

THE INSIGHT



Quarterly Newsletter for the Seasoned Adult

2nd Quarter 2026



Stay Safe From These Travel Scams

According to the Federal Trade Commission, here are some of the most common travel scams:

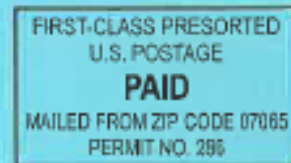
- Travel scam websites - Ads for “free” vacations or emails, calls, or text messages stating that you have won a vacation, even though you never entered to win one.
- Robocalls about vacation deals - You may get robocalls offering you vacation deals at a discounted price. These companies are trying to sell you something illegal unless the companies got written permission from you to call you that way.
- International travel document scams - Websites that claim to be able to get you an international travel visa, passport, or other documents. Some sites are legitimate businesses, while others are just copycats of official websites. These imposter sites charge you high fees, including fees for services that are free on the U.S. Department of State's website.

- International driving permit scams - Scammers create websites to sell fake IDPs, or try to sell them to you in person or some other way. If you buy a fake IDP, you'll be paying for a worthless document. But, even worse, you also could face legal problems or travel delays if you're detained for using it to drive in a foreign country.
- Vacation home scams - Scammers can hijack real rental listings and advertise them as their own, so when you show up for vacation, you find out that other people are also booked for the same property. Other scammers make up listings for places that aren't really for rent or don't exist. Searching online for the rental property's address, plus the name of the property owner or rental company listed, can help you avoid this scam.

How to Protect Yourself from Scams:

- Use Secure Payment Methods: Use credit cards for transactions, which offer better fraud protection than debit cards, wire transfers, or gift cards.
- Verify Listings: Research vacation rentals thoroughly, check reviews, and avoid deals that seem too good to be true.
- Don't Click Links: Do not click links in unexpected emails or texts regarding deliveries or services.
- Verify Official Sites: If you receive a notice about a utility or service, look up the official phone number yourself to verify, rather than using the contact info in the message.
- Beware of High Pressure: Scammers often push for immediate action.

**IMPORTANT NOTICE:
IMMEDIATE RESPONSE NEEDED**



**Mortgage ID:
545-161-512**

You have recently closed on your mortgage with **INSOUTH BANK**.
We are trying to reach you regarding a matter of importance concerning your mortgage with INSOUTH BANK.
This is time sensitive so please call us at **(800) 411-2119**.
Mortgage ID# 545-161-512.
Please respond by: **6/15/2026**

Please be aware of this recent mail scam. We have been made aware of customers receiving a false notice in the mail. If you receive a mail notice like this, please do not call the number on the false notice and contact us directly at your local branch or call us at 866-348-3614.

Please be aware of these warning signs: Urgency & Threats: Demands immediate action, such as threatening suspension of services. Suspicious Links/QR Codes. Personal Information Requests: Asks for sensitive data like Social Security numbers, bank account numbers, or passwords.

You're Never a Burden — We're Here to Help

If something doesn't feel right, please don't feel embarrassed or afraid to call us. Scams are becoming more common, and according to AARP.com, older adults reported losing nearly \$4.9 billion to scams and fraud in 2024, with more than 147,000 complaints submitted by people aged 60 and older. These situations can happen to anyone. At INSOUTH Bank, our goal is to protect your personal information and your hard-earned money to the very best of our ability. We are always happy to listen, answer questions, and help you decide what steps — if any — should be taken. No concern is too small. If you receive a call, text, email, or request that worries you, please don't hesitate to contact your local INSOUTH branch. We are here to support you and help keep you safe.

If you or a loved one suspects scam or fraud, please **contact us immediately**.

Millington - (901) 872-4545

Brownsville - (731) 772-1201

Atoka - (901) 837-9675

Memphis - (901) 747-5555

Covington - (901) 476-3330

Jackson - (731) 574-2500

Holiday Hours Notice

Just a friendly reminder that INSOUTH Bank will be closed in observance of the following holidays. You can still access your accounts anytime through online and mobile banking.*

Juneteenth: Friday, June 19th

Labor Day: Monday, September 7th

*Message and data charges may apply with your cellular provider. Registration required. Online and Mobile Banking may be subject to additional terms and conditions and/or third party service provider fees. Registration and approval required for mobile deposit.



TEXT MESSAGE ALERT

Fake text messages asking you to click a "secure portal" link are circulating.

We're warning you about text messages currently being sent to INSOUTH Bank customers. These texts claim a check payment needs to be reviewed and ask you to tap a link to a "secure portal" to view account alerts and updates.

The link in these texts does not lead to INSOUTH Bank. It leads to a fake site designed to steal your online banking login. Do not tap it.

HOW TO SPOT THE FAKE

- **A message about a check payment needing "review"** through a link, rather than through our app.
- **A web address that isn't ours.** Look closely — scam links often contain extra words like "secure" and end in unfamiliar domains, not our real website.
- **Instructions to copy and paste the link** into your phone's browser if it doesn't open. INSOUTH Bank will never tell you to do this — it's a major red flag.

What to do right now

1. **Don't tap the link.** Not even to "check what it is."
2. **Don't copy or paste it** into your mobile browser, even if the text says it's not working.
3. **Delete the text message.**
4. **Check your account the safe way** — open our official app or go directly to our website by typing the address yourself.

Example of this scam text message — do not tap any links:

INSOUTH Bank:

To review the check payment that was initiated, please access the secure portal provided. The portal will allow you to view real-time alerts and updates related to your banking account.

<https://websecureinsouthbank.secure-s529i.com/258>

Please note, if there's any trouble with going to secure portal please copy & paste portal on mobile browser.

If you've already tapped the link or entered any information, contact us right away so we can help protect your account.

Call us now: 866-348-3614

This is our trusted, official number — save it to your contacts.

Our Customer Service email is customer.service@insouth.com.