Office of the
CHIEF INFORMATION
SECURITY OFFICER
State of Texas

TLP: White

SUBJECT: FBI PSA: FBI Sees Rise in Fraud Schemes Related to the (COVID-19) Pandemic with Example Emails
TLP: WHITE

DATE(S) ISSUED:
March 20, 2020

OVERVIEW:
There has been a marked increase in the number of phishing attempts using COVID-19 (Coronavirus) themes. These threat actors are capitalizing on the current situation.

These phishing attempts may impersonate trusted, official sources such as the U.S. Center for Disease Control (CDC), the World Health Organization (WHO), or mimic agency or company specific emails related to COVID-19.

Fake CDC Emails

Watch out for emails claiming to be from the Centers for Disease Control and Prevention (CDC) or other organizations claiming to offer information on the virus. Do not click links or open attachments you do not recognize. Fraudsters can use links in emails to deliver malware to your computer to steal personal information or to lock your computer and demand payment. Be wary of websites and apps claiming to track COVID-19 cases worldwide. Criminals are using malicious websites to infect and lock devices until payment is received.

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. While talk of economic stimulus checks has been in the news cycle, government agencies are *not* sending unsolicited emails seeking your private information in order to send you money. Phishing emails may also claim to be related to:

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

Counterfeit Treatments or Equipment

Be cautious of anyone selling products that claim to prevent, treat, diagnose, or cure COVID-19. Be alert to counterfeit products such as sanitizing products and Personal Protective Equipment (PPE), including N95 respirator masks, goggles, full face shields, protective gowns, and gloves. More information on unapproved or counterfeit PPE 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. Report counterfeit products at www.ic3.gov and to the National Intellectual Property Rights Coordination Center at iprcenter.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. The best sources for authoritative information on COVID-19 are www.cdc.gov and www.coronavirus.gov.

The FBI is reminding you to always use good cyber hygiene and security measures. By remembering the following tips, you can protect yourself and help stop criminal activity:

- Do not open attachments or click links within 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 an 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).

For the full FBI PSA, visit: https://www.ic3.gov/media/2020/200320.aspx

For examples of identified COVID-19 phishing email attempts, please review the attachment.

Texas Department of Information Resources

Transforming How Texas Government Serves Texans