UNITEDHEALTH GROUP®

COVID-19 Fraud: Tips to Follow and Schemes to Avoid

Unfortunately, fraudulent schemes quickly emerge during times of crisis and catastrophe. It is no different with the COVID-19 pandemic.

Listed below are tips on how to avoid being a victim of COVID-19 fraud, examples of fraudulent schemes to be aware of, links to COVID-19 resources, and information on where to report potential fraud.

Tips: Don't Be a Victim of COVID-19 Fraud:

- Don't trust unsolicited phone calls, or anyone knocking on your door offering you a COVID-19 test or vaccine.
- Be wary of unsolicited emails or social media ads offering information, supplies, or treatment for COVID-19 or requesting your personal information for medical purposes.
- As of April 21, 2020, no vaccines, pills, potions, lotions, lozenges or other prescription or over-the-counter products are available to treat or cure Coronavirus disease 2019 (COVID-19) — online or in stores. Remember, if there is a medical breakthrough, you won't hear about it for the first time through an email, online ad, or unsolicited sales pitch.
- Only a physician or other qualified health care provider should recommend or approve requests for COVID-19 testing.
- Don't click on links or open attachments from unknown or unverified sources. Even if it looks legitimate, take the extra steps to verify the identity of any company, charity, or individual contacting you about COVID-19.
- Make sure your anti-virus and anti-malware software is operating and up to date on your computer.

Examples of COVID-19 Related Fraud Schemes:

- **Treatment Schemes:** Trying to sell fake cures and fake vaccinations for COVID-19.
- **Counterfeit Supply/Product Schemes:** Creating fake shops and websites selling medical supplies that are in high demand (surgical/face masks, 'test kits', thermometers, etc.). The supplies are not real, and once the items are paid for, no supplies will be delivered. Or, if delivered, the supplies may be damaged, expired, counterfeit, or items that may not be safe to use.
- **Phishing Schemes:** Sending phishing emails and texts purporting to be national or global health authorities (i.e. CDC or WHO) or legitimate companies. They may look very real, but they are not. They may also try tricking you into opening fake websites impersonating information sites (i.e. Johns Hopkins or government websites). They are trying to trick you into downloading malware or providing personal identifying and

financial information. Once you click on an inappropriate link, or open an attached document, the malware or virus may now be on your computer or phone.

- **Provider Schemes:** Contacting people by phone or email, pretending to be doctors, clinics, or hospitals that have treated a friend or relative for COVID-19 and are demanding money for payment.
- **Bogus Charity or Relief Schemes:** Requesting donations for individuals or groups that may be in an affected area for COVID-19.
- **Mobile App Schemes:** Creating or manipulating apps designed to track COVID-19 but the app will include malware and will compromise users' devices and personal information.
- **Phone Calls (Telemarketing, Robocalls, etc.) Schemes:** Requesting personal information, passwords, selling 'test kits' or supplies, or asking for donations.
- **Investment Schemes:** Offering and promoting products or services claimed to prevent, detect, or cure COVID-19, and that the stock of these companies will dramatically increase. These promotions are often styled as "research reports."
- **Medicare Schemes:** Targeting Medicare beneficiaries through telemarketing, social media and even in-person, door-to-door contact. Offering a COVID-19 test, most likely a "free" test in exchange for providing personal information (i.e., Medicare ID, other insurance ID, SS#, etc.).

Resources for COVID-19 Updates:

The United States Department of Justice Coronavirus (COVID-19)
https://www.justice.gov/coronavirus

For the most up to date information on COVID-19, visit World Health Organization (WHO) Coronavirus (COVID-19) and Centers for Disease Control (CDC) and Prevention.gov

For online resources for donating wisely, visit the Federal Trade Commission (FTC) website.

For information on how to avoid investment fraud, visit the U.S. Securities and Exchange Commission (SEC) website.

Reporting Potential COVID-19 Fraud

Suspicious Emails at Work: Do not open or click on any links within suspicious emails or texts. Check for resources on the Hub pertaining to your example, for instance: Is It Phishing or Junk Mail

Report Suspicious Activity!

You do not need to contact the fraud hotline for phishing activities. Use the appropriate links above.

UHG Employees with Coverage through UHC Report Suspect COVID-19 Healthcare Fraud: If you suspect fraud or suspicious activity, or you gave out your private or protected health information inadvertently, report on The Hub under Report Suspected Health Care Fraud, Waste or Abuse. If you are unable to report via the link above, you may contact the number on the back of your ID Card or the UHC Member Internal Fraud Hotline toll-free number at 1-866-242-7727.

Resources for Reporting Non-Healthcare COVID-19 Related Fraud: The Department of Justice has enacted the ***National Center for Disaster Fraud Hotline***. If you feel you have been a victim of a COVID-19 scam, you are asked to call **1-866-720-5721** or email disaster@leo.gov.