Protect yourself from these Common Scams

Scams can happen to anyone, and it's okay to ask for help when something doesn't seem right. If you ever feel unsure about something, do not hesitate to ask. We are always here to help. It is better to double-check than to take a risk with your hard-earned money.

Phishing Scams

Scammers send emails, text messages, or social media messages that appear to be from legitimate companies asking for personal information like passwords, credit card numbers, or Social Security numbers. ***Example:*** An email claiming to be from your bank asking you to update your account details by clicking on a link.

Tech Support Scams

Scammers pose as tech support agents from well-known companies, claiming your computer is infected with a virus. They may ask you to provide remote access to your computer or pay for unnecessary software. ***Example:*** A pop-up message, email, or phone call saying your computer is infected and directing you to call a number for support.

Lottery and Sweepstakes Scams

Victims are told they have won a large sum of money or a prize but must pay a fee or provide personal information to claim it. ***Example:*** An unexpected notification saying you've won a lottery (that you didn't enter) and need to pay a processing fee to claim your prize.

Online Shopping Scams

Fake online stores or listings offer goods at unbelievably low prices. Victims pay but receive nothing or get counterfeit or inferior products. ***Example:*** A website selling high-end electronics at a fraction of the market price but never delivering the items.

Investment Scams (Ponzi Schemes)

Scammers promise high returns on investments with little risk. Early investors might see returns (from new investors' money), but eventually, the scheme collapses. ***Example:*** A "can't miss" and urgent investment opportunity offering guaranteed returns that far exceed market rates.

Government Impersonation Scams

Scammers pose as government officials, like the IRS, and claim you owe taxes or are entitled to a grant, demanding payment or personal information. ***Example:*** A phone call from someone claiming to be an IRS agent threatening arrest if you don't pay immediately.

Protect yourself from these Common Scams

Employment Scams

Fake job offers require payment for training, supplies, or background checks and ask for personal information to commit identity theft. ***Example:*** A job listing for a "work-from-home" position requiring you to pay an upfront fee for training.

Impersonation Scams (Grandparent Scams)

Scammers impersonate a relative (often a grandchild) in distress, claiming to need money for emergencies, like bail or medical expenses ***Example:*** A caller claiming to be your grandchild asking for money to get out of a legal problem.

Romance Scams

Scammers create fake profiles on dating sites or social media to establish relationships and ask for money for emergencies. ***Example:*** A person you meet online quickly professes love and asks for money to help with medical bills or travel expenses.

Resources

Legacy Bank Support Center – 405-748-2535

Contact the Federal Trade Commission (FTC) at 1-877-FTC-HELP (1-877-382-4357) or visit https://reportfraud.ftc.gov/ to report scams or fraud.

Forward any messages that claim to be from the IRS to phishing@irs.gov.

Report any online scam at to the FBI at https://www.ic3.gov/Home/FileComplaint.

Report unemployment identity fraud by calling Oklahoma's labor department at 405-525-1500