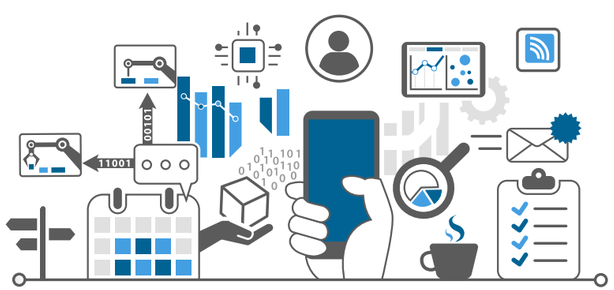
and Small Manufacturers

When scammers target your business, it can hurt your reputation and your bottom line.

Learn the signs of scams that target small manufacturers.



Scammers Strategies:

PRETENDING

They make themselves seem believable by pretending to relate to a partner, supplier, or utility you know and with which you may do business.

SENSE OF URGENCY

They rush you into making a quick decision before you have all of the details or realize the offer isn't real.

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.

UNTRACEABLE PAYMENT

They often want payment through wire transfers, reloadable cards, cryptocurrency, or gift cards that are nearly impossible to reverse or track.

Common Scenarios

FAKE INVOICES

Scammers create phony invoices that look like they're for products or services your business uses — like office supplies or materials. Scammers hope the person who pays your bills will assume the invoices are for things your company ordered and create that sense of urgency. They want you to pay first and ask questions later.

UNORDERED PRODUCTS

Someone calls to confirm an existing order of equipment or materials, to verify an address, or offer a free catalog or sample. When you give the information, unordered merchandise arrives at your doorstep, followed by high-pressure demands to pay for it.

DIRECTORY LISTING & ADVERTISING SCAMS

Scammers pretend to be from the Yellow Pages or other directory listings. They may ask you to provide 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 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, cryptocurrency, or a reloadable/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 manufacturers 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 nonexistent 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 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 nonexistent or useless computer maintenance program. They may even access sensitive data like passwords, credit card, and proprietary information.

BUSINESS PROMOTION & 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.

SOCIAL ENGINEERING, PHISHING, & RANSOMWARE

Cyber scammers can trick employees into giving up confidential or sensitive 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.

CHANGING ONLINE REVIEWS

Some scammers claim they can replace negative reviews of your product(s), or boost your scores on ratings sites. However, posting fake reviews is illegal.

CREDIT CARD PROCESSING & EQUIPMENT LEASING SCAMS

Scammers know that manufacturers 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 signature on a contract. Some unscrupulous sales agents ask manufacturers to sign documents that still have key terms left blank. Others have been known to change terms after the fact.

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 delightful story to explain the overpayment — they're stuck out of the country, they need you to cover taxes or fees, you'll 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 get to repay the bank.

Ways to Protect Your Business

TRAIN YOUR EMPLOYEES

- Explain to your staff the tactics used by scammers and share this brochure with them.
- Encourage people to talk with their coworkers if they spot a scam. Scammers often target multiple people in a company, 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.

DON'T LET TECHNOLOGY FOOL YOU

- Don't believe your caller ID. Scammers often fake caller ID information so you'll be more likely to believe them when they claim to be a vendor you trust.
- Remember that email addresses and websites that look legitimate are easy for scammers to fake. Check the link carefully. Don't open attachments or download files from unexpected emails.
- Secure your organization's files, passwords, and financial information. For more information about protecting your computer systems, check out the MEP National Network's Cybersecurity Resources for Manufacturers by visiting https://www.nist.gov/mep/cybersecurity-resources-manufacturers.

VERIFY INVOICES & PAYMENTS

- Check all invoices closely. Never pay unless you know the bill is for items that were ordered and delivered.
- Make sure procedures are clear for approving invoices or expenditures. 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. If you are asked to pay with a wire transfer, cryptocurrency, reloadable card, or gift card, you can bet it's a scam.

KNOW WHO YOU ARE 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 trust-worthy sources. Positive word-of-mouth input is more reliable than any sales pitch.
- Don't pay for "free" information. Do your research or get help from the Manufacturing Extension Partnership (MEP) National Network, a public-private partnership with Centers in all 50 states and Puerto Rico dedicated to serving small and medium-sized manufacturers.

REPORT

You can help stop a scam from happening to you or other manufacturers. If you spot a scam:

- Report it to the Federal Trade Commission https://www.ftccomplaintassistant.gov/
- Alert your state Attorney General http://www.naag.org/
- Alert local law enforcement, many have Cybercrime units that can investigate

MEP National Network™

Contact your local MEP National Network™ Center for assistance or to learn more.

(800) MEP-4MFG

mfg@nist.gov

https://www.nist.gov/mep/mep-national-network

NIST National Institute of Standards and Technology U.S. Department of Commerce