The customer explained that his funding was being held up because the return of the other vehicle had to clear.



What John wants other businesses to know:

- ➔ **Ask more questions.**
- ➔ **Verify information with more than one source.**
- ➔ **Consider potential risks and put a plan in place.**
- ➔ **Educate your employees to mitigate risks.**

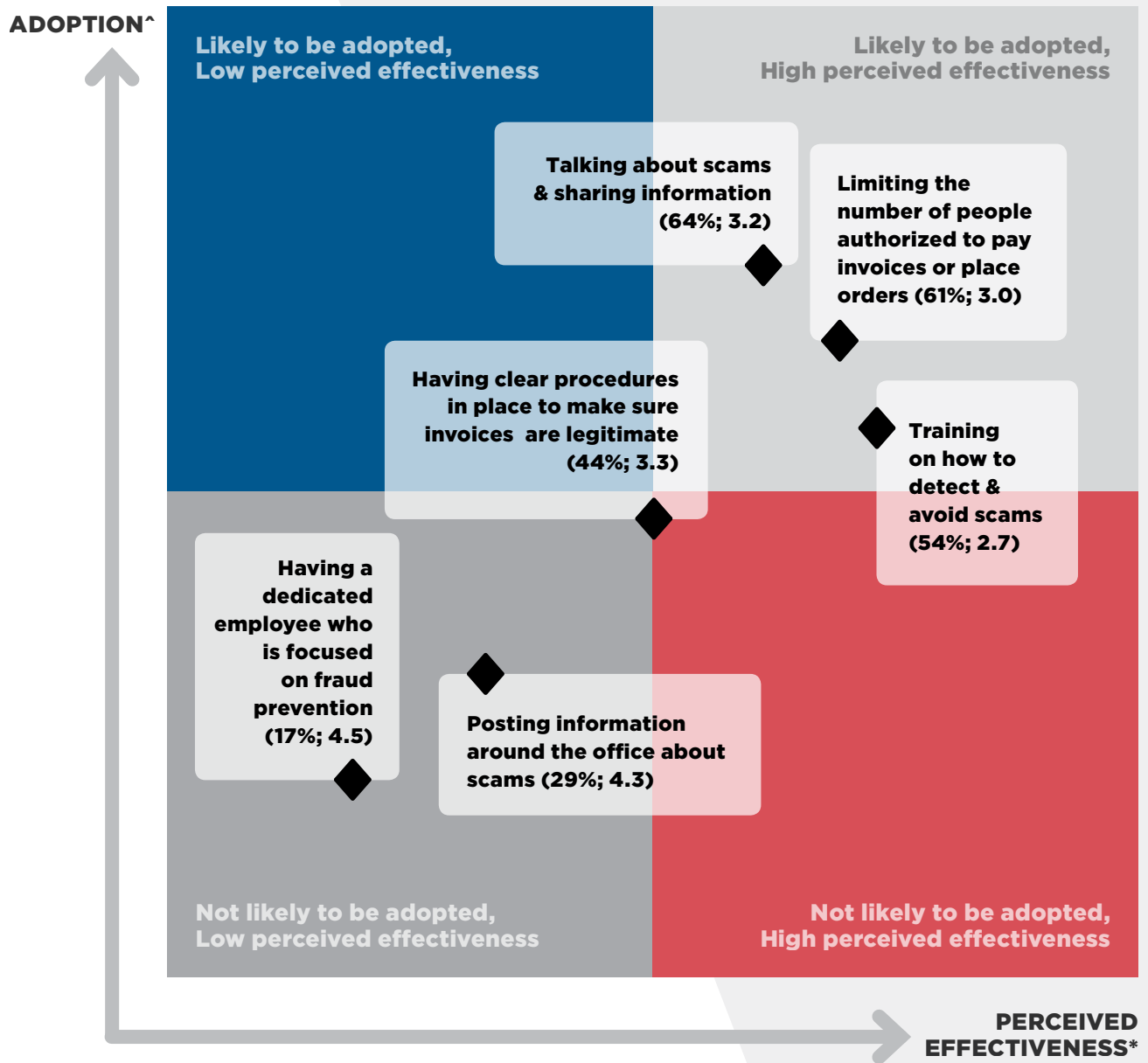


Preparedness: Being Proactive is Key

Being proactive is important in risk management, but because small businesses face so many other urgent priorities, prevention efforts often end up at the bottom of the priority list. When it comes to preparation to avoid and address scams, leadership is critical. Approximately eight out of 10 respondents identified the CEO/Owner/Partner as the most responsible for leading prevention efforts and dealing with scams if they happen. Fortunately, approximately six out of 10 businesses claimed to have scam prevention measures in place to safeguard their companies. This ongoing vigilance is crucial for prevention. As shown in Figure 8, the most effective preventive measures were perceived to be:

- Training on how to detect and avoid scams;
- Limiting the number of people authorized to pay invoices or place orders;
- Talking about scams and sharing information in employee meetings; and
- Having clear procedures in place to make sure invoices are legitimate.

FIGURE 8
Preventive Measures in Place:
Adoption vs. Perceived Effectiveness



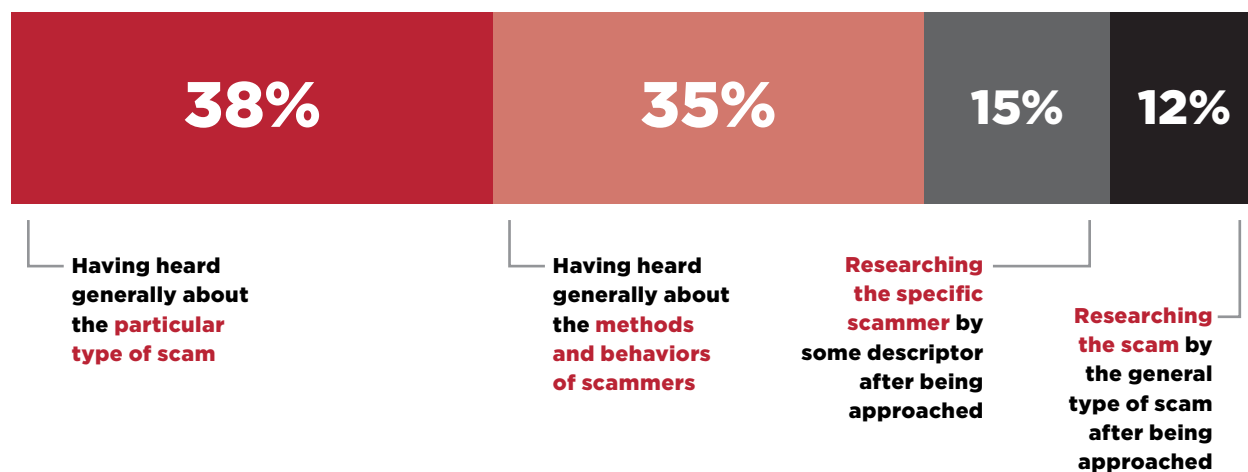
^ Question: What preventive measures do you have in place to safeguard your business? Select all that apply.

* Question: Rank the preventive measures in terms of how effective you think they are or would be if implemented. [1, most effective; 6, least effective]

Respondents were asked to identify factors that were most important in helping their business avoid becoming the victim of a scam attempt. The results (Figure 9) reinforce the importance of being proactive. They also suggest that general knowledge of the types of scams currently being deployed and the common methods and behaviors of scammers prior to being targeted are highly effective preventive measures. More than 70 percent of respondents identified one of these two factors as most effective, while 27 percent identified research done after being approached by a scammer as most effective. This is consistent with the results from our previous study, *Cracking the Invulnerability Illusion*.⁹ The most effective preventive measure is to learn about scams, the most common scam types and how they are perpetrated.

FIGURE 9

Think of a time your business was the target of an unsuccessful scam attempt. From the options below, what was most helpful in avoiding a scam?



The top self-identified (i.e., fill in the blank) choices to research scams for both the BBB Accredited Business and Non-Accredited Business samples (calculated separately) were:

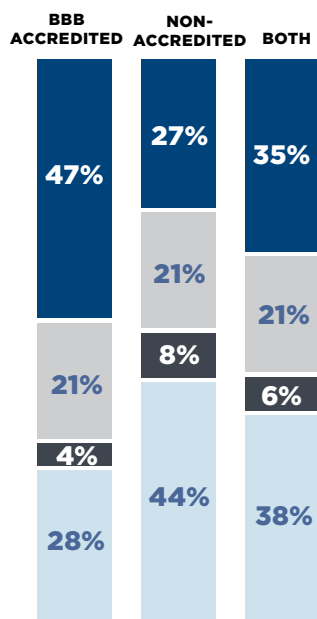


FIGURE 10
TOP THREE CHOICES TO RESEARCH A BUSINESS SCAM

Question: What organization or entity would be your first choice to research a business scam?

■ BBB
■ GOOGLE
■ INTERNET
■ OTHERS

⁹ Emma Fletcher and Rubens Pessanha. *Cracking the Invulnerability Illusion: Stereotypes, Optimism Bias, and the Way Forward for Marketplace Scam Education*. BBB Institute for Marketplace Trust, 2016. www.bbb.org/truthaboutscams.

To help inspire action, below are a few selected responses on what businesses are doing to prepare for and avoid scams.

“All employees are **fully trained** to deal with all possible risks to our company operations. We have a very **effective set of policies** in effect which must be adhered to by every employee every day.”

“A general sense of **alertness**. Staying informed.”

“Be vigilant and cautious. **Investigate** always.”

“Being **suspicious** of all inquiries.”

“Ask proper questions to prevent it. Stay in **good communication with clients.**”

“Always double or triple **checking sources** before starting anything... if it sounds too good to be true...”

“Always **look carefully** before opening up emails.”

“Always look them up on the internet and **read the scam alerts** provided by the BBB.”

“**Awareness** through training, education, and discussions.”

“Have team meeting to **educate** [employees].”

“**Do not give out any confidential information.**”

“Just relaying knowledge and we did invest in a pretty **secure firewall** a year ago for our IT network.”

“Constantly **comparing notes with other small business owners**. I subscribe to a scam alert service.”

“Our business does business with **trusted partners.**”

“**Training** on opening emails and making sure they are from who they say they are from. Not clicking on links. Not downloading any programs without approval.”



Looking Forward

Forty-three percent of small businesses believe they will likely be the target of a business scam in the next 12-month period, and about one out of 10 small businesses expects to lose money to a scam. Small businesses cite lack of information, resources and time as the top factors that hinder security efforts against business scams (Figure 11).

Findings also show that news stories or articles and word of mouth are the top sources of information about business scams most likely to reach the business community (Figure 12). Looking forward, it is critical that BBB and other like-minded organizations create and distribute information about the best ways to prevent scams aimed at small businesses, and encourage the business community to join the effort to create and share best practices. It is also paramount that as organizations and agencies engaged in business education think about their approach to outreach, they consider how best to engage the media to tell this important story.

FIGURE 11

What is the top factor that hinders your organization's ability to advance security efforts against business scams?

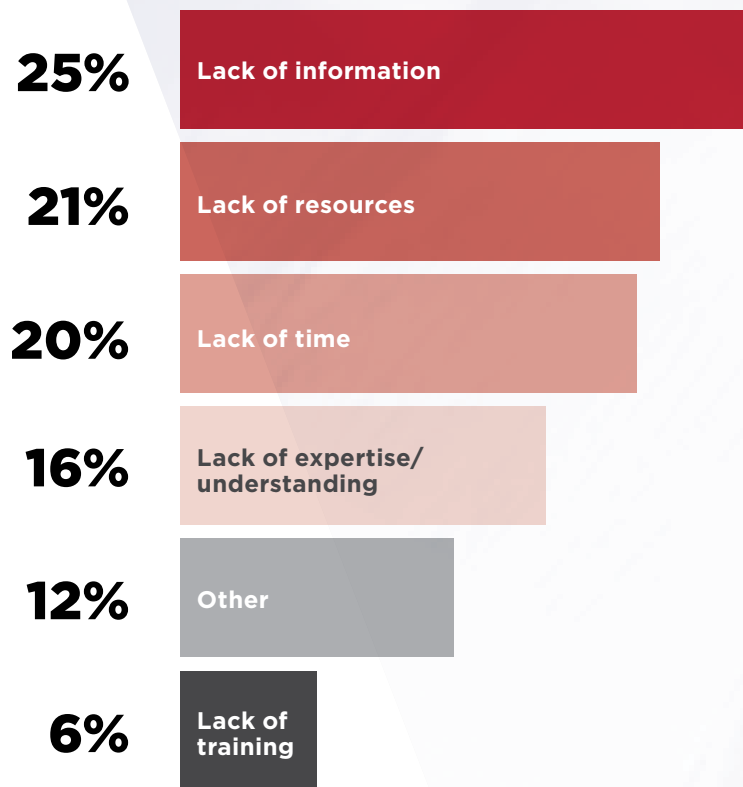
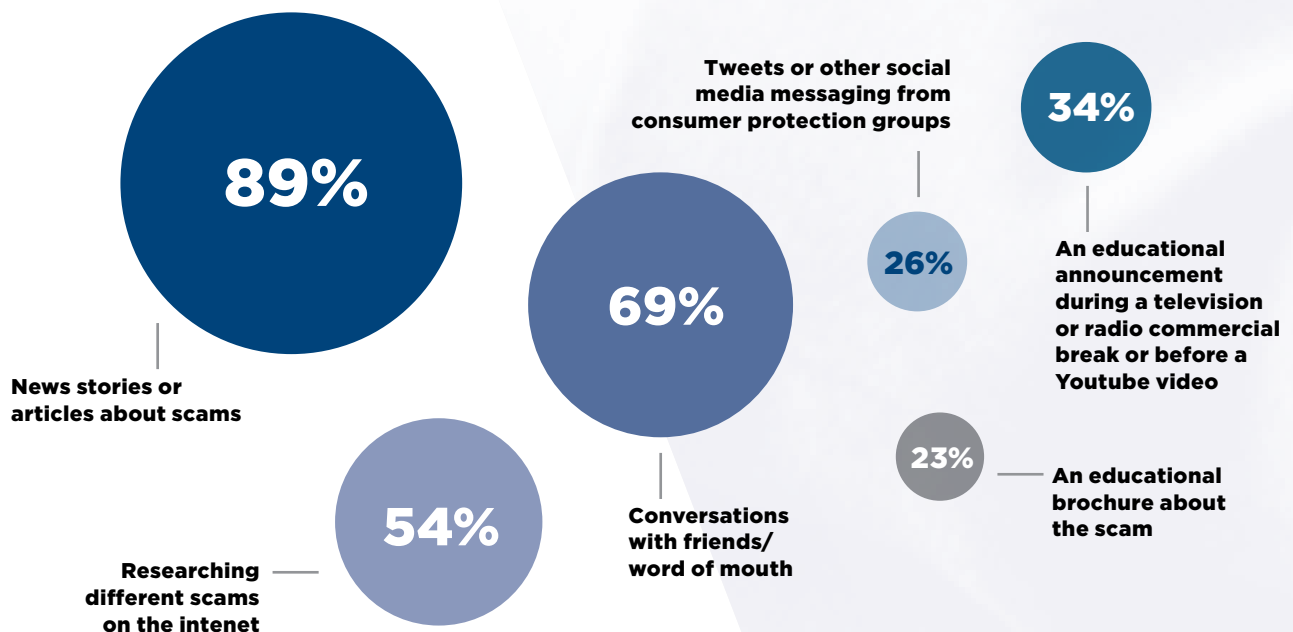


FIGURE 12

Of the following sources of information about business scams, choose the top three that are most likely to reach you.



Reporting Practices

Small businesses are not known to report scams in great numbers.

However, a surprising 91 percent of businesses responding to our survey indicated that they would report scams. This suggests businesses are open to or aspire to reporting scams. Their primary motive to do so would be to warn others about the scam (Figure 13). For those who are unlikely to report, as shown in Table 5, the main reasons were the time involved, the prevalence of the problem (i.e., too many), the perceived null impact of reporting (i.e., doesn't make a difference), and the lack of knowledge about to whom/how to report. In relation to this last point, BBB Scam Tracker (see box on page 34) could serve as an easy method for reporting scams.

In order to verify our findings from the survey research, we estimated via text mining that approximately 5 percent of the scams reported to BBB Scam Tracker in 2017 targeted small businesses. We divided this estimate by the number of small businesses in the United States and compared this ratio with the adult population reporting ratio. Based on our estimates, small businesses appear less likely than the public at-large to report scams.

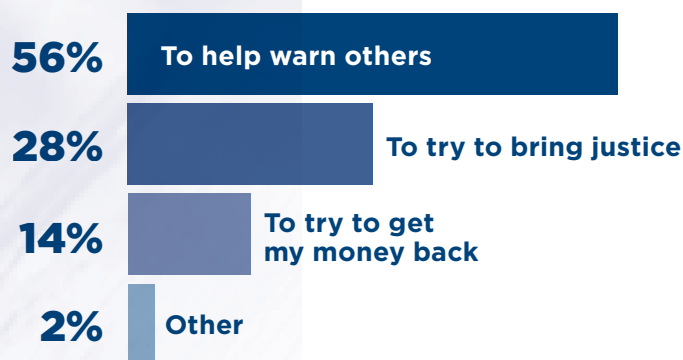


FIGURE 13
Reporting Practices

If your business were the target of a scam, would you report it?



If you were to report a business scam, what would be your primary motivation?



Why wouldn't you report the business scam?

FIGURE 14
First Choice to Report a Scam

The top self-identified choices (i.e., fill-in-the-blank formatted question) to report business scams (Question: What organization or entity would be your first choice to report a scam?) for both the BBB Accredited Business and Non-Accredited Business samples were: BBB, the police and the Office of the Attorney General.

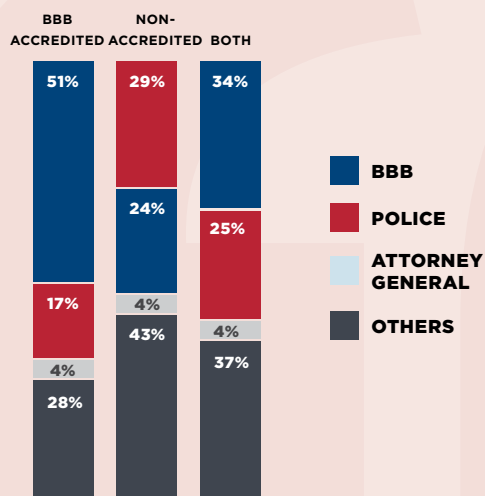


TABLE 5
Why wouldn't you report the business scam?

Don't Have Time/ Too Much Work/ Too Many

"No easy way to report attempted scams."

"Too numerous, time consuming and nothing would be done."

"Don't have time."

Don't Know to Whom or How to Report

"Do not know who to report to."

"I wouldn't know how."

Doesn't Make a Difference to Report

"Don't believe anything would or could be done about it."

"Every time I have tried to report it to authorities, they always said they didn't have manpower to deal with it."

"I already have and there were no results or return of money."

It Depends

"Depends on how much I lost."

"Depends on how critical the scam was."

BBB Scam Tracker

Learning About and Reporting Scams Made Easy

To help businesses fight back, BBB is using technology to help businesses fight against increasingly high-tech and complex scams. BBB Scam Tracker, launched in 2015, is an online tool that enables the public and businesses to report scam activity, from fake-invoice scams to phishing scams to directory listing and advertising scams.

BBB Scam Tracker collects and presents scam data in a searchable online “heat map,” showing users the number and types of scams and hoaxes reported in their communities.

The tool provides a window on the scam landscape, enabling data-driven alerts and tips based on current information. Data is also shared with law enforcement agencies for investigative purposes.

BBB Scam Tracker’s crowdsourced approach is designed to leverage the altruistic impulse of people. The details of a scam report appear on the BBB Scam Tracker map alongside the stories of other victims and targets who have come forward to help. The information is easily searchable by key word, so visitors can quickly find out if others have had similar experiences.

ATTENTION

When reporting business scams to BBB Scam Tracker, please select “Business” on the question below:

Did this scam target an individual or a business?

- ***Individual***
- ***Business***

LEARN → PROTECT → REPORT

Go to [BBB.org/ScamTracker](https://www.bbb.org/scamtracker)

Conclusion

While small business scams abound, scammers do not always succeed in claiming a victim. Fighting back and passing on the message to help others is an important step in advancing marketplace trust. Scams are continuously evolving, and it's difficult to keep up with all of them. But if you can just remember these four things, you can avoid most scams and help protect your business.¹⁰

Train and inform your employees.

- Explain to your staff how scams happen and share information with them.
- Encourage your employees to talk to their coworkers if they spot a scam.
- Train employees not to send passwords or sensitive information by email, even if the email seems to come from a manager.

Verify invoices and payments.

- Never pay unless you know the bill is for items that were actually ordered.
- Make sure procedures are clear for approving invoices or expenditures.
- Limit the number of people who are authorized to place orders and pay invoices.
- Make sure major spending can't be triggered by an unexpected call, email or invoice.
- Pay attention to how someone asks you to pay. Tell your staff to do the same.

Be tech-savvy.

- Don't believe your caller ID. Imposters often fake caller ID to gain your trust.
- Remember that today it's easy to create legitimate-looking email addresses and websites.
- Stop and think about whether it could be a scam before you click.
- Don't open attachments or download files from unexpected emails.
- Secure your organization's files, passwords, and financial information.

Know who you're dealing with.

- Before doing business with a new company, search the company's name online with the term "scam" or "complaint." Read what others are saying about that company. Check BBB.org to see if there is a Business Profile on the company.
- When it comes to products and services for your business, ask for recommendations from other business owners in your community. Positive word-of-mouth feedback from trustworthy people is more reliable than any sales pitch.
- Don't pay for "free" information.

¹⁰Download educational material at [BBB.org/SmallBusiness](https://www.bbb.org/SmallBusiness).

In order to thrive and prosper, businesses must be able to operate in a fair and transparent marketplace. Scammers undermine trust, distort the playing field, and siphon off money from legitimate transactions that benefit businesses, thus impeding economic growth. Small business scams, although similar in many ways to scams that target consumers, could be hampered through a more focused and segmented approach in research, reporting, and educational outreach. We know that we have much more to learn and do, but we hope that this report will serve as a step forward in expanding this important conversation.

Lastly, we have included a few more resources (see below) on how business owners can better prepare their employees to prevent scams and help increase awareness among the business community on this important topic.

Resources: Learn How to Protect Your Business from Scams

For more tips on protecting your organization from scams, visit [FTC.gov/SmallBusiness](https://www.ftc.gov/smallbusiness).

Stay connected with the FTC by subscribing to the FTC's business blog at [FTC.gov/Subscribe](https://www.ftc.gov/subscribe) or signing up for scam alerts at [FTC.gov/Scams](https://www.ftc.gov/scams).

Research businesses at [BBB.org](https://www.bbb.org) to find out about previous customers' experiences.

Visit the U.S. Small Business Administration (SBA): [sba.gov/content/Beware-Scams](https://www.sba.gov/content/beware-scams).

If you spot a scam, report it to [FTC.gov/Complaint](https://www.ftc.gov/complaint) and to the Better Business Bureau at [BBB.org/ScamTracker](https://www.bbb.org/scamtracker). Your report can help stop the scam.

Learn more about scams that target consumers in the BBB Scam Tracker Annual Risk Report at [BBB.org/RiskReport](https://www.bbb.org/riskreport).

Learn how to protect your business and your customers with BBB's "5 Steps to Better Business Cybersecurity" at [BBB.org/Cybersecurity](https://www.bbb.org/cybersecurity).

Alert your state Attorney General. You can find contact information at [NAAG.org](https://www.naag.org).

Download copies of this publication at [BBB.org/SmallBusiness](https://www.bbb.org/smallbusiness). Order free publications about avoiding fraud at [FTC.gov/BulkOrder](https://www.ftc.gov/bulkorder).

Authors/Contributors

Dr. Rubens Pessanha, senior director of market research, insights and strategy at the Council of Better Business Bureaus, 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 recently completed his doctorate at George Washington University. As a hobby, Pessanha teaches project management, business ethics, strategy and marketing at Strayer University.

Melissa “Mel” Trumpower is the director of programs and operations for the BBB Institute for Marketplace Trust. She has more than 20 years of experience working with not-for-profits and associations. In her last position, she created and launched a groundbreaking disaster-recovery technology tool that ensures the most-needed product donations are delivered to the right place at the right time. Trumpower has a bachelor’s degree from Cornell University and a master’s degree from Johns Hopkins University.

Amy Gwiazdowski is the director of internal strategic communications for the Council of Better Business Bureaus, actively engaging with BBBs across North America to better understand their needs. Before joining CBBB, she was the communications director for a business trade association for companies with employee stock ownership plans (ESOPs) in Washington, DC. Previously, she spent a few years working for the publishing industry’s trade association, where she focused on First Amendment and copyright issues.

Matt Scandale has worked for the Council of Better Business Bureaus 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.

Melissa Bittner is the curriculum development and training manager with the BBB Institute for Marketplace Trust. Throughout her career, she has created educational programs, tools, and experiences that bring communities together toward a common goal. Her work has supported the growth of youth programs, adult training, and professional development opportunities, as well as citywide festivals and campaigns. She has a master’s degree in public administration with a concentration in ethical leadership from Marist College.

Alexis Chng-Castor, director of brand creative at the Council of Better Business Bureaus, is an experienced marketer and creative director with an award-winning brand portfolio. Native to Singapore and fluent in three languages, she leverages her knowledge and experience with Asian markets in all aspects of marketing and design. During her free time, she channels her love for design into her personal projects.

Lisa Jemtrud provides overall management and leadership of the foundation, communications, and community relations divisions for the BBB of Minnesota and North Dakota. Jemtrud holds a master's degree in administration of justice from Southern Illinois University with an emphasis in alternative dispute resolution and white-collar crime. She is past president of the Society of Consumer Affairs Professionals, Minnesota Chapter. She currently participates in Leadership Twin Cities and co-chairs the Coalition Against Marketplace Fraud, a regional law enforcement partnership.

Heather Aal serves the BBB of Minnesota and North Dakota in community relations. She has taken the lead in educational efforts regarding scams, fraud, and the importance of business ethics, working with students, seniors, and business leaders. Aal has a bachelor's degree from North Dakota State University and is completing her master's from Arizona State University in nonprofit leadership and management.

Thanks to the following Better Business Bureaus that made this project possible.

BBB of Central Oklahoma

BBB of the Northwest and Pacific

BBB of Minnesota and North Dakota

BBB of Western Pennsylvania

BBB of Northern Colorado and Wyoming

BBB of Wisconsin

We thank the BBB Institute for Marketplace Trust for its collaboration on this report.

The Better Business Bureau Institute for Marketplace Trust (BBB Institute), the educational and research foundation of the Better Business Bureau, works with BBBs in communities across North America to support BBB's mission of advancing marketplace trust. By focusing on 21st century digital marketplace trust issues, such as cybersecurity, data ethics and digital literacy, the BBB Institute supports trustworthy businesses while protecting and empowering consumers. In 2017, the BBB Institute reached more than 20 million consumers through education and awareness programs such as BBB Scam Tracker, BBB AdTruth, Smart Investing, the Military & Veterans Initiative and Digital IQ.





For more than 100 years, from small community stores to multinational enterprises, BBB has been on the forefront of positive marketplace change by partnering with leading companies committed to the best practices of business ethics, marketplace excellence and effective industry self-regulation. Trust always matters. BBB is deeply committed to building and advancing a better marketplace, a trusted marketplace for all.

Council of Better Business Bureaus

3033 Wilson Blvd., Suite 600
Arlington, VA 22201

www.bbb.org | insights@council.bbb.org