



So Many Scams, So Little Time

Jennifer Sands, VP – BSA & Security Officer,
Bank of Labor

You've heard the adage that if it sounds too good to be true, it probably is. That's doubly true when it comes to money scams.

Take for example, the **Lottery Scam**. It's a classic swindle where the victim receives a communication (email, phone, text) delivering the good news! There's one small caveat - in order to get your winnings, you have to pay a fee. Once you've paid your fee, you never hear from them again. Your dream to quit your job to live off your riches has ended. Plus, now you're out the fee.

The best way to avoid this type of scam is to be aware of the red flags:

- (1) You should not have to pay a fee to collect legitimate lottery winnings,
- (2) You don't recall buying lottery tickets anyway,
- (3) NEVER send money to someone you don't know.

If you receive a communication like this, do not click on any links in the email, do not communicate back, and immediately delete the communication.

Businesses need to be on the lookout for scams, as well. One that has grown in popularity is the **Fake Invoice Scam**.

Running your business keeps you busy! Scammers hope that you don't pay attention to the small details like invoices. Scammers send fake invoices that look like they're for products or services that your business uses. The person handling the accounting of your business may assume the invoice is real and pay it. Problem is that it's not. It's a bill for items that your business doesn't use or supplies that were never ordered. Once the payment has been made, the money may be gone.

To help you and your business avoid this racket, don't pay first and ask questions later. Know your vendors, review invoices, and only pay for services or supplies your business uses.

Business aside, more of us are using the Internet to look for love. Unfortunately, those who search online for companionship sometimes fall prey to a **Romance Scam**.

Continued on page 2 >

A person can pretend to be anyone they want when they are online. Most often, they say they are away working on an oil rig/are at sea, in the military, or are in construction. The relationship moves quickly. Their online profile seems too good to be true. Often, that's exactly what it is.

Some of the best ways to spot and/or avoid this type of scam is:

- (1) Be wary of someone professing their love for you early on in the relationship,
- (2) Steer clear of requests to send money, gift cards, cryptocurrency or anything of value to help the person get out of the turmoil they claim to be in (examples include the need to get a new passport, pay someone off at the borders to be able to cross, or an ill family member),
- (3) They repeatedly break their promises to visit



You should also watch out for **Employment Scams**.

In a job search, everyone wants great pay and benefits with some flexibility. The scammers know this and have been known to reach out via LinkedIn or Career Builder or pose as a recruiter through an email indicating they are interested in hiring you.

One common fake employment ruse is to offer

applicants the opportunity to be an assistant or a 'secret shopper'. Be extremely suspicious of anyone who asks you to detail your customer experience or who sends you a check to cash at your bank and instructs you to then send money to other places. If you transact that check and the check is not good, you'll be on the hook for any losses. Do **NOT** provide them with a copy of your ID, social security number, or bank account information.

You can avoid these types of scams by:

- (1) Asking for details and references and check them out,
- (2) Check the sender's email address (Jane Doe who works at Bank of Labor is not going to ask you to send your resume to her email address at janedoe@hotmail.com),
- (3) Call the employer using the phone number found in a legitimate search engine.

Overpayment scams are another big one. As you're doing some house cleaning and purging items you no longer want or need, you want to sell the item. You find a buyer who's willing to pay you more for the item than the price you listed. They send you a check or money order (through US Postal Service, FedEx, or UPS) for more money than the item was listed and ask you to send the overpayment back, quickly through MoneyGram, PayPal or another expedited delivery method. Don't do it! The check they've sent is usually no good. Once you've sent the money (again, don't send money to someone you don't know), you won't get it back.

To avoid this rip-off:

- (1) Don't send money to someone you don't know,
- (2) Don't send money to a shipping company or a private shipping agent as that's part of the scam,
- (3) Don't provide your bank account information.

If you're ever in doubt, call us at 913.321.4242 or stop by to talk with one of our bankers if you have any questions or concerns. They can give you tip-offs to avoid rip-offs!