

Protect Yourself From Scammers Pretending to Be Your Bank



Beware of Phishing and Fraud Attempts

Cybercriminals are increasing efforts to steal personal and financial information by pretending to be trusted organizations, including banks. These scams are commonly known as phishing.

Phishing attempts may come through:

- Phone calls
- Text messages
- Emails
- Social media messages

These messages often create urgency and pressure you to act quickly.



What Scammers May Ask For

Fraudsters may claim to be bank employees and request:

- Online banking usernames or passwords
- One-time passcodes or verification codes
- Debit or credit card numbers
- PINs
- Social Security numbers
- Account numbers
- Wire information

Our bank will never contact you unexpectedly and ask for this information.



Know the Warning Signs

Be cautious if someone:

- Urges immediate action ("Your account will be locked")
- Threatens negative consequences
- Asks you to verify personal or account information
- Requests payment or gift cards
- Calls from an unfamiliar or spoofed phone number

If something feels off, trust your instincts.



How to Protect Yourself

To stay safe:

- Never share sensitive information with unknown callers, texters, or email senders
- Do not click links or open attachments from unexpected messages
- Hang up if a call seems suspicious
- Contact us directly using the phone number on our website, statement, or debit card
- Monitor your accounts regularly for unfamiliar activity

If something feels off, trust your instincts.



What to Do If You Are Contacted

If you receive a suspicious call, text, or email:

- Do not respond or provide any information
- End the communication immediately
- Contact our bank using a trusted number to report the attempt

Early reporting helps protect you and other customers.



Learn More About Fraud Prevention

Scan the QR code to visit Liberty Bank's Security Center for tips, resources, and the latest fraud alerts.



We Are Committed to Your Security

Protecting your information is a top priority. While we have safeguards in place, your awareness is the strongest defense against fraud. If you ever have questions about a message claiming to be from us, contact us directly before taking action.