AVOID BUSINESS EMAIL COMPROMISE SCAMS

Fraudsters will take advantage of any opportunity to steal your money and personal information.

Business email compromise (BEC) is a scam that targets anyone who performs legitimate funds transfers. In a typical BEC scheme, the victim receives 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.

To protect yourself from this fraud, watch for these red flags:

- Unexplained urgency
- Last minute changes in wire instructions or recipient account information
- Last minute changes in established communication platforms or email account addresses
- Communications only in email and refusal to communicate via telephone or online video platforms
- Requests for advanced payment of services when not previously required
- Requests from employees to change direct deposit information

The FBI also recommends the following tips to help protect yourself and your assets:

- Be skeptical of last minute changes in wiring instructions or recipient account information
- Verify any changes and information via the contact information on file—do not contact the vendor through the number provided in the email
- Ensure the URL in emails is associated with the business it claims to be from
- Be alert to hyperlinks that may contain misspellings of the actual domain name
- Verify the email address used to send emails, especially when using a mobile or handheld device, by ensuring the sender's email address appears to match who it is coming from

If you discover you are the victim of a fraudulent incident, immediately contact Heritage Bank at 800.455.6126 to report the fraud and request a recall of funds.

As soon as possible, file a complaint with the FBI's Internet Crime Complaint Center at www.ic3.gov. For business email or personal email account compromise victims, please visit bec.ic3.gov.

Heritage BANK

Information provided by the FDIC