Scams and Your Small Business:

A Guide for Business

When scammers go after your business or non-profit organization, it can hurt your reputation and your bottom line. Your best protection? Learn the signs of scams that target businesses. Then tell your employees and colleagues what to look for so they can avoid scams.

▶ Scammers' Tactics

- **Scammers pretend to be someone you trust.** They impersonate a company or government agency you know to get you to pay. But it's a scam.
- **Scammers create a sense of urgency, intimidation, and fear.** They want you to act before you have a chance to check out their claims. Don't let anyone rush you to pay or to give sensitive business information.
- **Scammers ask you to pay in specific ways.** They often demand payment through wire transfers,

cryptocurrency, or gift cards. Don't pay anyone who demands payment this way. It's a scam.

▶ Protect Your Business

Train Your Staff

- Your best defense is an informed staff. Train employees not to send passwords or sensitive information by email, even if the email seems to come from a manager. Explain to your staff how scams happen and encourage them to talk with their coworkers if they suspect a scam. Order free copies of this brochure at **ftc.gov/bulkorder** and share them with your staff.

Verify Invoices and Payments

- Make sure procedures are clear for approving purchases and invoices and ask your staff to check all invoices closely. Pay attention to how someone asks you to pay and tell your staff to do the same. If someone demands that you pay with a wire transfer, cryptocurrency, or gift cards, don't pay. It's a scam.

Spot Tech-Related Scams

- Since scammers often fake their phone numbers, don't trust caller ID. If you get an unexpected text message or email, don't click any links, open attachments, or download files. That's how scammers load malware onto your network or try to convince you to send money or share sensitive.

information. Scammers sometimes even hack into the social media accounts of people you know, sending messages that seem real — but aren't. Learn more about protecting your small business or non-profit organization from cyber scammers and hackers: check out **Cybersecurity for Small Business** at **ftc.gov/cybersecurity**.

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. Ask people you trust for recommendations. You also may be able to get free business development advice and counseling through programs like **SCORE.org**.

▶ Common Scams that Target Small Business

Fake Invoices and Unordered Merchandise

Scammers create phony invoices that look like you ordered products or services for your business. They hope the person who pays your bills will assume the invoices are real and make the payment. Except it's all fake. Or a scammer might call, claiming they want to "confirm" an existing order, "verify" an address, or offer a "free" catalog or sample. If you say yes to any of those, unordered merchandise will arrive at your doorstep — followed by high-pressure demands to

pay for it. Don't pay. And remember, if you receive merchandise you didn't order, you have a legal right to keep it and use it for free.

Online Listing and Advertising Scams

Scammers try to fool you into paying for nonexistent advertising or a listing in a phony business directory. They may ask you to give your contact information for a "free" listing, or say the call is simply to "confirm" your information. Later, you'll get a big bill, and the scammer may use details — or even a recording — of the earlier call to pressure you to pay.

Business and Government Impersonation Scams

Scammers pretend to be someone you know or trust and try to scare or rush you into paying or giving them information. For example:

- Scammers say they're calling from a utility company and your gas, electric, or water service is about to be interrupted because of a (fake) late bill.
- Scammers say they're a government agent and threaten to suspend your business licenses, fine you, or even sue you. They might say it's because you owe taxes or need to renew a license or registration.
- Some scammers convince you to buy workplace compliance posters that you can get for free from the U.S. Department of Labor.

- Some scammers trick you into paying to apply for so-called business grants from government programs that turn out to be fake.
- Scammers impersonate the U.S. Patent and Trademark Office and threaten that you'll lose your trademark if you don't pay a fee immediately. Other times, they lie and say you owe money for additional registration services.
- Some scammers say they're calling from a tech company, threatening that your business will lose its website URL if you don't pay immediately.

Tech Support Scams

Tech support scams start with a call or an alarming pop-up message on your screen. The scammers pretend to be from a well-known tech company, telling you there is a problem with your computer's security. Their goal is to get your money, access to your computer, or both. They may ask you to pay to fix a problem you don't really have, enroll your business in a nonexistent or useless computer maintenance program, or sneak on your computer network to grab confidential data they can use to commit identity theft.

Social Engineering, Phishing, and Ransomware

Cyber scammers can trick employees into sending them money or giving up confidential or sensitive information like passwords or bank information. It often starts with a phishing email, social media contact, or

a call that seems to come from a trusted source — for example, a supervisor or other senior employee — that creates urgency or fear. Other emails may look like routine password update requests or other automated messages, but are actually attempts to steal your information. Scammers also can use malware to lock organizations' files and hold them for ransom.

Business Coaching Scams

Some scammers sell bogus business coaching programs, often using fake testimonials, videos, seminar presentations, and telemarketing calls. They falsely promise amazing results if you pay for their exclusive "proven" system to succeed in business. They also may lure you in with low initial costs, only to ask for thousands of dollars later. In reality, the scammers leave budding entrepreneurs without the help they sought and with thousands of dollars of debt.

Changing Online Reviews

Some scammers claim they can replace negative reviews of your product or service, add positive reviews, or boost your scores on ratings sites. However, posting fake reviews is illegal. FTC guidelines say endorsements — including reviews — must reflect the honest opinions and experiences of the endorser.

Credit Card Processing and Equipment Leasing Scams

Some scammers promise lower rates for processing credit card transactions, or better deals on equipment leasing. These scammers resort to fine print, half-truths, and flat-out lies to get a business owner's signature on a contract. Some unscrupulous sales agents ask business owners to sign blank documents. (Don't do it.) Others have been known to change terms after the fact. Ask the salesperson to give you copies of all documents right then and there. If they refuse or put you off with a promise to send them later, that could be a sign you're dealing with a scammer.

Fake Check Scams

Some scammers give you what seems like a plausible reason to overpay you with a check. Then, they'll ask you to send the extra money back to them or to someone else. But the check will be fake, even though it might show up as "cleared" in your account. By the time the bank discovers the check was bad, the scammer already has the money you sent them. You'll be stuck repaying the bank.

▶ Other Questionable Practices

Sometimes scammers hide behind other questionable practices — like claiming to offer big-money gig economy jobs, but then failing to live up to their money-making promises. Or they may try to sell

you unnecessary services with the false claim that you need to pay to improve your business's credit report. And after natural disasters strike, unlicensed contractors and scammers may show up with false promises that they'll get your business back up and running with quick repairs, clean-up, or debris removal that never happens.

▶ Learn More

- For more advice on protecting your organization from scams, visit **ftc.gov/SmallBusiness**.
- Stay connected with the FTC by subscribing to the FTC's Business Blog at **ftc.gov/subscribe**.

▶ Report

- If you spot a scam, report it to **ReportFraud.ftc.gov**. Your report can help stop the scam.
- Alert your state Attorney General. You can find contact information at **NAAG.org**.

▶ Engage

- Remember: Your best defense is an informed workforce. Talk to your staff about how scams happen.
- Share this brochure with your staff.
- Order free copies of this brochure in English, Spanish and other languages at **ftc.gov/bulkorder.**

About the FTC

The FTC works to help small business owners avoid scams, protect their computers and networks, and keep their customers' data safe. To find information for small business, go to **ftc.gov/SmallBusiness**. There you'll find information about scams targeting small business and how to avoid them, and information on cybersecurity for small business to help owners keep their networks safe.

To get the latest information for small business, subscribe to the FTC's Business Blog at **ftc.gov/subscribe**.

This brochure is part of the FTC's efforts to help small business owners avoid scams. It explains common scams that target small businesses and non-profit organizations, describes scammers' tactics, and provides steps business owners can take to protect their company from scams. Order print copies for free at **ftc.gov/bulkorder**.

FEDERAL TRADE COMMISSION

business.ftc.gov

July 2023