NEWS ALERT
Eastern Contractors Association, Inc. • 6 Airline Drive, Albany, NY 12205 • 518-869-0961

March 26, 2020

FRAUD ALERT

Several departments/agencies have advised that COVID-19 has fostered malicious behavior. Be aware that criminals are attempting to exploit COVID-19 worldwide through a variety of scams.

There have been reports of:

- Individuals and businesses selling fake cures for COVID-19 online and engaging in other forms of fraud
- Phishing emails from entities posing as the World Health Organization or the Centers for Disease Control and Prevention
- Malicious websites and apps that appear to share virus-related information to gain and lock access to your devices until payment is received
- Seeking donations fraudulently for illegitimate or non-existent charitable organizations

During these trying times, your profession continues to provide important services to our State and the Nation.

The FBI has released a public safety announcement on this issue. See page 2-3 of this News Alert. Additional information is available on the US Dept. of Justice web page:

- http://www.justice.gov/coronavirus

Criminals will likely continue to use new methods to exploit COVID-19 worldwide.

If you think you are a victim of a scam or attempted fraud involving COVID-19, you can report it without leaving your home though a number of platforms:

- Contact the National Center for Disaster Fraud Hotline at 866-720-5721 or via email at disaster@leo.gov
- Report it to the FBI at www.tips.fbi.gov
- If it's a cyber scam, submit your complaint through www.ic3.gov

A public alert by the FBI follows:

Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

March 20, 2020

Alert Number

I-032020-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office**.

Local Field Office Locations: www.fbi.gov/contact-us/field

FBI Sees Rise in Fraud Schemes Related to the Coronavirus (COVID-19) Pandemic

Scammers are leveraging the COVID-19 pandemic to steal your money, your personal information, or both. Don't let them. 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 (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

Federal Bureau of Investigation
Public Service Announcement

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. You may also consult your primary care physician for guidance.

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).

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