FLUXLABS

GUIDE · FOR OWNERS AND BOOKKEEPERS

Fake invoices and payment fraud

Payment fraud costs businesses more than any other online crime. A few simple rules stop almost all of it.

Scammers don't need to hack your bank. They only need someone in accounting to believe one email. They watch a real conversation, or fake one, and then ask for a payment to go somewhere new.

How it usually happens

1. **Changed bank details.**
   A real vendor's email account is broken into. The next invoice arrives from their real address with "our new bank account".
2. **The boss in a hurry.**
   "I'm in a meeting, please wire this today and keep it quiet." It's from a lookalike address, or the owner's hacked account.
3. **Fake invoices.**
   An invoice for something you never ordered, small enough that nobody asks: domain renewals, directory listings, office supplies.
4. **Payroll changes.**
   An employee "asks" HR to send their paycheck to a new account.
5. **Closing and settlement money.**
   Law firms, title companies and their clients get fake wiring instructions right before a closing.

> **The warning sign is the change, not the sender**
> These emails often come from the real address of someone you know, because their account was broken into. A correct sender doesn't make a request safe.

Rules that stop it

- [ ] **Call to confirm any new or changed bank details**, using a phone number you already had, never one from the email.
- [ ] **Two people for new payees and changes.** One person sets it up, a second checks and approves.
- [ ] **A waiting period** for changed details, for example one business day, so a real vendor has time to notice.
- [ ] **Payroll changes in person or by phone**, never by email alone.
- [ ] **Check new vendors** before the first payment: a real address, a phone number you looked up yourself.
- [ ] **Ask your bank** about payee confirmation and alerts for new wires.
- [ ] **Turn on two-step sign-in** for email, banking and accounting systems, so one stolen password isn't enough.
- [ ] **Train everyone who touches money**, at least once a year, using real examples.

If money already went out

1. **Call your bank's fraud line now.**
   Ask them to recall the payment. The first few hours matter most.
2. **Call your IT support.**
   They can check whose email was broken into and lock it down.
3. **Report it at ic3.gov.**
   The FBI's internet crime center can sometimes help freeze the money.
4. **Call your insurance agent.**
   Many cyber and crime policies cover this, but only if you report it quickly.

Check a suspicious email for free