Increased Cyber Activity During Times of Crisis

During times of crisis, cybercriminals often exploit financial institutions and their customers for financial or political gain.

Be aware of the following:

1. Social engineering schemes remains the top method of cyber attacks. **Social engineering** is the art of manipulating people so they give up confidential information.

2. Be aware that your institution's logo/brand might be used in a fraudulent alert. These fraudulent alerts may state that your bank account has been temporarily suspended. The victim (you) may receive a link that looks like your bank's login screen, encouraging you to log in with your banking username and password.

3. Dis-information campaigns are already underway. You should only rely on government and well-established news sources for credible information such as the CDC, the World Health Organization (WHO), and the Department of Homeland Security. Be wary of unreliable websites and random social media posts.

4. Scams are preying on fear and interest in COVID-19. Be extra cautious about clicking links and providing sensitive or confidential information.
    a. Do not click on attachments or links from individuals or organizations that you are not expecting or from someone you do not know.
    b. Pay close attention to email and web addresses. Look for misspellings, grammar mistakes or other red flags.
    c. Hover the mouse cursor over hyperlinks to see where they lead.
    d. Avoid messages that urge you to *act now*. This sense of urgency is meant to pressure you into making irrational decisions.

5. Be cautious of communications with the following or similar subjects:
    a. Obtaining U.S. government funding related to Coronavirus relief.
    b. Check for an updated Coronavirus map in your city.
    c. Coronavirus infection warnings from local school districts/governmental entities.
    d. Keep your children safe from Coronavirus.
    e. 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.)