BANK OF
Bird-in-Hand
a full service community bank

Phony Phone Calls and Text Messages

We have recently heard reports from other area community banks that customers are receiving texts, emails, or phone calls claiming internal theft has occurred at their local financial institution and that customer's money may not be safe. The scammers are instructing individuals to withdraw funds from accounts and deposit into bitcoin accounts around Lancaster County. Please be extra vigilant with communications from people or phone numbers you don't recognize. If you've received a message like this regarding your Bank of Bird-in-Hand accounts, please report it by calling 717-929-2263.

Here are four surefire signs that it's a scam:

1. Scammers PRETEND to be from an organization you know.

Scammers often pretend to be contacting you on behalf of the government. They might use a real name, like the Social Security Administration, the IRS, or Medicare, or make up a name that sounds official. Some pretend to be from a business you know, like a utility company, a tech company, or even a charity asking for donations.

They use technology to change the phone number that appears on your caller ID. So the name and number you see might not be real.

2. Scammers say there's a PROBLEM or a PRIZE.

They might say you're in trouble with the government. Or you owe money. Or someone in your family had an emergency. Or that there's a virus on your computer.

Some scammers say there's a problem with one of your accounts and that you need to verify some information.

Others will lie and say you won money in a lottery or sweepstakes but have to pay a fee to get it.

3. Scammers PRESSURE you to act immediately.

Scammers want you to act before you have time to think. If you're on the phone, they might tell you not to hang up so you can't check out their story.

They might threaten to arrest you, sue you, take away your driver's or business license, or deport you. They might say your computer is about to be corrupted.

4. Scammers tell you to PAY in a specific way.

They often insist that you pay by using cryptocurrency, by wiring money through a company like MoneyGram or Western Union, or by putting money on a gift card and then giving them the number on the back.

Some will send you a check (that will later turn out to be fake), then tell you to deposit it and send them money.

How To Avoid a Scam

Block unwanted calls and text messages. Take steps to block unwanted calls and to filter unwanted text messages. Make sure your phone numbers (both landline and cell phone) are listed on the National Do Not Call Registry.

Don't give your personal or financial information in response to a request that you didn't expect. Honest organizations won't call, email, or text to ask for your personal information, like your Social Security, bank account, or credit card numbers.

If you get an email or text message from a company you do business with and you think it's real, it's still best not to click on any links. Instead, contact them using a website you know is trustworthy. Or look up their phone number. Don't call a number they gave you or the number from your caller ID.

Resist the pressure to act immediately. Honest businesses will give you time to make a decision. Anyone who pressures you to pay or give them your personal information is a scammer.

Know how scammers tell you to pay. Never pay someone who insists you pay with cryptocurrency, a wire transfer service like Western Union or MoneyGram, or a gift card. And never deposit a check and send money back to someone.

Stop and talk to someone you trust. Before you do anything else, tell someone — a friend, a family member, a neighbor — what happened. Talking about it could help you realize it's a scam.