8 February 2021

COVID-19 Scams
Heroes and Zeroes: Pandemic Crystallizes Best and Worst

LtCol Bradley T. Farrar, USMCR

A little over a year ago in the United States if you walked into a bank wearing a mask the teller might have hit the panic button. Today, if you enter a bank without a mask on, the same teller might hit the panic button. The changes in our day-to-day routines in the last few months are too numerous to recount.

The first case of the COVID-19 ("Coronavirus Disease" identified in 2019) was reported to have occurred in November 2019 in the Hubei province of China. From "Patient Zero" it has traveled the globe, to date resulting in 105,599,679 cases, and 2,299,516 deaths. Those who keep the dreary statistics in this area also report that there have been 77,300,048 "recoveries."[1] There are questions about the accuracy of such numbers, but with a problem as widespread as this one, perfection may be unattainable.

As of the date of this publication there have been 27,282,497 confirmed cases of COVID-19 in the United States, 467,434 deaths, and 17,034,751 recoveries. Those numbers became outdated almost as soon as they were typed.

Many refer to the pandemic as unprecedented…but global health crises have been with us since the beginning of time.

The earliest recorded pandemic occurred around 430 B.C. during the Peloponnesian War.

The Justinian Plague that began in 541 A.D. and continued for two centuries, killed fifty million people, or slightly more than a quarter of the world's population at that time.

The Black Death in the 1300s A.D. wiped out one-third of the world's population.

Leprosy, cholera, smallpox, the bubonic plague, measles, the Russian Flu, Spanish Flu, and untold other epidemics and pandemics (the latter spreading beyond a country's borders, while the former is contained to one nation) throughout the centuries have taken an incalculable toll on human population. And in recent history, the Asian Flu, HIV/AIDS, SARS, H1N1, Ebola and Zika and other diseases worked their way around the globe, resulting in significant losses of life in many areas.[2]

There have been great stories of heroes in the medical profession, tirelessly working to find a cure, or at least a treatment, for a disease that has tested the limits of scientific achievement.

---

[1] Coronavirus Update (Live): 105,599,679 Cases and 2,299,516 Deaths from COVID-19 Virus Pandemic - Worldometer (worldometers.info)

[2] Pandemics That Changed History: Timeline - HISTORY

But not every account is an inspiring case of self-sacrifice and compassion brought about by this health emergency. The opportunists among us plot and scheme, operating under the belief that one should, "never let a good crisis go to waste." Or, as some say in the competitive world of free enterprise, "if you can't be part of the solution, there's still good money to be made from prolonging the problem." Follow the money.

This article explores some of the more common Coronavirus scams, how to spot them, how to protect yourselves from exploitation, and where to report such activity to try to help others.

The Scams

The U.S. Department of Health and Human Services Office of Inspector General, the Federal Trade Commission, state and local watchdog agencies and others are warning of innumerable scams related to COVID-19, its treatment, prevention, vaccines and other virus-related issues.

Tactics include telemarketing, robocalls, text messages, social media, and even door-to-door efforts all designed to separate you from your money, with little, and most often, nothing in return. In addition to spending money on bogus products and services, scammers use customers' personal information to pursue other illicit activities through identity theft.

As with any mission, let's first get a better understanding of the operational environment. Just what are some of the scams you might expect to see?

The following is a non-exhaustive list of some of the unfair, deceptive, and in many cases, malicious Coronavirus schemes those with impure motives hope to exploit during this time of uncertainty, anxiety, and isolation:

- **Testing and Prevention Scams**
    - Free test kits overnight (playing on the crisis nature of the virus and immediate need for testing).
    - Delivery of sanitation and hygiene supplies overnight ("…you've got to clean, and clean now!").
    - Offers of ineffective COVID-19 tests for Medicare patients.
    - *Internet* "anti-virus" protection—in a pernicious twist on a *double entendre,* scammers promise to provide a "Corona-Antivirus" product to protect your computer from hackers, while also protecting you from the Coronavirus…so long as the app is running.
    - A software program that promises to identify people in your neighborhood who are infected by COVID-19, while stealing your private credit card information.

- Door-to-Door Sales of Test Kits—a scam that actually violates social distancing precautions.
- "COVID-19 testing appointments" scam designed to get people out of their homes at specific times to more easily steal their personal information and property.
- Free COVID-19 testing kits for diabetes patients—seeking personal and health insurance information.
- COVID-19 tracker app virus—instead of downloading an app to help you track the worldwide and local spread of the virus, this software steals your personal identifying information and money.
- Door-to-door "CDC" workers offering free test kits.
- Coronavirus tracking malware.
- Mandatory online COVID tests—under the guise of the U.S. Department of Health and Human Services, this scam offers "mandatory" online COVID-19 testing.
- Pop-up Coronavirus Testing Sites—used to obtain health insurance, SSNs and "testing fees."
- At-home Coronavirus testing by "trained professionals."
- Cleaning services to eliminate COVID from the air.
- Herbal defense against Coronavirus.
- Homeopathic drugs to prevent and cure COVID-19.
- Essential oils to treat and prevent Coronavirus.
- Toothpaste "that can kill Coronavirus."
- Home visit test scams.
- Fake drive-through testing sites.

- **PPE and Mask Scams**
  - Face masks and PPE when you download certain apps.

- Sales of N95 Masks—problem is, they take your order and the money, but the masks are never sent.

- **Cure or Treatment Scams**

  - False claims and testimonials of miracle at-home cures, such as

    - Essential oils
    - Aromatherapy
    - "Holistic" clinics
    - Herbs
    - COVID-curing CBD Oil

  - Calls to reserve "your COVID-19 vaccine."

  - Sales of pills to "cure" COVID-19.

  - Bitcoin payments for Coronavirus remedies—promises of nonexistent Coronavirus cures.

  - Fake vaccine kit.

  - Immune stabilizer tincture to cure life-threatening virus.

  - Hemp products to prevent and cure COVID-19.

  - Natural products to prevent and cure COVID-19

  - Other products to cure and prevent Coronavirus.

  - CBD oil to "Crush Corona."

  - Saline therapy to treat and prevent COVID-19.

Worst of the Rest

Some of the catchall scams include:

- Robocalls focusing on health or financial concerns, possible job loss and economic fears.

- Scams that seek your insurance information or that try to get you to commit to some payment.

- Targeting older Americans.

- Health insurance enrollment— ("let's make sure you are enrolled in all programs to which you are entitled…").

- Refinancing mortgages due to "COVID Relief" measures—promising low rates "if you act now."

- Imitating government agencies or trusted institutions to steal your SSN.

- Aid to small businesses with problems in *Google* listings—exploiting the business losses environment caused by COVID.

- Free *iPhone* (if you download malware).

- Pay Day loans. "Get money now with no credit check" to pay overdue bills and relieve financial distress…except that the interest rate is in triple digits and the loan comes due in as little as two weeks. (See details at "Payday Loans, an Anchor Not a Lifesaver," at the website of Legal services Support Team Lejeune, Legal Assistance / Consumer Law folder.)

- Phishing e-mails purportedly from the World Health Organization or the "Centers of Disease Control"—U.S. and international public health agencies spoofed and misused as authorities you normally should be able to trust.

- Complete U.S. census survey in exchange for a stimulus check.

- Free school lunches during the pandemic in exchange for bank information.

- Robocalls threatening you for being caught breaking quarantine, claiming that "the police have a warrant out for your arrest," and if you pay your fine over the phone you will not be arrested.

- Emails actually threatening to infect you with Coronavirus if a bitcoin ransom is not paid.

- Threats from agencies mimicking the Social Security Administration or the IRS to withhold a stimulus check if personal info is not provided.

- Advance Fee Loans—promising relief checks due to COVID financial losses, designed to steal your identity.

- Tech Support—"order confirmation" scam for something you never ordered.

- Website to "track" malicious sites, or scammers offering to protect you from scammers—services designed to prevent the very thing those calling are trying to do to you.

- Phishing emails scaring you into believing you've been exposed to the virus, this Excel attachment encourages you to complete and take to the nearest hospital, downloading a malicious program once opened.

- Texts giving false information about a "national quarantine."

- Fake health insurance coverage scams.

- Virus-related small business funding and loans.

- Free *Netflix* phishing survey.

- FDIC impersonators requesting personal information.

- Student loans "call back" scam.

- Misinformation: National Quarantine warning telling people to stock up on supplies.

- Work from Home Opportunity scams.

- Robocall offering debt consolidation.

- Impersonating Banks scam.

- Fake login to restore bank account.

- Social Security scam.

- COVID-19 defender patches—like nicotine patch, supposedly.

- Fake travel insurance—for your trip that is in jeopardy due to travel restrictions.

- COVID-19 donation requests.

- Financial assistance for small business owners.

- Malware email attachments.

- Phishing email about protecting yourself during COVID-19.

- Low-rate mortgage refinancing.
- COVID-19 grants—prepaid gift care of wire transfer for "grants" of up to $300K.
- Stimulus check phishing message—often uses *Facebook* "friend" to alert you to a pending deposit to your bank account.
- $50,000 for seniors affected by coronavirus—references legitimate entities to request seniors' SSNs.
- Expedited stimulus check receipt scam.
- Bogus *Costco, Netflix* and other popular brand links discount or credit scams.
- Utility shut-off threat—use prepaid debit card to keep utilities from being shut off during the virus.
- Social Security suspension scam—more "older American" scare tactics.
- Gift card donation scam.
- Fake *Instagram* survey reward.
- Cash App "cash flipping"—targets *Twitter* users who tweet celebrity-hosted COVID-19 giveaways. Once they donate, scammers block them and their money is lost.
- Unemployment scam—claims of help for the unemployed, such as debt consolidation or mortgage refinancing.
- Cryptocurrency pandemic essentials scam—"get face masks, hand sanitizer, and medication in exchange for payments in cryptocurrency."
- Vaccine cover-up email scam—prays upon government conspiracy theorists who believe nations are covering up a COVID vaccine and cure.
- CDC vaccine-donation scam.
- Business email compromise scam—a ransomware variant that holds hostage business activities.
- Money "mule" scam—"help me move (stolen) money through a funds wire transfer…commission for you."

    - Grandparent scam—"beloved grandchild in trouble, needs to pay emergency room bill or leave a foreign country in the middle of the pandemic!"

- Paycheck protection loan fee scam—scammers call businesses saying they need to pay a fee to access a paycheck protection loan.
- Doordash COVID-19 bonus check scam—bonus for drivers, but need your phone number (for money transfer via app…).
- Scammers posing as Medicare representatives making calls offering coronavirus test kits.
- Fake coronavirus instructions from the White House.
- Fake hospital email claims to identify "infected staff."
- Email scam offering flight refunds for those whose travel plans have been disrupted.
- Tech support scam exploiting individuals working from home.
- Fake contact tracing scams, with scammers posing as Public Health representatives.
- Scammers posing as energy company workers are praying on public fears about rising utility bills.
- Text messages claim that Target is offering free groceries for customers

What Scammers Want

According to the Federal Trade Commission (FTC), common types of information scammers are after include:

- Passwords
- Social Security numbers
- Account numbers
- Other payment information

All of these COVID-19 scams are intended to steal 1) your personal information, 2) your money, 3) or both.

The Red Flags—How to Spot Scams and How to Protect Yourself

The Federal Trade Commission, the U.S. Department of Health and Human Services, and others suggest you take particular note of any of the following red flags with offers that sound too good to be true:

1. Watch out for anyone who is trying to push you into an immediate action. What's the hurry? If it's such a good deal, it will last until you can do some simple research. Trust, but verified.

2. Be wary of anyone who wants you to use a payment method that has little of no fraud protection. Why do I need to wire money anywhere? When have I ever needed to wire money to someone to conduct business?

3. Be suspicious of any robocall. Do legitimate businesses or agencies typically call me, unsolicited, for any reason?

4. Watch e-mails from anyone you do not know, especially ones that ask you to:

    - Click on a link
    - Download an attachment
    - Or provide a link for you to "log in" to your account

Protect yourself by:

- Not sharing personal information just because someone asks for it.
- Monitoring your bank and credit accounts regularly.
- Protecting your computer using security software.
- Protecting your mobile phone, set the software to automatically update.
- Using complex passwords and changing them often.
- Signing up for fraud alerts on your credit cards and bank accounts.
- Not opening emails from people you don't know.
- Not answering robocalls.
- Not clicking on links from sources you don't know.

- Talking to someone about a possible scam before you take action. The FTC reports that people who talk to someone else about suspicious offers are less likely to lose money than people who don't.
- Not responding to texts, emails or calls from "the government" about stimulus checks.
- Not responding to online offers for home vaccinations and test kits.
- Watching out for emails claiming to be from the CDC or WHO.
- Doing your homework before donating money.
- Watching out for poorly worded e-mails or ones that provide little detail.
- Being suspicious of any unexpected calls or visitors offering COVID-19 tests or supplies. If you receive a suspicious call, hang up immediately.
- Not responding to, or opening hyperlinks in, text messages about COVID-19 from unknown individuals.
- Ignoring offers or advertisements for COVID-19 testing or treatments on social media sites. If you make an appointment for a COVID-19 test online, make sure the location is an official testing site.
- Not giving your personal or financial information to anyone claiming to offer HHS grants related to COVID-19.
- Being aware of scammers pretending to be COVID-19 "contact tracers." Legitimate contact tracers will never ask for your Medicare number, financial information, or attempt to set up a COVID-19 test for you and collect payment information for the test.

Here are some resources if you suspect you have been the victim of a scam, or targeted for one:

- Email suspected scam information to the U.S. Department of Health Services at Covid19Fraud@dhs.gov.
- Fill out a scam report on the BBB's Scam Tracker site.
- File a complaint with your state attorney general or consumer affairs advocate
- Contact the Federal Trade Commissions' ReportFraud.ftc.gov, which shares information with law enforcement
- Call the FBI's tipline, at tips.fbi.gov or 1-800-CALL-FBI; or
- Contact the HHS Office of Inspector General, at tips.hhs.gov or 1-800-HHS-TIPS

If you have been hacked, had your identity stolen or your finances compromised, consider placing a credit freeze on your accounts, and sign up for fraud alerts. The Federal Trade Commission posts a checklist of actions for people who have been the victim of identity theft.

Lastly, if you have been scammed, don't beat yourself up—you are not alone. And the good news is that despite those opportunists and scam artists lurking among the everyday heroes, there are still people you can trust. When in doubt, ask your health care provider, your doctors' offices and their staffs.

And use common sense. Chances are, your judgment is at least as good as the person contacting you in an unsolicited fashion, and you are in control of where you click, who you talk to, and what you do with your personal, financial, health and other information. Guard it as you would your health, and you can avoid the minefield of COVID-19 scams, tricks and traps for the unwary.

###