Citizens

Travel Fraud Tips

Travel opens the door to new experiences, whether for business or pleasure, but it can also create opportunities for scammers. When you're on the move, distracted or relying on unfamiliar technology, your personal and financial information can be easier to target. Knowing what to watch for and how to protect yourself can help you focus on enjoying your trip with more confidence.

Common travel scams:	How to protect yourself:
Payment red flags Pressure to pay via wire transfers, gift cards or peer-to-peer payments.	Scammers rely on urgency. **Hang up or ignore the email.**
Fake booking sites and travel "deals" Websites or emails for hotels, vacation rentals or excursions that don't exist or charge hidden fees.	Make sure you're **using official websites and apps** when booking travel or transportation.
ATM and card skimming Criminals install devices on ATMs or payment terminals to steal card data.	**Conduct a visual inspection** before inserting your card to check for loose, raised or misaligned card readers.
Public Wi-Fi hacking Change to: Free, unprotected Wi-Fi may not be secure, and fraudsters can capture logins and personal information.	**Use a personal mobile hotspot or a Virtual Private Network (VPN)** when possible.

If you think you've been targeted or compromised:

- Call our Fraud Customer Service Center at 800-974-2260.
- Report fraud in the Citizens mobile app.*
- Change passwords on affected accounts immediately.
- Lock or freeze payment cards with CiZi, your virtual assistant in the Citizens mobile app.*
- Monitor account activity closely for unauthorized charges or changes.
- Save documentation, emails and screenshots related to the incident

Protect yourself from travel fraud.
To learn more, speak to a banker or visit our Fraud and Security Center at **citizensbank.com/fraud-protection.**

*Wireless carrier, text, and/or data charges may apply.