Linkun Foundation

EDUCATE · EQUIP · ELEVATE

FREE TOOLKIT · EVERY SMALL BUSINESS

Fraud Protection Toolkit

The scams that target small businesses most, the warning signs, and the simple habits and bank tools that stop them, plus what to do in the first hour if you've been hit.

- Most fraud against small businesses comes from impersonation: a fake vendor, boss, bank, or government agency asking you to pay or share a code.
- One habit stops most of it: verify any change in payment instructions by calling a number you already have, never the one in the message.
- Ask your bank about fraud tools such as Positive Pay, payment alerts, and dual approval for transfers.
- If you've been hit, call your bank right away. Speed matters most in the first hours.

Fill it in on screen (any PDF reader) or print it. Prefer a version that tailors itself to your business? Use the interactive toolkit at linkunfoundation.org/resources/toolkits/fraud-protection.

linkunfoundation.org · 444 Huntington Drive, Arcadia, CA 91006 · hello@linkunfoundation.org

What's inside

01 The scams that target small businesses

02 Habits that stop most fraud

03 Tools to ask your bank about

04 Lock down your accounts

05 Rate your risk

06 If you've been hit

07 Use AI as a second pair of eyes

How to use the business-type notes: sections marked “For wholesalers”, “For storefronts” and so on apply only to that kind of business. Read the general guidance, then the notes that fit you.

SECTION 01

The scams that target small businesses

Scam	How it works	Warning sign
Fake payment change	An email that looks like it's from a real supplier says their bank details changed and asks you to pay the new account.	Any request to change where you send money, especially with urgency.
Boss or owner impersonation	A message that appears to come from the owner or a manager asks an employee to buy gift cards or send a quick wire.	Secrecy, urgency, gift cards, a new phone number.
Check fraud and washing	Checks you mail are stolen, the ink is washed off, and the payee and amount are rewritten. Or your check details are used to print fakes.	Checks clearing for amounts or payees you don't recognize.
Overpayment scam	A "customer" pays too much and asks you to refund the difference. Their original payment later bounces or is reversed.	Overpayment plus a request to send money back fast.
Fake invoices and directory listings	Bills for services you never ordered: directory listings, domain renewals, trademark or filing services that look official.	An official-looking invoice from a company you don't know.
Government impersonation	Calls or letters claiming you owe the IRS, the state, or a utility and must pay today by gift card, wire, or crypto.	Threats of arrest or shutoff and unusual payment methods.
Account takeover	A fake login page or a call "from your bank" tricks you into sharing a password or one-time code.	Anyone asking you to read back a verification code.
Payment app and card scams	Fake payment screenshots, card testing with many small charges, or "friendly fraud" chargebacks after delivery.	Payments you can't see in your own account, bursts of tiny charges.

FOR CALIFORNIA BUSINESSES

Watch for mailers that look like state notices offering to file your Statement of Information or other filings for a large fee. You can file directly with the California Secretary of State for much less. Always check who is asking.

FOR ONLINE SELLERS

Watch for card testing (many small orders in a short time), orders with mismatched billing and shipping addresses, and requests to ship to a freight forwarder. Turn on your payment processor's fraud filters and require signatures on high-value deliveries.

FOR STOREFRONTS

Train staff on counterfeit bills, refund fraud, and "quick change" tricks. Limit who can process refunds, and review refunds and voids weekly.

FOR BUSINESSES THAT WORK WITH SUPPLIERS ON TERMS

Supplier payment changes are the costliest scam for businesses that pay vendors regularly. Keep a vendor list with phone numbers you verified when you started working together.

SECTION 02

Habits that stop most fraud

- [ ] Verify any change in payment instructions by calling the vendor at a number you already have on file.
- [ ] Never share a one-time passcode or password with anyone who calls or texts you, even if they say they're from your bank.
- [ ] Require two people to approve payments over a set amount, or approve them yourself from a second device.
- [ ] Pay suppliers by ACH or card when possible instead of mailing checks. If you mail checks, use the post office counter, not a mailbox.
- [ ] Use a separate business account and card for online purchases and subscriptions.
- [ ] Reconcile your bank accounts at least weekly, and daily if you have many transactions.
- [ ] Pause and check any message that is urgent, secret, or asks for gift cards, wires, or crypto.
- [ ] Train every employee to say: "I'll call you back on the number we have."

SECTION 03

Tools to ask your bank about

Tool	What it does
Positive Pay (checks)	You send the bank a list of checks you wrote. Checks that don't match are held for your review.
ACH debit block or filter	Only companies you approve can pull money from your account.
Payment and balance alerts	Texts or emails for transfers, large withdrawals, or low balances.
Dual approval for transfers	A second person must approve wires and ACH payments.
Separate accounts	One account for incoming payments and another for paying bills limits what a thief can reach.

Many community banks and credit unions offer these tools to small businesses at low or no cost. Ask which ones you have and turn them on.

SECTION 04

Lock down your accounts

- [ ] Turn on two-step verification for email, banking, payroll, payment processors, and your website.
- [ ] Use a password manager and a different password for every account.
- [ ] Keep your computer, phone, and point-of-sale software updated.
- [ ] Give each employee their own login, and remove access the day someone leaves.
- [ ] Back up important files automatically, with one copy offline or in a separate account.
- [ ] Use a separate email address for banking that isn't published on your website.
- [ ] Make sure you, not a former web designer, own your domain name and website accounts.

SECTION 05

Rate your risk

Quick fraud risk score

Score each from 0 (not true) to 2 (very true).

We mail paper checks to vendors 0–2

One person can send payments without anyone else seeing them 0–2

Some accounts don't have two-step verification 0–2

We look at bank activity less than once a week 0–2

Staff haven't been told how payment scams work 0–2

We don't call to verify vendor bank changes 0–2

= Your risk score (0 to 12; 5 or more means act this month)

SECTION 06

If you've been hit

The first hour

- [ ] Call your bank's fraud line right away and ask them to stop or recall the payment.
- [ ] Change passwords on email and banking from a device you trust, and turn on two-step verification.
- [ ] If a vendor's email was spoofed or hacked, call the vendor so they can warn others.
- [ ] Write down what happened: dates, amounts, account numbers the money went to, and copies of messages.

The first week

- [ ] Report internet and email fraud to the FBI at ic3.gov.
- [ ] Report scams to the Federal Trade Commission at ReportFraud.ftc.gov.
- [ ] File a police report if your bank or insurer needs one.
- [ ] Tell your insurance agent. Some business policies cover cyber or crime losses.
- [ ] Review what let it happen and add one new control.

SECTION 07

Use AI as a second pair of eyes

An AI assistant can help you spot red flags in a message before you act on it. Remove names, account numbers, and personal details before pasting.

AI PROMPT Is this message a scam?

I run a {industry} business in {location}. I received the message below and need to decide whether it's legitimate.
Point out every red flag (urgency, payment changes, unusual payment methods, mismatched sender details, requests for codes), rate how likely it is to be a scam, and tell me exactly how to verify it safely without using any contact details in the message.
Message (personal and account details removed):
[paste the message here]

Replace the [brackets] with your details, then paste into ChatGPT, Claude, Gemini, Copilot or any AI assistant.

AI PROMPT Write my payment security policy

Write a one-page payment security policy for my {industry} business. Team size: {size}. We sell through {channel} and our customers are {buyer}.
Cover: who can approve payments and up to what amount, how we verify vendor bank changes, rules for gift cards and wires, refund approvals, password and two-step verification rules, and what employees should do if they suspect fraud.
Use plain language a new employee can follow.

Replace the [brackets] with your details, then paste into ChatGPT, Claude, Gemini, Copilot or any AI assistant.

Frequently asked questions

What is the most common fraud against small businesses?

Impersonation scams are among the most common and costly: messages that pretend to be a supplier, the owner, a bank, or a government agency and ask for a payment or a code. Fake changes to a vendor's bank details are especially costly.

How can I protect my business from check fraud?

Pay by ACH or card when you can, mail checks at the post office counter, reconcile your account often, and ask your bank about Positive Pay, which holds checks that don't match the list you send.

What should I do if I sent money to a scammer?

Call your bank's fraud line immediately and ask them to recall the payment. Then secure your email and banking passwords, document everything, and report it at ic3.gov and ReportFraud.ftc.gov.

Does my business need two-step verification?

Yes. Turn it on for email, banking, payroll, and payment accounts. It stops most account takeovers, even when a password has been stolen.

FREE 1:1 COACHING

Talk it through with a mentor

Bring this toolkit, your numbers, and your questions. Book a free session:
https://calendar.app.google/Y9th1oVrDYsY7tbk8

This toolkit is educational and is not legal, tax, accounting, or investment advice. Rules change and vary by state; confirm decisions with a qualified professional or a free advisor at your local Small Business Development Center. © Linkun Foundation, a 501(c)(3) nonprofit.