

## Avoiding COVID-19 Scams

Scammers, fraudsters, and other criminals are taking advantage of rapidly changing data and facts associated with COVID-19, both in the workplace and in our homes. Government agencies, corporations, and news outlets continue to warn individuals to be mindful of increased fraudulent activities during these uncertain times.

These scams, which can be sent via email, text message, and social media claim to provide COVID-19 updates, sell products, ask for charitable donations, or reference government aid packages. These messages appear to be legitimate in nature but seek to fraudulently obtain personal information, financial gain, and create panic. Use these tips to identify and avoid scams:

- **Watch for emails claiming to be from the Centers for Disease Control and Prevention (CDC)** or experts claiming to have inside information on the virus. There are currently no vaccines, potions, lozenges, or other prescriptions available online or in-store to treat or cure COVID-19.
- **Do your homework prior to donating to charities or crowdfunding sites.** Confirm the validity of the organization as fraudsters are now advertising fake charities. Do not let anyone rush you into a donation, particularly those who ask for cash, gift cards, or wiring of funds.
- **Do not click on links or open attachments from sources you do not know.** Cybercriminals are using the COVID-19 headline as a tactic to spread viruses and steal information. Do not provide personal information, payment information or sensitive workplace information via suspicious email addresses.
- **Be suspicious of urgent demands and emergency requests.** The health and safety of you and your family is the top priority. Do not fall for scammers threatening fees or fines, cancelled deliveries, and health concerns in exchange for financial gain.
- **If it sounds too good to be true, it likely is.** Many individuals have begun to receive robo-calls and social media requests for social security numbers, banking information, and gift cards. Scammers promise high paying work from home opportunities, free sanitation and cleaning, as well as COVID-19 protection in exchange for payment and sensitive information.
- **Be mindful of scammers using government aid packages for criminal gain.** Lawmakers have announced plans to send Americans checks to assist with the financial burden of the virus, with details still in discussion. The government will not request payment, nor will anyone reach out requesting personally sensitive health or financial information in exchange for financial support.
- **Obtain your news from a trusted source.** Be mindful of text message scams, social media polls and fraudulent email accounts sharing false information to create panic. Before acting on information, review its source and check a trusted news outlet to confirm its validity.

When in doubt, ask a coworker, family member, or friend for their opinion. Two sets of eyes are better than one. If you believe you have fallen victim of a scam, call your local police at their non-emergency number and consider reporting to the FBI's IC3 Internet Crime Database.

If you have any questions or concerns, please do not hesitate to contact our office.