PEOPLES BANK & TRUST

P. O. Box G • Troy, MO 63379 • (636) 528-7001 • FAX (636) 528-7016 • www.pbtc.net

At Peoples Bank & Trust Co., we value security. This includes doing what we can to help protect our customers from the many scams that are prevalent in today's society. Below is information to help protect you from scams, but a good rule of thumb is:

"If it sounds too good to be true, it probably is!"

NEVER:

- Give payment instructions over the phone unless you initiated the phone call.
  - *Legitimate loan companies will not call to make a loan.*
  - *Requests for money to be sent in advance to cover "processing" for a prize or to be sent overseas or large US cities is a sure sign of a scam.*
  - *You should never have to pay a fee before receiving something free.*
- Give out personal information, PIN numbers or online banking login information over the phone to an unknown company or person.
  - *ASK yourself: Have you ever met this person, in person?*
  - *ASK for the company's name and address along with a phone number where they can be reached at a later time and talk to a close friend or relative.*
- Automatically trust websites. Look for security features such as a padlock in the address bar and check out the name of the company before making a purchase.
- Automatically trust a hyperlink. Before clicking, hover over it and ensure it displays the same information as to where the link should take you.
- Trust a computer pop-up or blue screen
  - *A common scam is a computer pop-up/blue screen asking you to call a number to unlock your computer.*
  - *Take your computer to a local computer repair shop to check it out.*
- Trust a caller requesting money is who they claim to be.
  - *If a caller claims to be family in trouble, verify the situation with a family member before sending money.*

BEWARE:

- Of encounters and "friend request" on social media such as Twitter and Facebook.
  - *Never say that you are a widow/widower or live alone anywhere online.*
  - *Be leary of someone online that starts asking to talk offline or asks for personal information or money, especially if you have never met them in-person.*
  - *If someone you met online starts professing their love very quickly – this is a sign of a scam.*
- Of a phone call from an unknown company/person asking for money or personal information such as credit card, bank account or Social Security numbers.
  - *Why would someone you've never met, need this information over the phone?*
  - *Don't just trust a company – Research them!*
- Of phone calls claiming that you won a prize. You can't win something if you didn't enter.
- Of high pressure tactics that attempt to convince you of something you need, but you didn't initiate the request.
- Of calls claiming to be the Internal Revenue Service.
  - *The IRS DOES NOT initiate phone calls demanding immediate payment by credit card, debit card, gift card or wire transfer.*
  - *The IRS sends all notices of payment due by mail.*
  - *If you are called and are concerned that you might actually owe money, hang up and call the IRS directly at 800-829-1040.*
- Of calls claiming to be Microsoft Tech Support, they do not make calls asking for information.
- Of trial periods or low cost offers, there is usually a hidden cost or cancellation deadline.

WE RECOMMEND:

- **TALKING** to family and close friends to get advice before giving out information or making a large purchase.
- **SIGNING** UP for the Do-Not-Call-Registry at www.donotcall.gov or (888) 382-1222.
- **TAKING** time before making a decision – legitimate companies won't pressure you to make a snap decision.
- **REPORTING** fraud to agencies such as the Federal Trade Commission: (877) 382-4357 or ftc.gov/complaint.
- **CALLING** PB&T if you feel your financial information has been compromised at (636) 528-7001 during normal business hours.