OPPORTUNISTIC FRAUDSTERS

Fraudsters are notorious for finding ways to scam people, especially when noteworthy, global or national events occur. We've seen a dramatic increase in fraud following natural disasters, civil unrest, economic uncertainty, pandemics, etc. These types of events create ample opportunities for dishonest individuals and criminal organizations to prey on people's anxieties through fear, urgency and isolation.

In more high-stress situations, be extra cautious of:

- **Business Email Compromise** – victims receive an email they believe is from a company they normally conduct business with, but this specific email requests funds be sent to a new account or otherwise alters the standard payment practices. It targets both businesses and individuals who perform legitimate funds transfer requests.
- **Account Takeover** – occurs when criminals successfully gain access to a person's online account(s), usually ones that contain either financial information or personally identifiable information.
- **Bank Imposter Scams** – victims receive a call, email or text that appears to come from their financial institution that indicates a problem with an account or transaction and direct them to click a link or call a given number.
- **Government Imposter Scams** – victims receive a call, email or text that appears to come from a government agency (IRS, FBI, FDIC, etc.) demanding payment or something bad will happen.
- **Investment Scams** – victims are lured with promises of high returns when investing in cryptocurrency, precious metals and private stock offerings without fully understanding the risks. Investment scams may be tied to romance scams or grandparent scams where someone unknowingly transfers assets to a fraudster.

We will never call, email, or text and ask you to share your personal information, card, account number, password, or PIN. **If you are pressured to send money and not tell anyone, including the bank, call Heritage Bank immediately at 800.455.6126.**

Heritage BANK