BANK OF OAK RIDGE
You matter here

PAYMENT FRAUD PREVENTION

Many payment scams start with a deceptive message via email, text, or a phone call designed to create urgency and gain your trust. Once scammers capture login credentials, verification codes, or convince you to "confirm" a transaction, they may push you toward fast payment channels, especially person-to-person apps like Zelle or Cash App, ACH transfers, or wire transfers, where funds can be difficult to recover.

HOW THEY CONTACT YOU

Phishing emails, smishing texts, fake account alerts, or Business Email Compromise (BEC) impersonating a government agency, loved one, internet/computer support, or financial institution.

WHAT SCAMMERS WANT

Passwords, multi-factor/verification codes, account access, updated "payment instructions," or a rushed payment approval.

HOW THEY TAKE YOUR MONEY

Victims are directed to send funds via P2P (person-to-person) like Zelle, Venmo, or Cash App, ACH (electronic transfer), or wire (typically fast and hard to reverse) to reroute a legitimate payment to a fraudulent account.

SCAMS TO WATCH FOR

Fake Bank & App Alerts

"**Your account will be suspended**" or "**Confirm this transaction/identity**" alerts lead to a look-alike login page that steals credentials.

Payment Change (Business Email Compromise)

Email is sent with updated ACH or wire instructions; payment is rerouted to the scammer.

Urgent Request

A message appears to be asking for an immediate wire, ACH or gift-card/P2P payment.

P2P Purchase Scams

Stolen card funded payments that later reverse, canceled/failed transfers, or overpayment/refund requests.

Requests for Verification Codes

A scammer asks you to "**confirm identity**" or "**reverse a charge**" using the code sent to your phone.

BEST PRACTICES TO REDUCE YOUR RISK

- **Verify Independently** by confirming using a trusted phone number, not the one given in the message.
- **Don't Use Links in Unexpected Messages,** instead go to our website or app directly and sign in from there. Don't use any link they provide that prompts you to login.
- **Protect Access** by enabling multi-factor authentication and never sharing passwords or verification codes. Remember that **Bank of Oak Ridge won't ever reach out to ask for your verification code.**
- **Be Cautious with P2P** and send money only to verified contacts and use money transfer apps for their intended purpose - sending money to people you personally know.
- **Set Up Account Alerts** to receive real-time notifications of account activity.

IF YOU SUSPECT FRAUD, STOP ANY CONVERSATION OR TRANSACTION AND CONTACT YOUR BANKER IMMEDIATELY. SAVE ANY DOCUMENTS OR CORRESPONDENCE.