



Treasury Management Newsletter

**CIBM
BANK**
4TH Quarter 2018

CIBM Bank is providing this newsletter to inform our clients of important banking regulations and fraud prevention tips.

Avoiding Tech Support Scams Source: Carol Kando-Pineda, Federal Trade Commission, 2018

You're working on your computer when, suddenly, a message pops up on the screen: "Virus detected! Call now for a free security scan and to repair your device." That's a tech support scam. Don't call, text, or email. Legit tech support companies don't operate that way.

Scammers pose as big-name companies and use pop-up messages, fake websites, and phone calls to trick you into thinking your computer has an urgent problem. Their plan is to get your money by selling you worthless software, enrolling you in fake programs, or getting you to pay for useless tech support. The scammers urge you to call a toll-free number immediately, threatening that you may lose personal data if you don't.

When you call, the scammer might ask you to give them remote access, pretend to run a diagnostic test, or tell you they've found a virus or other security issue. They try to sell you a security subscription or other "services" that range from worthless (for instance, they're available for free elsewhere) to malicious (they install dangerous software that can help them steal your personal information.)

What should you do? If you get a pop-up to call a number to fix a virus on your computer, ignore it. Your computer is almost certainly fine. But if you're concerned about your computer, call your security software company directly — and don't use the phone number in the pop-up or on caller ID. Use a number you know is real, like the one on a software package or your receipt. Tech support scammers like to place online ads pretending to be legitimate companies, so be sure you have the correct telephone number for the real tech company before calling.

And if someone asks you to pay for anything — including tech support services — with a gift card, cash reload card, or a wire transfer, that's a scam. No legitimate company will tell you to pay that way. If you see that, report it at FTC.gov/complaint.

Spear Phishing Scammers Want More From You Source: Lisa Lake, Federal Trade Commission, 2018

"I'm calling from [pick any bank]. Someone's been using your debit card ending in 2345 at [pick any retailer]. I'll need to verify your Social Security number — which ends in 8190, right? — and full debit card information so we can stop this unauthorized activity..."

So the caller ID shows the name of your bank. And the caller knows some of your personal details. Does that mean it's legit? No. It's a scam — and scammers are counting on the call being so unsettling that you might not stop to check your bank statement.

We've started hearing about phone scams like this, which combine two scammer tricks: spear phishing and caller ID spoofing. In a phishing attempt, scammers may make it look like they're from a legitimate company. And when they call or email with specific details about you — asking you to verify the information in full (things like your Social Security number or address) — that's called spear phishing.

The other nasty wrinkle in this scam is caller ID spoofing. That's when scammers fake their caller ID to trick you into thinking the call is from someone you trust.

Here's how you can avoid these scam tactics:

- Don't assume your caller ID is proof of whom you're dealing with. Scammers can make it look like they're calling from a company or number you trust.
- If you get a phone call, email, or text from someone asking for your personal information, don't respond. Instead, check it out using contact info you know is correct.
- Don't trust someone just because they have personal information about you. Scammers have ways of getting that information.

CIBM BANK

Branches of CIBM Bank:

CENTRAL
ILLINOIS BANK

MARINE BANK
Milwaukee | Indianapolis

AVENUE BANK

Solutions to count on.

2913 W. Kirby Avenue
Champaign, Illinois 61821
cibmbank.com

 EQUAL HOUSING LENDER. MEMBER FDIC.



Treasury Management Newsletter

CIBM BANK

4TH Quarter 2018

Speare Phishing Scammers Want More From You (continued)

If you gave a scammer your information, go to IdentityTheft.gov. You'll learn what to do if the scammer made charges on your accounts.

Even if you didn't give personal information to the scammer, report the scam to the FTC. Your reports help us understand what's happening and can lead to investigations and legal action to shut scammers down.

Product Spotlight: Fast Track Loans, Small Business Loans, and Commercial Lending Source: CIBM Bank, 2018

Based on your business needs we will develop a relationship package that is right for you. Whether you are just getting started or looking to finance a project, our lending solutions can help you along the way. We understand that the growth and success of your business is vital to you. Let us provide you with the expertise you need to help meet your business goals.

Fast Track Loans: CIBM Bank makes getting the money you need for your business quick and easy. Our Fast Program offers term loans and lines of credit ranging from \$15,000 to \$100,000 with quick approvals, no application fees, and attractive rates.

Small Business Loans: When your business needs funds to grow CIBM Bank may be the answer. Our Small Business Lenders focus on helping you obtain the extra cash flow you need to get started or complete the next project.

Commercial Loans: CIBM Bank assists middle market business obtain the capital they need to keep their business moving forward. Companies can count on us to provide flexible and creative financing solutions in a timely manner.

For more information, contact your Treasury Management Officer or local branch.

CIBM Bank Holiday Closing and Processing Schedules

Monday, December 24, 2018 - Christmas Eve:
All branches of CIBM Bank will close at 12 p.m. CT
Wire, ACH, and RDC processing deadline at 11 a.m. CT

Tuesday, December 25, 2018 - Christmas Day:
All branches of CIBM Bank and the Federal Reserve Bank will be closed.

Monday, December 31, 2018 - New Year's Eve:
All branches of CIBM Bank will close at 3 p.m. CT
Wire, ACH, and RDC processing deadline at 2 p.m. CT

Tuesday, January 1, 2019 - New Year's Day:
All branches of CIBM Bank and the Federal Reserve Bank will be closed.

**As we look ahead,
we are excited to share an upcoming milestone.
We will unify our brands across all of our CIBM markets to our legal name, CIBM Bank in 2019.
We are the same company with the same great people – just a new look!
All of us at CIBM Bank wish you and yours a joyous holiday season,
and success in the new year.**

CIBM Bank takes your security seriously: CIBM Bank is committed to protecting your personal and account information. We have account monitoring systems and other controls in place to recognize and help prevent fraud. We will never attempt to gain your personal or account information via email, text message or automated phone calls. Attempts such as these should be considered fraud. If you are contacted in this manner or believe you are the victim of bank fraud, contact us immediately.