WHAT SHOULD I KNOW ABOUT RECENT FRAUD TRENDS CONCERNING COVID-19 or GOVERNMENT STIMULUS PROGRAMS?

During times of crisis, cybercriminals and nation-state actors often exploit financial institutions and their customers for financial or political gain. People are subject to scams because fraudsters prey on fear and interest in COVID-19. Below are some reminders to increase awareness and to help combat against fraud.

- The institution's brand might be used in a fraudulent alert to customers. These fraudulent alerts may state that the customer's bank account has been temporarily suspended. The victim may receive a link that looks like your bank's login screen, encouraging them to log in with their banking username and password.
- When receiving emails, be extra cautious about clicking links and providing sensitive or confidential information. Be extra vigilant to follow secure cyber practices:
    - Do not click on attachments or links from individuals or organizations that you are not expecting or from someone you do not know.
    - Pay close attention to email and web addresses. Look for misspellings, grammar mistakes or other red flags.
    - Hover the mouse cursor over hyperlinks to see where they lead.
    - Avoid messages that urge you to *act now*. This sense of urgency is meant to pressure people into making irrational decisions.
- Please be cautious of communications with the following or similar subjects:
    - Obtaining U.S. government funding related to Coronavirus relief.
    - Check for an updated Coronavirus map in your city.
    - Coronavirus infection warnings from local school districts/governmental entities.
    - Keep your children safe from Coronavirus.
    - Raise funds for Coronavirus victims – (If you wish to donate money, consider only working with known and established organizations and donate through their official websites or phone numbers. Avoid responding directly to email solicitations.)