PLEASE READ THIS FRAUD ALERT

The FBI reports seeing a rise in fraud schemes related to the COVID-19 pandemic and is giving consumers advice on how to protect themselves from scammers who are leveraging the COVID-19 pandemic to steal money, personal information or both.

Protect yourself and do your research before clicking on links purporting to provide information on the virus; donating to a charity online or through social media; contributing to a crowdfunding campaign; purchasing products online; or giving up your personal information in order to receive money or other benefits. The FBI advises you to be on the lookout for the following.

FAKE CDC EMAILS: Watch out for emails claiming to be from the Centers for Disease Control and Prevention or other organizations claiming to offer information on the virus. **DO NOT CLICK LINKS OR OPEN ATTACHMENTS YOU DO NOT RECOGNIZE.** The links can deliver malware to your computer to steal personal information or lock your computer and demand payment.

PHISHING EMAILS: Look out for phishing emails asking you to verify your personal information in order to receive an economic stimulus check from the government. The government is not seeking personal information through email. Other phishing emails may also claim to be related to:

Charitable contributions
General financial relief
Airline carrier refunds
Fake cures and vaccines
Fake testing kits

COUNTERFIET TREATMENTS OR EQUIPMENT: Be cautious of anyone selling products that claim to prevent, test, diagnose or cure COVID-19. More information on unapproved or counterfeit protective equipment can be found at www.cdc.gov/niosh. You can also find information on the U.S. Food and Drug Administration website, www.fda.gov and the Environmental Protection Agency website, www.epa.gov.

If you are looking for accurate and up-to-date information on COVID-19, the CDC has posted extensive guidance and information that is updated frequently. Best sources for authoritative information on COVID-19 are www.cdc.gov and www.coronavirus.gov. You may also consult your primary care physician for guidance.

In conclusion; remember the following tips:

- Do not open attachments or click links in emails from senders you don't recognize.
- Do not provide your username, password, date of birth, social security number, financial data or other personal information in response to email or robocall.
- Always verify the web address of legitimate websites and manually type them into your browser.
- Check for misspellings or wrong domains within a link (for example, an address that should end in a "gov" ends in "com" instead.

If you believe you are the victim of an internet scam or cyber crime or want to report suspicious activity, please visit the FBI's Internet Crime Complaint Center at www.ic3.gov.