Stay Alert: COVID-19 Related Scams

- The FBI issued a PSA on March 20, 2020
- Scammers are leveraging the COVID-19 pandemic to steal money and/or personal information
- Be on the lookout for:
  - Fake CDC emails
  - Phishing emails
  - Counterfeit treatments or Equipment

- Phishing emails may claim to be related to:
  - Charitable contributions
  - General Finance Relief
  - Airline & Travel refunds
  - Fake cures, vaccines and testing kits

- Use "Good Cyber Hygiene" for Emails & Robo Calls:
  - Do NOT click links or open attachments from senders you don’t recognize
  - Do NOT provide your user name, password, or PII
  - Always verify the web address of legitimate websites and manually type them into your browser
  - Check for misspellings or wrong domains within a link
    EXAMPLE: address that ends in "gov" or "com"

For more information, click here.