THE INFORMER

Quarterly Newsletter for
INSOUTH's Business Customers

3rd Quarter

INSOUTH BANK Member FDIC

www.insouth.com

Member FDIC

EQUAL HOUSING LENDER

Bank Holiday Schedule

Columbus Day
Closed
Monday, October 13th

Veterans Day
Closed
Tuesday, November 11th

**Thanksgiving Day &
Day After Thanksgiving**
Closed
Thursday, November 27th &
Friday, November 28th

Christmas Eve
Closed at 12pm
Wednesday, December 24th

Christmas Day
Closed
Thursday, December 25th

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!

Power your business forward with our streamlined INBusiness Checking Accounts!

- INBusiness Commercial Checking - For businesses with complex banking needs!
- INBusiness Interest Checking Plus - An account for those businesses that want to earn interest!
- INBusiness Basic Checking - Perfect for most businesses!

LEARN MORE

https://www.insouth.com/business/accounts/inbusiness-checking

Keeping your Business ON THE MONEY

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.

The INformer
3rd Quarter

QR Code (Quishing) Attacks are on the Rise

There has been an emerging threat involving malicious QR codes, also known as “quishing” attacks (QR phishing). These attacks are being used by cybercriminals to steal credentials, install malware, or trick users into revealing sensitive information. Quishing, or QR phishing, is a cybersecurity threat in which attackers use QR codes to redirect victims to malicious websites or prompt them to download harmful content. The goal of this attack is to steal sensitive information, such as passwords, financial data, or personally identifiable information (PII), and use that information for other purposes, such as identity theft, financial fraud, or ransomware.

This type of phishing often bypasses conventional defenses like secure email gateways. Notably, QR codes in emails are perceived by many secure email gateways as meaningless images, making the users vulnerable to specific forms of phishing attacks. QR codes can also be presented to intended victims in a number of other ways.

How the attack works:

Malicious QR codes are placed in public spaces, printed materials, emails, or fake notices. When scanned, they may redirect users to:

- A fake login page designed to steal credentials
- A malware-infected app or file
- A spoofed company page that appears legitimate

Examples of suspicious QR code behavior:

- QR codes with no clear source or context
- Messages urging urgent action, such as “Your account is at risk!” or “Update now!”
- Codes in emails claiming to be from IT, HR, or your bank

What you should do:

- Do not scan QR codes from unknown or unverified sources
- Verify any QR code communication with the sender before scanning
- Report any suspicious codes to your IT/Security team

How can end-users prevent quishing?

Make sure to verify the URL associated with the code, and refrain from submitting personal information, making payments, or downloading anything from a site assessed through a QR code. By adopting these practices, individuals can reduce the risk of falling victim to quishing attacks. Please make sure and take the time to look at your emails thoroughly, and notify your employees of these attacks so that they can also take caution.

Information provided from: https://www.cloudflare.com/learning/security/what-is-quishing/