Fraud Prevention & Preparedness

Protecting you from
Scams, Fraud & Cyber Threats

⚠ Fraud and scam attempts are rising. Customers Bank will **never** call, text, or email asking for your password, PIN, or one-time passcode.

Criminals use phone calls, texts, emails, and social media to steal your money and personal information. **Knowing how these scams work is your first line of defense.**

Common Scams to Watch For

Impersonation Scams

Someone poses as your bank, IRS, or a family member to create urgency and pressure you to act fast.

Phishing & Smishing

Fake emails or texts direct you to spoofed sites designed to steal your login credentials.

Romance Scams

Fraudsters build fake relationships online, then ask for money via gift cards or wire transfers.

Investment Fraud

Promises of guaranteed returns pressure you to send funds. Once sent, the money disappears.

Overpayment Scams

A buyer overpays, asks you to refund the difference, then the original check bounces.

Zelle™ & P2P Fraud

Scammers pose as bank staff and convince you to transfer funds "for safety." Rarely reversible.

Red Flags to Recognize

- Requests for immediate payment by wire, gift card, or crypto
- Urgent pressure to act before it's "too late"
- Familiar-looking caller ID — scammers can spoof these
- Requests to share a one-time code sent to your phone
- Unsolicited job offers asking you to transfer funds
- Requests to keep a transaction secret from your bank
- Links that don't match official website addresses

Never Share or Do This

× Your PIN, password, or one-time passcode — ever

× Your full Social Security number by phone or email

× Remote access to your device from an unsolicited caller

× Payment via gift cards — no real business asks for these

× Funds on behalf of someone you've only met online

How to Protect Yourself

✓ Set up account alerts in online banking

✓ Use strong passwords and multi-factor authentication

✓ Hang up and call the number on your card to verify

✓ Check your credit report at annualcreditreport.com

✓ Pause before you act — scammers rely on urgency

Think You've Been Targeted?

Customer Service: **1-866-476-2265** | Fraud Hotline: **1-844-552-6902** (Mon–Fri, 9am–5pm)

Report Cybercrime

FBI Internet Crime Complaint Center: **ic3.gov**

Security Center

Visit **customersbank.com/security** for fraud prevention resources.