SMALL BUSINESS SCAMS

Federal Trade Commission | business.ftc.gov

An invoice bears the familiar "walking fingers" logo and the name "Yellow Pages." It says you owe hundreds of dollars for a business listing. Perhaps you get a letter saying you could lose your web address or trademark if you don't send money immediately. Maybe some toner cartridges or other office supplies show up at your office out of the blue — with a bill.

What's going on? It's a scam by con artists who know some small and medium-sized businesses, churches, and not-for-profit groups will end up paying the bogus invoices in the mistaken belief they owe money or that it's simply a misunderstanding.

What's the best way to protect your business? Learn the telltale signs of five common scams so you can stop fraudsters in their tracks.

The Directory Listing Scam

In this operation, con artists all businesses, claiming to "verify" or "confirm" a company's contact information for its listing in a business directory. Of course, there's no existing listing — and maybe not even a real business directory — but the employee who picked up the phone doesn't know that. Persuasive double-talkers bulldoze the employee into saying yes. Later, if the company complains it didn't agree to the listing, the fraudsters may play back a tape of the call (which might have been doctored) as "proof."

Next, the scammers send urgent invoices for hundreds of dollars. The invoices might even include the "walking fingers" logo and the Yellow Pages name. In many cases, the person paying the bills will simply cut a check, not realizing that the company never agreed to pay the hefty fee for the directory. When a business disregards the invoice, the bad guys up the

ante by making collection calls and sending collection notices, piling on late fees and other penalties. The fraudsters sometimes even threaten to ruin the credit of the company or its owners and employees, to take them to court, or to refer the debt to a debt collector.

If companies stand firm in their refusal to pay for services they didn't authorize, the scammer may try to smooth things over by offering a phony discount. Or they may agree to cancel the listing going forward to stop any new bills. At this stage, many companies pay up just to stop the hounding. What they don't know is that they'll likely get more bogus invoices — either from the same scam artist or from others who have bought their contact information for a new scheme.

Sometimes the first contact with the fraudster is through an advertisement sent by mail, fax, or email that asks the company to "verify" or "confirm" its contact information for a free listing service or a free social networking page. Fine print on the advertisement, however, may say that by returning the mailer or responding to the fax, the company is agreeing to an expensive business directory listing.

The Supply Swindle

Every company needs office supplies, but small businesses and non-profits may not have a formal procurement process in place. So when supplies show up at the door, employees pay for them, assuming a colleague must have OKed the buy. The box contains unordered merchandise or maybe it's empty. Or a con artists may call, falsely claiming to verify an existing order. The next step: tricking an unsuspecting employee into saying yes. That triggers high-pressure threats if the business refuse to pay. Either way, the company is left holding the bag — and the bill.

The URL Hustle

"Your web address is about to expire if you don't pay immediately to renew your registration." That's enough to send an online marketer into warp speed. Since the invoice emphasizes that time is of the essence, some businesses pay first and ask questions later. Of course, the invoice isn't from the entities that really handle things like that. It's from a fraudster, banking on the fact that companies with a web presence will be too busy to investigate. In a variation on that scam, fraudsters send letters warning businesses that they'll lose their trademarks if they don't pay a fee immediately or that they owe money for additional registration services. The brazen ones falsely claim an affiliation with the U.S. Patent and Trademark Office or some other agency. The USPTO has advice for businesses at **uspto.gov** on how to tell if a letter about trademarks is the real deal — or a possible rip-off.

The Charity Con

Many businesses make it a point to support worthy causes in the community. So when a group claiming to help fire fighters, veterans, police, or kids asks a company to buy space in a calendar or publication, they're happy to chip in. Scammers take that money and disappear. Of course, crooks cover their tracks by picking names confusingly similar to reputable charities, so it's hard for businesses to find out they've been had. *Donating to Public Safety Fundraisers* at **business.ftc.gov** offers tips on making sure your donated dollars wind up with reputable groups.

The Check Cheat

Not all solicitations you get in the mail look like bills, invoices, or account statements. Your business may get something that looks like a refund or rebate check. Read the fine print on the front and back carefully. By cashing the check, you may be agreeing to be billed monthly for something you don't want or need, like Internet access or a listing in an online directory.

How can I protect my business?

Take the following steps to protect your company from this kind of fraud:

Train your staff.

Educate your employees about how these scams work. In addition to your regular receptionist, talk to everyone who may pick up the phone. Put a copy of this article in employee mailboxes. Mention it in a staff meeting. Post it on the break room bulletin board or where employees clock in and out.

Inspect your invoices.

Depending on the size and nature of your business, consider implementing a purchase order system to make sure you're paying only legitimate expenses. At a minimum, designate a small group of employees with authority to approve purchases and pay the bills. Train your employees to send all inquiries to this group. Compile a list of the companies you typically use for directory services, supplies, and other recurring expenses. Encourage the people who pay the bills to develop a "show me" attitude when it comes to unexpected invoices from companies they're not familiar with, even if those invoices list one of your employee's names. Don't pay for products or services you're not sure you ordered.

Verify to clarify.

If you get a message that looks to be from a bank, credit card company, or government agency, investigate before responding. Using a phone number you know to be legit, contact the office directly to ask if the inquiry is on the up and up. Furthermore, many business directory scam artists are headquartered in Canada or in other foreign countries, but use post office boxes or mail drops to make it look like they are in the United States. Before paying, check them out for free at **bbb.org**, and read the BBB's report on them.

File a complaint.

If a scammer is sending you bogus bills, speak up.

- File a complaint with the FTC at **ftc.gov/complaint** and with the BBB at **bbb.org**. Complaints help shape the FTC's law enforcement agenda, so it's important to sound off when you spot a scam. Concerned about business directory fraudsters' threats to tarnish your credit if you don't pay? Many will simply drop the matter — and may even provide a refund — if they know you've complained.

- If you think you've been victimized in a fraud scheme that involves the U.S. Mail, submit a Mail Fraud Complaint Form to the U.S. Postal Inspection Service at **postalinspectors.uspis.gov**.

- Alert your state Attorney General. You can find contact information at **www.naag.org**, or check the blue pages of the phone book under State Government.

Your Opportunity to Comment

The National Small Business Ombudsman and 10 Regional Fairness Boards collect comments from small businesses about federal compliance and enforcement activities. Each year, the Ombudsman evaluates the conduct of these activities and rates each agency's responsiveness to small businesses. Small businesses can comment to the Ombudsman without fear of reprisal. To comment, call toll-free 1-888-REGFAIR (1-888-734-3247) or go to **sba.gov/ombudsman**.

About the FTC

The FTC works for the consumer to prevent fraudulent, deceptive, and unfair practices in the marketplace and to provide information to businesses to help them comply with the law. To file a complaint or to get free information on consumer issues, visit **ftc.gov** or call toll-free, 1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4261. Watch a video, *How to File a Complaint*, at **ftc.gov/video t**o learn more. The FTC enters consumer complaints into the Consumer Sentinel Network, a secure online database and investigative tool used by hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.

Federal Trade Commission
BCP Business Center
business.ftc.gov
June 2014