Fraud Tactics & Trends Most: Common Business Scams

By JoAnn Lombardi, President VR Business Brokers/Mergers & Acquisitions

The recent ransomware attacks have prompted many businesses to re-evaluate how they protect their cyber assets.

Some 71% of cyberattacks occur at businesses with under 100 employees. Cybercriminals know that small businesses tend to be easy targets, and that accessing a small business's computer networks often gives them entrée to client and vendor networks, too.

JoAnn Lombardi, President
VR Business Brokers/Mergers
& Acquisitions

Did you know that more than 90% of ransomware and targeted business attacks start with a spoofed email (aka phishing)?

Scam artists have become more adept at exploiting the weaknesses of small businesses. While some of these business scams are golden oldies, they're still putting money into the scammer's pocket – effectively taking it out of the pockets of many small business owners. The best defense against these is awareness and vigilance.

Here are five of the most common small business scams and how to avoid them:

1. Advance Fee Loan Scams

Whether it's offered in an ad on the internet or by e-mail, this scam offers money at reasonable rates – if you send them money. They may say they need the money for insurance purposes or to get the money across the border. Whatever the reason, you'll never see that money again – or the money they were supposedly going to loan your business.

How to Avoid This Scam: Be aware that it is illegal in both Canada and the U.S. to ask for money upfront for a loan. If you're asked to pay anything before you've received an agreed-on loan, walk away.

Related Scam: Bogus Equipment Leasing Deals – Your business receives a letter saying that you're pre-approved for leasing. All you have to do is send in your first (or your first and last months') payment. The scam is that you never receive the equipment that you were expecting to lease.

2. Fraudulent Billing Scams

Your business receives an invoice for goods or services that you didn't buy. The hope of the scammers that are sending these out is that your business will just pay up – easy money for them, easy loss for you.

How to Avoid This Scam: Examine your invoice carefully. Educate your staff about phony invoices. Set up your payables system so that at least two people must authorize any payments.

Related Scam: The Surprise Check – Your business receives a check for a small amount. The catch is that the check is actually a "promotional incentive." If you cash it, the company will claim that you've agreed to whatever terms are printed on the back of the check, and start the billing process immediately.

3. Business Identity Theft

Identity theft itself is the fastest-growing fraud in North America, according to the Better Business Bureau. Just as someone can steal your personal identity, your business's identity can be stolen. Once it's stolen, scammers can use your business name and financial information to open a bank account and run up expenses.

How to Avoid This Scam: Take steps to protect your business data. Shred all your discarded paper, including anything that has your business name on it. Be careful when responding to e-mail asking you to do such things as verify your account. Be wary about information you give out over the phone.

Related Scam: Phishing or internet "come-ons" are another that trick consumers and small businesses into providing bank or other financial information.

4. Work-at-Home Scam

Preying on people who want to have home-based businesses, these scams offer the opportunity to "make big bucks" working at home. Sometimes the ads say all you have to do is own a computer. Other times, the work-at-home scam involves stuffing envelopes or assembly work. The scam is simple; you buy the information or the materials you supposedly need. Rather than being the key to make money, what you receive is useless.

How to Avoid This Scam: Don't bite. These are not profitable opportunities; the only ones who make money from them are the scammers if it seems too good to be true, it is. You never have to send money to get information about legitimate business opportunities.

5. Credit Card Scams

Fraudulent use of credit cards is also on the rise. In the standard credit card scam, someone will call and place an order, offering to pay with fraudulently obtained credit card information. The business processes the ordering, but later is informed that the credit card was stolen and the amount of the transaction will be charged back to the business's account.

How to Avoid This Scam: Always use due diligence to ensure that orders are legitimate. Be particularly leery of overseas callers, new callers placing large orders and/or callers requesting rush shipping. If you are suspicious, ask the customer for the name of the credit card's issuing bank and its toll-free customer service number, which is printed on the back of all credit cards. Tell the customer you will check with the bank and call him or her back.

JoAnn Lombardi, President
VR Business Brokers/Mergers & Acquisitions