COVID-19: Security Alert

Protecting yourself from phishing attempts

One of the most common scams are phishing attempts. Phishing is when an imposter impersonates health organizations and businesses to gather personal and financial information or sell fake test kits, supplies, vaccines, or cures for COVID-19. They might impersonate the Bank in an email, phone call, or text, asking a person to confirm their information or saying they have won something—and it might appear legitimate. An example of a phishing attempt:

- You get an email that appears to be from Flushing Bank. The email asks you to reply or click a link, which takes you to a website that looks like flushingbank.com, where you'll be asked to give your username, password, account number, personal identification number (PIN), Social Security number, or other personal information.

Protecting yourself from other common COVID-19 scams

Other common COVID-19 fraud-related scams to be aware of include:

- **Stimulus check or economic relief scams**. Scammers state that you can get more money from the government – or get your stimulus check faster – if you share personal details and pay a small "processing fee." The government will NOT ask for a fee to receive these funds, nor will they ask for your personal or account information.
- **Charity scams**. Fraudsters seek donations for illegitimate or non-existent organizations.
- **Provider scams**. Scammers impersonate doctors and hospital staff, claim to have treated a relative or friend for COVID-19 and demand payment for treatment.
- **Bank/FDIC scams**. Scammers impersonate FDIC or bank employees and falsely claim that banks are limiting access to deposits or that there are security issues with bank deposits.
- **Investment scams**. Often styled as "research reports," fraudsters claim that products or services of publicly traded companies can prevent, detect, or cure COVID-19.

Flushing Bank will never make or send unsolicited calls, emails, or texts asking you to provide personal information.

If you are contacted, never share any personal information, including:

- Your verification codes, usernames, passwords or other online account credentials
- Your social security, account numbers, debit/credit card numbers, or PIN

If you think you have shared your personal information or if you notice suspicious activity on your account, please contact us at 1-800-581-2889.