Joel Poole, Business Development Manager, Central National Bank

Are You Safe From Fraud?

Adapted from a blog article written by Amanda Rolfs for blog.centralnational.com

Joel Poole, has been a Business Development Manager for Central National Bank since 2014. He has a degree in Economics from Kansas State University, and an emphasis in leadership studies within the Flint Hills Region.

Do you feel confident that the safety measures you have in place are adequate to protect your business from cybercrime? Where do you have room for improvement? If you feel like now is a good time to look into it, here's five common scam methods, and four areas that YOU can investigate internally.

Five Common Scam Methods

1. Fake Invoices

Fake invoices are one way that scammers will try to get you to send money. In this instance, the scammer is hoping that whoever handles your accounts payable does not question the invoice. The goal is to encourage prompt payment so you avoid critically thinking about the bill. They might even make threats to instill fear, such as shutting down your website or utilities.

2. Browser Pop Ups

Another way scammers try to get information from you is by taking advantage of technology. The tech support scam is one example. When this occurs, you may get a pop-up saying your "computer's security is at risk." The pop up will instruct you to call a specific number to get help maintaining security. Scammers will try to gain access to your computer when you call, thus putting all files, customer records, passwords and other confidential information, at risk. Scammers may also attempt to do this through social engineering and phishing attempts.

3. The Fake Check Scam

Have you ever received a check for a product or service that's in an amount much larger than what your customer owes? In a fake check scam the scammer will request you send back the remaining amount. The catch here is that the original check will not clear, which leaves you with less money than you started. If you ever receive a check and are instructed to return excess funds, it is best to ask for a new check to be sent for the correct amount.

4. The Fake Contract Scam

Watch out for scams where someone is trying to get you to sign a contract, but there are details to be determined later. Sometimes the scammer won't give you a copy of the contract up front. These are common signs that you're working on an illegitimate deal.

5. Poor Reviews Removal

One of the methods that may be easier to catch includes a scammer calling and claiming they can remove poor online reviews or boost your online reviews. The Federal Trade Commission has declared this to be illegal, stating that reviews should always be honest opinions. If you get a sales pitch regarding online reviews it's best to steer clear.

Four Areas for You to Check

1. Debit Card & Credit Card Fraud

The most common area for fraud to occur is right at the register with your payments system. Take a look at the software and equipment you're using. How old is it? Who has provided it to you? Are you certain it has the latest technology? If it's bank-provided, ask your banker what additional steps you can take to keep your customer information safe. It's also a good time to take inventory of the types of

If the hustle and bustle of running a business wasn't enough, fraudsters are trying to take it away just as quick as you can earn it.

ACH data that is part of your business. How is that data, or information, collected, stored, transmitted and destroyed? Finally, is all of your customer data stored online or on a computer? Make sure you're properly storing and destroying paper documents as well.

In addition to keeping your customer card information safe, it's important to make sure you're keeping your own account information safe. Don't buy supplies from sources you don't trust. It's also a good idea to keep your personal banking information separate from your business accounts. That way, if you do have a security breach, the crooks can't get everything you have all at once.

2. Computers & Passwords

How old is your computer? Does it have virus detection software? Do you click "Update" when it tells you you're due for an update? Do you back it up regularly to an external source? A few dollars paid out to a local software/computer expert could save you thousands, and a massive headache. All you have to do is make sure your systems are up-to-date. And if you don't feel confident enough to ensure that, hire an expert. Just make sure that you are comfortable with the hire as to avoid the Browser Pop-up Scam.

It's also a good idea to make your passwords hard to crack. It seems like common knowledge these days to coach people on using a secure password with a variety of letters, numbers and symbols, but that doesn't seem to stop people from setting their passwords to "teddybear79".

3. Your Employees

Your employees are the first step to fighting cybercrime and also your weakest links. Do your best to make sure your systems and software are secure, but also take the time to educate your employees about common scams and the importance of protecting customer information. Your business reputation depends on it!

At the end of the day, if your people can't follow basic security protocols it's probably time to make sure they have very little less access to the secure aspects of your business.

4. Positive Pay

Many Financial Institutions offer Positive Pay services for you to ensure that the checks clearing your account are in-fact the ones that you have written. By uploading a file to the bank with your outstanding/issued checks, the bank can return any items that attempt to clear without your prior permission. Cut the fraudsters legs out from underneath them with the protection of Positive Pay.

While the evolution of fraud seems to be daunting, diligence and forward-thinking are your biggest tools of prevention. If the hustle and bustle of running a business wasn't enough, fraudsters are trying to take it away just as quick as you can earn it. Financial Institutions are highly educated in these areas, and are there for you when you need the support. **MEMBER FDIC**