Protecting Your Business

Your best defense is an informed workforce.

Talk to your staff about how scams happen and share this important information from the Federal Trade Commission (FTC).

Train Your Employees

- Encourage people to talk with their coworkers if they spot a scam. Scammers often target multiple people in an organization, so an alert from one employee about a scam can help prevent others from being deceived.
- Train employees not to send passwords or sensitive information by email, even if the email seems to come from a manager. Then stick with the program — don't ever ask for sensitive data from employees by email.

Verify Invoices and Payments

- Check all invoices closely. Never pay unless you know the bill is for items that were actually ordered and delivered. Tell your staff to do the same.
- Make sure procedures are clear for approving invoices or expenditures. To reduce the risk of a costly mistake, limit the number of people who are authorized to place orders and pay invoices. Review your procedures to 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. If you are asked to pay with a wire transfer, reloadable card, or gift card, you can bet it's a scam.

Be Tech-Savvy

- Don't believe your caller ID. Imposters often fake caller ID information so you'll be more likely to believe them when they claim to be a government agency or a vendor you trust.
- Remember that email addresses and websites that look legitimate are easy for scammers to fake. Stop and think about whether it could be a scam before you click. Scammers even can hack into the social media accounts of people you trust and send you messages that appear to be from them. Don't open attachments or download files from unexpected emails; they may have viruses that can harm your computer.
- Secure your organization's files, passwords, and financial information. For more information about protecting your small business or non-profit organization's computer system, check out the FTC's Small Business Computer Security Basics.

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.
- When it comes to products and services for your business, ask for recommendations from other business owners in your community. Positive word-of-mouth from trustworthy people is more reliable than any sales pitch.
- Don't pay for "free" information. You may be able to get truly free business development advice and counseling through programs like SCORE.org.

Scammers' Tactics

- **Pretending to be someone you trust.** They make themselves seem believable by pretending to be connected with a company you know or a government agency.
- **Creating a sense of urgency.** They rush you into making a quick decision before you look into it.
- **Intimidation and fear.** They tell you that something terrible is about to happen to get you to send a payment before you have a chance to check out their claims.
- **Using untraceable payment methods.** They often want payment through wire transfers, reloadable cards, or gift cards that are nearly impossible to reverse or track.

Common Scams Targeting Small Businesses

Watch out for these common scams:

Fake Invoices
Scammers create phony invoices to look like they're for products or services your business uses, such as office supplies or domain name registrations. Scammers hope the person who pays your bills will assume the invoices are for things the company actually ordered. Scammers know that when the invoice is for something critical, like keeping your website up and running, you may pay first and ask questions later. Except it's all fake, and if you pay, your money may be gone.

Unordered Office Supplies and Other Products
Someone calls to confirm an existing order of office supplies or other merchandise, verify an address, or offer a free sample. If you say yes, then unordered merchandise arrives at your doorstep, followed by high-pressure demands to pay for it. If you don't pay, the scammer may even play back a tape of the earlier call as "proof" that the order was placed. Keep in mind that if you receive merchandise you didn't order, you have a legal right to keep it for free.

Directory Listing and Advertising Scams
Scammers try to fool you into paying for non-existent advertising or directory listing. They often pretend to be from the Yellow Pages and may ask you to provide contact information for a "free" listing or to confirm your information for an existing order. Later, you'll get a big bill, and the scammers may use details or even a recording of the earlier call to pressure you to pay.

Utility Company Imposter Scams
Scammers pretend to call from a gas, electric, or water company saying your service is about to be interrupted. They want to scare you into believing a late bill must be paid immediately, often with a wire transfer or a reloadable card or gift card. Their timing is often carefully planned to create the greatest urgency.

Government Agency Imposter Scams
Scammers impersonate government agents, threatening to suspend business licenses, impose fines, or even take legal action if you don't pay taxes, renew government licenses or registrations, or other fees. Some businesses have been scared into buying workplace compliance posters that are available for free from the U.S. Department of Labor. Others have been tricked into paying to receive non-existent business grants from fake government programs. Businesses have received letters, often claiming to be from the U.S. Patent and Trademark Office, warning that they'll lose their trademarks if they don't pay a fee immediately, or saying that they owe money for additional registration services.

Tech Support Scams
Tech support scams start with a call or an alarming pop-up message pretending to be from a well-known company, telling you there is a problem with your computer security. Their goal is to get your money, access to your computer, or both. They may ask you to pay them to fix a problem you don't really have, or enroll your business in a non-existent or useless computer maintenance program. They may even access sensitive data like passwords, customer records, or credit card information.

Social Engineering, Phishing, and Ransomware
Cyber scammers can trick employees into giving up confidential or sensitive information, such as 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, such as a supervisor or other senior employee, but creates urgency or fear. Scammers tell employees to wire money or provide access to sensitive company information. 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 Promotion and Coaching Scams
Some scammers sell bogus business coaching and internet promotion services. Using fake testimonials, videos, seminar presentations, and telemarketing calls, the scammers falsely promise amazing results and exclusive market research for people who pay their fees. 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, 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
Scammers know that small businesses are looking for ways to reduce costs. Some deceptively 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 documents that still have key terms left blank. Don't do it. Others have been known to change terms after the fact. If a sales person refuses to give you copies of all documents right then and there, or tries to put you off with a promise to send them later, that could be a sign that you're dealing with a scammer.

Fake Check Scams
Fake check scams happen when a scammer overpays with a check and asks you to wire the extra money to a third party. Scammers always have a good story to explain the overpayment (they are stuck out of the country, need you to cover taxes or fees, need to buy supplies, or something else). By the time the bank discovers you've deposited a bad check, the scammer already has the money you sent them, and you're stuck repaying the bank. This can happen even after the funds are made available in your account and the bank has told you the check has "cleared."

For more tips on protecting your organization from scams, visit FTC.gov/SmallBusiness.