COVID-19 UPDATE

CORONAVIRUS-RELATED SCAMS - BE AWARE!

Malicious cyber actors could take advantage of public concern surrounding COVID-19 by conducting phishing attacks and disinformation campaigns.

Account Fraud and Phishing Attacks on the Rise

Fraudsters are impersonating health organizations, such as WHO and CDC, to lure victims into clicking on links or attachments and providing sensitive information in order to steal login credentials and money and to launch malware.

Some scams use fear-based language such as “Outbreak in your area,” “Updated list of new cases,” or “Safety Measures” to get victims to react quickly.

Other scams include bogus online purchases, such as vaccines or supplies, investment opportunities, and charitable donations.

NOTE: *BOK Financial will never request your username and passwords, full account numbers, or security questions over the phone. Always validate any requests using a trusted, known phone number or email address to inquire directly.*

AVOID UNSOLICITED EMAILS

CHECK THE LINK BEFORE YOU CLICK

VALIDATE THE SENDER’S EMAIL ADDRESS

NEVER PROVIDE CREDENTIALS

CALL TO VERIFY ANY REQUESTS THAT SEEM VALID

THINK BEFORE YOU CLICK

RESOURCES:

- Department of Homeland Security I CISA: “Risk Management for Novel Coronavirus (COVID-19)”
- Federal Trade Commission: “Coronavirus: Scammers follow headlines”

SECURE TOGETHER.