HOW TO DEFEND YOURSELF AND STAY SAFE AMID COVID-19 SCAMS

Sterling Bank and Trust, FSB ("Sterling") would like to take this time to warn our customers to remain vigilant on an increase in potential Fraud Schemes and Scams that may be related to the Coronavirus Disease (COVID-19). These Fraud Schemes and Scams may come in a variety of forms including phishing emails with malicious links and attachments or other methods that may attempt to trick victims into revealing sensitive financial and personal information. These Fraud Schemes and Scams could also come in the form of requests for donations to fake charities. Please exercise your due diligence when opening or responding to any phone call, email, social media or text related to COVID-19.

Some examples of known or suspected Scams associated with COVID-19 activity:

- Testing or Treatment Fraud: Fraudsters that may be selling fake at-home test kits or that may be offering to sell fake cures, vaccines, and advice on unproven treatments for COVID-19.
- Supply or Product Fraud: Fraudsters that may be creating fake websites, social media accounts, and email addresses claiming to sell medical supplies currently in high demand, such as surgical masks.
- Medical Provider Fraud: Fraudsters that may contact people by phone, social media, text or email pretending to be doctors or hospitals that have treated a friend or relative for COVID-19, and demanding payment for that treatment.
- Charity Fraud: Fraudsters that attempt to solicit donations for individuals, organizations, groups, or areas affected by COVID-19.
- Public Health Organizations Fraud: Fraudsters that pose as national and global health authorities, including the World Health Organization (WHO) and the Centers for Disease Control and Prevention (CDC).
- Investment Fraud: Fraudsters that may offer online or social media promotions seeking investors for products or services that allegedly can prevent, detect, or cure COVID-19.

Some important tips you need to know:

- Avoid clicking on links found in unsolicited text or emails and be wary of attachments. Email and text scammers often try to elicit a sense of fear or urgency in victims to trick them into providing personal information.
- Use only trusted sources, such as legitimate government websites for the most up-to-date fact based information about COVID-19.
- Do not reveal personal information or financial information in an email or text, and do not respond to solicitations for this information.
- Always verify a charity before making donations by contacting the charity directly or verify the charities existence. Do not donate if the solicitor is using high-pressure tactics or insists on a cash donation.
- Trust your instincts - if an email, text or attachment seems suspicious, do not open it. Don't let your curiosity put you, your personal data, or computer at risk

REMEMBER: Sterling will never ask you for your sensitive or unique personal information by e-mail.

If you think you might be a victim, report it to Sterling at:
https://www.sterlingbank.com/departmentcontact.html?dep=w_reportfraud.
Customer service representatives are available to discuss your accounts at 1-800-944-BANK (2265).

Sterling bank & trust

SBT advantage bank℠

Member FDIC