THE INFORMER

Quarterly Newsletter for INSOUTH's Business Customers

1st Quarter

INSOUTH® BANK Member FDIC

www.insouth.com

Member FDIC | EQUAL HOUSING LENDER

Bank Holiday Schedule

Presidents' Day
Closed
Monday, February 16th

Good Friday
Closed
Friday, April 3rd

Memorial Day
Closed
Monday, May 25th

Juneteenth
Closed
Friday, June 19th

IMPORTANT TIPS TO HELP PREVENT FRAUD:

- **Check your account daily and watch payees on physical checks.**
- **Watch emails requesting changes to invoice remittance.**

READY TO REBOOT YOUR BUSINESS STRATEGY?

A lot can change in a year. Let's reconnect to explore new ways INSOUTH can support your evolving goals—from smart savings tools to business credit options.

Need help with cash flow, banking, or credit options? Give us a call or visit us today!

UNLOCK YOUR BUSINESS'S POTENTIAL

we're here to help!

FUEL YOUR GROWTH

with us today

Get the funding you need to grow with our **business loan options.***

Why choose us:

- Flexibility
- Competitive Interest Rates[1]
- Regional Expertise
- Local Decision-Making
- Personalized Support

Our Loan Team would be happy to assist you!

NMLS 400032. *All loans are subject to credit and/or collateral approval. 1)Interest rates are subject to credit approval and may vary based on loan amount, term, and borrower qualifications. Terms and conditions apply.

Intended for use by real-estate and lending professionals only and should not be considered as promoting an offer of credit to consumers.

Need assistance? Call us!

Millington: (901) 872-4545
Atoka: (901) 837-9675
Covington: (901) 476-3330
Brownsville: (731) 772-1201
Memphis: (901) 747-5555
Jackson: (731) 574-2500
Electronic Banking: (866) 348-3614
Debit Card Support: (800) 541-3891
Fraud Prevention Services: (877) 253-8964

INSOUTH Bank is your business partner. If you would like for us to meet with you or your employees to discuss how to protect your money and your information, please do not hesitate to contact us!

Common Scams Targeting Small Businesses

Scams can impact every business, regardless of location, size, or industry. But they are especially a problem for small businesses. Knowledge is the best protection to protect your business from scams and fraud. Staying informed and keeping your employees informed about these common scams is imperative for the protection of your business.

Phishing scams. Phishing scams attempt to steal sensitive information about your business. These scams often appear to be legitimate emails or text messages. However, when you click on the link, you download a virus that captures personal information or loads a form that asks for bank account or credit card details. Be leery of unsolicited messages, and don't click on links. Instead, hover over the link with your cursor to see the real address. Also, be sure your computer has the proper firewall and computer protection software.

Business Email Compromise ("BEC"). Business email compromise fraud is an email phishing scam that typically targets people who pay bills in businesses, government, and nonprofit organizations. According to the Federal Bureau of Investigations, it has resulted in more losses than any other type of fraud in the U.S. In Canada, BEC scams are among the top reported scams recorded by the Canadian Anti-Fraud Centre (CAFC).
In BEC fraud, the scammer poses as a vendor or other trusted source who emails an accountant or chief financial officer. The email asks them to wire money, buy gift cards or send personal information, often for a plausible reason. If money is sent, it goes into an account controlled by the con artist.

Ransomware attacks. Cybercriminals encrypt a company's data and demand payment for its release, with small and medium-sized businesses increasingly targeted.

Phony invoices. Businesses receive fake invoices demanding payment for products or services never ordered or received. The most common scams involve office supplies, website or domain hosting services, and directory listings. If you look closely, you'll often see the fine print that identifies the bill as a solicitation. Generally, the amount is small enough not initially to raise a red flag.

Tech support scams. Fraudsters pose as IT professionals, claiming to fix non-existent computer issues to gain access to systems or extract payment.

Overpayment scams. In this scam, the person you are doing business with sends you a check for more than the amount they owe you. Then, they instruct you to wire the balance back to them. Or, they send a check and tell you to deposit it, keep part of the amount for your compensation, and then wire the rest back. The results are the same: the check eventually bounces, and you're stuck, responsible for the full amount, including what you wired to the scammer.

Information provided from: https://www.bbb.org/article/business/19932-bbb-warning-businesses-dont-fall-for-that-scam

Think You've Been Targeted by a Scam? Use This Quick Checklist

- **Stop communication immediately.** Do not reply to emails, texts, or phone calls from the suspected scammer.

- **Secure your logins.** Change passwords for email, accounting, payroll, and vendor systems. Turn on multi-factor authentication where available.

- **Check recent activity.** Review bank transactions, credit cards, ACH payments, wires, and vendor payments for anything unusual.

- **Alert your team.** Notify employees—especially those handling payments, payroll, or vendor requests—to watch for similar messages.

- **Preserve evidence.** Save emails, texts, phone numbers, screenshots, and any instructions you received. Do not delete them.

- **Report the incident.** Consider filing a report with:
  - Your IT provider or cybersecurity firm
  - Local law enforcement, if funds or data were compromised

- **Watch for follow-up attempts.** Scammers often try again. Be cautious of "recovery" offers claiming they can get your money back.

- **Review internal controls.** Confirm approval processes for wire transfers, ACH payments, payroll changes, and vendor updates.

Helpful Prevention Tips for Businesses

- Verify all payment or wiring changes by phone using a known contact, not the information in the email
- Be cautious of urgent or threatening language—pressure is a common scam tactic
- Limit who has authority to approve payments or change vendor information
- Provide regular scam awareness reminders to employees

If something feels off, trust your instincts. Taking action quickly can make a difference.